RZECZPOSPOLITA POLSKA

MINISTERSTWO SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

RZĄDOWY PROGRAM OCHRONY CYBERPRZESTRZENI RZECZYPOSPOLITEJ POLSKIEJ NA LATA 2011-2016

Wersja 1.1

WARSZAWA

CZERWIEC 2010

Metryka dokumentu:

Autor	*Departament Ewidencji Państwowych i Teleinformatyki MSWiA*
Tytuł	*Rządowy program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016*
Wersja	*1.1*
Status	*Projekt dokumentu kierowany do uzgodnień resortowych*
Liczba stron	*33*
Liczba załączników	*27*

Decyzja do rozesłania dokumentu do uzgodnień międzyresortowych:

Data	Organ
13.09.2010	*Podsekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji*

Przyjęcie dokumentu:

Data	Organ
	Komitet do Spraw Europejskich

Przyjęcie dokumentu:

Data	Organ
	Komitet Rady Ministrów ds. Informatyzacji i Łączności

Przyjęcie dokumentu:

Data	Organ
	Stały Komitet Rady Ministrów

Przyjęcie dokumentu:

Data	Organ
	Rada Ministrów

Spis treści:

Rysunki:

Załączniki:

1. Wprowadzenie

W obliczu globalizacji, ochrona cyberprzestrzeni stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa. W czasie, gdy panuje swoboda przepływu osób, towarów, informacji i kapitału – bezpieczeństwo demokratycznego państwa zależy od wypracowania mechanizmów pozwalających skutecznie zapobiegać i zwalczać zagrożenia dla bezpieczeństwa cyberprzestrzeni.

Obecnie w cyberprzestrzeni granica między pokojem a wojna staje się coraz bardziej umowna. Wynika stąd potrzeba zagwarantowania odpowiednich form komunikacji pomiędzy częścią wojskową (co do zasady niejawną w rozumieniu UOIN), a częścią cywilną (w zasadniczej części jawną w rozumieniu UOIN). W dodatku obiektem cyber wojny są elementy infrastruktury cywilnej. Należy w związku z tym dopracować mechanizmy komunikacji w obszarze cywilnym, uregulować prawnie, wprowadzając dotkliwe sankcje karne za ich łamanie – z jednej strony – a z drugiej intuicyjnie istnieje konieczność ustanowienia kanałów wymiany informacji w obie strony. Uważa się, iż w przypadku cyberataku, zaatakowane zostaną zarówno struktury wojskowe jak i cywilne, które powinny mieć zdolność współpracy, która bez sprawnych kanałów wymiany informacji skaże Państwo na porażkę.

Rada Europejska w przyjętej w 2003 roku Europejskiej Strategii Bezpieczeństwa uznała zjawisko terroryzmu za podstawowe zagrożenie dla interesów UE.

Systemy i sieci teleinformatyczne eksploatowane przez administrację rządową, organy władzy ustawodawczej, władzy sądowniczej, samorządu terytorialnego, a także strategiczne z punktu widzenia bezpieczeństwa państwa przedsiębiorcy (np. podmioty działające w obszarze telekomunikacji, energii, gazu, bankowości, a także podmioty o szczególnym znaczeniu dla obronności i bezpieczeństwa państwa, podmioty działające w obszarze ochrony zdrowia) jak również przedsiębiorcy oraz użytkownicy indywidualni cyberprzestrzeni będą objęte niniejszym *Programem* i rozumiani jako użytkownicy cyberprzestrzeni.

Z uwagi na wzrost zagrożeń ze strony sieci publicznych, od których całkowita separacja jest niemożliwa, a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne, niezbędne jest skoordynowanie działań w zakresie zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni, które umożliwią szybkie i efektywne reagowanie na ataki wymierzone przeciwko systemom, sieciom teleinformatycznym i oferowanym przez nie usługom.

Przedmiotem niniejszego „*Rządowego Programu w zakresie ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016”*, zwanego dalej *Programem* – są propozycje działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni.

Program nie obejmuje swoim obszarem zadaniowym niejawnych sieci i systemów teleinformatycznych. Należy podkreślić, że obszar ochrony informacji niejawnych posiada własne regulacje prawne i stosowne mechanizmy ochronne. Posiada struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych, przechowywanych w wydzielonych systemach i sieciach teleinformatycznych. Podstawowym dokumentem prawnym jest ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 2005 r. Nr 196, poz.1631 z późn. zm.).

1.1.Definicje

1. *Cyberprzestrzeń* – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.
2. *Cyberprzestrzeń RP (dalej jako CRP)* – cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe).
3. *Cyberprzestępstwo* – czyn zabroniony popełniony w obszarze cyberprzestrzeni.
4. *Cyberterroryzm* – cyberprzestępstwo o charakterze terrorystycznym.
5. *Cyberatak* – celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni, bez konieczności angażowania personelu lub innych użytkowników. Umożliwia ominięcie lub osłabienie sprzętowych i programowych mechanizmów kontroli dostępu.
6. *Incydent* – związany z bezpieczeństwem informacji, rozumiany jako pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji – (wg norm PN-ISO/IEC 27000). Incydent rozumiany jest także, jako niekorzystne zdarzenie związane z systemem informatycznym, które według wewnętrznych reguł lub zaleceń dotyczących bezpieczeństwa, jest awarią i/lub powoduje domniemanie lub faktyczne naruszenie ochrony informacji, albo powoduje naruszenie własności.
7. *Krytyczna infrastruktura teleinformatyczna* – infrastruktura krytyczna wyodrębniona w systemie łączności i sieciach teleinformatycznych i ujawniona w wykazie Infrastruktury Krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym.
8. *Ochrona cyberprzestrzeni* – zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu niezakłócone funkcjonowanie i bezpieczeństwo cyberprzestrzeni.
9. *Operator teleinformatycznej infrastruktury krytycznej* – właściciel oraz posiadacz samoistny i zależny[1] obiektów, instalacji, urządzeń i usług infrastruktury krytycznej, wyodrębnionych w systemie łączności i sieci teleinformatycznych i ujawnionych w wykazie infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym.
10. *OSI* – Open System Interconnection – jest to model odniesienia dla większości rodzin protokołów komunikacyjnych. Podstawowym założeniem modelu jest podział na systemów na 7 warstw współpracujących ze sobą w ściśle określony sposób.;
11. *Przedsiębiorca*– jest przedsiębiorcą w rozumieniu art. 4 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2007 r. Nr 155, poz. 1095, z późn. zm.) lub każda inna jednostka organizacyjna, niezależnie od formy własności.
12. *Punkt sektorowy* – punkt kontaktu pomiędzy podmiotami działającymi w tej samej branży umożliwiający przepływ informacji pomiędzy nimi a właściwymi zespołami CERT lub Abuse. CERT (Computer Emergency Response Team) jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. Abuse to zwyczajowa nazwa działu bezpieczeństwa u dostawcy usług internetowych, który zarządza procesem reagowania na incydenty komputerowe i rozpatrywaniem skarg dotyczących nadużyć.

[1] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z dnia 18 maja 1964 r. z późn. zm.) - Tytuł IV. Posiadanie - art. 336. Posiadaczem rzeczy jest zarówno ten, kto nią faktycznie włada jak właściciel (posiadacz samoistny), jak i ten, kto nią faktycznie włada jak użytkownik, zastawnik, najemca, dzierżawca lub mający inne prawo, z którym łączy się określone władztwo nad cudzą rzeczą (posiadacz zależny).

1.2. Cel strategiczny

Celem strategicznym Programu jest zapewnienie ciągłego bezpieczeństwa cyberprzestrzeni Państwa.

Osiągnięcie celu strategicznego wymaga stworzenia ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy administracją publiczną, oraz innymi podmiotami i użytkownikami cyberprzestrzeni RP, w tym przedsiębiorcami.

1.3. Cele szczegółowe

1. Zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej, w tym teleinformatycznej infrastruktury krytycznej państwa.
2. Zmniejszenie skutków naruszeń bezpieczeństwa cyberprzestrzeni.
3. Zdefiniowanie kompetencji podmiotów odpowiedzialnych za ochronę cyberprzestrzeni.
4. Stworzenie i realizacja spójnego dla wszystkich podmiotów administracji publicznej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych.
5. Stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za ochronę cyberprzestrzeni oraz przedsiębiorcami, dostarczającymi usługi w cyberprzestrzeni i operatorami teleinformatycznej infrastruktury krytycznej.
6. Zwiększenie świadomości użytkowników w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni.

Cele *Programu* będą realizowane poprzez:

- stworzenie systemu koordynacji przeciwdziałania i reagowania na zagrożenia i ataki na cyberprzestrzeń, w tym ataki o charakterze cyberterrorystycznym;
- powszechne wdrożenie wśród jednostek administracji publicznej, a także podmiotów niepublicznych mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń dla bezpieczeństwa cyberprzestrzeni oraz właściwemu postępowaniu w przypadku stwierdzonych incydentów;
- powszechną edukację społeczną oraz specjalistyczną edukację w zakresie ochrony cyberprzestrzeni RP.

1.4. Adresaci programu

Adresatami *Programu* są wszyscy użytkownicy cyberprzestrzeni w obrębie państwa i w lokalizacjach poza jego terytorium gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe). Cyberprzestrzeń państwa w przypadku Polski określana jest również mianem cyberprzestrzeni RP (CRP).

Ze względu na charakter i istotę celów Programu, należy wyróżnić kilka grup adresatów:

1. Organy władzy publicznej:
   1.1. administracja rządowa;
      a) naczelne organy administracji rządowej: Prezes Rady Ministrów, Rada Ministrów, ministrowie i przewodniczący określonych w ustawach komitetów;
      b) centralne organy administracji rządowej: organy inne niż wymienione w pkt. 1.1 lit. a), tj. organy podporządkowane Prezesowi Rady Ministrów bądź poszczególnym ministrom;
      c) terenowe organy administracji rządowej: wojewoda, organy administracji zespolonej i niezespolonej.

1.2. administracja samorządowa (szczebel gminny, powiatowy i wojewódzki):
   a) organy stanowiące (sejmik województwa, rada powiatu, rada gminy);
   b) organy wykonawcze (marszałek i zarząd województwa, starosta i zarząd powiatu, wójt (burmistrz, prezydent);

   a także inne, podległe im jednostki organizacyjne lub przez nie nadzorowane.

1.3. administracja państwowa (jednostki nie należące do administracji rządowej i samorządowej):
   a) Prezydent Rzeczypospolitej Polskiej;
   b) Krajowa Rada Radiofonii i Telewizji;
   c) Rzecznik Praw Obywatelskich;
   d) Rzecznik Praw Dziecka;
   e) Krajowa Rada Sądownictwa;
   f) organy kontroli państwowej i ochrony prawa;
   g) Narodowy Bank Polski;
   h) Komisja Nadzoru Finansowego;
   i) centralne organy administracji podległe Sejmowi i Senatowi Rzeczypospolitej Polskiej, nie wymienione powyżej;
   j) państwowe osoby prawne i inne niż wymienione powyżej państwowe jednostki organizacyjne.

