# OPIS ZAŁOŻEŃ PRZEDSIĘWZIĘCIA INFORMATYCZNEGO O PUBLICZNYM ZASTOSOWANIU

| | | | |
|---|---|---|---|
| **Tytuł przedsięwzięcia** | Polska Tarcza PNT Moduł 1 | | |
| **Wnioskodawca** | Minister Finansów i Gospodarki | | |
| **Beneficjent** | Główny Urząd Geodezji i Kartografii (GUGiK) | | |
| **Partnerzy** | Ministerstwo Obrony Narodowej (MON) | | |
| **Źródło finansowania** | Budżet państwa: część budżetowa cz. 83 przynależna do cz. 27 oraz środki programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie FERC.04.01 Wzmocnienie cyberbezpieczeństwa oraz rozwój odpornej infrastruktury przetwarzania danych | | |
| **Całkowity koszt przedsięwzięcia** | 27 000 000,00 zł | | |
| **Planowany okres realizacji przedsięwzięcia** | 11-2026 do 10-2028 | | |
| **Osoba kontaktowa** | Szymon Wajda | szymon.wajda@gugik.gov.pl | 225322565<br>501561626 |

# 1. POWODY PODJĘCIA PRZEDSIĘWZIĘCIA

## 1.1. Identyfikacja problemu i potrzeb

Projekt wypełnia lukę w cyberodporności państwa dotyczącą usług pozycji, nawigacji i czasu (PNT) opartych na GNSS. Usługi te są krytycznym komponentem procesów cyfrowych, administracyjnych, gospodarczych, naukowych i obronnych, ponieważ zapewniają wiarygodną informację o położeniu, czasie i synchronizacji. System ASG-EUPOS, utrzymywany przez GUGiK, realizuje geodezyjne układy odniesienia w Polsce (PL-ETRF2000, PL-ETRF89) i obsługuje ponad 20 tys. użytkowników, w tym podmioty geodezyjne, budowlane i drogowe.
Problemem jest rosnąca ekspozycja usług PNT na zagrożenia hybrydowe i cyberfizyczne, w szczególności jamming i spoofing GNSS, prowadzące do utraty dostępności i integralności danych, błędnego wyznaczania pozycji, zaburzeń synchronizacji czasu oraz decyzji opartych na niewiarygodnych informacjach. Skutki dotyczą geodezji, transportu, energetyki, telekomunikacji, lotnictwa, zarządzania kryzysowego, infrastruktury krytycznej i obronności.
Obecnie podmioty te nie mają zintegrowanej państwowej warstwy cyberbezpieczeństwa PNT/GNSS. Brakuje monitoringu jakości sygnału i usług ASG-EUPOS, detekcji, kategoryzacji i lokalizacji zakłóceń, korelacji zdarzeń, jednego obrazu sytuacyjnego, wymiany alertów oraz wsparcia ciągłości działania przy degradacji sygnału. Brak tych produktów powoduje rozbieżność między dojrzałą usługą referencyjną a oczekiwanym modelem odporności państwa. Projekt usuwa tę rozbieżność przez budowę i modyfikację systemów i modułów analitycznych, API, usług statusowych, alertowych i raportowych oraz platformy integracyjnej Polska Tarcza PNT. Monitoring GNSS i ASG-EUPOS zapewni ocenę jakości PNT. Moduły detekcji jammingu i spoofingu umożliwią wykrywanie, klasyfikację i ocenę wpływu incydentów. Platforma integracyjna stworzy jedno źródło danych o zakłóceniach sygnałów GNSS dla GUGiK, MON, służb, JST, regulatorów i operatorów infrastruktury krytycznej. API i feedy alertowe umożliwią dystrybucję informacji, szybsze reagowanie i utrzymanie wiarygodnych usług PiT

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|---|---|---|
| Pracownicy GUGiK | Brak jednej, zintegrowanej i interoperacyjnej warstwy państwowej do monitorowania jakości GNSS i ASG-EUPOS, automatycznej dystrybucji alertów, obsługi incydentów PNT oraz wymiany danych między resortami i jednostkami realizującymi zadania publiczne. Szacowaną grupę stanowią 20 pracowników IT oraz 200 pracowników nie-IT odpowiedzialnych za utrzymanie jakości danych GNSS i ASG-EUPOS | 220 |
| Organy odpowiedzialne za bezpieczeństwo | Brak ciągłego monitorowania jakości PNT/ GNSS, szybkiej detekcji, klasyfikacji i lokalizacji zakłóceń oraz wspólnego obrazu sytuacyjnego dla działań operacyjnych, zarządzania kryzysowego i reagowania. Szacuje się, że bezpośrednimi lub pośrednimi użytkownikami projektowanej warstwy monitorowania, detekcji i ostrzegania PNT może być ok. 10 tys. przedstawicieli Sił Zbrojnych RP, organów odpowiedzialnych za cyberbezpieczeństwo oraz służb mundurowych i ratunkowych. Grupa ta obejmuje w szczególności stanowiska dowodzenia, komórki geoinformacyjne, łączności, cyberbezpieczeństwa, zarządzania kryzysowego, dyspozytorskie, operacyjne i analityczne. Szacunek nie oznacza liczby obecnych kont w ASG-EUPOS, lecz potencjalną liczbę osób korzystających z danych, alertów lub informacji o jakości i wiarygodności usług PNT w ramach realizacji zadań bezpieczeństwa, obronności i reagowania kryzysowego. | 10000 |
| Organy regulacyjne i nadzorcze | Brak ustandaryzowanej wymiany informacji o jakości PNT, metryk SLA i feedów alertowych dla sektorów regulowanych oraz ograniczona baza do oceny ryzyka w obszarach telekomunikacji, lotnictwa, kolei, energetyki i dozoru technicznego.<br>Zakłada się, że grupę odbiorców po stronie organów regulacyjnych i nadzorczych stanowi 5 instytucji: UKE, ULC, UTK, URE i UDT. Szacowana liczba przedstawicieli korzystających bezpośrednio z danych, metryk jakości PNT, raportów SLA i feedów alertowych wynosi ok. 80–160 osób, przy wartości roboczej ok. 120 osób. Są to przede wszystkim pracownicy komórek nadzoru, bezpieczeństwa, analiz ryzyka, kontroli, regulacji technicznych, ciągłości działania | 120 |

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|---|---|---|
| | oraz obsługi incydentów w sektorach telekomunikacji, lotnictwa, kolei, energetyki i dozoru technicznego. Projekt odpowiada na potrzebę ustandaryzowanej wymiany informacji o jakości usług PNT oraz budowy wspólnej podstawy do oceny ryzyka zakłóceń GNSS w sektorach regulowanych. | |
| Biznes | Przedsiębiorstwa prywatne, firmy usługowe oraz rolnictwo.<br>Zakłócenia GNSS obniżają wiarygodność pomiarów, ciągłość wykorzystania ASG-EUPOS oraz bezpieczeństwo procesów zależnych od precyzyjnej pozycji i czasu. Brak bieżącej informacji o rejonach degradacji sygnału utrudnia zapewnienie jakości materiałów przekazywanych do zasobu geodezyjnego, realizację inwestycji budowlanych i drogowych, sterowanie maszynami, prowadzenie rolnictwa precyzyjnego, obsługę procesów logistycznych oraz wykonywanie zadań JST opartych na danych przestrzennych. W sektorze finansowym i gospodarce cyfrowej brak odpornej dystrybucji czasu oraz informacji o degradacji PNT zwiększa ryzyko zaburzeń synchronizacji transakcji, znakowania czasu, korelacji zdarzeń, rozliczeń i ciągłości usług cyfrowych. W sektorach specjalistycznych brak alternatywnych i odpornych metod PNT oraz wyspecjalizowanej informacji sektorowej ogranicza bezpieczeństwo zastosowań w gospodarce morskiej i offshore, nauce, B+R, metrologii oraz automatyzacji przemysłowej. Grupę odbiorców biznesowych można oszacować na co najmniej na 20 000 aktywnych użytkowników systemu ASG-EUPOS, zależnych od jakości sygnału GNSS, usług PNT oraz wiarygodnej dystrybucji czasu. Grupa ta obejmuje geodetów, wykonawców budowlanych i drogowych, operatorów maszyn, przedsiębiorstwa przemysłowe, rolnictwo precyzyjne, logistykę, banki, domy maklerskie, operatorów płatności, izby rozliczeniowe, dostawców usług cyfrowych, centra danych, operatorów chmury, podmioty gospodarki morskiej i offshore, jednostki naukowe, laboratoria metrologiczne oraz JST realizujące zadania zależne od danych przestrzennych. | 20000 |

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|---|---|---|
| Operatorzy infrastruktury krytycznej i przedsiębiorstwa sieciowe | Brak odpornych źródeł czasu i pozycji oraz brak szybkiej informacji o zakłóceniach PNT zwiększa ryzyko utraty ciągłości działania systemów energetycznych, telekomunikacyjnych, transportowych i centrów przetwarzania danych,<br>Szacuje się, że grupę odbiorców po stronie operatorów infrastruktury krytycznej i przedsiębiorstw sieciowych stanowi ok. 500–1 200 organizacji, w tym operatorzy energetyczni, telekomunikacyjni, transportowi, centra przetwarzania danych, dostawcy usług chmurowych oraz inne przedsiębiorstwa utrzymujące systemy sieciowe i infrastrukturalne. Liczbę przedstawicieli korzystających bezpośrednio z danych o jakości PNT, alertów o zakłóceniach, informacji o degradacji sygnału GNSS oraz metryk ciągłości usług można oszacować na ok. 3 000–8 000 osób, przy wartości roboczej ok. 5 000 osób. Są to przede wszystkim pracownicy centrów nadzoru, dyspozytorni, zespołów utrzymania infrastruktury, bezpieczeństwa, cyberbezpieczeństwa, ciągłości działania, zarządzania kryzysowego i eksploatacji systemów OT/ICT. Projekt odpowiada na potrzebę zapewnienia odpornych źródeł czasu i pozycji oraz szybkiej informacji o zakłóceniach PNT, ograniczając ryzyko utraty ciągłości działania systemów energetycznych, telekomunikacyjnych, transportowych i centrów przetwarzania danych. | 5000 |
| Pracownicy MRiT | Brak narzędzi do ciągłego monitorowania jakości PNT/GNSS oraz możliwości przeciwdziałania skutkom zakłócania sygnału. | 10 |

## 1.2. Opis stanu obecnego

Obecnie GUGiK realizuje zadania państwowej referencji przestrzennej z wykorzystaniem systemu ASG-EUPOS oraz sieci stacji referencyjnych podstawowej osnowy geodezyjnej klasy fundamentalnej. System działa od 2008 r., utrzymuje geodezyjne układy odniesienia w Polsce i stanowi bazę dla pomiarów GNSS. Jest powiązany z EUREF Permanent Network i zwiększa dokładność pomiarów w geodezji, budownictwie i drogownictwie.

W obecnych procesach przetwarzane są obserwacje GNSS ze stacji permanentnych, dane do realizacji układów odniesienia, dane usługowe ASG-EUPOS oraz informacje niezbędne do zapewnienia dokładności prac geodezyjnych. Poziom digitalizacji jest wysoki w części referencyjnej i usługowej, bo Beneficjent dysponuje dojrzałym systemem teleinformatycznym

wykorzystywanym przez szerokie grono odbiorców.

Niewystarczający pozostaje poziom digitalizacji cyberodporności warstwy PNT/GNSS. Brakuje integracji danych z wielu źródeł, wspólnej wizualizacji sytuacji, wymiany alertów oraz technicznego środowiska współdziałania GUGiK z administracją, MON i operatorami infrastruktury krytycznej w zakresie monitorowania, detekcji i reagowania. Potrzebę projektu potwierdza skala jammingu i spoofingu GNSS w Europie Wschodniej i regionie Morza Bałtyckiego oraz 1 543 zgłoszenia zakłóceń GPS/GNSS odnotowane w 2025 r. przez ULC, w tym 1 172 nad terytorium RP.

