

# OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Podłączenie podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem S46 (S46-react)		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	NASK PIB		
Partnerzy			
Źródło finansowania	Program Operacyjny Polska Cyfrowa, Oś priorytetowa V „Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU”		
Całkowity koszt projektu	29 802 581,25 zł		
Planowany okres realizacji projektu	09-2021 do 06-2023		
Osoba kontaktowa	Andrzej Skrzeczkowski	Andrzej.Skrzeczkowski@nask.pl	602411923

## 1. POWODY PODJĘCIA PROJEKTU

### 1.1. Identyfikacja problemu i potrzeb

Infrastruktura teleinformatyczna państwa – co szczególnie unaocznili okres pandemii – jest kluczową infrastrukturą dla gospodarki narodowej, administracji, zdrowia publicznego, kultury itp. Zatem jej ochrona powinna być traktowana jako ochrona istotnego interesu bezpieczeństwa państwa. Ochrona ta jest realizowana przez systemy zapewniające cyberbezpieczeństwo różnych podmiotów – na poziomie lokalnym. Skuteczne kierowanie ochroną cyberbezpieczeństwa wymaga także działań perymetrycznych ponadlokalnych, regionalnych, a także centralnych. Uruchomiony 1 stycznia 2021 roku system S46 ma za zadanie zarządzanie cyberbezpieczeństwem na poziomie państwa – realizując w ten sposób efektywne działanie krajowego systemu cyberbezpieczeństwa (KSC).

Z punktu widzenia Państwa, współdziałanie podmiotów krajowego systemu cyberbezpieczeństwa oraz udostępnianie jednostkom krajowym informacji o obrazie sytuacyjnym cyberbezpieczeństwa, ich ostrzeganie, jak i prewencyjne wskazywanie podatności jest jednym z podstawowych i istotnych zagadnień zwiększających holistycznie odporności systemu informacyjnego RP na działania naruszające bezpieczeństwo wewnętrzne i zewnętrzne. Istotnym problemem jaki się pojawia w działaniu systemu S46 jest zapewnienie dostępu do niego szerokim grupom ważnych odbiorców – tworzących wspólnie spójny obraz cyberbezpieczeństwa w Polsce oraz nadążanie za wyzwaniami w niezwykle szybko zmieniającym się otoczeniu cyfrowym.

O tym, że problem cyberbezpieczeństwa staje się znaczącym wyzwaniem może świadczyć fakt, że JST i szpitale są obecnie celem ataków (ransomware), które rok do roku zwiększyły się o 60 procent.

Szczegółowe problemy, jakie zostały zidentyfikowane i które mają być rozwiązane przez realizację przedmiotowego projektu przedstawia tabela.

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

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Jednostki samorządu terytorialnego i jednostki im podległe (Urzędy Marszałkowskie, JST zarządzające większymi miastami, spółki wodno-kanalizacyjne itp.), urzędy współpracujące przy zagadnieniach związanych z cyberbezpieczeństwem JST, a także uczestniczące w zintegrowanym systemie zarządzania kryzysowego (Urzędy Wojewódzkie, RCB), większe szpitale	<ul style="list-style-type: none"> <li>Brak narzędzi do skutecznego zarządzania i dystrybucji informacji na temat cyberbezpieczeństwa w JST i ich jednostkach organizacyjnych</li> <li>Wysoki początkowy koszt podłączenia do s46</li> <li>Nie otrzymywanie ostrzeżeń o zagrożeniach i zagregowanej informacji o podatnościach – w sposób systemowy, zintegrowany – a przez to skuteczny</li> <li>Brak podłączenia do s46 wskazanych jednostek powoduje niepełny obraz sytuacji cyberbezpieczeństwa oraz ryzyka dynamicznego świadczonej usługi – w szczególności dla jednostek uczestniczących w zintegrowanym systemie zarządzania kryzysowego</li> </ul>	100
Przedstawiciele JST i jednostek im podległych, urzędów współpracujących przy zagadnieniach związanych z cyberbezpieczeństwem JST, a także uczestniczących w zintegrowanym systemie zarządzania kryzysowego (Urzędy Wojewódzkie, RCB)	<ul style="list-style-type: none"> <li>niewystarczający poziom wiedzy pracowników jednostek organizacyjnych samorządów terytorialnych oraz innych – wskazanych podmiotów o cyberbezpieczeństwie</li> <li>brak wiedzy pracowników jednostek organizacyjnych samorządów terytorialnych oraz innych – wskazanych podmiotów o sposobie funkcjonowania systemu S46</li> </ul>	200
Jednostka nadzorująca i budująca System S46	Dołączenie jednostek przewidywanych w projekcie, skutkuje koniecznością modyfikacji i rozbudowy systemu S46 w celu modernizacji jego funkcjonalności, narzędzi podnoszących poziom bezpieczeństwa oraz zapewnienia ciągłości jego działania.	1

