



Główny Urząd Statystyczny rozpoczyna realizację projektu grantowego pn. Cyberbezpieczna Statystyka, w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności - Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo – Cyberbezpieczny Rząd.

## Cele projektu:

Celem projektu jest zwiększenie poziomu bezpieczeństwa informacji w trzech kluczowych obszarach cyberbezpieczeństwa, tj.: organizacji, technologii i kompetencji. Ten zostanie zrealizowany poprzez:

- wzmocnienie ciągłości działania systemów poprzez zapewnienie wsparcia dla infrastruktury wirtualizacyjnej oraz gwarancji na infrastrukturę HPE (Hewlett Packard Enterprise). System wirtualizacyjny wraz z infrastrukturą HPE pozwoli między innymi na sprawną eksploatację posiadanych produktów z zakresu cyberbezpieczeństwa, takich jak: system EDR (Endpoint Detection and Response), AV (Antivirus), ochrona poczty, skaner podatności, PKI (Public Key Infrastructure), systemy do monitorowania serwerów i usług czy też system backupu;
- wdrożenie systemu SOAR (Security Orchestration, Automation and Response), tj. narzędzia automatyzującego czynności administratorów bezpieczeństwa) zapewniającego automatyzację reakcji na incydenty bezpieczeństwa informacji oraz rozbudowę systemu kopii zapasowych;
- wzmocnienie kompetencji pracowników jednostek służb statystyki publicznej poprzez specjalistyczne szkolenia dotyczące zarządzania bezpieczeństwem informacji oraz podniesienia umiejętności w obszarze IT, w tym zarządzania incydentami;
- przeprowadzenie audytu na zgodność z KRI[1]/UoKSC[2] posiadanego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), obejmującego Główny Urząd Statystyczny i 18 jednostek podległych. Umożliwi to sprawdzenie zgodności Systemu Bezpieczeństwa Informacji (SBI), w szczególności polityk i procedur, z wymaganiami wynikającymi z implementacji dyrektywy NIS 2[3].

## Grupy docelowe:

Główny Urząd Statystyczny i 18 jednostek podległych

## Efekty/produkty/usługi/korzyści:

- Ocena zgodności z KRI/UoKSC oraz identyfikacja luk bezpieczeństwa informacji  
Realizacja działania pozwoli na przeprowadzenie oceny zgodności procesów i systemów z wymaganiami prawnymi wynikającymi z KRI i UoKSC. W efekcie zostaną zidentyfikowane potencjalne luki i zagrożenia w obszarze bezpieczeństwa informacji, co umożliwi ich eliminację oraz spełnienie obowiązujących wymogów prawnych.
- Budowanie świadomości cyberzagrożeń wśród pracowników  
W ramach projektu pracownicy jssp wezmą udział w szkoleniach zewnętrznych, w szczególności zostaną przeprowadzone szkolenia, które wzmocnią kompetencje zespołu w zakresie przeprowadzania audytów bezpieczeństwa informacji i systemów informatycznych, co przełoży się na podniesienie poziomu

bezpieczeństwa w jssp.

- Wzmocnienie kompetencji pracowników w zakresie bezpieczeństwa i IT

Specjalistyczne szkolenia podniosą kwalifikacje personelu w zakresie bezpieczeństwa informacji, umożliwiając doskonalenie technicznych umiejętności związanych z obsługą infrastruktury IT, w tym zarządzaniem incydentami bezpieczeństwa w systemie SOAR.

- Modernizacja i odnowienie wsparcia kluczowej infrastruktury IT

Zapewnione zostanie utrzymanie ciągłości działania i bezpieczeństwa systemów poprzez odnowienie wsparcia technicznego dla infrastruktury HPE Synergy 12000, a także oprogramowania do backupu.

Dodatkowo planowany jest zakup subskrypcji na oprogramowanie do wirtualizacji, co pozwoli na efektywne zarządzanie środowiskami wirtualnymi.

- Wdrożenie systemu SOAR

Zaimplementowanie rozwiązania SOAR zapewni automatyzację procesów reagowania na incydenty bezpieczeństwa, integrację z istniejącymi narzędziami zabezpieczającymi, skrócenie czasu reakcji na zagrożenia oraz centralizację zarządzania informacjami o incydentach, co przełoży się na zwiększenie poziomu bezpieczeństwa i efektywności działań zespołu bezpieczeństwa

- Rozszerzenie systemu backupowego CPD GUS

Rozbudowa systemu backup-u o bibliotekę LTO i dodatkową licencję Veeam Backup&Replication umożliwią zabezpieczenie plików backupowych na taśmках LTO8, oraz zabezpieczą wykonywanie kopii zapasowych serwerów fizycznych z systemami Microsoft Windows Server. Wdrożenie obu tych elementów pozwoli na zapewnienie ciągłości działania systemów.

Stan realizacji:

Projekt będzie realizowany do 30.06.2026 roku.

Rozpoczęcie rzeczowe – lipiec 2025 r.

Łączna wartość przyznanego dofinansowania z Unii Europejskiej wynosi 9.993.157,65 PLN (netto).

#NextGenerationEU

#FunduszeUE

---

[1] Rozporządzenie 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. 2024 poz. 773).

[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560 z późn.zm.).

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) z dnia 14 grudnia 2022 r. (Dz.Urz.UE.L Nr 333, str. 80).

Podmiot publikujący: Główny Urząd Statystyczny

Autor informacji: Monika Ostrowska (Wydział Koordynacji Projektów Strategicznych)

Publikujący informację: Magdalena Zarodkiewicz (Wydział Standardów Publikowania)

Publikacja informacji: 14.07.2025 14:03

Aktualizacja informacji: 29.01.2026 12:28

[Sprawdź historię zmian](#)