STRATEGIA CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ NA LATA 2016–2020

POSZANOWANIE PRAW I WOLNOŚCI W CYBERPRZESTRZENI
KOMPLEKSOWE PODEJŚCIE DO BEZPIECZEŃSTWA
CYBERBEZPIECZEŃSTWO ISTOTNYM ELEMENTEM POLITYKI PAŃSTWA

Ministerstwo Cyfryzacji
Warszawa 2016

Spis treści

1. Cele i zakres strategii

Celem Strategii jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa rozumianego jako zapewnienie zdolności do:

1) realizacji funkcji Państwa,
2) zapewnienie ludności i przedsiębiorcom niezbędnych dostaw towarów i usług,
3) niezakłóconego dostępu i korzystania z sieci Internet,

– w sytuacji gdy realizacja wymienionych aktywności zależna jest od cyberprzestrzeni.

Osiągnięcie celu strategicznego będzie zrealizowane poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami tego systemu.

Cele szczegółowe strategii to:

1) zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej Państwa;
2) zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni;
3) zmniejszenie skutków incydentów godzących w bezpieczeństwo cyberprzestrzeni;
4) określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni;
5) stworzenie i realizacja spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych;
6) stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni;
7) zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni.

Strategia będzie oddziaływała na następujące grupy użytkowników:

1) **obywateli - poprzez:**
   a) zwiększenie bezpieczeństwa obywateli w cyberprzestrzeni,
   b) podniesienie poziomu zaufania do korzystania z e-usług,
   c) bezpieczny i nieprzerwany dostęp do e-usług;
2) **przedsiębiorców - poprzez:**
   a) podniesienie poziomu zaufania do korzystania z e-usług w procesach biznesowych,

b) zwiększenie bezpieczeństwa operacji, w tym technologicznych i finansowych,
c) bezpieczny i nieprzerwany dostęp do e-usług,
d) rozwój narodowych technologii w sektorze cyberbezpieczeństwa;

3) **pracownicy administracji publicznej - poprzez:**
   a) zapewnienia nieprzerwanej realizacji istotnych funkcji Państwa,
   b) zapewnienie odpowiedniego poziomu bezpieczeństwa informatyzacji procesów administracyjnych i usług,
   c) zapewnienie ciągłości świadczenia e-usług,
   d) zwiększenie odporności na ataki cybernetyczne,
   e) stworzenie zasobu eksperckiego administracji publicznej w zakresie cyberbezpieczeństwa i teleinformatyki;
4) **operatorów usług kluczowych - poprzez:**
   wskazanie kierunków działań państwa mających na celu wspomaganie nieprzerwanego świadczenia usług kluczowych.

ZAKRES STRATEGII

Strategia będzie oddziaływać bezpośrednio lub pośrednio na wszystkich użytkowników cyberprzestrzeni w obrębie Państwa (obywateli, administrację rządową, samorządową, przedsiębiorców) i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe).

Należy podkreślić, że Strategia nie będzie bezpośrednio dotyczyła niejawnych systemów teleinformatycznych, gdyż obszar ochrony informacji niejawnych posiada własne regulacje prawne i stosowne mechanizmy ochronne. Należy jednak mieć na uwadze, że zagrożenia dotyczące systemów jawnych dotyczą również systemów niejawnych, dlatego też działania podejmowane w obszarze właściwym dla Strategii będą miały pośrednie przełożenie na bezpieczeństwo systemów przetwarzających informacje klasyfikowane.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej nie jest strategią rozwoju w rozumieniu ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (*Dz. U. 2016 poz. 383*).

Osiągnięcie celów Strategii wymagać będzie:

1) zorganizowania krajowego systemu cyberbezpieczeństwa, z uwzględnieniem roli podmiotów publicznych i prywatnych (wliczając w to rolę organizacji pozarządowych) oraz obywateli;
2) koordynacji krajowych działań w dziedzinie cyberbezpieczeństwa z działaniami na arenie międzynarodowej, zarówno na poziomie strategiczno-politycznym, jak i operacyjnym;
3) współpracy z ośrodkami akademickimi, sektorem prywatnym oraz organizacjami pozarządowymi w celu zarządzania wiedzą i stymulowania innowacji w dziedzinie cyberbezpieczeństwa w Polsce.

Nowe podejście do problematyki cyberbezpieczeństwa ma polegać na:

1) ochronie w cyberprzestrzeni istotnych funkcji Państwa, tzn. zapewnienia dostaw energii, usług bankowych, transportu, ochrony zdrowia itd.;
2) zapewnieniu całodobowego nadzoru nad bezpieczeństwem w cyberprzestrzeni istotnych danych, usług, serwisów i użytkowników;
3) wprowadzeniu trzypoziomowego systemu ochrony cyberprzestrzeni:
a) zapewnieniu skoordynowanej ochrony cyberprzestrzeni RP już na transgranicznych punktach wymiany Internetu (IXP),
b) dostosowaniu architektury sieci do potrzeb bezpieczeństwa na poziomie branżowym, terytorialnym lub funkcjonalnym (klastry bezpieczeństwa),
c) zapewnieniu bezpieczeństwa danych na poziomie architektury poszczególnych systemów (archiwizacja danych, kopie zapasowe);
4) bezpiecznym użytkowaniu indywidualnych środków komunikacji cyfrowej wykorzystywanych przez obywateli do komunikacji z systemami państwowym (kilkadziesiąt mln urządzeń: PC, tablety, telefony);
5) wprowadzeniu procesu edukacji i szkoleń dla specjalistów odpowiedzialnych za:
a) bezpieczeństwo teleinformatyczne,
b) projektowanie systemów teleinformatycznych,
c) eksploatację systemów teleinformatycznych,
d) użytkowanie systemów teleinformatycznych;
6) wprowadzeniu procedur reagowania na incydenty i współpracy w wymiarze krajowym i zagranicznym;

7) wprowadzeniu standardów dotyczących technologii w zakresie bezpieczeństwa teleinformatycznego.

2. Poszanowanie praw i wolności w cyberprzestrzeni

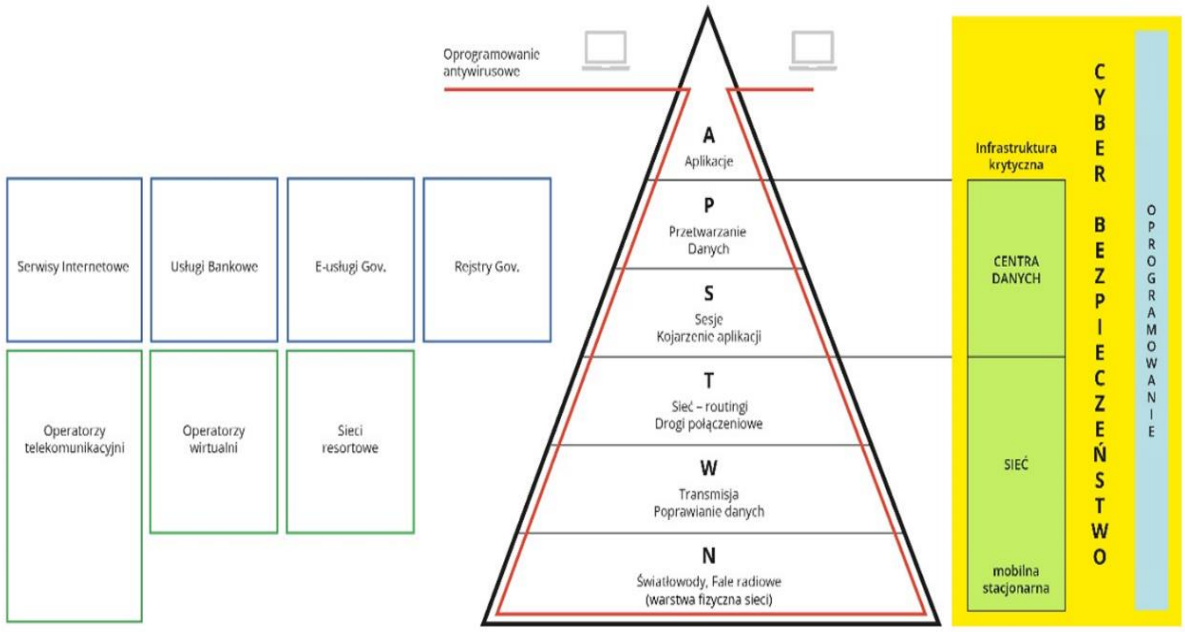
Wszelkie działania podejmowane przez rząd Rzeczypospolitej Polskiej w dziedzinie zwiększania cyberbezpieczeństwa będą się odbywały z poszanowaniem prawa i wolności obywateli. Rząd RP w pełni respektuje prawo do prywatności oraz stoi na stanowisku, że wolny i otwarty Internet jest bardzo istotnym elementem funkcjonowania dzisiejszego społeczeństwa.