Projekt odpowiada na te luki. Brak monitoringu jakości GNSS zostanie zaadresowany przez budowę stacji monitorujących i serwisów statusowych. Brak detekcji jammingu i spoofingu rozwiążą moduły analityczne, algorytmy wykrywania anomalii i klasyfikacja incydentów. Brak wspólnego obrazu sytuacyjnego usunie platforma integracyjna Polska Tarcza PNT – Moduł 1. Brak wymiany alertów zostanie rozwiązany przez API, feedy alertowe, raporty sektorowe i wielopoziomowy dostęp do informacji, a brak wsparcia ciągłości działania przez mechanizmy oceny wiarygodności PNT oraz analizy wpływu degradacji sygnału na usługi publiczne, gospodarcze i obronne.

# 2. EFEKTY PRZEDSIĘWZIĘCIA

## W jaki sposób przedsięwzięcie realizuje Strategię Cyfryzacji Państwa?

Przedsięwzięcie realizuje bezpośrednio opisane poniżej cele Strategii Cyfryzacji Państwa.
W pierwszej kolejności przedsięwzięcie wspiera realizację celu 1.3.1 „Funkcjonujący krajowy system cyberbezpieczeństwa jest dojrzały i efektywny”. Strategia wskazuje w ramach tego celu m.in. potrzebę wzmacniania potencjału instytucji odpowiedzialnych za zapewnianie cyberbezpieczeństwa na poziomie krajowym, rozwijania mechanizmów wymiany informacji oraz zwiększania efektywności reagowania na zagrożenia.
Projekt Polska Tarcza PNT – Moduł 1 odpowiada na te założenia poprzez budowę zintegrowanej zdolności monitorowania jakości i wiarygodności usług PNT/GNSS, wykrywania, klasyfikacji i lokalizacji zakłóceń oraz wymiany informacji o zdarzeniach wpływających na pozycję, nawigację i czas. Platforma integracyjna, mechanizmy analityczne, system alertowania oraz wspólny obraz sytuacyjny będą wspierały współdziałanie administracji publicznej, Sił Zbrojnych RP, służb, organów regulacyjnych i nadzorczych oraz operatorów infrastruktury krytycznej. Przedsięwzięcie zwiększy tym samym zdolność instytucji państwa do identyfikacji zagrożeń, szybkiej wymiany informacji, oceny ich wpływu oraz koordynacji działań podejmowanych w odpowiedzi na incydenty dotyczące PNT/GNSS.
Przedsięwzięcie bezpośrednio wspiera również realizację celu 1.3.3 „Systemy informacyjne w sferze publicznej (w tym militarnej) oraz prywatnej posiadają wysoki poziom odporności”. Strategia przewiduje w ramach tego celu m.in. rozwój rozwiązań cyberbezpieczeństwa, monitorowanie bezpieczeństwa systemów i rejestrów państwowych, stałe podnoszenie zdolności reagowania na incydenty oraz wdrażanie nowych rozwiązań technicznych, proceduralnych i systemowych.
Projekt realizuje te założenia w odniesieniu do warstwy PNT/GNSS, stanowiącej istotny element funkcjonowania wielu systemów informacyjnych państwa i gospodarki. Rozwiązania przewidziane w projekcie umożliwią ciągłe monitorowanie jakości sygnałów GNSS i usług ASG-EUPOS, wykrywanie jammingu, spoofingu i innych anomalii, ocenę wpływu zdarzeń na użytkowników i systemy zależne od PNT, dystrybucję alertów oraz tworzenie wspólnego obrazu sytuacyjnego. Pozwoli to zwiększyć odporność systemów publicznych, militarnych i prywatnych zależnych od wiarygodnej informacji o pozycji, nawigacji i czasie oraz ograniczyć ryzyko utraty ciągłości ich działania.

Dodatkowym i szczególnie precyzyjnym potwierdzeniem zgodności przedsięwzięcia ze Strategią jest cel 4.4.1 „Technologie obserwacji Ziemi są udoskonalane na potrzeby monitorowania środowiska i zarządzania katastrofami". W ramach działania określonego w pkt 4.4.1 lit. e) Strategia wskazuje wprost na potrzebę rozwoju krajowych narzędzi i systemów monitorowania i alarmowania o zakłóceniach systemów nawigacji satelitarnej GNSS (GPS, Galileo), w szczególności pod kątem jammingu, spoofingu i meaconingu.
Zakres przedsięwzięcia Polska Tarcza PNT – Moduł 1 jest bezpośrednio zgodny z tym działaniem. Projekt przewiduje bowiem rozwój krajowych zdolności monitorowania GNSS, identyfikacji i klasyfikacji zakłóceń, alarmowania o ich wystąpieniu oraz dystrybucji informacji o jakości i wiarygodności usług PNT do podmiotów publicznych, sektora bezpieczeństwa i obronności oraz operatorów infrastruktury krytycznej.
W konsekwencji przedsięwzięcie należy traktować przede wszystkim jako element wzmacniający dojrzałość i efektywność krajowego systemu cyberbezpieczeństwa oraz odporność systemów informacyjnych, zgodnie z celami 1.3.1 i 1.3.3 Strategii. Cel 4.4.1 lit. e) stanowi natomiast dodatkowe, bezpośrednie potwierdzenie zasadności realizacji projektowanych rozwiązań w obszarze monitorowania i alarmowania o zakłóceniach GNSS.

## Jakie inne strategie, polityki publiczne lub wymagania strategiczne realizuje przedsięwzięcie?

1. Strategia Bezpieczeństwa Narodowego RP 2020

Przedsięwzięcie wpisuje się w obszar odporności państwa, przeciwdziałania zagrożeniom hybrydowym oraz zapewnienia ciągłości funkcjonowania państwa i odtwarzania kluczowych zdolności.
Projekt wzmacnia odporność państwa na zakłócenia usług pozycjonowania, nawigacji i czasu, w szczególności na jamming i spoofing GNSS. Budowa zintegrowanej warstwy monitorowania, detekcji, lokalizacji zakłóceń i alarmowania zwiększy zdolność administracji, służb, wojska, operatorów infrastruktury krytycznej i sektorów regulowanych do utrzymania ciągłości działania w warunkach zagrożeń hybrydowych.

2. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Przedsięwzięcie realizuje cele związane z rozwojem krajowego systemu cyberbezpieczeństwa, podnoszeniem odporności systemów informacyjnych w sferze publicznej i prywatnej oraz rozwojem zdolności zapobiegania i reagowania na incydenty.
Projekt tworzy państwową warstwę cyberodporności dla usług PNT/GNSS. Produkty projektu, w tym platforma integracyjna, mechanizmy detekcji incydentów, alertowania, analityki i raportowania, umożliwią szybszą identyfikację incydentów, ocenę ich wpływu oraz koordynację reakcji między podmiotami publicznymi i sektorowymi.

3. Program Fundusze Europejskie na Rozwój Cyfrowy 2021–2027, Działanie 4.1 „Wzmocnienie cyberbezpieczeństwa oraz rozwój odpornej infrastruktury przetwarzania danych"

Przedsięwzięcie bezpośrednio wpisuje się w działanie 4.1 FERC, którego celem jest zwiększenie poziomu bezpieczeństwa informacji, odporności infrastruktury teleinformatycznej oraz zdolności zapobiegania i reagowania na incydenty w systemach informacyjnych państwa.
Projekt realizuje ten cel przez wdrożenie systemu zwiększającego bezpieczeństwo informacji i odporność usług publicznych zależnych od wiarygodnej pozycji, czasu i synchronizacji.
Zakładane produkty obejmują systemy bezpieczeństwa informacji, infrastrukturę monitorującą, komponenty analityczne, środowisko chmurowe oraz szkolenia użytkowników.

4. Narodowy Program Ochrony Infrastruktury Krytycznej

Przedsięwzięcie wpisuje się w priorytety dotyczące współpracy uczestników systemu ochrony infrastruktury krytycznej, zapewnienia ciągłości działania kluczowych systemów i usług oraz zarządzania ryzykiem.
Projekt ogranicza ryzyko przerw w funkcjonowaniu systemów energetycznych, telekomunikacyjnych, transportowych, centrów danych i innych usług zależnych od czasu oraz pozycji. Dostarcza operatorom infrastruktury krytycznej informacje o degradacji sygnału, alerty, dane analityczne i wspólny obraz sytuacyjny wspierający ciągłość działania.

5. Program Otwierania Danych na lata 2021–2027
Projekt wpisuje się w cele dotyczące poprawy interoperacyjności i jakości danych, automatycznego udostępniania i aktualizowania zasobów danych oraz ponownego wykorzystania danych sektora publicznego.
Przedsięwzięcie zwiększa jakość, aktualność i użyteczność danych dotyczących PNT/GNSS. Dane o jakości sygnału, stanie usług, zakłóceniach i obszarach degradacji będą mogły być udostępniane w ustandaryzowanej formie, co wspiera ich ponowne wykorzystanie przez administrację, sektor prywatny, naukę i operatorów usług krytycznych.
6. Krajowy Program Kosmiczny na lata 2021–2026
Przedsięwzięcie wpisuje się w cele dotyczące zwiększenia wykorzystania danych satelitarnych przez administrację, naukę, przemysł i społeczeństwo oraz wykorzystania technologii satelitarnych dla bezpieczeństwa i obronności kraju.
Projekt wykorzystuje dane i technologie GNSS jako kluczową część krajowego ekosystemu usług satelitarnych. Rozbudowa monitorowania jakości GNSS, wykrywania zakłóceń i ochrony usług PNT wzmacnia bezpieczeństwo wykorzystania technologii satelitarnych w administracji, gospodarce, obronności i zarządzaniu kryzysowym.
7. Strategia Zrównoważonego Rozwoju Transportu do 2030 r.
Projekt wpisuje się w cel dotyczący poprawy bezpieczeństwa, efektywności i niezawodności sektora transportowego.
Przedsięwzięcie wspiera bezpieczeństwo i ciągłość działania procesów transportowych zależnych od precyzyjnej pozycji i czasu, w tym lotnictwa, kolei, logistyki, transportu drogowego i systemów zarządzania ruchem. Alerty o degradacji GNSS pozwolą szybciej identyfikować obszary ryzyka i ograniczać skutki zakłóceń.

