

# OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Utworzenie zespołów specjalistów cyberbezpieczeństwa działających lokalnie i wspierających podmioty krajowego systemu cyberbezpieczeństwa w obsłudze incydentów i odzyskiwaniu danych oraz prowadzenie działań podnoszących świadomość o cyberbezpieczeństwie		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	NASK-PIB		
Partnerzy	Komendant Główny Policji – zadania projektowe będą realizowane przez jednostki organizacyjne KGP (Komendy Głównej Policji) oraz CBZC (Centralnego Biura Zwalczania Cyberprzestępczości).		
Źródło finansowania	Krajowy Plan Odbudowy i Zwiększania Odporności, działanie C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo; budżet państwa, część budżetowa - w takcie ustaleń;		
Całkowity koszt projektu	44 143 026,21 zł		
Planowany okres realizacji projektu	11-2024 do 06-2026		
Osoba kontaktowa	Piotr Kozyra	piotr.kozyra@nask.pl	885910130

## 1. POWODY PODJĘCIA PROJEKTU

### 1.1. Identyfikacja problemu i potrzeb

Postępująca cyfryzacja usług Państwa to proces nieuchronny i nieodwracalny, przyspieszony dodatkowo przez pandemię, co zwiększyło znaczenie operowania na danych. Niezakłócony dostęp do zbiorów danych stanowi fundament współczesnych usług. Każdorazowe awarie, prace serwisowe lub ataki na środowiska przetwarzania danych prowadzą do zakłóceń w świadczeniu usług, generując rozległe skutki społeczne i ekonomiczne. W latach 2022-2024 podmioty publiczne raportowały do CSIRT NASK ataki na swoje środowiska przetwarzania danych: 24 razy w 2022, 37 razy w 2023 i 25 razy w 2024. Ataki te były przeprowadzane przez wyspecjalizowane grupy przestępcze, wykorzystujące szkodliwe oprogramowanie typu ransomware, żądając okupu za odzyskanie danych lub zaniechanie ich publikacji w Internecie. CSIRT NASK konsekwentnie rekomenduje niepłacenie przestępcom. Ataki ransomware stanowią globalny trend, który z dużym prawdopodobieństwem będzie się nasilał i ewoluował. Każde tego rodzaju zdarzenie wymaga skoordynowanych działań przywracających ciągłość usług, dogłębnej analizy incydentu i ustalenia sprawców. Presja medialna i społeczna dodatkowo utrudnia zarządzanie sytuacją. Ze względu na operowanie na danych ulotnych oraz możliwość celowego niszczenia artefaktów analitycznych, konieczna jest szybka i precyzyjna reakcja. Analitycy CSIRT i funkcjonariusze organów ścigania muszą ściśle współpracować, mając jasne procedury działania. Brak zunifikowanego systemu analizy incydentów skutkuje fragmentaryzacją danych, wydłużonym czasem reakcji i ograniczoną możliwością efektywnej współpracy. Utworzenie centralnego systemu preanalitycznego umożliwi automatyzację wnioskowania, ustrukturyzowaną analizę materiału dowodowego oraz szybsze podejmowanie decyzji operacyjnych, co znacząco podniesie skuteczność reakcji na incydenty cyberbezpieczeństwa.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Funkcjonariusze i Pracownicy Policji	<ul style="list-style-type: none"> <li>• Brak niezbędnych narzędzi i procedur wynikający z niedostatku specjalistycznych rozwiązań wsparcia analizy i obsługi incydentów, a także brak ujednoliconych metodyk postępowania.</li> <li>• Niedostatek szkoleń specjalistycznych na poziomie eksperckim utrudnia sprawną reakcję w zmieniających się zagrożeniach w świecie cyfrowym.</li> <li>• Niedobory sprzętowe i infrastrukturalne – Brak zasobów technicznych pozwalających na efektywne zabezpieczanie danych oraz prowadzenie prac analitycznych w sytuacjach krytycznych.</li> <li>• Brak skutecznych mechanizmów komunikacji generujący trudności w wymianie informacji i koordynacji działań między kluczowymi interesariuszami, co opóźnia proces decyzyjny.</li> <li>• Błędne adresowanie problemów w sytuacjach kryzysowych wynikające z braku wypracowanych procedur i jasnych ścieżek eskalacji, co powoduje opóźnienia w reakcji na incydenty i wzrost ich skutków.</li> <li>• Nieoptymalna wymiana materiału analitycznego i dowodowego ze służbami spowodowana brakiem wypracowanych procedur i kanałów przekazywania materiałów do Policji i Prokuratury powoduje utrudnienia w procesach dochodzeniowych i ogranicza możliwość skutecznego ścigania sprawców cyberprzestępstw.</li> </ul>	3500
<p>Podmioty Publiczne (Każda instytucja publiczna posiadająca infrastrukturę / usługi sieciowe)</p> <p><a href="https://www.gov.pl/web/cyfryzacja/podmioty-publiczne">https://www.gov.pl/web/cyfryzacja/podmioty-publiczne</a></p>	<ul style="list-style-type: none"> <li>• Brak priorytyzacji oraz koordynacji działań po wystąpieniu ataku skutkujący brakiem klarownej kolejności postępowania i opóźnieniem odzyskania ciągłości działania.</li> <li>• Niewystarczający poziom wiedzy pracowników w zakresie postępowania wobec incydentów cyberbezpieczeństwa.</li> <li>• Nieprawidłowa identyfikacja źródła incydentu (nawracające incydenty) wynikająca z Błędneho określenia lub przeoczenia pierwotnej przyczyny ataku prowadzi do sytuacji, w której incydent (np. ransomware) może się powtórzyć po pewnym czasie.</li> <li>• Utrata kluczowych danych ulotnych istotnych dla analizy spowodowane brakiem mechanizmów do odpowiednio szybkiego i bezpiecznego zabezpieczania danych wrażliwych (m.in. logów, śladów</li> </ul>	76000