2. Operatorzy infrastruktury krytycznej, których działalność jest zależna i nie zależna od prawidłowego funkcjonowania cyberprzestrzeni.
3. Przedsiębiorcy oraz użytkownicy indywidualni cyberprzestrzeni.
4. Inne instytucje będące użytkownikami cyberprzestrzeni.

1.5. Realizatorzy - rola i odpowiedzialność

Za ochronę CRP odpowiedzialny jest Prezes Rady Ministrów, który zadania w tym zakresie wykonuje poprzez:

1. Ministra Spraw Wewnętrznych i Administracji,
2. Ministra Obrony Narodowej,
3. Szefa Agencji Bezpieczeństwa Wewnętrznego,
4. Szefa Służby Kontrwywiadu Wojskowego.

Wiodące role w realizacji *Programu* odgrywają: Ministerstwo Spraw Wewnętrznych i Administracji (MSWiA), Agencja Bezpieczeństwa Wewnętrznego (ABW), Ministerstwo Obrony Narodowej oraz Służba Kontrwywiadu Wojskowego (w zakresie systemów leżących w gestii Ministerstwa Obrony Narodowej), jako podmioty odpowiedzialne za bezpieczeństwo wewnętrzne państwa zgodnie z posiadanymi kompetencjami. Natomiast Rządowe Centrum Bezpieczeństwa odpowiedzialne jest za koordynację działań w zakresie ochrony teleinformatycznej infrastruktury krytycznej.

Z uwagi na cel i przedmiot *Programu*, realizacja zadań oraz osiągnięcie zakładanych skutków wymaga stworzenia mechanizmów zaangażowania i współpracy podmiotów pozostających poza administracją publiczną, w szczególności przedsiębiorców.

Ponieważ jedynie część infrastruktury teleinformatycznej jest własnością państwa, natomiast większość zasobów stanowi własność prywatną, dużą rolę w realizacji programu powinny mieć ci przedsiębiorcy, którzy są właścicielami zasobów stanowiących infrastrukturę państwa.

Za realizację programu, zgodnie z posiadanymi kompetencjami, odpowiadają:

- Prezes Rady Ministrów;
- Minister Edukacji Narodowej;
- Minister Nauki i Szkolnictwa Wyższego;
- Minister Obrony Narodowej;
- Minister Spraw Wewnętrznych i Administracji;
- Szef Agencji Bezpieczeństwa Wewnętrznego;
- Szef Służby Kontrwywiadu Wojskowego;
- Dyrektor Rządowego Centrum Bezpieczeństwa;
- Komendant Główny Policji;
- Komendant Główny Straży Granicznej;
- Komendant Główny Państwowej Straży Pożarnej;
- inne organy administracji publicznej;
- przedsiębiorcy – właściciele zasobów stanowiących krytyczną infrastrukturę teleinformatyczną państwa.

1.6. Nadzór i koordynacja wdrożenia Programu

Ze względu na międzyresortowy charakter *Programu,* organem nadzorującym jego wdrożenie jest Rada Ministrów. Natomiast podmiotem odpowiedzialnym za realizację *Programu* w imieniu Rady Ministrów jest Minister Spraw Wewnętrznych i Administracji, który poprzez Urząd Ministra będzie obsługiwał powołany *Międzyresortowy Zespół ds. Koordynacji Ochrony Cyberprzestrzeni RP*.

Sposób, zasady oraz uprawnienia Ministra Spraw Wewnętrznych i Administracji zostaną przedstawione w rozporządzeniu Rady Ministrów w sprawie powołania *Międzyresortowego Zespołu ds. Koordynowania Ochrony Cyberprzestrzeni RP*.

1.7. Kontekst prawny

Podstawowymi w obszarze bezpieczeństwa zasobów teleinformatycznych są następujące akty prawne:

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. *(Dz.U. z 1997 r. Nr 78, poz.483, z późn. zm.)*;
- Ustawa z dnia 6 czerwca 1997 r. Kodeks karny *(Dz.U. z 1997, Nr 88, poz. 53, z późn. zm.);*
- Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne *(Dz. U. z 2004 r. Nr 171, poz.1800, z późn. zm.);*
- Ustawa z dnia 24 marca 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu *(Dz.U. z 2002 r. Nr 74, poz. 676, z późn. zm.);*
- Ustawa z dnia 6 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego *(Dz.U. z 2006 r. Nr 104, poz. 709, z późn. zm.);*
- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym *(Dz.U. z 2007 r. Nr 89, poz. 590);*
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne *(Dz. U. z 2005 r. Nr 64, poz. 565, z późn. zm.);*

- Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych *(Dz.U. z 2005 r. Nr 196, poz.1631, z późn. zm.);*
- Ustawa z dnia 29 sierpnia 1997 r o ochronie danych osobowych *(Dz.U. 2002 nr 101, poz. 926 ze zm.);*
- Ustawa z dnia 27 lipca 2001r. o ochronie baz danych *(Dz.U. 2001 nr 128, poz. 1402);*
- Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe *(Dz.U. 1997 nr 140, poz. 939);*
- Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego *(Dz.U. z 2005 r. Nr 171, poz. 1433);*
- Rozporządzenie Rady Ministrów z dnia 28 marca 2005 r. w sprawie Planu Informatyzacji Państwa na lata 2007-2010 *(Dz.U. z 2007 Nr 61, poz. 415);*
- Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych *(Dz.U. z 2005 r. Nr 212, poz. 1766);*
- Decyzja Ministra Obrony Narodowej nr 357/MON z dnia 29 lipca 2008 roku w sprawie organizacji systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.

Obowiązujące regulacje prawne dotyczące zasobów teleinformatycznych mają głównie charakter branżowy regulujący poszczególne aspekty związane z funkcjonowaniem zasobów. Z tego powodu powyższy wykaz aktów prawnych nie ma charakteru wyczerpującego. Przepisy prawne mające znaczenie dla funkcjonowania zasobów teleinformatycznych istnieją również w innych dziedzinach prawa, np. przepisach o ochronie danych osobowych, prawie bankowym, itd. Właściwym będzie również zaczerpniecie dobrych praktyk z regulacji prawnych w zakresie ochrony informacji niejawnych.

Należy również zaznaczyć, iż Polska jest stroną konwencji międzynarodowych, które również mają znaczenie dla bezpieczeństwa teleinformatycznego. Na potrzeby niniejszego dokumentu należy wymienić w szczególności:

- Konwencja Rady Europy o zwalczaniu terroryzmu z dnia 27 stycznia 1977r. *(Dz.U. z 1996 r. Nr 117, poz. 557)*[2]*;*
- Konwencja o zwalczaniu cyberprzestępczości RE z dnia 23 listopada 2001 r. (ETS No. 185)[3];
- Konwencja Rady Europy o zapobieganiu terroryzmowi, sporządzoną w dniu 16 maja 2005 r. (CETS No. 196)[4];
- Program Sztokholmski (doc. 5731/10)[5] wraz z Planem Działania [COM(2010) 171 final];
- Strategia Bezpieczeństwa Wewnętrznego (doc.7120/10)[6];

[2] Do Konwencji sporządzony został protokół zmieniający w dniu 15 maja 2003 r. (CETS No. 190).

[3] Konwencja weszła w życie w dniu 18 marca 2004 r., sporządzony został do niej protokół dodatkowy o kryminalizacji aktów rasizmu i ksenofobii popełnianych z wykorzystaniem systemów komputerowych (ETS No. 189).

[4] Konwencja weszła w życie w dniu 1 czerwca 2007 r.

[5] Konieczność wzmocnienia zwalczania cyberprzestępczości należy do priorytetów UE. W Programie Sztokholmskim Rada Europejska apeluje m.in.: do państw członkowskich o udzielenie pełnego poparcia krajowym platformom powiadamiania, odpowiedzialnym za walkę z cyberprzestępczością i podkreśla, że konieczna jest współpraca z krajami spoza Unii Europejskiej, a także wzywa państwa członkowskie do poprawy współpracy sądowej w sprawach dotyczących cyberprzestępczości. Program Sztokholmki odwołuje się także do wzmocnienia/usprawnienia partnerstw publiczno-prywatnych (zadanie dla KE) oraz do zintensyfikowania analizy strategicznej w zakresie cyberprzestępczości (zadanie dla Europolu). Ponadto dokument wskazuje na możliwość podjęcia działań na rzecz utworzeniu europejskiej platformy identyfikowania cyberprzestępczości, przy wykorzystaniu możliwości oferowanych przez Europol.

- Strategia i Plan działania w dziedzinie zwalczania terroryzmu (doc. 144469/05, doc. 15358/09)[7];
- Rezolucje 1267 (1999 r.) Rady Bezpieczeństwa ONZ dot. sankcji wobec Al.-Kaidy i Talibów, 1373 (2001 r.) zobowiązującej państwa członkowskie do pociągania odpowiedzialności karnej osobę lub organizacje finansującą terroryzm, a także 62/272 (2008 r.) dot. Globalnej Strategii Walki z Terroryzmem;
- Decyzja Rady Ministerialnej OBWE nr 3/04 z dnia 7 grudnia 2004 r., nr 7/06 z 5 grudnia 2006 r. w sprawie działań związanych ze zwalczeniem wykorzystywania Internetu do celów terrorystycznych;
- Decyzja Rady Ministerialnej OBWE nr 5/07 z dnia 30 listopada 2007 r. związana z partnerstwem publiczno-prytwanym z zwalczaniu terroryzmu;
- Europejska Agenda Cyfrowa Rady Europejskiej [KOM(2010)245].

Ponadto Polska ratyfikowała Konwencję Rady Europy z dnia 23 listopada 2001 r. o cyberprzestępczości.

Dodatkowo, *Program* wpisuje się w przyjęty przez Komisję Europejską dokument: Europejską Agendę Cyfrową Rady Europejskiej [KOM(2010)245], której celem jest uzyskanie trwałych korzyści ekonomicznych i społecznych z jednolitego rynku cyfrowego w oparciu o szybki Internet i interoperacyjne aplikacje.

1.8. Ramy czasowe

Przyjmuje się, że zawarte w dokumencie cele zostaną osiągnięte w latach **2011-2016**. Należy jednak podkreślić, że bezpieczeństwo jest pojmowane, jako proces ciągły a nie stan lub produkt końcowy. Zmieniające się w czasie uwarunkowania wymagają ciągłej dbałości o właściwą adaptację wdrożonych rozwiązań.

Niniejszy *Program* przedstawia działania niezbędne do ustanowienia ładu prawnego i organizacyjnego, umożliwiającego wdrożenia mechanizmów ochrony cyberprzestrzeni RP i to dla tych działań przewiduje się podane ramy czasowe. Natomiast sam proces ochrony zasobów teleinformatycznych jest traktowany, jako proces ciągły, niezmiennie istotny z punktu widzenia funkcjonowania państwa i przez to nieograniczony żadną datą zakończenia programu.

Analiza i przegląd *Programu* będzie następować nie rzadziej, niż raz do roku.