# 2.1. Cele i korzyści wynikające z przedsięwzięcia

| | |
|---|---|
| **Cel - 1** | Podniesienie poziomu odporności państwa poprzez wdrożenie wokół ASG-EUPOS zintegrowanych systemów monitorowania jakości GNSS i usług ASG-EUPOS, wykrywania i lokalizacji zakłóceń oraz ochrony warstwy fizycznej PNT. |
| **Cel strategiczny** | 1. Strategia Cyfryzacji Państwa.,<br>obszar horyzontalny 1.3 Cyberbezpieczeństwo, cel/kierunek 1.3.3 „Centralne pozyskiwanie i rozwój rozwiązań cyberbezpieczeństwa”.<br>Projekt Polska Tarcza PNT – Moduł 1 realizuje założenia Strategii poprzez budowę zintegrowanej zdolności monitorowania jakości i wiarygodności usług PNT/GNSS, wykrywania, klasyfikacji i lokalizacji zakłóceń oraz wymiany informacji o zdarzeniach wpływających na pozycję, nawigację i czas. Platforma integracyjna, mechanizmy analityczne, system alertowania oraz wspólny obraz sytuacyjny będą wspierały współdziałanie administracji publicznej, Sił Zbrojnych RP, służb, organów regulacyjnych i nadzorczych oraz operatorów infrastruktury krytycznej. Przedsięwzięcie zwiększy tym samym zdolność instytucji państwa do identyfikacji zagrożeń, szybkiej wymiany informacji, oceny ich wpływu oraz koordynacji działań podejmowanych w odpowiedzi na incydenty dotyczące PNT/GNSS.<br>2. Strategia Bezpieczeństwa Narodowego RP 2020<br>Cel: Odporność państwa i obrona powszechna – podniesienie odporności państwa na zagrożenia, w tym zagrożenia o charakterze hybrydowym; budowanie zdolności do odtwarzania niezbędnych zasobów.<br>3. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej, przyjęta przez Radę Ministrów 10 marca 2026 r.<br>Cel szczegółowy 1. Rozwój krajowego systemu cyberbezpieczeństwa<br>Cel szczegółowy 3. Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej<br>(w tym militarnej) oraz prywatnej .<br>4. Narodowy Program Ochrony Infrastruktury Krytycznej |

| | |
|---|---|
| | Priorytet 1. pogłębienie współpracy między uczestnikami Programu w obszarze ochrony IK,<br>5. Program Otwierania Danych na lata 2021–2027<br>Cel 2: poprawa interoperacyjności i jakości danych; działania dotyczące podnoszenia jakości danych oraz automatycznego udostępniania i aktualizowania zasobów danych.<br>6. Krajowy Program Kosmiczny na lata 2021–2026<br>Cel 2. zwiększenie wykorzystania danych satelitarnych przez administrację, naukę, przemysł<br>i społeczeństwo;<br>Cel 3. wykorzystanie technologii satelitarnych do zwiększenia bezpieczeństwa i obronności kraju.<br>7. Strategia Zrównoważonego Rozwoju Transportu do 2030 roku<br>Cel główny: zwiększenie dostępności transportowej kraju oraz poprawa bezpieczeństwa uczestników ruchu i efektywności sektora transportowego<br>8. Krajowy Plan Bezpieczeństwa 2026–2028 |
| **Korzyść:** | Projekt przyniesie kluczową korzyść w postaci utworzenia jednej panoramy PNT dla państwa, czyli wspólnego, zintegrowanego obrazu sytuacji w zakresie jakości sygnałów GNSS, działania usług ASG-EUPOS, występowania zakłóceń oraz wpływu degradacji sygnału na usługi publiczne, gospodarcze, obronne i infrastrukturalne. Obecnie informacje o stanie usług PNT są rozproszone, sektorowe i nie tworzą jednolitego obrazu sytuacyjnego. Projekt pozwoli na przejście od reakcji fragmentarycznej do zarządzania opartego na wspólnych danych, metrykach jakości, mapach degradacji, alertach i analizie wpływu incydentów.<br>Istotną korzyścią będzie natychmiastowe alarmowanie i triage incydentów PNT. System umożliwi szybkie wykrywanie, klasyfikowanie i priorytetyzowanie zdarzeń, takich jak jamming, spoofing, degradacja jakości GNSS, utrata dostępności usług lub anomalie w pracy stacji referencyjnych. Dzięki temu administracja publiczna, MON, służby, regulatorzy, operatorzy infrastruktury krytycznej i wybrane sektory gospodarki uzyskają możliwość szybkiego rozpoznania, czy dane zdarzenie ma charakter lokalny, sektorowy, transgraniczny, przypadkowy czy potencjalnie wrogi. Pozwoli to skrócić czas reakcji, ograniczyć skutki zakłóceń oraz usprawnić koordynację działań między instytucjami.<br>Projekt zwiększy również zdolność państwa do utrzymania ciągłości wyznaczania pozycji i czasu w modelu usługowym, nawet przy aktywnych zakłóceniach GNSS. Oznacza to, że użytkownicy nie będą otrzymywać wyłącznie informacji o awarii lub degradacji, lecz dostęp do uporządkowanych usług wspierających ocenę wiarygodności pozycji i czasu, identyfikację obszarów ryzyka, wybór bezpieczniejszych źródeł danych oraz kontynuację działania procesów zależnych od PNT. Jest to szczególnie ważne dla geodezji, budownictwa, transportu, energetyki, telekomunikacji, finansów, lotnictwa, służb ratunkowych i infrastruktury krytycznej.<br>W efekcie projekt podniesie odporność państwa poprzez zapewnienie wspólnego obrazu sytuacyjnego, szybkiego ostrzegania, lepszego zarządzania incydentami oraz ciągłości usług zależnych od precyzyjnej pozycji i czasu. Korzyści będą miały charakter systemowy: zwiększą bezpieczeństwo danych przestrzennych, ograniczą ryzyko błędów pomiarowych i operacyjnych, poprawią współdziałanie instytucji oraz wzmocnią zdolność administracji i sektorów regulowanych do funkcjonowania w warunkach zakłóceń hybrydowych. |

| | |
|---|---|
| **KPI:** | KPI 1 – Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych.<br>KPI 2– Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa.<br>KPI 3– Liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych.<br>KPI 4 – Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym.<br>KPI 5– Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym.<br>KPI 6 – Liczba systemów, modułów lub komponentów służących zwiększeniu poziomu bezpieczeństwa informacji.<br>KPI 7 - Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych<br>KPI 8 - Średni czas wykrywania incydentów PNT |
| **Wartość aktualna i docelowa KPI:** | KPI 1- 0<br>KPI 2- 0<br>KPI 3- 0<br>KPI 4- 0<br>KPI 5- 0<br>KPI 6- 0<br>KPI 7- 0<br>KPI 8- nie jest monitorowany<br>KPI 1- 1<br>KPI 2- 2<br>KPI 3- 0<br>KPI 4- 20<br>KPI 5- 200<br>KPI 6- 7<br>KPI 7- 10000<br>KPI 8- 20 |
| **Metoda pomiaru KPI** | Pomiar wskaźników produktu będzie prowadzony narastająco w trakcie realizacji projektu, w powiązaniu z odbiorami etapowymi, dokumentacją projektową, protokołami odbioru oraz dokumentacją szkoleniową. Dla każdego KPI określa się następujący sposób pomiaru, źródło danych, częstotliwość pomiaru oraz termin pomiaru wartości docelowej:<br>KPI 1 – Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych<br>Sposób pomiaru: liczba instytucji publicznych objętych wsparciem w ramach projektu, potwierdzona udziałem w realizacji lub odbiorze produktu cyfrowego.<br>Źródło danych: umowa o dofinansowanie, dokumentacja projektowa, protokoły odbioru produktów, dokumenty potwierdzające udział Beneficjenta w projekcie.<br>Częstotliwość pomiaru: po zakończeniu kluczowych etapów realizacji projektu oraz przy odbiorze końcowym.<br>Termin pomiaru wartości docelowej: do dnia zakończenia rzeczowej realizacji projektu, tj. do 31.10.2028 r.<br>KPI 2 – Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa<br>Sposób pomiaru: liczba podmiotów, które uzyskały wsparcie w zakresie cyberbezpieczeństwa poprzez udział w projekcie, dostęp do produktów projektu, komponentów bezpieczeństwa, procedur, alertów, szkoleń lub rozwiązań wzmacniających odporność PNT/GNSS. |

| | |
|---|---|
| | Źródło danych: umowa o dofinansowanie, porozumienia lub umowy partnerskie, protokoły odbioru, dokumentacja wdrożeniowa, rejestry udostępnienia produktów projektu.<br>Częstotliwość pomiaru: kwartalnie w trakcie realizacji projektu oraz przy odbiorze końcowym.<br>Termin pomiaru wartości docelowej: do dnia zakończenia rzeczowej realizacji projektu, tj. do 31.10.2028 r.<br>KPI 3 – Liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych<br>Sposób pomiaru: liczba podmiotów, które uzyskały wsparcie poprzez wdrożenie lub udostępnienie usług, produktów lub procesów cyfrowych powstałych w projekcie - nie dotyczy<br>KPI 4 – Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym<br>Sposób pomiaru: liczba pracowników IT, którzy ukończyli szkolenie, ćwiczenie lub instruktaż związany z obsługą, utrzymaniem, bezpieczeństwem lub rozwojem produktów projektu.<br>Źródło danych: listy obecności, rejestry uczestników szkoleń, raporty z systemu LMS/LRS, certyfikaty ukończenia, testy wiedzy, protokoły realizacji szkoleń.<br>Częstotliwość pomiaru: po każdym szkoleniu lub cyklu szkoleniowym oraz zbiorczo kwartalnie.<br>Termin pomiaru wartości docelowej: najpóźniej do zakończenia etapu szkoleń i odbioru końcowego projektu, tj. do 31.10.2028 r.<br>KPI 5 – Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym<br>Sposób pomiaru: liczba pracowników nie-IT, w szczególności operatorów, dyspozytorów, analityków, pracowników komórek operacyjnych, zarządzania kryzysowego, administracji i innych użytkowników instytucjonalnych, którzy ukończyli szkolenie dotyczące korzystania z produktów projektu, interpretacji alertów, raportów i informacji o jakości PNT/GNSS.<br>Źródło danych: listy obecności, rejestry uczestników szkoleń, raporty LMS/LRS, ankiety poszkoleniowe, certyfikaty, protokoły realizacji szkoleń.<br>Częstotliwość pomiaru: po każdym szkoleniu lub cyklu szkoleniowym oraz zbiorczo kwartalnie.<br>Termin pomiaru wartości docelowej: najpóźniej do zakończenia etapu szkoleń i odbioru końcowego projektu, tj. do 31.10.2028 r.<br>KPI 6 – Liczba systemów, modułów lub komponentów służących zwiększeniu poziomu bezpieczeństwa informacji<br>Sposób pomiaru: liczba odebranych i uruchomionych systemów, modułów lub komponentów służących zwiększeniu poziomu bezpieczeństwa informacji, w szczególności w zakresie monitorowania, detekcji, analizy, alertowania, raportowania, integracji danych, kontroli dostępu, rejestrowania zdarzeń i ochrony usług PNT/GNSS: Status GNS, Status ASG EUPOS, MultiPNTPoint, GNSS Signal Quality Monitoring, Interface Serach & Find, Coordinates monitoring, Platforma integracyjna,<br>Źródło danych: protokoły odbioru, dokumentacja techniczna, dokumentacja powykonawcza, raporty z testów bezpieczeństwa i wydajności, potwierdzenia uruchomienia produkcyjnego.<br>Częstotliwość pomiaru: po odbiorze każdego systemu, modułu lub komponentu oraz zbiorczo przy odbiorach etapowych i końcowym.<br>Termin pomiaru wartości docelowej: do dnia odbioru końcowego i uruchomienia systemu Polska Tarcza PNT – Moduł 1, tj. do 31.10.2028 r. |

| | |
|---|---|
| | KPI 7 - Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych<br>Sposób pomiaru: pomiar na podstawie liczby unikalnych kont lub identyfikatorów korzystających z paneli Status GNSS/ASG-EUPOS, portalu ISAC PNT, dashboardów NOC, feedów publicznych, usług ASG-EUPOS. Liczba aktywnych kont lub kluczy API z sektora publicznego raportowana półrocznie.<br>Źródło: IdP/IdM, gateway API, logi SIEM, baza danych ASG-EUPOS.<br>Termin pomiaru wartości docelowej: 12 miesięcy od dnia odbioru końcowego i uruchomienia systemu Polska Tarcza PNT – Moduł 1, tj. do 31.10.2029 r.<br>KPI 8 - Średni czas wykrywania incydentów PNT<br>Sposób pomiaru: Średni czas wykrycia incydentu PNT, liczony jako czas od zaistnienia incydentu do powiadomienia o zaistnieniu incydentu;<br>źródło – logi systemowe oraz raporty z pomiarów terenowych wykonanych w terminie 12 miesięcy od dnia odbioru końcowego i uruchomienia systemu Polska Tarcza PNT – Moduł 1, tj. do 31.10.2029 r. |

