

OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Centrum Cyberbezpieczeństwa NASK (CCN)		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB)		
Partnerzy	nie dotyczy		
Źródło finansowania	Budżet państwa: część 27 - Informatyzacja Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie FERC 02.02: Wzmocnienie krajowego systemu cyberbezpieczeństwa		
Całkowity koszt projektu	361 874 675,57 zł		
Planowany okres realizacji projektu	10-2023 do 12-2029		
Osoba kontaktowa	Agnieszka Suchodolska	agnieszka.suchodolska@nas k.pl	538895987

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Projekt CCN jest odpowiedzią na szybko rosnący poziom zagrożeń polskiego Internetu i związane z nimi straty gospodarcze będące bezpośrednio lub pośrednio wynikiem cyberprzestępstw. Od kilku lat obserwuje się szybki wzrost zagrożeń cyberprzestrzeni. „Roczny Raport działalności CERT Polska. Krajobraz bezpieczeństwa polskiego Internetu”, wskazuje, że w 2024 roku zespół CSIRT NASK zanotował 600 990 zgłoszeń, które zostały przeanalizowane. Na ich podstawie zarejestrowano 103 449 incydentów bezpieczeństwa, które miały lub mogły mieć niekorzystny wpływ na cyberbezpieczeństwo. Liczba zgłoszeń w 2024 roku w porównaniu z rokiem 2023 wzrosła o 62%. Wzrost ten, wpisuje się w globalne trendy opisane w aktualnym (za rok 2024) raporcie Agencji ENISA „ENISA Threat Landscape”. ONZ szacuje, że globalny poziom strat gospodarczych przekroczy w 2025 r. 10,5 bln €. Uczyni to cyberprzestępczość najbardziej zyskownym biznesem w historii ludzkości.

Projekt CCN jest projektem inwestycyjno-budowlanym z elementami projektu infrastrukturalnego. Dokumentacja projektowa uwzględnia zapisy dot. problemów i potrzeb. Dodatkowo projekt jest realizowany od roku 2023 na podstawie zaakceptowanego przez CPPC oraz Komitet monitorujący FERC Wniosku o dofinansowanie i Studium Wykonalności.

Projekt CCN uzyskał dofinansowanie w wysokości 310 mln zł (umowa FERC.02.02-IP.01-0002/23-00 z 31.10.2023 r). Niniejszy OZPI jest składany w związku z koniecznością zwiększenia zakresu finansowania projektu CCN. Przygotowany przez Biuro Projektowe (Projmors sp. z o.o.) i zweryfikowany przez Inżyniera Kontraktu (Ekocentrum sp. z o.o.) Projekt Architektoniczno-Budowlany CCN, wskazuje że koszt robót budowlanych i wyposażeniowych obiektu CCN, oraz kosztów dostosowania terenu nieruchomości, będzie wyższy niż zakładano pierwotnie (w 2023 roku) o około 51,87 mln zł.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
---------------	-------------------------	--------------------------

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
NASK-PIB (beneficjent)	<ul style="list-style-type: none"> - Ograniczone możliwości zapewnienia sprawnej i skutecznej współpracy jednostek odpowiedzialnych za funkcjonowanie Krajowego Systemu Cyberbezpieczeństwa (CSIRT'ów poziomu krajowego i ministra właściwego ds. informatyzacji) w ramach tzw. Połączonego Centrum Operacyjnego Cyberbezpieczeństwa, w świetle szybko rosnącej fali cyberzagrożeń; - Niedostateczne warunki techniczne i organizacyjne konieczne dla uruchomienia Krajowego Systemu Certyfikacji Cyberbezpieczeństwa (patrz ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa z 28.07.2025 r Dz.U. 1017 z 2025 r); - Niedostateczne zaplecze CSIRT NASK niezbędne do oceny bezpieczeństwa rozwiązań IT w szczególności do testowania ich metodą fuzzingu, badania złośliwego oprogramowania i oceny bezpieczeństwa rozwiązań AI; - Rosnąca liczba, coraz bardziej wyrafinowanych cyberataków, związanych z niszczeniem / kradzieżą danych; - Brak zaplecza pozwalającego na organizację i prowadzenie szeroko zakrojonych kampanii szkoleniowo-informacyjnych w zakresie cyberbezpieczeństwa nakierowanych na różne grupy odbiorców, w tym szkoleń certyfikacyjnych; - Niedostateczne zaplecze techniczne do wsparcia Jednostek Samorządu Terytorialnego w obliczu narastającej fali cyberzagrożeń. 	1
Operatorzy Usług Kluczowych (OUK)	<ul style="list-style-type: none"> - Problemy z zapewnieniem ciągłości funkcjonowania OUK po skutecznym ataku, w którym zniszczeniu uległy dane w formie cyfrowej (w szczególności problemy z szybkim i skutecznym odtworzeniem danych); - Niedostateczne możliwości ustawicznego podnoszenia kompetencji personelu OUK w obszarze cyberbezpieczeństwa i brak dedykowanych im programów szkoleń specjalistycznych. 	385
Dostawcy Usług Cyfrowych (DUC)	<ul style="list-style-type: none"> - Problemy z zapewnieniem ciągłości działania DUC po skutecznym ataku, w którym zniszczeniu uległy dane w formie cyfrowej (w szczególności problemy z szybkim i skutecznym odtworzeniem danych); 	1500

