MONITOR POLSKI

DZIENNIK URZĘDOWY RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 30 października 2019 r.

Poz. 1037

UCHWAŁA NR 125
RADY MINISTRÓW

z dnia 22 października 2019 r.

w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024

Na podstawie art. 68 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) Rada Ministrów uchwala, co następuje:

§ 1. Przyjmuje się Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zwaną dalej „Strategią Cyberbezpieczeństwa", stanowiącą załącznik do uchwały.

§ 2. Członkowie Rady Ministrów oraz organy i jednostki organizacyjne im podległe lub przez nich nadzorowane współpracują z ministrem właściwym do spraw informatyzacji przy realizacji Strategii Cyberbezpieczeństwa.

§ 3. Minister właściwy do spraw informatyzacji przedstawia Radzie Ministrów, w terminie do dnia 30 marca danego roku, informację o realizacji Strategii Cyberbezpieczeństwa.

§ 4. Pierwszą informację o realizacji Strategii Cyberbezpieczeństwa minister właściwy do spraw informatyzacji przedstawi Radzie Ministrów w terminie sześciu miesięcy od dnia wejścia w życie niniejszej uchwały.

§ 5. Traci moc uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.

§ 6. Uchwała wchodzi w życie z dniem 31 października 2019 r.

Prezes Rady Ministrów: *M. Morawiecki*

Załącznik do uchwały nr 125 Rady Ministrów
z dnia 22 października 2019 r. (poz. 1037)

Strategia Cyberbezpieczeństwa

Rzeczypospolitej Polskiej

na lata 2019–2024

Ministerstwo
Cyfryzacji

Spis treści

1. Wstęp – przesłanki do działań zwiększających cyberbezpieczeństwo

Rozwój społeczny i gospodarczy w coraz większym stopniu zależny jest od szybkiego i nieskrępowanego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz sektorze publicznym. Dynamiczny rozwój systemów informacyjnych służy rozwojowi gospodarki narodowej, w szczególności w obszarze komunikacji, handlu, transportu czy też usług finansowych. Z wykorzystaniem technologii cyfrowych tworzących cyberprzestrzeń[1)] kształtowane są relacje społeczne, a usługi w sieci Internet stały się narzędziem do wpływania na zachowania grup społecznych, a także oddziaływania w sferze politycznej.

Każde znaczące zakłócenie funkcjonowania cyberprzestrzeni, czy to o charakterze globalnym, czy lokalnym, będzie miało wpływ na bezpieczeństwo obrotu gospodarczego, poczucie bezpieczeństwa obywateli, sprawność funkcjonowania instytucji sektora publicznego, przebieg procesów produkcyjnych i usługowych, a w rezultacie na ogólnie pojmowane bezpieczeństwo narodowe.

Ochrona systemów informacyjnych oraz przetwarzanych w nich informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów informacyjnych, organów władzy publicznej, organów odpowiedzialnych za bezpieczeństwo narodowe, a także wyspecjalizowanych podmiotów zajmujących się cyberbezpieczeństwem w sferze operacyjnej. Jest to tym istotniejsze, iż Polska jest ściśle powiązana z innymi państwami przez współpracę międzynarodową w ramach takich organizacji jak Unia Europejska (EU), Organizacja Traktatu Północnoatlantyckiego (NATO), Organizacja Narodów Zjednoczonych (ONZ) czy Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE). Współpraca ta odgrywa istotną rolę w reagowaniu na zwiększającą się liczbę incydentów powodowanych nielegalnymi działaniami w cyberprzestrzeni, powodujących rosnące z roku na rok straty materialne i wizerunkowe. W działaniach przestępczych uczestniczą pojedyncze osoby, zorganizowane grupy przestępcze oraz grupy sponsorowane przez instytucje rządowe i siły zbrojne państw prowadzących ofensywne działania w cyberprzestrzeni, ukierunkowane w szczególności na cyberszpiegostwo oraz rozpoznanie zdolności obronnych innych państw.

---

1) Cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848 i 1590), wraz z powiązaniami między nimi oraz relacjami z użytkownikami – zgodnie z art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2017 r. poz. 1932).

2. Kontekst strategiczny cyberbezpieczeństwa w Rzeczypospolitej Polskiej

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 jest kontynuacją i rozszerzeniem działań, podejmowanych przez administrację rządową, mających na celu podniesienie poziomu cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Poprzednie działania obejmowały wejście w życie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560)[2)] oraz przyjęcie przez rząd:

- w roku 2013 Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej,
- w roku 2017 Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 zastępuje Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 przyjęte uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.

Zamierzeniem niniejszego dokumentu jest określenie celów strategicznych oraz odpowiednich środków politycznych i regulacyjnych, mających na celu uzyskanie wysokiego poziomu cyberbezpieczeństwa – czyli przede wszystkim odporności systemów informacyjnych operatorów usług kluczowych[3)], operatorów infrastruktury krytycznej, dostawców usług cyfrowych[4)] oraz administracji publicznej na cyberzagrożenia, a także zwiększenie poziomu ochrony informacji w systemach informacyjnych przez standaryzację zabezpieczeń. Realizacja celów strategicznych ma również wpływać na podniesienie bezpieczeństwa narodowego, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań o charakterze hybrydowym (w tym działań o charakterze terrorystycznym) i szpiegowskim w cyberprzestrzeni.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 jest spójna z prowadzonymi działaniami dotyczącymi systemów teleinformatycznych operatorów infrastruktury krytycznej oraz uwzględnia potrzeby zapewnienia zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych.

Podejmując działania mające na celu wdrożenie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, rząd będzie w pełni gwarantował prawo do prywatności oraz stał na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa.

---

2) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w zakresie swojej regulacji wdraża dyrektywę 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 194 z 19.07.2016, str. 1).

3) Dotyczy operatorów usług kluczowych, o których mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

4) Dotyczy dostawców usług cyfrowych, o których mowa w art. 17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3. Zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024

Strategia uwzględnia w szczególności[5)]:

1) cele i priorytety w zakresie cyberbezpieczeństwa;
2) podmioty zaangażowane we wdrażanie i realizację Strategii;
3) środki służące realizacji celów Strategii;
4) określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym;
5) podejście do oceny ryzyka;
6) działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa;
7) działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa.

Ponadto Strategia uwzględnia międzynarodową współpracę w zakresie cyberbezpieczeństwa.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 wprowadzona w drodze uchwały Rady Ministrów oddziałuje w sposób bezpośredni na podmioty administracji rządowej, a w sposób pośredni, po przyjęciu z inicjatywy Rady Ministrów przepisów prawa powszechnego, na pozostałe podmioty władzy publicznej, przedsiębiorców i obywateli.