## 2.2. Udostępnione e-usługi

| Lp. | Nazwa e-usługi | Typ | Zakres oddziaływania | Poziom dojrzałosci e-usługi |
|---|---|---|---|---|
| | | | | |

## 2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

## 2.4. Produkty końcowe przedsięwzięcia

| Nazwa produktu | Planowana data wdrożenia |
|---|---|
| Raport z inicjalnego testu prywatności | 12-2026 |
| Dokumentacja analityczna | 01-2027 |
| Projekt architektury Systemu | 01-2027 |
| Projekty wykonawcze teletechniczne | 04-2027 |
| Infrastruktura teletechniczna stacji referencyjnych i monitorujących | 10-2027 |
| Dokumentacja powykonawcza | 02-2028 |
| Materiały szkoleniowe | 06-2028 |
| Raport z testów wydajności | 09-2028 |
| Raport z testów bezpieczeństwa | 09-2028 |
| System teleinformatyczny Polska Tarcza PNT - Moduł 1 | 10-2028 |
| API systemu teleinformatycznego Polska Tarcza PNT - Moduł 1 | 10-2028 |

| Nazwa produktu | Planowana data wdrożenia |
|---|---|
| Zmodyfikowany system ASG-EUPOS | 10-2028 |
| Raport z weryfikacyjnego testu prywatności | 10-2028 |

# 3. KAMIENIE MILOWE

| Kamienie milowe | Planowany termin osiągnięcia |
|---|---|
| Przeprowadzony inicjalny test prywatności | 2026-12-31 |
| Zatwierdzony projekt architektury Systemu | 2027-01-31 |
| Rozstrzygnięte postępowanie przetargowe na dostawę urządzeń oraz opracowanie komponentów systemu | 2027-05-31 |
| Uruchomione stacje referencyjne i monitorujące | 2027-10-30 |
| Rozpoczęte procesy testowania oprogramowania | 2028-01-03 |
| Rozpoczęty pilotaż operacyjny | 2028-03-01 |
| Uzyskany pozytywny wynik testów wydajności i bezpieczeństwa | 2028-08-30 |
| Przeprowadzony weryfikacyjny test prywatności | 2028-10-10 |
| Zakończone szkolenia | 2028-10-20 |
| Uruchomiony system teleinformatyczny Polska Tarcza PNT - Moduł 1 | 2028-10-30 |

# 4. KOSZTY

## 4.1. Koszty ogólne przedsięwzięcia wraz ze sposobem finansowania

| | | |
|---|---|---|
| **Całkowity koszt przedsięwzięcia (netto oraz brutto), w tym** | Netto 22 895 622,44 zł<br>Brutto 27 000 000,00 zł | |
| **Procent dofinansowania ze środków UE (brutto)** | 89,93% | |
| **Procent dofinansowania ze środków z innych źródeł zagranicznych (brutto)** | | |
| **Procent środków z budżetu państwa (brutto)** | 10,07% | |
| **Podział całkowitego kosztu przedsięwzięcia na poszczególna lata (netto oraz brutto)** | 2026 | Netto 317 168,80 zł<br>Brutto 317 168,80 zł |
| | 2027 | Netto 14 994 315,12 zł<br>Brutto 17 831 209,48 zł |
| | 2028 | Netto 7 584 138,52 zł<br>Brutto 8 851 621,72 zł |

## 4.2. Wykaz poszczególnych pozycji kosztowych

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|---|---|---|---|
| Oprogramowanie | Zakup oprogramowania dedykowanego oraz wytworzenie platformy integracyjnej Polska Tarcza PNT Moduł 1 | 16 176 848,46 zł | Pozycja kosztowa jest niezbędna do budowy centralnego, wysokodostępnego środowiska integracji, akwizycji, przetwarzania i wizualizacji danych PNT/GNSS, stanowiącego podstawę „jednej panoramy PNT dla państwa”. Pozycja zawiera koszt zakupu dedykowanych rozwiązań aplikacyjnych w wysokości 13 139 497,46 zł. oraz koszt pracy zespołu programistów i zespołu bezpośrednio zaangażowanego w wytwarzanie oprogramowania w wysokości 3 037 351,00 zł. |
| Infrastruktura | Sprzęt pomiarowy i teleinformatyczny wraz z montażem oraz instalacją i | 8 290 000,00 zł | Pozycje kosztowe dotyczące sprzętu są niezbędne do budowy rozproszonej, odpornej warstwy pomiarowej i brzegowej projektu, |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|---|---|---|---|
| | konfiguracją. Zasoby infrastruktury obliczeniowej (CPU/GPU/NPU, RAM, storage, stos sieciowy, routing, load balancing) | | obejmującej odbiorniki GNSS, anteny, sensory, urządzenia czasu, elementy detekcji zakłóceń, osprzęt, montaż, konfigurację oraz utrzymanie lokalizacji. Sprzęt ten zapewni pozyskiwanie wiarygodnych danych źródłowych w terenie, lokalne przetwarzanie sygnałów, weryfikację jakości PNT/GNSS, wykrywanie anomalii oraz zasilanie centralnej platformy integracyjnej danymi w czasie zbliżonym do rzeczywistego. Bez zakupu i instalacji komponentów sprzętowych niemożliwe byłoby osiągnięcie zakładanych zdolności monitorowania, alarmowania, lokalizacji zakłóceń oraz utrzymania ciągłości usług PNT w warunkach degradacji lub aktywnych zakłóceń GNSS. Zasoby infrastruktury obliczeniowej służyć będą do do obsługi danych z ASG-EUPOS i systemów dziedzinowych, trenowania oraz uruchamiania modeli AI, a także generowania alertów i raportów w czasie zbliżonym do rzeczywistego.Bez tego komponentu niemożliwe byłoby spójne zarządzanie usługami, szybka kwalifikacja i priorytetyzacja incydentów, interoperacyjna wymiana informacji i utrzymanie ciągłości działania usług PNT przy zakłóceniach GNSS. |
| Koszty UX i grafiki | | | |
| Bezpieczeństwo | Testy bezpieczeństwa rozwiązania | 40 000,00 zł | Testy bezpieczeństwa zlecone podmiotowi zewnętrznemu. |
| Wydajność rozwiązań | Testy wydajności rozwiązania | 10 000,00 zł | Testy wydajności zlecone podmiotowi zewnętrznemu. |
| Szkolenia | Szkolenia personelu | 465 000,00 zł | Szkolenia są niezbędne do zapewnienia prawidłowego wykorzystania wdrażanych systemów monitorowania, detekcji, alarmowania i analizy |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|---|---|---|---|
| | | | jakości PNT/GNSS przez administratorów, operatorów oraz użytkowników instytucjonalnych. Obejmą obsługę platformy, interpretację alertów i raportów, procedury reagowania na incydenty, zarządzanie dostępem, wymianę informacji oraz utrzymanie ciągłości usług w sytuacji zakłóceń GNSS. Bez komponentu szkoleniowego pełne wykorzystanie funkcjonalności projektu, prawidłowa reakcja na incydenty oraz trwałość efektów wdrożenia byłyby istotnie ograniczone. : Materiały szkoleniowe, instrukcje oraz pozostałe materiały edukacyjne opracowane w ramach projektu będą spełniały obowiązujące wymagania dostępności cyfrowej, w tym wymagania WCAG 2.2 na poziomie AA, w zakresie mającym zastosowanie do danego rodzaju materiału. |
| Działania informacyjno-promocyjne | Tablica informacyjna | 5000,00 zł | Wykonanie tablicy informacyjnej zgodnie z zasadami promocji |
| Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego) | Zespół zarządzający i administracyjny GUGiK | 2 013 151,54 zł | Koszty zarządzania i wsparcia są niezbędne do zapewnienia koordynacji projektu, kontroli harmonogramu, budżetu, ryzyk, jakości produktów oraz zgodności realizacji z wymaganiami programu. Obejmują wynagrodzenia personelu wspomagającego, który będzie nie tylko obsługiwał projekt administracyjnie i rozliczeniowo, lecz także współtworzył rozwiązanie poprzez udział w analizie wymagań, uzgodnieniach z partnerami, testach, odbiorach, przygotowaniu procedur, dokumentacji użytkowej i organizacji wdrożenia. Bez tego zaangażowania skuteczna realizacja złożonego, |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|---|---|---|---|
| | | | wielopodmiotowego systemu byłaby obarczona ryzykiem opóźnień, błędów formalnych, niespójności wymagań oraz ograniczonej użyteczności końcowego rozwiązania. |

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

| Całkowity koszt utrzymania trwałości przedsięwzięcia (brutto) | 1 926 038,00 zł | | Źródło finansowania |
|---|---|---|---|
| Podział całkowitego kosztu utrzymania trwałości przedsięwzięcia na poszczególna lata (netto oraz brutto) | 2028 | 68 412,00 zł (brutto)<br>(55 619,51 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2029 | 430 991,00 zł (brutto)<br>(350 399,19 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2030 | 452 541,00 zł (brutto)<br>(367 919,51 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2031 | 475 168,00 zł (brutto)<br>(386 315,44 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2032 | 498 926,00 zł (brutto)<br>(405 630,89 zł netto) | krajowe środki publiczne - budżet państwa |

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

- 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 przedsięwzięcia

| Nazwa ryzyka | Siła oddziaływania | Prawdopo-dobieństwo wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
|---|---|---|---|
| Niepowodzenia wyboru wykonawców w planowanych terminach w ramach postępowań przetargowych | Duża | Średnie | Stały monitoring etapu realizacji, zabezpieczenie w zespole wsparcia w zakresie sprawnego przygotowania i prowadzenia postępowań przetargowych tak, aby ograniczyć ryzyko opóźnień. |
| Niedoszacowanie kosztów projektu. | Duża | Średnie | Stały monitoring realizacji projektu i poszczególnych etapów, elastyczne reagowanie na warunki rynkowe. |
| Odejście z pracy / zaangażowanie do innych inicjatyw osób kluczowych dla realizacji projektu. Rotacja na stanowiskach osób zaangażowanych w realizację działań projektowych. | Średnia | Średnie | Zapewnienie odpowiedniej komunikacji w projekcie. System motywacyjny dla zespołu projektowego.<br>Zapewnienie stabilnego zespołu projektowego w całym okresie realizacji projektu. |
| Ryzyko braku lub opóźnienia integracji z systemami zewnętrznymi: e-CzasPL, Geoportal, IMGW | Średnia | Niskie | Analiza udostępnianych mechanizmów API. |
| Ryzyko powstania ograniczeń w udostępnianiu danych operacyjnych lub wrażliwych, szczególnie danych o źródłach zakłóceń i incydentach | Duża | Średnie | Wdrożenie modelu wielopoziomowego dostępu do informacji, obejmującego klasyfikację danych według poziomu wrażliwości, kontrolę dostępu opartą na rolach, anonimizację lub generalizację danych lokalizacyjnych oraz rozdzielenie warstwy publicznej, sektorowej i operacyjnej systemu. Dane o incydentach PNT/GNSS będą udostępniane w zakresie adekwatnym do potrzeb odbiorców: publicznie w formie statusów, alertów i informacji zagregowanych, a szczegółowo wyłącznie uprawnionym instytucjom. Dodatkowo zostaną wdrożone procedury zatwierdzania komunikatów, rejestracji dostępu, szyfrowania transmisji oraz |