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	<ul style="list-style-type: none"> - Brak narzędzi, procedur i reguł umożliwiających skuteczne dbanie o cyberbezpieczeństwo rozwiązań bazujących na AI; - Brak systemowego podnoszenia kompetencji personelu DUC w obszarze cyberbezpieczeństwa i dedykowanych im programów szkoleń. 	
Jednostki samorządu terytorialnego	<ul style="list-style-type: none"> - Niedostateczne kompetencje personelu JST w obszarze cyberbezpieczeństwa i brak dedykowanych im programów szkoleniowych; - Problemy z zapewnieniem ciągłości usług JST po skutecznym ataku, w którym zniszczeniu uległy dane w formie cyfrowej (w szczególności problemy z szybkim i skutecznym odtworzeniem danych); - Brak zdolności JST do podejmowania skutecznych działań zapobiegawczych przed wystąpieniem potencjalnych incydentów oraz sprawnego i skutecznego reagowania na nie. 	2809
Minister właściwy ds. informatyzacji (wnioskodawca)	<ul style="list-style-type: none"> - Wynikająca z ustawy o KSC konieczność zapewnienia skutecznej współpracy jednostek Krajowego Systemu Cyberbezpieczeństwa (CSIRT'ów poziomu krajowego i nadzorującego ich ministra właściwego ds. informatyzacji), w szczególności wdrożenia procedur i rozwiązań pozwalających na sprawną, bezpieczną i niezawodną wymianę informacji; - Wynikająca z ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz.U. 1017 z 2025 r) konieczność uruchomienia procesu oceny bezpieczeństwa rozwiązań teleinformatycznych i uruchomienia Krajowego Systemu Certyfikacji Cyberbezpieczeństwa; - Wynikająca z ustawy o KSC konieczność organizowania przez pełnomocnika ds. cyberbezpieczeństwa, intensywnych kampanii szkoleniowo-informacyjnych w zakresie cyberbezpieczeństwa, nakierowanych na różne grupy interesariuszy. 	1
CSIRT'y poziomu krajowego (poza CSIRT NASK)	<ul style="list-style-type: none"> - Niedostateczna jakość (skuteczność) obecnie stosowanych narzędzi współpracy jednostek odpowiedzialnych za funkcjonowanie Krajowego Systemu Cyberbezpieczeństwa (CSIRT'ów poziomu krajowego i nadzorującego ich ministra właściwego ds. informatyzacji), w kontekście lawinowo narastającej fali cyberataków 	2

1.2. Opis stanu obecnego

Ustawa o krajowym systemie cyberbezpieczeństwa (Dz.U. 2023 poz. 913) wyznacza trzy tzw. CSIRT poziomu krajowego (Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego działające na poziomie krajowym). Kluczową rolę odgrywa CSIRT-NASK, który odpowiada za funkcjonowanie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), koordynuje incydenty zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych i samorząd terytorialny. Do CSIRT NASK incydenty mogą także zgłaszać osoby fizyczne – obywatele.

CSIRT NASK funkcjonuje obecnie w przestrzeni biurowej budynku NASK-PIB przy ul. Kolskiej 20. Do obsługi zgłoszeń wykorzystywany jest specjalistyczny, wydzielony, wewnętrzny System Zgłoszeń CSIRT NASK.

Analiza przeprowadzona przez NASK-PIB, wskazuje że aktywne i efektywne przeciwdziałanie rosnącej fali cyberzagrożeń przez CSIRT NASK (w szczególności realizacja nowych wymagań nakładanych dyrektywą NIS2), wymaga znaczących inwestycji, wykraczających poza prosty rozwój lub bardziej optymalne wykorzystanie obecnych zasobów NASK-PIB. Głównym czynnikiem blokującym i niezbędnym dla rozwoju CSIRT NASK, są bowiem obecne uwarunkowania lokalowe i infrastrukturalne NASK PIB.

Istotą projektu CCN jest dlatego utworzenie jakościowo nowego Centrum Cyberbezpieczeństwa NASK (CCN). Projekt CCN jest projektem inwestycyjno-budowlanym z elementami projektu infrastrukturalnego. Dokumentacja projektowa uwzględnia uwarunkowania dot. infrastruktury i obecnej realizacji zadań. Projekt jest realizowany od roku 2023 na podstawie zaakceptowanego przez CPPC oraz Komitet monitorujący FERC Wniosku o dofinansowanie i Studium Wykonalności (umowa FERC.02.02IP.01-0002/23-00 z 31.10.2023 r).

2. EFEKTY PROJEKTU

2.1. Cele i korzyści wynikające z projektu

Cel - 1	Zwiększenie zdolności do reagowania na incydenty w systemach informacyjnych państwa oraz podmiotach mających kluczowe znaczenie dla gospodarki przez CSIRT-NASK
Cel strategiczny	Cel strategiczny FERC (RS01.2): Czerpanie korzyści z cyfryzacji dla obywateli, przedsiębiorstw, organizacji badawczych i instytucji publicznych
Korzyść:	Wzmocnienie krajowego systemu cyberbezpieczeństwa, poprzez utworzenie Centrum Cyberbezpieczeństwa NASK (CCN), na które złożą się jakościowo nowe specjalistyczne centra, ośrodki i laboratoria a w konsekwencji ograniczenie strat społeczno-gospodarczych z tytułu cyberprzestępstw.
KPI:	KPI 1) Liczba zdarzeń obsługiwanych przez CSIRT NASK (Computer Security Incident Response Team) KPI 2) Liczba wspartych podmiotów, dla których obsługa incydentów koordynowana jest przez CSIRT NASK (Computer Security Incident Response Team)
Wartość aktualna i docelowa KPI:	KPI 1) Wartość aktualna: 0 KPI 2) Wartość aktualna: 0 KPI 1) Wartość docelowa: 50 000 KPI 2) Wartość docelowa: 300
Metoda pomiaru KPI	1 i 2: Dane nt. liczby obsługiwanych zdarzeń oraz wspartych podmiotów z systemu ewidencjonowania zgłoszeń CSIRT NASK (CSIRT RT). Dane w systemie CSIRT RT są rejestrowane na bieżąco, w sposób ciągły. Wartość

