PARP
Grupa PFR

grudzień 2025

# Pilotażowy program wsparcia MSP w zakresie systemowego podejścia do bezpieczeństwa cyfrowego

Raport końcowy z procesu projektowego

Opracowanie:

Maciej Szałaj, Sylwia Rink - Departament Analiz i Strategii

Fundusze Europejskie dla Nowoczesnej Gospodarki
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR

# Spis treści

Kluczowe pojęcia i skróty ..... 3
1. Wstęp i kontekst ..... 4
1.1. Kontekst problemowy ..... 4
1.2. Kontekst instytucjonalny ..... 6
2. Założenia programu (teoria interwencji) ..... 7
2.2. Cel programu ..... 10
2.3. Odbiorcy programu ..... 10
2.4. Oczekiwana zmiana ..... 10
3. Opis programu wsparcia ..... 12
3.1. Ścieżka uczestnika programu ..... 12
3.1.1. Selekcja firm do programu ..... 13
3.1.2. Diagnoza firm i audyt ekspercki ..... 14
3.1.3. Wypełnienie wniosku o dofinansowanie ..... 15
3.1.4. Wdrożenie systemów *cybersec* ..... 16
3.1.5. Utrzymania systemu ..... 18
3.2. Usługi dostępne dla Beneficjentów ..... 19
4. Formuła programu ..... 21
4.1. Sposób wdrażania ..... 21
4.2. Harmonogram ..... 22
4.3. Budżet i zasady finansowania ..... 22
4.2. Kryteria kwalifikujące Beneficjentów ..... 22
4.3. Wskaźniki efektów pilotażu ..... 23
4.4. Ryzyka ..... 25
4.5. Kwestia wymagające doprecyzowania ..... 26
5. Proces projektowy ..... 28
5.1. Uczestnicy/czki procesu projektowego ..... 28
5.2. Metodologia ..... 28
5.3. Definiowanie problemu i kierunki projektowe ..... 29
5.4. Prototypowanie ..... 30
5.5. Testowanie I ..... 30
5.6. Prototypowanie II ..... 32

5.7. Testowanie II ..... 32
5.8. Prototyp III: spis najważniejszych zmian po testach ..... 33
5.9. Planowanie wdrożenia ..... 33

## Kluczowe pojęcia i skróty

**CERT Polska** – zespół działający w strukturach Naukowej i Akademickiej Sieci Komputerowej (NASK) powołany do reagowania na incydenty bezpieczeństwa komputerowego na poziomie krajowym.

**CSIRT** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (ang. *Computer Security Incident Response Team*)

**Cyberbezpieczeństwo** – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy [1], a także działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami[2]

**DORA** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011

**EDIH** – Europejskie huby innowacji cyfrowych (European Digital Innovation Hub), ośrodki wsparcia przedsiębiorców, w tym małych i średnich przedsiębiorstw w wyzwaniach cyfrowych

**NIS 2** – 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

[1] Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 roku.
[2] Definicja zgodna z nową ustawą o krajowym systemie certyfikacji cyberbezpieczeństwa z dnia 28 lipca 2025r, która powołuje się na zapisy w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)

# 1. Wstęp i kontekst

Celem niniejszego raportu jest przedstawienie wyników prac nad nowym instrumentem wsparcia mikro-, małych i średnich przedsiębiorstw w obszarze cyberbezpieczeństwa. Instrument ten będzie wdrażany pilotażowo w ramach projektu Inno_LAB, realizowanego w latach 2024–2029 przez Ministerstwo Rozwoju i Technologii oraz Polską Agencję Rozwoju Przedsiębiorczości.

Misją projektu Inno_LAB jest wspieranie rozwoju krajowego ekosystemu innowacji oraz doskonalenie sposobów publicznego wsparcia innowacyjności w Polsce. W tym kontekście szczególne znaczenie ma projektowanie narzędzi wsparcia, które są adekwatne do krajowych uwarunkowań i realnych potrzeb przedsiębiorców, co przekłada się na większą skuteczność całego ekosystemu innowacji.

Założenia pilotażu zaprezentowane w niniejszym raporcie zostały wypracowane w toku procesu projektowego realizowanego zgodnie z metodyką service design. W prace projektowe zaangażowani byli przedstawiciele Polskiej Agencji Rozwoju Przedsiębiorczości oraz ośrodków sieci EDIH, przedsiębiorcy należący do grupy docelowej programu, a także eksperci z zakresu bezpieczeństwa cyfrowego oraz dostawcy usług działający w tym obszarze.

## 1.1. Kontekst problemowy

W ostatnich latach przedsiębiorstwa – w tym sektor MSP – funkcjonują w coraz bardziej złożonym otoczeniu regulacyjnym dotyczącym cyberbezpieczeństwa. Dyrektywa NIS2 oraz projektowana ustawa o krajowym systemie cyberbezpieczeństwa istotnie podnoszą wymagania wobec podmiotów świadczących usługi kluczowe i ważne, nakładając na nie nowe obowiązki w zakresie zarządzania ryzykiem, wdrażania adekwatnych środków ochrony oraz raportowania incydentów. Wymogi te obejmują zarówno dostosowanie istniejących procesów, jak i wdrażanie nowych rozwiązań technicznych, prawnych oraz organizacyjnych. Ich niedopełnienie może skutkować nie tylko dotkliwymi sankcjami finansowymi, lecz także utratą zaufania i pogorszeniem reputacji przedsiębiorstw.[3]

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2); projekt ustawy o krajowym systemie cyberbezpieczeństwa (UKSC) - https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=1955

Wzrost obciążeń regulacyjnych następuje w warunkach dynamicznie rosnącej skali zagrożeń cybernetycznych. Należymy przy tym do krajów o najwyższej skali i dynamice ataków cybernetycznych w ostatnich latach[4]. Z najnowszych analiz wynika, że w 2024 r. zespół CERT Polska odnotował rekordowy wzrost liczby zgłoszeń incydentów cyberbezpieczeństwa (ponad 600 tys.). CSIRT NASK zarejestrował wzrost liczby zgłoszeń o 64 proc. a liczba incydentów w jego rejestrze wzrosła z 80 267 do 103 449. Średnia dzienna liczba incydentów obsługiwanych przez NASK wzrosła z 220 do 283. Odnotowano również 57 proc. więcej tzw. incydentów poważnych – tych, które mogą wpływać na ciągłość działania instytucji – oraz 58 proc. więcej incydentów w sektorze publicznym[5]. Ataki coraz częściej wymierzone są przy tym w podmioty o ograniczonych zasobach ochronnych, w tym w sektor MSP, który może być postrzegany przez cyberprzestępców jako relatywnie łatwy cel.