## 1.2. Opis stanu obecnego

Zobowiązanie do zbudowania systemu S46 jako strategicznego przedsięwzięcia zostało wprowadzone w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. 2020 poz. 1369) – dalej „Ustawa”. W art. 89 Ustawy nałożono na ministra właściwego do spraw informatyzacji zadanie polegające na utworzeniu i udostępnieniu systemu teleinformatycznego wymienionego w art. 46 ust. 1, wspierającego koordynację działań i współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa,

wypracowanie i przekazywanie rekomendacji podnoszących poziom cyberbezpieczeństwa, zapewnienie zgłaszania incydentów i umożliwiającego wspomaganie ich łagodzenia przez CSIRT GOV, CSIRT MON, CSIRT NASK oraz ostrzegania o zagrożeniach cyberbezpieczeństwa podmiotów KSC i zapewniającego obserwację ryzyka na poziomie krajowym.

W 2019 r. NASK PIB zostało zlecone zadanie publiczne polegające na „rozwoju systemu teleinformatycznego”, którego celem było dostosowanie produktów projektu Narodowej Platformy Cyberbezpieczeństwa do wymagań Ustawy. W dniu 01.01.2021 r. system S46 został uruchomiony operacyjnie.

System S46 jest systemem wydzielonym i ma charakter zamknięty. Składa się z redundantnego systemu centralnego, wydzielonej sieci teleinformatycznej opartej na MPLS, podłączonych z jej wykorzystaniem uczestników (z zainstalowanymi u nich urządzeniami dostępowymi – SBU) oraz podłączonymi do systemu centralnego podmiotami KSC: CSIRT GOV, CSIRT MON, CSIRT NASK, organami właściwymi, Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa i innymi.

## 2. EFEKTY PROJEKTU

### 2.1. Cele i korzyści wynikające z projektu

<b>Cel - 1</b>	Zwiększenie liczby podmiotów krajowego systemu cyberbezpieczeństwa podłączonych do S46.
<b>Cel strategiczny</b>	<p>Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:</p> <p>1/ Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP) w odniesieniu do celu 4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office) oraz 4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej</p> <p>2/ Cele Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, w szczególności celu szczegółowego nr 1 – Rozwój krajowego systemu cyberbezpieczeństwa. Cel ten powinien być realizowany poprzez wdrożenie systemowego rozwiązania pozwalającego na wymianę informacji, w tym dotyczącego, podatności, zagrożeń i incydentów. Ponadto, wskazuje się na konieczność wdrożenia na poziomie krajowym dynamicznego i statycznego szacowania ryzyka w obszarze cyberbezpieczeństwa. Cele te realizuje zintegrowany system zarządzania cyberbezpieczeństwem – system S46.</p> <p>3/ Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU. Zwiększenie liczby połączeń do systemu S46 wraz z przeszkoleniem użytkowników i tym samym wzrost poziomu cyberbezpieczeństwa RP, wpisuje się bezpośrednio w zakres osiągnięcia wyżej wymienionych celów strategicznych.</p>
<b>Korzyść:</b>	<ol style="list-style-type: none"><li>osiągnięcie synergii poprzez włączenie do systemu dużej liczby podmiotów</li><li>Usprawnienie, upowszechnienie i udrożnienie wymiany informacji na temat cyberbezpieczeństwa dla wskazanych podmiotów.</li><li>Podniesienie skuteczności monitorowania ryzyk wiążących się z działaniem w cyberprzestrzeni RP znacznej liczby podmiotów publicznych.</li></ol>
<b>KPI:</b>	Liczba JST, które zwiększyły swój potencjał cyfrowy.
<b>Wartość aktualna i</b>	100