5) Art. 69 ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

4. Wizja, cel główny, cele szczegółowe

4.1. Wizja

Pomyślny rozwój Rzeczypospolitej Polskiej, wzrost jej zasobności, efektywności gospodarki, sprawności działania instytucji, podmiotów, w tym i aktywność społeczna oraz codzienne funkcjonowanie indywidualnego członka społeczeństwa, są związane ze sprawnym i bezpiecznym działaniem systemów informacyjnych i środków komunikacji elektronicznej. Dlatego w ramach działań zaplanowanych w Strategii Cyberbezpieczeństwa do roku 2024 rząd będzie systematycznie wzmacniał i rozwijał krajowy system cyberbezpieczeństwa. Działania uwzględniają systemowe rozwiązania organizacyjne, operacyjne, technologiczne, prawne, kreowanie postaw społecznych oraz prowadzenie badań naukowych tak, aby zapewnić spełnienie wysokich standardów cyberbezpieczeństwa w obszarze oprogramowania, urządzeń i usług cyfrowych. Działania rządu będą podejmowane z poszanowaniem praw i wolności obywateli oraz przez budowę zaufania między poszczególnymi sektorami rynkowymi a administracją publiczną.

4.2. Cel główny

Podniesienie poziomu odporności na cyberzagrożenia[6)] oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.

4.3. Cele szczegółowe

Cel szczegółowy 1. Rozwój krajowego systemu cyberbezpieczeństwa.

Cel szczegółowy 2. Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.

Cel szczegółowy 3. Zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni.

---

6) Cyberzagrożenie to wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów teleinformatycznych, użytkowników takich systemów oraz innych osób – zgodnie z rozporządzeniem 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).

Cel szczegółowy 4. Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa.

Cel szczegółowy 5. Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

5. Cel szczegółowy 1 – rozwój krajowego systemu cyberbezpieczeństwa

5.1. Wdrożenie i ocena funkcjonowania przepisów o krajowym systemie cyberbezpieczeństwa

Podstawą rozwoju krajowego systemu cyberbezpieczeństwa jest dokonanie pełnego wdrożenia i oceny funkcjonowania przepisów ustanawiających ten system, w powiązaniu z innymi przepisami, w szczególności z ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398), ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742), Strategią Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Rezultatem dokonanej oceny może być konieczność przygotowania niezbędnych zmian przepisów usuwających bariery dla skutecznej wymiany informacji oraz skoordynowanego i niezakłóconego reagowania na incydenty.

Zmiany przepisów regulujących funkcjonowanie krajowego systemu cyberbezpieczeństwa będą również wynikały z praktyki funkcjonowania na szczeblu europejskim dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1), zwanej dalej „dyrektywą NIS". Doświadczenia związane ze stosowaniem przepisów prawa w tym zakresie będą również przesłanką do wnioskowania na poziomie Unii Europejskiej w sprawie zmiany przepisów samej dyrektywy NIS tak, aby zwiększyć skuteczność jej oddziaływania – jednym z obszarów wymagających zmian zwiększających efektywność dyrektywy NIS będzie doprecyzowanie obowiązków dostawców usług cyfrowych, w szczególności świadczących usługi chmur obliczeniowych, które w coraz większym stopniu będą wykorzystywane jako model przetwarzania danych dla usług kluczowych.

Za przygotowanie propozycji zmian prawnych w zakresie cyberbezpieczeństwa w swoich obszarach kompetencyjnych odpowiadają ministrowie według właściwości wynikającej z ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2019 r. poz. 945, 1248 i 1696) oraz organy właściwe wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

W ramach prac legislacyjnych minister właściwy do spraw informatyzacji, we współpracy z innymi resortami i organami właściwymi odpowiedzialnymi za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach, dokona przeglądu regulacji sektorowych i szczególnych, które dotyczą omawianej problematyki, oraz regulacji prawnych, które mogą mieć oddziaływanie na inne obszary, na przykład na ochronę danych osobowych czy infrastrukturę krytyczną w kontekście Narodowego Programu Ochrony Infrastruktury Krytycznej. Niezbędne będzie również podjęcie prac legislacyjnych mających na celu uregulowanie obszaru z zakresu wytwarzania, posiadania, pozyskiwania oraz wykorzystywania specjalistycznych narzędzi podwójnego zastosowania do prowadzenia działań defensywno-ofensywnych w cyberprzestrzeni.

W ramach realizacji Strategii Cyberbezpieczeństwa uregulowane zostaną kwestie współpracy operacyjnej, w tym właściwej koordynacji działań i wymiany informacji między instytucjami odpowiedzialnymi za bezpieczeństwo narodowe, działania antyterrorystyczne oraz bezpieczeństwo wewnętrzne i porządek publiczny.

Z uwagi na dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie ciągłe monitorowanie zjawisk tam zachodzących i inicjowanie ewentualnych zmian w przepisach prawa. Propozycje kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa będą opiniowane przez Kolegium do Spraw Cyberbezpieczeństwa działające przy Radzie Ministrów. Jest to organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności zespołów

CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa.

5.2. Podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa

Podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa będzie realizowane przez uruchomienie do dnia 1 stycznia 2021 r., przez ministra właściwego do spraw informatyzacji, systemu teleinformatycznego wspierającego:

1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
3) zgłaszanie i obsługę incydentów;
4) szacowanie ryzyka na poziomie krajowym;
5) ostrzeganie o cyberzagrożeniach.

Organy właściwe, odpowiedzialne za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe, będą prowadziły działania mające na celu wspieranie operatorów i dostawców w zapewnieniu bezpieczeństwa świadczonych przez nich usług. Organy właściwe będą mogły w tym celu wydawać zalecenia organizacyjne i techniczne, a także udostępniać narzędzia i wiedzę dotyczącą najlepszych praktyk sektorowych i ponadsektorowych podnoszących cyberbezpieczeństwo.

Rozwój krajowego systemu cyberbezpieczeństwa wiąże się również ze zwiększaniem zdolności struktur zajmujących się cyberbezpieczeństwem na poziomie operacyjnym, w tym trzech zespołów CSIRT poziomu krajowego, współpracujących z nimi sektorowych zespołów cyberbezpieczeństwa, a także centrów analizy i wymiany informacji. Niezbędne jest wdrożenie systemowych rozwiązań pozwalających na wymianę informacji między interesariuszami i dzielenie się wiedzą co do podatności, zagrożeń i incydentów.

Rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz jednostek samorządu terytorialnego w zakresie podnoszenia kompetencji w projektowaniu procesów zwiększających cyberbezpieczeństwo, w szczególności: w doborze, wdrażaniu i utrzymaniu środków technicznych zwiększających cyberbezpieczeństwo, w tym korzystania z nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych, tworzenia bezpiecznych aplikacji oraz korzystania z bezpiecznych systemów mobilnych.

Efektywność funkcjonowania krajowego systemu cyberbezpieczeństwa ma również podnieść wprowadzenie standaryzacji rozwiązań zabezpieczających, w tym wprowadzenie minimalnych wymagań bezpieczeństwa dla sieci i systemów teleinformatycznych używanych przez administrację publiczną. Standaryzacja i wymagania cyberbezpieczeństwa, opracowane i wykorzystywane przez administrację publiczną w ramach Narodowych Standardów Cyberbezpieczeństwa, powinny stać się także wyznacznikiem dobrych praktyk dla sektora prywatnego oraz dla obywateli.

Efektywność funkcjonowania krajowego systemu cyberbezpieczeństwa będzie weryfikowana podczas ćwiczeń sektorowych oraz ćwiczeń krajowych inicjowanych przez Pełnomocnika Rządu do spraw Cyberbezpieczeństwa. W ramach ćwiczeń krajowych i międzynarodowych będą także podnoszone

zdolności Sił Zbrojnych Rzeczypospolitej Polskiej do prowadzenia operacji defensywnych w cyberprzestrzeni.

5.3. Rozbudowa systemu wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym

W celu usprawnienia zarządzania bezpieczeństwem prowadzone będą działania mające na celu wymianę informacji i uzgadnianie reakcji, tak na poziomie strategicznym, jak i poziomie operacyjnym, w szczególności między sferą cywilną i sferą wojskową. Niezbędna jest budowa odpornego na cyberzagrożenia systemu wymiany informacji dla potrzeb administracji publicznej, wykorzystującego najnowocześniejsze technologie wymiany informacji, uwzględniające konieczność wysokiej mobilności. System ten będzie wykorzystywany w różnych stanach nadzwyczajnych oraz stanach gotowości obronnej państwa.

5.4. Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej

Technologie informatyczne (IT)[7)] wykorzystywane przez operatorów usług kluczowych, dostawców usług cyfrowych, operatorów infrastruktury krytycznej (w tym operatorów telekomunikacyjnych) stanowią element krytyczny dla ciągłości działania państwa oraz zapewniania bezpieczeństwa obywatelom. Co więcej bezpieczeństwo najważniejszych sektorów gospodarki, ze szczególnym uwzględnieniem sektora energii, zależy od zapewnienia niezakłóconego działania przemysłowych systemów sterowania (OT)[8)]. Dlatego zapewnienie cyberbezpieczeństwa zarówno IT, jak i OT, będzie traktowane przez rząd jako priorytet. Wyrazem tego są przygotowywane już analizy dotyczące doprecyzowania wymagań bezpieczeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G, która w przyszłości będzie podstawą funkcjonowania państwa w zakresie mobilnej telekomunikacji. Zakłada się, że będą w tym obszarze konieczne zmiany prawne, aby umożliwić odpowiednią kontrolę nad zapewnieniem cyberbezpieczeństwa.

Oprócz tego, mając na uwadze, że odpowiedzialność za zapewnienie bezpieczeństwa usług leży przede wszystkim po stronie podmiotów je świadczących, rząd podejmie działania wspierające budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa wśród operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych, uwzględniając ich różnorodną specyfikę i różny stopień dojrzałości w zakresie cyberbezpieczeństwa. Ponadto rząd będzie wspierał te podmioty w reagowaniu na incydenty istotne, krytyczne i poważne, szczególnie w przypadku wystąpienia incydentów ponadsektorowych.

W pierwszej kolejności zostanie zapewniona spójność działań w zakresie opracowywania kryteriów identyfikacji operatorów infrastruktury krytycznej i operatorów usług kluczowych, uwzględniająca potrzebę włączenia tych podmiotów do systemu zarządzania kryzysowego. Proces ten przebiegał będzie we współpracy ze wszystkimi sektorami. Wykorzystując mechanizmy przewidziane prawem, rekomendowane będą minimalne wymagania w zakresie cyberbezpieczeństwa ze szczególnym uwzględnianiem zarządzania ciągłością działania.

---

7) IT – ang. information technologies.
8) OT – ang. operational technologies.

Analogicznym reżimem objęci zostaną dostawcy usług cyfrowych, jednak rząd ma pełną świadomość międzynarodowej specyfiki tych podmiotów oraz konieczności zapewnienia takich regulacji, które będą sprzyjały rozwojowi rynku cyfrowego w Polsce. Stąd działania w tym obszarze będą prowadzone na forum europejskim, przede wszystkim w ramach Grupy Współpracy dyrektywy NIS, a także w ramach współpracy transatlantyckiej z brytyjskimi i amerykańskimi instytucjami stymulującymi podnoszenie standardów cyberbezpieczeństwa przez dostawców usług cyfrowych.

5.5. Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym

Na potrzeby zarządzania cyberbezpieczeństwem na poziomie krajowym wdrożona zostanie wspólna metodyka statycznego i dynamicznego szacowania ryzyka, uwzględniająca specyfikę poszczególnych sektorów, a także operatorów infrastruktury krytycznej, operatorów usług kluczowych i dostawców usług cyfrowych. Zapewni to porównywalność szacowań, w tym określenie poziomu ryzyka, w szczególności na potrzeby raportu o zagrożeniach bezpieczeństwa narodowego, sporządzanego na podstawie przepisów o zarządzaniu kryzysowym. Szacowanie ryzyka stanie się procesem ciągłym i umożliwi zobrazowanie poziomu ryzyka w czasie zbliżonym do czasu rzeczywistego.

Metodyka i narzędzia umożliwiające statyczne i dynamiczne szacowania ryzyka dla systemów teleinformatycznych powstają w ramach projektu Narodowej Platformy Cyberbezpieczeństwa finansowanego przez Narodowe Centrum Badań i Rozwoju – zakończenie prac planowane jest do końca 2020 r.[9)]

5.6. Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym

W zakresie zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze hybrydowym (w tym działań o charakterze terrorystycznym) ważne jest zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich ich fazach. W tym celu wymagana jest współpraca oraz koordynacja działań organów ścigania niezależnie od motywów, którymi kierują się sprawcy przestępstw, a szczególnie istotne znaczenie ma prawidłowe zabezpieczenie dowodów cyfrowych.