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	systemowych) uniemożliwia przeprowadzenie całościowej analizy incydentu.	
Podmioty KSC	<ul style="list-style-type: none"> <li>• Niewystarczające rozpoznanie zagrożeń zmaterializowanych w obrębie danego sektora lub rynku i płynący z nich brak efektywnej wymiany informacji oraz kompletnej wiedzy o występujących zagrożeniach, co utrudnia trafne wyciąganie wniosków i utwardzanie środowisk teleinformatycznych.</li> <li>• Niewłaściwy poziom utrzymania i zabezpieczenia usług oraz infrastruktury - Niedostateczne działania utrzymaniowe i prewencyjne, zwiększające podatność na ataki i skutkujące dłuższym czasem przywracania sprawności po incydencie.</li> </ul>	40 000 (Po implementacji NIS2)
Pracownicy NASK PIB / CSIRT NASK / CERT Polska	<ul style="list-style-type: none"> <li>• Wydłużony czas realizacji analiz ze względu na brak jakościowego materiału analitycznego - Niedostateczne zabezpieczanie logów, obrazów dysków czy maszyn wirtualnych ogranicza możliwość sprawnego odtworzenia incydentu i powoduje znaczne opóźnienia w przygotowaniu kompleksowych raportów.</li> <li>• Wydłużony czas rozpoznania incydentu z powodu braku wypracowanej metodyki współpracy między zaatakowanym podmiotem a służbami - Brak jasno określonych procedur i odpowiedzialności przekłada się na nieefektywną wymianę informacji i utrudnia przeprowadzenie szybkich działań zaradczych. Może to skutkować błędnie obranymi priorytetami w obsługiwanym incydencie.</li> <li>• Brak standardowej metodyki komunikacji ze służbami w zakresie przyjmowania, wymiany i przekazywania materiału dowodowego oraz raportów - Niewypracowane kanały i formaty współpracy opóźniają przekazywanie kluczowych danych, prowadząc do przedłużenia całego procesu analitycznego i dochodzeniowego.</li> </ul>	1100
Analitycy CSIRT MON, CSIRT GOV	<ul style="list-style-type: none"> <li>• Zbyt długi czas rozpoznania i analizy incydentów o wysokiej skali zagrożenia – opóźniona wymiana informacji pomiędzy CSIRT-ami i służbami powodują, że w przypadku poważnych incydentów proces rozpoznania i neutralizacji zagrożenia jest znacząco wydłużony.</li> </ul>	50 (analitycy MON, GOV)
Pracownicy prokuratury	<ul style="list-style-type: none"> <li>• Brak ujednoliconej metodyki postępowania w sprawach cyberprzestępczości – Różnice w</li> </ul>	100

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	<p>podejściu do analizy i klasyfikacji incydentów pomiędzy jednostkami prokuratury skutkują niespójnością działań i wydłużeniem procesów dochodzeniowych.</p> <ul style="list-style-type: none"> <li>• Ograniczona wiedza specjalistyczna w zakresie analizy incydentów cyberbezpieczeństwa – Niski poziom wyspecjalizowania prokuratorów w obszarze kompetencji dot. Informatyki śledczej utrudnia efektywną współpracę z zespołami CSIRT oraz służbami, co może prowadzić do błędnej kwalifikacji czynów lub trudności w zabezpieczaniu materiału dowodowego.</li> <li>• Brak efektywnego systemu wymiany informacji z CSIRT-ami i służbami – Niedostateczne mechanizmy przekazywania analiz, raportów technicznych i materiałów dowodowych powodują, że postępowania są wydłużone, a ich skuteczność ograniczona.</li> <li>• Problemy w zakresie zabezpieczania i przechowywania dowodów cyfrowych – Brak wypracowanych standardów dotyczących ochrony materiałów pochodzących z cyberprzestępstw prowadzi do ryzyka ich utraty, niewłaściwego przechowywania lub kwestionowania ich integralności w procesach sądowych.</li> </ul>	

## 1.2. Opis stanu obecnego

Artykuł 34.1 UoKSC mówi: CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezp. oraz podmioty świadczące usługi z zakresu cyberbezp. współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań. Począwszy od 2018 roku funkcjonujący w ramach NASK PIB zespół CERT Polska rozpoczął systemowe budowanie relacji na rzecz współpracy przy incydentach teleinformatycznych w sektorze publicznym dla których zaistniało przestępstwo zdefiniowane w Kodeksie Karnym (Art.269 KK). W celu doskonalenia systemu przeprowadzono szereg inicjatyw na rzecz rozwoju obszaru styku NASK PIB oraz Policji. Poza częścią warsztatową (CyberPOL, inicjatywa NASK PIB w latach 2018-2019), identyfikującą luki kompetencyjno-proceduralne dla tego typu spraw, dnia 26.05.2022 podpisano porozumienia kierunkowe pomiędzy jednostkami, dające podwaliny pod uruchomienie szerszego wymiaru współpracy, w tym na rzecz rozwoju szeroko rozumianych systemów. Od 08.2022, nawiązano stałą współpracę operacyjną z Sekcją Obsługi Całodobowej WWK CBZC. W ramach tej współpracy, za pośrednictwem komunikatora CSIRT NASK, prowadzona jest komunikacja w przedmiocie występujących na terenie RP spraw tego typu. W ramach kanału następuje koordynacja działań podejmowanych we współpracy z policją operującą lokalnie. Działania sprowadzają się do ustalenia możliwości (limitowanych przez posiadane zasoby sprzętowe) i potrzeby wsparcia podmiotu poprzez przedstawicieli CSIRT NASK oraz CBZC. Dalsze kroki w ramach wsparcia są przedmiotem każdorazowych ustaleń pomiędzy stronami. Raport przedstawiający wyniki przeprowadzonych przez CSIRT NASK prac analitycznych jest przekazywany do jednostki prowadzącej lub prokuratury nadzorującej

postępowanie w formie elektroniczne, w końcowej fazie obsługi incydentu.