---

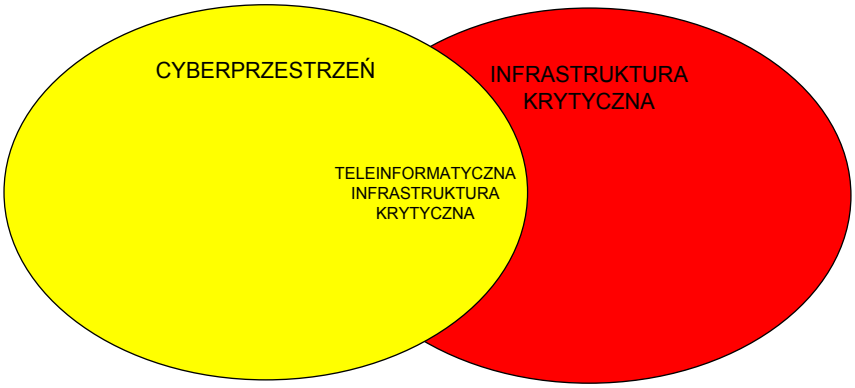
[6] Cyberprzestępczość stanowi globalne techniczne, transgraniczne i anonimowe zagrożenie naszych systemów informacyjnych, dlatego stwarza wiele dodatkowych problemów służbom ochrony porządku publicznego. Zagrożeniem „o globalnym zasięgu i katastrofalnych skutkach" jest także terroryzm. W dokumencie sformułowano 10 wytycznych, pozwalających zagwarantować w nadchodzących latach bezpieczeństwo wewnętrzne UE. Są to m.in. prewencja i uprzedzanie wypadków: profilaktyka oparta na danych wywiadowczych, opracowanie kompleksowego modelu wymiany informacji, współpraca operacyjna, współpraca organów wymiaru sprawiedliwości w sprawach karnych, zewnętrzny wymiar bezpieczeństwa wewnętrznego a współpraca z państwami trzecimi.

[7] Instrumenty legislacyjne ujęte w aktualnym Planie Działania a wynikające z Deklaracji 25 marca 2004 r. dot. zwalczania terroryzmu zostały zaimplementowane do prawa polskiego. Są to m.in.: Decyzja Ramowa Rady 2002/465/WSiSW z 13 czerwca 2002 r. dot. powołania wspólnych zespołów dochodzeniowo-śledczych; Decyzja Ramowa Rady 2002/475/WSiSW z 13 czerwca 2002 r. dot. zwalczania terroryzmu; Decyzja Ramowa 2001/500/WSiSW z 26 czerwca 2001 r. dot. prania pieniędzy oraz identyfikacji, wykrywania, zamrożenia, zajęcia i konfiskaty narzędzi oraz zysków pozyskanych z przestępstwa; Decyzja Ramowa 2003/577/WSiSW z 22 lipca 2003 r. dot. konfiskaty korzyści pochodzących z przestępstwa; Decyzja Ramowa 2005/222/JHA z 24 lutego 2005 r. przeciwko atakom na system informacyjny;

2. Charakterystyka cyberprzestrzeni

2.1. Teleinformatyczna infrastruktura krytyczna a cyberprzestrzeń

Teleinformatyczna Infrastruktura Krytyczna (zwana dalej TIK) i cyberprzestrzeń obejmują wszystkie warstwy modelu OSI jednakże TIK jest częścią cyberprzestrzeni o krytycznym znaczeniu dla jej funkcjonowania.



2.2. Identyfikacja zasobów, funkcji i zależności pomiędzy systemami a CRP

W ramach programu szczegółowego „Ocena ryzyka" opisanego w załączniku numer 1 zostanie przeprowadzona identyfikacja zasobów, podsystemów, funkcji i zależności od innych systemów istotnych z punktu widzenia funkcjonowania CRP.

2.3. Podmioty zaangażowane w działania na rzecz ochrony CRP

- Kancelaria Prezesa Rady Ministrów;
- Ministerstwo Spraw Wewnętrznych i Administracji;
- Ministerstwo Obrony Narodowej;
- Ministerstwo Edukacji Narodowej;
- Ministerstwo Infrastruktury;
- Ministerstwo Nauki i Szkolnictwa Wyższego;
- Rządowe Centrum Bezpieczeństwa;
- Agencja Bezpieczeństwa Wewnętrznego;
- Służba Kontrwywiadu Wojskowego;
- Komenda Główna Policji;
- Komenda Główna Straży Granicznej;
- Komenda Główna Państwowej Straży Pożarnej;
- Naukowa i Akademicka Sieć Komputerowa – Zespół CERT Polska;
- Przedsiębiorcy telekomunikacyjni, posiadający własną infrastrukturę telekomunikacyjną.

2.4. Obecne inicjatywy

ABUSE-FORUM – jest to ciało nieformalna grupa ekspercka, skupiające przedstawicieli zespołów typu CERT oraz zespołów bezpieczeństwa przedsiębiorców telekomunikacyjnych oraz dostarczycieli treści w polskim Internecie.

ARAKIS[8] – jest systemem wczesnego ostrzegania o zagrożeniach w sieci. Jego głównym zadaniem jest wykrywanie i opisywanie zautomatyzowanych zagrożeń występujących w sieci na podstawie agregacji i korelacji danych z różnych źródeł, w tym rozproszonej sieci honeypotów, sieci darknet, firewalli oraz systemów antywirusowych. ARAKIS jest projektem zespołu CERT Polska działającego w ramach NASK. Rozwijany jest we współpracy z Działem Rozwoju Oprogramowania oraz z działem naukowym NASK. W wyniku współpracy z ABW powstała rządowa implementacja systemu ARAKIS pod nazwą ARAKIS-GOV.

HoneySpider Network – jest wspólnym projektem działającego w ramach NASK zespołu CERT Polska, rządowego CERTu Holenderskiego GOVCERT.NL oraz akademickiego operatora w Holandii SURFnet. Projekt ma na celu zbudowanie nowych oraz wykorzystanie istniejących technik klienckich honeypotów do wykrywania ataków na aplikacje klienckie, w szczególności przeglądarki WWW. Projekt powstał w odpowiedzi na obserwacje nowego trendu w propagacji zagrożeń Internetowych, w szczególności pojawienie się zagrożeń typu ataki drive-by download, które do skutecznego zarażenia systemu operacyjnego wymagają jedynie odwiedzenia odpowiednio spreparowanej strony internetowej. Podobnie jak w przypadku systemu ARAKIS, istnieje rządowa implementacja rozwiązania pod nazwą HSN-GOV.

WOMBAT[9] – celem projektu jest utworzenie globalnego systemu monitorowania i analizy zagrożeń internetowych, w szczególności złośliwego oprogramowania. Projekt powstaje przy współpracy specjalistów ds. bezpieczeństwa z wielu podmiotów zaangażowanych w działania monitorujące oraz zwiększające bezpieczeństwo Internetu. W wyniku projektu powstają nowe metody analizy zagrożeń pojawiających się masowo w Internecie. W projekcie zostaną wykorzystane m.in. informacje zarejestrowane przez globalny rozproszony system honeypotów Leurre.com, obsługiwany przez Instytut Eurecom, oraz dane z największej na świecie kolekcji złośliwego oprogramowania, zgromadzone przez firmę Hispasec (w ramach projektu Virustotal).

FISHA[10] – Głównym celem projektu jest opracowanie prototypu systemu EISAS (European Information Sharing and Alerting System), czyli europejskiego systemu wymiany i dostępu do informacji dotyczących bezpieczeństwa komputerowego oraz ostrzegania przed zagrożeniami w Internecie. System ma działać w oparciu o istniejące już w krajach Unii Europejskiej systemy podobnego typu i stać się w przyszłości ogólnoeuropejskim forum informacyjnym. Przeznaczeniem systemu jest wzrost świadomości w kwestii bezpieczeństwa on-line wśród użytkowników domowych oraz kadry pracowniczej sektora MŚP. Docelowo, każde z państw członkowskich UE będzie miało własny, krajowy portal, na którym publikowane będą w przystępny sposób aktualne informacje dotyczące bezpieczeństwa komputerowego, pozyskiwane w ramach systemu EISAS. Projekt realizowany jest we współpracy pomiędzy NASK, CERT-em węgierskim (CERT-Hungary) oraz niemieckim instytutem badawczym Internet Security Centre z Uniwersytetu Gelsenkirchen i zakończy się na początku 2011 roku.

[8] Agregacja, Analiza i Klasyfikacja Incydentów Sieciowych
[9] Worldwide Observatory of Malicious Behavior and Attack Threats
[10] A Framework for Information Sharing and Alerting

3. Realizacja programu

3.1. Zarządzanie ryzykiem

Zarządzanie ryzykiem związanym z funkcjonowaniem cyberprzestrzeni jest kluczowym elementem procesu ochrony cyberprzestrzeni, determinującym i uzasadniającym działania podejmowane w celu jego obniżenia do akceptowalnego poziomu.

Każda instytucja, o której mowa w pkt. 2.3, każdego roku przekazuje do MSWiA podsumowujące sprawozdanie zawierające ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów zdiagnozowanych w każdym z sektorów, w których działa i za które odpowiada instytucja oraz sposobów postępowania z ryzykiem.

MSWiA opracuje wspólny wzór takich sprawozdań we współpracy z instytucjami wymienionymi w pkt. 2.3.

Każde sprawozdanie może zostać opatrzone klauzulą tajności na poziomie uznanym za odpowiedni przez instytucję wymienioną w pkt. 2.3.

Na podstawie sprawozdań, o których mowa powyżej, MSWiA i instytucje wymienione w pkt. 2.3. oceniają, czy należy na poziomie współpracy rozważyć dalsze środki ochrony. Działania te podejmowane są w połączeniu z przeglądem niniejszego programu.

MSWiA we współpracy z zaangażowanymi instytucjami opracuje wspólne wytyczne w sprawie metod przeprowadzania analiz ryzyka w odniesieniu do teleinformatycznej infrastruktury krytycznej. Używanie takich wytycznych będzie obligatoryjne dla zaangażowanych instytucji.

W ramach *Programu* zostanie opracowana i wskazana do stosowania wszystkim użytkownikom cyberprzestrzeni RP jednolita metodyka szacowania ryzyka zakłócenia jej funkcjonowania.

ABW wspólnie z SKW przedstawiają podmiotom administracji publicznej, w celu zunifikowanego podejścia, opracowane katalogi zawierające specyfikację zagrożeń oraz możliwych podatności.

Szczegóły powyższe zostały zawarte w załączniku nr 1 – Ocena ryzyka.

3.2. Ustalenie hierarchii priorytetów realizacji programu

3.2.1. Działania legislacyjne

Podstawowym elementem realizacji *Programu*, przewidzianym do wykonania w pierwszej kolejności, są działania legislacyjne. Działania te mają na celu stworzenie infrastruktury prawnej, dającej podstawy do podejmowania dalszych działań w ramach *Programu*. W przypadku istniejących przepisów przeprowadzony zostanie ich przegląd i dostosowanie do potrzeb *Programu*, zgodnie z programem szczegółowym. Budowa nowej infrastruktury prawnej zostanie przeprowadzona poprzez realizację programów szczegółowych mających na celu osiągniecie nowych kompetencji.

