**WZÓR**

**OPISU 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 |

|  |
| --- |
| **TREŚĆ W KOLORZE NIEBIESKIM** została dodana do dokumentu w celu objaśnienia kolejnych elementów.  -- Należy usunąć tę instrukcję po uzupełnieniu dokumentu – |

# POWODY PODJĘCIA PROJEKTU

<<maksymalnie 2000 znaków>>

## Identyfikacja problemu i potrzeb

<< Proszę wyjaśnić, na jakie problemy, potrzeby społeczne odpowiada planowane przedsięwzięcie. Problem (sytuacja problemowa) istnieje wówczas, gdy mamy do czynienia z różnicą pomiędzy stanem istniejącym a oczekiwanym (na przykład celem, normą, oczekiwaniem społecznym).

## Należy wskazać jakich grup interesariuszy dotyczy projekt, proszę wypełnić poniższą tabelę>>

Infrastruktura teleinformatyczna państwa – co szczególnie unaocznił 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** |
| *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* | * **Brak** narzędzi do skutecznego zarządzania i dystrybucji informacji na temat cyberbezpieczeństwa w JST i ich jednostkach organizacyjnych * **Wysoki początkowy koszt** podłączenia do s46 * **Nie otrzymywanie** ostrzeżeń o zagrożeniach i zagregowanej informację o podatnościach – w sposób systemowy, zintegrowany – a przez to skuteczny * Brak podłączenia do s46 wskazanych jednostek powoduje **niepełny obraz** sytuacyjny cyberbezpieczeństwa oraz ryzyka dynamicznego świadczonych usług – w szczególności dla jednostek uczestniczących w zintegrowanym systemie zarządzania kryzysowego   Szacowana wielkość grupy wskazana jest jako liczba minimalna. | *100* |
| *Przedstawiciele JST i jednostek im podległych, urzędów współpracujące przy zagadnieniach związanych z cyberbezpieczeństwem JST, a także uczestniczących w zintegrowanym systemie zarządzania kryzysowego (Urzędy Wojewódzkie, RCB)* | * **niewystarczający** poziom wiedzy pracowników jednostek organizacyjnych samorządów terytorialnych oraz innych – wskazanych podmiotów o cyberbezpieczeństwie * **brak** wiedzy pracowników jednostek organizacyjnych samorządów terytorialnych oraz innych – wskazanych podmiotów o sposobie funkcjonowania systemu S46   Szacowana wielkość grupy wskazana jest jako liczba minimalna. | 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* |

## Opis stanu obecnego

# Zobowiązanie do zbudowania systemu S46 jako strategicznego przedsięwzięcia zostało wprowadzone w ustawie o krajowym systemie cyberbezpieczeństwa (KSC) (Dz. U. 2020 poz. 1369) – dalej „Ustawa”. W art. 89 nałożono na ministra właściwego ds. informatyzacji zadanie polegające na utworzeniu i udostępnieniu systemu teleinformatycznego wymienionego w art. 46 ust. 1, wspierającego koordynację działań i współpracę podmiotów wchodzących w skład KSC, 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 szacowanie ryzyka na poziomie krajowym.

# Za podmioty KSC, zgodnie z art. 4 Ustawy, uznaje się m.in. operatorów usług kluczowych, jednostki sektora finansów publicznych (art. 9 pkt 1-6, 8-9, 11-12 ustawy o finansach publicznych w zw. z art. 21 Ustawy; np. JST, szpitale publiczne, inne państwowe lub samorządowe osoby prawne utworzone na podst. odrębnych ustaw w celu wykonywania zadań publicznych), spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy o gospodarce komunalnej (np. szpitale, spółki wodno-kanalizacyjne).