## 2. EFEKTY PROJEKTU

### 2.1. Cele i korzyści wynikające z projektu

<b>Cel - 1</b>	Modernizacja i ujednolicenie metodyki postępowania przy atakach typu ransomware (lub innych wyczerpujących znamiona przestępstwa (Art.269 KK) w podmiotach krajowego systemu cyberbezpieczeństwa (CSIRT NASK oraz Policji), w celu szybszego przywracania ciągłości usług oraz ograniczenia strat finansowych i społecznych.
<b>Cel strategiczny</b>	Wpisuje się w realizację celu szczegółowego nr 2 Strategii Cyberbezpieczeństwa RP (2019–2024), zakładającego podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego. Strategii Cyberbezpieczeństwa RP na lata 2019–2024, w tym w cel strategiczny nr 2: „Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty”.
<b>Korzyść:</b>	<ul style="list-style-type: none"><li>- Skrócenie czasu reakcji na incydenty.</li><li>- Zwiększenie skuteczności w ustalaniu sprawców oraz zabezpieczaniu materiału dowodowego.</li><li>- Podniesienie poziomu zaufania społecznego do zdolności organów ścigania w zakresie zwalczania cyberprzestępczości.</li></ul>
<b>KPI:</b>	KPI 1: Opracowanie metodyki oraz skonfigurowanie odpowiedniego zaplecza systemowego, pozwalających na kompleksową, powtarzalną i szybką reakcję na incydenty typu ransomware (i inne poważne zdarzenia)  KPI 2: Liczba podmiotów krajowego systemu cyberbezpieczeństwa (KSC) wdrażających nową metodykę postępowania przy atakach ransomware.
<b>Wartość aktualna i docelowa KPI:</b>	KPI 1: - wartość aktualna: 0  KPI 2: - wartość aktualna: 0 KPI 1: - wartość docelowa: 1  KPI 1: - wartość docelowa: 2
<b>Metoda pomiaru KPI</b>	KPI 1: Ćwiczenia tabletop z wykorzystaniem wytworzonego systemu. (Wytworzono kompletną nową metodykę oraz zakupiono i skonfigurowano zaplecze sprzętowe / systemowe do końca I kw. 2026 r.) <ul style="list-style-type: none"><li>• Sposób pomiaru: Realizacja ćwiczenia tabletop opartego o nową metodykę</li><li>• Źródło pomiaru: Lista obecności i/lub protokół odbioru</li><li>• Częstotliwość pomiaru: Jednorazowo w dniu zakończenia projektu</li></ul> KPI 2: Raport z zastosowania metodyki w analizie incydentów. (podmioty podlegające pod KSC wdrożyły nową metodykę do końca II kw.

	2026 r) <ul style="list-style-type: none"> <li>• Sposób pomiaru: Realizacja wdrożenia</li> <li>• Źródło pomiaru: Raport z wdrożenia metodyki</li> <li>• Częstotliwość pomiaru: Jednorazowo w dniu zakończenia projektu</li> </ul>
<b>Cel - 2</b>	Stworzenie i wdrożenie centralnego systemu preanalitycznego służącego do bezpiecznego transferu i analizy danych dowodowych, umożliwiającej sprawną współpracę pomiędzy Policją (CBZC), Prokuraturą oraz CSIRT NASK.
<b>Cel strategiczny</b>	Wpisuje się w zadania wskazane w KPO (Komponent C3.1.1. Cyberbezpieczeństwo – CyberPL), zmierzające do optymalizacji i cyfryzacji współpracy służb państwowych odpowiedzialnych za bezpieczeństwo. Wpisuje się w realizację Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), Komponent C3.1.1. Cyberbezpieczeństwo – CyberPL, w tym w cel strategiczny: „Zwiększenie skuteczności krajowego systemu cyberbezpieczeństwa poprzez cyfryzację procesów współpracy służb odpowiedzialnych za bezpieczeństwo”.
<b>Korzyść:</b>	<ul style="list-style-type: none"> <li>- Usprawniona koordynacja międzyinstytucjonalna.</li> <li>- Krótszy czas obsługi incydentu dzięki szybkiemu udostępnianiu materiałów i raportów.</li> <li>- Zwiększenie skuteczności postępowań karnych dzięki lepszemu zabezpieczeniu dowodów cyfrowych.</li> </ul>
<b>KPI:</b>	KPI 1: Uruchomienie systemu wspierającego współpracę międzyinstytucjonalną  KPI 2: Uśredniony czas obsługi incydentów wymagających współpracy międzyinstytucjonalnej  KPI 3: Liczba spraw, w których nowy system został wykorzystany w analizie materiałów dowodowych
<b>Wartość aktualna i docelowa KPI:</b>	KPI 1: - wartość aktualna: 0  KPI 2: - wartość aktualna: 90 dni (średni czas obsługi w 2024 r.).  KPI 3: - wartość aktualna: 0 KPI 1: - wartość docelowa: 1  KPI 2: - wartość docelowa: 30 dni (średni czas obsługi w 06.2026 r. po wdrożeniu systemu).  KPI 3: - wartość docelowa: 30 spraw rocznie
<b>Metoda pomiaru KPI</b>	KPI 1: Wdrożenie systemu w wersji produkcyjnej <ul style="list-style-type: none"> <li>• Sposób pomiaru: Notatka z wdrożenia</li> <li>• Źródło pomiaru: Repozytorium kodu</li> <li>• Termin pomiaru: Jednorazowo w dniu 2026-05-29</li> </ul>

