

PROGRAM PRAC DLA OBSZARU CYBERBEZPIECZEŃSTWO 2025-2027

Krajowe Centrum Kompetencji
Cyberbezpieczeństwa (NCC-PL)



Zadania NCC-PL



Programy unijne dofinansowujące cyberbezpieczeństwo

PROGRAM CYFROWA
EUROPA

EUROPEJSKI FUNDUSZ
OBRONNY

HORYZONT EUROPA

Program Cyfrowa Europa - filar Cyberbezpieczeństwo



Ministerstwo
Cyfryzacji



NCC-PL
Krajowe Centrum Kompetencji
Cyberbezpieczeństwa



Co-funded by
the European Union



ECCCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

DEP Cybersecurity Work Programme 2025-2027

- Lista tematów
- Informacje dla każdego z tematów - rok naboru, zakres i cele, budżet, czas trwania projektu, beneficjenci, rodzaj działania (= wysokość dofinansowania), kwestia konsorcjum
- Work Programme a Call Document

DEP Cybersecurity Work Programme 2025-2027

Areas and topics with indicative allocations (in million EUR)		2025	2026	2027	Total
New technologies, AI & post-quantum transition					142
2.1	Cybersecure tools, technologies and services relying on AI	15	15	15	45
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions		20		20
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	25			25
2.4	Transition to post-quantum Public Key Infrastructures	15			15
2.5	Migration of Cyber Hubs to PQC			7	7
2.6	Uptake of innovative cybersecurity solutions for SMEs	15		15	30
Cyber Solidarity Act Implementation					121
2.7	National Cyber Hubs	20	15		35
2.8	Cross-Border Cyber Hubs	20		20	40
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		2		2
2.10	Coordinated preparedness testing and other preparedness actions	5	15	20	40
2.11	Mutual assistance		2	2	4
Additional actions improving EU cyber resilience					118
2.12	Enhancing the NCC Network	10	16	20	46
2.13	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		20	12	32
2.14	Dedicated action to reinforce hospitals and healthcare providers	30			30
2.15	Dual-use technologies		10		10
Programme Support Actions		3	3	3	9
TOTAL (in million EUR)		158	118	114	390

Nabory 2025

- I tura:
 - otwarcie – I połowa czerwca 2025,
 - zamknięcie – 7 października 2025,
- II tura:
 - otwarcie – 1 września 2025,
 - zamknięcie – 22 stycznia 2026 r.
- Przetarg - ?

I nabór 2025 (czerwiec – 7 października 2025 r.)

Tematy:

1. Transition to post-quantum Public Key Infrastructures
2. Coordinated preparedness testing and other preparedness actions
3. Enhancing the NCC Network
4. Dedicated action to reinforcing hospitals and healthcare providers

I nabór 2025: Transition to post-quantum Public Key Infrastructures

- Cel konkursu - sprostanie wyzwaniom związanym ze skuteczną integracją algorytmów PQC w Infrastrukturze Klucza Publicznego (PKI),
- Konkurs tylko w 2025 r.
- Budżet konkursu – 15 mln EUR, w tym 4 – 5 mln EUR per grant
- Simple grant – dofinansowanie do 50% kosztów
- Przewidywany czas trwania projektu – 3 lata
- Beneficjenci: wszystkie podmioty w łańcuchu PKI

I nabór 2025: Coordinated preparedness testing and other preparedness actions

- Cel konkursu
 - zwiększenie poziomu ochrony i odporności na cyberzagrożenia, w szczególności w odniesieniu do krytycznych instalacji i infrastruktury przemysłowej, poprzez wspieranie państw członkowskich w ich wysiłkach na rzecz poprawy ich gotowości na cyberzagrożenia i incydenty.
- Konkurs powtarzany w latach 2025, 2026, 2027, ale w 2025 r. – tylko działanie pierwsze

I nabór 2025: Coordinated preparedness testing and other preparedness actions

- Działania:
 - 1) skoordynowane testowanie gotowości podmiotów działających w sektorach kluczowych w UE, w tym testy penetracyjne, ocena zagrożeń i ocena ryzyka (sektory kluczowe zgodnie z Załącznikiem 1 do Dyrektywy NIS2)
 - 2) inne działania w zakresie zapewnienia gotowości dla podmiotów działających w sektorach kluczowych i sektorach ważnych (m. in. ocena zagrożeń i ryzyka, ujawnianie i zarządzanie podatnościami, ćwiczenia i szkolenia).

I nabór 2025: Coordinated preparedness testing and other preparedness actions

- Budżet konkursu – 5 mln EUR w 2025 r.,
- Simple grant – dofinansowanie do 50% kosztów projektu
- Przewidywany czas trwania projektu – 3 lata
- Beneficjenci – w 2025 r. tylko podmioty publiczne (działające jako właściwe organy ds. cyberbezpieczeństwa lub CSIRTy, podmioty publiczne objęte dyrektywą NIS 2 i innymi regulacjami)

I nabór 2025: Dedicated action to reinforcing hospitals and healthcare providers

- Cel: wzmocnienie cyberbezpieczeństwa szpitali i podmiotów świadczących opiekę zdrowotną
 - zapewnienie, aby mogły skutecznie wykrywać, monitorować i reagować na cyberzagrożenia, w szczególności ransomware.
- Konkurs tylko w 2025 r.
- Budżet konkursu – 30 mln EUR
- Simple grant – dofinansowanie do 50% kosztów
- Przewidywany czas trwania projektu: 1,5 – 2 lata