# 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 system S46 został uruchomiony operacyjnie.

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

## Cele i korzyści wynikające z projektu <<maksymalnie 2000 znaków>>

<<Należy wskazać najważniejsze wymierne (mierzalne) korzyści, spodziewane do uzyskania w wyniku osiągniecia poszczególnych celów projektu, jak również wskazać sposób i częstotliwość pomiaru tych korzyści. W przypadku projektów współfinansowanych ze środków UE w ramach programów operacyjnych, należy wykazać wskaźniki obowiązujące dla danego programu.>>

|  |  |
| --- | --- |
| **Cel - 1** | Zwiększenie liczby podmiotów krajowego systemu cyberbezpieczeństwa podłączonych do S46. |
| **Cel strategiczny** | Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:  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  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.  3/ Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU.  Zwiększenie liczby podłączeń do systemu S46 (wraz z przeszkoleniem użytkowników) i tym samym wzrost poziomu cyberbezpieczeństwa RP, wpisuje się bezpośrednio w zakres osiągnięcia wyżej wymienionych celów strategicznych. |
| **Korzyść:** | 1. **Osiągnięcie synergii** poprzez włączenie do systemu dużej liczby podmiotów 2. **Usprawnienie, upowszechnienie i udrożnienie** wymiany informacji na temat cyberbezpieczeństwa dla wskazanych podmiotów. 3. **Podniesienie skuteczności** monitorowania ryzyk wiążących się z działaniem w cyberprzestrzeni RP znacznej liczby podmiotów publicznych. |
| **KPI:** | Liczba podmiotów objętych wsparciem w zakresie zwalczania lub przeciwdziałania skutkom pandemii COVID-19. |
| **Wartość aktualna i docelowa KPI:** | Wartość aktualna: 0  Wartość docelowa: 100 |
| **Metoda pomiaru KPI** | Liczba protokołów instalacji systemów brzegowych dla JST, jednostek podległych lub nadzorowanych przez JST oraz jednostek realizujących zadania publiczne wspierające JST, zarejestrowanych w systemach dokumentacyjnych NASK, pomiar na koniec każdego kwartału kalendarzowego. |

|  |  |
| --- | --- |
| **Cel - 2** | Zwiększenie liczby podmiotów krajowego systemu cyberbezpieczeństwa posiadających umiejętność posługiwania się systemem S46. |
| **Cel strategiczny** | Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:  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.  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.  3/ Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU  Zwiększenie liczby podłączeń do systemu S46 (wraz z przeszkoleniem użytkowników) i tym samym wzrost poziomu cyberbezpieczeństwa RP, wpisuje się bezpośrednio w zakres osiągnięcia wyżej wymienionych celów strategicznych. |
| **Korzyść:** | Projekt zapewni:   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. 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. |
| **KPI:** | Liczba pracowników objętych szkoleniami w zakresie umiejętności cyfrowych. |
| **Wartość aktualna i docelowa KPI:** | Wartość aktualna: 0  Wartość docelowa: 200 |
| **Metoda pomiaru KPI** | Lista osób przeszkolonych z używania Systemu S46 zarejestrowanych w systemach dokumentacyjnych NASK, pomiar na koniec każdego kwartału kalendarzowego. |

|  |  |
| --- | --- |
| **Cel - 3** | Zwiększenie liczby podmiotów krajowego systemu cyberbezpieczeństwa posiadających umiejętność posługiwania się systemem S46. |
| **Cel strategiczny** | Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:  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.  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.  3/ Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU  Zwiększenie liczby podłączeń do systemu S46 (wraz z przeszkoleniem użytkowników) i tym samym wzrost poziomu cyberbezpieczeństwa RP, wpisuje się bezpośrednio w zakres osiągnięcia wyżej wymienionych celów strategicznych. |
| **Korzyść:** | Projekt zapewni:   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. 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. |
| **KPI:** | Liczba pracowników (kobiet) objętych szkoleniami w zakresie umiejętności cyfrowych. |
| **Wartość aktualna i docelowa KPI:** | Wartość aktualna: 0  Wartość docelowa: 20 |
| **Metoda pomiaru KPI** | Lista kobiet przeszkolonych z używania Systemu S46 zarejestrowanych w systemach dokumentacyjnych NASK, pomiar na koniec każdego kwartału kalendarzowego. |

|  |  |
| --- | --- |
| **Cel - 4** | Zwiększenie liczby podmiotów krajowego systemu cyberbezpieczeństwa posiadających umiejętność posługiwania się systemem S46. |
| **Cel strategiczny** | Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:  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.  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.  3/ Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU  Zwiększenie liczby podłączeń do systemu S46 (wraz z przeszkoleniem użytkowników) i tym samym wzrost poziomu cyberbezpieczeństwa RP, wpisuje się bezpośrednio w zakres osiągnięcia wyżej wymienionych celów strategicznych. |
| **Korzyść:** | Projekt zapewni:   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. 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. |
| **KPI:** | Liczba pracowników (mężczyzn) objętych szkoleniami w zakresie umiejętności cyfrowych. |
| **Wartość aktualna i docelowa KPI:** | Wartość aktualna: 0  Wartość docelowa: 180 |
| **Metoda pomiaru KPI** | Lista mężczyzn przeszkolonych z używania Systemu S46 zarejestrowanych w systemach dokumentacyjnych NASK, pomiar na koniec każdego kwartału kalendarzowego. |

