Ministerstwo Cyfryzacji

Zatwierdzam:

……

Minister Cyfryzacji
Koordynator Krajowych Ram Polityki Cyberbezpieczeństwa
Rzeczypospolitej Polskiej na lata 2017 - 2022

PLAN DZIAŁAŃ
na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022

Warszawa, październik 2017 r.

Spis treści

Załącznik 1:
Katalog zadań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022

Załącznik 2:
Wykaz działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022

1. Wprowadzenie

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022 (dalej: KRPC) przyjęte przez Radę Ministrów uchwałą[1] dnia 27 kwietnia 2017 r. stanowią deklarację celu, jaki ma zostać osiągnięty w zakresie cyberbezpieczeństwa w perspektywie roku 2022, celów szczegółowych oraz kierunków interwencji służących ich osiągnięciu.

KRPC zobowiązuje Koordynatora[2] do przygotowania planu działań będącego głównym narzędziem wdrażania strategii i bieżącego monitoringu.

Plan działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022 (dalej: *Plan działań KRPC*) został przygotowany we współpracy z członkami Rady Ministrów oraz kierownikami urzędów centralnych oraz Dyrektorem Rządowego Centrum Bezpieczeństwa

Podczas prac nad *Planem działań KRPC* współpracowano z instytucjami spoza administracji rządowej, a w szczególności z Biurem Bezpieczeństwa Narodowego oraz NASK Państwowym Instytutem Badawczym.

***Plan działań KRPC* będąc <u>dokumentem planistycznym</u> (narzędzie wdrażania KRPC)** przedstawia:

- kierunki interwencji organów administracji rządowej do 2022 roku;
- wykaz zadań służących osiągnięciu celów KRPC;
- wykaz działań w odniesieniu do zidentyfikowanych zadań;
- zagadnienia monitorowania i sprawozdawczości;

Plan działań KRPC umożliwia w usystematyzowany sposób identyfikację działań niezbędnych do osiągnięcia celów szczegółowych KRPC, a przez to osiągnięcie celu głównego na koniec okresu planistycznego. Jednocześnie plan będzie służyć prowadzeniu monitorowania i opracowywania sprawozdań dotyczących skuteczności wdrażania KRPC. Monitorowanie realizacji planu umożliwi jego modyfikację w miarę zaistniałych potrzeb oraz będzie stanowić podstawę wnioskowania zmian w samych KRPC.

Rolą *Planu działań KRPC* jest także uzyskanie zsynchronizowanego podejścia do działań poszczególnych organów na rzecz krajowego systemu cyberbezpieczeństwa i zapewnienie, że żadne z zadań niezbędnych dla osiągnięcia celów szczegółowych KRPC nie zostanie pominięte. Poszczególne działania planowane będą z jednej strony z uwzględnieniem zasobów będących w posiadaniu organu je planującego niezbędnych do ich realizacji, z drugiej zaś strony powinny uwzględniać przyszłe, planowane działania, dla których potrzebne są źródła finansowania,. Przewiduje się, że katalog zadań oraz wykaz działań prezentowany w załącznikach do *Planu działań KRPC* będą uzupełniane na wniosek zainteresowanego podmiotu co 6 miesięcy i aktualizowane co 2 lata. Z uwagi na zmieniające się warunki społeczno-gospodarcze zarówno katalog zadań oraz wykaz działań mogą być uzupełniane o nowe zadania i działania, z uwzględnieniem projektów współfinansowanych ze środków europejskich.

[1] Uchwała Rady Ministrów nr 52/2017 z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022, nie publikowana w M.P.

[2] Koordynatorem na podstawie § 2 ust. 3 uchwały Rady Ministrów nr 52/2017 z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022 jest minister właściwy do spraw informatyzacji, któremu RM powierzyła koordynowanie i nadzorowanie wdrażania KRPC.

Plan działań KRPC będzie rozpatrywany i opiniowany przez organy zobowiązane do jego realizacji, a następnie zatwierdzony przez Koordynatora i przedłożony do wiadomości Rady Ministrów.

2. Kierunki interwencji organów administracji rządowej do 2022 roku

We wdrażanie KRPC w horyzoncie czasowym do 2022 roku będą zaangażowane organy administracji rządowej.