	docelowa wskaźników zostanie określona w momencie zakończenia rzeczowej realizacji projektu.
Cel - 2	Wzmocnienie odporności i zdolności CSIRT-NASK do skutecznego przeciwdziałania cyberzagrożeniom w systemach informacyjnych państwa oraz podmiotach mających kluczowe znaczenie dla gospodarki
Cel strategiczny	Cel strategiczny FERC (RS01.2): Czerpanie korzyści z cyfryzacji dla obywateli, przedsiębiorstw, organizacji badawczych i instytucji publicznych.
Korzyść:	Wzmocnienie krajowego systemu cyberbezpieczeństwa poprzez utworzenie Centrum Cyberbezpieczeństwa NASK (CCN), na które złożą się jakościowo nowe specjalistyczne centra, ośrodki i laboratoria, a w konsekwencji ograniczenie strat społeczno-gospodarczych z tytułu cyberprzestępstw.
KPI:	KPI 3) Liczba osób objętych działaniami edukacyjnymi z grup docelowych w ramach ośrodka treningowo – szkoleniowego w obszarze cyberbezpieczeństwa CCN (OSC).
Wartość aktualna i docelowa KPI:	KPI 3): Wartość aktualna: 0 KPI 3): Wartość docelowa: 50 000
Metoda pomiaru KPI	Lista obecności szkoleń stacjonarnych / raport z platformy webinarowej / raport z platformy e-learningowej (w zależności od formy szkolenia). Dane nt. uczestników są rejestrowane na bieżąco. Wartość docelowa wskaźnika zostanie określona w momencie zakończenia rzeczowej realizacji projektu.

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
Budynek Centrum Cyberbezpieczeństwa NASK stworzony wg zasady security-by-design zapewniające warunki do skutecznej realizacji zadań przez CSIRT-NASK.	09-2029
Stworzenie systemowych rozwiązań dla zapewnienia ciągłości funkcjonowania podmiotów po skutecznym ataku, w którym zniszczeniu	09-2029

Nazwa produktu	Planowana data wdrożenia
uległy dane w formie cyfrowej (Krajowe Centrum Odzyskiwania Danych).	
Stworzenie systemowych warunków współpracy pomiędzy CSIRT poziomu krajowego oraz wdrożenie procedur i rozwiązań pozwalających na bezpieczną współpracę i wymianę informacji między interesariuszami i dzielenie się wiedzą co do podatności, zagrożeń i incydentów (Krajowe Centrum Operacyjne Cyberbezpieczeństwa).	09-2029
Stworzenie systemowych warunków i modelowych rozwiązań umożliwiających ustawiczne podnoszenie kompetencji w obszarze cyberbezpieczeństwa (Modelowy Ośrodek treningowo – Szkoleniowy w obszarze Cyberbezpieczeństwa).	09-2029
Implementacja narzędzi, procedur i reguł dbania o cyberbezpieczeństwo rozwiązań AI (Laboratorium Bezpieczeństwa AI).	09-2029
Stworzenie systemowych warunków niezbędnych do rozwoju Krajowego Systemu Certyfikacji Cyberbezpieczeństwa (Ośrodek Modelowania Certyfikacji Cyberbezpieczeństwa).	09-2029
Stworzenie systemowych warunków badania projektów metodą fuzzingu oraz badania złośliwego oprogramowania i bezpiecznego współdzielenia wyników tych badań (Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania).	09-2029
Stworzenie systemowych warunków dla wsparcia zdolności JST do podejmowania skutecznych działań zapobiegawczych przed wystąpieniem potencjalnych incydentów oraz skutecznego reagowania na nie (Krajowe Centrum Wsparcia Security dla JST).	09-2029
Zapewnienie sprawności i skuteczności działania CSIRT NASK poprzez rozbudowę środowiska sieciowego, infrastruktury serwerowej i infrastruktury bezpieczeństwa NASK PIB.	09-2029

3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Pozyskana nieruchomość na cele CCN	2024-10-31
Podpisana umowa z Biurem Projektowym .	2025-01-31
Podpisana umowa z Inżynierem Kontraktu	2025-06-30
Uzyskane pozwolenie na budowę	2026-06-30
Rozpoczęcie funkcjonowania OMCC	2026-12-31
Podpisana umowa z Wykonawcą Robót Budowlanych	2026-12-31
Uruchomienie laboratorium AITAS	2026-12-31
Gotowa infrastruktura wspólna NASK-PIB	2027-06-30
Budynek CCN - uzyskane pozwolenia na użytkowanie	2028-12-31

Kamienie milowe	Planowany termin osiągnięcia
Gotowość OSC do realizacji szkoleń	2028-12-31
Uruchomione laboratorium KCOD w docelowej lokalizacji	2029-03-31
Uruchomione KCOC w docelowej lokalizacji	2029-03-31
Uruchomione laboratorium FUMAL w docelowej lokalizacji	2029-03-31
Uruchomione laboratorium KCWS JST w docelowej lokalizacji	2029-03-31
Zakończona rzeczowa realizacja projektu	2029-09-30