I nabór 2025: Dedicated action to reinforcing hospitals and healthcare providers

- Zakres: dofinansowane zostaną projekty pilotażowe, których efektem będzie m. in.:
 - Zmapowanie potrzeb szpitali i podmiotów świadczących opiekę zdrowotną w zakresie cyberbezpieczeństwa,
 - Opracowanie wytycznych dla podmiotów świadczących opiekę zdrowotną dotyczących określenia ich obecnego stanu ochrony w zakresie cyberbezpieczeństwa i ich potrzeb
 - Opracowanie technicznych planów w zakresie cyberbezpieczeństwa w celu zwiększenia gotowości i cyberodporności tych podmiotów
 - Demonstracyjne wdrożenie tych planów w partnerskich szpitalach i placówkach świadczących opiekę zdrowotną

I nabór 2025: Dedicated action to reinforcing hospitals and healthcare providers

- Kto może ubiegać się o grant:
 - konsorcja obejmujące:
 - związki szpitali i podmiotów świadczących opiekę zdrowotną z co najmniej 2 krajów członkowskich UE
 - oraz podmioty dostarczające usługi w zakresie cyberbezpieczeństwa

I nabór 2025: Enhancing the NCC network

Konkurs dla krajowych ośrodków koordynacji wyznaczonych w poszczególnych krajach UE

II nabór 2025 (1 września 2025 – 22 stycznia 2026)

Tematy:

1. Cybersecure tools, technologies and services relying on AI
2. Uptake of innovative cybersecurity solutions for SMEs
3. National Cyber Hubs
4. Cross-Border Cyber Hubs

II nabór 2025: Cybersecure tools, technologies and services relying on AI

- Cel – rozwijanie i wdrażanie technologii opartych na AI dla organów krajowych, podmiotów publicznych i podmiotów prywatnych objętych Dyrektywą NIS2.
- Konkurs będzie powtarzany w 2025, 2026 i 2027 r.
- Budżet na 2025 r. – 15 mln EUR
- Simple grant – dofinansowanie do 50% kosztów projektu
- Przewidywany czas trwania projektu: 3 lata
- Beneficjenci: podmioty publiczne i prywatne

II nabór 2025: Uptake of innovative cybersecurity solutions for SMEs

- Cel – wsparcie MŚP w zakresie ich przygotowania do spełnienia wymogów zawartych w unijnych aktach prawnych dotyczących cyberbezpieczeństwa, np. CRA
- Konkurs będzie powtarzany w 2025 oraz w 2027 r.
- Budżet na 2025 r. – 15 mln EUR
- SME support action: dla MŚP – dofinansowanie do 75% kosztów, dla pozostałych podmiotów - dofinansowanie do 50% kosztów
- Przewidywany czas trwania projektu: 3 lata
- Beneficjenci: m. in. MŚP, podmioty publiczne i prywatne wdrażające Dyrektywę NIS2, CRA, uczelnie, podmioty badawcze

II nabór 2025: National Cyber Hubs, Cross-Border Cyber Hubs

- Realizacja Cyber Solidarity Act
- Adresowane do podmiotów, które zostały wyznaczone przez władze ich kraju członkowskiego do roli National Cyber Hub.
- Cel – tworzenie lub wzmacnianie takich ośrodków.

Zamówienie 2025: Deployment of a European testing infrastructure for the transition to PQC in different usage domains

- Cel: stworzenie europejskiej globalnej infrastruktury do testowania porównawczego w celu przejścia na PQC, dostępnej dla różnego rodzaju podmiotów, w celu przeprowadzania testów w oparciu o rzeczywiste przypadki i identyfikacji wyzwań związanych z wdrażaniem systemów PQC.
- Budżet – 25 mln EUR
- Przewidywany czas trwania projektu: 4 lata

Granty NCC-PL dla MŚP prowadzących działalność w obszarze cyberbezpieczeństwa

Granty dla cyber MŚP

- Finansowanie kaskadowe w ramach projektu „National Coordination Centre – Poland”, dofinansowane z DEP - Cyberbezpieczeństwo
- Całkowita wartość planowanego dofinansowania - 1 800 000 EUR
- Poziom dofinansowania – 100% kosztów projektu
- Wysokość 1 grantu: 30 000 – 60 000 EUR
- Podmioty które mogą ubiegać się o grant: polscy mali i średni przedsiębiorcy prowadzący działalność w obszarze cyberbezpieczeństwa

Granty dla cyber MŚP

- zakres działań:
 - rozwój istniejącego produktu lub usługi w obszarze cyberbezpieczeństwa,
 - stworzenia nowego rozwiązania w obszarze cyberbezpieczeństwa,
 - zwiększenie rozpoznawalności produktów i usług w obszarze cyberbezpieczeństwa na rynku,
 - certyfikacja produktu lub usługi w obszarze cyberbezpieczeństwa

Finansowanie kaskadowe z projektów DEP

Cyberbezpieczeństwo

- Projekty dofinansowane w ramach poprzednich Work Programmes obejmujące udzielenie grantów dla podmiotów europejskich (finansowanie kaskadowe):
 - CYSSDE - granty dla podmiotów przeprowadzających testy penetracyjne i ocenę podatności
 - CYBERSTAND - granty na działania zmierzające do wypracowania zharmonizowanych standardów na potrzeby Cyber Resilience Act (nabory do 20 czerwca 2025 r.)
 - SECURE – granty dla europejskich MŚP w celu wsparcia ich we wdrażaniu Cyber Resilience Act

Dziękuję za uwagę!

ncc@cyfra.gov.pl

<https://www.gov.pl/web/cyber-nccpl>
<https://www.linkedin.com/company/ncc-pl/>