Jednocześnie europejskie i krajowe dokumenty strategiczne, takie jak Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 oraz Strategia Produktywności 2030, podkreślają konieczność systemowego wzmacniania odporności cyfrowej gospodarki jako jednego z kluczowych warunków jej długofalowego rozwoju i konkurencyjności[6]. Elementem tego ekosystemu jest również Krajowy System Certyfikacji Cyberbezpieczeństwa, promujący podnoszenie standardów technicznych i organizacyjnych. Ponadto, europejskie rozporządzenie DORA, które od 17 stycznia 2025 r. wprowadza jednolite wymogi dotyczące odporności cyfrowej w sektorze finansowym, służy jako punkt odniesienia dla innych branż o wysokim ryzyku operacyjnym[7].

Międzynarodowe raporty, takie jak ENISA Threat Landscape 2024, wskazują, że zagrożenia cybernetyczne w Unii Europejskiej obejmują szerokie spektrum taktyk wykorzystywanych przez cyberprzestępców oraz obejmują tysiące analizowanych incydentów w różnych

[4] Microsoft Digital Defense Report 2025 – Polska 3. miejsce w Europie pod względem cyberataków sponsorowanych przez inne państwa (zaraz za Ukrainą i Wielką Brytanią). https://tvpworld.com/89505347/microsoft-poland-no-3-in-europe-for-state-cyberattacks-turn0search13

[5] CERT Polska, Raport roczny 2024 „Krajobraz bezpieczeństwa polskiego internetu" – dane o ponad 600 tys. zgłoszeń: https://cert.pl/uploads/docs/Raport_CP_2024.pd

[6] Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa RP na lata 2019–2024*; Ministerstwo Rozwoju i Technologii, *Strategia Produktywności 2030*

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 (DORA) – jednolite wymogi w sektorze finansowym.

sektorach gospodarki, co dodatkowo uwypukla skalę wyzwań stojących przed firmami i instytucjami[8].

## 1.2. Kontekst instytucjonalny

W momencie rozpoczęcia prac projektowych zagadnienia związane z cyberbezpieczeństwem zyskiwały coraz wyraźniejsze znaczenie w debacie publicznej. W licznych opiniach i analizach podkreślano potrzebę podjęcia bardziej aktywnych i skoordynowanych działań publicznych w tym obszarze. Jednocześnie krajowy system cyberbezpieczeństwa[9] pozostawał w fazie przejściowej, co wynikało z oczekiwania na ostateczny kształt ustawy implementującej przepisy dyrektywy NIS2. Większość potencjalnych inicjatyw znajdowała się wówczas na etapie planowania lub wczesnego projektowania.

Można przy tym zakładać, że w trakcie wdrażania pilotażu jego kontekst instytucjonalny będzie ulegał dalszemu rozwojowi i stanie się bardziej złożony, wraz z uruchamianiem kolejnych instrumentów wsparcia oraz doprecyzowywaniem ram regulacyjnych. Z tego względu, na etapie opracowywania założeń programu, poszukiwano możliwych synergii z działaniami, których formuła była już znana lub które znajdowały się na zaawansowanym etapie realizacji. W toku prac zidentyfikowano następujące inicjatywy:

- **Firma Bezpieczna Cyfrowo**[10] – program realizowany przez NASK, ukierunkowany na wsparcie polskich przedsiębiorców w rozwijaniu kompetencji cyfrowych oraz podnoszeniu poziomu cyberbezpieczeństwa w sektorze MŚP. Program obejmuje dwa główne komponenty: diagnozę oceniającą aktualny poziom cyberbezpieczeństwa i kompetencji cyfrowych przedsiębiorstwa oraz raport wskazujący jego mocne strony, obszary wymagające poprawy oraz rekomendowane działania.
- **Partnerstwo dla Cyberbezpieczeństwa**[11] – inicjatywa rozwijana i koordynowana przez NASK, skupiająca ponad 100 firm, organizacji i instytucji reprezentujących sektor publiczny i prywatny. Jej celem jest wspieranie podmiotów Krajowego Systemu

[8] ENISA Threat Landscape 2024 – raport Agencji UE ds. Cyberbezpieczeństwa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[9] Przez krajowy system bezpieczeństwa cyfrowego rozumieć należy otoczenie instytucjonalne oparte na spójnych procedurach i podziale ról, które tworzą podmioty wskazane we właściwym regulacjach, w tym operatorzy usług kluczowych, dostawcy usług cyfrowych, Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) oraz dostawcy usług z zakresu cyberbezpieczeństwa.

[10] Pełny opis inicjatywy dostępny na stronie https://firmabezpiecznacyfrowo.pl/

[11] Pełny opis inicjatywy dostępny na stronie: https://cyberpolicy.nask.pl/program-partnerstwo-dla-cyberbezpieczenstwa/

Cyberbezpieczeństwa w identyfikacji zagrożeń, analizie ryzyk oraz wdrażaniu adekwatnych rozwiązań w obszarze cyberbezpieczeństwa.

- **CYBERSEC EDIH**[12] – Krajowe Centrum Bezpiecznej Transformacji Cyfrowej jest specjalistycznym Hubem Innowacji Cyfrowych (EDIH) w obszarze cyberbezpieczeństwa. Celem działania Centrum jest oferowanie podmiotom z grupy małych i średnich przedsiębiorstw, a także instytucjom państwowym i samorządowym, portfolio usług umożliwiających bezpieczne funkcjonowanie w pełni zdigitalizowanym otoczeniu oraz, szczególnie w przypadku przedsiębiorstw, wdrażanie w nim własnych rozwiązań dojrzałych technologicznie – ale jednocześnie odpornych na zaawansowane cyberataki.
- **Granty na cyberbezpieczeństwo dla MŚP**[13] – nabór realizowany był od sierpnia do października 2025 r. w ramach programu „Cyfrowa Europa", którego celem jest udzielenie pomocy de minimis w formie grantów na realizację projektów z zakresu cyberbezpieczeństwa przez mikro-, małe i średnie przedsiębiorstwa. Dofinansowanie przyznawane było na rozwój istniejących produktów lub usług, tworzenie nowych produktów lub usług, zwiększenie rozpoznawalności oferty beneficjentów oraz certyfikację produktów lub usług**.** Obecnie nabór jest już zamknięty.
- **Portal cyber.gov.pl**[14] – platforma przygotowana przez Ministerstwo Cyfryzacji i NASKW, dedykowana przedsiębiorcom, podmiotom KSC, a także obywatelom, która w jednym miejscu integruje kluczowe usługi do zgłaszania incydentów, udostępniania informacji o zagrożeniach i oferuje dostęp do narzędzi takich jak S46, moje.cert.pl czy bezpiecznedane.gov.pl. Platforma ma stanowić wiarygodne, centralne źródło aktualnych informacji z zakresu cyberbezpieczeństwa.