Zwiększenie efektywności czynności procesowych i operacyjnych wymaga podjęcia i poszerzenia współdziałania organów ścigania z innymi podmiotami, które mogą posiadać wiedzę w zakresie ustalenia istoty przestępstwa lub mogą przyczynić się do ustalenia jego sprawcy. Dotyczy to współpracy z krajowymi oraz międzynarodowymi podmiotami prywatnymi, szczególnie z sektora telekomunikacyjnego, bankowego i ubezpieczeniowego. Niezbędne jest także zapewnienie ciągłej wymiany informacji o zagrożeniach i podatnościach zarówno na poziomie krajowym, jak i międzynarodowym.

Mając na uwadze specyfikę cyberprzestrzeni, zwalczanie cyberprzestępczości wymaga transgranicznej współpracy organów ścigania oraz podmiotów typu CERT/CSIRT. W czynnościach

[9)] Metodyka i narzędzia umożliwiające statyczne i dynamiczne szacowanie ryzyka dla systemów teleinformatycznych są opracowywane w ramach projektu badawczego pn. „Narodowej Platformy Cyberbezpieczeństwa", realizowanego przez Naukową i Akademicką Sieć Komputerową i finansowanego przez Narodowe Centrum Badań i Rozwoju w ramach Programu CyberSecIdent – Cyberbezpieczeństwo i e-Tożsamość.

procesowych lub w procesie rozpoznania operacyjnego dotyczących przestępstw dokonywanych w cyberprzestrzeni krytyczny jest upływ czasu. Oznacza to, że wymagane są sprawne i zaufane kanały wymiany informacji między organami ścigania różnych państw.

Biorąc pod uwagę dynamikę przestępstwa w cyberprzestrzeni i związaną z tym konieczność podejmowania czynności operacyjnych i procesowych, niezbędne jest wprowadzenie przepisów umożliwiających przetwarzanie dokumentów procesowych w postaci elektronicznej i przesyłanie ich w takiej postaci.

Szybko zmieniające się metody popełniania przestępstw wymagają rozwijania badań naukowych w obszarze zwalczania cyberprzestępczości, których wyniki zapewnią wsparcie dla organów ścigania. Wyniki tych badań będą wykorzystywane w pracy organów ścigania i wymiaru sprawiedliwości, jak też będą stanowić materiał do opracowania działań profilaktycznych. Wdrożone zostaną skierowane do społeczeństwa programy informacyjne o zagrożeniach cyberprzestępczością oraz metodach unikania skutków tych zagrożeń. Wskazane zostaną sposoby postępowania dla osób dotkniętych przestępstwem. Ważną rolę do odegrania w tego typu działalności będą mieli operatorzy usług kluczowych, dostawcy usług cyfrowych, dostawcy usługi dostępu do Internetu oraz organizacje pozarządowe, a także podmioty publiczne.

6. Cel szczegółowy 2 – Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty

6.1. Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń

Wykorzystując potencjał intelektualny ekspertów zgromadzonych w komitetach technicznych Polskiego Komitetu Normalizacyjnego, ośrodkach naukowych, akademickich i instytutach badawczych, a także w zainteresowanych podmiotach publicznych i prywatnych, opracowane zostaną nowe standardy lub nastąpi przełożenie istniejących norm i standardów na konkretne rekomendacje w zakresie ich wdrażania.

W celu zwiększenia odporności systemów informacyjnych administracji publicznej na cyberzagrożenia niezbędne jest opracowanie Narodowych Standardów Cyberbezpieczeństwa, jako zbioru wymagań organizacyjnych i technicznych dotyczących, w szczególności, bezpieczeństwa:

1) aplikacji;

2) urządzeń mobilnych;

3) stacji roboczych;

4) serwerów i sieci;

5) modeli chmur obliczeniowych.

W celu zapewnienia bezpiecznej i optymalnej kosztowo infrastruktury przetwarzania systemów IT administracji publicznej, która już w bliskiej przyszłości rozpocznie korzystanie z nowych form przetwarzania i przechowywania informacji, m.in. przez wykorzystywanie usług chmury obliczeniowej, niezbędne będzie przygotowanie zaleceń i promowanie dobrych praktyk podnoszących odporność na potencjalne cyberzagrożenia.

Realizacja zadań publicznych, w szczególności związanych z cyberbezpieczeństwem, będzie wspierana przez stosowanie Polskich Norm, bazujących na normach europejskich i międzynarodowych. Odwołania do norm powinny być szeroko stosowane na wszystkich etapach cyklu życia systemu teleinformatycznego. Istotne jest również wspieranie wdrożenia rekomendacji wydawanych przez regulatorów rynkowych.

6.2. Bezpieczeństwo łańcucha dostaw

Zapewnienie cyberbezpieczeństwa wymaga stosowania zabezpieczeń organizacyjnych i technicznych na wszystkich etapach cyklu życia systemów teleinformatycznych. Działania te składają się na tak zwany bezpieczny łańcuch dostaw, który obejmuje projektowanie, budowę, wdrażanie, eksploatację oraz wycofywanie z użycia. Pod pojęciem łańcucha dostaw należy rozumieć system, na który składają się podsystemy produkcji, dystrybucji, transportu, magazynowania oraz recyklingu komponentów systemów teleinformatycznych, jak również ich instalacja, uruchomienie, bieżące utrzymanie, serwisowanie oraz naprawy.

Ważnym elementem zapewnienia jakości w łańcuchu dostaw jest ocena i certyfikacja produktów (w szczególności oprogramowania, urządzeń i usług). Priorytetowe w tym zakresie będzie utworzenie, a następnie utrzymanie i rozwój krajowego systemu oceny i certyfikacji cyberbezpieczeństwa bazującego na działalności akredytowanych jednostek oceniających zgodność, co umożliwi Rzeczypospolitej Polskiej uzyskanie pełnego i rozpoznawanego na arenie europejskiej i międzynarodowej statusu państwa producenta w dziedzinie rozwiązań cyberbezpieczeństwa.

Rzeczpospolita Polska aktywnie włączy się w prace nad ustanowieniem europejskich programów certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem 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).

Działania na poziomie krajowym będą obejmowały, w szczególności, wyznaczenie krajowego organu ds. certyfikacji cyberbezpieczeństwa, który będzie wydawał europejskie certyfikaty cyberbezpieczeństwa oraz nadzorował krajowe jednostki oceniające zgodność produktów, usług i procesów z wymaganiami określonymi w europejskich programach certyfikacji cyberbezpieczeństwa oraz współpracował z krajową jednostką akredytującą – Polskim Centrum Akredytacji, w celu monitorowania i nadzorowania działalności akredytowanych jednostek oceniających zgodność w odniesieniu do wymagań rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881.