Cyberbezpieczeństwo nie może być zapewniane przez Państwo kosztem praw człowieka. Miarą cyberbezpieczeństwa jest nie tylko stopień zabezpieczenia i przeciwdziałanie zagrożeniom dla rozwoju sektora e-commerce, funkcjonowania e-państwa i infrastruktury krytycznej, ale także stopień zabezpieczenia swobodnego pozyskiwania informacji oraz ich przekazywania za pomocą sieci Internet, jak również stopień zabezpieczenia innych form realizacji praw podstawowych w cyberprzestrzeni.

Prawa i wolności nie oznaczają jednak braku odpowiedzialności podczas korzystania z usług dostępnych w sieci Internet. Każda osoba korzystająca z zasobów w cyberprzestrzeni musi być świadoma zagrożeń, jakie mogą ją spotkać lub sama może je stworzyć, gdy w nieodpowiedzialny sposób będzie z tych zasobów korzystała. W Polsce liczba urządzeń umożliwiających korzystanie z Internetu, będących w dyspozycji osób prywatnych, szacowana jest na dziesiątki milionów. Urządzenia te wykorzystywane w celach komunikacji osobistej, rozrywki, zdobywania informacji, prowadzenia aktywności gospodarczej, mogą być podczas kontaktu ze stronami internetowymi o złej reputacji zainfekowane złośliwym oprogramowaniem. Następnie, urządzenia te, łącząc się z systemami zaufanymi, takimi jak systemy administracji publicznej czy bankowości elektronicznej, stwarzają dla nich poważne zagrożenie. Zachowanie w sieci każdego obywatela ma wpływ na bezpieczeństwo pozostałych użytkowników, dlatego działania na rzecz cyberbezpieczeństwa muszą mieć charakter kompleksowy, obejmujący zarówno elementy infrastruktury teleinformatycznej, procedury niezbędne do sprawnego funkcjonowania systemu, jak również zasady dla użytkowników korzystających z tych zasobów. Właśnie minister właściwy ds. informatyzacji musi uwzględniać tę problematykę jako istotną z punku widzenia cyberbezpieczeństwa.

3. Cyberbezpieczeństwo jako istotny element polityki Państwa

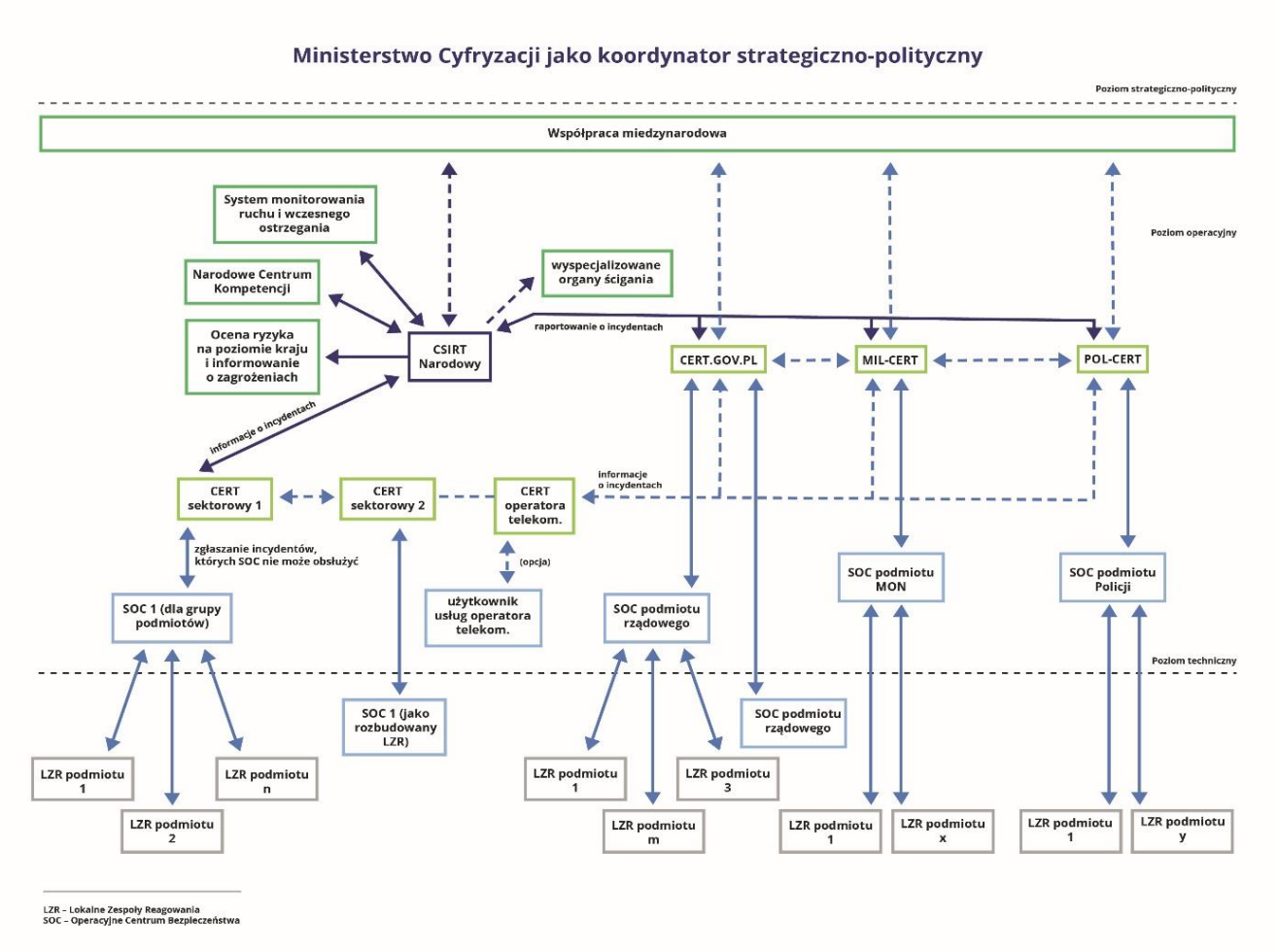
Punktem wyjścia dla działań mających na celu wdrożenie Strategii jest model sieci znany jako Open Systems Interconnection Reference Model (model OSI). Dla każdej z warstw modelu OSI podjęte zostaną stosowne działania, tak w obszarze organizacyjnym, jak i technologicznym.



Rysunek 1. Powiązanie warstw modelu OSI z obszarami cyberbezpieczeństwa.

Wymaga to ścisłego współdziałania zarówno służb odpowiedzialnych za infrastrukturę krytyczną, jak i tych odpowiedzialnych za funkcjonowanie e-usług. Ataki z cyberprzestrzeni mogą dotyczyć nie tylko systemów informacyjnych administracji publicznej i sektora prywatnego, lecz również systemów automatyki przemysłowej (sterowniki PLC, SCADA), w tym automatyki w obiektach infrastruktury krytycznej. Dlatego też systemowe określenie sfer odpowiedzialności za poszczególne sektory bezpieczeństwa cyberprzestrzeni ma fundamentalne znaczenie. Proces zapewniania cyberbezpieczeństwa przebiegać będzie na trzech płaszczyznach: strategicznej, operacyjnej i technicznej. W każdej z tych płaszczyzn wyróżnia się działania o charakterze zarządczym i działania o charakterze technologicznym. Na płaszczyźnie strategicznej dominować będą działania o charakterze zarządczym, natomiast

na płaszczyźnie technicznej działania o charakterze technologicznym. Opisane powyżej podejście ilustruje poniższy rysunek.



Rysunek 2. Struktura krajowego systemu cyberbezpieczeństwa.