# 2. Założenia programu (teoria interwencji)

## 2.1. Przesłanki podjęcia interwencji

Na etapie projektowania pilotażu podjęto decyzję o zastosowaniu podejścia branżowego, polegającego na skoncentrowaniu wsparcia na wybranym sektorze gospodarki. Takie rozwiązanie umożliwia precyzyjne dopasowanie zakresu interwencji do specyficznych uwarunkowań działalności przedsiębiorstw, w tym profilu ryzyk, obowiązków regulacyjnych

[12] Pełny opis inicjatywy dostępny na stronie: https://cyber-sec.net.pl/
[13] Szczegółowe informacje o naborze i zasadach: https://www.gov.pl/web/cppc/nabor-dep010125
[14] Link do portalu: https://cyber.gov.pl/

oraz realnych możliwości organizacyjnych i kompetencyjnych podmiotów objętych wsparciem. W warunkach pilotażu podejście branżowe pozwala również na bardziej spójną realizację działań diagnostycznych i wdrożeniowych oraz na uzyskanie porównywalnych i użytecznych wniosków na potrzeby dalszego projektowania instrumentów wsparcia.

Skierowanie pilotażu do konkretnej branży wynikało ponadto z potrzeby skoncentrowania ograniczonych zasobów na obszarze, w którym ryzyka związane z cyberbezpieczeństwem są szczególnie wysokie, a potencjalne skutki incydentów mają istotny wymiar społeczny. Wybór jednego sektora umożliwia także testowanie kompleksowego modelu wsparcia – obejmującego diagnozę, audyt oraz wdrożenie systemowych rozwiązań – w warunkach pozwalających na rzetelną ocenę jego skuteczności i skalowalności.

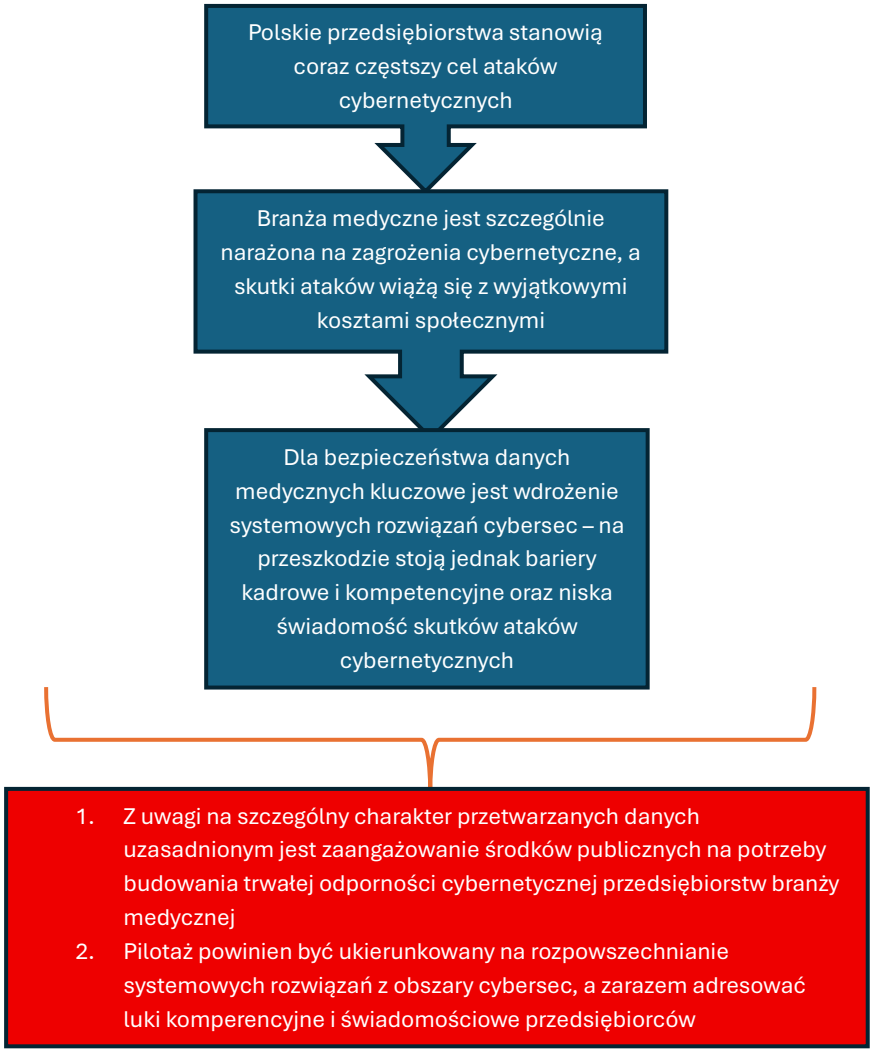
Mając na uwadze wyzwania, z jakimi mierzą się polscy przedsiębiorcy w obszarze cyberbezpieczeństwa, na szczególną uwagę zasługuje branża usług medycznych. Jest ona wskazywana jako jedna z najczęściej dotkniętych cyberatakami, a jednocześnie jako sektor o relatywnie niskiej odporności na tego rodzaju zagrożenia. Podmioty medyczne – zarówno działające w obszarze ochrony zdrowia, jak i świadczące usługi laboratoryjne, diagnostyczne czy terapeutyczne – przetwarzają dane o wyjątkowo wrażliwym charakterze. W konsekwencji incydenty związane z bezpieczeństwem cyfrowym mogą wpływać nie tylko na ciągłość funkcjonowania tych podmiotów, lecz także bezpośrednio na zdrowie, prywatność i bezpieczeństwo pacjentów.

W tym kontekście, publiczne wsparcie skierowane do przedsiębiorstw działających w branży medycznej nabiera szczególnego znaczenia. Podmioty te funkcjonują w środowisku wymagającym przetwarzania wrażliwych danych, podlegają rosnącym obowiązkom regulacyjnym, a jednocześnie często nie dysponują wystarczającymi zasobami kadrowymi ani kompetencjami umożliwiającymi samodzielne wdrażanie zaawansowanych środków ochrony cyfrowej. Ukierunkowana interwencja publiczna może zatem przyczynić się do przyspieszenia procesu dostosowania przedsiębiorstw do nowych wymogów, ograniczenia ryzyka incydentów wpływających na bezpieczeństwo danych oraz wzmocnienia ogólnej odporności cyfrowej sektora medycznego.