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

Całkowity koszt projektu (netto oraz brutto), w tym	Netto 272 531 238,43 zł Brutto 361 874 675,57 zł	
Procent dofinansowania ze środków UE (brutto)	65,85%	
Procent środków z budżetu państwa (brutto)	34,15%	
Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto)	2023	Netto 30 631,56 zł Brutto 45 172,63 zł
	2024	Netto 6 590 125,65 zł Brutto 9 036 229,87 zł
	2025	Netto 9 116 459,56 zł Brutto 12 401 684,57 zł
	2026	Netto 62 504 786,81 zł Brutto 83 324 533,63 zł
	2027	Netto 91 183 028,18 zł Brutto 120 408 410,44 zł
	2028	Netto 76 232 150,05 zł Brutto 100 621 751,77 zł
	2029	Netto 26 874 056,62 zł Brutto 36 036 892,66 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej	Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
-------------------------	---------------------------	--

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Koszt wartości niematerialnych i prawnych (w szczególności licencji oprogramowania specjalistycznego) niezbędnego dla stworzenia i funkcjonowania CCN	30 240 516,23 zł	Zakupy oprogramowania specjalistycznego niezbędnego dla stworzenia i funkcjonowania CCN m.in. oprogramowania do analizy danych, do klasyfikacji treści, do analizy zdarzeń w Sieci, platformy e-learningu, oprogramowania do obsługi szkoleń i e-learningu itd.
Infrastruktura	a) Zakupy środków trwałych oraz materiałów niezbędnych dla stworzenia i funkcjonowania CCN; b) Koszty robót budowlanych związanych ze stworzeniem i wyposażeniem budynku CCN; c) Usługi zewnętrzne wynikające z procesu inwestycyjnego przy realizacji projektów budowlanych.	253 153 544,75 zł	a) zakup sprzętu i materiałów (wraz z oprogramowaniem systemowym i narzędziowym) niezbędnego dla stworzenia i funkcjonowania CCN m.in. serwerów i macierzy z wyposażeniem, urządzeń do wykonywania kopii bezpieczeństwa, specjalistycznego sprzętu do laboratoriów CCN, wyposażenia symulacyjnego, sprzętu stanowiskowego, urządzeń audio-video, urządzeń sieciowych i bezpieczeństwa oraz mobilnych laboratoriów teleinformatycznych; b) koszty robót budowlanych związanych ze stworzeniem i wyposażeniem budynku CCN oraz koszty zagospodarowania nieruchomości; c) koszty usług zewnętrznych związanych z procesem inwestycyjnym.
Koszty UX i grafiki	nie dotyczy	0,00 zł	Projekt nie obejmuje tworzenia rozwiązań teleinformatycznych związanych z e-usługami publicznymi lub udostępnianiem danych.
Bezpieczeństwo	nie dotyczy	0,00 zł	Projekt nie obejmuje tworzenia rozwiązań teleinformatycznych związanych z e-usługami publicznymi lub udostępnianiem danych.
Wydajność rozwiązań	nie dotyczy	0,00 zł	Projekt nie obejmuje tworzenia rozwiązań teleinformatycznych związanych z e-usługami

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
			publicznymi lub udostępnianiem danych.
Szkolenia	Szkolenia personelu CCN, podnoszenie kompetencji w obszarze cyberbezpieczeństwa oraz przygotowanie systemu szkoleń.	6 389 500,40 zł	Szkolenia personelu CCN, podnoszenie kompetencji w obszarze cyberbezpieczeństwa, wdrożenie platformy e-learningu oraz zarządzania szkoleniami wraz z przygotowaniem treści cyfrowych.
Działania informacyjno-promocyjne	Działania informacyjno-promocyjne związane z projektem CCN.	580 349,70 zł	Działania związane z promocją projektem CCN wynikające z opracowanego planu informacyjno-promocyjnego.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Koszty osobowe obejmujące wszystkie działania realizowane przez personel projektu zgodnie z zatwierdzoną strukturą projektową.	71 510 764,49 zł	Koszty osobowe personelu projektu w tym: personel merytoryczny, zarządzanie i wsparcie projektu CCN.

4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania (okres 5 lat)

Całkowity koszt utrzymania trwałości projektu (brutto)	225 619 498,93 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto)	2030	42 477 249,00 zł (brutto) (30 203 371,00 zł netto)	krajowe środki publiczne - budżet państwa
	2031	43 733 656,88 zł (brutto) (31 108 249,49 zł netto)	krajowe środki publiczne - budżet państwa
	2032	45 030 266,64 zł (brutto) (32 042 415,07 zł netto)	krajowe środki publiczne - budżet państwa
	2033	46 365 680,01 zł (brutto) (33 004 995,90 zł netto)	krajowe środki publiczne - budżet państwa

	2034	48 012 646,40 zł (brutto) (34 205 698,28 zł netto)	krajowe środki publiczne - budżet państwa
--	------	---	---

4.4. Planowane koszty ogólne realizacji (w przypadku projektu współfinansowanego – wkład krajowy z budżetu państwa) oraz koszty utrzymania projektu:

- zostaną pokryte w ramach budżetów odpowiednich dysponentów części budżetowych bez konieczności występowania o dodatkowe środki z budżetu państwa
- ~~- będą powodować konieczność przyznania dodatkowych kwot~~

