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

CEL SZCZEGÓŁOWY KRPC: 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

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
Kierunek interwencji 1.1. Dostosowanie otoczenia prawnego do potrzeb i wyzwań w obszarze cyberbezpieczeństwa												
1.1.1	Opracowanie podstaw prawnych krajowego systemu cyberbezpieczeństwa	1 1.1.1 Opracowanie projektu ustawy o krajowym systemie cyberbezpieczeństwa	L	I 2016	XII 2017	Przekazanie projektu ustawy do Sejmu	MC	pozostałe ministerstwa	Stworzenie podstawy prawnej do funkcjonowania krajowego systemu cyberbezpieczeństwa. Transpozycja dyrektywy NIS	w ramach działań statutowych ministerstw		R
		1 1.1.2. Opracowanie projektów aktów wykonawczych do ustawy o krajowym systemie cyberbezpieczeństwa	L	I 2018	VI 2018	Uzgodnienie treści aktów	MC	pozostałe ministerstwa	Stworzenie podstawy prawnej do funkcjonowania krajowego systemu cyberbezpieczeństwa. Transpozycja dyrektywy NIS	w ramach działań statutowych ministerstw		P
1.1.3	Opracowanie słownika terminologii z obszaru cyberbezpieczeństwa używanej w aktach prawnych	1.1.3.1 Zorganizowanie prac nad opracowaniem słownika terminologii z obszaru cyberbezpieczeństwa używanej w aktach prawnych	O	VI 2017	XII 2018	Słownik terminologii z obszaru cyberbezpieczeństwa używanej w aktach prawnych	MC	IŁ PKN BBN	Ujednolicenie słownictwa w zakresie cyberbezpieczeństwa stosowanego w aktach prawnych	150 000		R
1.1.4	Dokonanie przeglądu istniejących regulacji prawnych, sektorowych i szczególnych, które dotyczą lub wymagają uzupełnienia o zakres cyberbezpieczeństwa.	1.1.4.1 Przegląd regulacji prawnych mających związek z cyberbezpieczeństwem	L	VI 2018	III 2019	Mapa powiązań przepisów w zakresie cyberbezpieczeństwa	MC	pozostałe ministerstwa	Dokonanie uspójnienia przepisów i usunięcie ewentualnych kolizji	w ramach działań statutowych ministerstw	w ramach działań statutowych ministerstw	P
Kierunek interwencji 1.2 Udoskonalenie struktury krajowego systemu cyberbezpieczeństwa												
1.2.2	Opracowanie koncepcji zmapowania zasobów osobowych i kompetencyjnych; prowadzenie rejestru/bazy danych tych zasobów cyberbezpieczeństwa	1.2.2.1 Opracowanie koncepcji bazy danych tych zasobów osobowych i kompetencyjnych w zakresie cyberbezpieczeństwa	O	VI 2018	XII 2018	Dokument koncepcji	MC	MON ABW NASK	Stworzenie bazy wiedzy o specjalistach z zakresu cyberbezpieczeństwa	30 000 budżet państwa		P
1.2.3	Opracowanie i wdrożenie programu pozyskiwania i retencji ekspertów cyberbezpieczeństwa w administracji państwowej	1,2,3,1 Opracowanie koncepcji pozyskiwania i retencji ekspertów cyberbezpieczeństwa w administracji państwowej	O	VI 2018	XII 2018	Dokument koncepcji	MC	MON, MRPiPS ABW NASK	Przeprowadzenie analizy wariantów rozwiązań pozwalających na skuteczne zasilanie administracji państwowej w specjalistów z zakresu cyberbezpieczeństwa	40 000 budżet państwa		P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
1.2.4	Określenie kompetencji organów właściwych, odpowiedzialnych za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe.	1.2.4.1 Określenie kompetencji organów właściwych, odpowiedzialnych za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe.	L	III 2017	V 2018	Projekt aktu prawnego	MC	pozo-stałe mini-ster-stwa	Stworzenie podstaw prawnych niezbędnych do sprawowania przez organy właściwe nadzoru nad podmiotami świadczącymi usługi kluczowe i usługi cyfrowe	w ramach działań statutowych ministerstw	ministerstw	R
1.2.5	Rozbudowa struktur zajmujących się cyberbezpieczeństwem na poziomie operacyjnym, w tym narodowego centrum cyberbezpieczeństwa (NC Cyber), CSIRT poziomu krajowego, , sektorowych zespołów reagowania na incydenty , centrów wymiany i analizy informacji	1.2.5.1 Wsparcie budowy kompetencji CERT/CSIRT w sektorach	O	X 2018	IX 2021	Osiągnięcie zakładanego poziomu dojrzałości zespołów CSIRT w sektorach i podsektorach	NASK		Celem projektu jest: a) opracowanie projektu technicznego umożliwiającego realizację usług z punktu widzenia technicznego (uwzględniają aspekty sieciowe, sprzętowe i oprogramowania) b) opracowanie procesów, procedur i instrukcji z uwzględnieniem specyfiki danego sektora c) pomoc w rekrutacji personelu na konkretne stanowiska, szkolenia personelu do pełnienia konkretnych ról w procesach d) pełne wdrożenie procesów wraz z mechanizmami pomiaru KPI i elementami raportowania zarządczego e) opracowanie i wdrożenie mechanizmów integracji systemów z NC Cyber i innymi interesariuszami w miarę potrzeb	50 000 budżet państwa	700 000 budżet państwa	P
		1.2.5.2 Budowa portalu Cyber-policy	O/T	IV 2017	II 2018	Działający portal Cyber-policy	NASK		Celem projektu jest uruchomienie jednego miejsca w Internecie (portalu) z którego interesariusze krajowego systemu ochrony cyberprzestrzeni mogliby czerpać wiedzę, zarówno nieprzetworzoną jak i opracowaną dotyczącą aspektów policy w dziedzinie cyberbezpieczeństwa.	50 000 budżet państwa		R