3.1. Uwarunkowania wewnętrzne

WYMIAR STRATEGICZNY

Działania związane z zapewnianiem cyberbezpieczeństwa i ochroną przed zagrożeniami pochodzącymi z cyberprzestrzeni muszą się wpisywać w ustanowiony przepisami ład konstytucyjny Państwa i wynikającą z tego ładu odpowiedzialność oraz kompetencje odpowiednich organów władzy publicznej. W wymiarze strategicznym odpowiedzialność za poszczególne sfery bezpieczeństwa Państwa jest następująca:

1) Biuro Bezpieczeństwa Narodowego jako organ doradczy Prezydenta RP opracowuje Doktrynę Cyberbezpieczeństwa Rzeczypospolitej Polskiej, wytyczając kierunki działania wpisujące się w sytuację międzynarodową;
2) Minister Sprawiedliwości pełni wiodąca rolę w procesie stanowienia prawa w zakresie zwalczania cyberprzestępczości;
3) Szef Agencji Bezpieczeństwa Wewnętrznego:

a) jest właściwy w zakresie organizacji systemu w przypadku zagrożenia istotnych interesów Państwa (w tym zagrożeń terrorystycznych),
b) w wykonywaniu bieżących zadań ściśle współpracuje z pozostałymi uczestnikami systemu; strategia nie wpływa na operacyjną obsługę przez ABW incydentów, której zasady wynikają z przepisów prawa;

4) Minister Obrony Narodowej:

a) jest właściwy w zakresie organizacji obrony Państwa,
b) dąży do pozyskania przez Siły Zbrojne RP pełnego spektrum zdolności do działań w cyberprzestrzeni w zakresie aktywnej obrony i działań ofensywnych,
c) organizuje działania na wypadek zagrożenia wojennego i czasu wojny z wykorzystaniem mechanizmów planowania obronnego,
d) przejmuje kierowanie systemem cyberbezpieczeństwa w wyższych stanach gotowości obronnej Państwa,
e) opracowuje w planie operacyjnym zasady działania CSIRT(Computer Security Incident Response Team) Narodowego w stanie kryzysu i czasu wojny,
f) w wykonywaniu bieżących zadań ściśle współpracuje z pozostałymi uczestnikami systemu;

5) Minister Spraw Wewnętrznych i Administracji:

a) jest właściwy w zakresie organizacji działań związanych z zapewnieniem ochrony systemów teleinformatycznych resortu spraw wewnętrznych i administracji,
b) w wykonywaniu bieżących zadań ściśle współpracuje z pozostałymi uczestnikami systemu;

6) Komendant Główny Policji:

a) jest właściwy w zakresie organizacji ścigania przestępstw w obszarze cyberprzestrzeni,
b) jest właściwy w zakresie organizacji działań związanych z zapewnieniem ochrony systemów teleinformatycznych Policji;

7) Minister Cyfryzacji:

a) w swoich działaniach pełni rolę „usługową”, nie wchodząc w kompetencje poszczególnych interesariuszy systemu,
b) jest właściwy w sprawach bezpieczeństwa cyberprzestrzeni zgodnie z ustawą o działach administracji rządowej,
c) podejmuje działania organizacyjno-prawne zwiększające bezpieczeństwo w cyberprzestrzeni: opracowuje projekty aktów prawnych oraz zalecenia w postaci tzw. dobrych praktyk, koordynuje i harmonizuje procesy i procedury zarządzania informacją w zakresie cyberbezpieczeństwa,
d) organizuje współdziałanie pomiędzy sektorami, takimi jak finanse, energetyka, transport, telekomunikacja, rejestry państwowe itd.,
e) organizuje system wczesnego ostrzegania i klastry bezpieczeństwa,
f) w wykonywaniu bieżących zadań zapewnia współpracę z pozostałymi uczestnikami systemu.

Ustawa o krajowym systemie cyberbezpieczeństwa w jasny sposób uporządkuje kompetencje pomiędzy podmiotami zaangażowanymi w ochronę cyberprzestrzeni RP.

Inicjatywy w zakresie cyberbezpieczeństwa podejmowane w Rzeczypospolitej Polskiej muszą zostać skoordynowane, tak by uniknąć ich „wyspowego” charakteru. Wdrożone zostaną mechanizmy współpracy podmiotów prywatnych i państwowych (model oparty na współpracy administracji, biznesu i nauki) przy zapewnieniu odpowiedniego finansowania działań związanych z cyberbezpieczeństwem.

WYMIAR OPERACYJNY

W wymiarze operacyjnym prowadzone będą działania mające na celu zapobieganie, wykrywanie, przeciwdziałanie w odniesieniu do potencjalnych ataków oraz reagowanie na rozwijający się atak, a także informowanie o możliwości wystąpienia ataku. Szybka wymiana informacji jest kluczowa z punktu widzenia minimalizacji potencjalnych negatywnych skutków dla krajowych systemów teleinformatycznych. System ostrzegania i informowania bazujący na ścisłym współdziałaniu wszystkich ogniw funkcjonujących w łańcuchu monitorowania cyberprzestrzeni to minimum zapewniające efektywność całego systemu.

Sprawność działań w wymiarze operacyjnym w dużym stopniu zależna jest od efektywnego systemu zarządzania ryzykiem. Kluczową rolę w tym obszarze odegra system szacowania różnych rodzajów ryzyka w czasie rzeczywistym. Na potrzeby tego procesu niezbędne jest zapewnienie:

1) ustanowienia jednolitej metodyki szacowania ryzyka;
2) prowadzenie bazy informacji o zidentyfikowanych podatnościach;
3) wyznaczenie dla każdego poziomu hierarchii systemu cyberbezpieczeństwa progów dla poziomów ryzyka, od których wymagane jest raportowanie na wyższy poziom.

Na szczycie hierarchii podmiotów zaangażowanych w krajowy system cyberbezpieczeństwa znajdzie się Narodowe Centrum Cyberbezpieczeństwa (NCCyber), z działającym w jego strukturze CSIRT Narodowym. NCCyber funkcjonować będzie przez całą dobę. Praca pozostałych elementów uzależniona będzie od oceny ryzyka dokonanej w sektorach funkcjonalnych. Głównym zadaniem NCCyber będzie zbieranie informacji o zaistniałych incydentach naruszenia bezpieczeństwa, agregowanie tych informacji i ocena pod kątem ryzyka, jakie incydenty te stwarzają dla bezpieczeństwa cyberprzestrzeni. CSIRT Narodowy będzie także udzielał wsparcia dla CSIRT sektorowych w rozwiązywaniu skomplikowanych problemów, w tym może udzielać wsparcia CSIRT sfery publicznej, a w szczególności CERT.GOV.PL, MIL-CERT, POL-CERT, na ich wniosek.

WYMIAR TECHNICZNY

Poziom techniczny to domena aktywności właścicieli sieci i systemów teleinformatycznych, którzy muszą wydzielić siły i środki służące:

1) aktywnej analizie ryzyka;
2) wdrażaniu zabezpieczeń zgodnie z oceną zidentyfikowanych rodzajów ryzyka;
3) monitorowaniu cyberbezpieczeństwa;
4) przeciwdziałaniu atakom.

3.2. Uwarunkowania międzynarodowe

Na forum międzynarodowym, zarówno w Unii Europejskiej, jak też poza nią, m.in. w ONZ, NATO, OBWE, toczą się coraz bardziej zaawansowane dyskusje na temat cyberbezpieczeństwa, które obecnie stało się istotnym elementem polityki zagranicznej państw. Dlatego Rzeczpospolita Polska wzmocni swoje wysiłki na rzecz wypracowania prawno-międzynarodowych warunków dla globalnego cyberbezpieczeństwa. Wymagać to będzie stworzenia silnego zaplecza analitycznego w dziedzinie prawa międzynarodowego i współpracy międzynarodowej w odniesieniu do cyberprzestrzeni.

Wiele krajów wykazuje zwiększoną aktywność w dyskusjach na temat bezpieczeństwa cybernetycznego prowadzonych na forach międzynarodowych, traktując je jako sposób na

realizację szerzej ujmowanych celów i interesów polityki wewnętrznej i zagranicznej, odnoszącej się do takich obszarów jak prawa człowieka, otwartość i nieskrępowany dostęp do Internetu, tworzenie norm i prawa międzynarodowego, realizacja pomocy rozwojowej, promowanie własnych firm z sektora IT, dyplomacja publiczna, pogłębianie współpracy bilateralnej oraz regionalnej.

Przejawem wzrastającego znaczenia międzynarodowych aspektów bezpieczeństwa cybernetycznego jest uwzględnianie ich w strategiach bezpieczeństwa poszczególnych krajów. Typowym rozwiązaniem jest umieszczanie strategii bezpieczeństwa cybernetycznego wśród celów narodowych. Także w strategii bezpieczeństwa cybernetycznego UE przyjętej w 2013 r. jeden z pięciu strategicznych priorytetów dotyczy ustanowienia spójnej polityki międzynarodowej oraz promowania wartości UE.