| Nazwa ryzyka | Siła oddziaływania | Prawdopo-dobieństwo wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
|---|---|---|---|
| | | | uzgadniania zasad wymiany informacji z partnerami, co pozwoli pogodzić potrzebę ostrzegania użytkowników z wymogami bezpieczeństwa państwa i ochrony danych operacyjnych. |
| Ryzyko niezachowania interoperacyjności i jakości danych: różne formaty, częstotliwości, opóźnienia, poziomy ufności, metadane i klasyfikacja zdarzeń. | Średnia | Niskie | Ryzyko to będzie ograniczane poprzez opracowanie wspólnego modelu danych i słowników pojęć, zdefiniowanie minimalnego zakresu metadanych, ujednolicenie klasyfikacji zdarzeń, określenie standardów API i formatów wymiany, a także wdrożenie mechanizmów walidacji, normalizacji, deduplikacji i kontroli jakości danych |
| Ryzyko opóźnień dostaw wyspecjalizowanego sprzętu (Np.GNSS/RF/SDR/czasu) | Duża | Średnie | Ryzyko będzie ograniczane przez wczesne rozpoczęcie postępowań zakupowych, analizę rynku przed zamówieniem, dopuszczenie rozwiązań równoważnych, unikanie nadmiernie zamkniętych specyfikacji, podział dostaw na pakiety, utrzymywanie rezerw czasowych oraz wymaganie dostępności serwisu, dokumentacji technicznej i wsparcia producenta |
| Przekroczenie harmonogramu realizacji projektu | Duża | Niskie | Ryzyko będzie zarządzane poprzez bieżące monitorowanie harmonogramu, identyfikację opóźnień na poziomie kamieni milowych i zadań krytycznych oraz wdrażanie działań korygujących, takich jak realokacja zasobów, priorytetyzacja prac, zwiększenie nadzoru nad wykonawcami i uruchamianie rezerw czasowych. |
| Nieosiągnięcie wskaźników produktu/celu oraz celu projektu | Średnia | Niskie | Ryzyko będzie ograniczane poprzez bieżący monitoring realizacji wskaźników produktu i celu na poziomie harmonogramu, odbiorów etapowych, rejestru ryzyk oraz cyklicznych raportów postępu, z przypisaniem odpowiedzialności za każdy wskaźnik do właścicieli merytorycznych i technicznych. W przypadku identyfikacji odchyleń wdrażane będą działania korygujące, w szczególności aktualizacja planu prac, zwiększenie nadzoru nad |

| Nazwa ryzyka | Siła oddziaływania | Prawdopo-dobieństwo wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
|---|---|---|---|
| | | | wykonawcami, priorytetyzacja produktów kluczowych dla osiągnięcia wskaźników oraz uruchomienie działań naprawczych przed odbiorem końcowym. |

## 5.2. Ryzyka wpływające na utrzymanie efektów

| Nazwa ryzyka | Siła oddziaływania | Prawdopo-dobieństwo wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
|---|---|---|---|
| Nieprzyznanie środków z budżetu państwa na utrzymanie produktów projektu | Duża | Średnie | Zabezpieczenie finansowania kosztów trwałości w budżecie państwa, coroczne planowanie potrzeb utrzymaniowych oraz przypisanie odpowiedzialności za eksploatację i utrzymanie produktów do GUGiK i IŁ-PIB zgodnie z zakresem trwałości projektu. Monitoring kosztów utrzymania i aktualizacja planów rzeczowo-finansowych w okresie trwałości. |
| Szybkie zestarzenie się technologii oraz nowe metody ataków cybernetycznych na systemy GPS/ GNSS/PNT | Duża | Średnie | Architektura w modelu rozwojowym o ciągłej aktualizacji. Planowanie aktualizacji, badanie trendów, monitorowanie sytuacji przez zespół devops. |
| Odejście kluczowych pracowników | Duża | Średnie | Dokumentacja wiedzy, plan sukcesji, prowadzenie ogólnego i specjalistycznego szkolenia wewnętrznego zespołu "gitdevsecops |
| Brak aktualizacji dokumentacji systemowej | Średnia | Średnie | Regularne przeglądy dokumentacji, bieżące dokumentowanie wprowadzanych zmian w systemie |
| Wzrost kosztów utrzymania | Duża | Średnie | Budżetowanie na utrzymanie, optymalizacja i monitoring wydatków. Sporządzanie kwartalnych notatek i meldunków dotyczących ewentualnego zwiększenia fnansowania projektu z środków budżetu państwa w celu zabezpieczenia prawidłowego rozwoju projektu. |

| Nazwa ryzyka | Siła oddziaływania | Prawdopo-dobieństwo wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
|---|---|---|---|
| Brak możliwości zatrudnienia osób o odpowiednich kompetencjach, Brak wystarczających środków na utrzymanie projektu | Duża | Niskie | Zgłaszanie z wyprzedzeniem do planów budżetów resortowych (MON, MC, MFiG, MRiT) oraz dysponentów potrzeb fnansowych na realizację i utrzymanie projektu. Sporządzanie kwartalnych notatek i meldunków dotyczących ewentualnego zwiększenia fnansowania projektu z środków budżetu państwa w celu zabezpieczenia prawidłowego rozwoju projektu. |
| Ryzyko braku stabilnego zespołu utrzymaniowego po zakończeniu projektu oraz utraty kompetencji domenowych PNT/GNSS/RF/IT. | Duża | Niskie | Ryzyko będzie ograniczane przez zaplanowanie modelu utrzymania już na etapie projektu, wskazanie właścicieli usług i ról operacyjnych, przygotowanie procedur eksploatacyjnych, dokumentacji technicznej, instrukcji reagowania na incydenty oraz planu przekazania wiedzy. Dodatkowo przewiduje się szkolenia administratorów i operatorów, udział personelu utrzymaniowego w testach i odbiorach, budowę bazy wiedzy, zapewnienie wsparcia producentów i wykonawców w okresie powdrożeniowym oraz określenie ścieżek rozwoju kompetencji dla zespołów GUGiK i IŁ |
| Ryzyko wzrostu kosztów chmury, licencji, cyberbezpieczeństwa, serwisu sprzętu i integracji API | Średnia | Średnie | Ryzyko będzie ograniczane przez przygotowanie modelu TCO dla fazy wdrożenia i utrzymania, wprowadzenie limitów zużycia zasobów chmurowych, monitoringu kosztów, mechanizmów skalowania, polityk retencji danych, optymalizacji liczby zapytań API oraz okresowej weryfikacji wykorzystania licencji. Dodatkowo przewiduje się stosowanie konkurencyjnych i przenaszalnych rozwiązań, negocjowanie warunków serwisu i wsparcia na kilka lat, zapewnienie rezerw budżetowych oraz regularny przegląd architektury pod kątem kosztów, bezpieczeństwa i efektywności utrzymania |
| Ryzyko dezaktualizacji modeli detekcji i | Duża | Niskie | Ryzyko będzie ograniczane przez zaplanowanie cyklicznej walidacji skuteczności modeli, okresowe |

| Nazwa ryzyka | Siła oddziaływania | Prawdopo-dobieństwo wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
|---|---|---|---|
| klasyfikacji zakłóceń oraz konieczności okresowego strojenia algorytmów AI/ML | | | dostrajanie progów detekcji, aktualizację zbiorów uczących, monitorowanie jakości klasyfikacji, testowanie modeli na danych historycznych i bieżących oraz utrzymywanie mechanizmów nadzoru eksperckiego nad wynikami automatycznej analizy. Ponadto przewiduje się wersjonowanie modeli, rejestrowanie decyzji algorytmicznych, możliwość ręcznej korekty klasyfikacji incydentów, procedury ponownego trenowania. |

# 6. OTOCZENIE PRAWNE

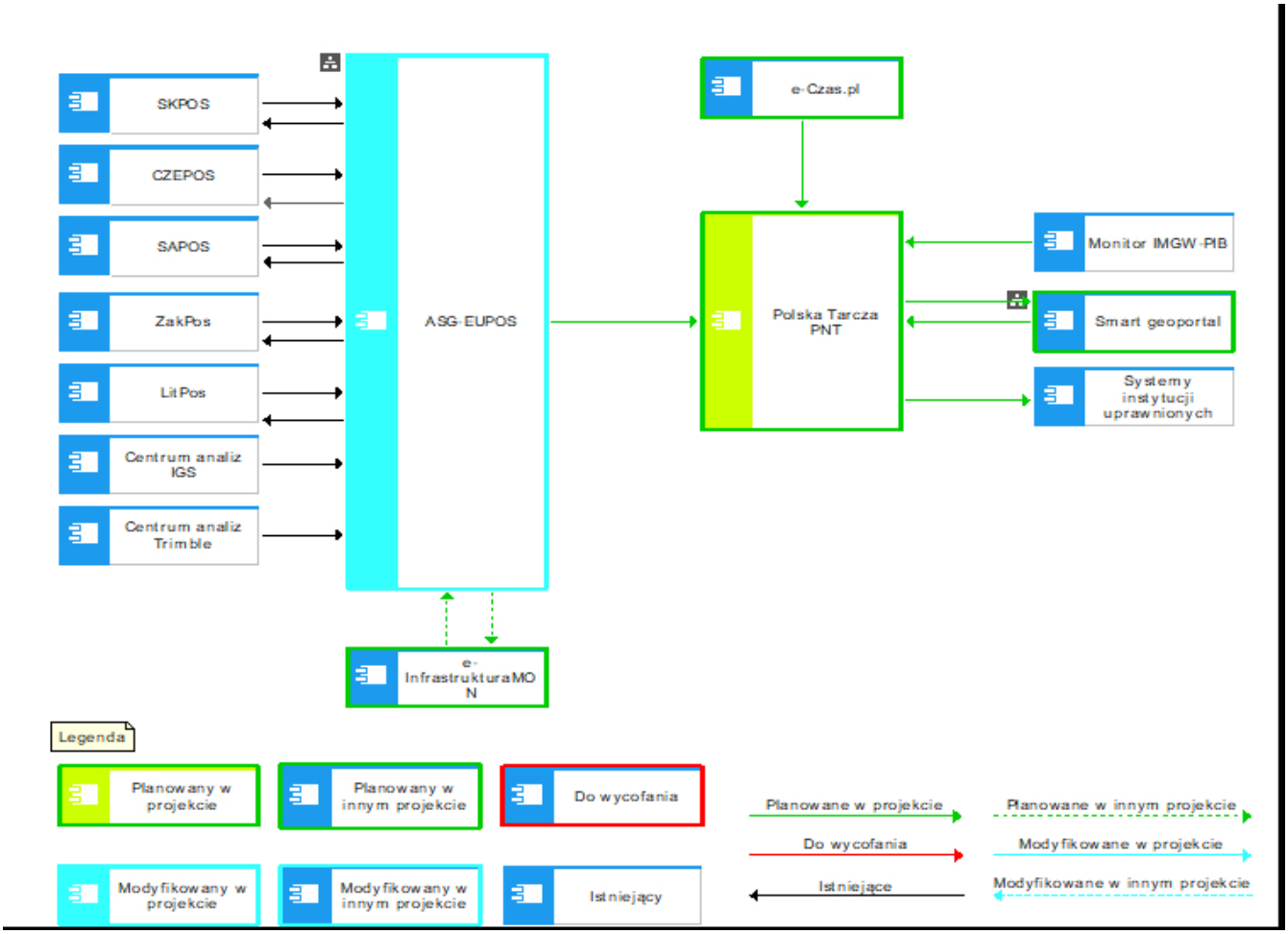
| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|---|---|---|---|---|
| 1 | Ustawa z 17 maja 1989 r. – Prawo geodezyjne i kartograficzne | ~~TAK~~/NIE | | |
| 2 | Ustawa z 4 marca 2010 r. o infrastrukturze informacji przestrzennej | ~~TAK~~/NIE | | |
| 3 | Rozporządzenie MAC z 16 stycznia 2015 r. w sprawie prac geodezyjnych i kartograficznych mających znaczenie dla obronności i bezpieczeństwa państwa oraz współdziałania GGK z MON | ~~TAK~~/NIE | | |
| 4 | Ustawa z 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa | ~~TAK~~/NIE | | |
| 5 | Ustawa z 11 marca 2022 r. o obronie Ojczyzny | ~~TAK~~/NIE | | |
| 6 | Rozporządzenie Rady Ministrów z 15 października 2012 r. w sprawie państwowego systemu odniesień przestrzennych | ~~TAK~~/NIE | | |
| 7 | Rozporządzenie MRPiT z 6 lipca 2021 r. w sprawie osnów geodezyjnych, grawimetrycznych i magnetycznych | ~~TAK~~/NIE | | |
| 8 | Rozporządzenie MRPiT z 7 lipca 2021 r. w sprawie standardów technicznych wykonywania geodezyjnych pomiarów sytuacyjnych i wysokościowych oraz opracowywania i przekazywania wyników | ~~TAK~~/NIE | | |

| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|---|---|---|---|---|
| | tych pomiarów do PZGiK | | | |
| 9 | Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne | ~~TAK~~/NIE | | |
| 10 | Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych | ~~TAK~~/NIE | | |
| 11 | Ustawa o krajowym systemie cyberbezpieczeństwa | ~~TAK~~/NIE | | |
| 12 | Ustawa o ochronie baz danych | ~~TAK~~/NIE | | |
| 13 | Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego | ~~TAK~~/NIE | | |
| 14 | Ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych | ~~TAK~~/NIE | | |
| 15 | Ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych | ~~TAK~~/NIE | | |
| 16 | Ustawa o doręczeniach elektronicznych | ~~TAK~~/NIE | | |
| 17 | Ustawa o usługach zaufania oraz identyfikacji elektronicznej | ~~TAK~~/NIE | | |
| 18 | Ustawa o ochronie informacji niejawnych | ~~TAK~~/NIE | | |
| 19 | Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), | ~~TAK~~/NIE | | |
| 20 | Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego | ~~TAK~~/NIE | | |
| 21 | Rozporządzenie Prezesa Rady Ministrów w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych | ~~TAK~~/NIE | | |
| 22 | Rozporządzenie Ministra Cyfryzacji w sprawie profilu zaufanego i podpisu zaufanego, | ~~TAK~~/NIE | | |

| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|---|---|---|---|---|
| 23 | Rozporządzenie Ministra Cyfryzacji w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników | ~~TAK~~/NIE | | |
| 24 | Ustawa o narodowym zasobie archiwalnym i archiwach | ~~TAK~~/NIE | | |

# 7. ARCHITEKTURA

## 7.1. Widok kooperacji aplikacji




## Lista systemów wykorzystywanych w przedsięwzięciu

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| 1 | ASG-EUPOS | Główny Urząd Geodezji i Kartografii | ASG-EUPOS – Aktywna Sieć Geodezyjna EUPOS to system wspierający przenoszenie i utrzymywanie na obszarze Polski geodezyjnych układów odniesienia oraz realizację precyzyjnych pomiarów satelitarnych GNSS.<br>Jego celem jest zapewnienie jednolitej, wiarygodnej i dokładnej państwowej infrastruktury odniesienia przestrzennego, zgodnej z europejskim systemem ETRS89, wykorzystywanej w geodezji, budownictwie, drogownictwie, administracji publicznej i innych zastosowaniach wymagających precyzyjnego określania ozycji. System wykorzystuje obserwacje satelitarne GNSS prowadzone przez sieć stacji referencyjnych rozmieszczonych na terenie Polski. Stacje te stanowią kluczowy element podstawowej osnowy geodezyjnej kraju i umożliwiają świadczenie usług korekcyjnych oraz obliczeniowych, w tym usług czasu rzeczywistego i postprocessingu. ASGEUPOS umożliwia także analizę stanu sygnałów GNSS, co ma znaczenie dla zapewnienia jakości, dokładności i niezawodności pomiarów.<br>Rejestry publiczne: system nie prowadzi | Modyfikowany | Rozszerzenie o monitoring jakości sygnału GNSS i statusu dostępności usług systemu ASG-EUPOS w ramach integracji z nowymi komponentami projektu: Status GNSS i Status ASG-EUPOS |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | rejestrów publicznych. Główne grupy funkcjonalności obejmują: - utrzymywanie i przenoszenie geodezyjnych układów odniesienia na obszarze Polski, - obsługę sieci stacji referencyjnych GNSS, - udostępnianie danych korekcyjnych w czasie rzeczywistym, - świadczenie usług RTK i DGNSS, - udostępnianie danych do obliczeń po zakończeniu pomiarów, - obsługę usług postprocessingu, - analizę obserwacji satelitarnych GNSS, wspieranie oceny jakości i stanu sygnału GNSS, zapewnienie danych dla prac geodezyjnych, kartograficznych, budowlanych i infrastrukturalnych. System integruje się z infrastrukturą referencyjną GUGiK, siecią stacji referencyjnych ASGEUPOS, systemami odbiorców usług GNSS oraz europejskimi strukturami odniesienia geodezyjnego, w tym z rozwiązaniami zgodnymi z ETRS89. W projekcie Polska Tarcza PNT system ASG-EUPOS stanowi bazowy państwowy zasób referencyjny, wokół którego rozwijane są zdolności monitorowania jakości GNSS, wykrywania zakłóceń oraz wzmacniania odporności usług PNT. | | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| 2 | Centrum analiz IGS | Międzynarodowy Serwis GNSS | System zagraniczny: Międzynarodowy Serwis GNSS (International GNSS Service - IGS) jest to organizacja naukowo-techniczna zrzeszająca Międzynarodowy Serwis GNSS (International GNSS Service - IGS) jest organizacją naukowo-techniczną zrzeszającą ośrodki badawcze, które obliczają i zapewniają dostęp do wysokiej jakości produktów GNSS obejmujących precyzyjne efemerydy satelitów GNSS, pozycje i prędkości stacji w globalnej sieci GNSS, parametry ruchu orbitalnego Ziemi (ruch i tempo zmian biegunów, długość dnia) oraz rozwiązania zegarowe dla stacji referencyjnych i satelitów. Celem IGS jest zachowanie jednolitości w opracowaniach GNSS. | Istniejący | Brak |
| 3 | Centrum analiz Trimble | Ośrodek techniczny firmy Trimble | System zagraniczny: Centrum analiz firmy Trimble, która jest producentem oprogramowania systemowego pracującego w systemie ASG-EUPOS. Na potrzeby prawidłowej pracy oprogramowania w systemie ASG-EUPOS są transmitowane z centrum analiz Trimble do centrów obliczeniowych ASG-EUPOS w czasie rzeczywistym przybliżone parametry orbit satelitów oraz poprawek do pracy zegarów satelitów. | Istniejący | Brak |
| 4 | CZEPOS | Państwowy system | System zagraniczny: Państwowy system stacji | Istniejący | Brak |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | Rpubliki Czeskiej | referencyjnych Republiki Czeskiej, (CZEPOS), to system wspierający pomiary GNSS na terenie Czech,który podobnie jak ASG-EUPOS posiada stacje referencyjne GNSS oraz centrum zarządzania z którego udostępnia usługi wspomagające i zwiekszające dokładność pomiarów GNSS. | | |
| 5 | e-Czas.pl | Główny Urząd Miar | e-CzasPL to system wspierający niezawodną i wiarygodną dystrybucję czasu urzędowego obowiązującego na terytorium Rzeczypospolitej Polskiej oraz polskiej realizacji czasu UTC(PL).<br>Jego celem jest zapewnienie administracji, obywatelom i podmiotom gospodarczym dostępu do źródła czasu generowanego w oparciu o państwowy wzorzec jednostek miar czasu i częstotliwości. System umożliwia synchronizację systemów komputerowych z czasem urzędowym przez Internet, a także udostępnia usługi monitorowania zgodności czasu użytkownika względem UTC(PL).<br>Rejestry publiczne:<br>system nie prowadzi rejestrów publicznych.<br>Główne grupy funkcjonalności obejmują:<br>- dystrybucję czasu urzędowego i UTC(PL) do systemów teleinformatycznych, - synchronizację czasu | Planowany | Brak |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | przez serwery czasu GUM, - monitorowanie zgodności czasu użytkownika względem UTC(PL), - prezentację czasu urzędowego w aplikacji e- Czas On-line, - udostępnianie informacji o różnicach między czasem systemowym użytkownika a czasem urzędowym, - wspieranie zastosowań wymagających wiarygodnego znakowania czasu, synchronizacji i kontroli poprawności czasu. System integruje się z systemami użytkowników poprzez usługi sieciowe synchronizacji czasu, w szczególności serwery czasu GUM: tempus1.gum.gov.pl i tempus2.gum.gov.pl. Rozwiązanie może być wykorzystywane przez administrację publiczną, przedsiębiorców, instytucje finansowe, przemysł oraz inne podmioty, dla których kluczowe znaczenie ma wiarygodny czas urzędowy, synchronizacja systemów i potwierdzanie zgodności czasu z UTC(PL). | | |
| 6 | e-InfrastrukturaMON | Ministerstwo Obrony Narodowej | e-InfrastrukturaMON to system wspierający gromadzenie, przetwarzanie i udostępnianie danych przestrzennych dotyczących infrastruktury wojskowej oraz obsługę elektronicznej | Planowany | Brak |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | komunikacji w sprawach związanych z planowaniem i zagospodarowaniem przestrzennym.<br>Celem systemu jest zapewnienie jednolitej bazy danych przestrzennych zawierającej informacje o infrastrukturze wojskowej, wspierającej procesy analityczne i decyzyjne związane z planowaniem i zagospodarowaniem przestrzennym, a także udostępnienie e-usług umożliwiających elektroniczną obsługę spraw i komunikację z interesariuszami.<br>System nie prowadzi rejestrów publicznych.<br>Główne grupy funkcjonalności<br>– Gromadzenie i udostępnianie danych przestrzennych o infrastrukturze wojskowej<br>– Wsparcie procesów planowania i zagospodarowania przestrzennego<br>– Udostępnianie e-usług umożliwiających elektroniczną obsługę spraw oraz komunikację z interesariuszami<br>– Udostępnianie narzędzi analitycznych wspierających procesy decyzyjne<br>– Analiza danych pozyskiwanych z obserwacji satelitarnych i systemów nawigacji satelitarnej<br>– Udostępnianie informacji o jakości sygnału GNSS | | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | – Udostępnianie informacji o warunkach pogody kosmicznej wpływających na technologie GNSS<br>System jest zintegrowany z krajowymi systemami teleinformatycznymi | | |
| 7 | LitPos | Państwowy system Litwy | System zagraniczny: Państwowy system stacji referencyjnych Litwy (LitPos), to system wspierający pomiary GNSS na terenie Litwy, który podobnie jak ASG-EUPOS posiada stacje referencyjne GNSS oraz centrum zarządzania z którego udostępnia usługi wspomagające i zwiekszające dokładność pomiarów GNSS. | Istniejący | Brak |
| 8 | Monitor IMGW-PIB | Instytut Meteorologii i Gospodarki Wodnej - Państwowy Instytut Badawczy | Monitor IMGW-PIB to system wspierający monitorowanie, analizę i prezentację danych meteorologicznych, hydrologicznych oraz klimatycznych na obszarze Polski.<br>Jego celem jest zapewnienie administracji, służbom, przedsiębiorcom i obywatelom dostępu do aktualnych informacji o warunkach pogodowych, stanie wód, zagrożeniach naturalnych oraz danych potrzebnych do zarządzania kryzysowego, ochrony ludności, planowania działań i oceny ryzyka. System gromadzi i udostępnia dane z sieci stacji meteorologicznych i hydrologicznych IMGWPIB oraz innych | Istniejący | Brak |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | źródeł pomiarowych. Umożliwia śledzenie bieżących warunków atmosferycznych, poziomów wód, zjawisk ekstremalnych, prognoz i ostrzeżeń. Wspiera decyzje w sytuacjach zagrożenia, w rolnictwie, gospodarce wodnej, transporcie, planowaniu przestrzennym, ochronie środowiska i badaniach klimatycznych.<br>Rejestry publiczne: system nie prowadzi rejestrów publicznych.<br>Główne grupy funkcjonalności obejmują: - monitoring meteorologiczny, w tym temperatury, opadów, ciśnienia, wiatru i innych parametrów pogodowych, - monitoring hydrologiczny, w tym stanów rzek, jezior i zbiorników wodnych, - prezentację danych pomiarowych w czasie rzeczywistym lub zbliżonym do rzeczywistego, - udostępnianie prognoz pogody i komunikatów, - publikację ostrzeżeń przed burzami, wichurami, powodziami, suszami i intensywnymi opadami, - dostęp do danych historycznych meteorologicznych i hydrologicznych, - wspieranie analiz klimatycznych, naukowych i planistycznych, - wspieranie zarządzania kryzysowego, ochrony ludności i gospodarki | | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | wodnej.<br>System integruje się z infrastrukturą pomiarową IMGW-PIB, sieciami stacji meteorologicznych i hydrologicznych, systemami prognozowania, bazami danych historycznych oraz kanałami udostępniania ostrzeżeń i komunikatów. Z systemu korzystają służby ratunkowe, administracja publiczna, rolnicy, planiści, przedsiębiorcy, naukowcy i obywatele potrzebujący wiarygodnych informacji o pogodzie, wodach i klimacie. | | |
| 9 | Polska Tarcza PNT | Główny Urząd Geodezji i Kartografii | Polska Tarcza PNT Moduł 1 to system wspierający monitorowanie, ochronę i utrzymanie ciągłości usług wyznaczania pozycji, nawigacji i czasu PNT/GNSS w Polsce. Jego celem jest podniesienie odporności państwa poprzez wdrożenie zintegrowanych narzędzi monitorowania jakości GNSS i usług ASG-EUPOS, wykrywania oraz lokalizacji zakłóceń, a także ochrony fizycznej warstwy usług PNT przed zagrożeniami takimi jak jamming, spoofing i degradacja sygnału. System tworzy wspólne środowisko analityczne i operacyjne dla administracji publicznej, GUGiK, MON, służb, operatorów infrastruktury krytycznej, regulatorów oraz użytkowników usług | Planowany | System, który powstanie w ramach projekt |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | zależnych od precyzyjnej pozycji i czasu. W projekcie przewidziano komponenty: Status GNSS, Status ASG-EUPOS, MultiPNTPoint, GNSS_signal quality monitoring, Interference Search&Find, Coordinates monitoring, Platforma integracyjna, co przedstawiono w schemacie kluczowych komponentów architektury rozwiązania. Rejestry publiczne: system nie prowadzi rejestrów publicznych. Główne grupy funkcjonalności obejmują: - monitorowanie jakości i dostępności sygnałów GNSS, - monitorowanie jakości i dostępności usług ASGEUPOS, - wykrywanie zakłóceń i anomalii PNT/GNSS, - lokalizację źródeł zakłóceń, - analizę wpływu zjawisk słonecznych na sygnały GNSS, - prezentację statusów, alertów, raportów i wizualizacji sytuacyjnych, - integrację danych z wielu źródeł referencyjnych i sektorowych, - wspieranie ciągłości wyznaczania pozycji i dystrybucji czasu, - ochronę usług PNT przed zakłóceniami w fizycznej warstwie cyberprzestrzeni. System integruje się z ASG-EUPOS, systemami monitorowania GNSS, systemami dziedzinowymi administracji publicznej, | | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | rozwiązaniami MON, infrastrukturą operatorów usług krytycznych oraz platformami wymiany informacji i alertów. W projekcie pełni rolę centralnej, państwowej warstwy monitorowania i odporności PNT, zapewniającej jedną panoramę sytuacyjną dla usług zależnych od pozycji, nawigacji i czasu. | | |
| 10 | SAPOS | Państwowy system Niemiec | System zagraniczny: Państwowy system stacji referencyjnych Niemiec (SAPOS), to system wspierający pomiary GNSS na terenie Niemiec, który podobnie jak ASG-EUPOS posiada stacje referencyjne GNSS oraz centrum zarządzania z którego udostępnia usługi wspomagające i zwiekszające dokładność pomiarów GNSS. | Istniejący | Brak |
| 11 | SKPOS | Państwowy system Słowacji | System zagraniczny: Państwowy system stacji referencyjnych Słowacji (SKPOS), to system wspierający pomiary GNSS na terenie Słowacji, który podobnie jak ASG-EUPOS posiada stacje referencyjne GNSS oraz centrum zarządzania z którego udostępnia usługi wspomagające i zwiekszające dokładność pomiarów GNSS. | Istniejący | Brak |
| 12 | Smart geoportal | Główny Urząd Geodezji i Kartografii | Smart Geoportal to system wspierający Główny Urząd Geodezji i Kartografii w pozyskiwaniu, przetwarzaniu, archiwizowaniu i | Planowany | Brak |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | udostępnianiu danych oraz usług geoprzestrzennych i fotogrametrycznych. Celem systemu jest integracja zasobów i usług GUGiK oraz zapewnienie obywatelom, administracji publicznej i przedsiębiorcom dostępu do danych, narzędzi analitycznych i wizualizacji wykorzystywanych m.in. w planowaniu przestrzennym, zarządzaniu kryzysowym, inwestycjach i analizach środowiskowych. System udostępnia informacje z rejestrów centralnych prowadzonych przez Głównego Geodetę Kraju: PRG, PRNG, PRPOG, EZiUDP, BDOT10k i BDOO, oraz stanowi punkt dostępu do rejestrów prowadzonych przez samorządy i inne organy, m.in. EGiB, GESUT, BDOT500, RCN i MPZP. W module PZGiK prowadzone są ewidencja materiałów zasobu, rejestr zgłoszeń prac geodezyjnych i kartograficznych oraz rejestr wniosków o udostępnienie materiałów zasobu. Główne grupy funkcjonalności obejmują: Geoportal 2D i 3D – wyszukiwanie, publikowanie, wizualizację i analizę danych przestrzennych, metadanych i dokumentów PZGiK; PZGiK – obsługę zgłoszeń i wniosków, | | |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | zakup oraz pobieranie danych i map; CAPAP – przetwarzanie danych, kontrolę ich jakości i spójności oraz udostępnianie analiz, usług i e-learningu; UMM – dostęp do danych PZGiK dla systemów powiadamiania ratunkowego; Wirtualnego Asystenta – wsparcie wyszukiwania informacji, doboru narzędzi analitycznych i dostępności usług. System wymienia dane z krajowymi systemami i rejestrami przez usługi IIP oraz interfejsy API, WMS, WMTS, WFS, SOAP i REST, m.in. z EMUiA, PRPOG, SZPRNG, SZNMT, SZPRG, ZSIN, systemami powiatowej części PZGiK, EGiB, ePUAP, Węzłem Krajowym, ISOK oraz systemami służb ratunkowych. Nie wymienia danych z systemami zagranicznymi. | | |
| 13 | Systemy instytucji uprawnionych | MON, organy regulacyjne i nadzorcze, JST, regulatorzy i operatorzy infrastruktury krytycznej | System wielokrotny. Systemy instytucji uprawnionych do korzystania z informacji o zagrożeniach GNSS to systemy wspierające wykorzystanie danych dotyczących jakości, dostępności i bezpieczeństwa sygnałów globalnych systemów nawigacji satelitarnej (GNSS) w działalności operacyjnej instytucji publicznych i innych uprawnionych podmiotów. Celem funkcjonowania tej | Istniejący | Brak |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|---|---|---|---|---|---|
| | | | klasy systemów jest zapewnienie dostępu do informacji o zagrożeniach i zakłóceniach systemów GNSS oraz umożliwienie ich wykorzystania w procesach monitorowania, analizy, podejmowania decyzji i realizacji zadań operacyjnych. | | |
| 14 | ZakPos | Prywatny system Ukrainy | System zagraniczny: Prywatny system stacji referencyjnych Ukrainy (ZakPos), to system wspierający pomiary GNSS na terenie Ukrainy, który podobnie jak ASG-EUPOS posiada stacje referencyjne GNSS oraz centrum zarządzania z którego udostępnia usługi wspomagające i zwiększające dokładność pomiarów GNSS. | Istniejący | Brak |