	<p>KPI 2:</p> <ul style="list-style-type: none"> <li>• Sposób pomiaru: Analiza danych operacyjnych</li> <li>• Źródło danych: System zgłoszeń incydentów, raporty podsumowujące działania międzyinstytucjonalne</li> <li>• Częstotliwość pomiaru: Jednorazowo w dniu zakończenia projektu</li> </ul> <p>KPI 3:</p> <ul style="list-style-type: none"> <li>• Sposób pomiaru: Ewaluacja ilościowa – liczba spraw wykorzystujących system</li> <li>• Źródło danych: Raporty z użytkowania systemu, dane operacyjne CBZC i CSIRT</li> <li>• Częstotliwość pomiaru: Jednorazowo w dniu zakończenia projektu</li> </ul>
<b>Cel - 3</b>	Modernizacja i rozwój komórek organizacyjnych Policji (CBZC), zajmujących się zwalczaniem cyberprzestępczości, ze szczególnym uwzględnieniem narzędzi do zabezpieczania danych ulotnych i odzyskiwania informacji.
<b>Cel strategiczny</b>	Realizuje założenia Strategii Cyberbezpieczeństwa RP w obszarze zwiększania zdolności operacyjnych organów ścigania. Wpisuje się w realizację Strategii Cyberbezpieczeństwa RP na lata 2019–2024, w tym w cel strategiczny nr 3: „Zwiększenie zdolności operacyjnych organów ścigania, administracji i sektora prywatnego do zwalczania cyberzagrożeń”.
<b>Korzyść:</b>	<ul style="list-style-type: none"> <li>- Skrócenie czasu analizy incydentu dzięki wyspecjalizowanym narzędziom.</li> <li>- Poprawa jakości zabezpieczanego materiału dowodowego (minimalizacja ryzyka utraty danych).</li> <li>- Możliwość szybszego identyfikowania i neutralizowania zagrożeń.</li> </ul>
<b>KPI:</b>	<p>KPI 1: Liczba zmodernizowanych komórek organizacyjnych Policji (CBZC) dysponujących nowym sprzętem.</p> <p>KPI 2: Liczba zmodernizowanych komórek organizacyjnych Policji (CBZC) dysponujących nowym oprogramowaniem.</p>
<b>Wartość aktualna i docelowa KPI:</b>	<p>KPI 1:</p> <ul style="list-style-type: none"> <li>- wartość aktualna: 0</li> </ul> <p>KPI 2:</p> <ul style="list-style-type: none"> <li>- wartość aktualna: 0</li> </ul> <p>KPI 1:</p> <ul style="list-style-type: none"> <li>- wartość docelowa: 18</li> </ul> <p>KPI 2:</p> <ul style="list-style-type: none"> <li>- wartość docelowa: 18</li> </ul>
<b>Metoda pomiaru KPI</b>	<p>KPI 1:</p> <p>Zakończona procedura zakupowa i wykonanie odbiorów sprzętu</p> <ul style="list-style-type: none"> <li>• Sposób pomiaru: Protokół odbioru</li> <li>• Źródło danych: Dokumentacja projektowa / protokół odbioru</li> <li>• Częstotliwość pomiaru: Jednorazowo w dniu zakończenia projektu</li> </ul> <p>KPI 2:</p> <p>Zakończona procedura zakupowa i wykonanie odbiorów</p> <ul style="list-style-type: none"> <li>• Sposób pomiaru: Protokół odbioru</li> <li>• Źródło danych: Dokumentacja projektowa / protokół odbioru</li> <li>• Częstotliwość pomiaru: Jednorazowo w dniu zakończenia projektu</li> </ul>
<b>Cel - 4</b>	Rozwój kompetencyjny funkcjonariuszy Policji (CBZC), Prokuratury oraz pracowników podmiotów krajowego systemu cyberbezpieczeństwa (KSC) w

	zakresie prewencji, detekcji i reakcji na ataki ransomware poprzez zintegrowany system szkoleń.
<b>Cel strategiczny</b>	Odpowiada wytycznym Strategii Cyberbezpieczeństwa RP, ukierunkowanym na rozwój kompetencji cyfrowych pracowników administracji oraz służb publicznych. Wpisuje się w realizację Strategii Cyberbezpieczeństwa RP na lata 2019–2024, w tym w cel strategiczny nr 5: „Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów IT oraz pracowników administracji publicznej”.
<b>Korzyść:</b>	<ul style="list-style-type: none"> <li>- Rozwój kompetencyjny uczestników KSC.</li> <li>- Wyższy poziom świadomości wśród pracowników i funkcjonariuszy (ograniczenie ryzyka ludzkich błędów).</li> <li>- Wzmocnienie autorytetu służb państwowych dzięki skuteczniejszym działaniom i transparentnym procedurom.</li> </ul>
<b>KPI:</b>	<p>KPI 1: Liczba funkcjonariuszy i pracowników podmiotów KSC objętych szkoleniami</p> <p>KPI 2: Liczba przeprowadzonych seminariów</p>
<b>Wartość aktualna i docelowa KPI:</b>	<p>KPI 1:</p> <ul style="list-style-type: none"> <li>- wartość aktualna: 0</li> </ul> <p>KPI 2:</p> <ul style="list-style-type: none"> <li>- wartość aktualna: 0</li> </ul> <p>KPI 1:</p> <ul style="list-style-type: none"> <li>- wartość docelowa: 1900</li> </ul> <p>KPI 2:</p> <ul style="list-style-type: none"> <li>- wartość docelowa: 1</li> </ul>
<b>Metoda pomiaru KPI</b>	<p>KPI 1:</p> <ul style="list-style-type: none"> <li>• Sposób pomiaru: Realizacja szkoleń</li> <li>• Źródło danych: Lista obecności i/lub protokół odbioru</li> <li>• Częstotliwość pomiaru: Pomiar jednorazowy na koniec projektu</li> </ul> <p>KPI 2:</p> <ul style="list-style-type: none"> <li>• Sposób pomiaru: Realizacja seminarium</li> <li>• Źródło danych: Dokumentacja seminarium, raporty organizatorów</li> <li>• Częstotliwość pomiaru: Pomiar jednorazowy na koniec projektu</li> </ul>

## 2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi
1	Zgłoszenie incydentu i przekazanie materiału do wspólnej analizy	A2B A2A	Podmioty KSC Pracownicy NASK PIB / CSIRT NASK / CERT Polska Pracownicy prokuratury Podmioty Publiczne	Dwustronna interakcja



Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi
			(Każda instytucja publiczna posiadająca infrastrukturę / usługi sieciowe)  <a href="https://www.gov.pl/web/cyfryzacja/podmioty-publiczne">https://www.gov.pl/web/cyfryzacja/podmioty-publiczne</a> Funkcjonariusze i Pracownicy Policji Analitycy CSIRT MON, CSIRT GOV (rocznie ok 100 transakcji)	
2	Dostęp do repozytorium wyników analiz i raportów	A2A	Pracownicy NASK PIB / CSIRT NASK / CERT Polska Pracownicy prokuratury Funkcjonariusze i Pracownicy Policji Analitycy CSIRT MON, CSIRT GOV (rocznie ok 50 transakcji)	Dwustronna interakcja
3	Dostęp do bazy wiedzy (wewnętrzna i zewnętrzna)	A2A	Pracownicy NASK PIB / CSIRT NASK / CERT Polska Pracownicy prokuratury Funkcjonariusze i Pracownicy Policji Analitycy CSIRT MON, CSIRT GOV (rocznie ok 100 transakcji)	Jednostronna interakcja

## 2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

## 2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
Materiały informacyjno-promocyjne zwiększające świadomość interesariuszy	09-2025

Nazwa produktu	Planowana data wdrożenia
na temat projektu i jego efektów	
REST API dla potrzeb komunikacji pomiędzy systemem zgłoszeń CSIRT NASK a CROPT	12-2025
Materiały szkoleniowe wspierające proces podnoszenia kompetencji	03-2026
Raport z testu prywatności	05-2026
Zmodyfikowany System Zgłoszeń CSIRT NASK	05-2026
CROPT - System teleinformatyczny	06-2026
Raport z testów bezpieczeństwa	06-2026
Raport z testów wydajności	06-2026
Raport z testów WCAG	06-2026