4. Organizacja krajowego systemu cyberbezpieczeństwa

Zakłada się wdrożenie krajowego systemu cyberbezpieczeństwa, który obejmował będzie całokształt przedsięwzięć niezbędnych do ustanowienia i utrzymania na zakładanym poziomie bezpieczeństwa w cyberprzestrzeni. Kompleksowe podejście do budowy krajowego systemu cyberbezpieczeństwa oznacza, że żaden element systemu nie będzie pominięty w procedurach reagowania na zagrożenia w cyberprzestrzeni.

Rysunek 3.Trzypoziomowy system ochrony cyberprzestrzeni.

Działania Państwa nie mogą ograniczać się wyłącznie do zasobów państwowych i samorządowych, równie istotne jest objęcie systemem sektora prywatnego i obywateli.

Indywidualni użytkownicy cyberprzestrzeni, ale też przedsiębiorcy sektora małych i średnich przedsiębiorstw, korzystając z niezaufanych serwisów internetowych, mogą zainfekować swoje urządzenia złośliwym oprogramowaniem. Sytuacja taka stwarza zagrożenie nie tylko tym użytkownikom, ale również innym użytkownikom cyberprzestrzeni, w tym systemom teleinformatycznym podmiotów publicznych.

Za najistotniejsze uznać należy stworzenie:

1) regulacji dotyczących minimalnych wymagań zapewniających bezpośrednią ochronę danych, uwzględniających budowę systemów zgodnie z normami i zasadami bezpieczeństwa oraz zasad zapewnienia ciągłości ich działania (planowane do ujęcia w ramach ustawy o krajowym systemie cyberbezpieczeństwa);
2) systemu koordynacji działań z zakresu zapobiegania zagrożeniom i atakom na systemy teleinformatyczne w cyberprzestrzeni oraz reagowania na takie zagrożenia i ataki w celu zapewnienia nieprzerwanej realizacji podstawowych funkcji Państwa;
3) mechanizmów służących zapobieganiu zagrożeniom bezpieczeństwa w cyberprzestrzeni i ich wczesnemu wykrywaniu, w tym właściwemu postępowaniu w przypadku zidentyfikowanych incydentów;
4) systemu wykrywania cyberataków i cyberprzestępczości, reagowania na nie i usuwania ich skutków, wraz z odpowiednimi strukturami, wielopoziomową platformą współpracy i stosownymi procedurami (uwzględniając progi reakcji);
5) systemu wczesnego ostrzegania mającego na celu wczesne wykrywanie ataków na kluczową infrastrukturę i istotne funkcje Państwa oraz przeciwdziałanie tym atakom;
6) klastrów bezpieczeństwa dla systemów administracji publicznej w celu zapewnienia bezpiecznego świadczenia usług i bezpieczeństwa danych;
7) programów mających na celu powszechną edukację społeczną oraz specjalistyczną w zakresie ochrony cyberprzestrzeni RP wraz z budowaniem świadomości zagrożeń, świadczenie usług związanych z pomocą w reagowaniu na incydenty komputerowe.

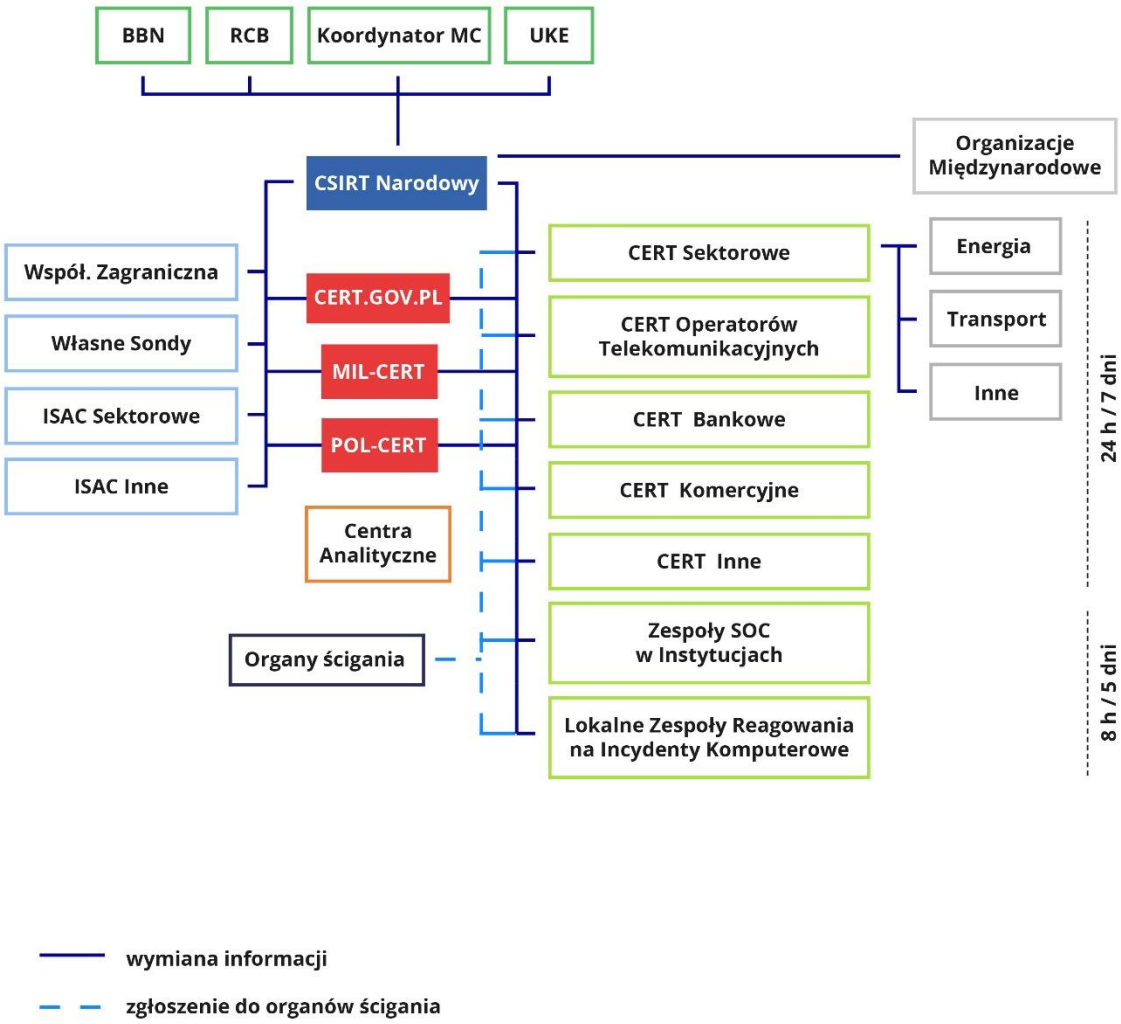
4.1. Budowa systemu

W skład krajowego systemu cyberbezpieczeństwa wejdą:

1) minister właściwy do spraw informatyzacji, jako rządowy organ koordynujący na poziomie polityczno-strategicznym;
2) właściwi ministrowie zgodnie z zakresami kompetencji;
3) NCCyber;

4) CSIRT sektorowe, dla sektorów: administracji publicznej, energetyki, transportu, bankowości, zdrowia, zaopatrzenia w wodę pitną i jej dystrybucji, infrastruktury rynków finansowych oraz infrastruktury cyfrowej;
5) kierownicy urzędów i instytucji objętych zakresem strategii, którzy będą odpowiedzialni za wdrożenie cyberbezpieczeństwa w podległych sobie urzędach i instytucjach.

Budowę systemu przedstawia poniższy schemat:



Rysunek 4. Krajowy system cyberbezpieczeństwa.

