

NASK

Centrum Cyberbezpieczeństwa

FERC.02.02-IP.01-0002/23-0



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Krajowy System Cyberbezpieczeństwa

- W Krajowym Systemie Cyberbezpieczeństwa centralną rolę pełni Ministerstwo Cyfryzacji.
- Kluczowe są trzy zespoły CSIRT (Computer Security Incident Response Team) poziomu krajowego:
 - **CSIRT NASK (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego w strukturach Państwowego Instytutu Badawczego NASK).**
 - CSIRT GOV w strukturach Agencji Bezpieczeństwa Wewnętrznego.
 - CSIRT MON w strukturach Resortu Obrony Narodowej (RON).
- **CSIRT NASK** koordynuje incydenty zgłaszane przez największy zakres podmiotów, w tym operatorów usług kluczowych, dostawców usług cyfrowych oraz samorząd terytorialny. Do CSIRT NASK incydenty mogą także zgłaszać osoby fizyczne – obywatele.
- NASK-PIB współtworzy zaplecze analityczne oraz badawczo-rozwojowe dla krajowego systemu



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Cel projektu CCN

- **Celem strategicznym projektu CCN jest** wzmocnienie krajowego systemu cyberbezpieczeństwa poprzez utworzenie Centrum Cyberbezpieczeństwa NASK (CCN), na które złożą się jakościowo nowe, tematyczne, specjalistyczne centra, ośrodki i laboratoria.
- CCN stanowi odpowiedź na szereg wyzwań i potrzeb wynikających z szybko rosnącej liczby coraz poważniejszych zagrożeń cyberprzestrzeni i wynikające z nich straty:
 - W 2023 r. obsłużono **ponad 80 tys. incydentów cyberbezpieczeństwa** (wzrost o ponad 100% r/r).
 - Wzrasta aktywność grup prowadzących nielegalne działania w świecie cyfrowym, począwszy od hakywistów, przez grupy cyberprzestępcze o charakterze zarobkowym, po grupy powiązane z państwami lub wręcz bezpośrednio stanowiące ich służby.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Zakres projektu CCN

- **Podzadanie 1 Utworzenie obiektu CCN**
- **Podzadanie 2 Utworzenie specjalistycznych centrów i laboratoriów**
 - **Działanie 2.1** Utworzenie Krajowego Centrum Odzyskiwania Danych (KCOD)
 - **Działanie 2.2** Utworzenie Krajowego Centrum Operacyjnego Cyberbezpieczeństwa (KCOC)
 - **Działanie 2.3** Utworzenie modelowego Ośrodka treningowo – szkoleniowego w obszarze Cyberbezpieczeństwa (OSC)
 - **Działanie 2.4** Utworzenie Laboratorium Bezpieczeństwa AI (AITAS)
 - **Działanie 2.5** Utworzenie Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania (FUMAL)
 - **Działanie 2.6** Utworzenie Krajowego Centrum Kompetencji Security dla JST (KCKS)
 - **Działanie 2.7** Utworzenie Ośrodka Certyfikacji Cyberbezpieczeństwa (OCC)
- **Podzadanie 3 Rozbudowa infrastruktury NASK PIB działającej na rzecz CSIRT NASK w tym aktualizacja procesów i realizacja szkoleń wewnętrznych**



Podzadanie 1: Utworzenie obiektu CCN

- Centra, ośrodki i laboratoria CCN (podzadanie 2) zostaną zlokalizowane w nowej, bezpiecznej lokalizacji, co zapewni sprawną pracę ich zespołów oraz wymianę wiedzy i informacji pomiędzy pracownikami zaangażowanymi w ochronę cyberprzestrzeni RP.
- Budynek zostanie zaprojektowany i zbudowany zgodnie z wymaganiami CSIRT, a nie dostosowany do jego potrzeb.
- Planowana lokalizacja CCN to działka 9/13 przy ul. 11 Listopada w Warszawie (obok siedziby NASK S.A.)