Efektem tych działań będzie uzyskanie na poziomie krajowym zdolności do wspierania polskich producentów, którzy uzyskując europejskie certyfikaty cyberbezpieczeństwa, będą mogli skuteczniej konkurować na jednolitym rynku cyfrowym UE.

6.3. Testy i audyty cyberbezpieczeństwa

Jednym ze środków, który pozwala na dokonanie oceny skuteczności wdrożonych systemów zarządzania bezpieczeństwem i adekwatności ustanowionych zabezpieczeń, są okresowe audyty. Metodyki audytów powinny uwzględniać normy, dobre praktyki oraz specyfikę poszczególnych sektorów. Celem takiego podejścia jest uzyskanie porównywalności wyników audytów.

Kolejnym środkiem oceny bezpieczeństwa są okresowe testy (w tym testy penetracyjne), które pozwalają na rzeczywistą ocenę odporności systemu na zagrożenia. Ich wyniki stanowią podstawę weryfikacji przyjętych założeń w zakresie ustanowionych zabezpieczeń. W celu wykorzystania potencjału społecznego w zakresie cyberbezpieczeństwa propagowane będzie testowanie zabezpieczeń w modelu tzw. *bug-bounty*[10)].

[10)] Bug-bounty – poszukiwanie podatności w oprogramowaniu przez osoby niezwiązane z producentem tego oprogramowania, zwykle za jego zgodą generalną.

7. Cel szczegółowy 3 – Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa

7.1. Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa

Rząd stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa przez stwarzanie warunków dla rozwoju przedsiębiorstw, w tym szczególnie MŚP oraz start-upów, a także ośrodków naukowo-badawczych, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. Jednym z priorytetów jest wzrost zdolności w obszarze projektowania i wytwarzania oprogramowania, urządzeń i usług wykorzystywanych we wszystkich gałęziach polskiego przemysłu, zwiększających jego konkurencyjność[11)]. Pozyskiwanie nowych technologii dla rozwoju rodzimych przedsięwzięć będzie realizowane przez udział w inicjatywach międzynarodowych kładących nacisk na innowacyjność w drodze współpracy dwustronnej oraz w ramach organizacji międzynarodowych, w tym w ramach planowanego przez Komisję Europejską i państwa członkowskie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych.

Ponadto rząd będzie dążył do aktywnego upowszechniania wśród polskich przedsiębiorców wiedzy, szkoleń i wdrażania technologii cyberbezpieczeństwa pozwalających na pełne wykorzystanie w procesach produkcji lub świadczenia usług potencjału innych najnowocześniejszych technologii cyfrowych, m.in. systemów autonomicznych opartych na sztucznej inteligencji.

Stymulowane będzie podnoszenie kompetencji ośrodków naukowych oraz wyższych uczelni w obszarze cyberbezpieczeństwa. Przez instrumenty prawne rząd będzie stymulował na wyższych uczelniach nauczanie służące pozyskiwaniu specjalistów z zakresu cyberbezpieczeństwa, w ramach studiów pierwszego i drugiego stopnia, szkół doktorskich oraz studiów podyplomowych.

W celu wyrównania szans polskich przedsiębiorców na globalnym rynku rząd będzie wspierał rozwój polskiego biznesu w uzyskiwaniu zdolności cyfrowych oraz zapewniał pomoc w ubieganiu się o środki na rozwój innowacyjnych rozwiązań, a także doradztwo w dostępie do nowych rynków, jak i pomoc w nawiązaniu współpracy z innymi przedsiębiorcami.

7.2. Nastawienie na rozwój współpracy między sektorem publicznym i prywatnym

Zapewnienie bezpieczeństwa w cyberprzestrzeni wymaga wspólnego wysiłku sektora prywatnego, publicznego oraz obywateli. Rząd będzie kontynuował budowanie efektywnego systemu partnerstwa publiczno-prywatnego opartego na zaufaniu i wspólnej odpowiedzialności za cyberbezpieczeństwo.

Jednocześnie administracja publiczna będzie doskonaliła swój potencjał w zakresie inicjowania i prowadzenia projektów w dziedzinie cyberbezpieczeństwa. Rząd będzie również aktywnie angażować się w istniejące i powstające formy europejskiej współpracy publiczno-prywatnej i tym samym będzie promować polski biznes na arenie międzynarodowej.

---

11) Jednym z przykładów działań nastawionych na rozwój polskiego przemysłu i jego konkurencyjności w dobie transformacji cyfrowej jest program realizowany przez ministra właściwego do spraw gospodarki pn.: "Przemysł 4.0". W ramach programu, w drodze konkursu, zostaną wyłonione Huby Innowacji Cyfrowej (Digital Innovation Hubs), które w sposób ustandaryzowany będą wspierać przedsiębiorców w transformacji cyfrowej, w tym także w obszarze cyberbezpieczeństwa.

Realizując nową wizję rozwoju kraju i wspierając innowacyjność polskiej gospodarki, istotna będzie budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa, prowadzonych we współpracy świata nauki oraz przedsiębiorstw komercyjnych.

7.3. Stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa

W związku z dynamicznie rozwijającym się rynkiem informatycznym, w szczególności w związku z przejściem na protokół komunikacyjny IPv6, a także w związku z rozwojem idei Internetu Rzeczy, Inteligentnych Miast, Przemysłu 4.0, jak również chmury obliczeniowych, sieci mobilnej łączności szerokopasmowej (5G i kolejnych generacji) czy megadanych (*Big Data)*, zachodzi konieczność intensyfikacji działań badawczych i rozwojowych oraz wytwórczych w zakresie cyberbezpieczeństwa. W tym celu wspólnie z Narodowym Centrum Badań i Rozwoju kontynuowane będą programy badawcze[12)], mające na celu przygotowanie i wdrożenie nowych metod ochrony przed cyberzagrożeniami.

W obliczu dynamicznie rozwijających się technologii związanych m.in. z Internetem Rzeczy należy zwrócić szczególną uwagę na konieczność zapewnienia bezpieczeństwa produktu, usługi lub procesu już na etapie projektowania (*Security by design*[13)]), a także ochronę danych i prywatności (Privacy by design)[14)]. Rząd będzie promował i wspierał podejście uwzględniające bezpieczeństwo już od etapu projektowania.

Ponadto we współpracy ze środowiskiem naukowo-akademickim zostaną opracowane programy badawcze mające na celu, w szczególności:

1) ocenę skuteczności zabezpieczeń i odporności na cyberzagrożenia;
2) ocenę skuteczności reagowania na incydenty;
3) metody wykrywania i analizy nowych typów cyberprzestępstw, cyberterroryzmu i cyberszpiegostwa;
4) badanie metod ataków (w tym ataków o charakterze hybrydowym) oraz sposobów przeciwdziałania i minimalizowania skutków tych ataków;
5) ochronę procesów demokratycznych przed zakłóceniami z wykorzystaniem cyberzagrożeń.