4.1.1. Rola ministra właściwego do spraw informatyzacji

Minister właściwy ds. informatyzacji będzie pełnić rolę koordynatora strategiczno-politycznego w sferze cyberbezpieczeństwa RP, odpowiadając za realizację następujących zadań:

1) przygotowanie projektów aktów prawnych niezbędnych do stanowienia wymagań w zakresie cyberbezpieczeństwa;
2) koordynację wypracowywania stanowiska w zakresie regulacji międzynarodowych,
3) koordynację działań związanych z zapewnieniem cyberbezpieczeństwa w administracji publicznej;
4) organizację współpracy z organami władzy publicznej w zakresie cyberbezpieczeństwa, w szczególności z Biurem Bezpieczeństwa Narodowego, a przedstawicielami jednostek samorządu terytorialnego w ramach Komisji Wspólnej Rządu i Samorządu Terytorialnego,
5) organizację współpracy z organizacjami pozarządowymi, w tym, w zakresie edukacji związanej z cyberbezpieczeństwem;
6) pełnienie roli punktu kontaktowego w rozumieniu przepisów dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej, zwanej dalej „Dyrektywą”;
7) nadzorowanie Narodowego Centrum Cyberbezpieczeństwa.

4.1.2. Rola NCCyber

Główne zadanie NCCyber to realizowanie, zadań operacyjnych, wynikających z oceny ryzyka w obszarze cyberbezpieczeństwa na szczeblu krajowym i międzynarodowym. NCCyber będzie także reprezentować Polskę w tworzonej europejskiej sieci CSIRT (CSIRT network).

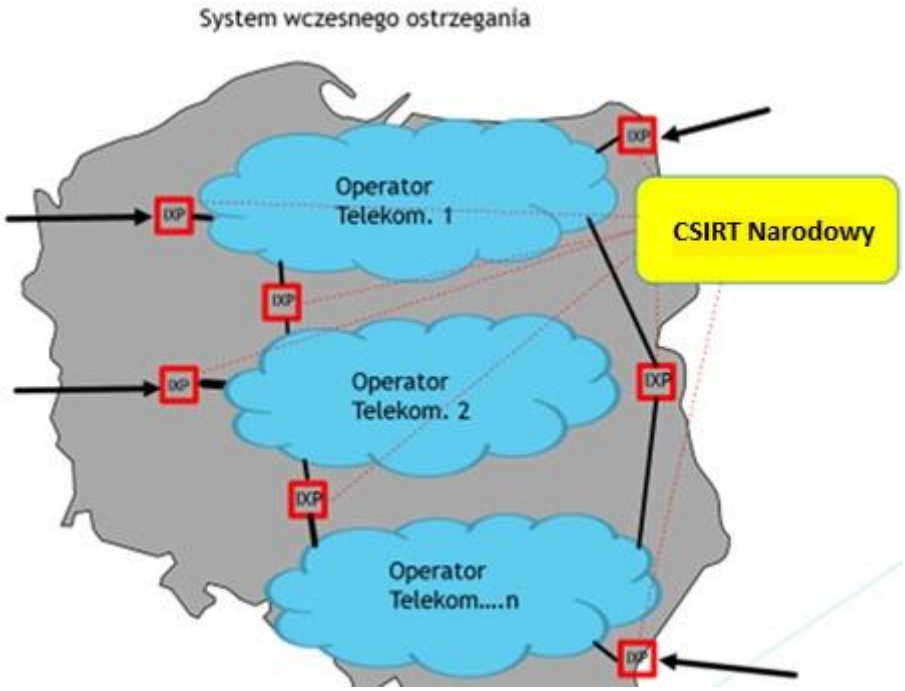
CERT[1] Polska w strukturach NCCyber będzie pełnił rolę CSIRT Narodowego ściśle współpracującego z CSIRT sektorowymi, tym samym będzie koordynował współpracę w ramach powstałej krajowej sieci CSIRT. NCCyber nawiąże także ścisłą współpracę ze

[1] CERT (Computer Emergency Response Team) jest nazwą zastrzeżoną przez Carnegie Mellon University i jej używanie wymaga zgody tego uniwersytetu. Zgodę taką posiada CERT Polska. Dyrektywa NIS posługuje się nazwą CSIRT.

swoimi odpowiednikami za granicą, w szczególności z zespołami CSIRT, które będą pełnić w krajach członkowskich UE rolę CSIRT narodowych.

Narodowe Centrum Cyberbezpieczeństwa zorganizuje i zapewni bezpieczne kanały komunikacyjne umożliwiające korzystanie z usług NCCyber. NCCyber będzie realizowało zadania operacyjne i świadczyło usługi w systemie 24-godzinnym, przez wszystkie dni w roku.

Ważnym zadaniem NCCyber będzie monitorowanie incydentów na poziomie krajowym oraz przekazywanie wczesnych ostrzeżeń, ogłaszanie alarmów, wydawanie ogłoszeń i przekazywanie informacji na temat różnych rodzajów ryzyka i incydentów (rys. 5), poprzez zbieranie danych z transgranicznych punktów wymiany Internetu (IXP). NCCyber jednocześnie będzie oceniało zagrożenia w ruchu międzynarodowym i międzyoperatorskim.



Rysunek 5. System wczesnego ostrzegania o atakach w cyberprzestrzeni.

NCCyber będzie ściśle współpracowało z operatorami usług kluczowych, służąc im merytorycznym wsparciem poprzez m.in. opracowywanie i promocję standardów z dziedziny

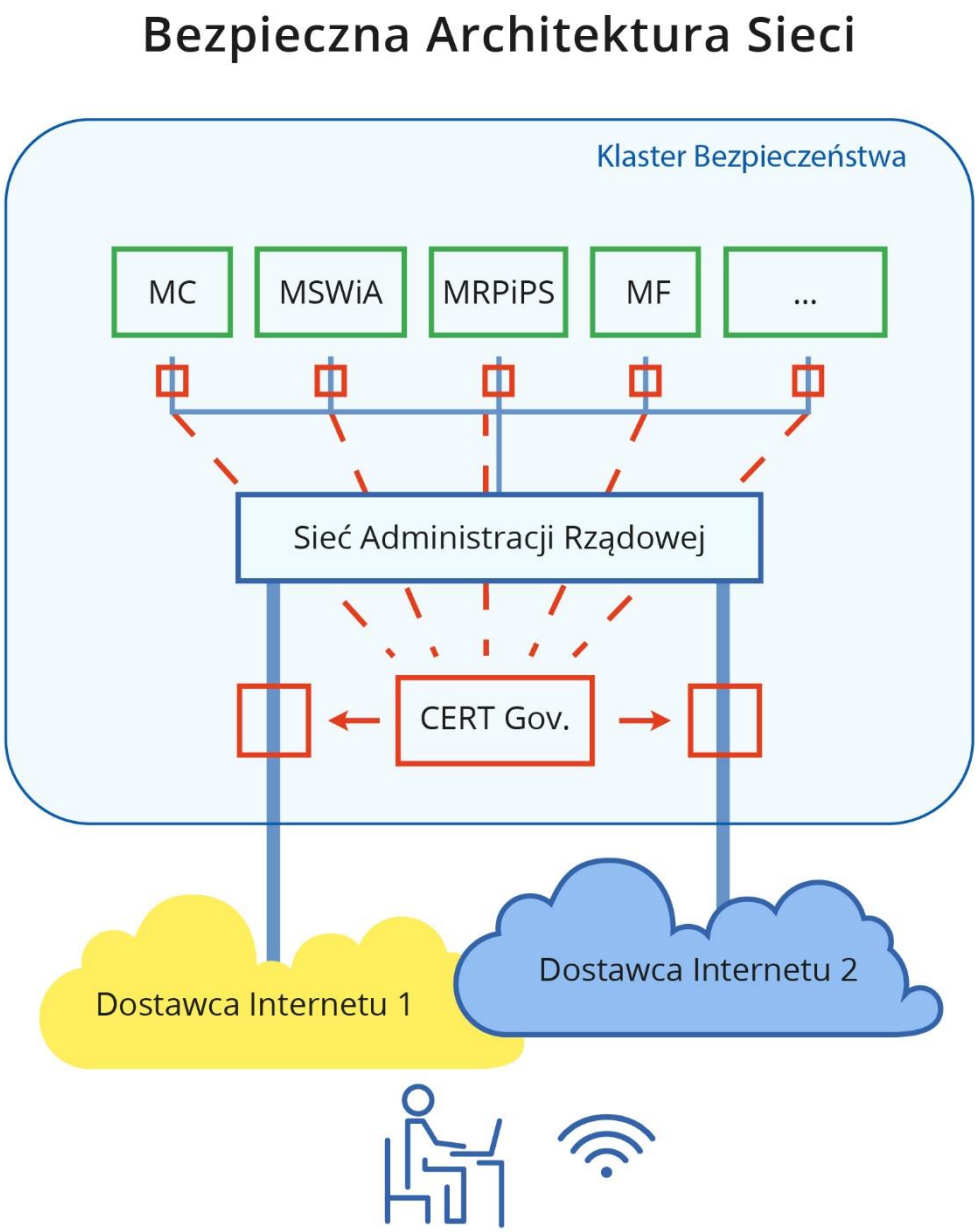
bezpieczeństwa. NCCyber i CERT.GOV.PL będą ściśle współpracować w zakresie incydentów dotyczących cyberbezpieczeństwa w systemach teleinformatycznych infrastruktury krytycznej.