3.2.2. Działania proceduralno-organizacyjne

Kolejnym etapem realizacji *Programu* będą działania proceduralno-organizacyjne. Mają one na celu optymalizację wykorzystania istniejącej infrastruktury cyberprzestrzeni, w drodze wprowadzenia w życie najlepszych praktyk i standardów w tym zakresie. Na tym etapie zostaną wykorzystane zarówno narzędzia prawne stworzone w pierwszym etapie, jak i mechanizm „miękkich" regulacji. Wykonanie tego etapu nastąpi poprzez uruchomienie programów szczegółowych.

3.2.3. Działania edukacyjne

W następnym etapie realizacji *Programu* wdrożone zostaną działania edukacyjne. Działania te będą prowadzone wśród obecnych oraz przyszłych użytkowników cyberprzestrzeni i mają na celu wzmocnienie efektu dwóch poprzednich działań, utrwalenie ich wśród użytkowników, a także stworzenie możliwości przejścia do następnego etapu realizacji *Programu*. Cele tego etapu zostaną osiągnięte w drodze realizacji programów szczegółowych.

3.2.4. Działania techniczne

Ostatnim etapem realizacji *Programu* na podstawie działań proceduralno organizacyjnych tj. np. planu postępowania z ryzykiem, będą działania techniczne, których celem będzie zmniejszenie ryzyka wystąpienia zagrożeń z cyberprzestrzeni. Wykonanie tego etapu nastąpi poprzez uruchomienie programów szczegółowych.

3.3. Wprowadzenie programów ochrony

Programy ochrony będą wprowadzane w oparciu o realizację programów szczegółowych wymienionych w załącznikach do niniejszego dokumentu.

3.3.1. Program w zakresie działań legislacyjnych

W ramach programu zostaną podjęte następujące działania mające na celu uregulowanie aspektów związanych z zarządzaniem i bezpieczeństwem cyberprzestrzeni RP poprzez wprowadzenie odpowiednich zapisów do ustaw i rozporządzeń już obowiązujących lub w nowej ustawie i rozporządzeniu wykonawczym w zakresie:

1. zdefiniowania pojęć dotyczących cyberprzestrzeni – CRP, cyberprzestępczości i cyberterroryzmu,
2. wskazania, że CRP należy traktować, jako dobro ogólne umożliwiające rozwój i niezakłócone funkcjonowanie społeczeństwa informacyjnego, komunikację – wymianę informacji oraz repozytorium wiedzy,
3. ustalenia odpowiedzialności za ochronę CRP – opisanie zakresów zadań, odpowiedzialności i zmian w strukturach organizacyjnych (Prezes Rady Ministrów, MSWiA, MON w tym służby ochrony cyberprzestrzeni tj. ABW i SKW),
4. wprowadzenia ścigania z urzędu naruszeń bezpieczeństwa w cyberprzestrzeni, które miały miejsce w odniesieniu do podmiotów administracji publicznej oraz infrastruktury krytycznej ujawnionej w wykazie. Wprowadzenie ścigania na wniosek pokrzywdzonego w przypadku wykrycia incydentu bezpieczeństwa w obszarze cyberprzestrzeni RP,
5. ustanowienia głównych sektorowych punktów kontaktowych CERT.GOV.PL dla obszaru administracji publicznej, CERT POLSKA dla obszaru cywilnego, MIL CERT

dla obszaru wojskowego oraz sektorowych punktów kontaktowych w ministerstwach właściwych dla danych sektorów gospodarki RP,
6. wprowadzenia roli Pełnomocnika Rządu ds. Ochrony Cyberprzestrzeni (POC) RP oraz ustalenie sposobów i form współpracy,
7. wprowadzenia funkcji pełnomocnika kierownika jednostki organizacyjnej ds. ochrony cyberprzestrzeni (POC) w podmiotach administracji publicznej i zalecenie utworzenia takiej roli u przedsiębiorców,
8. umocowania prawnego Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL,
9. wprowadzenia obowiązku dla podmiotów publicznych i zalecenia dla pozostałych użytkowników cyberprzestrzeni informowania (nie dłużej niż w ciągu jednego dnia od wykrycia zdarzenia przez personel) do właściwego zespołu CERT o wykrytych incydentach bezpieczeństwa związanych z CRP.

Szczegóły powyższe zostały zawarte w załączniku nr 2 – Zmiany legislacyjne w zakresie ochrony CRP.

3.3.2. Programy w zakresie działań proceduralno-organizacyjnych

3.3.2.1. Zarządzanie bezpieczeństwem cyberprzestrzeni RP

W ramach zarządzania cyberprzestrzenią RP zostanie powołany międzyresortowy zespół odpowiedzialny za koordynacje wszelkich działań związanych z jej bezpieczeństwem zwany *Międzyresortowym Zespołem Koordynującym ds. Ochrony Cyberprzestrzeni RP*.

Podstawowym zadaniem ww. zespołu będzie koordynowanie działań instytucji realizujących zadania nałożone przez *Program* oraz organizacja cyklicznych spotkań i rekomendowanie proponowanych rozwiązań z zakresu bezpieczeństwa cyberprzestrzeni.

Szczegóły powyższe zostały zawarte w załączniku nr 3 – Powołanie zespołu koordynującego realizację *Programu*.

W zakresie zarządzania bezpieczeństwem cyberprzestrzeni RP w obszarze administracji publicznej, szczególną rolę pełni Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL.

Szczegóły powyższe zostały zawarte w załączniku nr 4 – Działanie Rządowego Zespołu Reagowania na incydenty komputerowe.

3.3.2.2. System zarządzania bezpieczeństwem w jednostce organizacyjnej[11]

W każdej jednostce organizacyjnej, w ramach ochrony cyberprzestrzeni, kierownik jednostki powinien ustanowić system zarządzania bezpieczeństwem informacji w cyberprzestrzeni, w oparciu o obowiązujące normy i najlepsze praktyki, z którego

[11] Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych: § 3. 1. Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych. 2. Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji.

wynikać powinny m.in. role administratorów i inspektorów bezpieczeństwa informacji przetwarzanych w jawnych systemach i sieciach teleinformatycznych.

Zgodnie z obowiązującymi przepisami podmioty publiczne realizujące zadania publiczne zobowiązane są do posiadania własnych polityk bezpieczeństwa..

Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych.

Przy opracowywaniu polityki bezpieczeństwa, podmiot publiczny powinien uwzględnić postanowienia Polskich Norm z zakresu bezpieczeństwa informacji, a w szczególności grupy norm serii PN ISO/IEC 27000 i innych norm z nią powiązanych.

Program stanowi podstawę do opracowywania polityki bezpieczeństwa cyberprzestrzeni Rzeczpospolitej Polskiej.

Zapewnieniu spójności polityk bezpieczeństwa informacji jednostek organizacyjnych służyć będą przygotowane przez MSWiA w porozumieniu z MON, ABW i SKW wytyczne, dotyczące systemów zarządzania bezpieczeństwem informacji.

Szczegóły powyższe zostały zawarte w załączniku nr 5 – „Ustanowienie w podmiotach publicznych systemu zarządzania bezpieczeństwem informacji".

3.3.2.3. Rola kierowników jednostek organizacyjnych

W ramach jednostki organizacyjnej powołany zostanie Pełnomocnik ds. ochrony cyberprzestrzeni (PKOC).

Zadania pełnomocnika w zakresie ochrony cyberprzestrzeni obejmą swoim zakresem:
- realizację obowiązków wynikających z przepisów aktów prawnych właściwych dla ochrony cyberprzestrzeni;
- ustalenie i wdrożenie procedur reagowania na incydenty komputerowe obowiązujących w organizacji;
- identyfikowanie i prowadzenie cyklicznych analiz zagrożeń;
- przygotowanie planów awaryjnych;
- niezwłoczne informowanie właściwych zespołów CERT o:
  - ✓ wystąpieniu incydentów komputerowych zgodnie z procedurami,
  - ✓ zmianie lokalizacji jednostki organizacyjnej.

Szczegóły powyższe zostały zawarte w załączniku nr 6 – Odpowiedzialność i zadania Pełnomocnika ds. ochrony cyberprzestrzeni.

3.3.3. Programy w zakresie działań edukacyjnych

3.3.3.1. Szkolenia pełnomocników ds. ochrony cyberprzestrzeni

W celu podniesienia kwalifikacji opracowany zostanie system szkoleń dla pełnomocników ds. ochrony cyberprzestrzeni. Szkolenia kończyć się będą wydaniem certyfikatu potwierdzającego odbycie przeszkolenia w zakresie bezpieczeństwa cyberprzestrzeni. Program szkoleń będzie obejmować w szczególności specjalistyczne szkolenie z zakresu reagowania na incydenty związane z bezpieczeństwem informacji. Szkolenia takie mogą być organizowane przez zespoły reagowania na incydenty (CERT), ABW i SKW lub firmy komercyjne.

Szkolenia w zakresie podstaw bezpieczeństwa eksploatacji systemów i sieci teleinformatycznych prowadzone będą przez ośrodki kształcenia, autoryzowane przez producenta (producentów) sprzętu komputerowego lub oprogramowania sieciowego.

W ramach *Programu* zostanie opracowany zakres obowiązkowych szkoleń dla pełnomocników ds. ochrony cyberprzestrzeni i administratorów w celu prawidłowego realizowania przez nich zadań z zakresu zachowania bezpieczeństwa cyberprzestrzeni RP..

Szczegóły powyższe zostały zawarte w załączniku nr 7 – Szkolenie pełnomocnika d.s. ochrony cyberprzestrzeni.

3.3.3.2. Racjonalizacja programów kształcenia na uczelniach wyższych

Jednym z podstawowych aspektów zapewnienia bezpieczeństwa cyberprzestrzeni jest posiadanie wysoko wykwalifikowanych kadr w sektorze publicznym i prywatnym odpowiadających za utrzymanie systemów i sieci teleinformatycznych ze szczególnym uwzględnieniem zasobów kluczowych dla bezpieczeństwa państwa. Aby zapewnić ciągły dopływ odpowiednio wyszkolonych specjalistów z dziedziny bezpieczeństwa teleinformatycznego konieczne jest zaangażowanie szkół wyższych w program ochrony cyberprzestrzeni . Zagadnienia związane z bezpieczeństwem cyberprzestrzeni powinny stać się stałym elementem każdego programu nauczania. W szczególności dotyczy to uczelni technicznych kształcących informatyków – bez względu na końcową specjalizację informatyczną. Nie można dopuszczać do sytuacji, w której projektanci programiści aplikacji skupiają się wyłącznie na funkcjonalności, zapominając o zasadach tworzenia bezpiecznego kodu, a administratorzy sieci i systemów za priorytet stawiają dostępność zasobów użytkowników zapominając o konieczności ochrony przetwarzanych informacji przed intruzami. W tym celu konieczne jest między innymi objęcie bezpieczeństwa teleinformatycznego długofalowym programem kierunków zamawianych, a także ustanowienie adekwatnego programu rozwoju kadry naukowej.