---

12) Kontynuowana będzie współpraca Ministerstwa Cyfryzacji z Narodowym Centrum Badań i Rozwoju m.in. w ramach Programu CyberSecIdent – Cyberbezpieczeństwo i e-Tożsamość.

13) Security by design – podejście do rozwoju produktów lub systemów, które polega na myśleniu o bezpieczeństwie i integracji funkcji bezpieczeństwa od samego początku. Komunikat Komisji – „Europejski program badań i innowacji w dziedzinie bezpieczeństwa" – wstępne stanowisko Komisji w sprawie głównych ustaleń i zaleceń europejskiego forum badań i innowacji w dziedzinie bezpieczeństwa (ESRIF) /*COM(2009)691 final/.

14) Privacy by design – podejście do ochrony danych i prywatności, zawierające odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, uwzględniające stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania. Na podstawie art. 25 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – Dz. Urz. UE L 119 z 04.05.2016, str. 1.

Działalność badawcza i rozwojowa realizowana będzie także w obszarze współpracy międzynarodowej w ramach UE i NATO.

Ważne zadania w systemie zapewnienia cyberbezpieczeństwa mają organizacje pozarządowe, które są bardzo sprawnymi organizatorami działań edukacyjnych w społeczeństwie, a także jako dostawcy analiz i opinii dla administracji publicznej. Możliwe jest także pozyskiwanie specjalistów o unikatowych umiejętnościach przez ośrodki analityczne na potrzeby rozwiązywania skomplikowanych problemów z zakresu cyberbezpieczeństwa.

7.4. Uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni

Siły Zbrojne Rzeczypospolitej Polskiej, jako podstawowy element systemu obronnego państwa, powinny angażować się w działania w cyberprzestrzeni na tym samym poziomie co w powietrzu, na lądzie i na morzu, zarówno w czasie pokoju, wojny, jak i w sytuacji kryzysowej. Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni muszą więc obejmować m.in.: rozpoznawanie zagrożeń, ochronę i obronę sieci i systemów teleinformatycznych oraz zwalczanie źródeł cyberzagrożeń.

Działania w cyberprzestrzeni stanowią integralną część planowanych operacji, które będą prowadzone przez Siły Zbrojne Rzeczypospolitej Polskiej zarówno samodzielnie, jak i w układzie sojuszniczym lub koalicyjnym. Struktury Sił Zbrojnych Rzeczypospolitej Polskiej będą udoskonalone przez utworzenie i wzmacnianie formacji przeznaczonych do realizacji zadań w cyberprzestrzeni, dysponujących zdolnościami w zakresie rozpoznawania, zapobiegania i zwalczania cyberzagrożeń. Budowana będzie zdolność do interoperacyjnego działania w cyberprzestrzeni w układzie militarnym i pozamilitarnym w wymiarze narodowym i międzynarodowym w ramach sojuszu, koalicji i porozumień. Kwalifikacje personelu prowadzącego działania militarne w cyberprzestrzeni będą stale podnoszone w ramach szkoleń. Jednocześnie prowadzone będzie na bieżąco rozpoznanie zagrożeń oraz ocena – również pod kątem zgodności z prawem międzynarodowym – sytuacji, co pozwoli na dobór właściwych metod i narzędzi do ochrony i obrony zasobów własnych oraz eliminację źródeł zagrożeń dla sieci i systemów teleinformatycznych zarówno infrastruktury stacjonarnej, jak i mobilnej. Mając na uwadze dynamikę rozwoju technologii tworzących środowisko, jakim jest cyberprzestrzeń, resort obrony narodowej będzie dążyć do wytworzenia bądź pozyskania innowacyjnych metod i narzędzi, które zapewnią skuteczność działania w tej domenie.

8. Cel szczegółowy 4 – Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa

8.1. Zwiększanie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa Rzeczypospolitej Polskiej

Podnoszenie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa Rzeczypospolitej Polskiej będzie realizowane przez stworzenie i wdrożenie takiego modelu funkcjonowania systemu edukacji akademickiej i doskonalenia zawodowego, który zapewni odpowiednie do wyzwań kwalifikacje pracowników. W tym celu opracowane zostaną modelowe programy edukacji akademickiej dla dedykowanego kierunku cyberbezpieczeństwo.

W ramach szeroko rozumianej edukacji eksperckiej, aby skuteczniej przeciwdziałać rozwijającej się cyberprzestępczości, zostanie wzmocniony system szkoleń dla wszystkich pracowników podmiotów istotnych dla cyberbezpieczeństwa oraz dla przedstawicieli organów ścigania i wymiaru sprawiedliwości, przez wdrożenie dedykowanego programu edukacyjnego zawierającego zarówno szkolenia teoretyczne, jak i praktyczne na realnych przykładach zagrożeń.

W celu utrzymania w administracji publicznej pracowników o wysokich kompetencjach, równolegle z wykorzystaniem innych instrumentów wspierających ich aktywność, podjęte będą działania w celu zbliżenia zarobków tych pracowników do poziomu, jaki mogliby uzyskać, zatrudniając się w sektorze prywatnym.

Równocześnie rząd przygotuje i wdroży systemowe rozwiązanie w celu zapewnienia merytorycznego wsparcia dla podniesienia kompetencji pracowników jednostek administracji samorządowej w zakresie cyberbezpieczeństwa.

Kierownictwo jednostek administracji rządowej będzie dynamicznie określało odpowiedzialność i uprawnienia dla osób pełniących istotną rolę w zakresie zarządzania cyberbezpieczeństwem i odpowiednio komunikowało te ustalenia wszystkim interesariuszom.

8.2. Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli

Edukacja w zakresie cyberbezpieczeństwa powinna być dostępna na jak najwcześniejszym etapie dostępu dzieci i młodzieży do usług cyfrowych – najlepiej, jeśli byłaby prowadzona przed wejściem w świat cyfrowy, a w praktyce często wymagana jest na etapie edukacji wczesnoszkolnej. Uwzględniając tematykę bezpiecznego korzystania z cyberprzestrzeni, zakłada się wsparcie nauczycieli w realizacji podstawy programowej, w szczególności w aktualizowaniu programów nauczania w ramach różnych zajęć zgodnie z aktualną wiedzą na temat bezpiecznego korzystania z nowoczesnych technologii.