4.1.3. Klastry Bezpieczeństwa

W obszarze administracji publicznej powstaną klastry bezpieczeństwa, które obejmą administrację rządową (na szczeblach centralnym i wojewódzkim) oraz administrację samorządową (na szczeblach gminy, powiatu i województwa). Klastry te zbudowane zostaną w celu zapewnienia dodatkowej ochrony danych oraz przeciwdziałania i zapobiegania niepożądanym zjawiskom w cyberprzestrzeni. W realizacji zadania uczestniczyć będą administratorzy sieci administracji publicznej oraz pełnomocnicy bezpieczeństwa cyberprzestrzeni (PBC), którzy powinni zostać powołani w jednostkach organizacyjnych administracji rządowej. Zadania, jakie w szczególności realizowane będą przez pełnomocników bezpieczeństwa cyberprzestrzeni to: opracowanie projektu systemu zarządzania bezpieczeństwem informacji w cyberprzestrzeni, identyfikowanie i prowadzenie cyklicznych analiz ryzyka, przygotowanie planów awaryjnych oraz ich testowanie.

Szczególną ochroną objęte zostaną rejestry państwowe i serwisy rządowe, które włączone zostaną w tzw. „Rządowy klaster bezpieczeństwa”. Istotną rolę w tym klastrze odgrywać będzie CERT.GOV.PL, znajdujący się w strukturach Agencji Bezpieczeństwa Wewnętrznego, który będzie także pełnił rolę CSIRT sektorowego dla administracji rządowej (rys. 6). CERT.GOV.PL prowadzić będzie obsługę incydentów mających miejsce w klastrze.

Ze względu na specyfikę działań, zarówno ABW jak i MON nie zostaną włączone do struktur klastra bezpieczeństwa.



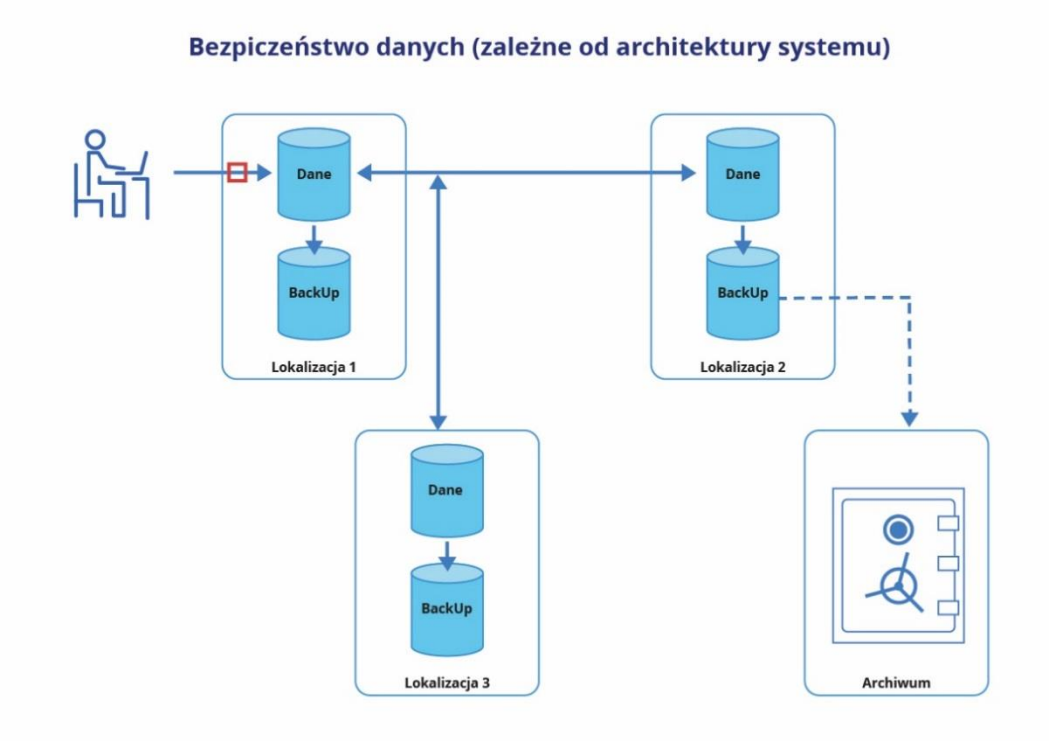
Rysunek 6. Koncepcja rządowego klastra bezpieczeństwa.

4.1.4. Bezpieczeństwo danych

Bezpieczeństwo danych musi być rozpatrywane w dwóch aspektach:

1) bezpośredniej ochrony danych, zależnej od polityki bezpieczeństwa i narzędzi zastosowanych do ochrony tych danych;

2) budowy architektury zwiększającej to bezpieczeństwo (rys. 7).



Rysunek 7. Bezpieczeństwo danych.

4.1.5. Rola kierownictwa podmiotów

W każdej instytucji objętej zakresem ustawy o krajowym systemie cyberbezpieczeństwa, w ramach ochrony cyberprzestrzeni, kierownik jednostki ustanowi system zarządzania bezpieczeństwem informacji w cyberprzestrzeni, w oparciu o obowiązujące normy i najlepsze praktyki (MON nie będzie objęte tym obowiązkiem). System zarządzania bezpieczeństwem informacji stanie się tym samym integralną częścią polityki bezpieczeństwa instytucji.

Przy opracowywaniu polityki bezpieczeństwa uwzględniane będą Polskie Normy z zakresu bezpieczeństwa informacji, a w szczególności grupy norm serii PN ISO/IEC 27000 i innych norm z nią powiązanych. Istotne jest również uspójnienie polityki bezpieczeństwa informacji jednostek organizacyjnych tak, aby zagwarantować wspólny minimalny poziom bezpieczeństwa. Każda instytucja będzie zobowiązana ustanowić, wdrożyć, eksploatować, monitorować, przeglądać, utrzymywać i doskonalić System Zarządzania Bezpieczeństwem Informacji (SZBI) uwzględniający bezpieczeństwo cyberprzestrzeni.

W celu zapewnienia nieprzerwanej realizacji podstawowych funkcji Państwa w sektorach objętych zakresem strategii wymagane będzie, po wprowadzeniu odpowiednich regulacji na poziomie ustawowym:

1) ustanawianie zabezpieczeń i zarządzanie bezpieczeństwem informacji z uwzględnieniem norm krajowych, a w przypadku ich braku – norm międzynarodowych, uznanych standardów niebędących normami oraz powszechnie akceptowanych dobrych praktyk;

2) opracowywanie planów ciągłości działania (Business Continuity Plan – BCP) oraz planów odtworzenia działalności po zaistnieniu incydentu (Disaster Recovery Plan – DRP) z uwzględnieniem norm krajowych, a w przypadku ich braku – norm międzynarodowych, uznanych standardów niebędących normami oraz powszechnie akceptowanych dobrych praktyk;

3) przekazywanie wskazanemu ośrodkowi rządowemu informacji o incydentach z zakresu bezpieczeństwa informacji;

4) funkcjonowanie w sieci wymiany informacji o zagrożeniach.

4.2. Wykwalifikowane kadry i świadome społeczeństwo

Dynamiczny rozwój sektora informatycznego tworzy zapotrzebowanie na wykwalifikowanych specjalistów. Nadchodząca era Internetu Rzeczy (IoT), Smart City, Smart Industry 4.0 znacznie zwiększy zapotrzebowanie na specjalistów z obszaru cyberbezpieczeństwa. Nie oznacza to jednak, że należy zaniedbywać edukację użytkowników. Zakłada się uruchomienie specjalnych programów kształcenia w zakresie cyberbezpieczeństwa, tak aby kształcić świadomych użytkowników systemów oraz wyspecjalizowane kadry, zarówno na potrzeby administracji publicznej, jak i sektora prywatnego. W tym celu administracja publiczna podejmie ścisłą współpracę z sektorem prywatnym, szkołami oraz ośrodkami akademickimi. Należy również dążyć do otwartości szkół i uczelni na współpracę z biznesem oraz otwartości biznesu na współpracę ze szkołami i uczelniami.