<b>docelowa KPI:</b>	
<b>Metoda pomiaru KPI</b>	Liczba protokołów instalacji systemów brzegowych dla JST, jednostek otoczenia JST i należących do JST, zarejestrowanych w systemach dokumentacyjnych NASK, pomiar na koniec każdego kwartału kalendarzowego.
<b>Cel - 2</b>	Zwiększenie liczby podmiotów krajowego systemu cyberbezpieczeństwa posiadających umiejętność posługiwania się systemem S46.
<b>Cel strategiczny</b>	<p>Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:</p> <p>1/ Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP) w odniesieniu do celu 4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office) oraz 4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej.</p> <p>2/ Cele Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, w szczególności celu szczegółowego nr 1 – Rozwój krajowego systemu cyberbezpieczeństwa. Cel ten powinien być realizowany poprzez wdrożenie systemowego rozwiązania pozwalającego na wymianę informacji, w tym dotyczącego, podatności, zagrożeń i incydentów. Ponadto, wskazuje się na konieczność wdrożenia na poziomie krajowym dynamicznego i statycznego szacowania ryzyka w obszarze cyberbezpieczeństwa. Cele te realizuje zintegrowany system zarządzania cyberbezpieczeństwem – system S46.</p> <p>3/ Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU Zwiększenie liczby połączeń do systemu S46 wraz z przeszkoleniem użytkowników i tym samym wzrost poziomu cyberbezpieczeństwa RP, wpisuje się bezpośrednio w zakres osiągnięcia wyżej wymienionych celów strategicznych.</p>
<b>Korzyść:</b>	<p>Projekt zapewni:</p> <ol style="list-style-type: none"> <li>1. Poszerzenie wiedzy podłączanych jednostek w sferze zasad i sposobów wymiany informacji na temat cyberbezpieczeństwa, a także wykorzystania tych informacji w bieżącej działalności. W ramach projektu S46-REACT planuje się przeprowadzenie szkoleń dotyczących wykorzystania systemu S46.</li> <li>2. Zwiększenie świadomości sytuacyjnej podłączanego podmiotu oraz umożliwienie monitorowania ryzyk wiążących się z działaniem w cyberprzestrzeni – poprzez nadanie dostępu do S46 (cel 1) wraz z przeszkoleniem.</li> </ol>
<b>KPI:</b>	Liczba pracowników objętych szkoleniami w zakresie umiejętności cyfrowych.
<b>Wartość aktualna i docelowa KPI:</b>	200
<b>Metoda pomiaru KPI</b>	Lista osób przeszkolonych z używania Systemu S46 zarejestrowanych w systemach dokumentacyjnych NASK, pomiar na koniec każdego kwartału kalendarzowego.
<b>Cel - 3</b>	Zwiększenie poziomu bezpieczeństwa systemu S46 i zapewnienie obsługi zwiększonej liczby połączeń.
<b>Cel</b>	Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:

<b>strategiczny</b>	<p>1/ Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP) w odniesieniu do celu 4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office) oraz 4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej.</p> <p>2/ Cele Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, w szczególności celu szczegółowego nr 1 – Rozwój krajowego systemu cyberbezpieczeństwa. Cel ten powinien być realizowany poprzez wdrożenie systemowego rozwiązania pozwalającego na wymianę informacji, w tym dotyczącego, podatności, zagrożeń i incydentów. Ponadto, wskazuje się na konieczność wdrożenia na poziomie krajowym dynamicznego i statycznego szacowania ryzyka w obszarze cyberbezpieczeństwa. Cele te realizuje zintegrowany system zarządzania cyberbezpieczeństwem – system S46.</p> <p>3/ Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU Zapewnienie obsługi zwiększonej liczby połączeń i zwiększenie bezpieczeństwa Systemu S46, wpisuje się pośrednio w zakres wyżej wymienionych celów strategicznych przez zapewnienie możliwości połączenia do S46, a przez to wzrost poziomu bezpieczeństwa RP.</p>
<b>Korzyść:</b>	<p>System S46 będzie zmodernizowany, dzięki czemu zapewni:</p> <ul style="list-style-type: none"> <li>a) wzmocnienie bezpieczeństwa poprzez zastosowanie zaawansowanych systemów bezpieczeństwa teleinformatycznego;</li> <li>b) podniesienie odporności na katastrofy usług;</li> <li>c) wzmocnienie stabilności S46 poprzez wykorzystanie platform systemowych i wirtualizacyjnych systemów posiadających stałe i gwarantowane wsparcie;</li> <li>d) zwiększenie odporności S46 w stanach nadzwyczajnych poprzez zwiększenie redundancji geograficznej centrów;</li> <li>e) zwiększenie wydajności i skuteczności obsługi Systemu S46 przez wyposażenie w centrum monitorowania SOC/NOC;</li> <li>f) podniesienie skuteczności i reaktywne wdrażanie nowych wersji oprogramowania, poprawek bezpieczeństwa itp. poprzez doposażenie środowisk testowych i deweloperskich w rozwiązania wykorzystywane na środowisku produkcyjnym systemu S46;</li> <li>g) przyspieszenie naprawy dla zwiększonego grona użytkowników Systemu S46 poprzez zakup puli urządzeń zapasowych.</li> </ul>
<b>KPI:</b>	Liczba wdrożonych systemów IT w obszarze cyberbezpieczeństwa.
<b>Wartość aktualna i docelowa KPI:</b>	1
<b>Metoda pomiaru KPI</b>	Protokół odbioru zmodernizowanego systemu S46 udokumentowany w systemach ewidencji majątku – pomiar na koniec każdego kwartału kalendarzowego.
<b>Cel - 4</b>	Zapewnienie trwałego wsparcia gospodarki w dziedzinie cyberbezpieczeństwa na wypadek zagrożeń – w tym epidemicznych.
<b>Cel strategiczny</b>	<p>Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:</p> <p>1/ Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP) w odniesieniu do celu 4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back</p>