## Lista przepływów

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|---|---|---|---|---|---|---|
| 1 | SKPOS | ASG-EUPOS | System SKPOS przesyła do systemu ASG-EUPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych.<br><br>Dane obserwacyjne GNSS | tryb odwołań bezpośrednich | realizowalny inną metodą | NTRIP / RTCM |
| 2 | ASG- | SAPOS | System ASG- | tryb odwołań | realizowalny | NTRIP / |

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|---|---|---|---|---|---|---|
| | EUPOS | | EUPOS przesyła do SKPOS dane obserwacyjne GNSS z przygrnicznych stacji referencyjnych . Dane obserwacyjne GNSS | bezpośrednich | inną metodą | RTCM |
| 3 | ASG-EUPOS | Polska Tarcza PNT | Dane usługowe i referencyjne ASG-EUPOS, obserwacje GNSS ze stacji referencyjnych, status dostępności usług, parametry jakości korekt, informacje o pracy stacji, dane RTK/ DGNSS/ postprocessing oraz dane potrzebne do monitorowania jakości usług ASG-EUPOS. | tryb odwołań bezpośrednich | krytyczny dla sukcesu projektu | usługa REST |
| 4 | ASG-EUPOS | CZEPOS | System ASG-EUPOS przesyła do SKPOS dane obserwacyjne GNSS z przygrnicznych stacji referencyjnych . Dane obserwacyjne GNSS | tryb odwołań bezpośrednich | realizowalny inną metodą | NTRIP / RTCM |
| 5 | ASG-EUPOS | e-Infrastruk | System ASG-EUPOS będzie | tryb odwołań bezpośrednich | realizowalny inną metodą | NTRIP / RTCM |

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|---|---|---|---|---|---|---|
| | | turaMON | przesyłał do e-infrastruktury MON obserwacje GNSS z wytypowanych stacji referencyjnych systemu ASG-EUPOS Dane obserwacyjne GNSS | | | |
| 6 | ZakPos | ASG-EUPOS | System ZakPos przesyła do systemu ASG-EUPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych . Dane obserwacyjne GNSS | tryb odwołań bezpośrednich | realizowalny inną metodą | NTRIP / RTCM |
| 7 | Centrum analiz IGS | ASG-EUPOS | Centrum analiz udostępnia na swoich serwerach wyniki obliczeń, a system ASG-EUPOS pobiera je przez internet. Dane: Precyzyjne orbity satelitów oraz poprawki zegarów satelitarnych | kopiowanie danych | Krytyczny dla sukcesu przedsięwzięcia | usługa REST |
| 8 | ASG-EUPOS | SKPOS | System ASG-EUPOS przesyła do SKPOS dane | tryb odwołań bezpośrednich | realizowalny inną metodą | NTRIP / RTCM |