### 3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Ukończone prace koncepcyjno-programistyczne	2025-04-30
Przygotowano harmonogram przeprowadzenia szkoleń	2025-09-30
Uruchomiony prototyp narzędzia do współdzielenia materiału ( Wdrożenie wersji testowej platformy w środowisku testowym oraz rozpoczęcie testów funkcjonalnych)	2025-12-31
Zakupione kluczowe elementy infrastruktury IT (serwery, stacje robocze, urządzenia do analizy incydentów teleinformatycznych)	2026-03-31
Uruchomiona wersja produkcyjna narzędzia do współdzielenia materiału ( Wdrożony system w środowisku operacyjnym).	2026-05-29
Przeprowadzono inicjalny test prywatności	2026-05-29
Zakończone testy bezpieczeństwa, wydajności, WCAG podsumowane raportami.	2026-06-30
Zmodernizowana infrastruktura sprzętowa i oprogramowanie CBZC (Zakupiony, zainstalowany i skonfigurowany sprzęt dla CBZC (m.in. narzędzia do odzyskiwania danych, sprzęt perymetryczny)).	2026-06-30
Zakończony proces zakupowy, komplet sprzętu projektowego znajduje się w siedzibie zamawiającego (NASK-PIB) i jest wykorzystywany operacyjnie.	2026-06-30

### 4. KOSZTY

#### 4.1. Koszty ogólne projektu wraz ze sposobem finansowania

<b>Całkowity koszt projektu (netto oraz brutto), w tym</b>	Netto 37 500 000,00 zł Brutto 44 143 026,21 zł	
<b>Procent dofinansowania ze środków UE (brutto)</b>	85%	
<b>Procent środków z budżetu państwa (brutto)</b>	15%	
<b>Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto)</b>	2024	Netto 0,00 zł Brutto 0,00 zł
	2025	Netto 35 114 331,35 zł Brutto 41 743 557,56 zł
	2026	Netto 2 385 668,65 zł Brutto 2 399 468,65 zł

## 4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Koszt wynagrodzenia personelu wytwarzającego oprogramowanie specjalistyczne – prace analityczne, programistyczne, wytwarzanie, testowanie, wdrożenie Zakup licencji i support do urządzeń sieciowych i do wirtualizacji	9 090 528,06 zł	Wytworzenie specjalistycznego oprogramowania jest niezbędny do wdrożenia nowych narzędzi analitycznych i systemów raportowania incydentów. Brak tych rozwiązań uniemożliwiłby sprawną obsługę zgłoszeń oraz szybką analizę incydentów. W efekcie ograniczyłoby to możliwość skutecznego zabezpieczania i odzyskiwania danych dotkniętych atakiem
Infrastruktura	Koszty wynagrodzeń personelu projektującego i wdrażającego elementy infrastruktury. Zakup urządzeń i wyposażenia technicznego (serwery, macierze dyskowe, zestawy	23 943 082,42 zł	„Modernizacja sprzętowa obejmująca serwery, macierze dyskowe i zestawy kryminalistyczne pozwala na wytworzenie i utrzymanie platformy do zarządzania incydentami i wymiany danych. Inwestycja jest kluczowa w kontekście realizacji kamieni milowych projektu.

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	kryminalistyczne, zapas nośników danych, sprzęt sieciowy i brzegowy)		
Koszty UX i grafiki	Koszty wynagrodzeń personelu wytwarzającego makiety systemu, projektującego i wdrażającego rozwiązania.	104 393,59 zł	Przejrzysty interfejs oraz czytelna warstwa graficzna zwiększają efektywność pracy użytkowników, zwłaszcza przy wieloetapowych procesach obsługi incydentów. Dzięki intuicyjnemu UX możliwe jest skrócenie czasu potrzebnego do poznania platformy i ograniczenie błędów ludzkich. Usprawnia to również współpracę międzyinstytucjonalną, gdy różne służby korzystają z jednego narzędzia.
Bezpieczeństwo	Zakup urządzeń oraz wynagrodzenia personelu konfigurujuącego elementy infrastruktury – sprzęt i usługi wytworzone w ramach projektu. Przeprowadzenie testów bezpieczeństwa, koszty utwardzania systemu i realizacji rekomendacji wynikających z przeprowadzonych testów.	332 765,42 zł	Środki na podniesienie poziomu bezpieczeństwa pozwalają uniknąć wycieku danych i nieautoryzowanego dostępu. W kontekście incydentów ransomware, a także krytycznych danych przetwarzanych w systemie, zabezpieczenie kluczowych systemów jest absolutnym priorytetem. Te inwestycje obniżają ryzyko strat finansowych i wizerunkowych. Środki na przeprowadzenie testów bezpieczeństwa.
Wydajność rozwiązań	Wynagrodzenie personelu odpowiadającego za optymalizacji wydajności wprowadzanych rozwiązań oraz przeprowadzenie analizy obciążenia i skalowalności systemów w kontekście przetwarzania	201 240,65 zł	Zapewnienie wydajności wdrażanych systemów (poprzez zapewnienie odpowiedniej mocy obliczeniowej) gwarantuje szybką sprawne działanie systemu zarządzania i współdzielenia incydentów i sprawniejszą reakcję na zagrożenia. Bez odpowiednich parametrów pracy narzędzi, podmioty nie będą w stanie obsłużyć rosnącej liczby zgłoszeń. Skalowalna architektura zapobiega

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	danych dowodowych.		utrudnieniom i utrzymuje stabilność usług w sytuacjach krytycznych. Środki na przeprowadzenie testów wydajności.
Szkolenia	Wynagrodzenia personelu realizującego szkolenia i przygotowującego materiały szkoleniowe. Zaawansowane kursy dla specjalistów zajmujących się cyberbezpieczeństwem.	6 477 785,65 zł	Rozwój kompetencji personelu w zakresie nowoczesnych technik analizy incydentów i odzyskiwania danych stanowi klucz do skutecznej reakcji na ataki i zapewnienia ciągłości działania systemów. Szkolenia m.in. BTL oraz SANS to rozpoznawalny standard branżowy, gwarantujący wysoki poziom wiedzy specjalistycznej. Materiały szkoleniowe.
Działania informacyjno-promocyjne	Promocja i informacja (materiały i koszty inne)	669 484,09 zł	Prezentacje i wystąpienia poszerzające świadomość o zagrożeniach cyberbezpieczeństwa wśród interesariuszy (instytucje publiczne, sektor biznesowy), a także wymiana doświadczeń z innymi krajowymi i międzynarodowymi ekspertami.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Wyjazdy służbowe związane z realizacją projektu (np. spotkania koordynacyjne, wizyty w innych jednostkach oraz wynagrodzenie personelu zarządzającego i wspomagającego. Zawiera również koszty pośrednie w wysokości 6% od wszystkich kosztów bezpośrednich.	3 323 746,33 zł	Prawidłowe zarządzanie projektem wymaga koordynacji działań między różnymi interesariuszami (Policja, Prokuratura, CSIRT NASK), co wiąże się z koniecznością odbywania delegacji. Dzięki temu możliwe jest ustalenie spójnych procedur i skoordynowanie planu wdrożenia nowych rozwiązań. Koszty pośrednie, w tym m.in. koszty personelu obsługowego, koszty utrzymania powierzchni biurowych, opłaty za energię i wodę, koszty materiałów biurowych, prowadzenia rachunków, ochrony czy sprzątnia.