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
	informacji.	1.2.5.3 Budowa centrum zapasowego kluczowych usług NC Cyber	T	VI 2018	V 2021	Oddanie centrum do eksploatacji	NASK		Celem projektu jest zbudowanie infrastruktury serwerowej i teletransmisyjnej wraz z urządzeniami sieciowymi i systemami bezpieczeństwa teleinformatycznego oraz osadzenie na tej infrastrukturze niezbędnych do zachowania ciągłości działania usług świadczonych przez narodowe centrum cyberbezpieczeństwa, a także zbudowanie interfejsów synchronizacji informacji, procedur utrzymania i przełączania funkcji pomiędzy lokalizacją podstawową i zapasową.	500 000 budżet państwa	4 500 000 budżet państwa	
Kierunek interwencji 1.3. Zwiększenie efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni RP												
1.3.1	Budowa zintegrowanego systemu wymiany informacji	1.3.1.1 Budowa centralnego modułu zintegrowanego systemu wymiany informacji NPC	T	IX 2017	VIII 2020	System wdrożony w NC Cyber w ramach realizacji projektu Narodowej Platformy Cyberbezpieczeństwa	NASK	MC, IŁ, PW, NCBJ	W ramach projektu NPC (Narodowa Platforma Cyberbezpieczeństwa) powstanie zintegrowany system wymiany informacji o zagrożeniach, incydentach i ryzykach w odniesieniu do cyberprzestrzeni RP	6 000 000 budżet państwa (NCBiR)	16 956 000 (sumaryczna wart. projektu z pkt. 1.3.1, 1.4.2, 1.6.1) budżet państwa (NCBiR)	R
		1.3.1.2 Zaprojektowane wydzielonej sieci NPCnet na potrzeby zintegrowanego systemu wymiany informacji	T	X 2017	XII 2018	Sporządzenie niezbędnej dokumentacji sieci NPCnet	NASK		1. Koncepcja sieci szkieletowej Narodowej Platformy Cyberbezpieczeństwa zawierająca analizę możliwych rozwiązań. 2. Projekt wykonawczy sieci szkieletowej Narodowej Platformy Cyberbezpieczeństwa, szczegółowo opisujący opracowaną koncepcję realizacji sieci szkieletowej. 3. Szczegółowy projekt wykonawczy realizacji podłączeń dla 3 podmiotów 4. Założenia i wytyczne projektowe przyłączeń do sieci szkieletowej Narodowej Platformy Cyberbezpieczeństwa dla pozostałych, podmiotów.	243 485 budżet państwa		P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
1.3.2	Przygotowanie programu ćwiczeń i treningów w skali kraju i w skali poszczególnych sektorów	1.3.2.1 Opracowanie i uruchomienie ćwiczeń Table Top	O	XI 2017	XII 2022	Przeprowadzenie ćwiczeń z udziałem CSIRT	NASK		Celem projektu jest weryfikacja procedur współpracy NC Cyber i zespołami CSIRT zakresie reagowania na incydenty cyberbezpieczeństwa.	50 000 budżet państwa	200 000 budżet państwa	P
		1.3.2.2 Opracowanie i uruchomienie programu CyberPOL	O	V 2017	XII 2022	Przeprowadzone ćwiczenia z udziałem organów ścigania	NASK		Celem projektu jest wzajemne podnoszenie kompetencji NC Cyber i organów ścigania w zakresie zwalczania cyberprzestępczości. W ramach projektu przeprowadzone będą ćwiczenia (do 5 rocznie), warsztaty (do 3 rocznie) oraz eksperymenty typu case study (do 6 rocznie).	150 000 budżet państwa	400 000 budżet państwa	P
		1.3.2.3 Organizacja ćwiczeń red-blue team	O	VI 2018	XII 2022	Przeprowadzone ćwiczenie	NASK		Celem projektu jest doskonalenie kompetencji zespołów reagowania (SOC/ CSIRT) w zakresie ochrony systemów teleinformatycznych. W ramach projektu przygotowany zostanie program ćwiczeń i wynajęta zostanie usługa na platformie typu Cyber Range	200 000 budżet państwa	800 000 budżet państwa	P
		1.3.2.4 Opracowanie lub zakup poligonu Cyber Range	T	I 2019	XII 2020	Udostępnienie środowiska do prowadzenia ćwiczeń	NASK		Celem projektu jest uzyskanie środowiska informatycznego do prowadzenia ćwiczeń z zakresu cyberbezpieczeństwa w warunkach symulacyjnych.		2 000 000 budżet państwa	P
1.3.3	Aktywny udział w ćwiczeniach prowadzonych zarówno przez organizacje krajowe, podmioty UE i NATO oraz inne podmioty międzynarodowe.	1.3.3.1 Aktywny udział w krajowych i międzynarodowych ćwiczeniach cybernetycznych	O/E	VI 2017	XII 2022	Udział w ćwiczeniach	NASK		Efektem działania jest udział w wielu ćwiczeniach krajowych i zagranicznych z dziedziny cyberbezpieczeństwa, solidne przygotowanie do ćwiczeń i podsumowanie po zakończeniu. Działanie ma także na celu budowę silnego zespołu narodowego.	60 000 budżet państwa	180 000 budżet państwa	R
1.3.4	Przystąpienie do zaufanych międzynarodowych forów wymiany informacji o zagrożeniach w cyberprzestrzeni.	1.3.4.1 Przystępowanie i aktywny udział w zaufanych międzynarodowych forach wymiany informacji p zagrożeniach w cyberprzestrzeni.	O/E	I 2017	XII 2022	Aktywny udział w forach.	NASK		NASK jest lub będzie członkiem takich organizacji i inicjatyw jak: FISRT, INHOPE, TF-CSIRT, ECSO, Trusted Introducer, APWG, NoMoreRansome i inne tego typu.	80 000 budżet państwa	225 000 budżet państwa	R
Kierunek interwencji 1.4. Zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej												

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
1.4.1	Opracowywanie standardowych procedur operacyjnych dotyczących współpracy w obsłudze incydentu w cyberprzestrzeni, w tym schematów raportowania dla operatorów usług kluczowych i dostawców usług cyfrowych	1.4.1.1 Opracowanie standardowych procedur operacyjnych dotyczących współpracy w obsłudze incydentu w cyberprzestrzeni, w tym schematów raportowania do operatorów usług kluczowych i dostawców usług cyfrowych.	O	I 2018	XII 2019	Opracowanie dokumentów i przekazanie do stosowania (i ew. umocowania w rozporządzeniach)	MC	NASK, RCB	Efektem działania będą opracowane schematy raportowania dla sektorów oraz pełne procedury operacyjne dotyczące współpracy w obsłudze incydentów w cyberprzestrzeni.	60 000 budżet państwa	100 000 budżet państwa	P
1.4.2	Opracowanie systemu wspierającego analizę współzależności pomiędzy sektorami operatorów usług kluczowych oraz pomiędzy operatorami a dostawcami usług cyfrowych oraz przeprowadzanie analiz na podstawie pozyskanych danych źródłowych	1.4.2.1 Opracowanie i wdrożenie rozwiązania teleinformatycznego wspierającego analizę współzależności pomiędzy sektorami operatorów usług kluczowych oraz pomiędzy operatorami a dostawcami usług cyfrowych.	T	IX 2017	VIII 2020	System wdrożony w NC Cyber w ramach realizacji projektu Narodowej Platformy Cyberbezpieczeństwa	NASK	RCB,MC	W ramach projektu NPC (Narodowa Platforma Cyberbezpieczeństwa) powstanie zintegrowany system ekspercki wspierający analizę współzależności pomiędzy sektorami operatorów usług kluczowych oraz pomiędzy operatorami a dostawcami usług cyfrowych oraz umożliwiający przeprowadzanie analiz na podstawie pozyskanych danych źródłowych	(w ramach budżetu projektu z pkt. 1.3.1)	W latach 2019-2020: (w ramach budżetu projektu z pkt. 1.3.1) W roku 2021: 40 000 budżet państwa (NCBiR)	R
		1.4.2.2 Utrzymywanie modelu powiązań i regularna weryfikacja jego poprawności oraz przeprowadzanie analiz na podstawie pozyskanych danych źródłowych.	I	VI 2018	XII 2022	Aktualny model powiązań z maksymalnie dobrze dobranymi parametrami powiązań.	NASK		Efektem tego działania jest utrzymywanie modelu powiązań usług kluczowych, operatorów usług kluczowych i dostawców treści cyfrowych na najwyższym poziomie. Stała analiza powiązań prowadząca do rekomendacji i usprawniania modelu w rzeczywistości.	20 000 budżet państwa	100 000 budżet państwa	P
1.4.3	Opracowanie kryteriów identyfikacji UK i IK z uwzględnieniem potrzeby ich integracji	1.4.5.1 Powołanie zespołu MC - RCB	O	XI 2017	V 2018	Opracowanie dokumentu opisującego kryteria	MC	RCB, NASK	Uzyskanie możliwości jednoznacznej i transparentnej identyfikacji usługodawców	30 000 budżet państwa		P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
1.4.4	Opracowanie minimalnych wymagań zapewnienia bezpieczeństwa teleinformatycznego (organizacyjne i techniczne) dla operatorów usług kluczowych (w obszarach IT, OT, kompetencji personelu)	1.4.4.1 Opracowanie minimalnych wymagań zapewnienia bezpieczeństwa teleinformatycznego (organizacyjne i techniczne) dla operatorów usług kluczowych (w obszarach IT, OT, kompetencji personelu)	O/T	VI 2016	XII 2018	Publikacja dokumentów zawierających dobre praktyki	MC	ABW RCB	Podniesienie poziomu cyberbezpieczeństwa w podmiotach świadczących usługi kluczowe	60 000 budżet państwa	75 000 budżet państwa	R
1.4.5	Opracowanie metodyki przeprowadzania wewnętrznych i zewnętrznych audytów bezpieczeństwa teleinformatycznego.	1.4.5.1 Opracowanie metodyki przeprowadzania wewnętrznych i zewnętrznych audytów bezpieczeństwa teleinformatycznego	O	I 2018	XI 2018	Publikacja dokumentu metodyki	MC	ABW IŁ RCB NASK	Ujednolicenie audytów w celu uzyskania porównywalności wyników w różnych podmiotach	150 000 budżet państwa		P
1.4.6	Opracowanie programu szkolenia dla operatorów IK/UK z zakresu bezpieczeństwa teleinformatycznego (uświadamiające oraz podnoszące kwalifikacje).	1.4.6.1 Opracowanie programu szkolenia dla operatorów IK/UK z zakresu bezpieczeństwa teleinformatycznego (uświadamiające oraz podnoszące kwalifikacje).	E	XII 2017	XI 2018	Publikacja programu szkolenia	MC	RCB	Podniesienie kompetencji pracowników podmiotów świadczących usługi kluczowe (operatorów infrastruktury krytycznej).	: 40 000 budżet państwa	: 60 000 budżet państwa	P
1.4.7	Budowa Rządowego Klastra Bezpieczeństwa.	1.4.7.1 Budowa Rządowego Klastra Bezpieczeństwa dla ministerstw i urzędów centralnych	O/T	IX 2016	XII 2021	Rozliczenie projektu	MC	NASK COI	Znaczące podniesienie poziomu bezpieczeństwa państwowych systemów teleinformatycznych poprzez zapewnienie właściwej infrastruktury w zakresie bezpieczeństwa fizycznego i środowiskowego oraz w zakresie bezpieczeństwa sieciowego	12 000 00	178 772 443,00 działanie 2.1 POPC	P
Kierunek interwencji 1.5. Opracowanie i wdrożenie standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych												
1.5.1	Opracowanie podręcznika konfiguracji oprogramowania standardowego w typowych zastosowaniach.	1.5.1.1 Opracowanie podręcznika konfiguracji oprogramowania standardowego w typowych zastosowaniach.	T	I 2018	XII 2018	Publikacja podręcznika	NASK	MON ABW, IŁ	Podniesienie poziomu bezpieczeństwa podmiotów realizujących zadania publiczne poprzez usunięcie znanych podatności	300 000		N
1.5.2	Przegląd istniejących norm/ standardów/dobrych praktyk, ich tłumaczenie i udostępnienie.	1.5.2.1 Przegląd istniejących norm/standardów/dobrych praktyk, ich tłumaczenie i udostępnienie.	O	IV kw. 2017	IV kw. 2018	Odbiór przetłumaczonych tekstów	RCB	Pozostałe ministerstwa, PKN	Posiadanie przez uczestników systemu cyberbezpieczeństwa jednolitych tekstów norm, standardów i dobrych praktyk w celu ich stosowania.		220 000,00 budżet państwa	P
Kierunek interwencji 1.6. Wypracowanie i wdrożenie systemu zarządzania ryzykiem na poziomie krajowym												