5. GŁÓWNE RYZYKA

5.1. Ryzyka wpływające na realizację projektu

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Nieuwzględnienie wszystkich potrzeb/wymagań, zakresów związanych z budynkiem CCN w zakładanym budżecie projektu.	Średnia	Wysokie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Szczegółowa analiza i weryfikacja zgłaszanych potrzeb pod kątem ich kluczowego znaczenia dla projektu, spełnienia zapisów SW i WoD, wskaźników. W przypadku konieczności zwiększenia budżetu wystąpienie z wnioskiem o zmianę do CPPC.
Roszczenia Wykonawców w trakcie realizacji umów.	Średnia	Średnie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Staranne i wnikliwe opracowywanie umów i dokumentacji. Cała dokumentacja projektowa oraz zapisy w OPZ, SWZ i Umowach powinny być wykonane w taki sposób, aby dawały Wykonawcy jak najmniejszą możliwość do przedkładania roszczeń.
Nieplanowane ewentualne koszty związane ze zmianami w infrastrukturze CSIRT oraz wydłużony czas potrzebny na adaptację pomieszczenia magazynowego na serwerownię	Mała	Wysokie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Stały monitoring Kierownika operacyjnego oraz Lidera biznesowego, ewentualny wzrost kosztów będzie eskalowany na poziom Komitetu Sterującego.

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
na poziomie -1 budynku NASK-PIB.			
Brak odpowiednio wysokiego priorytetu realizacyjnego dla zadań w ramach projektu CCN.	Średnia	Średnie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Systematyczny przegląd najważniejszych działań projektowych oraz nadanie wysokiego priorytetu realizacyjnego przez Liderów biznesowych oraz Sponsora dla kluczowych zadań w projekcie CCN.
Unieważnienie postępowania o udzielenie zamówienia.	Średnia	Wysokie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Weryfikacja dokumentacji przetargowej i zapisów PZP. Unieważnienie postępowania o udzielenie zamówienia powoduje ponowne rozpoczęcie postępowania. Czynność zamawiającego polegająca na unieważnieniu postępowania o udzielenie zamówienia wywołuje skutek nieważności wszystkich czynności podjętych przez zamawiającego i wykonawców w toku takiego postępowania, jak również skutki tych czynności.
Niedoszacowanie wartości zamówień w ramach projektu na etapie planowania budżetu.	Średnia	Średnie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Analiza planów zakupowych pod względem ich niezbędności dla projektu w kontekście dostępnego budżetu i realizacji kluczowych zakupów niezbędnych do wypełnienia umowy o dofinansowanie oraz studium wykonalności. Ewentualna korekta w uzgodnieniu z instytucją pośredniczącą/zarządzającą (IP/CPPC).
Fluktuacja członków zespołu projektowego i trudności w znalezieniu specjalistów.	Średnia	Niskie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Transfer wiedzy w Zespołach. W NASK-PIB wdrożony jest system rozwoju kapitału ludzkiego bazujący na pozyskiwaniu doświadczonych specjalistów z rynku.
Opóźnienia w rozpoczęciu wykazywania realizacji wskaźnika projektu: 50 tys. przeszkolonych	Średnia	Średnie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Konieczność potwierdzenia sposobu uczestnictwa i ukończenia szkolenia (formuła list, dane na listach). Ostateczne potwierdzenie możliwości łączenia KPI z innych projektów. Zakup narzędzia, w którym możliwe będzie

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
osób.			organizowanie dedykowanych szkoleń przez NASK i który będzie umożliwiał tworzenie list obecności zgodnie z wytycznymi do potwierdzenia realizacji wskaźnika.
Opóźnienie w uzyskaniu Pozwolenia na Budowę.	Średnia	Średnie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Ścisła współpraca pomiędzy NASK - Biuro Projektowe (BP) - właściwy konserwator zabytków, UM, ZDM. Stały kontakt z właściwym konserwatorem zabytków. W razie wystąpienia sytuacji wymagających uzyskania wyjaśnienia właściwego konserwatora zabytków czy innego Urzędu zaangażowanego w sprawę szybka organizacja z spotkania roboczego.
Opóźnienie w uzyskaniu Pozwolenia na prowadzenie robót budowlanych przy zabytku wpisanym do rejestru.	Średnia	Niskie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Stały kontakt z właściwym konserwatorem zabytków. W razie wystąpienia sytuacji wymagających uzyskania wyjaśnienia właściwego konserwatora zabytków szybka organizacja z nim spotkania.
Przedłużające się procedury przetargowe.	Średnia	Niskie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Staranne planowanie zamówień (plan zamówień) poprzedzone gruntownym rozeznaniem rynku. Uruchamianie postępowań z wyprzedzeniem.
Niedostateczne kompetencje Wykonawców.	Średnia	Niskie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Wymiana zasobów kadrowych Wykonawcy na wniosek Zamawiającego.
Współpraca z podmiotami zewnętrznymi.	Średnia	Wysokie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Ścisła współpraca z zaangażowanymi podmiotami zewnętrznymi. Organizacja spotkań statusowych dot. realizowanych prac i ich postępu. Eskalacja na poziom Kierownictwa/Dyrekcji danej Instytucji.
Ograniczona funkcjonalność pomieszczeń laboratoryjnych CCN.	Średnia	Niskie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Ścisła współpraca z Biurem Projektowym nad koncepcją funkcjonalno-użytkową pomieszczeń CCN, w szczególności w formie spotkań