	<p>office) oraz 4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej.</p> <p>2/ Cele Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, w szczególności celu szczegółowego nr 1 – Rozwój krajowego systemu cyberbezpieczeństwa. Cel ten powinien być realizowany poprzez wdrożenie systemowego rozwiązania pozwalającego na wymianę informacji, w tym dotyczącego, podatności, zagrożeń i incydentów. Ponadto, wskazuje się na konieczność wdrożenia na poziomie krajowym dynamicznego i statycznego szacowania ryzyka w obszarze cyberbezpieczeństwa. Cele te realizuje zintegrowany system zarządzania cyberbezpieczeństwem – system S46.</p> <p>3/ Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU Zapewnienie obsługi zwiększonej liczby podłączeń z przeszkoleniem użytkowników i zwiększenie bezpieczeństwa Systemu S46, wpisuje się pośrednio w zakres wyżej wymienionych celów strategicznych przez zapewnienie możliwości podłączenia do S46. Wpisuje się to w zapewnienie odporności państwa i gospodarki na cyberzagrożenia specyficzne dla okresu wymagającego stabilnego i intensywnego wykorzystania infrastruktury ICT – szczególnie w okresie pandemii.</p>
<b>Korzyść:</b>	Podniesienie reaktywności na zagrożenia cyberbezpieczeństwa dzięki realizacji zadań inwestycyjnych, poprzez uzyskanie bazy składającej się na środki trwałe i wartości niematerialne i prawne, które umożliwią osiągnięcie celów systemu S46 w sytuacjach ewentualnych przyszłych zagrożeń – co wynika z doświadczeń zebranych w okresie epidemii COVID-19
<b>KPI:</b>	Wartość sprzętu IT oraz oprogramowania/licencji finansowanych w odpowiedzi na COVID-19 - inne obszary
<b>Wartość aktualna i docelowa KPI:</b>	12 490 000,00 zł
<b>Metoda pomiaru KPI</b>	Dokumenty księgowe potwierdzające wartość przyjętych na stan środków trwałych i wartości niematerialnych i prawnych (wartości netto). Pomiar na koniec każdego kwartału kalendarzowego.

## 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
Zakupione oraz udostępnione zainteresowanym instytucjom materiały promocyjne i szkoleniowe	06-2023
Zainstalowane i uruchomione systemy brzegowe Systemu S46	06-2023
Przeprowadzone szkolenia dla użytkowników	06-2023
Zmodernizowany System S46 (zakupiona i uruchomiona infrastruktura oraz oprogramowanie)	06-2023