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
1.6.1	Stworzenie systemu monitorującego zagrożenia i podatności w trybie rzeczywistym i dokonującego bieżącej oceny ryzyka naruszenia bezpieczeństwa państwa.	1.6.1.1 Stworzenie systemu monitorującego zagrożenia i podatności w trybie rzeczywistym i dokonującego bieżącej oceny ryzyka naruszenia bezpieczeństwa państwa	T	VIII 2017	XII 2020	System wdrożony w NC Cyber w ramach realizacji projektu Narodowej Platformy Cyberbezpieczeństwa	NASK	MC	W ramach projektu NPC (Narodowa Platforma Cyberbezpieczeństwa) powstanie zintegrowany system monitorującego zagrożenia i podatności w trybie rzeczywistym i dokonującego bieżącej oceny ryzyka naruszenia bezpieczeństwa państwa. W kolejnych latach: rozwój i utrzymanie	(w ramach budżetu projektu z pkt. 1.3.1) NCBiR	W latach 2019-2020; w ramach budżetu projektu z pkt. 1.3.1) W roku 2021: 350 000 budżet państwa (NCBiR)	P
1.6.3	Opracowanie metodyki szacowania ryzyka naruszenia bezpieczeństwa państwa, uwzględniającej specyfikę poszczególnych sektorów, a także operatorów infrastruktury krytycznej, usług kluczowych i dostawców usług cyfrowych i spójnej z metodyką szacowania ryzyka na potrzeby raportu o stanie bezpieczeństwa państwa.	1.6.3.1 Opracowanie metodyki – koncepcja dynamicznego szacowania ryzyka	O	VII 2017	IX 2017	Dokument opisujący metodykę dynamicznego szacowania ryzyka.	NASK		W ramach działania opracowania zostanie koncepcja sposobu dynamicznego szacowania ryzyka w cyberprzestrzeni.	72 000 budżet państwa		R
		1.6.3.2 Wdrożenie komponentów dynamicznego szacowania ryzyka	T	VI 2018	VI 2019	Działające rozwiązanie technologiczne.	NASK		W ramach działania wdrożona zostanie metodyka dynamicznego szacowania ryzyka w cyberprzestrzeni RP.	W ramach NPC z NCBiR	budżet państwa w ramach NPC z NCBiR	R
		1.6.3.3 Wdrożenie procesów szacowania ryzyka w cyberprzestrzeni RP, dystrybucja raportów i rozwój merytoryczny.	O	IX 2018	VI 2019	Działające procesy szacowania ryzyka i dystrybucji raportów do interesariuszy KSC.	NASK		Opracowane zostaną procesy wraz z procedurami i instrukcjami stanowiskowymi, wyszkolony zostanie personel. Zakres informacji i forma raportów uzgodniona zostanie z interesariuszami.	20 000 budżet państwa	40 000 budżet państwa	P
Kierunek interwencji 1.7. Zapewnienie bezpiecznego łańcucha dostaw												
1.7.1	Zbudowanie krajowego systemu oceny i certyfikacji wyrobów sektora IT i uzyskanie pełnego członkostwa w SOGIS MRA	1.7.1.1 Zbudowanie krajowego systemu oceny i certyfikacji wyrobów sektora IT i uzyskanie pełnego członkostwa w SOGIS MRA	O/T	VI 2016	XII 2019	Akredytacja laboratoriów i jednostki certyfikującej przez PCA	IŁ PIB	NASK-PIB EMAG MR	Uzyskanie zdolności do certyfikacji wyrobów sektora ITK według normy PN ISO/IEC 15408 Osiągnięcie statusu Polski w porozumieniu SOGIS MRA na członka wydającego certyfikaty zgodne z Common Criteria uznawane globalnie.		19 961 224,00 budżet państwa (NCBiR)	R
1.7.2	Opracowanie modelu bezpiecznego łańcucha dostaw	1.7.2.1 Opracowanie koncepcji bezpiecznego łańcucha dostaw w administracji rządowej	O	III 2018	XII 2018	Dokument koncepcji	MC	MON MR ABW NASK	Zapewnienie bezpiecznych komponentów systemów teleinformatycznych przeznaczonych dla administracji rządowej	100 000 budżet państwa		P
Kierunek interwencji 1.8. Zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń												