Podzadanie 2: Utworzenie specjalistycznych laboratoriów, centrów i ośrodków (1)

- Podzadanie obejmuje uruchomienie jakościowo nowych, tematycznych centrów, ośrodków i laboratoriów niezbędnych z punktu widzenia wzmocnienia krajowego systemu cyberbezpieczeństwa.
- Ich utworzenie jest niezbędne do zwiększenia odporności i zdolności CSIRT-NASK do skutecznego przeciwdziałania cyberzagrożeniom oraz do sprawnego i skutecznego reagowania na incydenty.

2.1 Krajowe Centrum Odzyskiwania Danych

- Umożliwi przywrócenie pełnej sprawności operacyjnej podmiotu, w którym wystąpił incydent utraty / zniszczenia danych
- Laboratorium + komponent mobilny

2.2 Krajowe Centrum Operacyjne Cyberbezpieczeństwa

- Zapewni sprawną i bezpieczną wymianę informacji i efektywną współpracę pomiędzy krajowymi CSIRT'ami
- Umożliwiająca szerszą analizę danych na temat cyberprzestępstw i atakowanych systemów

2.3 Ośrodek treningowo – szkoleniowy w obszarze cyberbezpieczeństwa

- Organizacja specjalistycznych szkoleń i warsztatów na bazie doświadczeń CSIRT
- Budowanie świadomości cyberbezpieczeństwa (kampanie medialne, e-learning i inne nowoczesne narzędzia)

2.4 Laboratorium Bezpieczeństwa AI

- Specjalistyczna komórka zajmująca się procesem implementacji narzędzi, procedur i reguł dbania o cyberbezpieczeństwo AI (w szczególności monitorowaniem, badaniami i propagowaniem najlepszych rozwiązań)



Podzadanie 2: Utworzenie specjalistycznych laboratoriów, centrów i ośrodków (2)

2.5 Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania

- Badanie metodą Fuzzingu podatności różnych projektów (aplikacji, oprogramowania, autonomicznych modeli samodecyzyjnych itp.) zgodnie z wymaganiami bieżącej pracy CISRT



2.5 Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania

- Bezpieczne badanie złośliwego oprogramowania i rozbudowa bazy MWDB (Malware Data Base), która będzie udostępniana profesjonalistom, w tym organom ścigania



2.6 Krajowe Centrum Kompetencji Security dla JST

- Punkt kontaktowy dla JST zapewniający wsparcie specjalistów CSIRT w reagowaniu na incydenty i wzmocnienia ich odporności oraz zdolności do podejmowania skutecznych działań zapobiegawczych
- Laboratorium + komponent mobilny



2.7 Ośrodek Certyfikacji Cyberbezpieczeństwa

- Fundament krajowego systemu certyfikacji cyberbezpieczeństwa zapewniającego systemowe podejście do analizy produktów, usług i procesów (w tym dla rozwiązań chmurowych, sieci mobilnych, IoT czy CSAM)
- Doskonalenie kadry certyfikującej posiadającej niepodważalne kompetencje



Podzadanie 3: Rozbudowa infrastruktury CSIRT NASK oraz aktualizacja procesów i realizacja szkoleń wewnętrznych

- Analiza przeprowadzona przez NASK-PIB, wskazuje że aktywne i efektywne przeciwdziałanie cyberzagrożeniom przez CSIRT NASK (w szczególności realizacja wymagań nakładanych dyrektywą NIS2), wymaga znaczących inwestycji infrastrukturalnych.
- Rozbudowana infrastruktura NASK obejmie zarówno obecnie eksploatowane zasoby jak i nowe, zainstalowane w związku z realizacją niniejszego projektu.
- Działanie obejmie też sukcesywne szkolenie z zasad cyberhigieny wszystkich pracowników NASK PIB. Jest to konieczne w celu ograniczenia ryzyka ataków (np. socjotechnicznych, dezinformacji) na pracowników NASK PIB, a w konsekwencji możliwego ataku na infrastrukturę używaną przez CSIRT NASK.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Rezultaty projektu CCN (1)