## 3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Rozstrzygnięcie postępowanie na sukcesywną dostawę urządzeń i oprogramowania bazowego systemów brzegowych s46	2021-12-31
Dostawa urządzeń i oprogramowania bazowego systemów brzegowych s46 oraz ich instalacja i uruchomienie dla 10 jednostek, które w ten sposób zostaną podłączone (narastająco) oraz przeszkolone 20 osób (narastająco)	2022-03-31
Rozstrzygnięcie postępowania zakupowego w zakresie dostawy nowej platformy wirtualizacyjnej, urządzeń i oprogramowania do rozwoju środowiska deweloperskiego oraz puli urządzeń zapasowych	2022-06-30
Dostawa urządzeń i oprogramowania bazowego systemów brzegowych s46 oraz ich instalacja i uruchomienie dla 40 jednostek, które w ten sposób zostaną podłączone (narastająco) oraz przeszkolone 80 osób (narastająco)	2022-09-30
Rozbudowany system S46 (zainstalowana i uruchomiona infrastruktura i oprogramowanie) w zakresie nowej platformy wirtualizacyjnej, rozwoju środowiska deweloperskiego i puli urządzeń zapasowych	2022-12-31
Rozstrzygnięcie postępowania zakupowego w zakresie dostawy infrastruktury i oprogramowania: zaawansowanych systemów bezpieczeństwa teleinformatycznego, narzędzi podnoszących odporność na katastrofy usług, zwiększających redundancję geograficzną centrów oraz wyposażenia centrum monitorowania SOC/NOC	2022-12-31
Dostawa urządzeń i oprogramowania bazowego systemów brzegowych s46 oraz ich instalacja i uruchomienie dla 80 jednostek, które w ten sposób zostaną podłączone (narastająco) oraz przeszkolone 160 osób (narastająco)	2023-03-31
Dostawa urządzeń i oprogramowania bazowego systemów brzegowych s46 oraz ich instalacja i uruchomienie dla 100 jednostek, które w ten sposób zostaną podłączone (narastająco) oraz przeszkolone 200 osób	2023-06-30

Kamienie milowe	Planowany termin osiągnięcia
(narastająco)	
Zrealizowana rozbudowa Systemu S46 – zainstalowane i uruchomione wszystkie systemy	2023-06-30

## 4. KOSZTY

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

Całkowity koszt projektu (netto oraz brutto), w tym	Netto 25 732 875,00 zł Brutto 29 802 581,25 zł	
Procent dofinansowania ze środków UE (brutto)	100%	
Procent środków z budżetu państwa (brutto)		
Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto)	2021	Netto 1 749 323,16 zł Brutto 1 947 261,89 zł
	2022	Netto 12 450 268,26 zł Brutto 14 289 262,76 zł
	2023	Netto 11 533 283,58 zł Brutto 13 566 056,60 zł

### 4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Zakup licencji na oprogramowanie komercyjne, wytworzenie oprogramowania w NASK PIB	6 351 657,00 zł	Modernizacja systemu
Infrastruktura	Zakup urządzeń i wyposażenia, usług instalacji, usług umożliwiających działanie, instalacja i wdrożenie	13 542 651,00 zł	Systemy i usługi związane z podłączanymi podmiotami, systemy i usługi rozbudowywanego systemu S46
Koszty UX i grafiki	Nie dotyczy	0,00 zł	W ramach projektu nie będzie



Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
			tworzona nowa szata graficzna dla S46, albo jego komponentów, gdyż są to zadania leżące w zakresie innego projektu (dotacyjnego).
Bezpieczeństwo	Zakup na cele dodatkowego centrum zapasowego, systemów zaawansowanego bezpieczeństwa teleinformatycznego , instalacja i wdrożenie	3 953 214,00 zł	Zapewnienie ciągłości działania i zaawansowane zabezpieczenie systemu
Wydajność rozwiązań	Zakup wyposażenia rozszerzonego centrum zarządzania, rozszerzenia środowiska wdrożeniowo – deweloperskiego oraz zapasowych urządzeń	3 351 996,00 zł	Umożliwienie sprawnej obsługi zgłoszeń użytkowników i sprawna modernizacja systemu umożliwi osiągnięcie jego wysokiej dostępności i dużej wydajności
Szkolenia	Wynagrodzenia i materiały konieczne do przeprowadzenia szkoleń użytkowników systemu	803 850,00 zł	Użytkownicy systemu (szczególnie nowi) muszą uzyskać odpowiednią informację o możliwości sprawnego użycia systemu S46.
Działania informacyjno-promocyjne	Promocja i informacja (materiały i koszty inne)	316 110,00 zł	Konieczne jest zachęcenie – przez promocję i informację – jednostek do podłączenia się do systemu (podłączenie nie jest obligatoryjne)
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Koszty pośrednie	1 483 103,25 zł	Koszty wynajmu biura do celów realizacji projektu, mediów i materiałów koniecznych do działania biura (bez wyposażenia stanowisk pracy przeznaczonych w co najmniej 50% do realizacji obsługi rozbudowanego Systemu S46, ujętego w kosztach bezpośrednich), zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)