|  |  |
| --- | --- |
| **Cel - 5** | Zwiększenie liczby podmiotów krajowego systemu cyberbezpieczeństwa posiadających umiejętność posługiwania się systemem S46. |
| **Cel strategiczny** | Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:  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.  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.  3/ Cele Programu Operacyjnego Polska Cyfrowa - Oś priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU  Zwiększenie liczby podłączeń do systemu S46 (wraz z przeszkoleniem użytkowników) i tym samym wzrost poziomu cyberbezpieczeństwa RP, wpisuje się bezpośrednio w zakres osiągnięcia wyżej wymienionych celów strategicznych. |
| **Korzyść:** | Projekt zapewni wsparcie w zakresie przeciwdziałania skutkom pandemii poprzez:   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. 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. |
| **KPI:** | Liczba osób objętych wsparciem w zakresie zwalczania lub przeciwdziałania skutkom pandemii COVID-19. |
| **Wartość aktualna i docelowa KPI:** | Wartość aktualna: 0  Wartość docelowa: 200 |
| **Metoda pomiaru KPI** | Lista osób przeszkolonych z używania Systemu S46 zarejestrowanych w systemach dokumentacyjnych NASK, pomiar na koniec każdego kwartału kalendarzowego. |

|  |  |
| --- | --- |
| **Cel – 6** | Zwiększenie poziomu bezpieczeństwa systemu S46 i zapewnienie obsługi zwiększonej liczby podłączeń. |
| **Cel strategiczny** | Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:  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.  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.  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 i zwiększenie bezpieczeństwa Systemu S46, wpisuje się pośrednio w zakres wyżej wymienionych celów strategicznych przez zapewnienie możliwości podłączenia do S46, a przez to wzrost poziomu bezpieczeństwa RP. |
| **Korzyść:** | System S46 będzie zmodernizowany, dzięki czemu zapewni:   1. **wzmocnienie** bezpieczeństwa poprzez zastosowanie zaawansowanych systemów bezpieczeństwa teleinformatycznego; 2. **podniesienie** odporności na katastrofy usług; 3. **wzmocnienie** stabilności S46 poprzez wykorzystanie platform systemowych i wirtualizacyjnych systemów posiadających stałe i gwarantowane wsparcie; 4. **zwiększenie** odporności S46 w stanach nadzwyczajnych poprzez zwiększenie redundancji geograficznej centrów; 5. **zwiększenie** wydajności i skuteczności obsługi Systemu S46 przez wyposażenie w centrum monitorowania SOC/NOC; 6. **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; 7. **przyspieszenie** naprawy dla zwiększonego grona użytkowników Systemu S46 poprzez zakup puli urządzeń zapasowych. |
| **KPI:** | Liczba wdrożonych systemów IT w obszarze cyberbezpieczeństwa. |
| **Wartość aktualna i docelowa KPI:** | Wartość aktualna: 0  Wartość docelowa: 1 |
| **Metoda pomiaru KPI** | Protokół odbioru zmodernizowanego systemu S46 udokumentowany w systemach ewidencji majątku – pomiar na koniec każdego kwartału kalendarzowego |

|  |  |
| --- | --- |
| **Cel – 7** | Zapewnienie trwałego wsparcia gospodarki w dziedzinie cyberbezpieczeństwa na wypadek zagrożeń – w tym epidemicznych. |
| **Cel strategiczny** | Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:  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.  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.  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. |
| **Korzyść:** | **Podniesienie** reaktywności na zagrożenia cyberbezpieczeństwa dzięki realizacji zadań inwestycyjnych, poprzez uzyskanie bazy składającej się na środki trwałe i wartości niematerialne i prawne, które umożliwią osiąganie celów systemu S46 w sytuacjach ewentualnych przyszłych zagrożeń – co wynika z doświadczeń zebranych w okresie epidemii COVID-19 |
| **KPI:** | Wartość sprzętu IT oraz oprogramowania/licencji finansowanych w odpowiedzi na COVID-19 - inne obszary |
| **Wartość aktualna i docelowa KPI:** | Wartość aktualna: 0  Wartość docelowa: 12 490 000,00 zł |
| **Metoda pomiaru KPI** | Dokumenty księgowe potwierdzające wartość przyjętych na stan środków trwałych i wartości niematerialnych i prawnych (wartości netto). Pomiar na koniec każdego kwartału kalendarzowego. |