Zadanie propagowania zmian w obszarze programów nauczania należeć będzie do Ministra Nauki i Szkolnictwa Wyższego.

Szczegóły powyższe zostały zawarte w załączniku nr 8 – Racjonalizacja programów kształcenia na uczelniach wyższych.

3.3.3.3. Kształcenie kadry urzędniczej oraz ustanowienie dodatkowych kryteriów obsady stanowisk w administracji publicznej

Konieczna jest edukacja pracowników administracji publicznej, mającej dostęp oraz korzystającej z cyberprzestrzeni RP, w zakresie zagadnień dotyczących bezpieczeństwa sieci – odpowiednio do zajmowanego stanowiska i ryzyka z nim związanego. Szkolenia powinny dotyczyć w szczególności zastosowania procedur ochrony informacji w instytucji, znajomości technik wyłudzania informacji stosowanych w cyberprzestępczości, konsekwencji złamania zabezpieczeń przez cyberprzestępców, procedur obowiązujących w przypadku udanego ataku cyberterrorystów. Wraz z rozwojem infrastruktury teleinformatycznej państwa, procedury bezpieczeństwa powinny być modyfikowane a szkolenia ponawiane – odpowiednio do zakresu wprowadzonych zmian. Szkolenia powinny zawsze kończyć się weryfikacją nabytej

wiedzy i umiejętności w formie egzaminu lub też w ramach ćwiczeń. Odrębnym zagadnieniem jest weryfikacja wiadomości wiedzy i umiejętności w zakresie bezpieczeństwa oraz ryzyka związanego z korzystaniem z sieci, dla osób ubiegających się o stanowiska w administracji publicznej. Konieczne jest, aby takie osoby posiadały wiedzę w tym zakresie – przynajmniej na poziomie minimalnych standardów określanych dla danego stanowiska służbowego przez kierownika jednostki organizacyjnej.
W trakcie procedury rekrutacyjnej sprawdzenia kompetencji mogą dokonać osoby administrujące zasobami teleinformatycznymi.

Szczegóły powyższe zostały zawarte w załączniku nr 9 – Wytyczne w zakresie obszarów obowiązkowych szkoleń dla pracowników administracji publicznej.

3.3.3.4. Kampania społeczna o charakterze edukacyjno-prewencyjnym

Powszechność korzystania przez obywateli z Internetu oraz zwiększające się znaczenie dostępności usług oferowanych przez sieć implikują konieczność uwrażliwienia obywateli na problem bezpieczeństwa teleinformatycznego, podnoszenia ich świadomości odnośnie bezpiecznych metod korzystania z Internetu. Każdy użytkownik komputera powinien pamiętać o tym, że korzystanie z globalnej sieci, oprócz niekwestionowanych korzyści niesie za sobą także szereg zagrożeń. Każdy użytkownik komputera wcześniej czy później zetknie się z nimi, nawet, jeśli będą one dla niego niezauważalne. Dlatego tak ważne jest szerzenie wśród całego społeczeństwa świadomości istnienia niebezpieczeństw w globalnej sieci oraz konieczności przeciwdziałania cyberzagrożeniom. Świadomość i wiedza na temat sposobów przeciwdziałania i zwalczania zagrożeń stanowią kluczowe elementy walki z tymi zagrożeniami. Jedynie odpowiedzialne zachowanie odpowiednio wyedukowanego użytkownika może skutecznie minimalizować ryzyko wynikające z istniejących zagrożeń. Należy podkreślić, iż we współczesnym świecie zapewnienie bezpieczeństwa teleinformatycznego nie zależy jedynie od działalności wyspecjalizowanych instytucji rządowych, specjalistów do spraw bezpieczeństwa teleinformatycznego, zespołów reagowania na incydenty, ani nawet administratorów sieci. Wraz z upowszechnieniem się dostępu do Internetu w domach, szkołach i miejscach pracy oraz zmianą sposobu przeprowadzania ataków komputerowych, gdzie do skutecznej infekcji wykorzystywana jest nie tylko podatność oprogramowania, lecz coraz częściej niewiedza lub niefrasobliwość użytkowników, odpowiedzialność za bezpieczeństwo spoczywa na każdym użytkowniku komputera.

Kampania społeczna o charakterze edukacyjno-prewencyjnym stanowi wyzwanie i jest istotnym elementem *Programu*. Ze względu na fakt, że przestępczością komputerową zagrożeni są zarówno użytkownicy indywidualni, jak również instytucje publiczne, przedsiębiorcy, organizacje społeczne, kampania będzie miała charakter wielowymiarowy i uwzględniać będzie konieczne zróżnicowanie form i treści przekazu w zależności od potrzeb jej adresatów. Zawierać się ona będzie w powszechnym oraz instytucjonalnie różnorodnym oddziaływaniu na postawy wszystkich użytkowników komputerów podłączonych do Internetu. Zakłada się długofalowy i powszechny charakter kampanii społecznej.

Ze względu na bezpieczeństwo teleinformatyczne warunkujące realizację zadań publicznych, adresatami akcji informacyjnych będą w szczególności pracownicy

administracji publicznej oraz podmioty, których zasoby należą do infrastruktury krytycznej.

Kampania edukacyjno-prewencyjna skierowana zostanie także do:

- **dzieci i młodzieży** – jako grupy najbardziej podatnej na wpływy. Edukacja powinna rozpocząć się już od najmłodszych lat, w celu wytworzenia pewnych nawyków, które uchronią najmłodszych przed zagrożeniami czyhającymi na nich w sieci (np. przed zjawiskiem zwanym *cyberbullying* – przemocy w sieci, zawieraniem niebezpiecznych znajomości, niecenzuralnymi treściami, piractwem, uzależnieniem od Internetu). Wiedzę na temat zagrożeń z cyberprzestrzeni, dziecko powinno uzyskiwać przede wszystkim w szkole podczas nauki na wszystkich poziomach edukacji (szkoła podstawowa, gimnazjum, szkoła średnia). Ogromna w tym rola Ministerstwa Edukacji Narodowej (MEN), by nie tylko poprzez zajęcia lekcyjne inicjować i propagować działania na rzecz bezpieczeństwa dzieci i młodzieży w Internecie.
- **rodziców** – jako najważniejszych nauczycieli i osoby odpowiedzialne za wychowanie kolejnych pokoleń. To na rodzicach spoczywa odpowiedzialność za przygotowanie dzieci do funkcjonowania w społeczeństwie, również w społeczeństwie informacyjnym. Statystyki wskazują, iż komputer przestaje być w Polsce traktowany jako dobro luksusowe, a staje się sprzętem codziennego użytku większości polskich rodzin. Stopniowo rośnie również liczba domowych szerokopasmowych przyłączy do Internetu. Aby zapewnić skuteczny nadzór nad działalnością dziecka w Internecie rodzice przede wszystkim sami powinni posiąść odpowiednią wiedzę na temat zagrożeń oraz metod ich eliminowania.
- **nauczycieli** – od roku 2004 kształcenie nauczycieli w ramach specjalizacji odbywa się zgodnie z rozporządzeniem Ministra Edukacji Narodowej, określającym standardy kształcenia nauczycieli[12]. W ramach zajęć obowiązkowych na studiach wyższych nauczyciele uzyskują podstawową wiedzę z zakresu technologii informacyjnej, w tym również bezpiecznego i świadomego korzystania z systemów teleinformatycznych.

Kampania społeczna adresowana do dzieci, młodzieży i ich rodziców w dużej mierze powinna być realizowana w placówkach oświatowych wszystkich szczebli.

Kampania społeczna edukacyjno – prewencyjna realizowana będzie także za pośrednictwem środków masowego przekazu. Media – jako istotny partner w promowaniu zagadnień ochrony cyberprzestrzeni RP oraz popularyzacji przedsięwzięć zawartych w *Programie* zwiększą skuteczność realizacji założonych celów. Dzięki ich pomocy w trakcie realizacji *Programu* możliwe będzie również przeprowadzenie rozmaitych akcji informacyjnych i kampanii edukacyjnych. W tym celu zaangażowane zostaną media ogólnopolskie, regionalne i lokalne.

W ramach kampanii społecznej informacje dotyczące bezpieczeństwa teleinformatycznego oraz przedsięwzięć edukacyjnych i organizacyjno-prawnych podejmowanych w ramach *Programu* prezentowanego będą na stronach internetowych MSWiA, oraz na stronie zespołu CERT.GOV.PL, gdzie będą dostępne także interaktywne kursy dotyczące zagadnienia bezpieczeństwa.

[12] rozporządzenie Ministra Edukacji Narodowej z dnia 7 września 2004 r. w sprawie standardów kształcenia nauczycieli (Dz. U. Nr 207, poz. 2110)

Szczegóły w powyższym zakresie zostały zawarte w programie szczegółowym: Załącznik numer 10 – Prowadzenie społecznej kampanii edukacyjno-prewencyjnej w mediach publicznych, oraz

załącznik numer 11 – Prowadzenie kampanii informacyjno-profilaktycznej na stronach internetowych.

3.3.4. Programy w zakresie działań technicznych

3.3.4.1. Programy badawcze

Ważne z punktu widzenia powodzenia wykonania *Programu* jest przygotowanie i uruchomienie krajowych programów badawczych dotyczących bezpieczeństwa teleinformatycznego o formule, która zachęciłaby do wspólnego prowadzenia badań naukowych nad bezpieczeństwem teleinformatycznym, podmioty zajmujące się bezpieczeństwem teleinformatycznym ze sfery administracji publicznej, ośrodki naukowe oraz innych przedsiębiorców telekomunikacyjnych.

Podmiotem koordynującym *Program* w tym zakresie jest Ministerstwo Nauki i Szkolnictwa Wyższego (MNiSW), jako ustawowo właściwe w sprawach badań naukowych i prac rozwojowych. Wykaz zadań w obszarze koniecznych programów badawczych, uwzględniających dynamikę stanu wiedzy określony zostanie na poziomie projektów szczegółowych *Programu* i może być uzupełniany z inicjatywy właściwych podmiotów odpowiedzialnych za realizację *Programu*.

Szczegóły w tym zakresie zostaną, w uzgodnieniu z zainteresowanymi podmiotami oraz uwzględniające istotne ustalenia programów szczegółowych, określone w programie ministra dotyczącym badań naukowych związanych z rozwojem zagrożeń dla cyberprzestrzeni i metod ich przeciwdziałania.

Szczegóły powyższe zostały zawarte w załączniku nr 12 – Programy badawcze.

3.3.4.2. Rozbudowa zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego w administracji publicznej

Aby możliwe było skuteczne prowadzenie działań związanych z ochroną cyberprzestrzeni, w tym reagowania na incydenty bezpieczeństwa teleinformatycznego, konieczne jest zapewnienie odpowiedniego zaplecza technicznego, nie tylko umożliwiającego realizację bieżących zadań, ale również uwzględniającego wzrastające zapotrzebowanie na specjalizowane systemy teleinformatyczne w przyszłości.