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

Całkowity koszt utrzymania trwałości projektu (brutto)	17 137 482,90 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto)	2023	1 489 860,00 zł (brutto) (1 248 666,67 zł netto)	krajowe środki publiczne - budżet państwa
	2024	2 979 720,00 zł (brutto) (2 497 333,33 zł netto)	krajowe środki publiczne - budżet państwa
	2025	2 979 720,00 zł (brutto) (2 497 333,33 zł netto)	krajowe środki publiczne - budżet państwa
	2026	3 015 193,20 zł (brutto) (2 526 173,33 zł netto)	krajowe środki publiczne - budżet państwa
	2027	3 726 858,90 zł (brutto) (3 104 763,33 zł netto)	krajowe środki publiczne - budżet państwa
	2028	2 946 130,80 zł (brutto) (2 432 626,67 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
Niechęć podmiotów KSC do podłączania do	Duża	Średnie	Łagodzenie – zwiększenie listy potencjalnie zainteresowanych podmiotów w stosunku do zamierzonej

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
S46			liczby połączeń Akceptacja – wykonywanie specjalnych działań promocyjnych (dodatkowe warsztaty, pokazy, wskazanie przykładu innych) w stosunku do podmiotów wyrażających wątpliwości
Brak odpowiedniej infrastruktury teleinformatycznej podłączanych podmiotów	Średnia	Niskie	Łagodzenie – zastosowanie w projekcie rozwiązań umożliwiających skorzystanie z systemu przy minimalnych środkach technicznych od strony podłączanej jednostki (np. terminal PC).
Wzrost kursu	Średnia	Średnie	Przeniesienie – realizacja postępowań zakupowych odpowiednio wcześniej i z odpowiednim budżetem, tak aby dodatkowe ryzyko przenieść na Wykonawcę. Mitygacja - zawarcie w umowie z wykonawcą stosownych klauzul w zakresie zmian wpływających na wysokość wynagrodzenia za realizację przedmiotu zamówienia.
Niedostępność rozwiązań związana np. z problemami epidemiologicznymi	Duża	Średnie	Unikanie – zmiany w harmonogramie projektu i dostosowanie go do realizujących się ryzyk. Mitygacja – poszukiwanie rozwiązań alternatywnych, które mogą być stosowane do zastąpienia niedostępnych rozwiązań.

## 5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Brak chęci do użytkowania systemu S46 przez podłączone podmioty	Duża	Średnie	Akceptacja – podejmowanie działań zaradczych na bieżąco Przeniesienie – zaangażowanie innych podmiotów w uświadamianie roli systemu S46
Zmiany legislacyjne, modyfikujące zadania systemu s46	Duża	Średnie	Akceptacja – podejmowanie działań zaradczych na bieżąco Unikanie – kontakt z legislatorami poprzez właściciela biznesowego systemu, w celu wprowadzenia

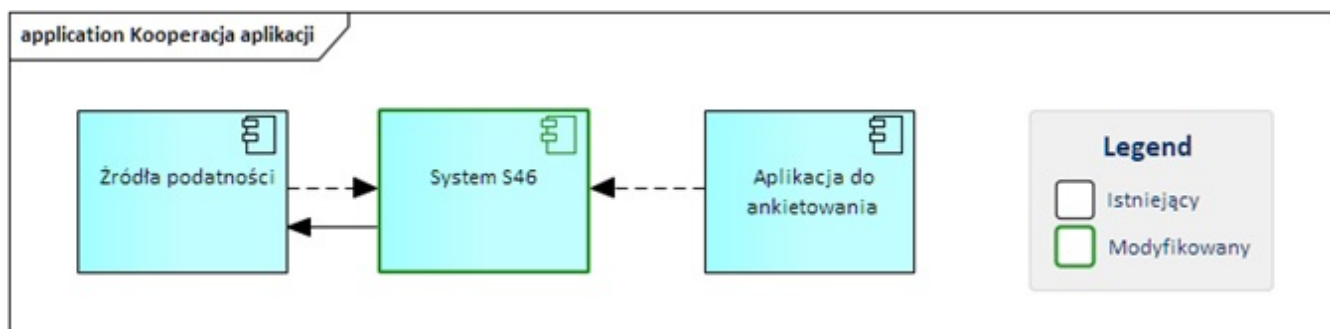
Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
			poprawek redukujących ryzyko.