Kierunki interwencji wspólne dla podmiotów zaangażowanych w realizację Planu działań KRPC skupiać się będą na:

- współdziałaniu mającym na celu zaprojektowanie, wdrożenie, a następnie utrzymywanie i doskonalenie krajowego systemu cyberbezpieczeństwa;
- włączaniu problematyki cyberbezpieczeństwa w zakres wszelkich działań urzędów obsługujących dany organ;
- monitorowaniu postępów w realizacji wyznaczonych kierunków interwencji KRPC w zakresie swojej właściwości;
- podejmowaniu inicjatyw zmierzających do zmniejszenia poziomu ryzyka dla działalności organu, związanego z zagrożeniami dla systemów teleinformatycznych wspierających realizację procesów, za które dany organ ponosi odpowiedzialność;
- planowaniu zasobów kadrowych i finansowych niezbędnych do realizacji poszczególnych działań służących realizacji celów KRPC;
- podwyższaniu standardów sprawnego zarządzania bezpieczeństwem informacji w urzędach obsługujących dany organ;
- udziale w edukacji na potrzeby cyberbezpieczeństwa, tak w odniesieniu do urzędników i pracowników urzędów, jak i odbiorców usług świadczonych z wykorzystaniem systemów teleinformatycznych;

Kierunki interwencji poszczególnych organów administracji rządowej zaangażowanych we wdrażanie KRPC.
Organy administracji rządowej realizując poszczególne działania występują w roli organu wiodącego, odpowiedzialnego za przygotowanie i poprowadzenie danego działania lub w roli organu współdziałającego, który wspiera organ wiodący w uzgodnionym zakresie. Organ administracji rządowej może wyznaczyć do realizacji działania podległą lub nadzorowana jednostkę organizacyjną. Rolę danego podmiotu określa Załącznik 2.

Poszczególne organy administracji rządowej biorą udział w realizacji działań w ramach następujących kierunków interwencji.

Minister właściwy do spraw informatyzacji w zakresie:

- Dostosowania otoczenia prawnego do potrzeb i wyzwań w obszarze cyberbezpieczeństwa;
- Udoskonalenia struktury krajowego systemu cyberbezpieczeństwa;
- Zwiększenia efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni RP;
- Zwiększenia bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej;

- Opracowania i wdrożenia standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych;
- Wypracowania i wdrożenia systemu zarządzania ryzykiem na poziomie krajowym;
- Zapewnienia bezpiecznego łańcucha dostaw;
- Zbudowania systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń;
- Zbudowania zdolności w zakresie analizy zagrożeń na poziomie krajowym;
- Audytów i testów bezpieczeństwa;
- Zbudowania mechanizmów współpracy między sektorem publicznym i prywatnym;
- Stymulowania badań i rozwoju w obszarze bezpieczeństwa systemów teleinformatycznych;
- Zwiększania kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni;
- Stworzenia warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli;
- Aktywnej współpracy międzynarodowej na poziomie strategiczno-politycznym;
- Aktywnej współpracy międzynarodowej na poziomie operacyjnym i technicznym.

Minister właściwy do spraw nauki i szkolnictwa wyższego w zakresie:

- Stymulowania badań i rozwoju w obszarze bezpieczeństwa systemów teleinformatycznych;
- Zwiększania kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni.

Minister właściwy do spraw obrony narodowej w zakresie:

- Uzyskania zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni;
- Zbudowania systemu bezpiecznej komunikacji na potrzeby bezpieczeństwa narodowego;
- Audytów i testów bezpieczeństwa;
- Rozbudowy zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa;
- Zbudowania mechanizmów współpracy między sektorem publicznym i prywatnym;
- Stymulowanie badań i rozwoju w obszarze bezpieczeństwa systemów teleinformatycznych;
- Zwiększania kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni;
- Aktywnej współpracy międzynarodowej na poziomie strategiczno-politycznym;
- Aktywnej współpracy międzynarodowej na poziomie operacyjnym i technicznym.

Minister właściwy do spraw oświaty i wychowania w zakresie:

- Stworzenia warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli;
- Zwiększania kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni.

Minister właściwy do spraw pracy oraz **Minister właściwy do spraw rodziny** w zakresie:

- Stworzenia warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli.
- Zwiększania kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni.