Dodatkowo niezmiernie ważne jest opracowanie wydajnego systemu szkoleń dla administracji publicznej, prowadzenie ewidencji osób przeszkolonych oraz właściwy system oceny szkoleń. Są to warunki niezbędne do właściwego funkcjonowania systemu.

4.2.1. Edukacja dla cyberbezpieczeństwa

Edukację w zakresie cyberbezpieczeństwa należy rozpocząć już w szkole podstawowej. W tym celu zakłada się powstanie specjalnych programów nauczania dla dzieci i młodzieży oraz kursów doszkalających dla nauczycieli informatyki.

Konieczne jest uruchomienie w szkołach wyższych nowych kierunków studiów kładących większy nacisk na zagadnienia związane z cyberbezpieczeństwem. Ponadto na pozostałych kierunkach studiów powinny być rozwijane specjalizacje interdyscyplinarne obejmujące zarządzanie bezpieczeństwem informacji, implementację prawa w Internecie oraz zagadnienia związane z rozwojem nowych technologii i wyzwaniami, jakie to stawia przed społeczeństwem.

Równolegle, we współpracy z organizacjami pozarządowymi oraz ośrodkami akademickimi, administracja publiczna podejmie systemowe działania uwrażliwiające społeczeństwo na zagrożenia płynące z cyberprzestrzeni, a także edukacyjne w zakresie praw i wolności w cyberprzestrzeni. Uruchomiona zostanie kampania społeczna, skierowana do różnych grup docelowych (m.in. dzieci, rodziców, seniorów).Społeczna kampania edukacyjno-prewencyjna realizowana będzie także za pośrednictwem środków masowego przekazu (ogólnopolskich, regionalnych i lokalnych).

W ramach kampanii społecznej informacje dotyczące bezpieczeństwa teleinformatycznego oraz przedsięwzięć edukacyjnych i organizacyjno-prawnych podejmowanych w ramach Strategii prezentowane będą na stronach internetowych administracji publicznej, gdzie będą dostępne także interaktywne kursy dotyczące zagadnień bezpieczeństwa.

4.2.2. Szkolenia dla organów ścigania

Ze względu na szybki postęp technologiczny i zmieniające się metody popełniania przestępstw w cyberprzestrzeni i aby skuteczniej przeciwdziałać wciąż rozwijającej się cyberprzestępczości i z nią walczyć, uruchomiony zostanie system szkoleń dla organów ścigania i wymiaru sprawiedliwości.

4.2.3. Szkolenia dla pracowników administracji publicznej

Powinien zostać opracowany i wdrożony system motywowania i podnoszenia kwalifikacji personelu odpowiedzialnego za infrastrukturę teleinformatyczną w jednostce, tak aby zapewnić wysoki poziom kwalifikacji niezbędny do realizacji zadań związanych z ochroną systemów teleinformatycznych. Szkolenia dotyczyć powinny przede wszystkim stosowania procedur ochrony informacji w instytucji, znajomości technik wyłudzania informacji stosowanych w cyberprzestępczości, konsekwencji złamania zabezpieczeń przez cyberprzestępców, oraz procedur obowiązujących w przypadku udanego ataku lub jego próby.

Szkolenia z zakresu bezpieczeństwa teleinformatycznego powinny obejmować wszystkich pracowników.

4.2.4. Program „Złota Setka”

W celu podnoszenia kompetencji pracowników administracji państwowej, równolegle z wykorzystaniem innych instrumentów wspierających ich aktywność, uruchomiony zostanie rządowy program „Złota Setka”. Będzie to program stypendialny dla specjalistów z obszaru IT i bezpieczeństwa teleinformatycznego mający na celu pozyskiwanie, utrzymywanie i promowanie najlepiej wykwalifikowanej kadry specjalistów w administracji państwowej. Minister właściwy do spraw informatyzacji dysponował będzie budżetem na stypendia dla najlepszych pracowników. Stypendium wypłacane będzie dodatkowo do pobieranej przez pracownika pensji. W ten sposób w administracji państwowej powstanie grupa bardzo dobrze wykwalifikowanych specjalistów, stanowiących jej zasób ekspercki. Na konieczność uruchomienia takiego programu wskazuje niekonkurencyjność płac w administracji państwowej w stosunku do realiów rynkowych. Zakłada się zakwalifikowanie do programu około stu specjalistów z obszaru bezpieczeństwa i informatyki o ponadprzeciętnych umiejętnościach. Specjaliści poszukiwani będą we wszystkich komórkach organizacyjnych administracji państwowej. Zakwalifikowanie do programu wymagało będzie spełnienia dwóch warunków:

1) ponadprzeciętne kwalifikacje (potwierdzone stosownymi certyfikatami bądź praktycznymi umiejętnościami);

2) zgoda przełożonego na to aby dana osoba, w razie potrzeby, mogła być skierowana, na wniosek ministra właściwego ds. informatyzacji, do wykonywania zadań na rzecz administracji państwowej.

4.3. Krajowy system monitorowania ryzyka

Minister właściwy ds. informatyzacji za pośrednictwem NCCyber będzie nadzorował i przeprowadzał krajowe szacowanie ryzyka. W tym celu stworzona zostanie, spójna z innymi, metodyka szacowania ryzyka. Docelowo dąży się do tego, by funkcjonowała jedna metodyka szacowania ryzyka, która obejmie wszystkie aspekty funkcjonowania instytucji (w tym także aspekt teleinformatyczny).

NCCyber, na podstawie informacji przekazywanych z instytucji administracji publicznej oraz operatorów usług kluczowych, prowadzić będzie krajowy system analizy ryzyka. W obszarze operacyjnym informacje te przekazywane będą w trybie online.

5. Koordynacja działań międzynarodowych w dziedzinie cyberbezpieczeństwa

Celem polityki Polski w zakresie cyberbezpieczeństwa będzie stymulacja środowiska międzynarodowego w taki sposób, aby uzyskać jak największe korzyści z rozwoju aktywności w cyberprzestrzeni przy równoczesnym poszanowaniu praw człowieka i wolności obywatela. Bezpieczeństwo cybernetyczne zyskuje coraz ważniejsze miejsce w polityce wewnętrznej i międzynarodowej krajów UE i NATO, czemu towarzyszy wzmacnianie zdolności operacyjnych, instytucjonalnych i militarnych. Także w Polsce dostrzegana jest konieczność systemowego zajęcia się tą problematyką, co znajduje odbicie m.in. w pracach podejmowanych w Ministerstwie Cyfryzacji, Ministerstwie Obrony Narodowej i Agencji Bezpieczeństwa Wewnętrznego.

Polska będzie wzmacniać obecność i aktywność w różnych międzynarodowych gremiach, m.in. na forum UE, NATO (wiodąca rola MON), OECD, ONZ. Obecnie podejmowane działania są rozproszone i mają charakter wyspowy. Konieczna jest więc ich konsolidacja i wypracowanie jednolitego, spójnego polskiego stanowiska na temat współpracy zagranicznej w zakresie cyberbezpieczeństwa.

Minister właściwy ds. informatyzacji, w ramach swoich kompetencji i we współpracy ze wszystkimi zainteresowanymi resortami, będzie dzielił niezbędną w tym zakresie wiedzę i koordynował wypracowywanie spójnych komunikatów (w szczególności poprzez koordynację działań i udział w grupach roboczych międzynarodowych gremiów m.in. na poziomie UE).

W ramach Narodowego Centrum Cyberbezpieczeństwa prowadzona będzie współpraca międzynarodowa na poziomie techniczno-operacyjnym. Na poziomie strategicznym współpracę tę realizował będzie Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji. Zadaniem departamentu będzie prowadzenie analiz i w razie potrzeby wypracowywanie roboczego stanowiska dotyczącego międzynarodowej tematyki cyberbezpieczeństwa. Dotyczy to takich aspektów cyberbezpieczeństwa jak: cyberdyplomacja, partnerstwo publiczno-prywatne, wypracowywanie norm prawa międzynarodowego, cyberprzestępczość oraz pośrednio lub bezpośrednio wszystkich innych powiązanych z cyberbezpieczeństwem tematów, tj. Internet Rzeczy, Inteligentne Miasta, Big Data, Cloud Computing itp.