## 6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (t. j. Dz. U. 2020 poz. 1369)	TAK/NIE		
2	Uchwała RM z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024	TAK/NIE		
3	Ustawa z dnia 17 lutego 2005 o Informatyzacji działalności podmiotów realizujących zadania publiczne	TAK/NIE		
4	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów informatycznych	TAK/NIE		

## 7. ARCHITEKTURA

### 7.1. Widok kooperacji aplikacji



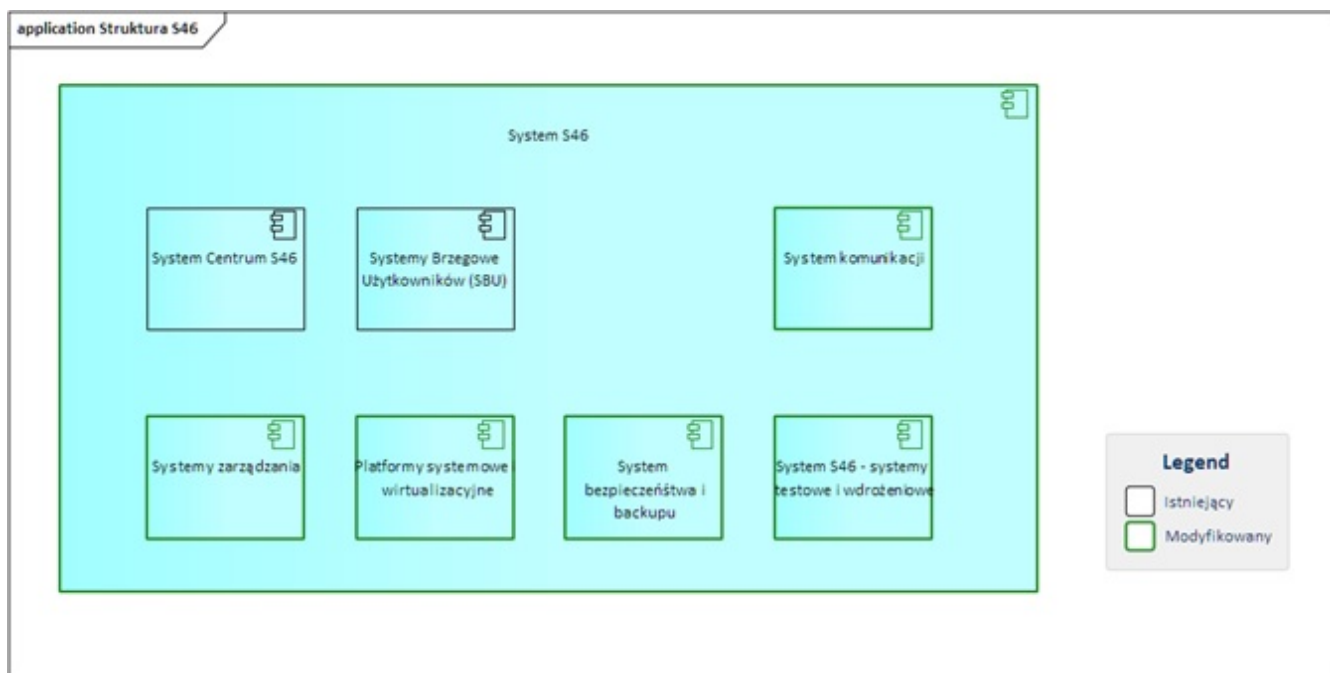
## Lista systemów wykorzystywanych w projekcie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	System S46	Minister Cyfryzacji/ KPRM	System realizujący założenia systemu teleinformatycznego z art. 46 ust. 1 Ustawy	Modyfikowany	Zwiększenie bezpieczeństwa i sprawności działania systemu
2	Źródła podatności	Podmioty komercyjne, społeczność	Źródła podatności takie jak MISP czy VULN	Istniejący	Brak
3	Aplikacja do ankietowania	Minister Cyfryzacji/ KPRM	Aplikacja przeznaczona do zbierania informacji o świadczonych usługach o podmiotach niepodłączonych bezpośrednio	Istniejący	Brak

## Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	System S46	Źródła podatności	Inicjowanie komunikacji, specyfikacja pobieranych podatności	tryb odwołań bezpośrednich - usługi sieciowe REST, kolejki	Krytyczny dla sukcesu projektu	Automatyczna wymiana
2	Źródła podatności	System S46	Informacje o podatnościach	tryb odwołań bezpośrednich - usługi sieciowe REST, kolejki	Krytyczny dla sukcesu projektu	Automatyczna wymiana
3	Aplikacja do ankietowania	System S46	Informacje o usługach, poziomach ryzyka	kopiowanie danych - plików	Krytyczny dla sukcesu projektu	Plikowy

## 7.2. Kluczowe komponenty architektury rozwiązania



## 7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Systemy zgodne z dotychczas używanymi (podłączenie w oparciu o serwery Dell R440 lub podobne, po zatwierdzeniu do użytkowania)
2.	Sieć i bezpieczeństwo	Sieć oparta o dedykowane włókna światłowodowe (z MACSec) i transmisje w części centralnej, podłączenie przez dwa MPLS L3VPN, szyfrowanie IPSec, SSL, rozbudowa w kierunku SOAR, RASP. PAM i innych rozwiązań, aplikacji analizy ruchu itp.
3.	Standardy wymiany danych	Zgodnie z istniejącym rozwiązaniem – nie podlega modyfikacji
4.	Systemy operacyjne serwerowe	Przebudowa w kierunku RedHat, Vmware
5.	Bazy danych	Zgodnie z istniejącym rozwiązaniem – nie podlega modyfikacji
6.	Serwery aplikacji	Zgodnie z istniejącym rozwiązaniem – nie podlega modyfikacji
7.	Portale	Zgodnie z istniejącym rozwiązaniem – nie podlega modyfikacji
8.	Inne	

## 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

System S46 został zaprojektowany w modelu wysokiej dostępności, obecnie eksploatowane są dwa centra danych pracujące w gorącej rezerwie, które dostarczają równoważne funkcjonalności. W niniejszym projekcie planowana jest rozbudowa systemu do trzech centrów danych. Zwiększy to niezawodność, używalność, wydajność, przenoszalność systemu. W systemie monitorowany jest poziom dostępności usług i zorganizowany jest system wsparcia użytkowników w oparciu o zespół serwisowy i opracowane procedury. Projektowanie i eksploatacja systemu odbywa się z uwzględnieniem Polskich Norm dotyczących bezpieczeństwa (w szczególności PN-EN ISO/IEC 27001) jak również dobrych praktyk ITIL.

Współpraca zorganizowana z podmiotami publicznymi jest realizowana z wykorzystaniem sieci teleinformatycznej wykorzystującej mechanizmy szyfrowania oparte na normach i standardach krajowych i światowych W3C, IETF, ITU – T. System jest zrealizowany w oparciu o WEB-serwisy, zasoby informacyjne udostępniane są w formatach zgodnych z KRI załącznik 2 i 3.

Dokumentacja projektowa systemu została opracowana zgodnie z Web Content Accessibility Guidelines (WCAG 2.0) i przyjęta przez MC/KPRM. System S46 jest objęty audytem bezpieczeństwa przez Agencję Bezpieczeństwa Wewnętrznego w bieżącym roku (2021r.) w zakresie zarządzania bezpieczeństwem informacji. NASK PIB ma opracowaną dokumentację SZBI (System Zarządzania Bezpieczeństwem Informacji) zgodnie z którą realizowane są procesy określone w minimalnych wymaganiach zawartych w KRI. Oprogramowanie jest uaktualniane systematycznie, zgodnie z pojawianiem się informacji o nowych wersjach (dotyczy to zarówno urządzeń jak i samodzielnego oprogramowania w systemie). Planowane jest w niniejszym projekcie zarządzanie uaktualnieniami w oparciu o specjalistyczne oprogramowanie. Obecnie w systemie retencjonowane są dane pochodzące z dzienników logów oprogramowania jak i historia działań użytkowników. System oparty jest na mechanizmie RBAC w obsłudze użytkowników.

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