Minister właściwy do spraw rozwoju regionalnego oraz **Minister właściwy do spraw gospodarki w zakresie**:

- Rozbudowy zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa;
- Zbudowanie mechanizmów współpracy między sektorem publicznym i prywatnym;
- Aktywnej współpracy międzynarodowej na poziomie strategiczno-politycznym.

Minister sprawiedliwości w zakresie:

- Zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, występującej w cyberprzestrzeni;
- Aktywnej współpracy międzynarodowej na poziomie strategiczno-politycznym;
- Aktywnej współpracy międzynarodowej na poziomie operacyjnym i technicznym.

Minister właściwy do spraw wewnętrznych w zakresie:

- Zwiększania zdolności do zwalczania cyberprzestępczości;
- Stymulowanie badań i rozwoju w obszarze bezpieczeństwa systemów teleinformatycznych;
- Zwiększania kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni;
- Aktywnej współpracy międzynarodowej na poziomie strategiczno-politycznym;
- Aktywnej współpracy międzynarodowej na poziomie operacyjnym i technicznym.

Minister właściwy do spraw zagranicznych oraz **minister właściwy do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej** w zakresie:

- Aktywnej współpracy międzynarodowej na poziomie strategiczno-politycznym.

Minister koordynator służb specjalnych w zakresie:

- Zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, występującej w cyberprzestrzeni;
- Zbudowania systemu bezpiecznej komunikacji na potrzeby bezpieczeństwa narodowego;
- Audytów i testów bezpieczeństwa**.**

Dyrektor Rządowego Centrum Bezpieczeństwa w zakresie:

- Opracowanie i wdrożenie standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych w odniesieniu do infrastruktury krytycznej.

3. Zadania i działania wdrażające KRPC

Katalog zadań i wykaz działań na rzecz wdrażania KRPC zostały przedstawione odpowiednio w załączniku nr 1 i nr 2. Zostały one uszeregowane zgodnie z układem celów szczegółowych i kierunków interwencji KRPC.
Krajowe Ramy Polityki Cyberbezpieczeństwa wyznaczają następujące cele szczegółowe:

Cel szczegółowy 1. Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa.
Cel szczegółowy 2. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom.
Cel szczegółowy 3. Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni.
Cel szczegółowy 4. Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

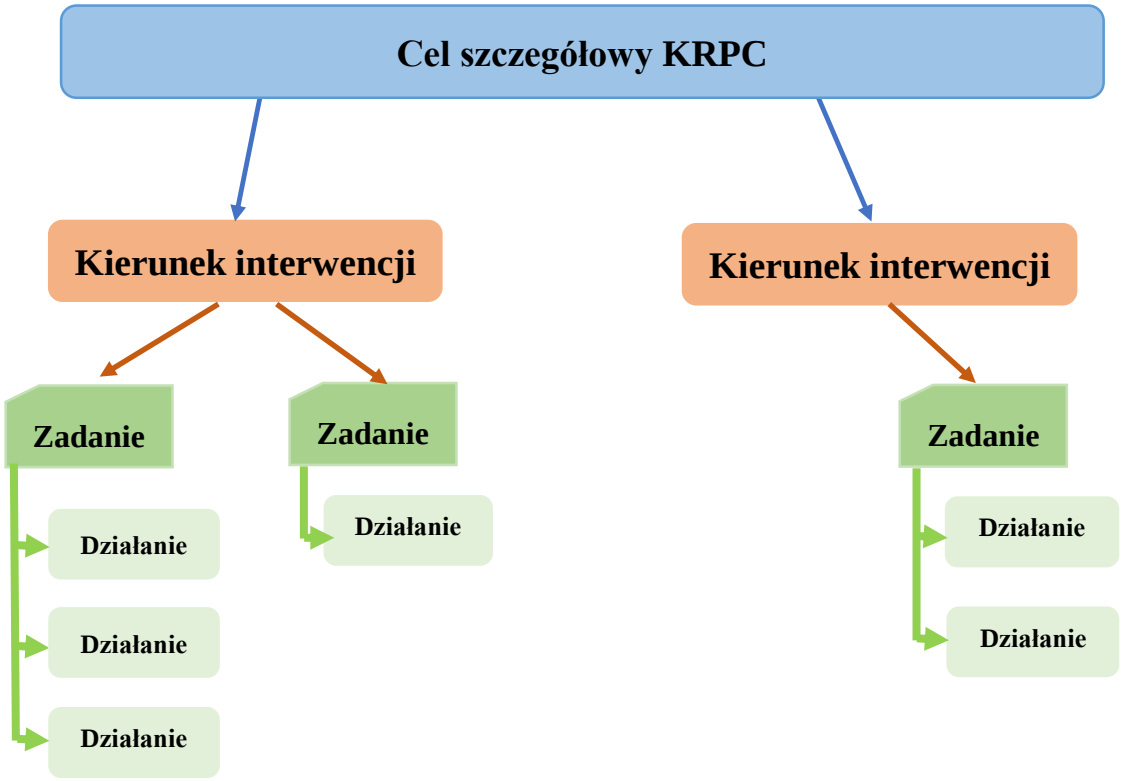
.