Ponadto realizowane będą działania wspierające ciągłe doskonalenie nauczycieli w obszarze nowoczesnych technologii i cyberbezpieczeństwa, z uwzględnieniem zdiagnozowanych potrzeb danej szkoły lub placówki.

Uczelnie wyższe będą zachęcane do tego, aby rozwijane były specjalizacje interdyscyplinarne, obejmujące między innymi zarządzanie bezpieczeństwem informacji, ocenę i weryfikację zabezpieczeń systemów teleinformatycznych, ochronę danych osobowych, ochronę własności intelektualnej w Internecie oraz zagadnienia związane z rozwojem nowych technologii i wyzwaniami, które są tego pochodnymi.

8.3. Rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni

We współpracy z organizacjami pozarządowymi, sektorem prywatnym oraz ośrodkami akademickimi administracja publiczna kontynuować będzie systemowe działania uwrażliwiające społeczeństwo na zagrożenia płynące z cyberprzestrzeni, a także działania edukacyjne w zakresie praw i wolności w środowisku cyfrowym oraz uprawnień osób, które padły ofiarą cyberataku i poniosły szkodę w wyniku naruszeń bezpieczeństwa w sieci. Kontynuowane będą m.in. kampanie społeczne, skierowane do różnych grup docelowych m. in. dzieci, rodziców, seniorów.

W obliczu coraz liczniejszych zagrożeń nakierowanych na wywarcie określonego wpływu na społeczeństwo, a także mając na uwadze konsekwencje celowego wykorzystywania narzędzi z obszaru inżynierii społecznej do działań o charakterze manipulacyjnym w postaci m.in. kampanii dezinformacyjnych lub działań inspiracyjnych bądź dezintegracyjnych, potrzebne jest podjęcie systemowych działań pozwalających na rozwijanie świadomości obywateli w kontekście weryfikacji autentyczności informacji oraz reagowania na próby jej zakłócenia. W kontekście obrony przed działaniami manipulacyjnymi, które mogą być jednym z elementów działań o charakterze hybrydowym, ważne jest budowanie w społeczeństwie zdolności do identyfikacji działań oddziaływujących na świadomość bądź ukierunkowanych na przekształcanie lub dezintegrację określonych środowisk.

9. Cel szczegółowy 5 – Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa

9.1. Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym

W obliczu wszechobecnych procesów globalizacyjnych i związanych z nimi współzależności państw międzynarodowa współpraca jest kluczowa dla osiągnięcia bezpieczeństwa globalnej cyberprzestrzeni.

Realizując te zadania na poziomie europejskim, Rzeczpospolita Polska zintensyfikuje działania na rzecz zapewnienia bezpieczeństwa jednolitego rynku cyfrowego UE, jako motoru wzrostu gospodarczego i innowacyjności. Ponadto istotne jest dążenie do szerszego uwzględnienia aspektów cyberbezpieczeństwa w pracach nad pogłębieniem Wspólnej Polityki Zagranicznej i Bezpieczeństwa Unii Europejskiej.

Członkostwo w Organizacji Traktatu Północnoatlantyckiego jest istotnym filarem bezpieczeństwa Rzeczypospolitej Polskiej, jak i bezpieczeństwa euroatlantyckiego. Nasilające się ataki o charakterze hybrydowym czynią nieodzownym inwestowanie w zdolności odstraszania i obronne, w tym doskonalenie swojej odporności i zdolności do szybkiego i skutecznego reagowania na cyberataki.

Współpracując w ramach systemu Organizacji Narodów Zjednoczonych, Rzeczpospolita Polska będzie dążyła do kontynuacji debaty dotyczącej sprawnie funkcjonującego systemu międzynarodowego zarządzania siecią globalną oraz zagadnień związanych z prawną oceną cyberataków, w celu wypracowania spójnych rozwiązań, gwarantujących pewność międzynarodowej wymiany informacji w Internecie. W kontekście aspektów prawno-międzynarodowych kluczowe jest dążenie do uzyskania wśród państw jak najszerszego konsensusu odnośnie do tego, w jaki sposób prawo międzynarodowe stosuje się do działań w cyberprzestrzeni. Rzeczpospolita Polska – we współpracy z partnerami prezentującymi podobny punkt widzenia – będzie promować stanowisko, zgodnie z którym obowiązujące prawo międzynarodowe, przede wszystkim Karta Narodów Zjednoczonych, stosuje się do cyberprzestrzeni. Rzeczpospolita Polska potwierdza swoje przywiązanie do wypracowanych w ramach prac Grup ekspertów rządowych ONZ dobrowolnych zasad odpowiedzialnego zachowania państw w cyberprzestrzeni, opowiada się za stosowaniem całego prawa międzynarodowego do działań państw w cyberprzestrzeni oraz za wdrożeniem środków budowy zaufania w celu zmniejszenia ryzyka konfliktu wynikającego z cyberzagrożeń. Rzeczpospolita Polska będzie angażować się we wzmacnianie środków budowy zaufania i bezpieczeństwa w ramach istniejących forów międzynarodowych, w tym OBWE. Rząd będzie włączał się również w działania na rzecz skutecznego zwalczania cyberprzestępczości w wymiarze międzynarodowym.

Istotna jest również współpraca z krajami regionu, w tym wzmocnienie współpracy w ramach Grupy Wyszehradzkiej, jak i z państwami tzw. Trójmorza.

Jednym z elementów realizacji polityki zagranicznej może być również zawieranie przez Rzeczpospolitą Polską dwustronnych i wielostronnych umów międzynarodowych lub porozumień o charakterze prawnie niewiążącym w zakresie współpracy w ramach cyberbezpieczeństwa z państwami o rozwiniętym potencjale technologicznym.

Wzmocnienie polskiej pozycji międzynarodowej będzie możliwe tylko na drodze wewnętrznej ścisłej kooperacji między instytucjami i agencjami odpowiadającymi w Rzeczypospolitej Polskiej za zapewnienie cyberbezpieczeństwa, w tym szczególnie między ministrem właściwym do spraw

informatyzacji oraz ministrem właściwym do spraw zagranicznych odpowiadającym za całokształt polskiej polityki zagranicznej.

Silna pozycja międzynarodowa Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa nie będzie możliwa bez odpowiedniego zaplecza merytorycznego. Zasób kadrowy wsparty odpowiednim finansowaniem będzie podstawą do zbudowania wizerunku Rzeczypospolitej Polskiej jako kompetentnego gracza na arenie międzynarodowej. W tym kontekście istotne jest, aby eksperci z Rzeczypospolitej Polskiej aktywnie uczestniczyli w dyskusjach prowadzonych na forach regionalnych i globalnych oraz pełnili kluczowe role w organizacjach międzynarodowych, przyczyniając się w ten sposób do skutecznej realizacji polityki zagranicznej w zakresie cyberbezpieczeństwa. Celem zdobywania umiejętności, rozwijania wiedzy i wymiany najlepszych praktyk Rzeczpospolita Polska będzie przykładała jeszcze większą wagę do współpracy międzynarodowej, dwu- i wielostronnej, w kwestiach edukacji, szkoleń, jak i budowania świadomości.