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
			warsztatowych. Raportowanie postępu realizowanych prac oraz napotkanych problemów.
Niezidentyfikowanie wszystkich wymagań do platformy e-learningowej (PEN).	Mała	Średnie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Zapewnienie odpowiedniego czasu na dogłębne przygotowanie SOPZ oraz pozyskanie wsparcia w identyfikacji wymagań i przygotowania opisu osób z innych działów, które organizują szkolenia.
Niedoszacowanie kosztów platformy e-learningowej (PEN).	Mała	Średnie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Ograniczenie funkcjonalności platformy do niezbędnych modułów gwarantujących możliwość realizacji zadania (szkoleń) zgodnie z zakresem.
Nieadekwatne określanie limitów kar umownych w podpisanych umowach z Wykonawcami.	Mała	Niskie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Staranne przygotowanie zapisów umowy w zakresie kar i ich weryfikacji. Dostosowanie wysokości kar do poziomu kiedy nie będą one ani rażąco wygórowane ani rażąco obniżone, w odniesieniu do wysokości wynagrodzenia.
Niedoszacowane ceny towarów i usług lub wyższe niż zakładano koszty eksploatacji rozwiązań jakie będą wykorzystywane w CCN (w tym koszty związane z wybudowaniem budynku).	Średnia	Wysokie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Staranne planowanie zadań, śledzenie cen asortymentu oraz cen towarów i usług. Zaplanowanie kosztów związanych z realizacją poszczególnych działań z zapasem amortyzującym możliwe zmiany. Analiza wymagań dla poszczególnych laboratoriów i podjęcie decyzji przez KS o ewentualnym obniżeniu wymagań w możliwym zakresie przy wypełnieniu celów projektu.
Nieadekwatne określenie kryteriów oceny ofert.	Mała	Niskie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Prawidłowe określenie kryteriów na etapie tworzenia dokumentacji lub korekta ich na etapie prowadzonego postępowania lub ostatecznie, unieważnienie postępowania.
Nieadekwatne określenie	Mała	Niskie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Rezygnacja z warunków

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
warunków udziału w postępowaniu.			udziału, które mogą okazać się nadmierne lub niewystarczające i w miarę możliwości zastępować warunki precyzyjnym opisem przedmiotu zamówienia lub stosować poza cenowe kryteria wyboru odnoszące się do przedmiotu zamówienia.
Zmiany prawa krajowego lub UE powodujące konieczność zmiany zakresu projektu.	Średnia	Znikome	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Stała analiza zmian prawnych jakie dzieją się w otoczeniu CSIRT-NASK (nie tylko w obszarze cyberbezpieczeństwa) ale również w zakresie prawa budowlanego dot. wybudowania obiektu CCN. Stała współpraca z urzędem ministra właściwego ds. informatyzacji (nadzorującego NASK-PIB) oraz śledzenie zmian w nowelizowanych ustawach dot. prawa budowlanego (Dzienniki ustaw, rozporządzenia).
Destabilizacja światowej gospodarki przejawiająca się zmiennością kursów walut, stóp procentowych, poziomu inflacji w trakcie przedsięwzięcia.	Duża	Niskie	Sposób reakcji: Akceptacja ryzyka. Opis reakcji: Śledzenie sytuacji na rynkach światowych i zmian w gospodarce co za tym idzie zmian cen towarów i usług. Monitorowanie cen towarów i usług, następnie eskalacja i podejmowanie decyzji na szczeblu KS co do konkretnych zakupów w projekcie.
Opóźnienia w dostawach sprzętu/usług/oprogramowania.	Średnia	Znikome	Sposób reakcji: Akceptacja ryzyka. Opis reakcji: Monitorowanie umów i weryfikacja planowanych dostaw zgodnie z zapisami umowy. Bieżąca komunikacja z Wykonawcami i ustalenie nowych terminów dostaw.
Zmiany organizacyjne uniemożliwiające realizację zadań.	Mała	Znikome	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Eskalacja i niezwłoczne wyznaczenie przez Lidera biznesowego kierunków i priorytetów działań w ramach projektu.
Nieodpowiednie opisanie przedmiotu zamówienia.	Mała	Znikome	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Korekta opisu przedmiotu zamówienia lub unieważnienie postępowania w przypadku złożenia już ofert.

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Niedostateczne środki na utrzymanie rezultatów projektu CCN.	Duża	Średnie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Pogłębiona analiza finansowa na etapie trwania projektu oraz monitorowanie cen towarów i usług na rynku, następnie eskalacja i podejmowanie decyzji na szczeblu Kierownictwa NASK co do konkretnych działań i źródeł finansowania.
Konieczność rozszerzenia zakresu funkcjonalnego CCN po formalnym zakończeniu projektu (np. w wyniku większej niż zakładano presji cyberzagrożeń).	Średnia	Średnie	Sposób reakcji: Mitygowanie ryzyka. Opis reakcji: Analiza możliwości rozszerzenia zakresu funkcjonalnego CCN, eskalacja i podejmowanie decyzji na szczeblu Kierownictwa NASK co do konkretnych działań i źródeł finansowania.