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
1.8.1	Zbudowanie systemu bieżącego zarządzania bezpieczeństwem cyberprzestrzeni, który na podstawie zgłaszanych informacji o zagrożeniach i podatnościach, umożliwi ich agregowane, analizowanie i korelowanie, a także wypracowanie ostrzeżeń na temat zagrożeń i podatności i przekazywanie ich do zainteresowanych stron w taki sposób, aby zachowane zostały zasady poufności informacji przekazywanych w zgłoszeniach.	1.8.1.1 Strategia NC Cyber wraz z Docelowym Modelem Operacyjnym działania (TOM v1.0).	O	VII 2016	V 2017	Dokumenty strategiczne: Wizja NC Cyber i Docelowy Model Operacyjny.	NASK		Opracowanie dokumentów strategicznych zgodnych z dokumentami strategicznymi kraju w obszarze cyberbezpieczeństwa. Wizja NC Cyber opisuje cele strategiczne i operacyjne, proponowany katalog usług i sugerowane projekty i inicjatywy. Docelowy Model Operacyjny opisuje sposób funkcjonowania Narodowego Centrum Cyberbezpieczeństwa w ujęciu personalnym, procesowym, projektowym i technologicznym.	50 000 środki NASK		Z
		1.8.1.2 Wdrożenie Docelowego Modelu Operacyjnego (TOM v1.0) Narodowego Centrum Cyberbezpieczeństwa	O	VII 2017	VI 2018	Działające w NC Cyber usługi w oparciu o zdefiniowane procesy i technologie.	NASK		Wynikiem działania jest opracowana dokumentacja w postaci procedur i instrukcji stanowiskowych, wdrożone zostaną niezbędne rozwiązania technologiczne, a kadra zatrudniona i przeszkolona do realizacji procesów.	100 000 środki NASK		R
		1.8.1.3 Rozwój dokumentów strategicznych (Wizja i Docelowy Model Operacyjny) w miarę zmieniających się warunków środowiska i uwzględniając kierunki dyktowane oczekiwaniami ze strony partnerów NC Cyber.	O	III 2018	XII 2020	Zaakceptowane dokumenty strategiczne w kolejnej wersji.	NASK		Wynikiem realizacji działania będzie nowa wersja dokumentów strategicznych dostosowana do nowych uwarunkowań środowiska (strategii cyberbezpieczeństwa RP, ustawy o krajowym systemie cyberbezpieczeństwa i innych) oraz potrzeb i oczekiwań interesariuszy krajowego sytemu cyberbezpieczeństwa. Przewiduje się co najmniej 2 takie aktualizacje.	60 000 Budżet państwa	120 000 budżet państwa	P
		1.8.1.4 Utrzymanie działań operacyjnych wszystkich 3 linii obsługi zgłoszeń i monitorowania sytuacyjnego.	O	V 2017	XII 2022	Poprawne funkcjonowanie wszystkich procesów zdefiniowanych w modelu operacyjnym.	NASK		W wyniku realizacji działania zapewnione zostaną odpowiednie zasoby osobowe na wszystkich liniach działań operacyjnych Narodowego Centrum Cyberbezpieczeństwa niezbędnych do realizacji procesów biznesowych NC Cyber wraz z procesami wspierającymi.	5 870 000 środki NASK budżet państwa	21 860 000 budżet państwa	R
		1.8.1.5 Wdrożenie technologii umożliwiającej śledzenie i obrazowanie zagrożeń propagowanych poprzez SPAM.	T	I 2018	XII 2018	Działający w NC Cyber podsystem monitorowania.	NASK		Efektem realizacji działania jest działające rozwiązanie identyfikujące, kategoryzujące i prezentujące obraz zagrożeń propagowanych poprzez rozsyłanie wiadomości niechcianych.	2 000 000 NCBiR		P
		1.8.1.6 Wdrożenie technologii budowania obrazu sytuacyjnego z honeypotów	T	VI 2018	V 2019	Działający w NC Cyber podsystem monitorowania.	NASK		Efektem realizacji działania jest działające rozwiązanie pozwalające na obrazowanie skali i aktywności zagrożeń propagujących się w sposób automatyczny.	100 000 SOASP	500 000 budżet państwa	P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
		1.8.1.7 Wdrożenie technologii monitorowania aktywnego zagrożeń typu drive-by-download	T	I 2018	IX 2018	Działający w NC Cyber podsystem monitorowania.	NASK		Efektem realizacji działania jest działające rozwiązanie pozwalające na cykliczne monitorowanie popularnych zasobów w Internecie i wykrywanie zagrożeń typu drive-by-download.	60 000 budżet państwa		P
		1.8.1.8 Wdrożenie technologii wspierającej monitorowanie zasobów informacyjnych w celu wczesnej identyfikacji informacji o zagrożeniach.	T	I 2018	XII 2018	Działający w NC Cyber podsystem monitorowania.	NASK		Efektem realizacji działania będzie działający system wspierający pracę analityków. Monitorowanie mediów społecznościowych i forów wymiany informacji na temat cyberbezpieczeństwa jest jednym z istotniejszych kanałów wczesnego pozyskania informacji o incydentach zmaterializowanych, szczególnie poza granicami RP.	500 000 NCBiR		P
		1.8.1.9 Wdrożenie systemu komunikacji z zespołami CERT/CSIRT poziomu krajowego i partnerami NC Cyber	T	X 2017	XII 2017	Działający w NC Cyber podsystem monitorowania.	NASK		Efektem realizacji działania będzie działający i przetestowany system komunikacji, pozwalający na częste i szybkie zestawianie połączeń tele i video konferencyjnych. System zostanie przetestowany z interesariuszami i będzie regularnie wykorzystywany w działaniach operacyjnych NC Cyber.	środki NASK		P
		1.8.1.11 Wdrożenie systemu wymiany informacji o zagrożeniach MISP z partnerami NC Cyber.	T	VI 2017	X 2017	Działający w NC Cyber podsystem wymiany informacji.	NASK		Efektem realizacji działania będzie działający w Narodowym Centrum Cyberbezpieczeństwa system wymiany informacji o zagrożeniach udostępniony partnerom NC Cyber.	środki NASK		
		1.8.1.12 Wdrożenie systemu prezentacji stanu bezpieczeństwa partnerów NC Cyber w oparciu o wiedzę platformy n6	T	XI 2017	VI 2019	Działający w NC Cyber podsystem informacyjny.	NASK		Efektem realizacji działania jest działający w Narodowym Centrum Cyberbezpieczeństwa system prezentujący aktualne zagrożenia dotykające partnerów NC Cyber.	SOASP	SOASP	
		1.8.1.13 Wdrożenie nowego systemu informacyjnego dla partnerów NC Cyber wraz z forum wymiany wiedzy.	T	III 2017	X 2017	Działający w NC Cyber podsystem informacyjny.	NASK		Efektem realizacji działania jest działający nowy system informacyjny i forum wymiany wiedzy wśród partnerów NC Cyber.	środki NASK		R
1.8.2	Utworzenie systemu informacyjnego dla obywateli, w celu ochrony użytkowników końcowych przed	1.8.2.1 Serwis Phishing Alert	T	IX 2018	V 2019	Działający serwis internetowy z funkcjami powiadomień	NASK		Efektem działania będzie funkcjonujący serwis internetowy na którym regularnie (w sposób (pół)automatyczny publikowane będę obserwowanie przez NC Cyber kampanie phishingowe. System powiadomień zapewniałby efektywne informowanie obywateli o nowych zagrożeniach tego typu.	200 000 budżet państwa	500 000 budżet państwa	P
		1.8.2.2 Utworzenie systemu informacyjnego dla obywateli i małych i średnich przedsiębiorców	T	IX 2018	IV 2020	Działający portal z listami dystrybucji informacji.	NASK		Efektem realizacji działania będzie działający, publicznie dostępny, portal udostępniający bieżące informacje o zagrożeniach wraz poradami jak się zabezpieczać i bronić.	30 000 budżet państwa	1 500 000 Budżet państwa	P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
	skutkami zidentyfikowanych zagrożeń.	1.8.2.3 Promocja usług dla obywateli	I/P	I 2018	XII 2019	Zakończenie 3 kampanii informacyjno-promocyjnych.	NASK		Efektem realizacji działania będzie przeprowadzenie min. 3 kampanii informacyjno-promocyjnych mających na celu uświadamianie istnienia zagrożeń, informowanie gdzie/co/w jaki sposób należy zgłaszać incydenty.	30 000 budżet państwa	500 000 budżet państwa	P
		1.8.2.4 Automatyzacja procesów informowania poprzez RSO	T	VI 2018	XII 2018	Działające rozwiązanie technologiczne.	NASK		Efektem działania będzie automatyzacja generowania i/lub publikowania ostrzeżeń o zagrożeniach w cyberprzestrzeni poprzez Regionalny System Ostrzegania (RSO).	100 000 budżet państwa		P

CEL SZCZEGÓŁOWY KRPC: Cel szczegółowy 2. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
Kierunek interwencji 2.1. Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, występującej w cyberprzestrzeni												
2.1.8	Organizacja systemu obowiązkowych szkoleń dla przedstawicieli organów ścigania i wymiaru sprawiedliwości zajmujących się zwalczaniem cyberprzestępczości (zadanie powiązane z 1.1.1).	2.1.8.1 Przygotowanie i przeprowadzenie szkoleń przez specjalistów NC Cyber	O/E	VI 2018	XII 2020	Przeprowadzenie min. 20 szkoleń.	NASK		Efektem realizacji działania będzie przeprowadzenie min. 20 szkoleń dla organów ścigania i wymiaru sprawiedliwości.	100 000 budżet państwa	300 000 budżet państwa	P
Kierunek interwencji 2.2. Uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni												
2.2.1	Uregulowanie obszaru wytwarzania, posiadania, pozyskiwania oraz wykorzystywania specjalistycznych narzędzi z zakresu prowadzenia działań militarnych w cyberprzestrzeni przez resort obrony narodowej.	Wg. dokumentów wewnętrznych MON.	L	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	MON		Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.
2.2.8	Wytwarzanie bądź pozyskiwanie nowatorskich narzędzi służących do podniesienia skuteczności działań militarnych w cyberprzestrzeni.	Wg. dokumentów wewnętrznych MON	T	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	MON		Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON. Wg. dokumentów we-wnętrzowych MON.	Wg. dokumentów wewnętrznych MON.
Kierunek interwencji 2.3. Zbudowanie zdolności w zakresie analizy zagrożeń na poziomie krajowym												