W oparciu o powyższe przesłanki, a także uwzględniając opisany wcześniej kontekst pilotażu oraz wstępne analizy i badania przeprowadzone w ramach procesu projektowego, przyjęto, że

wsparcie zostanie skierowane właśnie do branży medycznej. Wybór ten był motywowany nie tylko wysoką podatnością tego sektora na cyberataki, lecz także potencjalnie wysokimi kosztami społecznymi takich incydentów (zagrożenie dla danych medycznych). Jednocześnie zidentyfikowano, że jednym z kluczowych wyzwań pozostaje upowszechnienie systemowego podejścia do bezpieczeństwa cyfrowego, przy czym istotną barierę stanowią czynniki kompetencyjne, w tym ograniczona znajomość dostępnych rozwiązań z zakresu cyberbezpieczeństwa oraz niewystarczająca świadomość skutków ataków cybernetycznych.

W konsekwencji wskazane przesłanki wyznaczyły ramy koncepcyjne dla procesu projektowego, oparte na przedstawionym poniżej ciągu argumentów -



## 2.2. Cel programu

Cel pilotażu sformułowany został następująco:

Wsparcie przedsiębiorców w wypracowaniu trwałej odporności wobec specyficznych dla ich branży zagrożeń cybernetycznych

## 2.3. Odbiorcy programu

Grupą docelową programu są firmy z sektora MSP, które spełniają łącznie poniższe kryteria:

- NIE posiadają rozwiązań systemowych w zakresie cyberbezpieczeństwa,
- prowadzą dominującą działalność gospodarczą w branży medycznej,
- zarządzają danymi medycznymi (przetwarzają dane medyczne i zarządzają nimi samodzielnie w całości lub częściowo),
- są gotowe przeznaczyć zasoby ludzkie i finansowe konieczne dla samodzielnego utrzymania systemu cyberbezpieczeństwa po zakończeniu pilotażu.

Przez **branżę medyczną** rozumiane są podmioty prowadzące działalność związaną z opieką medyczną i zdrowotną (w tym podmioty świadczące usługi z obszaru zdrowia psychicznego), diagnostyką medyczną (z wyłączeniem laboratoriów zajmujących się prowadzeniem prac b+r), ratownictwem lub rehabilitacją.

## 2.4. Oczekiwana zmiana

Poprzez projektowany instrument dążymy do wprowadzenia zmiany na dwóch poziomach: mikro – poziom odbiorców rozwiązania oraz makro – zmiana na poziomie całego ekosystemu branży medycznej[15].

Poniżej znajduje się tabela przestawiająca oczekiwaną zmianę.

[15] Efekty na poziomie branżowym będą oczywiście warunkowane skalą prowadzonych działań. W przypadku pilotażu ich występowanie może być istotnie ograniczone. Zakładana teoria interwencji znajduje jednak odniesienie wobec ewentualnych przyszłych działań o większej skali, które bazowały będą na doświadczeniach związanych z wdrażaniem tego instrumentu.

**Tabela 1.** Oczekiwana zmiana na poziomie poszczególnych przedsiębiorstw oraz na poziomie systemowym

| Stan obecny | Pożądana zmiana |
|---|---|
| **Poziom systemowy** | |
| Branża medyczna, będąca szczególnie wrażliwym obszarem ze względu na dane pacjentów i ciągłość świadczenia usług zdrowotnych, charakteryzuje się niskim poziomem cyberbezpieczeństwa. | Podmioty świadczące usługi medyczne osiągają trwałą odporność cybernetyczną, zapewniając ochronę danych pacjentów i ciągłość krytycznych usług zdrowotnych. |
| **Poziom przedsiębiorstw** | |
| Przedsiębiorcy postrzegają cyberbezpieczeństwo jako koszt, a nie inwestycję – brak świadomości realnego ryzyka i wagi tematu. | Przedsiębiorcy dostrzegają wagę cyberbezpieczeństwa i rozumieją, że problem ich bezpośrednio dotyczy. Traktują cyberbezpieczeństwo jako element wyróżniający firmę na rynku i budujący przewagę konkurencyjną. |
| Przedsiębiorcy podejmują w zakresie cyberbezpieczeństwa działania punktowe i nieusystematyzowane. | Przedsiębiorcy wdrażają systemowe podejście do cyberbezpieczeństwa z jasno określoną odpowiedzialnością i procedurami. |
| Przedsiębiorcy działają reaktywnie – reagują na incydenty, gdy już się wydarzą, zamiast działać prewencyjnie. | Przedsiębiorcy podejmują działania prewencyjne i proaktywnie zabezpieczają firmę przed zagrożeniami, zanim dojdzie do incydentów. |
| Przedsiębiorcy mają ograniczoną wiedzę branżową – nie znają dostępnych rozwiązań, dostawców ani standardów w zakresie cyberbezpieczeństwa. | Przedsiębiorcy posiadają wiedzę z zakresu cyberbezpieczeństwa dopasowaną do ich potrzeb i specyfiki działalności, znają dostępne na rynku rozwiązania. |

| | |
|---|---|
| Przedsiębiorcy nie zdają sobie sprawy z nadchodzących regulacji NIS 2 i wymagań, którym będą podlegać. | Przedsiębiorcy są świadomi wymagań dyrektywy NIS 2 oraz potrafią przygotować firmę do ich spełnienia. |

# 3. Opis programu wsparcia

## 3.1. Ścieżka uczestnika programu

Planowane w ramach pilotażu wsparcie będzie realizowane w formule pięciu następujących po sobie kroków, które można przyporządkować do dwóch głównych części:

**Część I – przygotowanie do złożenia wniosków o dofinansowanie**

Na etapie przygotowania do złożenia wniosków realizacja pilotażu będzie angażować podmioty zrzeszone w sieci EDIH (*European Digital Innovation Hubs*). Szczegółowe informacje dotyczące sposobu wyłaniania tych podmiotów oraz zasad współpracy pomiędzy nimi a Polską Agencją Rozwoju Przedsiębiorczości zostały przedstawione w rozdziale 4. Formuła programu.

**Część II – wdrażanie dofinansowanych projektów**

Druga część pilotażu będzie bezpośrednio związana z wdrażaniem systemowych rozwiązań w obszarze cyberbezpieczeństwa. Działania te będą finansowane w ramach projektów zaplanowanych na podstawie diagnoz i audytów przeprowadzanych na wcześniejszym etapie przez ośrodki EDIH.