Przewiduje się, że zmiany wprowadzane do katalogu i wykazu (aktualizacje) będą mogły mieć różny charakter:,

- będą mogły być wprowadzane nowe zadania wraz z inicjatywami je wdrażającymi (czyli działaniami),
- będą dodawane nowe działania w ramach zadań,
- będą weryfikowane poszczególne działania m.in. pod względem ich stanu wdrażania.

Załącznik 2 uwzględnia działania o charakterze projektowym, zmierzające do wprowadzania zmian organizacyjnych, prawnych i proceduralnych oraz technologicznych w różnych obszarach funkcjonowania państwa w celu podniesienia poziomu cyberbezpieczeństwa. . W załączniku 2 nie uwzględniono działań mających charakter ciągły, powtarzalny cyklicznie, wynikający z przepisów prawa czy kompetencji danego organu administracji rządowej, takich jak na przykład realizacja przez pracodawcę szkoleń wewnętrznych zmierzających do podniesienia kompetencji zawodowych pracowników, wymiana i utrzymanie funkcjonujących urządzeń informatycznych, przygotowywanie sprawozdań czy opinii, dostosowywanie planów zarządzania kryzysowego do nowych procedur, organizowanie cyklicznych spotkań czy konferencji, itp.

Struktura Planu działań KRPC



Zadania i działania realizacji zostały usystematyzowane w tabelach zgodnie z celami szczegółowymi i kierunkami interwencji KRPC. Poszczególne kolumny tabel w załączniku 2 oznaczają:

1. **numer zadania**. – liczbowy identyfikator zadania;
2. **zadanie** – nazwa zadania o charakterze kompleksowym i realizowanym przez podejmowanie różnych działań w danym obszarze zagadnieniowym;
3. **działanie** – nazwa oraz liczbowy identyfikator działania służącego realizacji zadania,
4. **typ działania** – działanie: legislacyjne, instytucjonalne, inwestycyjne, programowe, edukacyjne, informacyjne, promocyjne, inny;
5. **harmonogram** – termin rozpoczęcia i termin zakończenia podejmowanej inicjatywy;
6. **forma zakończenia działania** – tryb/sposób wdrożenia podejmowanej inicjatywy;
7. **organ/organy** – organy wiodące i współpracujące przy realizacji podejmowanej inicjatyw;
8. **oczekiwane efekty** – syntetyczna informacja o oczekiwanych efektach wdrożenia podejmowanego działania;
9. **szacowany koszt działania** – informacja o szacowanym koszcie działania wraz z przewidywanym źródłem finansowania;
10. **stan wdrażania działania**: „R” – realizowane; „P” – planowane, „M” – zmodyfikowane; „Z” – zakończone; „W” – wykreślone; „N” – nie zdefiniowane w aktualnej wersji Planu.

Wzór tabeli załącznika 1

Katalog zadań

Planu działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa

Kierunek interwencji	Zadanie	Charakter
Cel szczegółowy		
Kierunek interwencji		

P – zadanie o charakterze projektowym C – zadanie o charakterze ciągłym

Wzór tabeli załącznika 2

Wykaz zadań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa o charakterze projektowym

CEL SZCZEGÓŁOWY KRPC:

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN} lata 2017 i 2018	Szacunkowy koszt realizacji [PLN} (lata 2019-2021)	stan wdrażania działania
				Termin rozpoczęcia działania (miesiąc/rok lub rok)	Termin zakończenia działania (miesiąc/rok lub rok)		wiodący	współpracujący		Źródło finansowania	Źródło finansowania	
Kierunek interwencji												

Typ działania:
L – legislacyjne,
O – organizacyjne,
T – technologiczne,
E – edukacyjne,
I – informacyjne,
P – promocyjne.