Wszystkie zespoły po unifikacji zakresów obowiązków oraz procedur reagowania, jak również określenia obszaru (*ang. constituency*) tworzyłyby krajowy system reagowania na incydenty komputerowe, który oprócz współdziałania obejmowałby również wspólne konferencje, szkolenia i ćwiczenia.

Szczegóły powyższe zostały zawarte w załączniku nr 13 – Ochrona rządowych kluczowych rozwiązań teleinformatycznych.

3.3.4.3. Rozbudowa systemu wczesnego ostrzegania oraz wdrażanie i utrzymanie rozwiązań prewencyjnych

W ramach *Programu* kontynuowane będą inicjatywy realizowane na podstawie wniosków zawartych w „*Sprawozdaniu z prac Zespołu ds. Krytycznej Infrastruktury Teleinformatycznej"*, zatwierdzonym w maju 2005 r. przez Kolegium ds. Służb Specjalnych. Departament Bezpieczeństwa Teleinformatycznego ABW wraz z zespołem CERT Polska działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK) dokonał wdrożenia systemu wczesnego ostrzegania przed zagrożeniami z sieci Internet – ARAKIS-GOV. Rozbudowa systemu będzie realizowana zgodnie z programem szczegółowym.

Szczegóły powyższe zostały zawarte w załączniku nr 14 – Rozbudowa systemu wczesnego ostrzegania.

Jednocześnie mając na uwadze postęp zachodzący w technologiach teleinformatycznych i związaną z nim tendencję pojawiania się coraz bardziej wyrafinowanych zagrożeń, podczas wdrażania *Programu* podjęte zostaną inicjatywy promujące tworzenie coraz nowocześniejszych rozwiązań wspierających bezpieczeństwo teleinformatyczne.

Należy dążyć do stosowania jak najszerszego spektrum różnych rodzajów systemów zabezpieczeń w celu zapewnienia bezpieczeństwa krytycznych zasobów teleinformatycznych.

3.3.4.4. Testowanie poziomu zabezpieczeń

W ramach testowania poziomu zabezpieczeń, dla adresatów *Programu* będą organizowane cyklicznie ćwiczenia polegające na przeprowadzaniu kontrolowanych ataków symulujących działania cyberterrorystyczne. Testy mają służyć ocenie bieżącej odporności cyberprzestrzeni na cyberataki, wskazaniu najsłabszych punktów zabezpieczeń, ogniw i przygotowaniu zaleceń do dalszych działań prewencyjnych.

Szczegóły powyższe zostały zawarte w załączniku nr 15A oraz 15B – Testowanie poziomu zabezpieczeń w cyberprzestrzeni (obszar administracji publicznej).

3.3.4.5. Rozwój Zespołów CERT

Zespoły te są centrami kompetencyjnymi służącymi pomocą merytoryczną zarówno na etapie tworzenia właściwych struktur i procedur jak również rozwiązywania problemów w trakcie ich eksploatacji w poszczególnych jednostkach organizacyjnych administracji czy też przedsiębiorców.

Konsultacje i doradztwo w zakresie bezpieczeństwa cyberprzestrzeni prowadzą zespoły CERT wobec wszystkich podmiotów administracji publicznej, przedsiębiorców oraz innych użytkowników cyberprzestrzeni posiadających zasoby objęte niniejszym *Programem*.

Ponadto, do zadań zespołów reagowania na incydenty komputerowe należy utrzymywanie informacyjnej witryny internetowej. Docelowo witryny zespołów utworzą główne źródła informacji związanych z bezpieczeństwem teleinformatycznym dla osób zajmujących się bezpieczeństwem teleinformatycznych w instytucjach administracji publicznej, a także innych osób zainteresowanych tą tematyką.

W szczególności witryny będą miejscem publikacji następujących informacji:

- aktualności związanych z bezpieczeństwem teleinformatycznym;
- informacji o podatnościach i zagrożeniach;
- biuletynów bezpieczeństwa;
- różnego rodzaju poradników, dobrych praktyk, itp.;
- raportów, informacji na temat trendów i statystyk;
- forum wymiany informacji oraz doświadczeń osób zaangażowanych w działania związane z bezpieczeństwem teleinformatycznym.

Witryny pełnić będą rolę jednego z dostępnych punktów zgłaszania incydentów bezpieczeństwa teleinformatycznego, który pozwala użytkownikowi na zgłoszenie incydentu bez posiadania większej wiedzy z zakresu informatyki oraz poszukiwania miejsca, gdzie zdarzenie można zgłosić.

Szczegóły powyższe zostały zawarte w załączniku nr 16 – Tworzenie i rozwój zespołów typu CERT.

3.3.4.6. Plany Ciągłości Działania

W celu zapewnienia nieprzerwanej realizacji procesów w cyberprzestrzeni RP wymagane jest opracowanie i skoordynowane *Planów ciągłości działania* tych procesów na wypadek zaistnienia sytuacji kryzysowej w obszarze cyberprzestrzeni skutkującej zaprzestaniem realizacji procesu.

W opracowywanie oraz testowanie Planów ciągłości działania zaangażowane powinny być wszystkie podmioty, zarówno zarządzające jak i wykorzystujące krytyczną infrastrukturę teleinformatyczną, które realizują ważne z punktu widzenia funkcjonowania CRP usługi.

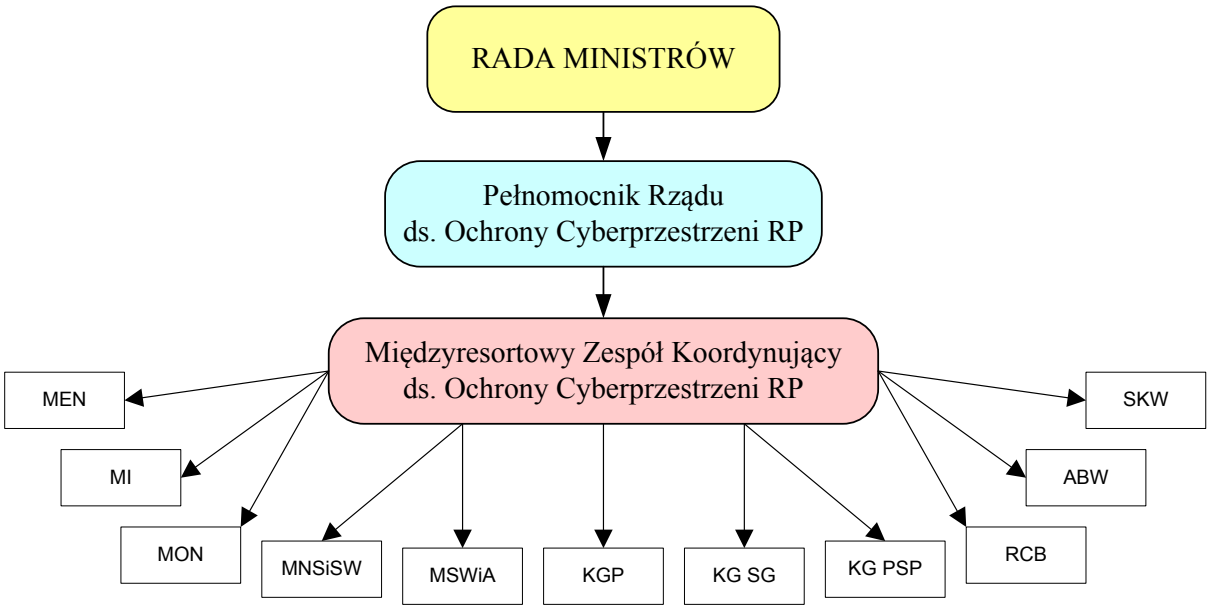
Szczegóły powyższe zostały zawarte w załączniku nr 17 – Wytyczne w zakresie tworzonego standardu planu ciągłości działania.

4. Koordynacja realizacji *Programu*

4.1. Rola instytucji koordynującej wdrażanie *Programu*

W ramach systemu ochrony cyberprzestrzeni zostanie powołany ***Międzyresortowy Zespół Koordynujący ds. Ochrony Cyberprzestrzeni RP (MZKOC)*** skupiający jednostki administracji rządowej, wyszczególnione w pkt. 2.3.

Podstawowym zadaniem MZKOC będzie koordynowanie działania instytucji realizujących zadania nałożone przez *Program* oraz organizacja cyklicznych spotkań i rekomendowanie proponowanych rozwiązań z zakresu bezpieczeństwa cyberprzestrzeni.



Rysunek 1: Schemat koordynacji realizacji Programu.

Informacje o realizacji *Programu* z obszaru użytkownika i przedsiębiorców oraz innych instytucji będą wynikały z analiz prowadzonych przez operatów, dostawców usług. Zasadniczym miernikiem stopnia wdrożenia *Programu* będą statystki incydentów obsługiwanych przez zespoły ds. naruszeń w sieci.

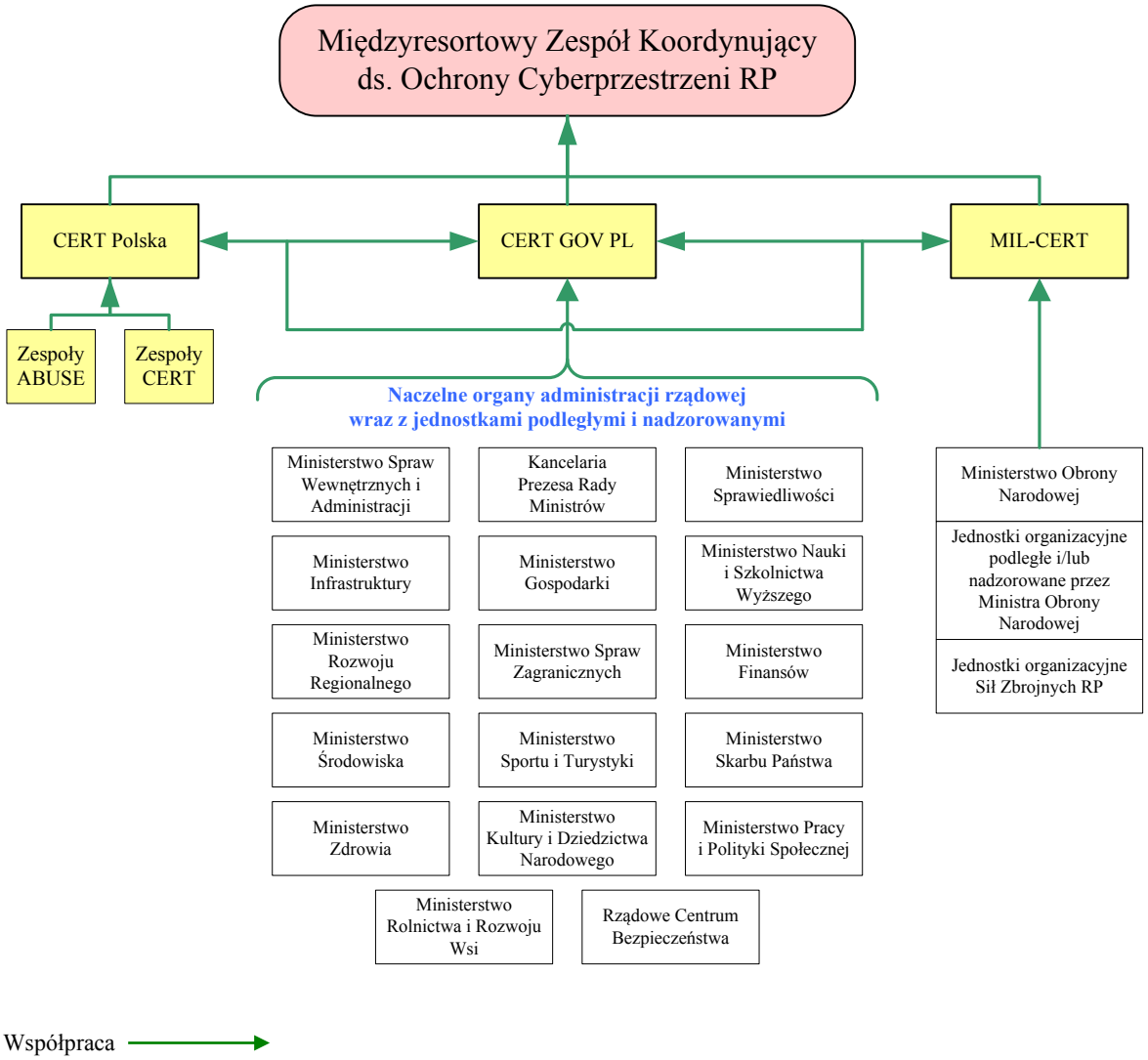
Docelowym wariantem rekomendowanym przez *Program* jest powołanie jednostki technicznej realizującej zadania zarządzania i koordynowania przedsięwzięć w zakresie ochrony CRP, podległej Prezesowi Rady Ministrów, która przejęłaby zadania MZKOC.