### 3.1.1. Selekcja firm do programu

Przewiduje się przeprowadzenie przez EDIH-y wstępnej weryfikacji przedsiębiorstw, które zgłoszą zainteresowanie udziałem w pilotażu. Na tym etapie analizowana będzie ogólna zgodność profilu zgłaszających się podmiotów z założeniami dotyczącymi grupy docelowej. W szczególności uwzględnione zostaną następujące aspekty:

- funkcjonowanie w sektorze małych i średnich przedsiębiorstw,
- prowadzenie dominującej działalności w obszarze usług medycznych, w tym stomatologicznych, rehabilitacyjnych lub psychoterapeutycznych,
- przetwarzanie danych medycznych pacjentów (w tym wyników badań diagnostycznych), przy założeniu, że kwestie bezpieczeństwa tych danych nie są w całości realizowane przez podmioty zewnętrzne (np. w ramach wykupionych usług chmurowych),
- brak lub ograniczone wykorzystanie systemowych rozwiązań w zakresie bezpieczeństwa cyfrowego.

Podmioty spełniające powyższe założenia zostaną zaproszone do udziału w kolejnym etapie pilotażu, obejmującym skorzystanie z usług diagnozy i audytu.

### 3.1.2. Diagnoza firm i audyt ekspercki

Na tym etapie świadczenie usług będzie realizowane przez ośrodki EDIH. Zakłada się, że oferowane wsparcie będzie oparte na usługach dostępnych już w portfolio ośrodków wybranych do współpracy lub – w razie potrzeby – na usługach zmodyfikowanych i dostosowanych do specyficznych założeń pilotażu.

W pierwszym kroku realizowane będą ankiety diagnostyczne, oparte na wystandaryzowanych kwestionariuszach. Zebrane w ich ramach informacje pozwolą na identyfikację kluczowych, z punktu widzenia bezpieczeństwa cyfrowego, procesów, zasobów oraz ryzyk charakterystycznych dla danej organizacji prowadzącej działalność w branży medycznej.

Efektem przeprowadzenia ankiety diagnostycznej będzie opracowanie wstępnego profilu bezpieczeństwa cyfrowego dla poszczególnych przedsiębiorstw oraz określenie szczegółowego planu audytu dostosowanego do ich specyfiki.

Audyty eksperckie będą prowadzone zgodnie z metodyką zaakceptowaną przez Polską Agencję Rozwoju Przedsiębiorczości, przy czym ich zakres każdorazowo będzie dostosowywany do potrzeb i uwarunkowań danego beneficjenta. Osoby realizujące audyty będą posiadały odpowiednią wiedzę specjalistyczną oraz doświadczenie w zakresie projektowania i wdrażania systemów bezpieczeństwa cyfrowego. Zakres prac audytorów obejmować będzie w szczególności analizę dokumentacji i obowiązujących procedur, wizyty w siedzibie beneficjenta oraz rozmowy z kadrą zarządzającą i administratorami danych.

Efektem przeprowadzenia diagnoz i audytów eksperckich będą **Raporty diagnostyczne.** Minimalny zakres zgromadzonych informacji powinien być wystarczający, aby każdy z Raportów zawierał następujące elementy:

**Zakres obszarów związanych z cyberbezpieczeństwem, która uwzględnione zostaną w Raportach diagnostycznych**

- Opis kluczowych zasobów ludzkich, infrastrukturalnych i informacyjnych,
- Wskazanie newralgicznych obszarów i procesów,
- Identyfikację kluczowych ryzyk,
- Odniesienie do kontekstu prawnego,
- Rekomendacje wdrożeniowe – w tym: zalecenie dotyczące wyboru oprogramowania, koniecznych inwestycji w infrastrukturę informatyczną – wskazanie działań koniecznych i zalecanych,
- Oszacowanie kosztów wdrożenia i utrzymania systemu zarządzania bezpieczeństwem cyfrowym,
- Opcjonalnie: Podsumowanie wyników testów penetracyjnych.

### 3.1.3. Wypełnienie wniosku o dofinansowanie

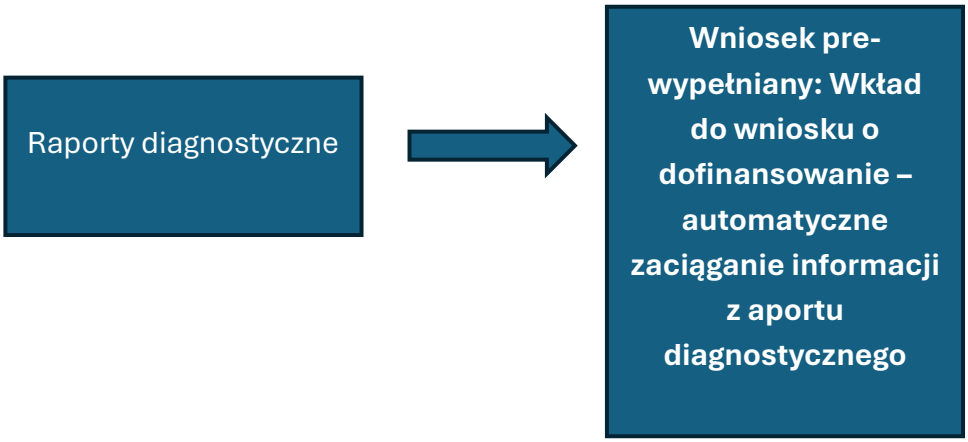
Raporty diagnostyczne stanowić będą podstawę do przygotowania wstępnie wypełnionych wniosków o dofinansowanie kosztów wdrożenia systemów bezpieczeństwa cyfrowego. W miarę dostępności odpowiednich rozwiązań technologicznych możliwe będzie automatyczne eksportowanie do wniosków wybranych danych i zapisów zawartych w Raportach.

W wariancie bazowym Raporty, opracowane w oparciu o wystandaryzowaną strukturę, będą stanowiły załączniki do składanych wniosków. Zakres informacji pozyskanych w toku diagnozy pozwoli każdorazowo na oszacowanie kosztów projektu oraz precyzyjne zdefiniowanie parametrów planowanych do wdrożenia rozwiązań.

Zastosowanie takiego podejścia umożliwi:

- ograniczenie do minimum obciążeń biurokratycznych po stronie przedsiębiorców,
- usprawnienie procesu oceny wniosków po stronie Polskiej Agencji Rozwoju Przedsiębiorczości,

- zapewnienie spójności założeń dofinansowanych projektów z wynikami przeprowadzonych diagnoz.




### 3.1.4. Wdrożenie systemów cybersec

Przedsiębiorcy, których wnioski uzyskają pozytywną ocenę, przystąpią do etapu wdrażania systemów cyberbezpieczeństwa. Zakres działań realizowanych na tym etapie obejmować będzie zakup rozwiązań technologicznych oraz usług objętych dofinansowaniem, a także – opcjonalnie – realizację dodatkowych działań rekomendowanych i wskazanych w Raportach diagnostycznych.