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

<b>Całkowity koszt utrzymania trwałości projektu (brutto)</b>	6 473 814,67 zł		<b>Źródło finansowania</b>
<b>Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto)</b>	2026	504 949,78 zł (brutto) (488 849,78 zł netto)	krajowe środki publiczne - budżet państwa
	2027	1 110 889,51 zł (brutto) (1 075 469,51 zł netto)	krajowe środki publiczne - budżet państwa
	2028	1 221 978,46 zł (brutto) (1 183 016,46 zł netto)	krajowe środki publiczne - budżet państwa
	2029	1 344 176,31 zł (brutto) (1 301 318,11 zł netto)	krajowe środki publiczne - budżet państwa
	2030	1 478 593,94 zł (brutto) (1 431 449,92 zł netto)	krajowe środki publiczne - budżet państwa
	2031	813 226,67 zł (brutto) (787 297,45 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
Brak możliwości zatrudnienia osób o odpowiednich kompetencjach	Duża	Średnie	Współpraca z uczelniami technicznymi i ośrodkami szkoleniowymi, dostosowanie polityki wynagrodzeń do konkurencyjnych stawek rynkowych.
Brak wystarczających zasobów	Duża	Średnie	Przesunięcie wewnętrznych zasobów, outsourcing części zadań, uwzględnienie elastycznych form współpracy (np.

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
kadrowych do realizacji projektu			umowy eksperckie, kontrakty krótkoterminowe).
Przekroczenie harmonogramu realizacji projektu	Duża	Średnie	Monitorowanie postępów w cyklach kwartalnych, wprowadzenie buforów czasowych, zapewnienie dodatkowego wsparcia kadrowego w kluczowych momentach projektu.
Nieosiągnięcie wskaźników produktu oraz celu projektu	Duża	Niskie	Bieżąca kontrola postępów i raportowanie w odniesieniu do KPI, dostosowanie działań projektowych w razie ryzyka nieosiągnięcia założeń.
Przekroczenie budżetu projektu	Duża	Niskie	Ścisła kontrola kosztów, bufor finansowy, monitorowanie kluczowych wydatków na bieżąco.
Opóźnienia w pozyskaniu sprzętu i oprogramowania wynikające z utrudnień procesu zakupowego w PZP, ryzyka odwołań do KIO, chwilowego braku dostępności wybranego sprzętu.	Średnia	Średnie	Ujęcie w harmonogramie dodatkowego czasu na dostawę sprzętu. Przydzielenie dodatkowych zasobów do realizacji procesów zakupowych
Opóźnienie we wdrożeniu metodyki przez CBZC / Policję oraz innych partnerów / podmioty KSC	Duża	Średnie	Wyznaczenie koordynatora: Osoby odpowiedzialnej za przepływ informacji między wszystkimi zaangażowanymi instytucjami.
Brak możliwości pełnej realizacji projektu w planowanych ramach czasowych Ograniczenia wynikające z czasu trwania projektu i kwalifikowalności wydatkowania	Duża	Średnie	Zapewnić kontynuację przedsięwzięcia z innego źródła finansowania

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
środków			
Zmiany regulacyjne i prawne	Duża	Niskie	<p>Monitoring legislacyjny: Wyznaczenie osoby lub zespołu śledzącego na bieżąco zmiany w prawie krajowym i unijnym.</p> <p>Elastyczne zapisy w dokumentacji projektowej: Umieszczenie klauzul o możliwej modyfikacji zakresu w razie istotnych zmian przepisów.</p> <p>Konsultacje z ekspertami prawnymi: Regularna weryfikacja projektu pod kątem zgodności z nowymi regulacjami (np. NIS2/ Nowelizacja KSC).</p>

## 5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Zmiana kształtu KSC (np. ograniczenie kompetencji CSIRT NASK)	Duża	Znikome	<ul style="list-style-type: none"> <li>- Ustanowienie dedykowanego zespołu lub koordynatora do bieżącego śledzenia prac nad ustawą o KSC (w tym potencjalnych nowelizacji) oraz analizowania ich konsekwencji dla projektu.</li> <li>- Regularne konsultacje z przedstawicielami administracji rządowej i innych interesariuszy (np. Ministerstwo Cyfryzacji, KPRM), aby jak najwcześniej uzyskać informacje o proponowanych zmianach w kompetencjach CSIRT NASK.</li> <li>- Wprowadzenie do umów klauzul o utrzymaniu i rozwoju rozwiązań w zakresie cyberbezpieczeństwa niezależnie od modyfikacji przepisów regulujących status jednego uczestnika systemu.</li> </ul>
Brak możliwości zatrudnienia osób o odpowiednich kompetencjach niezbędnych do utrzymania	Duża	Średnie	Utworzenie długoterminowej ścieżki kariery dla kluczowych ekspertów, współpraca z ośrodkami edukacyjnymi, programy szkoleniowe dla pracowników.



Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
efektów projektu			
Brak wystarczających zasobów kadrowych do utrzymania efektów projektu	Duża	Średnie	Zabezpieczenie etatów w ramach budżetu operacyjnego, elastyczne modele zatrudnienia, rotacja pracowników w ramach różnych zespołów.
Brak wystarczających środków na utrzymanie efektów projektu	Duża	Średnie	Opracowanie długoterminowego planu finansowania, zabezpieczenie środków w budżecie państwa lub w ramach funduszy UE.
Niska adopcja nowego systemu przez użytkowników końcowych	Średnia	Średnie	Intensywne szkolenia dla użytkowników, uproszczona dokumentacja, wsparcie techniczne po wdrożeniu.
Nieosiągnięcie wszystkich zaplanowanych korzyści	Duża	Niskie	Regularna ewaluacja rezultatów projektu, wdrożenie planu optymalizacji i doskonalenia wypracowanych narzędzi.