|  |  |
| --- | --- |
| **Cel – 8** | Zapewnienie trwałego wsparcia gospodarki w dziedzinie cyberbezpieczeństwa na wypadek zagrożeń – w tym epidemicznych. |
| **Cel strategiczny** | Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:  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.  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.  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. |
| **Korzyść:** | **Podniesienie** reaktywności na zagrożenia cyberbezpieczeństwa dzięki realizacji zadań inwestycyjnych, poprzez uzyskanie bazy składającej się na środki trwałe i wartości niematerialne i prawne, które umożliwią osiąganie celów systemu S46 w sytuacjach ewentualnych przyszłych zagrożeń – co wynika z doświadczeń zebranych w okresie epidemii COVID-19 |
| **KPI:** | Wartość sprzętu IT oraz oprogramowania/licencji finansowanych w odpowiedzi na COVID-19 (CV 4) |
| **Wartość aktualna i docelowa KPI:** | Wartość aktualna: 0  Wartość docelowa: 12 490 000,00 zł |
| **Metoda pomiaru KPI** | Dokumenty księgowe potwierdzające wartość przyjętych na stan środków trwałych i wartości niematerialnych i prawnych (wartości netto). Pomiar na koniec każdego kwartału kalendarzowego. |

|  |  |
| --- | --- |
| **Cel – 9** | Zapewnienie trwałego wsparcia gospodarki w dziedzinie cyberbezpieczeństwa na wypadek zagrożeń – w tym epidemicznych. |
| **Cel strategiczny** | Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:  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.  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.  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. |
| **Korzyść:** | **Podniesienie** reaktywności na zagrożenia cyberbezpieczeństwa dzięki poszerzeniu liczby podmiotów obsługiwanych przez system S46, a także jego rozbudowa, co umożliwi osiąganie celów systemu S46 w sytuacjach ewentualnych przyszłych zagrożeń – co wynika z doświadczeń zebranych w okresie epidemii COVID-19 |
| **KPI:** | Wartość wydatków kwalifikowalnych przeznaczonych na działania związane z pandemią COVID-19 |
| **Wartość aktualna i docelowa KPI:** | Wartość aktualna: 0  Wartość docelowa: 25 732 875,00 zł |
| **Metoda pomiaru KPI** | Dokumenty księgowe potwierdzające wartość wydatków kwalifikowanych (wartości netto). Pomiar na koniec każdego kwartału kalendarzowego. |

## Udostępnione e-usługi <<maksymalnie 2000 znaków>>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa  e-usługi** | **Typ** | **Zakres oddziaływania** | **Poziom dojrzałości  e-usługi[[1]](#footnote-2)** |
|  |  |  |  |  |

## Udostępnione informacje sektora publicznego i zdigitalizowane zasoby <<maksymalnie 2000 znaków>>

Czy wszystkie zdigitalizowane zasoby objęte projektem będą udostępniane bezpłatnie? ~~TAK~~/NIE [[2]](#footnote-3)

Projekt nie zakłada digitalizacji i publicznego udostępniania zasobów ze względu na swój charakter i ograniczenie zasięgu do podłączonych do Systemu S46 podmiotów.

|  |  |  |
| --- | --- | --- |
| **Rodzaj**  **informacji / zasobów** | **Planowana data udostępnienia** | **Szacowana liczba obiektów objętych digitalizacją (udostępnianiem informacji)** |
| Nie dotyczy | Nie dotyczy | Nie dotyczy |

## Produkty końcowe projektu <<maksymalnie 2000 znaków>>

<<należy wskazać produkty projektu inne niż w pkt 2.2 i 2.3>>

|  |  |
| --- | --- |
| **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 |