1. Wzmocnienie odporności i zdolności CSIRT-NASK do skutecznego przeciwdziałania cyberzagrożeniom w systemach informacyjnych państwa oraz podmiotach mających kluczowe znaczenie dla gospodarki, a w szczególności:

- a) wzmocnienie cyberodporności podmiotów włączonych w prowadzone przez CSIRT-NASK działania.
- b) podnoszenie praktycznej wiedzy na temat cyberbezpieczeństwa w formie specjalizowanych szkoleń i zajęć warsztatowych.
- c) rozszerzenie zakresu badań i prac rozwojowych w obszarze nowych technologii (zwłaszcza rozwiązań bazujących na sztucznej inteligencji) związanych z cyberbezpieczeństwem.
- d) zwiększenie możliwości bezpiecznego badania złośliwego oprogramowania oraz wykrywania podatności metodą fuzzingu.
- e) usprawnienie procesu certyfikacji operatorów usług kluczowych lub dostawców usług cyfrowych co przekłada się bezpośrednio na obniżenie ich strat z tytułu incydentów.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Rezultaty projektu CCN (2)

2. Zwiększenie zdolności do reagowania na incydenty w systemach informacyjnych państwa oraz podmiotach mających kluczowe znaczenie dla gospodarki przez CSIRT-NASK, a w szczególności:

- a) sprawniejsze reagowanie CSIRT-NASK na incydenty poprzez skrócenie maksymalnego czasu reakcji.
- b) usprawnienie obecnych procedur wymiany informacji związanych z incydem, ze szczególnym podkreśleniem bezpiecznej wymiany informacji chronionych.
- c) sprawniejsze przywracanie pełnej sprawności operacyjnej podmiotu, w którym wystąpił incydent.
- d) zwiększenie możliwości pełnego odtworzenia danych zaatakowanego podmiotu.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Budżet i czas realizacji projektu CCN

Szacowana wartość projektu	310 000 000,00 zł
Wkład UE	247 101 000,00 zł (79.71% całkowitej wartości projektu)
Wkład własny	62 899 000,00 zł dofinansowany z budżetu Państwa
Okres rzeczowej realizacji projektu	31.10.2023 r. – 30.09.2029 r.