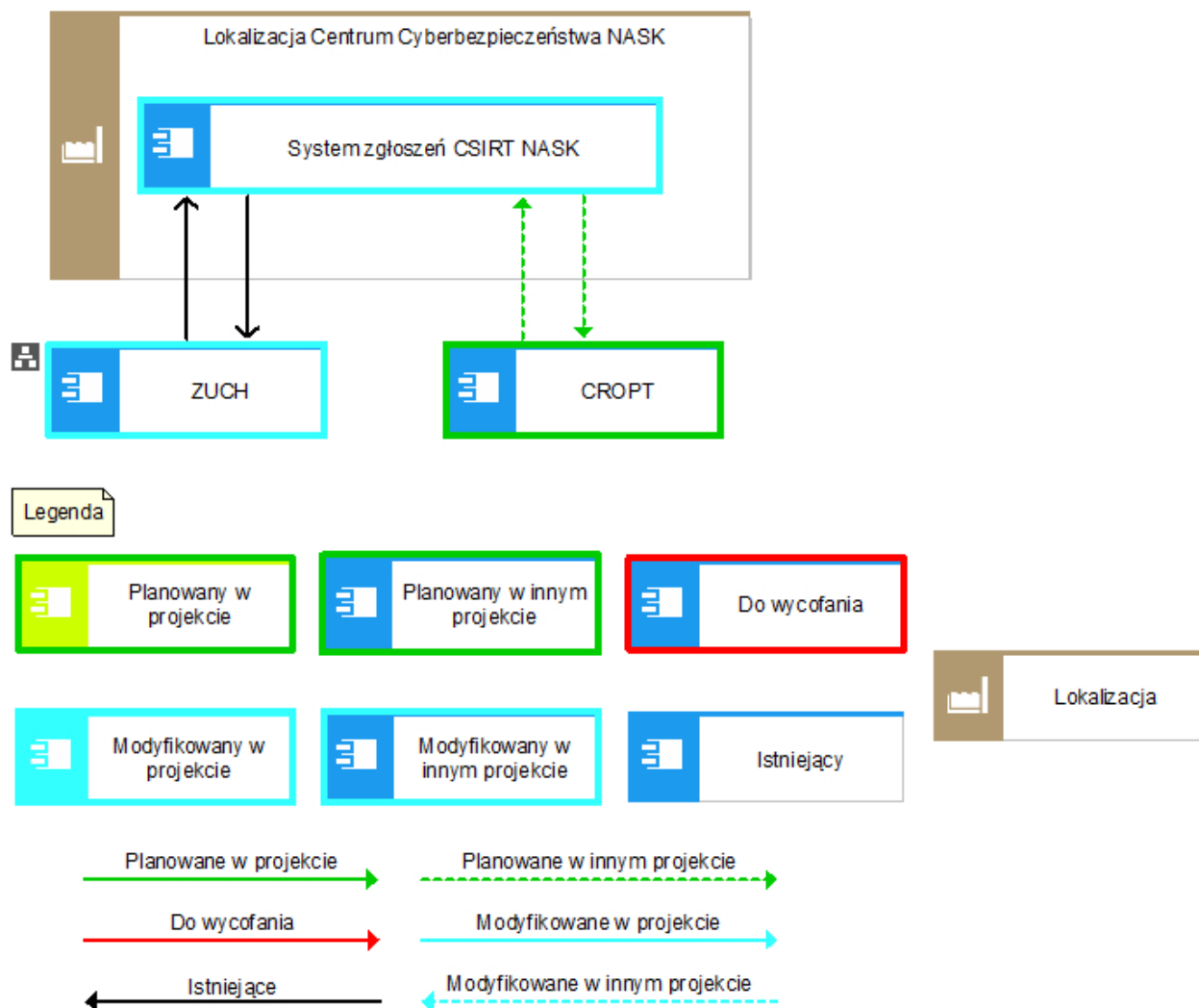
6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa z 5 lipca 2018 r o krajowym systemie cyberbezpieczeństwa.	TAK/NIE		
2	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.	TAK/NIE		
3	Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.	TAK/NIE		
4	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.	TAK/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
5	Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.	TAK/NIE		
6	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).	TAK/NIE		
7	Ustawa z 27 lipca 2025 r o krajowym systemie certyfikacji cyberbezpieczeństwa.	TAK/NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



Lista systemów wykorzystywanych w projekcie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	CROPT	NASK-PIB	Centralny system preanalityczny do współdzielenia materiałów związanych z postępowaniami prowadzonymi przez zespoły reagowania i analityków. CROPT ma umożliwić szybkie i bezpieczne przekazywanie zabezpieczonego materiału wiążanego z prowadzonymi działaniami mających na	Planowany	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>celu analizę zaistniałego incydentu. Umożliwia współdzielenie materiału oraz wymianę informacji dotyczących ustaleń i wyników analiz. Posiada możliwość zarządzania rolami i uprawnieniami w dostępie do wspomnianego materiału, jak i do ustaleń związanych z prowadzoną analizą.</p> <p>System CROPT ma obejmować kilka komponentów: CORE – zarządzanie systemem, CASE – zarządzanie incydentem, UPLOADER – transfer materiałów, Baza wiedzy - moduł pomagający użytkownikowi przejść przez zabezpieczanie materiału, dostarczający informacji jak korzystać z systemu.</p>		
2	System zgłoszeń CSIRT NASK (CSIRT RT)	NASK-PIB	<p>System zgłoszeń CSIRT NASK to system wspierający rejestrację i obsługę zgłoszeń dotyczących incydentów komputerowych w obszarze określonym w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Celem tego systemu jest zapewnienie sprawnego zarządzania zgłoszeniami incydentów, koordynacja działań analitycznych oraz wsparcie w procesie obsługi incydentów cyberbezpieczeństwa przez CSIRT-NASK. System ten pełni funkcje centralnego narzędzia</p>	Modyfikowany	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			ticketowego (RTIR) dla CSIRT poziomu krajowego, realizuje funkcje związane ze zwalczaniem nadużyć w komunikacji i obsługuje blokady domen internetowych. Umożliwia w ten sposób sprawne reagowanie na incydenty bezpieczeństwa teleinformatycznego przez CSIRT-NASK i koordynację tego procesu przez CSIRT poziomu krajowego.		
3	ZUCH	Ministerstwo Cyfryzacji	<p>System Zapewniania Usług Chmurowych (ZUCH) to narzędzie informatyczne służące do wsparcia administracji publicznej w procesie zamawiania usług chmur obliczeniowych oraz wsparcia w zakresie obsługi pozyskanych usług z Publicznych Chmur Obliczeniowych (PChO) oraz Rządowej Chmury Obliczeniowej (RChO).</p> <p>ZUCH został uruchomiony w kwietniu 2020 r. przez Ministerstwo Cyfryzacji pod adresem https://chmura.gov.pl/ i jest kluczowym elementem Wspólnej Infrastruktury Informatycznej Państwa WIIP.</p> <p>System ZUCH umożliwia pozyskanie usług chmurowych dla Odbiorców usług poprzez udostępnione Katalogi usług RChO lub PChO. Wybór odpowiedniego katalogu usług wspiera proces kwalifikacji</p>	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			systemu informatycznego opisany zgodnie ze Standardami Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) i udostępniony w postaci ankiety na ZUCH.		