# KAMIENIE MILOWE <<maksymalnie 1000 znaków>>

|  |  |
| --- | --- |
| **Kamienie milowe** | **Planowany termin osiągnięcia** |
| Rozstrzygnięte 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 30 jednostek, które w ten sposób zostaną podłączone (podłączone 40 jednostek narastająco) oraz przeszkolone 60 osób (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 40 jednostek, które w ten sposób zostaną podłączone (podłączone 80 jednostek narastająco) oraz przeszkolone 80 osób (przeszkolone 160 osób narastająco) | 2023-03-31 |
| Dostawa urządzeń i oprogramowania bazowego systemów brzegowych s46 oraz ich instalacja i uruchomienie dla 20 jednostek, które w ten sposób zostaną podłączone (podłączone 100 jednostek narastająco) oraz przeszkolone 40 osób (przeszkolone 200 osób narastająco) | 2023-06-30 |
| Zrealizowana rozbudowa Systemu S46 – zainstalowane i uruchomione wszystkie systemy | 2023-06-30 |

# KOSZTY

## Koszty ogólne projektu wraz ze sposobem finansowania

|  |  |  |
| --- | --- | --- |
| **Całkowity koszt projektu (netto oraz brutto), w tym:** | 29 802 581,25 zł brutto  25 732 875,00 zł netto | |
| **Procent dofinansowania ze środków UE (brutto)** | 100% kosztów kwalifikowanych | |
| **Procent środków z budżetu państwa (brutto)** | 0% | |
| **Podział całkowitego kosztu projektu na poszczególna lata (netto oraz brutto)** | *2021* | 1 749 323,16 zł netto, 1 947 261,89 zł brutto |
| *2022* | 12 450 268,26 zł netto, 14 289 262,76 zł brutto |
| *2023* | 11 533 283,58 zł netto, 13 566 056,60 zł brutto |

## 

## Wykaz poszczególnych pozycji kosztowych <<maksymalnie 2000 znaków>>

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa pozycji kosztowej:**  <<zakres należy dostosować do typu projektu. Dane prezentowane w tej kolumnie powinny korelować z częścią 2.2-2.4 >> | | Przewidywany koszt brutto:  <<kwoty wyrażone w formacie: 1 485 000,00 zł. Należy wskazać przewidywany całościowy koszt dla każdej pozycji>> | Uzasadnienie pozycji kosztowej (przeznaczenie):  <<zwięzłe uzasadnienie potrzeby wydatkowania środków na tę pozycję kosztową; maksymalnie 3 zdania>> |
| 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 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) |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Całkowity koszt utrzymania trwałości projektu (brutto)** | <<kwota wyrażona w formacie: 12 485 000,00 zł>> | | **Źródło finansowania** |
| **Podział całkowitego kosztu utrzymania trwałości projektu na poszczególna lata (netto oraz brutto)** | 2023 | 1 489 860,00 zł | budżet państwa |
| 2024 | 2 979 720,00 zł | budżet państwa |
| 2025 | 2 979 720,00 zł | budżet państwa |
| 2026 | 3 015 193,20 zł | budżet państwa |
| 2027 | 3 726 858,90 zł | budżet państwa |
| 2028 | 2 761 630,80 zł | 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.[[3]](#footnote-4)~~

# GŁÓWNE RYZYKA <<maksymalnie 2000 znaków>>

## Ryzyka wpływające na realizację projektu

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa ryzyka** | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
| Niechęć podmiotów KSC do podłączania do S46 | duża | średnie | Łagodzenie – zwiększenie listy potencjalnie zainteresowanych podmiotów w stosunku do zamierzonej liczby podłączeń (utworzenie listy rezerwowej)  Akceptacja – wykonywanie specjalnych działań promocyjnych (dodatkowe warsztaty, pokazy, wskazanie przykładu innych) w stosunku do podmiotów wyrażających wątpliwości |
| Brak odpowiedniej infrastruktury teleinformatycznej podłączanych podmiotów | średnia | małe | Łagodzenie – zastosowanie w projekcie rozwiązań umożliwiających skorzystanie z systemu przy minimalnych środkach technicznych od strony podłączanej jednostki (np. terminal PC). |
| Wzrost kursu | średnia | średnie | Mitygacja – realizacja postępowań zakupowych odpowiednio wcześnie 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. |