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
2.3.1	Rozbudowanie zdolności analitycznych CERT Polska i NC Cyber w taki sposób aby uzyskać pełne spektrum zdolności analitycznych w cyberprzestrzeni na poziomie krajowym (powiązane z działaniem 1.8.1)	2.3.1.1 Rozbudowanie zdolności analitycznych CERT Polska i NC Cyber	O/T/E	IV 2018	IX 2021	Wdrożone narzędzia, procedury, testy, szkolenia i ćwiczenia konieczne do zaawansowanych działań analitycznych	NASK		Rozwinięcie w CERT Polska/NC Cyber kwalifikacji oraz narzędzi pozwalających na zaawansowane analizy sytuacyjne, zagrożeń, artefaktów oraz incydentów w cyberprzestrzeni na poziomie krajowym	250 000 budżet państwa	2 000 000. NCBiR/KE/budżet państwa	P
2.3.2	Stworzenie narzędzi badawczych pozwalających na prowadzenie zaawansowanych analiz na big data w obszarze cyberbezpieczeństwa	2.3.2.1 Nowe metody detekcji zagrożeń w cyberprzestrzeni	T	VI 2018	XII 2021	Biblioteki metod detekcji zagrożeń w cyberprzestrzeni.	NASK		Efektem realizacji działania są gotowe do wykorzystania komponenty lub narzędzia detekcji nowych rodzajów zagrożeń lub poprawa efektywności wykrywania istniejących zagrożeń, a także prace analityczne w zakresie opracowania technologii bigdata, metod statystycznych, uczenia maszynowego i analizy sieci społecznościowych. Wszystkie wytworzone rozwiązania mają posiadać możliwość integracji z Narodową Platformą Cyberbezpieczeństwa.	500 000 Budżet państwa/ KE	9 500 00 Budżet państwa/KE	P
		2.3.2.2 Budowa platformy monitorującej zdarzenia związane z dystrybucją pornografii dziecięcej	T	IX 2018	XII 2019	Działające rozwiązanie technologiczne	NASK		Efektem realizacji działania jest działająca platforma użytkowana przez analityków NC Cyber.	80 000 budżet państwa	400 000 budżet państwa	P
		2.3.2..3 Opracowanie i wdrożenie systemu rozpoznawania i analizy obrazów w celu poprawnej (pół) automatycznej klasyfikacji treści CASM	T	I 2019	XII 2020	Działające rozwiązanie technologiczne.	NASK		Efektem realizacji działania jest działający system wpierający analizę nielegalnych treści (obrazów) związanych z pornografią dziecięcą.		500 000 budżet państwa	P
2.3.3	Wypracowanie zdolności kształcenia i rozwoju wykwalifikowanego personelu dla prowadzenia zadań analitycznych	2.3.3.1 Zaawansowany program kształcenia (szkoleniowy) dla rozwoju kwalifikacji pracowników NASK prowadzących działania analityczne związane z bezpieczeństwem cyberprzestrzeni.	E	I 2018	VI 2020	Opracowany program kształcenia wraz z pozyskaniem wykładowców	NASK		Efektem realizacji działania jest przeprowadzenie min. 20 szkoleń podnoszących kwalifikacje pracowników oraz uzyskanie poświadczeń/ certyfikatów nabytych w ten sposób kompetencji (np. CISSP)	150 000 budżet państwa	600 000 budżet państwa	P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
2.3.4	Rozwijanie możliwości prowadzenia projektów badawczych w oparciu o dane pozyskane w ramach funkcjonowania krajowego systemu cyberbezpieczeństwa	Rozwijanie współpracy B+R z partnerami NC Cyber i zespołami CERT/CSIRT poziomu krajowego	O/T	III 2018	XII 2020	Realizacja wspólnie min 10 projektów organizacyjnych i/ lub technologicznych.	NASK	MC	Efektem realizacja działania ma być opracowanie założeń i zrealizowanie projektów badawczych wraz z partnerami NC Cyber i innymi interesariuszami Krajowego Systemu Cyberbezpieczeństwa.	100 000 budżet państwa	900 000 budżet państwa	P
Kierunek interwencji 2.4. Zbudowanie systemu bezpiecznej komunikacji na potrzeby bezpieczeństwa narodowego												
2.4.1	Zbudowanie spójnego systemu łączności jawnej i niejawnej całej administracji rządowej na potrzeby systemu kierowania bezpieczeństwem narodowym.	Wg. dokumentów wewnętrznych MON.	L	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	MON		Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.	Wg. dokumentów wewnętrznych MON.
Kierunek interwencji 2.5. Audyty i testy bezpieczeństwa												
2.5.1	Opracowanie spójnej metodyki audytów, na podstawie norm i dobrych praktyk oraz uwzględniając specyfiki poszczególnych sektorów	2.5.1.1 Opracowanie spójnej metodyki audytów, na podstawie norm i dobrych praktyk oraz uwzględniając specyfiki poszczególnych sektorów	O	I 2018	XII 2019	Opracowanie dokumentu metodyki audytu	MC	MON, ABW, NASK	1. Zapewnienia pokrycia całej przestrzeni audytowanego obszaru. 2. Zapewnienie porównywalności audytów przeprowadzanych w różnych instytucjach.	30 000 budżet państwa	90 000 budżet państwa	P
2.5.2	Opracowanie metodyki testów penetracyjnych.	2.5.2.1 Opracowanie metodyki testów penetracyjnych.	O	I 2018	XII 2019	Opracowanie dokumentu metodyki testów penetracyjnych	MC	MON, ABW, NASK	1. Zapewnienia pokrycia całej przestrzeni testowanego obszaru. 2. Zapewnienie porównywalności testów przeprowadzanych w różnych instytucjach .	30 000 budżet państwa	90 000 budżet państwa	P
2.5.3	Utworzenie repozytorium audytów i testów	2.5.3.1 Utworzenie repozytorium audytów i testów	T	I 2018	XII 2018	Oddanie repozytorium do eksploatacji	MC	NASK	Utworzona baza wiedzy pozwoli na podejmowanie całościowych działań o charakterze korekcyjnym i naprawczym.	90 000 budżet państwa		P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
2.5.4	Uregulowanie przygotowania i posiadania specjalistycznych narzędzi do prowadzenia testów penetracyjnych oraz ich prowadzenie.	2.5.4.1 Uregulowanie przygotowania i posiadania specjalistycznych narzędzi do prowadzenia testów penetracyjnych oraz ich prowadzenie.	L	IX 2017	VI 2018	Wprowadzenie regulacji	MC	pozostałe ministerstwa	Zapewnienie bezpieczeństwa prawnego dla podmiotów realizujących zadania z zakresu cyberbezpieczeństwa	w ramach działań statutowych mini-sterstw		R

CEL SZCZEGÓŁOWY KRPC: Cel szczegółowy 3. Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
Kierunek interwencji 3.1. Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa												
3.1.1	Uruchomienie programu Cyberpark Enigma.	3.1.1.1 Wypracowanie strategii dla uruchomienia produkcyjnej linii pilotażowej dla produktów z obszarów mikroelektroniki	O	XI 2017		Powołanie zespołu eksperckiego dla wypracowania strategii wyboru technologii oraz uruchomienia linii produkcyjnej dla produktów z dziedziny mikroelektroniki	MR	MON MC MSWiA MNiSW	1. Zapewnienie suwerenności Państwa w produkcji urządzeń z dziedziny mikroelektroniki na potrzeby kryptologii/Sił Zbrojnych RP 2. Zbudowanie polskich zdolności produkcyjnych w dziedzinie mikroelektroniki, jak i komercjalizacji wypracowanych rozwiązań 3. Powołanie programów rozwijających polskie zdolności w zakresie produktów i usług cyberbezpieczeństwa	60 000 000 budżet państwa		P
3.1.2	Uruchomienie hubów innowacyjności.	3.1.2.1 Budowa akceleratora branżowego w obszarze cyberbezpieczeństwa	O	III 2018		Stworzenie mechanizmu wsparcia MŚP działających w sektorze cyberbezpieczeństwa oraz ułatwienie współpracy MŚP z podmiotami państwowymi przy wypracowywaniu i wdrażaniu technologii	PARP	MR MC	1. Agregacja polskich podmiotów MŚP działających w obszarze cyberbezpieczeństwa; 2. Wypracowanie i wsparcie polskich technologii cyberbezpieczeństwa; 3. Wdrożenie polskich technologii cyberbezpieczeństwa w polskich podmiotach państwowych; 4. Wsparcie działań biznesowych polskich MŚP funkcjonujących na rynku ICT;			P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działani a
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
3.1.3	Budowa sieci laboratoriów na uczelniach / Powstanie Naukowego Klastra Cyberbezpieczeństwa (NKC)	3.1.3. 1 Utworzenie Centrum Mistrzostwa Informatycznego	O			Powołanie Centrum Mistrzostwa Informatycznego do koordynacji i organizacji warsztatów informatycznych w sieci szkół dedykowanych na terenie RP	MR	MC MNiSW MEN	Wzmocnienie polskiego potencjału intelektualnego w dziedzinie informatyki utrzymanie wysokiej pozycji Polski w prestiżowych konkursach informatycznych w kraju i za granicą.	. 1 300 000 budżet państwa		P
Kierunek interwencji 3.2. Zbudowanie mechanizmów współpracy między sektorem publicznym i prywatnym												
3.2.1	Rozbudowa systemów partnerskich w NC Cyber	3.2.1.1 Rozbudowa systemów partnerskich w NC Cyber	T/O	2018	2021	W pełni operacyjne systemy partnerskie NC Cyber	NASK		Wdrożenie technologii (systemów IT) i procedur współpracy dla systemów partnerskich NC Cyber (min. Strefa partnerów, Platforma Współpracy Analitycznej, Abuse Forum)	750 000 Ustawa budżetowa	2 000 000 . budżet państwa (NCBiR)	
3.2.2	Budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa.	3.2.2.1 Budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa.					MC		Organizowanie projektów B+R w sektorach / wśród Partnerów	NASK: 300 000 budżet państwa	NASK 1 500 000 budżet państwa (NCBiR)	
Kierunek interwencji 3.3. Stymulowanie badań i rozwoju w obszarze bezpieczeństwa systemów teleinformatycznych												
3.3.1	Uruchomienie w NCBiR programów badawczo-rozwojowych w obszarze cyberbezpieczeństwa / Przygotowanie projektów w ramach HORYZONT 2020	3.3.1.1 CyberSecIdent	O	V 2017	VI 2017	Uruchomienie programu	MC	NCBiR	Umożliwienie finansowania przedsięwzięć z zakresu cyberbezpieczeństwa	70 000 000 budżet państwa (uwaga – środki do wykorzystania w poszczególnych działaniach w perspektywie do roku 2023)		Z
		3.3.1.3 CEF-TC-2017-2: przygotowanie wniosku 1	O	VII 2017	IX 2017	Przygotowanie wniosku.	NASK		Efektem realizacji działania jest złożenie wniosku.	20 000 budżet państwa		Z