4.2. Szczebel sektorowy

W ramach współdziałania jednostek organizacyjnych w zakresie ochrony cyberprzestrzeni zostaną stworzone sektorowe (resortowe) punkty kontaktowe. Sektorowe punkty kontaktowe staną się elementem systemu komunikacji instytucji związanych z ochroną cyberprzestrzeni.

Sektorowy Punkt Kontaktowy – będzie odpowiedzialny za organizację współpracy, wymianę informacji o podatnościach, zagrożeniach, trendach w formie raportów,

biuletynów itp. Umożliwiał będzie abonentom, dostawcom usług, zespołom CERT itp. spełnienie wszystkich procedur operacyjnych niezbędnych do obsługi incydentu oraz prowadzenia działań zgodnie z uprawnieniami ustawowymi tak, aby nie musieli oni zwracać się do kilku właściwych resortów, departamentów lub organów (w ramach jednej organizacji) w celu zebrania wszelkich potrzebnych informacji. Obejmuje to pełny cykl obsługi incydentu oraz inne ustalone w toku wzajemnych porozumień procedury. Wyłączeniu podlegać będą raporty o zagrożeniach oraz procedury dochodzeniowo-śledcze i odwoławcze o charakterze sądowym lub administracyjnym, jak również formalne dokumenty kierowane do kierownictwa resortu/firmy.



Rysunek 2: Schemat współpracy MZKOC i punktów sektorowych

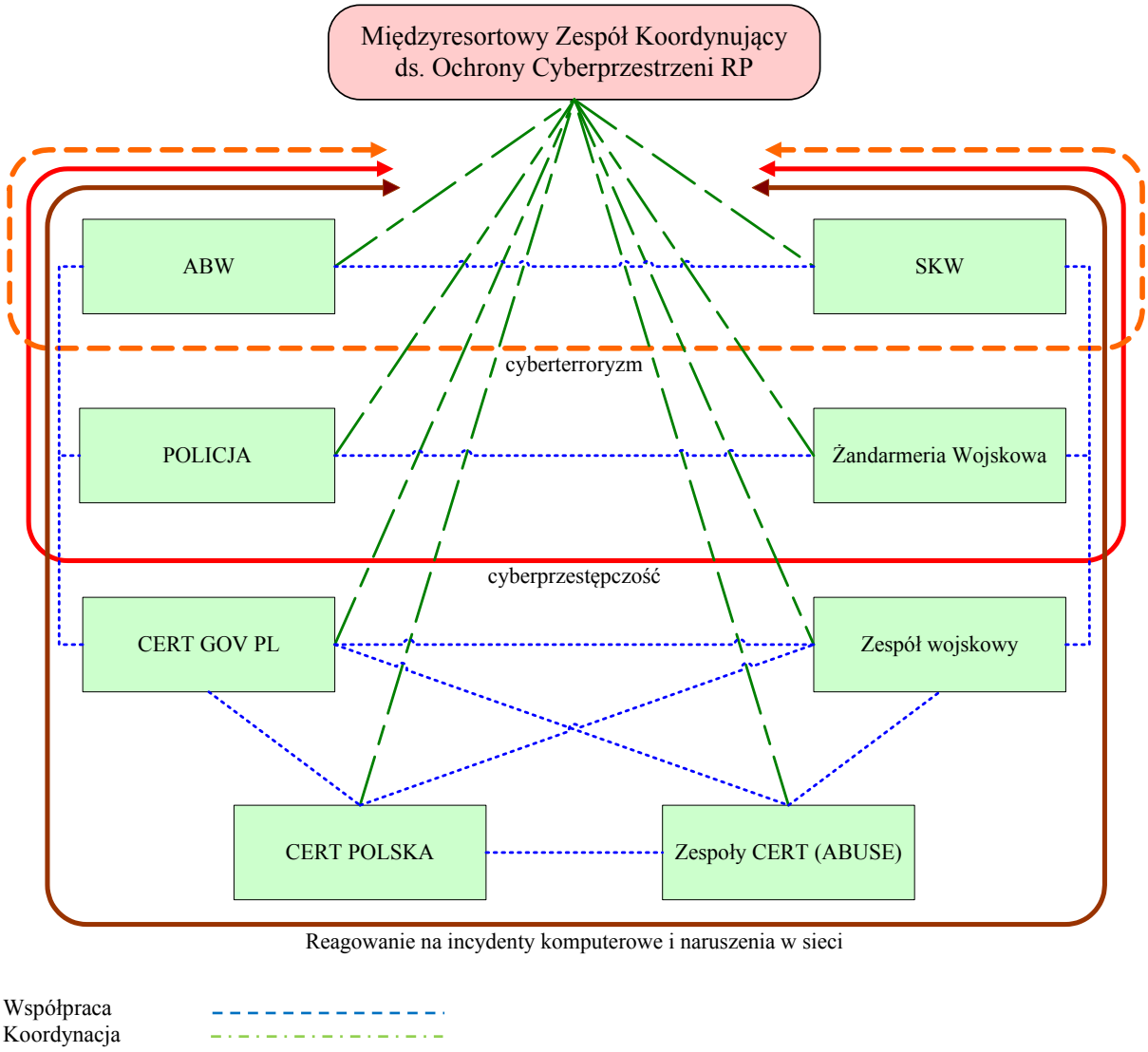
Szczegóły powyższe zostały zawarte w załączniku nr 18 – Sektorowe punkty kontaktowe.

5. Współpraca w realizacji *Programu*

5.1. Sposoby i formy współpracy

W ramach realizacji *Programu* zostaną wypracowane formy współpracy pomiędzy organami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz odpowiedzialnymi za zwalczanie przestępczości komputerowej o charakterze kryminalnym. Powyższe formy współpracy będą miały zarówno postać roboczą, w celu zminimalizowania opóźnień reakcji na incydenty komputerowe, jak i sformalizowaną służącą eliminowaniu problemów kompetencyjnych.

Szczegóły powyższe zostały zawarte w załączniku nr 19 – Sposoby i formy współpracy**.**



Rysunek 3: Współpraca pomiędzy organami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni

5.2. Współpraca krajowa

Istotną formą współpracy w zakresie ochrony cyberprzestrzeni będą bezpośrednie robocze kontakty krajowych zespołów reagowania na incydenty komputerowe, między innymi takich jak:

- Rządowy Zespół Reagowania na Incydenty Komputerowe – CERT.GOV.PL,
- System Reagowania na Incydenty Komputerowe resortu obrony narodowej,
- CERT Polska,
- CERT-y powołane przez przedsiębiorców telekomunikacyjnych,
- Inne zespoły ds. naruszeń w sieci a w szczególności członkowie ABUSE Forum.

Szczegóły powyższe zostały zawarte w załączniku nr 20 – Współpraca krajowa.

5.3. Współpraca z producentami urządzeń i systemów teleinformatycznych

Ważnymi partnerami dla instytucji rządowych i innych podmiotów odpowiedzialnych za bezpieczeństwo teleinformatyczne w działaniach zmierzających do zwiększenia bezpieczeństwa w cyberprzestrzeni są producenci sprzętu i oprogramowania. Rozwój współpracy z tymi partnerami, w tym wymiana doświadczeń i oczekiwań, stanowić będzie jeden z ważniejszych czynników mających duży wpływ zarówno na system edukacji społecznej i specjalistycznej, jak i na jakość tworzonych systemów. Szczególne znaczenie dla rozszerzenia spektrum dostępnych narzędzi ma współpraca podmiotów odpowiedzialnych za bezpieczeństwo teleinformatyczne z producentami systemów zabezpieczeń. Należy dążyć do udostępniania pojedynczym jak i instytucjonalnym użytkownikom jak największego wachlarza rozwiązań służących szeroko rozumianemu bezpieczeństwu teleinformatycznemu oraz ochronie informacji.

Szczegóły powyższe zostały zawarte w załączniku nr 21 – Współpraca z producentami sprzętu i oprogramowania**.**

5.4. Współpraca z przedsiębiorcami telekomunikacyjnymi

Ze względu na globalny charakter zagrożeń w cyberprzestrzeni wymagana jest ścisła skoordynowana współpraca pomiędzy Urzędem Komunikacji Elektronicznej (UKE), przedsiębiorcami telekomunikacyjnymi i użytkownikami cyberprzestrzeni.

Szczegóły powyższe zostały zawarte w załączniku nr 22 – Współpraca z przedsiębiorcami telekomunikacyjnymi.

5.5. Współpraca międzynarodowa

Ze względu na globalny charakter problemów związanych z ochroną cyberprzestrzeni, istotnym elementem jest utrzymanie i rozwijanie współpracy międzynarodowej w tym zakresie.

Rada Europejska w przyjętej w 2003 roku Europejskiej Strategii Bezpieczeństwa uznała zjawisko terroryzmu za podstawowe zagrożenie dla interesów UE. Ostatnim efektem prac w zakresie przeciwdziałania aktom terroru jest specjalny program „Zapobieganie, gotowość i zarządzanie skutkami aktów terroryzmu" przyjęty w ramach programu ogólnego

„Bezpieczeństwo i ochrona wolności" na lata 2007-2013. Polska jest również stroną międzynarodowych i europejskich porozumień w sprawie zwalczania terroryzmu (jest sygnatariuszem Europejskiej Konwencji o zwalczaniu terroryzmu) oraz ratyfikowała Konwencję Rady Europy o zapobieganiu terroryzmowi, sporządzoną w Warszawie, w dniu 16 maja 2005 r.