Fundusze Europejskie
na Rozwój Cyfrowy

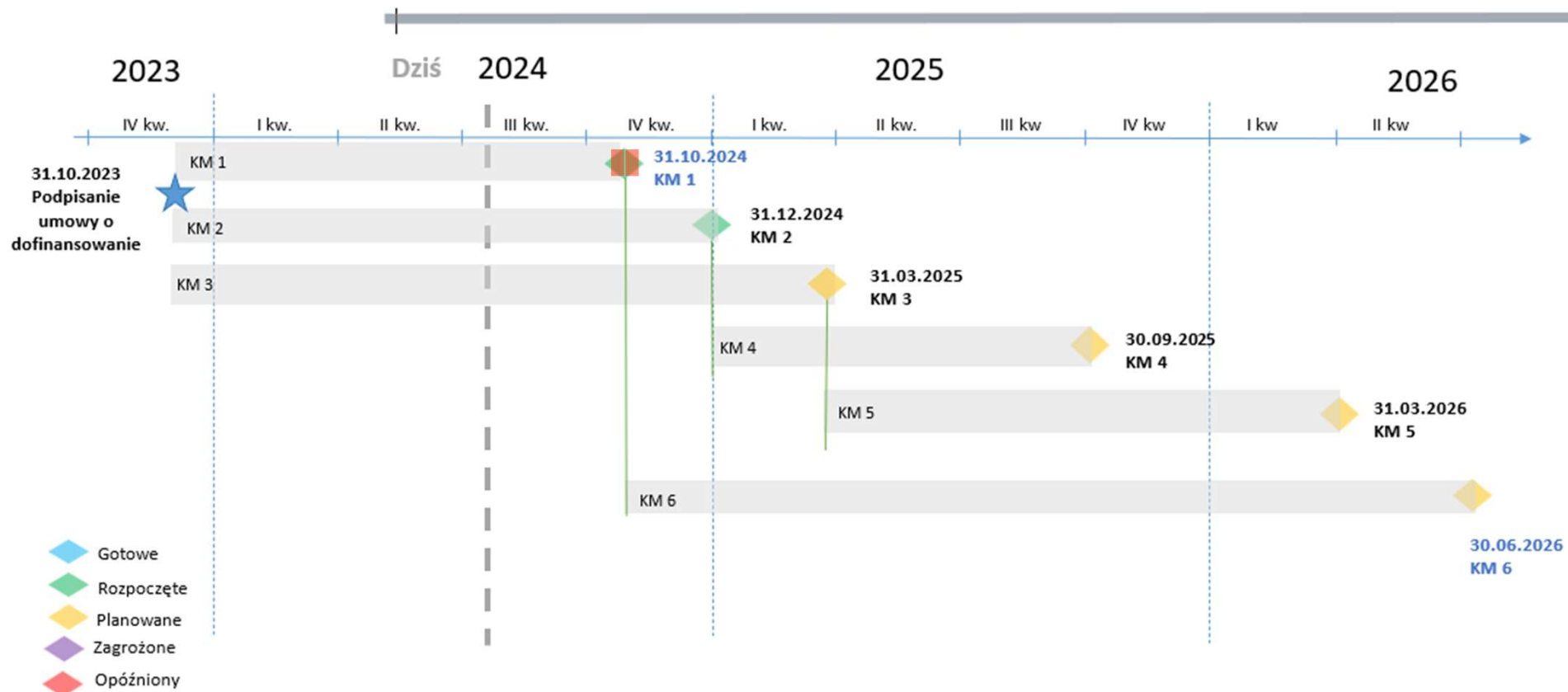


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską

**NASK**

HARMONOGRAM PROJEKTU



Fundusze Europejskie
na Rozwój Cyfrowy



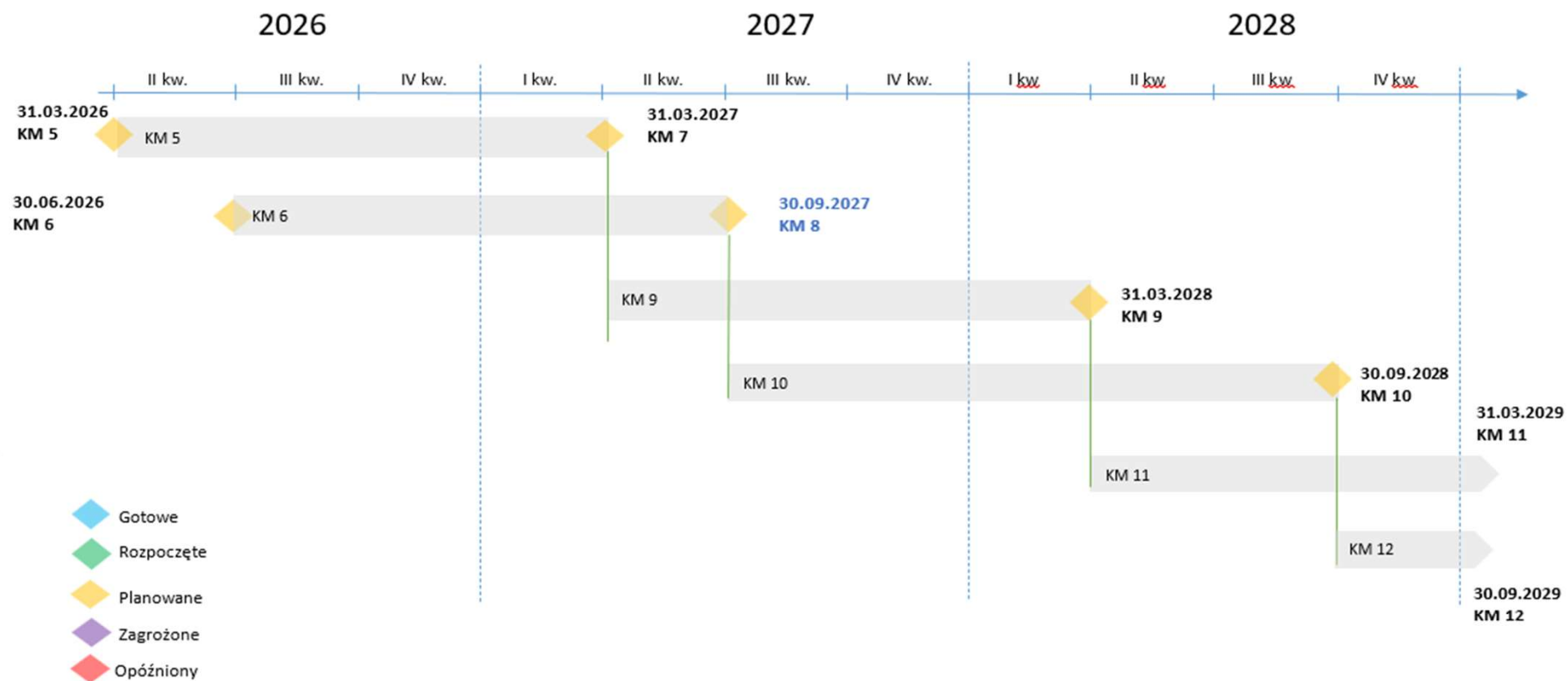
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