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
		3.3.1.4 CEF-TC-2017-2: przygotowanie wniosku 2	O	VII 2017	IX 2017	Przygotowanie wniosku.	NASK		Efektem realizacji działania jest złożenie wniosku.	20 000 budżet państwa		Z
		3.3.1..5 Przygotowanie wniosków w nowych wezwaniach H2020 lub innych programach KE	O	I 2018	XII 2021	Złożenie wniosków	NASK		Efektem realizacji działania jest złożenie 5 wniosków o środki z programów unijnych do realizacji zadań zdefiniowanych w przedmiotowym Planie Działań.	80 000 Budżet państwa	240 000 Budżet państwa	P
3.3.2	Doradztwo w zakresie określania kierunków badań	3.3.2.1 Udział przedstawicieli NASK w forach doradczych	O	I 2018	XII 2021	Udokumentowany udział w spotkaniach.	NASK		Efektem realizacji działania jest faktyczny udział przedstawicieli NASK w forach/organizacjach doradczych B+R (np. ECSO), sporządzone raporty wraz z rekomendacjami/wytycznymi w zakresie działań rozwojowych.	70 000 budżet państwa	200 000 budżet państwa	P
3.3.3	Opracowanie programów badawczych we współpracy ze środowiskiem naukowo-badawczym.	3.3.3.1 Opracowanie programów badawczych istotnych z punktu widzenia NASK	O	I 2018	XII 2020	Opracowane min. 4 programy badawcze	NASK		Efektem realizacji działania będą opracowane min. 4 programy badawcze we współpracy ze środowiskiem naukowo-badawczym. W ramach działania przewidywany jest udział w radach programowych i forach oraz praca merytoryczna przy opracowywaniu programów.	100 000 budżet państwa	300 000 budżet państwa	P
3.3.4	Opracowanie zadań w systemie zapewnienia cyberbezpieczeństwa dla organizacji pozarządowych.	3.3.4.1 Opracowanie wytycznych do konkursu na realizację zadania publicznego w zakresie podnoszenia kompetencji w obszarze cyberbezpieczeństwa	E	I 2018	XII 2020	Przyznanie dotacji organizacjom pozarządowym	MC		Efektem będą działania edukacyjne realizowane w ramach zadań publicznych przez organizacje pozarządowe. Działania te będą miały na celu propagowanie higieny cybernetycznej i podnoszenia świadomości zagrożeń. Działania te będą adresowane do ogółu społeczeństwa, JST oraz MŚP	1 000 000 budżet państwa	3 000 000 Budżet państwa	P
3.3.5	Uruchomienie naboru/programu pozyskania specjalistów o unikatowych umiejętnościach przez ośrodki analityczne na potrzeby rozwiązywania skomplikowanych problemów z zakresu cyberbezpieczeństwa	3.3.5.1 Program wymiany kadry między interesariuszami Krajowego Systemu Cyberbezpieczeństwa	O	I 2018	XII 2021	Przeprowadzone min. 8 wymian pracowników/ specjalistów między min. 4 interesariuszami	NASK		Efektem realizacji działania będzie min. 8 wymian pracowników pomiędzy interesariuszami KSC, co przyczyni się do podniesienia wśród pracowników.	50 000 budżet państwa	200 000 budżet państwa	P
Kierunek interwencji 3.4. Zwiększanie kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni												
		3.4.1.1 Programy szkoleniowe	O	I 2018	XII 2021	Przygotowane i przeprowadzone szkolenia	NASK		- Programy szkoleniowe przeznaczone dla różnych grup odbiorców: - dzieci i młodzieży, - nauczycieli - funkcjonariuszy organów ścigania - urzędników - innych grup ekspertów/profesjonalistów zajmujących się cyberbezpieczeństwem dzieci i młodzieży - Szkolenia eksperckie - specjalistyczne szkolenia kierowane do sektora biznesu, administracji publicznej oraz instytucji akademickich	200 000 budżet państwa	800 000 budżet państwa	P
		3.4.1.2 Organizacja wydarzeń związanych z cyberbezpieczeństwem	O	I 2007	XII 2021	Zorganizowanie wydarzeń	NASK		Efektem działania jest realizacja wydarzeń takich jak: - Dzień Bezpiecznego Internetu - Europejski Miesiąc Cyberbezpieczeństwa	100 000 budżet państwa	400 000 budżet państwa	R

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
3.4.1	Rozwój działań prowadzonych w ramach Akademii NASK	3.4.1.3 Akademia Cyfrowej Przyszłości	O	I 2018	XII 2021	Publikacja analiz i raportów, organizacja spotkań (debat, forów).	NASK		Efektem działania jest stworzenie środowiska eksperckiego oraz odpowiadanie na najbardziej aktualne zapotrzebowane ze strony społeczeństwa w obszarze reagowania i monitorowania ryzyka i zagrożeń dot. społecznych aspektów cyberbezpieczeństwa, w tym identyfikacja i diagnoza zjawisk społecznych związanych z używaniem nowoczesnych technologii komunikacyjnych.	100 000 budżet państwa	300 000 budżet państwa	P
		3.4.1.4 Telefoniczne Centrum Informacyjne	T/O	VI 2018	V 2020	Uruchomienie Telefonicznego Centrum Informacyjnego	NASK		Efektem działania jest utworzenie telefonicznego centrum informacyjnego i reagującego dla dorosłych oraz pomocowego dla dzieci i młodzieży ofiar cyberprzestępstw.	300 000 budżet państwa	1 500 000 budżet państwa	P
		3.4.1.5 Portal informacyjno-edukacyjny	T	IX 2018	VIII 2019	Uruchomienie portalu.	NASK		Efektem działania jest stworzenie portalu informacyjno-edukacyjnego dla szerokiego odbiorcy i poszczególnych grup społecznych stanowiącego platformę komunikacji i integracji działań dla instytucji i organizacji	100 000 budżet państwa	500 000 budżet państwa	P
3.4.2	Opracowanie i wdrożenie systemu obligatoryjnych, cyklicznych szkoleń i ćwiczeń kadr administracji państwowej na wszystkich szczeblach, dostosowanych do wykonywanych zadań	Opracowanie metodyki szkoleń i materiałów szkoleniowych, opracowanie założeń do przeprowadzenia ćwiczeń reagowania na ataki sieci i systemów teleinformatycznych kadr instytucji administracji państwowej. Prowadzenie cyklicznych ćwiczeń.	E	I 2018	XII 2022	Cykliczne ćwiczenia	MC	NASK	Celem ćwiczenia jest praktyczne sprawdzenie znajomości istniejących procedur reagowania na incydenty komputerowe w uczestniczących w ćwiczeniu podmiotach na wypadek możliwości wystąpienia realnych zagrożeń w cyberprzestrzeni wymagających uruchomienia odpowiednich procedur. Efektem będzie podniesienie świadomości kadr administracji publicznej.	300 000 Budżet państwa		P
3.4.3	Ustanowienie programu stypendialnego „Złota Setka”	Opracowanie koncepcji i przebiegu programu stypendialnego dla specjalistów z obszaru IT i bezpieczeństwa teleinformatycznego, zatrudnionych w administracji publicznej	O	III 2018	XII 2018	Wytyczne do uruchomienia programu	MC	MNiSW	Uruchomienie programu stypendialnego przyczyni się do zatrzymania w administracji publicznej pracowników o wysokich kompetencjach w obszarze cyberbezpieczeństwa, równolegle z wykorzystaniem innych instrumentów wspierających ich aktywność.	200 000 Budżet państwa		P
3.4.4	Opracowanie programów studiów dla szkół wyższych w specjalnościach z zakresu cyberbezpieczeństwa	Opracowanie wytycznych do efektów kształcenia na uczelniach wyższych nowych kadr w zakresie specjalności bezpieczeństwa teleinformatycznego	O	III 2018	XII 2018	Wytyczne do wprowadzenia zmian w efektach kształcenia	MC	MNiSW	Uruchamiania na studiach wyższych stadiów w obszarze bezpieczeństwa teleinformatycznego, odpowiadających na wymagania rynkowe w tym obszarze	300 000 Budżet państwa		P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
3.4.5	Ustanowienie nowych zawodów i specjalności w obszarze cyberbezpieczeństwa	3.4.5.1 Wprowadzenie do Klasyfikacji Zawodów i Specjalności nowych zawodów z zakresu cyberbezpieczeństwa	O	XI 2017	VI 2019	wprowadzenie do Klasyfikacji zawodów i specjalności nowych zawodów i specjalności w obszarze cyberbezpieczeństwa. Określenie nowych kwalifikacji zawodowych. Wprowadzenie na rynek nowych szkoleń i certyfikacji. Ujednolicenie wymagań i systemu certyfikacji.	MC	MRPiPS	Celem działania jest rozpoznanie potrzeb rynku/pracodawców odnoszących się do kompetencji pracowników zajmujących się problematyką bezpieczeństwa sieci i systemów teleinformatycznych, jak: zarządzanie bezpieczeństwem sieci, audytów bezpieczeństwa, testów penetracyjnych, analizy incydentów mających niekorzystny wpływ na cyberbezpieczeństwo organizacji, funkcjonowania zespołów reagowania na tego rodzaju incydenty itp. Ponadto działanie to ma celu rozpoznanie potrzeb uzupełniania i podnoszenia kwalifikacji pracowników poprzez różnego rodzaju formy dokształcania i certyfikacji umiejętności.	W ramach zadań statutowych ministerstw MC i MRPiPS	W ramach zadań statutowych ministerstw MC i MRPiPS	P
3.4.8	Opracowanie modelu zarządzania zasobami ludzkimi w obszarze cyberbezpieczeństwa.	3.4.8.1 Opracowanie koncepcji modelu zarządzania zasobami ludzkimi w obszarze cyberbezpieczeństwa (w ramach działania 1,2,3,1)	O	VI 2018	XII 2018	Dokument koncepcji	MC		Zapewnienie procesowego podejścia do zarządzania zasobami ludzkimi w obszarze cyberbezpieczeństwa	w budżecie działania 1.2.3.1		P
Kierunek interwencji 3.5. Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli												