Rząd Rzeczypospolitej Polskiej deklaruje, poprzez swoich przedstawicieli, organy rządowe, instytucje państwowe oraz współpracę z instytucjami pozarządowymi, aktywne działania zmierzające do zwiększenia bezpieczeństwa CRP oraz międzynarodowej.

5.5.1. Unia Europejska

W zakresie współpracy z organizacją ENISA[13] Polskę reprezentują przedstawiciele:

- członek Rady Zarządzającej (Management Board),
- zastępca członka Rady Zarządzającej,
- krajowy oficer łącznikowy (Liaison Officer).

Szczegóły powyższe zostały zawarte w załączniku nr 23 – Współpraca z europejskimi strukturami zajmującymi się bezpieczeństwem cyberprzestrzeni – w szczególności z agencją ENISA.

5.5.2. NATO

Szef ABW stanowi Krajowy Punkt Centralny *(Focal Point)* w ramach polityki ochrony cyberprzestrzeni.
Podmiotami odpowiedzialnymi w sferze rządowej za koordynację reagowania na incydenty w sieciach i systemach komputerowych są:

- rządowy zespół reagowania na incydenty komputerowe w odniesieniu do cyberprzestrzeni RP,
- wojskowy zespół reagowania na incydenty komputerowe Ministerstwa Obrony Narodowej w odniesieniu do sieci i systemów komputerowych leżących w gestii Ministerstwa Obrony Narodowej.

Minister Obrony Narodowej i Szef ABW przy współpracy z ministrem właściwym do spraw wewnętrznych występują, jako bezpośredni partnerzy *NATO Cyber Defence Management Authority* (*CDMA).*

Szczegóły powyższe zostały zawarte w załączniku nr 24 – Utrzymanie NATO Focal Point.

5.6. Sfera cywilna

Rządowy Zespół Reagowania na Incydenty Komputerowe - CERT.GOV.PL między innymi współpracował będzie na forum międzynarodowym i krajowym w zakresie ochrony cyberprzestrzeni z organizacjami zrzeszającymi zespoły CERT z różnych krajów, takimi jak np. FIRST[14].

Szczegóły powyższe zostały zawarte w załączniku nr 25 – Współpraca CERT.GOV.PL z FIRST.

[13] Europejska Agencja Bezpieczeństwa Sieci i Informacji – European Network and Information Security Agency
[14] Forum of Incident Response and Security Teams

5.7. Mechanizm wymiany informacji

Sprawny system koordynacji zapewni wymianę informacji pozyskanych ze współpracy międzynarodowej, bez ponoszenia dodatkowych kosztów, pomiędzy zespołami rządowymi, wojskowymi i cywilnymi, zgodnie z obowiązującymi przepisami prawa, a w szczególności zgodnie z ustawą o ochronie danych osobowych oraz ustawą o ochronie informacji niejawnych.

6. Finansowanie *Programu*

Koszty realizacji zadań, które zostały określone w programach szczegółowych, stanowiących załączniki do niniejszego *Programu*, przypisane poszczególnym jednostkom, ponoszone będą w ramach ich budżetów oraz projektów UE.

W trakcie obowiązywania *Programu*, w latach 2012-2016, realizacja jego celów nie powinna pociągać za sobą dodatkowych skutków finansowych.

Obecnie jednostki organizacyjne administracji publicznej realizują częściowo cele wymienione w *Programie* oraz programach szczegółowych. *Program* od momentu jego wejścia w życie zakłada kontynuację i koordynację już realizowanych bądź zaplanowanych działań związanych z ochroną cyberprzestrzeni w sposób ujednolicony i usystematyzowany dla całej administracji publicznej.

W roku 2011, realizacja celów *Programu* nie będzie pociągała za sobą skutków finansowych, jednakże od chwili wejścia *Programu* w życie, poszczególne jednostki będą szacowały koszty realizacji zadań nałożonych na nie niniejszym *Programem* w celu ujęcia ich w planie następnego roku budżetowego. Poszczególne jednostki organizacyjne, oszacowane przez siebie koszty realizacji zadań, przekażą do *Międzyresortowego Zespołu Koordynującego ds. Ochrony Cyberprzestrzeni RP* celem przygotowania zbiorczego oszacowania kosztów realizacji RPOC.

7. Ocena skuteczności *Programu*

Mierniki skuteczności mierzą stopień osiągnięcia zamierzonych celów i mogą mieć one zastosowanie na wszystkich szczeblach klasyfikacji zadaniowej.

Przykład:

Liczba zamkniętych incydentów w stosunku do ogólnej liczby sklasyfikowanych incydentów.

Mierniki produktu odzwierciedlają wykonanie danego zadania w krótkim okresie i pokazują konkretne dobra oraz usługi wyprodukowane przez sektor publiczny. Mierniki produktu – mierzą stopień wykonania celów operacyjnych.

Przykładowe mierniki produktu:

- liczba odpowiedzi na zgłoszone przez obywateli incydenty,
- liczba obsłużonych incydentów,
- liczba spotkań Zespołu.

Mierniki rezultatu mierzą efekty uzyskane w wyniku działań objętych zadaniem lub podzadaniem, realizowanych za pomocą odpowiednich wydatków, na poziomie zadania/podzadania/działania. Mierzą zatem skutki podejmowanych działań. Mierniki rezultatu – mierzą bezpośrednie skutki podejmowanych działań w krótkiej lub średniej perspektywie czasowej.

Przykładowe mierniki rezultatu:

- skrócenie czasu obsługi incydentu,
- średni czas odpowiedzi na incydent.

Mierniki oddziaływania mierzą długofalowe konsekwencje realizacji zadania. Mogą one mierzyć bezpośrednie skutki wdrażania zadania, ale które ujawniają się po dłuższym okresie czasu. Mierniki oddziaływania odnoszą się czasem do wartości, które tylko w części są efektem realizacji zadania (na efekty wpływają także inne, zewnętrzne czynniki).

Przykładowe mierniki oddziaływania:

- zwiększenie poczucia bezpieczeństwa w sieci Internet w Polsce (badania CBOS).

Szczegóły powyższe zostały zawarte w załączniku nr 26 – Ocena skuteczności *Programu* w zakresie działań organizacyjno-prawnych, technicznych i edukacyjnych.

7.1. Przewidywane efekty *Programu*

Przewiduje się następujące długofalowe efekty skutecznego wdrożenia niniejszego *Programu*:

- większy poziom bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa oraz większy poziom odporności państwa na ataki cyberterrorystyczne,

- spójną dla wszystkich zaangażowanych podmiotów administracji publicznej i innych współstanowiących krytyczną infrastrukturę teleinformatyczną państwa politykę dotycząca bezpieczeństwa cyberprzestrzeni,
- mniejszą skuteczność ataków cyberterrorystycznych i mniejsze koszty usuwania następstw ataków cyberterrorystycznych,
- funkcjonujący skuteczny system koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami odpowiedzialnymi za zapewnianie bezpieczeństwa cyberprzestrzeni oraz władającymi zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa,
- większą kompetencję odnośnie bezpieczeństwa cyberprzestrzeni podmiotów zaangażowanych w ochronę krytycznej infrastruktury teleinformatycznej państwa,
- większe zaufanie obywateli do właściwego zabezpieczenia usług państwa świadczonych drogą elektroniczną, upowszechnienie elektronicznej drogi korzystania z tych usług,
- większą świadomość obywateli, co do metod bezpiecznego użytkowania systemów dostępnych elektronicznie i sieci teleinformatycznych.

7.2. Metody oceny skuteczności podjętych działań

Stopień realizacji przedsięwzięć związanych z realizacją celu strategicznego oraz celów szczegółowych *Programu* oceniany będzie przez następujące kryteria:

- W1 – stopień nasycenia wszystkich jednostek organizacyjnych, objętych ochroną w systemy ochrony i wczesnego ostrzegania w stosunku do liczby urzędów administracji publicznej;
- W2 – poziom integracji:
  - sposób i tryb wymiany informacji między zespołami z zapewnieniem poufności, integralności i dostępności,
  - możliwość i zakres osiągania wspólnego, dynamicznego zobrazowania cyberprzestrzeni objętej ochroną;
- W3 – stopień standaryzacji – stopień wdrożenia norm, kategorii incydentów i procedur;
- W4 – stopień wyposażenia systemów i sieci w kompleksowe oprogramowanie antywirusowe, firewalle, antyspamowe w stosunku do wymaganych objęciem taką ochroną (szacowanie zasobów).

Stopień realizacji, o którym mowa powyżej zostanie oceniamy w procentach, przy czym za 100% rozumie się realizację wszystkich zadań wskazanych w RPOC.

W ciągu 6 miesięcy od wejścia *Programu* w życie, każda zaangażowana jednostka, o której mowa w pkt. 1.4 ust. 1 *Programu*, oszacuje (w %) w jakim stopniu są już zrealizowane założenia przedmiotowego *Programu*.

7.3. Skuteczność działań

Miarą skuteczności podjętych w ramach *Programu* działań, będzie ocena stworzonych regulacji, instytucji i relacji, które umożliwią rzeczywiste zaistnienie skutecznego systemu ochrony cyberprzestrzeni.

Jedną z podstawowych metod wpływania na skuteczność założonych działań wykonywanych przez wiele instytucji jest precyzyjne ustalenie zakresu zadań każdego

z podmiotów oraz, co powinno być z tym tożsame, precyzyjne ustalenie odpowiedzialności za realizację – poszczególnych zadań.

7.4. Raportowanie o postępach

Raporty przesyłane będą przez jednostki wyszczególnione w pkt. 1.4 oraz jednostki przewodnie danego podprogramu do Ministra Spraw Wewnętrznych i Administracji (zgodnie z zapisami pkt. 1.6).

Przez jednostkę przewodnią, rozumie się jednostkę wyszczególnioną w pkt. 10 w każdym z załączników do *Programu* – „*Podmiot odpowiedzialny za monitoring*".

7.5. Sprawozdawczość

Każda zaangażowana instytucja, (o której mowa w pkt. 2.3) przeprowadza ocenę zagrożenia w odniesieniu do wyznaczonych podsektorów w ciągu roku od daty zgłoszenia (wyznaczenia) danego podsektora do Teleinformatycznej Infrastruktury Krytycznej.

Każda zaangażowana instytucja, raz w roku, do końca pierwszego kwartału przekazuje MSWiA podsumowujące sprawozdanie za poprzedni rok, zawierające ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów oraz ogniw stwierdzonych w każdym z sektorów.

MSWiA opracuje wzór sprawozdań we współpracy z zaangażowanymi instytucjami oraz określi tryb, zasady i terminy ich składania.

Każde sprawozdanie może zostać opatrzone klauzulą tajności na poziomie uznanym za odpowiedni przez zaangażowaną instytucję.

Na podstawie sprawozdań, o których mowa powyżej, MSWiA i zaangażowane instytucje oceniają, czy należy na poziomie współpracy rozważyć dalsze środki ochrony. Działania te podejmowane są w połączeniu z przeglądem niniejszego *Programu*.