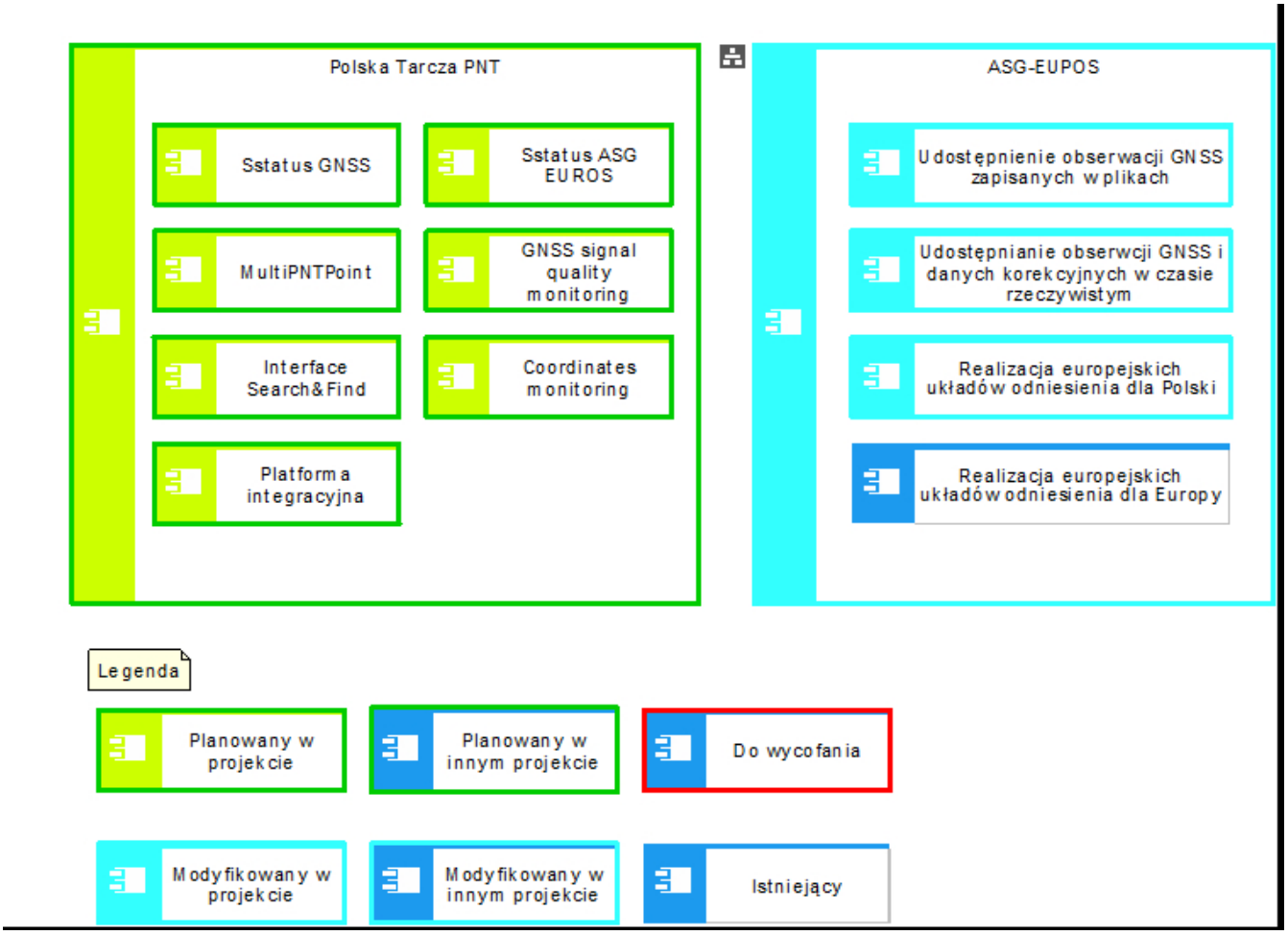
| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|---|---|---|---|---|---|---|
| | | | obserwacyjne GNSS z przygrnicznych stacji referencyjnych . Dane obserwacyjne GNSS | | | |
| 9 | CZEPOS | ASG-EUPOS | System CZEPOS przesyła do systemu ASG-EUPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych Dane obserwacyjne GNSS | tryb odwołań bezpośrednich | realizowalny inną metodą | NTRIP / RTCM |
| 10 | SAPOS | ASG-EUPOS | System SAPOS przesyła do systemu ASG-EUPOS dane obserwacyjne GNSS z przygranicznych stacji referencyjnych Dane obserwacyjne GNSS | tryb odwołań bezpośrednich | realizowalny inną metodą | NTRIP / RTCM |
| 11 | e-InfrastrukturaMON | ASG-EUPOS | Dane w postaci numerycznej lub mapowej z naniesionymi wizualizacjami wyników analiz pozyskanych z e-infrastruktura MON. | tryb odwołań bezpośrednich | realizowalny inną metodą | usługa REST |
| 12 | ASG- | ZakPos | System ASG- | tryb odwołań | realizowalny | NTRIP / |

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|---|---|---|---|---|---|---|
| | EUPOS | | EUPOS przesyła do SKPOS dane obserwacyjne GNSS z przygrnicznych stacji referencyjnych . Dane obserwacyjne GNSS. | bezpośrednich | inną metodą | RTCM |
| 13 | Centrum analiz Trimble | ASG-EUPOS | Centrum analiz udostępnia na swoich serwerach wyniki obliczeń, a system ASG-EUPOS pobiera je przez internet. Dane: Precyzyjne orbity satelitów oraz poprawki zegarów satelitarnych | kopiowanie danych | realizowalny inną metodą | usługa REST |
| 14 | ASG-EUPOS | LitPos | System ASG-EUPOS przesyła do SKPOS dane obserwacyjne GNSS z przygrnicznych stacji referencyjnych . Dane obserwacyjne GNSS | tryb odwołań bezpośrednich | realizowalny inną metodą | NTRIP / RTCM |
| 15 | LitPos | ASG-EUPOS | System LitPos przesyła do systemu ASG-EUPOS dane obserwacyjne GNSS z | tryb odwołań bezpośrednich | realizowalny inną metodą | NTRIP / RTCM |

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|---|---|---|---|---|---|---|
| | | | przygranicznych stacji referencyjnych. Dane obserwacyjne GNSS | | | |
| 16 | e-Czas.pl | Polska Tarcza PNT | Dane referencyjne czasu urzędowego i UTC(PL), informacje o wiarygodnym źródle czasu, dane synchronizacyjne oraz parametry umożliwiające kontrolę zgodności czasu wykorzystywanego przez komponenty projektu | tryb odwołań bezpośrednich | Krytyczny dla sukcesu przedsięwzięcia | usługa REST |
| 17 | Monitor IMGW-PIB | Polska Tarcza PNT | Dane meteorologiczne, hydrologiczne i środowiskowe, w tym informacje o zjawiskach mogących wpływać na propagację sygnałów, warunki pracy infrastruktury terenowej, ocenę ryzyka operacyjnego oraz kontekst dla analiz jakości GNSS. | tryb odwołań bezpośrednich | realizowalny inną metodą | usługa REST |
| 18 | Smart | Polska | Dane | tryb odwołań | realizowalny | usługa REST |

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|---|---|---|---|---|---|---|
| | geoportal | Tarcza PNT | podkładowe do systemów mapowych prezentujących wyniki analiz Polska Tarcza PNT. | bezpośrednich | inną metodą | |
| 19 | Polska Tarcza PNT | Systemy instytucji uprawnionych | Dane wynikowe z przeprowadzonych analiz sygnałów GNSS udostępnione w różnych formatach w zależności od rodzaju analiz. Dane w postaci map z naniesionymi wizualizacjami wyników. W najszerszym zakresie wykorzystanie API i REST. | tryb odwołań bezpośrednich | realizowalny inną metodą | usługa REST |
| 20 | Polska Tarcza PNT | Smart geoportal | Dane w postaci map z naniesionymi wizualizacjami wyników analiz pozyskanych z Polskiej Tarczy PNT. | tryb odwołań bezpośrednich | realizowalny inną metodą | usługa REST |

## 7.2. Kluczowe komponenty architektury rozwiązania




## 7.3. Przyjęte założenia technologiczne

| Lp. | Obszar | Założenie technologiczne |
|---|---|---|
| 1. | Infrastruktura | Architektura chmura–mgła–brzeg. System będzie funkcjonował w całości w multi chmurze PL-GRID.<br>Federalizacja klastrów funkcjonujących w różnych chmurach będzie pozytywnie wpływała na aspekty bezpieczeństwa danych, ciągłości działania i dostępności.<br>Architektura Rozwiązania IT zapewnia jego wysoką dostępność oraz mechanizmy wymiany danych z systemami zewnętrznymi poprzez interfejsy integracyjne. Infrastruktura będzie zarządzana w technologii Infrastructure as Code (IaC), co pozwoli na automatyzację wdrożeń, zarządzania konfguracją oraz łatwe skalowanie zasobów |
| 2. | Sieć i bezpieczeństwo | Wymagana jest redundancja łączności i zasilania oraz integracja z krajową warstwą obsługi incydentów i wymiany informacji.<br>Rozwiązanie ma wspierać kontrolowany dostęp do zasobów operacyjnych.<br>Zapewnienie bezpieczeństwa powierzone zostanie operatorowi chmury PL-GRID. |
| 3. | Standardy wymiany danych | API, interfejsy statusowe i integracyjne dla administracji oraz feedy STIX/TAXII dla wymiany informacji o zagrożeniach. W |

| Lp. | Obszar | Założenie technologiczne |
|---|---|---|
| | | obszarze czasu projekt wspiera mechanizmy PTP/NTP i Time-as-a-Service. |
| 4. | Systemy operacyjne serwerowe | W projekcie nie zakłada się wskazywania producentów systemów. Dobór systemów będzie podporządkowany bezpieczeństwu, wysokiej dostępności i architekturze platformy centralnej.<br>Za dobór systemów operacyjnych serwerów odpowiedzialny będzie operator chmury PL-GRID. |
| 5. | Bazy danych | W projekcie nie zakłada się wskazywania producenta silnika bazodanowego. Rozwiązanie musi obsłużyć dużą ilość danych telemetrycznych, o zdarzeniach, statusowych i raportowych .<br>Za dobór baz danych odpowiedzialny będzie operator chmury PL-GRID. |
| 6. | Serwery aplikacji | Platforma integracyjna obejmie środowisko chmurowe IaaS oraz projekt platformy kubernetesowej zarządzanej tradycyjnie i „AI READY".<br>Za dobór serwerów odpowiedzialny będzie operator chmury PL-GRID. |
| 7. | Portale | Warstwa dostępowa obejmuje serwis internetowy Status_ASG-EUPOS oraz wizualizacje „źródła prawdy" dobrane według preferencji użytkowników. Portale opracowane w ramach projektu będą spełniały obowiązujące wymagania dostępności cyfrowej, w tym wymagania WCAG 2.2 na poziomie AA. |
| 8. | Inne | Projekt zakłada wykorzystanie edge computing, SDR, sensorów ADS-B, stacji meteo, wykrywania wyładowań atmosferycznych oraz metod AI/ML do analizy zakłóceń GNSS i incydentów cybernetycznych. |

## 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 § 19 rozporządzenia 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. poz. 773)) 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

Ze względu na charakter projektu przyjęty zostanie podwyższony poziom ochrony, właściwy dla systemu przetwarzającego dane operacyjne dotyczące jakości PNT/GNSS, zakłóceń, alertów,

statusów usług ASG-EUPOS oraz informacji istotnych dla administracji, obronności i infrastruktury krytycznej. Dane będą udostępniane zgodnie z modelem wielopoziomowego dostępu, z rozdzieleniem warstwy publicznej, sektorowej i operacyjnej oraz z ograniczeniem dostępu do informacji wrażliwych, w szczególności dotyczących źródeł zakłóceń i szczegółów incydentów.