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	System zgłoszeń CSIRT NASK	CROPT	Dane incydentu	Kopiowanie danych	realizowalny inną metodą	Wymiana plików XML
2	CROPT	System zgłoszeń CSIRT NASK	Status zarejestrowanego incydentu	kopiowanie danych	realizowalny inną metodą	Wymiana plików XML
3	ZUCH	System zgłoszeń CSIRT NASK	Dane opisujące system informatyczny wraz z proponowaną klasyfikacją zgodnie z wymaganiami SCCO (Uchwała WIIP)	kopiowanie danych	realizowany inną metodą	Wymiana plików XML
4	System zgłoszeń CSIRT NASK	ZUCH	Opinia potwierdzająca poprawność klasyfikacji zgodnie z SCCO.	kopiowanie danych	realizowalny inną metodą	Wymiana plików XML

7.2. Kluczowe komponenty architektury rozwiązania



Legenda



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	
2.	Sieć i bezpieczeństwo	
3.	Standardy wymiany danych	
4.	Systemy operacyjne serwerowe	
5.	Bazy danych	
6.	Serwery aplikacji	
7.	Portale	
8.	Inne	<p>CERT Polska, działający w strukturach NASK-PIB (Państwowy Instytut Badawczy), korzysta z szeregu autorskich oraz specjalistycznych narzędzi do monitorowania, analizy i reagowania na zagrożenia w polskiej przestrzeni internetowej. Do kluczowych narzędzi należą:</p> <ul style="list-style-type: none"> - n6 (Network Security Incident eXchange): Autorski system CERT Polska do automatycznego zbierania, przetwarzania i wymiany informacji o incydentach (tzw. threat intelligence). - Artemis: System służący do skanowania i wykrywania podatności w systemach internetowych. Pozwala na

Lp.	Obszar	Założenie technologiczne
		<p>automatyczne skanowanie bezpieczeństwa stron udostępnianych w sieci i powiadamianie administratorów o zagrożeniach.</p> <p>- moje.cert.pl: Darmowe narzędzie udostępnione przez NASK, które umożliwia użytkownikom i administratorom sprawdzenie, czy ich infrastruktura (domeny, strony) jest bezpieczna.</p> <p>- Lista Ostrzeżeń przed niebezpiecznymi stronami: Baza domen wykorzystywanych do phishingu i oszustw online, udostępniana operatorom w celu automatycznego blokowania złośliwych stron.</p> <p>- Numer 8080: Specjalny kanał do zgłaszania podejrzanych wiadomości SMS.</p> <p>- MWDB (Malware Database): Wewnętrzna baza danych i platforma do analizy złośliwego oprogramowania.</p> <p>- Narzędzia do odzyskiwania plików (Ransomware Decryptors): Specjalistyczne narzędzia tworzone do odzyskiwania danych zaszyfrowanych przez ransomware, np. Vortex czy Mapo.</p> <p>- Formularz zgłoszeniowy: Dostępny na stronie cert.pl, służący do zgłaszania incydentów bezpieczeństwa przez użytkowników (do wprowadzenia do CSIRT RT).</p> <p>Narzędzia te są kluczowe w realizowaniu zadań CSIRT NASK (Computer Security Incident Response Team), zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa.</p>

7.4. Opis zasobów danych przetwarzanych w planowanym rozwiązaniu

Czy nowy system będzie tworzył zasoby danych o charakterze rejestru publicznego?

TAK/NIE

Czy nowy system będzie przetwarzał (używał, zmieniał) zawartość innych rejestrów publicznych?

TAK/NIE

7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności [...]) (Dz. U. 2012, poz. 526 z późn. zm.) w zakresie dot. systemu zarządzania bezpieczeństwem informacji:

- system nie podlega rygorom KRI – należy wyjaśnić czy istnieją inne normy bezpieczeństwa, które będą spełnione przez system zgodnie z wymogami KRI

Niniejsze przedsięwzięcie obejmuje w szczególności przebudowę i dostosowanie infrastruktury teleinformatycznej CSIRT-NASK niezbędnej do wzmocnienia jego zadań wynikających z ustawy o KSC.

Wszystkie systemy wykorzystywane przez NASK (w tym eksploatowane przez CSIRT-NASK) są budowane, eksploatowane i rozwijane zgodnie z wytycznymi zawartymi w Narodowych Standardach Cyberbezpieczeństwa (patrz <https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber>). Dotyczy to w szczególności niniejszego projektu, który został zdefiniowany i opracowany zgodnie z przywołanymi zasadami.

~~-dodatkowe zabezpieczenia powyżej wymogów KPI: należy wskazać uzasadnienie~~