W obszarze współpracy międzynarodowej Rzeczpospolita Polska będzie aktywnie włączać się w ćwiczenia prowadzone zarówno przez organizacje krajowe, podmioty UE i NATO oraz inne podmioty międzynarodowe.

9.2. Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym

Współpraca międzynarodowa na poziomie operacyjno-technicznym realizowana będzie m.in. w ramach Sieci CSIRT na poziomie Unii Europejskiej, na innych forach wymiany informacji i dokonywania analiz sytuacji bezpieczeństwa IT danego sektora, przez inne międzynarodowe sieci współpracy typu FIRST czy TF-CSIRT, platformy wymiany informacji typu MISP czy n6 oraz w ramach współpracy dwu- i wielostronnej. W tym kontekście szczególne znaczenie będzie miało wypracowanie wspólnych procedur działania w ramach UE i NATO oraz Grupy Wyszehradzkiej. Współpraca na tym poziomie będzie służyła nie tylko skutecznemu przeciwdziałaniu zagrożeniom w cyberprzestrzeni, ale przyczyni się do wymiany doświadczeń między personelem technicznym w ramach wspólnych przedsięwzięć. Będzie również okazją do promowania polskich rozwiązań technologicznych i polskiej kadry eksperckiej.

Doskonalenie współpracy międzynarodowej możliwe jest także przez uczestnictwo podmiotów publicznych zaangażowanych w zapewnienie cyberbezpieczeństwa w oficjalnych międzynarodowych forach wymiany informacji o zagrożeniach i podatnościach.

10.Zarządzanie Strategią Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Strategia Cyberbezpieczeństwa uchwalana jest na okres 5 lat.

Koordynatorem wdrażania Strategii Cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji.

Po dwóch latach od przyjęcia oraz w czwartym roku obowiązywania dokument podlega przeglądowi i ocenie efektów jego oddziaływania. Wyniki przeglądu przedstawiane są Radzie Ministrów. W wyniku dokonanego przeglądu minister właściwy do spraw informatyzacji opracowuje propozycję działań korygujących lub projekt dokumentu na kolejny okres pięcioletni. W przypadku wystąpienia uzasadnionych okoliczności Strategia Cyberbezpieczeństwa może być aktualizowana w innych terminach niż te, o których mowa powyżej.

Koordynator w terminie do sześciu miesięcy od przyjęcia Strategii Cyberbezpieczeństwa we współpracy z członkami Rady Ministrów, kierownikami urzędów centralnych, dyrektorem Rządowego Centrum Bezpieczeństwa oraz innymi organami właściwymi określonymi w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa opracuje i przedstawi do akceptacji Radzie Ministrów Plan działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa. Przy opracowywaniu Planu działań wymienione powyżej organy uwzględniają w swoich działaniach problematykę cyberbezpieczeństwa w zakresie zgodnym z ustawowymi kompetencjami. Plan działań obejmować będzie w szczególności:

1) nazwę celu szczegółowego;
2) nazwę zadania;
3) nazwę działania służącego realizacji zadania;
4) typ działania – działanie: legislacyjne, organizacyjne, technologiczne, edukacyjne, informacyjne, promocyjne, inne;
5) harmonogram – termin rozpoczęcia i termin zakończenia podejmowanej inicjatywy;
6) organ lub organy – organ wiodący i organy współpracujące przy realizacji zadania (o ile występują);
7) oczekiwane efekty wynikające z realizacji działania;
8) szacunkowy koszt realizacji działania.

Plan działań obejmuje działania o charakterze projektowym, charakteryzujące się początkiem i końcem okresu realizacji oraz produktami powstałymi w wyniku realizacji danego działania.

Minister Obrony Narodowej w uzgodnieniu z Koordynatorem może opracować odrębny Plan działań, który podlega akceptacji Prezesa Rady Ministrów. W stosunku do pozycji Planu działań zawierających informacje o charakterze niejawnym zastosowanie mają przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. poz. 742). Minister Obrony Narodowej przesyła, w celach informacyjnych i zapewnienia koordynacji, zaakceptowany Plan działań ministrowi właściwemu do spraw informatyzacji i Pełnomocnikowi Rządu do spraw Cyberbezpieczeństwa.

Koordynator będzie corocznie przygotowywał sprawozdanie o postępach wdrażania Strategii Cyberbezpieczeństwa za rok poprzedni na podstawie informacji otrzymywanych od podmiotów

zaangażowanych w jej realizację. Sprawozdania będą przedkładane Radzie Ministrów w terminie do 30 września.

W przypadku opracowania odrębnego Planu działań Minister Obrony Narodowej przedkłada sprawozdanie z jego realizacji Radzie Ministrów za pośrednictwem Koordynatora.

11.Finansowanie

Na mocy obowiązujących przepisów podmioty realizujące zadania publiczne są zobowiązane do ujmowania w swoich planach finansowych nakładów na cyberbezpieczeństwo. Koszty te powiększyły się o nakłady przeznaczone na działania związane z budową krajowego systemu cyberbezpieczeństwa oraz o nakłady ponoszone na realizację pozostałych przedsięwzięć Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa.

Szczegółowa wielkość i struktura kosztów poszczególnych przedsięwzięć będzie określona w procesie inicjowania konkretnych projektów. Oszacowanie kosztów finansowania wdrażania Strategii Cyberbezpieczeństwa nastąpi w ramach Planu działań.

Źródłami finansowania realizacji działań opisanych w dokumencie będą plany finansowe poszczególnych jednostek zaangażowanych we wdrażanie Strategii Cyberbezpieczeństwa, a także środki pochodzące z Narodowego Centrum Badań i Rozwoju oraz środki Unii Europejskiej[15)], w miarę zaistnienia takich możliwości.

15) Programy Unii Europejskiej umożliwiające finansowanie projektów związanych z cyberbezpieczeństwem, w szczególności: program Horyzont 2020, program Connecting Europe Facilities (CEF Telcom) – oba w ramach Wieloletnich Ram Finansowych UE 2014–2021. Natomiast w kolejnej perspektywie finansowej UE (na lata 2021–2028) planowane są do uruchomienia dwa duże programy: program „Cyfrowa Europa” oraz program „Horyzont Europa”.