## 6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC) (Dz.U.2024.1077 t.j. z dnia 2024.07.19)	TAK/NIE		
2	DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U.U.E.L.2022.333.80 z dnia 2022.12.27)	TAK/NIE		
3	Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie przyjęcia	TAK/NIE		

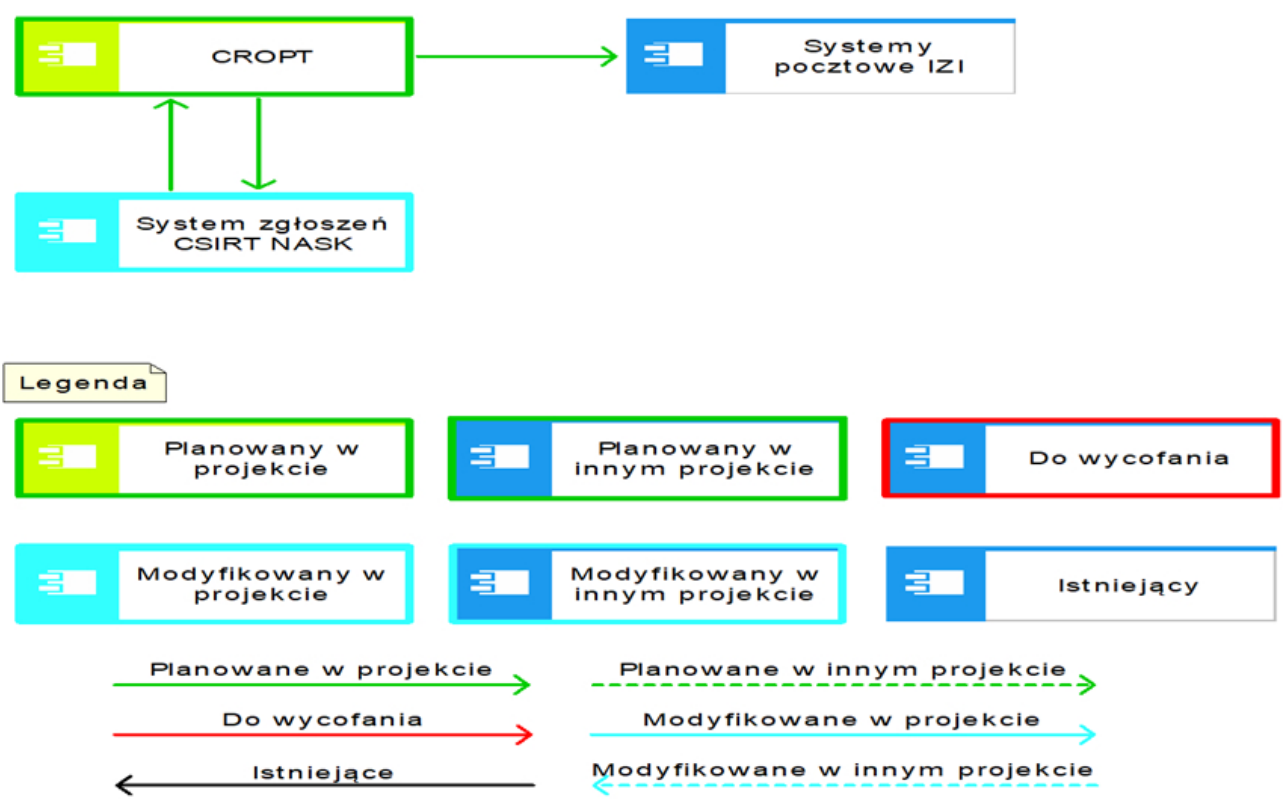
Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (uchwała nr 125/2019) (M.P.2019.1037 z dnia 2019.10.30)			
4	Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U.2024.145 t.j. z dnia 2024.02.06)	<del>TAK</del> /NIE		
5	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2024.1557 t.j. z dnia 2024.10.21)	<del>TAK</del> /NIE		
6	Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2024.773 z dnia 2024.05.22)	<del>TAK</del> /NIE		
7	Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. z 2019 r. poz. 2479)	<del>TAK</del> /NIE		
8	Krajowy Plan Odbudowy i Zwiększania Odporności (KPO), Komponent C3.1.1 – „Cyberbezpieczeństwo – CyberPL”	<del>TAK</del> /NIE		
9	Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U.2024.1320 t.j. z dnia 2024.08.30)	<del>TAK</del> /NIE		
10	Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46)	<del>TAK</del> /NIE		
11	Rozporządzenie Prezesa Rady Ministrów z dnia 26 kwietnia 2023 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U.2011.159.948 z dnia 2011.08.01)	<del>TAK</del> /NIE		
12	Rozporządzenie Prezesa Rady Ministrów z dnia 14 października 2023 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy,	<del>TAK</del> /NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	wzorów i kopii dokumentów elektronicznych (Dz. U. z 2023 r. poz. 1023)			
13	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 - RODO) (Dz.U.UE.L.2016.119.1 z dnia 2016.05.04)	<del>TAK</del> /NIE		
14	Ustawa z dnia 27 lipca 2001 r. o ochronie baz Danych (Dz.U.2024.1769 t.j. z dnia 2024.12.03)	<del>TAK</del> /NIE		
15	Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U.2023.1524 t.j. z dnia 2023.08.04)	<del>TAK</del> /NIE		
16	Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U.2023.1440 t.j. z dnia 2023.07.27)	<del>TAK</del> /NIE		
17	Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz.U.2025.311 t.j. z dnia 2025.03.13)	<del>TAK</del> /NIE		
18	Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U.2024.1045 t.j. z dnia 2024.07.16)	<del>TAK</del> /NIE		
19	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U.2024.1725 t.j. z dnia 2024.11.25)	<del>TAK</del> /NIE		
20	Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie profilu zaufanego i podpisu zaufanego (Dz.U.2023.2551 t.j. z dnia 2023.11.24)	<del>TAK</del> /NIE		
21	Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz.U.2020.399 z dnia 2020.03.11)	<del>TAK</del> /NIE		
22	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2019.1781 t.j. z dnia 2019.09.19)	<del>TAK</del> /NIE		
23	Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2024.632 t.j. z	<del>TAK</del> /NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	dnia 2024.04.25)			