HARMONOGRAM PROJEKTU



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską

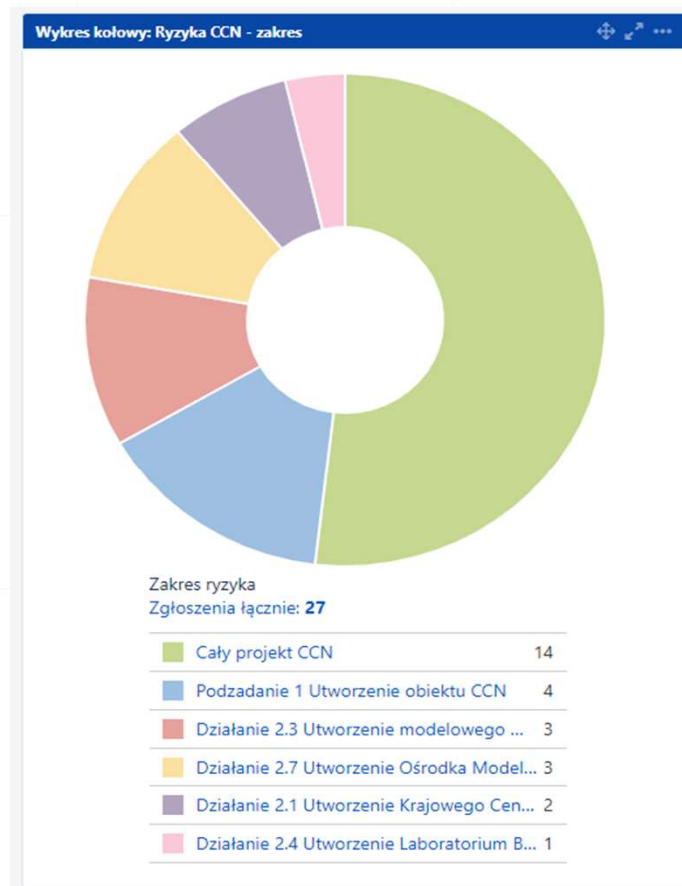
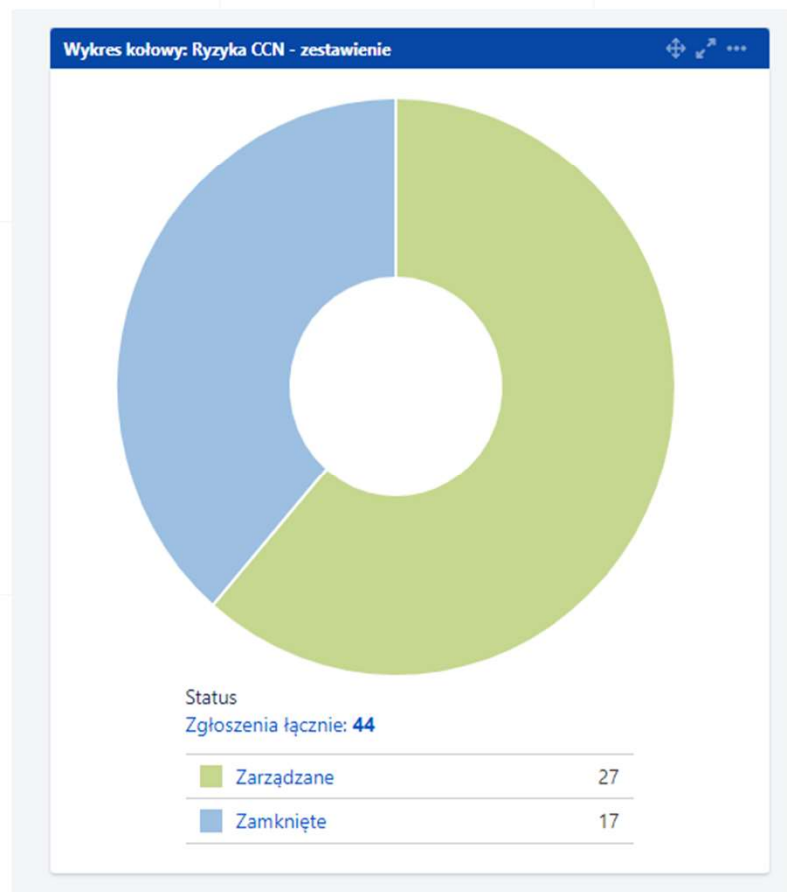