W ramach dofinansowanych projektów jako kwalifikowane uznane będą następujące kategorie kosztów:

- koszty wartości niematerialnych i prawnych, w szczególności licencje roczne lub miesięczne (do 12 miesięcy),
- subskrypcje,
- koszty usług niezbędnych do wdrożenia systemów bezpieczeństwa cyfrowego (w tym: doradztwo wdrożeniowe),
- koszty pozostałych usług doradczych (w tym: usługi doradztwa prawnego w zakresie cyberbezpieczeństwa, NIS-2, regulacji dotyczących zastosowania narzędzi sztucznej inteligencji),
- koszty usług szkoleniowych (w tym: szkoleń związanych z przygotowaniem do wdrożenia i utrzymania systemów bezpieczeństwa cyfrowego),

- koszty usług informatycznych polegających na przygotowaniu i przeprowadzeniu testów penetracyjnych.

**WAŻNE: W toku procesu projektowego podjęto decyzję, że do kosztów kwalifikowanych NIE zastaną zaliczone jakiekolwiek wydatki przeznaczone na zakup środków trwałych, które w przypadku tego pilotażu mogłyby obejmować przede wszystkim elementy infrastruktury informatycznej (np. komputery, serwery)**

Decyzja ta wynikała z dążenia do:

- Koncentracji na newralgicznych potrzebach branży – wedle prowadzonych w trakcie procesu badań, kluczowe luki dotyczą dostępności adekwatnego oprogramowania oraz systemowego podejście do bezpieczeństwa cyfrowego, a nie infrastruktury sprzętowej
- Zachowania zasady dodatkowości interwencji publicznych – zakup niezbędnego sprzętu IT jest standardowym kosztem prowadzenia działalności i nie powinien być finansowany ze środków publicznych.
- Ograniczenia ryzyka nadużyć – istniało ryzyko „pompowania" budżetu projektów sprzętem, co odbiegałoby od celu interwencji.

Beneficjenci zaangażują do realizacji projektu osoby lub zespoły odpowiedzialne za obsługę oraz utrzymanie wdrożonych rozwiązań po zakończeniu pilotażu, w tym administratorów systemów cyberbezpieczeństwa. Wskazane zostaną również osoby pełniące funkcje zarządcze, do których kompetencji należeć będzie nadzór nad prawidłowym funkcjonowaniem systemów cyberbezpieczeństwa.

Zakup dofinansowanych usług i rozwiązań będzie realizowany przez beneficjentów z zachowaniem zasad konkurencyjności oraz procedur właściwych dla projektów objętych dofinansowaniem w ramach programu FENG.

Efektem tego etapu będzie faktyczne wdrożenie systemów bezpieczeństwa cyfrowego, ukierunkowanych na ochronę zasobów informacyjnych, ze szczególnym uwzględnieniem danych medycznych. Przez kompletny i wdrożony system rozumiany będzie:

- ***Spisany zestaw spójnych procedur definiujących sposoby identyfikowania zagrożeń cybernetycznych, a także zapobiegnia ich materializacji i niwelowania skutków ich wystąpienia wraz z przypisanymi zadaniami i zakresami odpowiedzialności (rolami), a także oprogramowaniem dedykowanym obsłudze systemu bezpieczeństwa cyfrowego.***

Kluczowym produktem wdrożenia będzie **Dokumentacja systemu zarządzania bezpieczeństwem cyfrowym.**

**Zakres Dokumentacji systemu zarządzania bezpieczeństwem cyfrowym -**

- Zakres zadań i charakterystyki pracy Administratora/Zespołu ds. Cyberbezpieczeństwa,
- Opis wymagań funkcjonalnych oprogramowania obsługującego system,
- Definicje reguł dotyczących identyfikacji, oceny i obsługi incydentów oraz zdarzeń (reguł korelacyjnych),
- Opis zgodności procedur z wymaganiami prawnymi, odniesienie do regulacji prawnych (w tym NITS2O),
- Polityka Bezpieczeństwa Informacji - określenie głównych celów, zakresu i zasad zarządzania cyberbezpieczeństwem w organizacji,
- Ocena Ryzyka - Dokumentacja identyfikująca i analizująca zagrożenia, wraz z planami postępowania z ryzykiem (nadrzędna dokumentacja w stosunku do procedur).

Opcjonalnie: Podsumowanie wyników testów penetracyjnych przeprowadzonych po wdrożeniu systemu.

### 3.1.5. Utrzymania systemu

Zgodnie z celami pilotażu beneficjenci powinni wdrożyć rozwiązania zapewniające trwałą odporność na zagrożenia cybernetyczne. Kluczowe znaczenie ma przy tym zdolność uczestników pilotażu do samodzielnego utrzymania pełnej funkcjonalności wdrożonych systemów również po zakończeniu okresu dofinansowania.

Koszty utrzymania systemów po zakończeniu projektów będą leżały po stronie Beneficjentów.

Na tym etapie, przedsiębiorcy zobowiązani będą zachować trwałość efektów wsparcia przez co najmniej 3 lata od zakończenia realizacji swoich projektów.

Z punktu widzenia zasobów zaangażowanych w utrzymania systemów kluczowe będzie:

- Sfinansowanie kosztów osobowych związanych z zapewnieniem administratorów systemów lub zespołów zarządzania cyberbezpieczeństwem,
- Zapewnienie funkcjonalności oprogramowania obsługującego system, w tym dokonywanie niezbędnych aktualizacji oraz konfiguracji odpowiadających dynamice zagrożeń i specyfiki biznesowej beneficjentów.

Szacowne koszty utrzymania systemów powinny zostać ustalone na etapie opracowywania Raportów diagnostycznych oraz być uwzględnione przez przedsiębiorców podejmujących decyzje o aplikowaniu do pilotażu.

## 3.2. Usługi dostępne dla Beneficjentów

**Doradztwo wdrożeniowe.** Będzie to kluczowa usługa, spajające ze sobą efekty pozostałych dofinansowanych działań. Punktem wyjścia dla pracy doradców będzie analiza zaleceń wskazanych w Raportach diagnostycznych, a na ich podstawie dostarczania beneficjentom wskazówek potrzebnych w trakcie wdrażania systemów bezpieczeństwa cyfrowego. Zadaniem doradców będzie także nadzorowanie wdrożenia oprogramowania obsługującego system *cybersec*, w tym jego odpowiedniego skonfigurowania. Doradcy odbędą ponadto w razie potrzeby wizyty w siedzibach beneficjentów, przeprowadzą rozmowy z kluczowymi osobami (menadżerami, administratorami systemów bezpieczeństwa). W razie potrzeby, zadaniem doradców będzie także przeprowadzenie dodatkowych rozmów diagnozujących potrzeby i ryzyka poszczególnych przedsiębiorstw. Usługa doradztwa wdrożeniowego będzie mogła być pozyskiwana na rynku w pakietach z oprogramowaniem lub innymi usługami przewidzianymi we wnioskach o dofinansowanie (np. wraz ze szkoleniami przygotowującymi do obsługi i utrzymania systemów).