Ze względu na wrażliwość tematu i konieczność łączenia kwestii współpracy międzynarodowej z wiedzą i praktycznym doświadczeniem (w szczególności operacyjno-

technicznym), minister właściwy ds. informatyzacji będzie dokonywał, na poziomie roboczym i w ramach swoich kompetencji, we współpracy z innymi zainteresowanymi podmiotami, szczegółowych analiz problemów z zakresu cyberbezpieczeństwa. Wypracowane stanowisko wykorzystywane będzie przy tworzeniu międzynarodowych ram prawnych.

Wszelkie decyzje wykraczające poza zakres roboczy będą konsultowane z Ministerstwem Spraw Zagranicznych, jako podmiotem odpowiedzialnym za politykę zagraniczną Polski. Działania podejmowane przez ministra właściwego ds. informatyzacji będą miały charakter pomocniczy i systematyzujący wiedzę nt. polityki zagranicznej w zakresie cyberbezpieczeństwa, nie będą stanowić ingerencji w kompetencje pozostałych podmiotów, w zakresie prowadzonej przez nie polityki międzynarodowej.

W celu zacieśnienia i usystematyzowania podejmowanych na arenie międzynarodowej działań zakłada się rozszerzenie kompetencji istniejącego Zespołu Zadaniowego ds. Bezpieczeństwa Cyberprzestrzeni RP, o kwestie związane z bieżącą wymianą informacji dotyczących podejmowanych w poszczególnych resortach działań z zakresu prowadzonej współpracy międzynarodowej w obszarze cyberbezpieczeństwa.

Polityka zagraniczna nie może być skutecznie prowadzona bez obecności przedstawicieli Polski na różnych forach międzynarodowych. Dlatego też Polska będzie stopniowo wzmacniać obecność za granicą poprzez wymianę informacji z innymi krajami, budowę niezbędnych koalicji i sojuszy, aktywne zaangażowanie w tworzenie międzynarodowego systemu cyberbezpieczeństwa.

6. Współpraca z ośrodkami akademickimi, sektorem prywatnym i organizacjami pozarządowymi

Niezwykle ważnym elementem budowania sprawnego systemu cyberbezpieczeństwa jest zaangażowanie wszystkich interesariuszy. Rozwijana będzie współpraca sektora publicznego z sektorem prywatnym i organizacjami pozarządowymi oraz ośrodkami akademickimi i centrami naukowo-badawczymi.

6.1. Forum ds. Cyberbezpieczeństwa

Minister właściwy ds. informatyzacji, we współpracy z pozostałymi instytucjami, zarówno z sektora publicznego jak i prywatnego, będzie diagnozował potrzeby i ustalał priorytety współpracy w zakresie cyberbezpieczeństwa. W tym celu powołane zostanie Forum do spraw Cyberbezpieczeństwa skupiające wszystkie zainteresowane krajowe podmioty. W ramach Forum powołane zostaną grupy eksperckie pracujące nad konkretnymi tematami. Dzięki

takiemu rozwiązaniu zapewniony zostanie właściwy przepływ informacji pomiędzy interesariuszami systemu oraz bieżąca wymiana myśli. Prawidłowo diagnozowane będą także kierunki działań i rozwoju cyberbezpieczeństwa w Polsce.

6.2. Współpraca publiczno-prywatna

W działaniach zmierzających do zwiększenia bezpieczeństwa w cyberprzestrzeni ważnymi partnerami dla instytucji rządowych i innych podmiotów odpowiedzialnych za bezpieczeństwo teleinformatyczne są producenci sprzętu i oprogramowania.

W celu podniesienia poziomu bezpieczeństwa teleinformatycznego użytkowników cyberprzestrzeni, a także systemów teleinformatycznych prowadzone będą działania polegające na współpracy z komercyjnymi partnerami będącymi producentami oprogramowania i sprzętu teleinformatycznego. Główny nacisk położony zostanie na:

1) powszechne wdrożenie w jednostkach administracji publicznej i podmiotach niepublicznych narzędzi służących zapobieganiu zagrożeniom bezpieczeństwa w cyberprzestrzeni i ich wczesnemu wykrywaniu, w tym właściwemu postępowaniu w przypadku zidentyfikowanych incydentów, a w szczególności:
    a) budowę systemu wczesnego ostrzegania mającego na celu wczesne wykrywanie ataków na kluczową infrastrukturę w Polsce i przeciwdziałanie im,
    b) budowę klastrów bezpieczeństwa dla systemów administracji publicznej w celu zapewniania nieprzerwanego świadczenia usług w przypadku rozległych ataków z cyberprzestrzeni na infrastrukturę tej administracji;
2) wprowadzanie na rynek urządzeń i oprogramowania standardowo zawierającego skonfigurowane rozwiązania pozwalające na zapewnienie minimalnego poziomu bezpieczeństwa.

Cyberbezpieczeństwo stanie się bodźcem do rozwoju polskich ośrodków akademickich oraz centrów naukowo-badawczych.

6.3. Prace badawcze i rozwojowe – wsparcie ze strony środowisk naukowo-badawczych oraz organizacji pozarządowych

W związku z dynamicznie rozwijającym się rynkiem usług cyfrowych, w szczególności z perspektywą zmiany aktualnie użytkowanego w sieci Internet protokołu IPv4 na rzecz protokołu IPv6, oraz w związku z rozwojem idei IoT, Smart City, jak również Industry 4.0

zachodzi konieczność intensyfikacji działań badawczych i rozwojowych dotyczących nowych zagrożeń z nimi związanych.

W tym celu wspólnie z Narodowym Centrum Badań i Rozwoju uruchomione zostaną programy badawcze, mające na celu przygotowanie i wdrożenie nowych metod ochrony przed zagrożeniami pochodzącymi z cyberprzestrzeni.

We współpracy ze środowiskiem naukowo-akademickim zostaną opracowane programy badawcze mające na celu:

1) ocenę skuteczności zabezpieczeń i odporności cyberprzestrzeni RP na cyberzagrożenia;
2) ocenę skuteczności reagowania za zagrożenia;
3) analizy tendencji w zakresie nowych cyberprzestępstw, cyberterroryzmu i metod ich zwalczania;
4) badanie metod ataków i sposobów przeciwdziałania tym atakom.

Do głównych zadań w tym zakresie należy zaliczyć m.in. badanie i opisywanie sposobów i metod ataków, badanie cyberprzestępstw, cyberterroryzmu, a także opracowywanie skutecznych metod przeciwdziałania. Zakłada się opracowanie rozwiązań umożliwiających:

1) szybką identyfikację zagrożeń;
2) usprawnienie systemu informowania o zagrożeniach;
3) podniesienie efektywności zabezpieczeń proceduralno-organizacyjnych i technicznych;
4) skuteczne informowanie użytkowników cyberprzestrzeni o zagrożeniach;
5) podnoszenie wiedzy informatycznej użytkowników cyberprzestrzeni;
6) wypracowanie metod obrony przed zmasowanymi atakami z cyberprzestrzeni.

6.4. Naukowy Akademicki Klaster Cyberbezpieczeństwa

W celu stworzenia platformy naukowej podnoszącej kompetencje ośrodków naukowych w obszarze cyberbezpieczeństwa, w oparciu o wyższe uczelnie oraz ośrodki naukowo-badawcze specjalizujące się w technicznej warstwie cyberbezpieczeństwa, planowane jest powstanie Naukowego Akademickiego Klastra Cyberbezpieczeństwa (NAKC). Budowa klastra pozwoli w pełni wykorzystać potencjał polskich naukowców i wzmocnić rozwój polskiej nauki. NAKC będzie wykorzystywany jako środowisko badawcze i edukacyjne, nie tylko dla studentów zajmujących się tematyką cyberbezpieczeństwa, ale także dla pozostałych członków systemu cyberbezpieczeństwa. Stanie się tym samym integralną częścią systemu cyberbezpieczeństwa RP.

7. Finansowanie

Realizacja Strategii wymaga dedykowanego systemu finansowania. Należy podkreślić, że już obecnie, na mocy obowiązujących przepisów[2], podmioty realizujące zadania publiczne są zobowiązane do ujmowania w swoich planach finansowych nakładów na cyberbezpieczeństwo. Koszty te powiększą się o nakłady przeznaczone na działania integracyjne związane z budową krajowego systemu cyberbezpieczeństwa. Szczegółowa wielkość i struktura kosztów poszczególnych projektów będzie określona w procesie inicjowania konkretnych projektów.

[2] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012 r., poz. 526 z późn. zm.)