## 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	CSIRT NASK	Centralny system preanalityczny do współdzielenia materiałów związanych z postępowaniami prowadzonymi przez	Planowany	

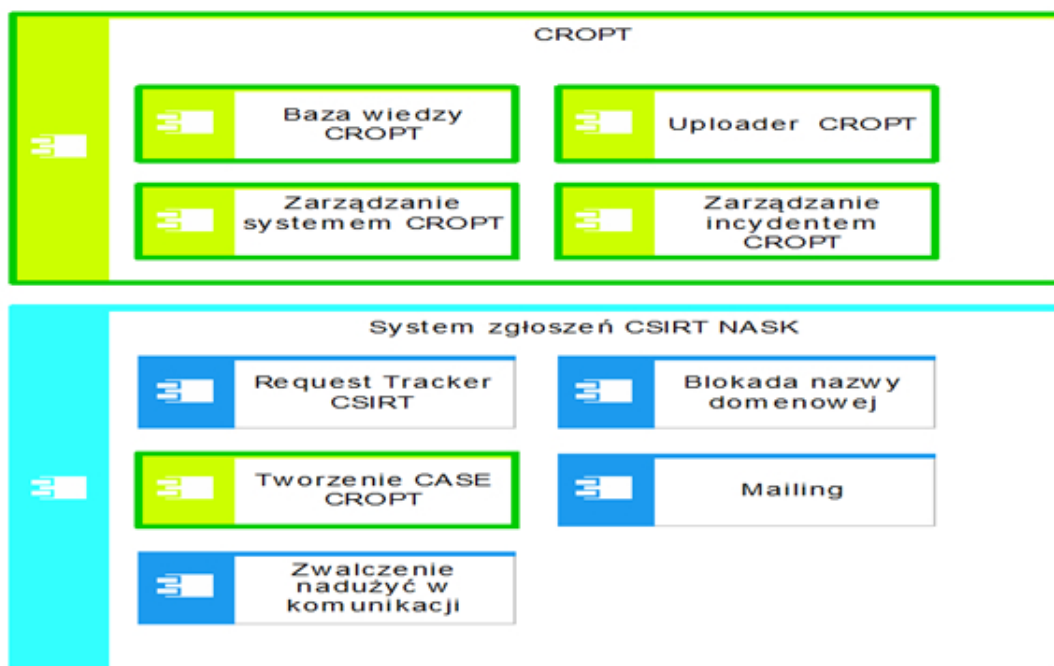
Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			zespoły reagowania i analityków. Umożliwia szybkie i bezpieczne przekazywanie zabezpieczonego materiału związanego z prowadzonymi działaniami mających na celu analizę zaistniałego incydentu. Umożliwia współdzielenie materiału oraz wymianę informacji dotyczących ustaleń i wyników analiz. Posiada możliwość zarządzania rolą i uprawnieniami dostępu do wspomnianego materiału, jak i do ustaleń związanych z prowadzoną analizą. System ma obejmować kilka komponentów: CORE – zarządzanie systemem, CASE – zarządzanie incydemtem, UPLOADER – transfer materiałów, Baza wiedzy - moduł pomagający użytkownikowi przejść przez zabezpieczanie materiału, dostarczający informacji jak korzystać z systemu.		
2	System zgłoszeń CSIRT NASK	CSIRT NASK	Bazowy system (pracujący w oparciu o silnik którym jest Request Tracker) zarządzania zgłoszeniami nadsyłanymi do CSIRT NASK w myśl obowiązków ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U.2018 poz.1560). Podstawowe narzędzie pracy analityków operujących w trybie	Modyfikowany	Wytworzenie i implementacja modułu o nazwie `tworzenia CASE CROPT`, którego celem jest zagwarantowanie ciągłości operowania oraz porządkowania działań prowadzonych

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			7/24/365. Miejsce gdzie następuje kanalizacja informacji w przedmiocie przebiegu, a także rezultatu obsługiwanego incydentu.		w incydencie.
3	Systemy pocztowe IZI	Instytucje Zgłaszające Incydent (IZI)	Systemy poczty elektronicznej Instytucji Zgłaszających Incydent na które adresowana jest informacja z CROPT.	Istniejący	

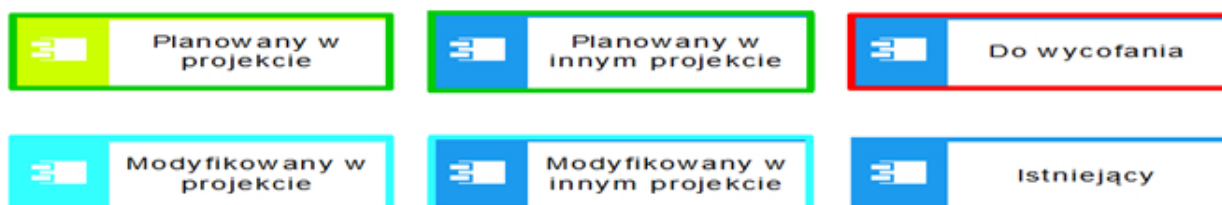
## Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	System zgłoszeń CSIRT NASK	CROPT	Numer identyfikacyjny sprawy zarejestrowanej przez operatora, dane IZI	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	Rest-api
2	CROPT	System zgłoszeń CSIRT NASK	Odesłanie do rezultatu prowadzonej analizy w CROPT	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	Rest-api
3	CROPT	Systemy pocztowe IZI	Informacje o statusie prowadzonej sprawy. Odesłanie do dedykowanego zasobu w ramach BAZY WIEDZY. Odesłanie do dedykowanego zasobu w ramach UPLOADERa	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	SMTP

## 7.2. Kluczowe komponenty architektury rozwiązania



#### Legenda



## 7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Wirtualizacja oparta o KVM, kubectl, docker
2.	Sieć i bezpieczeństwo	UTM, WAF, Firewall
3.	Standardy wymiany danych	Rest-api
4.	Systemy operacyjne serwerowe	Linux
5.	Bazy danych	PostgreSQL
6.	Serwery aplikacji	Python
7.	Portale	Python
8.	Inne	narzędzia kryptograficzne adekwatne do danych przetwarzanych w systemie tj. LUKS, OpenZFS native encryption, TLS

## 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~~
- ~~-dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie~~