**Zakup licencji lub Cybersecurity as a Service (CSaaS).** Systemy bezpieczeństwa cyfrowego

obsługiwane są przez dedykowane do tych celów aplikacje. Ich zakup może wiązać się z wysokimi kosztami, dlatego też wydatki z tym związane objęte zostały dofinansowaniem pilotażu. Dopuszcza się różne formy pozyskiwania tego typu oprogramowania, w tym licencje, usługi udzielane na zasadzie opłat za subskrypcje oraz aplikacje szyte na miarę bazujące na dostępnych rozwiązaniach typu *open source.*

**Szkolenia dla administratorów i osób zarządzających.** Szkolenia będą miały rolę uzupełniającą

wobec doradztwa wdrożeniowego. Będą one skierowane do osób zarządzających oraz administrujących bezpieczeństwem cyfrowym. Tematyka szkoleń związana będzie bezpośrednio z obsługą i utrzymaniem wdrażanych systemów. Ich celem nie będzie natomiast uwrażliwienie szerokiego grona pracowników w zakresie zagrożeń. Przyjęto bowiem, że tego typu usługi są obecnie szeroko dostępne w formie bezpłatnej lub nisko kosztowej, a zatem ich finansowania w ramach pilotażu nie znajduje uzasadnienia.

**Doradztwo prawne.** Usługi tego rodzaju będą miały przede wszystkim na celu wsparcie

beneficjentów w weryfikacji – w przypadkach wymagających pogłębionej analizy – zgodności wdrażanych oraz dotychczas stosowanych rozwiązań z regulacjami dotyczącymi ochrony danych osobowych i danych medycznych, a także z przepisami wynikającymi z dyrektyw odnoszących się do bezpieczeństwa cyfrowego. Wsparcie to będzie mogło obejmować również ocenę poprawności proceduralnej oraz zgodności regulacyjnej narzędzi opartych na rozwiązaniach sztucznej inteligencji wykorzystywanych przez beneficjentów.

**Symulacje ataków i wykrywanie słabych punktów**. Testy będą przeprowadzane po

zakończeniu wdrażania systemów cyberbezpieczeństwa. Ich celem będzie ocena faktycznej odporności beneficjentów na zagrożenia cybernetyczne oraz identyfikacja ewentualnych podatności. Realizacja tych usług, podobnie jak na etapie diagnozy, będzie miała charakter fakultatywny.

Rekomendacje wynikające z przeprowadzonych testów powinny zostać ujęte w Dokumentacji systemu zarządzania bezpieczeństwem cyfrowym oraz wdrożone najpóźniej do zakończenia okresu trwałości projektu.

# 4. Formuła programu

## 4.1. Sposób wdrażania

W realizację pilotażu zaangażowane zostaną organizacje działające w ramach sieci **EDIH (*European Digital Innovation Hubs*)**. Jest to sieć punktów kompleksowej obsługi przedsiębiorstw, w tym mikro-, małych i średnich, ukierunkowana na wspieranie ich w podnoszeniu poziomu cyfryzacji oraz zwiększaniu konkurencyjności.

Ośrodki EDIH tworzone są w formule partnerstw obejmujących jednostki naukowe, instytucje otoczenia biznesu oraz przedsiębiorstwa. W swojej działalności współpracują one z szerokim gronem podmiotów zaangażowanych w rozwój technologiczny, w tym z uczelniami wyższymi, parkami technologicznymi, inkubatorami przedsiębiorczości, agencjami rozwoju oraz dostawcami rozwiązań cyfrowych.

Zadania ośrodków EDIH związane będą z realizacją pierwszej części pilotażu. Ich kluczowym zadaniem będzie prowadzenie diagnoz i audytów oraz przygotowanie raportów diagnostycznych, stanowiących wkład do wniosków o dofinansowanie.

Usługi w zakresie diagnozy oraz audytu eksperckiego będą realizowane w oparciu o ofertę dostępną już w portfolio wybranych ośrodków EDIH. Z tego względu zakłada się, że w realizację pilotażu zaangażowane zostaną ośrodki wyspecjalizowane w obszarze cyberbezpieczeństwa. Polska Agencja Rozwoju Przedsiębiorczości nie będzie szczegółowo określać metodyki realizacji tych usług, przy czym ośrodki EDIH zobowiązane będą do zapewnienia odpowiednio wykwalifikowanej kadry oraz do przygotowania raportów diagnostycznych w oparciu o wystandaryzowaną strukturę. Usługi EDIH - o ile odpowiadać będą zadaniom realizowanym w ramach Działania 2.22 FENG - świadczone będą bezpłatnie, na zasadach pomocy *de minimis.* . Rozliczenie kosztów będzie realizowane w ramach dotacji przyznanych na działalność EDIH. Proces oceny wniosków przygotowanych w oparciu o raporty diagnostyczne będzie realizowany przez Polską Agencję Rozwoju Przedsiębiorczości. W drugiej części pilotażu beneficjenci wyłonieni w wyniku oceny będą realizować swoje projekty zgodnie z założeniami

określonymi w raportach diagnostycznych, korzystając z usług objętych dofinansowaniem, opisanych we wcześniejszym rozdziale.

W celu uniknięcia potencjalnych konfliktów interesów podmioty tworzące ośrodki EDIH, zaangażowane w realizację pierwszej części pilotażu, nie będą uprawnione do świadczenia dofinansowanych usług na rzecz beneficjentów na etapie wdrażania projektów

## 4.2. Harmonogram

W przypadku poszczególnych beneficjentów okres uczestnictwa w pilotażu powinien wynosić **18 miesięcy**, licząc od momentu zakwalifikowania do udziału w diagnozie i audycie (Część I pilotażu) do momentu zakończenia wdrożenia systemu bezpieczeństwa cyfrowego (Część II pilotażu). Zarazem na realizację Części II powinno być przeznaczone nie więcej niż **12 miesięcy**

## 4.3. Budżet i zasady finansowania

Usługi świadczone przez ośrodki EDIH w Części I pilotażu będą realizowane na zasadach pomocy de minimis, a ich wartość będzie uwzględniania w limitach poszczególnych Beneficjentów. Koszty usług będę rozliczane w ramach dotacji przyznanych ośrodkom EDIH.