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
3.5.1	Uwzględnienie tematyki bezpieczeństwa informacyjnego w programach nauczania szkół podstawowych i średnich. / Opracowanie wkładów do programu nauczania	3.5.1.1 Podkreślenie w przepisach ustawy Prawo oświatowe, że jednym z zadań systemu oświaty jest upowszechnianie wśród dzieci i młodzieży wiedzy o bezpieczeństwie oraz kształtowanie właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem z technologii informacyjno-komunikacyjnych. Zapis ten musi być brany pod uwagę w planowaniu i realizowaniu działań przez wszystkie podmioty działające w ramach systemu oświaty w Polsce.		IX 2017	VIII 2024	Zapis w przepisie prawa	MEN		Nabycie przez dzieci i młodzież wiedzy o bezpieczeństwie oraz właściwych postaw wobec zagrożeń związanych z korzystaniem z technologii informacyjno-komunikacyjnych.	plan finansowy MEN	plan finansowy MEN	R
		3.5.1.2 Opracowanie i wdrożenie nowej podstawy programowej kształcenia ogólnego dla wszystkich etapów edukacyjnych (określa ją Minister Edukacji Narodowej w rozporządzeniu). Nowa podstawa programowa edukacji informatycznej oraz informatyki rozszerza zapisy dotyczące bezpieczeństwa, o przestrzeganie prawa. Zapisy nowej podstawy odnoszą się do respektowania prywatności informacji, ochrony danych, praw własności intelektualnej oraz bezpiecznego poruszania się w cyberprzestrzeni. Oprócz treści nauczania, ww. dokument określa warunki i sposób realizacji tych treści, pozwalające na ich optymalne zrealizowanie.		IX 2017	VIII 2024	Dokument podstawy programowej	MEN		Nabycie przez dzieci i młodzież wiedzy o bezpieczeństwie oraz właściwych postaw wobec zagrożeń związanych z korzystaniem z technologii informacyjno-komunikacyjnych	plan finansowy MEN	plan finansowy MEN	R

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
		3.5.1.3 Przygotowanie poradników dla nauczycieli dotyczących realizacji treści nowej podstawy programowej zajęć informatycznych i informatyki, w tym w zakresie bezpieczeństwa informacyjnego. Opracowaniem materiałów zajmie się Ośrodek Rozwoju Edukacji (ORE) - publiczna placówka doskonalenia nauczycieli o zasięgu ogólnokrajowym prowadzona przez Ministra Edukacji Narodowej.		IX 2017	VIII 2024	Wydanie poradnika	MEN		Nabycie przez dzieci i młodzież wiedzy o bezpieczeństwie oraz właściwych postaw wobec zagrożeń związanych z korzystaniem z technologii informacyjno-komunikacyjnych	plan finansowy MEN	plan finansowy MEN	R

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
3.5.2	Opracowanie planu doskonalenia zawodowego nauczycieli odpowiedzialnych za nauczanie w zakresie bezpieczeństwa informacyjnego w szkołach.	3.5.2.1 Przygotowanie następujących materiałów, kursów i szkoleń dla nauczycieli i innych pracowników systemu oświaty. Opracowaniem materiałów zajmie się Ośrodek Rozwoju Edukacji (ORE) - publiczna placówka doskonalenia nauczycieli o zasięgu ogólnokrajowym prowadzona przez Ministra Edukacji Narodowej. a) Bezpieczne funkcjonowanie w mediach społecznościowych (bezpłatny materiał edukacyjny oraz szkolenie). Cel: przygotowanie uczestników do wspierania n-li w zakresie wykorzystywania mediów społecznościowych w procesie dydaktycznym i wychowawczym oraz kształtowania u uczniów kompetencji odpowiedzialnego korzystania z mediów społecznościowych. b) Cyfrowe portfolio - bezpieczeństwo w komunikacji i w mediach (kurs e-learningowy). Cele: kształtowanie postaw poprzez: – podnoszenie kompetencji w zakresie bezpiecznego korzystania z mediów, w tym kształtowanie postaw i wychowanie do wartości, – kształtowanie postaw etycznych i i promowanie wartości w komunikacji i w mediach. c) Opracowanie ramowego programu szkolenia dla nauczycieli odpowiedzialnych za nauczanie w zakresie bezpieczeństwa informacyjnego w szkołach (bezpłatna publikacja). Cel: - przygotowanie pracowników ośrodków doskonalenia nauczycieli do prowadzenia szkoleń nauczycieli odpowiedzialnych za nauczanie w zakresie bezpieczeństwa informacyjnego w szkołach.		I 2018	XII 2018	Wydanie materiałów szkoleniowych	MEN		Nabycie oraz rozwinięcie przez nauczycieli i innych pracowników systemu oświaty kompetencji umożliwiających optymalne realizowanie treści w zakresie bezpieczeństwa informacyjnego.	Realizowane są w ramach środków przeznaczonych na oświatę i wychowanie i nie wymagają dodatkowego finansowania.		P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
3.5.3	Opracowanie i realizacja planu podnoszenia świadomości społecznej w obszarze cyberbezpieczeństwa; prewencja cyberprzestępczości; koordynacja inicjatyw/kampanii społecznych podejmowanych przez poszczególne instytucje, organizacje pozarządowe, sektor prywatny.	3.5.3.1 Popularyzacja informacji na temat cyberbezpieczeństwa	O	IX 2017	XII 2021	Regularna publikacja informacji.	NASK		Lokalizacja kampanii STOP.THINK.CONNECT Utrzymanie i rozwój materiałów STOP.THINK.CONNECT Tłumaczenie i dystrybucja biuletynów OUCH	50 000 Budżet państwa	200 000 budżet państwa	R