## Ryzyka wpływające na utrzymanie efektów

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa ryzyka** | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
| Brak chęci do użytkowania systemu S46 przez podłączone podmioty | duża | średnie | Akceptacja – podejmowanie działań zaradczych na bieżąco (monitorowanie, dodatkowe szkolenia, pomoc w identyfikacji problemów itp.)  Przeniesienie – zaangażowanie innych podmiotów w uświadamianie roli systemu S46 – w szczególności zaangażowanie podmiotów o podobnym charakterze, aktywnie używających S46 do wskazania sposobów użycia S46 przy rozwiązywaniu konkretnych problemów w dziedzinie, w której działa podmiot. |
| 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 poprawek redukujących ryzyko. |

# OTOCZENIE PRAWNE <<maksymalnie 1000 znaków>>

<<Należy wykazać gotowość do realizacji projektu w istniejącym otoczeniu prawnym lub wskazać wszystkie akty prawne niezbędne do zmiany w celu zapewnienia takiej gotowości oraz aktualny etap prac legislacyjnych (np. uzgodnienia międzyresortowe, KSE, KRMC, Sejm, Senat)>>

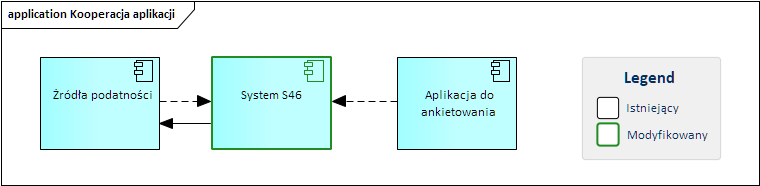
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp** | Tytuł aktu prawnego | Czy wymaga zmian? | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|  | Ustawa o Krajowym Systemie Cyberbezpieczeństwa (t. j. Dz. U. 2020 poz. 1369) | ~~TAK~~/NIE[[4]](#footnote-5) |  |  |
|  | Uchwała RM z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 | ~~TAK~~/NIE[[5]](#footnote-6) |  |  |
|  | Ustawa z dnia 17 lutego 2005 o Informatyzacji działalności podmiotów realizujących zadania publiczne | ~~TAK~~/NIE[[6]](#footnote-7) |  |  |
|  | 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]](#footnote-8) |  |  |

# ARCHITEKTURA

<< Diagramy mają być zamodelowane w Archimate 3.0 przy użyciu dowolnego narzędzia, np.: Archi Tool (bezpłatny), Sparx Enterprise Architect (płatny), MS Visio (płatny) >>

## Widok kooperacji aplikacji

<< Celem diagramu kooperacji aplikacji jest pokazanie wszystkich systemów wykorzystanych w projekcie oraz przepływów pomiędzy nimi (włączając systemy partnerów zewnętrznych). Na modyfikowanych w ramach rozwiązania relacjach można wskazać dane przepływające pomiędzy systemami. Statusy systemów i przepływów należy oznaczyć kolorami. Przykład:



| Status | Opis |
| --- | --- |
| Modyfikowany | System modyfikowany, rozszerzany na potrzeby projektu. |
| Istniejący | System działający produkcyjnie, gotowy do wykorzystania |

Lista systemów wykorzystywanych w projekcie <<maksymalnie 2000 znaków>>

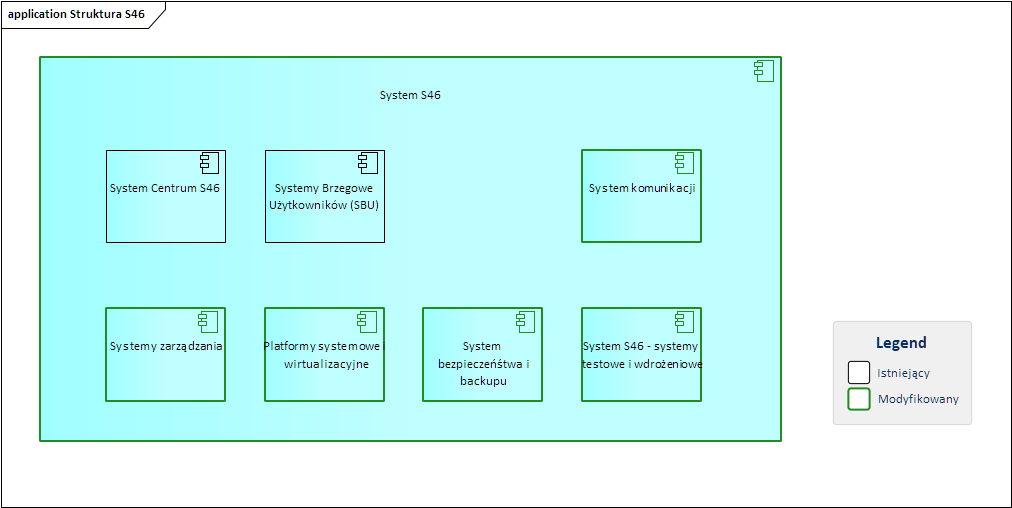
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa systemu** | **Gestor systemu** | **Opis systemu** | **Status** | **Krótki opis ewentualnej zmiany** |
| 1 | System S46 | Minister Cyfryzacji/KPRM | System realizujący założenia systemu teleinformatycznego z art. 46 ust. 1 Ustawy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