NASK

Ryzyka projektowe

NASK

Centrum
Cyberbezpieczeństwa



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Ryzyka projektowe

Kluczowe ryzyko projektowe: **Problemy z pozyskaniem nieruchomości na cele projektu.**

Przyczyna ryzyka: Przeciągające się procedury formalno-prawne dot. zakupu/pozyskania nieruchomości mogą spowodować niemożność realizacji projektu w zakładanym zakresie i czasie.

Sposób reakcji na ryzyko: Redukowanie/mitygacja

Opis reakcji/podejmowanych działań:

- ✓ Ścisła współpraca z Instytucjami (IAS, MRiT, UM) zaangażowanymi w przekazanie działki.
- ✓ Zapewnienie wsparcia Ministra Cyfryzacji (nadzorującego NASK-PIB) w pozyskaniu gruntu.
- ✓ Analiza dostępnych nieruchomości pod kątem wymagań CCN – zrealizowane.



Fundusze Europejskie
na Rozwój Cyfrowy



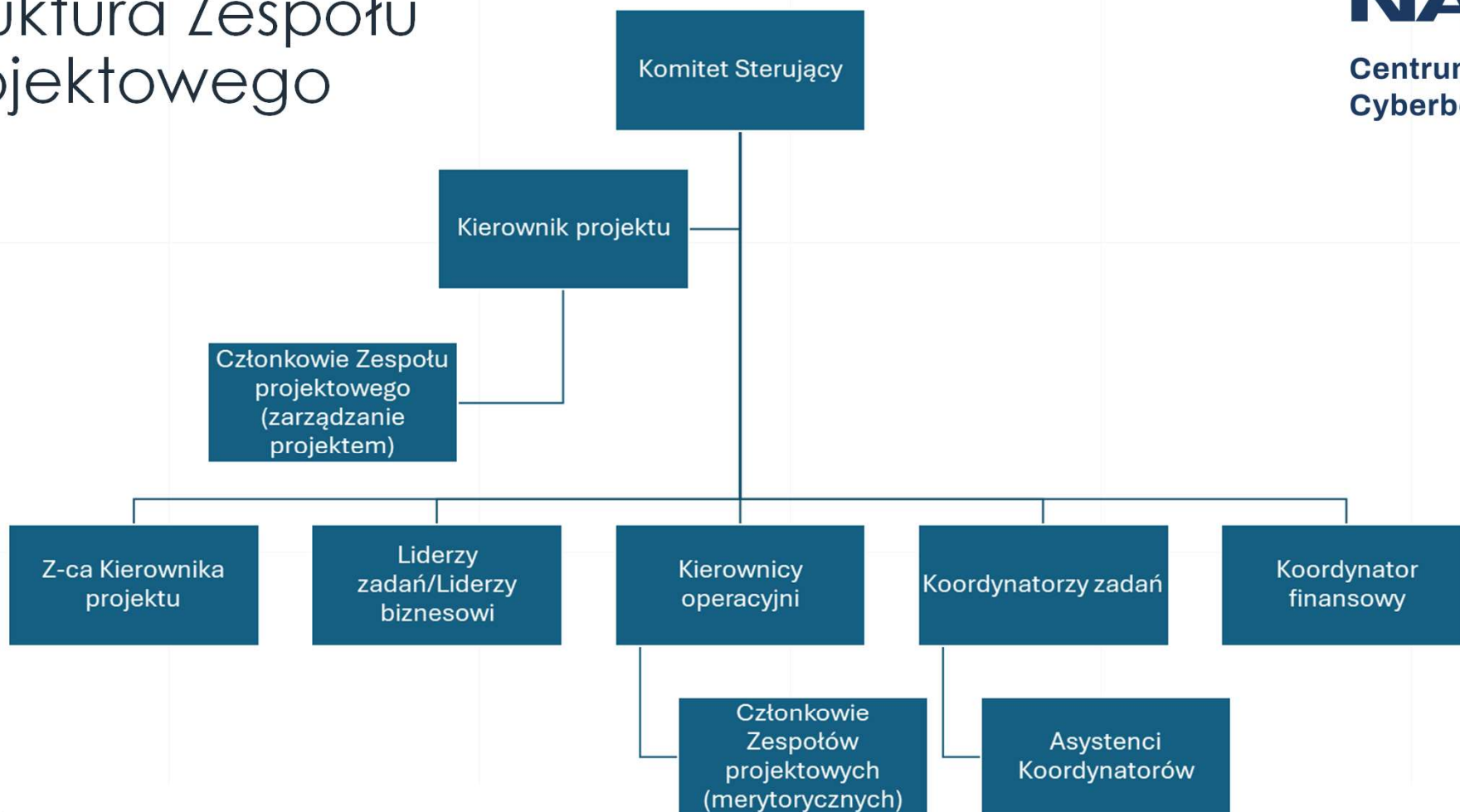
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Struktura Zespołu projektowego



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Aktualnie realizowane kluczowe działania projektowe

1. Projekt – Przetarg – Budowa

- Biuro projektowe – postępowanie w trakcie realizacji.
- Inżynier kontraktu – gotowa dokumentacja, gotowość do ogłoszenia przetargu.
- Generalny Wykonawca – dokumentacja w przygotowaniu.

2. Pozyskanie działki pod budowę CCN

- Ścisła współpraca z Instytucjami (IAS, MC, MRiT, UM m.st. Warszawy) zaangażowanymi w przekazanie działki przy ul. 11 listopada pod budowę CCN.

3. Przygotowanie lab/centrów/ośrodków do działania w docelowej lokalizacji

- Postępowania zakupowe dot. sprzętu i infrastruktury IT.
- Prace nad budowaniem poszczególnych laboratoriów i opracowywanie koncepcji ich funkcjonowania.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

NASK

Dziękujemy za uwagę.

Kierownik projektu CCN
Agnieszka Suchodolska

agnieszka.suchodolska@nask.pl

Obserwuj NAS(K)