CEL SZCZEGÓŁOWY KRPC: Cel szczegółowy 4. Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
Kierunek interwencji 4.1. Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym												
4.1.3	Przeprowadzenie kampanii na rzecz uzyskania miejsca w kolejnej Grupie Ekspertów Rządowych ds. cyberbezpieczeństwa (w przypadku decyzji ZO ONZ o powołaniu w grupy w kolejnych latach).	4.1.3.1 Przeprowadzenie kampanii na rzecz uzyskania miejsca w kolejnej Grupie Ekspertów Rządowych ds. cyberbezpieczeństwa (w przypadku decyzji ZO ONZ o powołaniu w grupy w kolejnych latach).	P	IX 2017	VI 2019	Wzmocnienie pozycji Polski i uzyskanie miejsca w grupie	MSZ	MC, MON, BBN	Uzyskanie wpływu na przebieg globalnej dyskusji nt. cyberbezpieczeństwa poprzez udział w pracach kolejnej Grupy Ekspertów Rządowych ONZ lub innego organu powołanego na jej miejsce	20 000 budżet państwa		P
		4.1.3.2 Przeprowadzenie konsultacji nt. cyberbezpieczeństwa w gronie przedstawicieli MSZ-ów państw Europy Środkowej i Wschodniej na marginesie jednej z dużych imprez międzynarodowych organizowanych w Polsce	P	IX 2018	IX 2018	Raport z konsultacji	MSZ	MC, MON, BBN	Wzmocnienie pozycji regionalnego lidera w zakresie międzynarodowych aspektów cyberbezpieczeństwa	10 000 budżet państwa		P
4.1.8	Prowadzenie przez NASK/NC Cyber współpracy z ENISĄ	4.1.8.1 dział NASK w działaniach ENISA	O	I 2004	XII 2021	Regularny udział w działaniach	NASK	MC	Efektem realizacji działania będzie udział kadry zarządzającej oraz ekspertów w działaniach Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA).	40 000 budżet państwa	160 000 budżet państwa	R

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
4.1.9	Budowanie w NC Cyber zdolności w zakresie wsparcia analitycznego dla administracji publicznej w obszarze strategicznym (policy).	4.1.9.1 Treść dla serwisu CyberPolicy	I	I 2018	XII 2021	Regularna publikacja treści	NASK		Efektem realizacji działania będzie regularna publikacja treści, którymi będą wszystkie informacje strategiczne z dziedziny cyberbezpieczeństwa, opracowywane i procedowane na szczeblu krajowym, unijnym i globalnym. (powiązane z 1.2.5)	100 000 budżet państwa	400 000 budżet państwa	P
		4.1.9.2 Biuletyn CyberPolicy	O	I 2018	XII 2021	Regularna publikacja biuletynu	NASK		Efektem realizacji działania będzie regularne (proponowany cykl to kwartał) publikowanie biuletynu zawierającego istotne informacje regulacyjne, czy strategiczne, ale też dobre praktyki i analizy istotne dla sektorów w tym administracji państwowej.	40 000 budżet państwa	120 000 budżet państwa	P
		4.1.9.3 Działanie centrum analiz strategicznych w NC Cyber	O	I 2018	XII 2021	Funkcjonujący zespół analiz strategicznych	NASK		Efektem realizacji działania jest funkcjonowanie zespołu analiz strategicznych w NC Cyber, którego zadaniami są regularne analizy dokumentów strategicznych, konsultacje na szczeblu krajowym i międzynarodowym, opracowywanie wkładów do oficjalnych stanowisk.	100 000 budżet państwa	350 000 budżet państwa	P
4.1.12	Opracowanie planu i prowadzenie nadzoru nad kampaniami promującymi Polskę i polskich przedsiębiorców	4.1.12.1 Kampania 1	I/P	IV kwartał 2017 r.	IV kwartał 2017 r.	Przeprowadzenie kampanii	MR	PAIH	Efektem kampanii będzie: • zwiększenie świadomości marki Polska wśród przedsiębiorców i społeczeństwa, • aktywniejsze wchodzenie polskich firm na rynki zagraniczne, • pobudzenie eksportu, • ostatecznie: wzmocnienie pozytywnego wizerunku polskiej gospodarki na arenie międzynarodowej. Ponadto, spodziewane jest zwiększenie liczby wejść na stronę Portalu Promocji Eksportu: www.trade.gov.pl	2 000 000 w 2017 r. projekt 3.3.2 PO IR		P
		4.1.12.2 Kampania 2	I/P	IV kwartał 2018 r.	IV kwartał 2018 r.	Przeprowadzenie kampanii	MR	PAIH		1 900 000 projekt 3.3.2 PO IR		P
		4.1.12.3 Kampania 3	I/P	IV kwartał 2019 r.	IV kwartał 2019 r.	Przeprowadzenie kampanii	MR	PAIH			1 900 000 projekt 3.3.2 PO IR	P
Kierunek interwencji 4.2. Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym												
4.2.1	Opracowanie i promowanie polskiego modelu współpracy w ramach sieci wymiany informacji.	4.2.1.1 Zorganizowanie warsztatów, wizyt studyjnych i eksperckich dla partnerów z Ukrainy	E/I/P	I 2017	XII 2018	Dokument podsumowujący działanie	MC	NASK	Włączanie problematyki cyberbezpieczeństwa do agendy konsultacji w ramach współpracy dwustronnej oraz organizacja odrębnych dwustronnych konsultacji z zakresu cyberbezpieczeństwa z wybranymi sojusznikami i partnerami.	100 000 budżet państwa z opcją pozyskania środków UE		R
		4.2.1.2 Zorganizowanie warsztatów, wizyt studyjnych eksperckich dla partnerów z Gruzji	E/I/P	II 2018	XII 2018	Dokument podsumowujący działanie	MC	NASK	Włączanie problematyki cyberbezpieczeństwa do agendy konsultacji w ramach współpracy dwustronnej oraz organizacja odrębnych dwustronnych konsultacji z zakresu cyberbezpieczeństwa z wybranymi sojusznikami i partnerami.	100 000 budżet państwa z opcją pozyskania środków UE		P

Nr zadania	Opis zadania	Opis działania	Typ działania	Harmonogram		Forma zakończenia działania	Organ/Organy		Oczekiwane efekty	Szacunkowy koszt realizacji [PLN] lata 2017 i 2018 Źródło finansowania	Szacunkowy koszt realizacji [PLN] (lata 2019-2022) Źródło finansowania	stan wdrażania działania
				Termin rozpoczęcia	Termin zakończenia		wiodący	współpracujący				
4.2.2	Budowa sieci wymiany informacji o zagrożeniach i współpraca na poziomie technicznym/operacyjnym z siecią CERT/CSIRT P.Cz. UE	4.2.2.1 Opracowanie koncepcji Budowa sieci wymiany informacji o zagrożeniach i współpraca na poziomie technicznym/operacyjnym z siecią CERT/CSIRT P.Cz. UE	O	VI 2018	XII 2018	Dokument koncepcji	MC	NASK	Umożliwienie efektywnej współpracy w sieci CSIRT UE	50 000 budżet państwa		P
4.2.6	Udział CERT Polska w międzynarodowych ćwiczeniach z zakresu cyberbezpieczeństwa	4.2.6.1 Przygotowania i udział zespołu CERT Polska w międzynarodowych ćwiczeniach	O	VI 2017	XII 2022	Aktywny udział w ćwiczeniach	NASK		Udział CERT Polska (w ramach 1.3.3)	W ramach 1.3.3	W ramach 1.3.3	R
4.2.7	Współpraca z ENISA	4.2.7.1 Udział ekspertów NASK w pracach ENISA	O	I 2018	XII 2022	Raport z prac za dany okres.	NASK		Efektem realizacji zadania jest współpraca ekspertów NASK z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji na poziomie techniczno-operacyjnym. Udział w organizowanych dyskusjach, wymianie informacji, warsztatach.	40 000 budżet państwa	160 000 budżet państwa	P
4.2.8	Współpraca CERT Polska z innymi zespołami CERT, udział w projektach i konferencjach	4.2.8.1 Aktywna współpraca z zespołami CERT/CSIRT i udział w projektach i konferencjach organizowanych przez organizacje zrzeszające zespoły reagujące	O/P	I 2005	XII 2022	Sprawozdanie.	NASK		Efektem działania będzie aktywna współpraca operacyjna z zespołami CSIRT oraz uczestniczenie w projektach i konferencjach organizacji zrzeszających zespoły reagujące (FIRST, TF CSIRT, NomoreRansome.ORG, APWG i innych)	200 000 budżet państwa	700 000 budżet państwa	R
		4.2.8.2 Projekt CyberExchange	O	VI 2018	V 2020	Zrealizowanie założeń projektu.	NASK		Efektem realizacji projektu będzie przeprowadzenie zakładanej liczby wymian pracowników pomiędzy 10 europejskimi zespołami CERT.	60 000 KE	180 000 KE	P
4.2.9	Udział CERT Polska w sieci CSIRT powołanej na mocy dyrektywy NIS	4.2.9.1 Udział CERT Polska w CSIRT Network	O	I 2017	XII 2022	Sprawozdania roczne.	NASK		Efektem realizacji działania jest aktywny udział ekspertów CERT Polska w spotkaniach, inicjatywach, wymianie informacji w ramach sieci CSIRT Network powołanej na mocy dyrektywy NIS.	40 000 budżet państwa	150 000 budżet państwa	R

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.