Lista przepływów <<maksymalnie 2000 znaków>>

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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 |
| 33. | Aplikacja do ankietowania | System S46 | Informacje o usługach, poziomach ryzyka | kopiowanie danych - plików | Krytyczny dla sukcesu projektu | Plikowy |

## Kluczowe komponenty architektury rozwiązania

<< Na diagramie należy przedstawić kluczowe komponenty funkcjonalne niezbędne do działania rozwiązania. Diagram należy przygotować tylko dla nowych bądź znacząco modyfikowanych systemów. Przykład:



## Przyjęte założenia technologiczne <<maksymalnie 2000 znaków>>

<< Czy w projekcie przyjęto sztywne założenia lub ograniczenia w zakresie technologii (na przykład serwery mainframe, sieci OST112, specyficzne algorytmy szyfrujące, wykorzystanie lub integracja z rozwiązaniami konkretnego producenta, inne). Przy braku sztywnych założeń pozostawić niewypełnione >>

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Obszar** | **Założenie technologiczne** |
|  | Infrastruktura | Systemy zgodne z dotychczas używanymi (podłączenie w oparciu o serwery Dell R440 lub podobne, po zatwierdzeniu do użytkowania) |
|  | 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. |
|  | Standardy wymiany danych | Zgodnie z istniejącym rozwiązaniem – nie podlega modyfikacji |
|  | Systemy operacyjne serwerowe | Przebudowa w kierunku RedHat, Vmware |
|  | Bazy danych | Zgodnie z istniejącym rozwiązaniem – nie podlega modyfikacji |
|  | Serwery aplikacji | Zgodnie z istniejącym rozwiązaniem – nie podlega modyfikacji |
|  | Portale | Zgodnie z istniejącym rozwiązaniem – nie podlega modyfikacji |
|  | Inne |  |

## Opis zasobów danych przetwarzanych w planowanym rozwiązaniu <<maksymalnie 2000 znaków>>

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

~~TAK~~/NIE [[8]](#footnote-9)

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Tworzony rejestr publiczny** | **Opis** |
|  |  |  |

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

~~TAK~~/NIE [[9]](#footnote-10)

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Rejestr publiczny** | **Opis** | **Zakres przetwarzania** |
|  |  |  | << użycie, zmiana>> |

## Bezpieczeństwo <<maksymalnie 2000 znaków>>

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>>~~~~[[10]](#footnote-11)~~

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.

1. Pięciostopniowa e-dojrzałość usług określona w badaniach „Digitizing Public Services in Europe: Putting ambition into action”, prowadzonych na zlecenie KE przez firmę Cap Gemini ec.europa.eu/newsroom/document.cfm?action=display&doc\_id=747 [↑](#footnote-ref-2)
2. Niepotrzebne skreślić. [↑](#footnote-ref-3)
3. Niepotrzebne skreślić [↑](#footnote-ref-4)
4. Niepotrzebne skreślić. [↑](#footnote-ref-5)
5. Niepotrzebne skreślić. [↑](#footnote-ref-6)
6. Niepotrzebne skreślić. [↑](#footnote-ref-7)
7. Niepotrzebne skreślić. [↑](#footnote-ref-8)
8. Niepotrzebne skreślić. [↑](#footnote-ref-9)
9. Niepotrzebne skreślić [↑](#footnote-ref-10)
10. Niepotrzebne skreślić [↑](#footnote-ref-11)