Stan wdrażania działania:
P – w przygotowaniu,
R – w realizacji,
Z – zakończone.

4. Finansowanie działań

Sam fakt zgłoszenia przez dany organ działania do Planu działań KRPC nie oznacza automatycznego zarezerwowania środków na ten cel w budżecie państwa. Stanowi natomiast informację pozwalającą prognozować koszty wdrażania KRPC. Organy występują o środki na finansowanie działań na ogólnych zasadach przewidzianych przepisami ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. 2016 r. poz. 1870, z późn. zm.). Działania będą realizowane w miarę uwzględnienia ich finansowania w budżecie państwa. Działania wskazane w Planie działań KRPC mogą być także finansowane z innych źródeł niż budżet państwa, w tym ze środków pomocowych Unii Europejskiej.
Suma szacunkowych kosztów realizacji poszczególnych działań ujętych w aktualnej wersji załącznika 2 nie odzwierciedla całości nakładów jakie będą niezbędne na osiągnięcie celu głównego KRPC w perspektywie roku 2022. Kolejne działania mogą się pojawiać w ramach aktualizacji Planu.

5. Monitorowanie i sprawozdawczość

Monitorowanie wdrażania zadań i działań będzie prowadzone przez Koordynatora w całym okresie programowym, tj. do 2022 roku. Informacje o stanie realizacji działań będzie przedstawiał organ wiodący odpowiedzialny za jego wykonanie w terminie uzgodnionym z Koordynatorem.

Niezależnie od prowadzonego monitoringu Koordynator będzie corocznie przygotowywać sprawozdanie o postępach wdrażania Planu działań na rzecz wdrożenia KRPC za rok poprzedni na podstawie informacji zebranych od organów wiodących w realizacji danego działania.
Sprawozdania będą przedkładane Radzie Ministrów. Pierwsze sprawozdanie zostanie opracowane za rok 2018.

Koordynator KRPC w celu usprawnienia pracy w zakresie wdrażania, monitorowania i sprawozdawczości wyznaczy komórkę organizacyjną w Ministerstwie Cyfryzacji, do zakresu której będzie należało prowadzenie spraw związanych z wykonywaniem ww. zadań. Ponadto podmioty wdrażające KRPC wyznaczą swoich przedstawicieli do bieżącej współpracy z Ministerstwem Cyfryzacji przy realizacji Planu.

6. Wykaz skrótów

ABW	Agencja Bezpieczeństwa Wewnętrznego
BBN	Biuro Bezpieczeństwa Narodowego
COI	Centralny Ośrodek Informatyki
ENISA	European Union Agency for Network and Information Security
ILiM	Instytut Logistyki i Magazynowania
IŁ	Instytut Łączności - Państwowy Instytut Badawczy
KPRM	Kancelaria Prezesa Rady Ministrów
MC	Ministerstwo Cyfryzacji
MEN	Ministerstwo Edukacji Narodowej
MNiSW	Ministerstwo Nauki i Szkolnictwa Wyższego
MON	Ministerstwo Obrony Narodowej
MR	Ministerstwo Rozwoju
MRPiPS	Ministerstwo Rodziny, Pracy i Polityki Społecznej
MS	Ministerstwo Sprawiedliwości
MSWiA	Ministerstwo Spraw Wewnętrznych i Administracji

MSZ	Ministerstwo Spraw Zagranicznych
NCBJ	Narodowe Centrum Badań Jądrowych
NCBiR	Narodowe Centrum Badań i Rozwoju
NASK	Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy
PAIH	Polska Agencja Inwestycji i Handlu
PARP	Polska Agencja Rozwoju Przedsiębiorczości
PW	Politechnika Warszawska
RCB	Rządowe Centrum Bezpieczeństwa
SOASP	Projekt realizowany przez NASK w ramach programu Common Facility Framerwork