Wdrażania systemów bezpieczeństwa cyfrowego (Część II) będzie odbywać się na podstawie umów o powierzenie grantu Wartość grantów przyznawanych poszczególnym beneficjentom mieścić się będzie w przedziale **od 80 000 do 500 000 zł.**

**Szacowana łączna wartość środków przeznaczonych na granty wyniesie 10 mln złotych, co powinno pozwolić na wsparcie około 30 projektów.**

Beneficjenci będą zobowiązani do wniesienia wkładu własnego w wysokości 20% kosztów kwalifikowanych projektu.

## 4.2. Kryteria kwalifikujące Beneficjentów

W toku procesu projektowego wypracowano kryteria kwalifikujące przedsiębiorców do udziału w Części II pilotażu, które podzielono na dwie kategorie. Wypracowania wymagają nadal kryteria rankingujące. Szczegółowy sposób kwalifikacji do Części I opracowany zostanie przez EDIH-y i odpowiadał będzie założeniom w zakresie celów pilotażu oraz charakterystyki jego uczestników.

**Kryteria dostępowe**

Kryteria dostępowe określają, czy przedsiębiorca może ubiegać się o wsparcie w ramach pilotażu. Obejmują one:

- przynależność do grupy docelowej pilotażu,
- posiadanie audytu przeprowadzonego przez ośrodek EDIH, wykonanego zgodnie z minimalnym zakresem określonym w programie, przy czym audyt ten stanowi podstawę do sformułowania rekomendacji, na które odpowiadać będzie planowane wsparcie.

**Kryteria merytoryczne**

Kryteria merytoryczne mają charakter zero-jedynkowy i służą ocenie adekwatności zgłaszanego projektu. Obejmują one następujące elementy:

- **spójność planowanych działań z rekomendacjami zapisanymi w Raporcie diagnostycznym** – zakres projektu musi w całości wynikać z przeprowadzonej diagnozy; nie dopuszcza się realizacji działań niepowiązanych z raportem audytowym,
- **adekwatność proponowanych działań do zidentyfikowanych potrzeb** – planowane działania powinny bezpośrednio odpowiadać na luki w obszarze cyberbezpieczeństwa zidentyfikowane w toku audytu,
- **kompletność i poprawność dokumentacji aplikacyjnej** – zgodność z wymaganiami proceduralnymi określonymi przez Polską Agencję Rozwoju Przedsiębiorczości,
- **zgodność zakresu projektu z katalogiem kosztów kwalifikowanych** – przy czym w ramach pilotażu wykluczono finansowanie środków trwałych,
- **realistyczność harmonogramu oraz wykonalność projektu** – możliwość realizacji zaplanowanych działań w okresie przewidzianym dla pilotażu.

## 4.3. Wskaźniki efektów pilotażu

Wypracowane wskaźniki efektów odnoszą się zarówno do produktów, rozumianych jako liczba usług świadczonych w ramach programu oraz działań zrealizowanych w związku z wdrażaniem projektów, jak i do rezultatów, czyli bezpośrednich efektów pilotażu. Wśród nich można wyróżnić wskaźniki, których pomiar będzie prowadzony w ramach bieżącej sprawozdawczości

(oznaczone literą „S”), oraz wskaźniki, których wartości zostaną określone w toku ewaluacji końcowej, przeprowadzanej nie wcześniej niż 6 miesięcy po zakończeniu pilotażu (oznaczone literą „E”).

**Wskaźniki produktowe**

1. Liczba przedsiębiorstw objętych audytem cyberbezpieczeństwa: liczba MŚP z branży medycznej, które ukończyły pełny audyt EDIH zgodnie z minimalnym zakresem (S).
2. Liczba przygotowanych raportów z audytu: liczba raportów zawierających diagnozę oraz rekomendacje działań (S).
3. Liczba przedsiębiorstw, które złożyły wnioski o dofinansowanie na podstawie audytu: liczba poprawnych i kompletnych wniosków wynikających bezpośrednio z rekomendacji audytu (S).
4. Liczba przedsiębiorstw objętych wsparciem w formie usług doradczych i wdrożeniowych: liczba firm, które rozpoczęły realizację działań rekomendowanych w audycie (S).
5. Liczba wdrożonych rozwiązań informatycznych zwiększających poziom cyberbezpieczeństwa: liczba instalacji, konfiguracji lub aktualizacji narzędzi wskazanych w audycie (S).

**Wskaźniki rezultatu**

1. Liczba przedsiębiorstw, które zakończyły pełne wdrożenie rekomendacji audytu – liczba mikro-, małych i średnich przedsiębiorstw, które zrealizowały wszystkie kwalifikowane rekomendacje audytu zgodnie z zakresem zatwierdzonego projektu (S).
2. Liczba przedsiębiorstw, u których potwierdzono wzrost poziomu cyberbezpieczeństwa – liczba przedsiębiorstw, w których potwierdzono poprawę poziomu cyberbezpieczeństwa, m.in. poprzez wdrożenie procedur organizacyjnych, funkcjonowanie narzędzi informatycznych wspierających system bezpieczeństwa cyfrowego oraz pozytywne wyniki testów bezpieczeństwa, w tym testów penetracyjnych (S – weryfikacja na podstawie dokumentacji zgromadzonej w trakcie realizacji projektów).
3. Liczba przedsiębiorstw, które uzyskały trwałe efekty w zakresie organizacji i zarządzania cyberbezpieczeństwem – liczba przedsiębiorstw utrzymujących

funkcjonujące systemy bezpieczeństwa cyfrowego po zakończeniu wsparcia, w tym wykazujących m.in. zmniejszenie liczby incydentów lub eliminację zidentyfikowanych podatności na zagrożenia cybernetyczne (E – pomiar na podstawie analizy danych sprawozdawczych oraz badania beneficjentów).

4. Skłonność do polecania uczestnictwa w programie – wartość wskaźnika NPS (Net Promoter Score), określana na podstawie badania beneficjentów po zakończeniu pilotażu (E).
5. Liczba przedsiębiorstw dostosowały się do wymogów NIS2 (E – pomiar na podstawie analizy danych sprawozdawczych oraz badania beneficjentów).
6. Liczba przedsiębiorstw objętych certyfikacją NASK (E – pomiar na podstawie badania beneficjentów).
7. Liczba pacjentów, których dane zostały objęte systemową ochroną (S – na początku wdrażania, na podstawie danych podanych we wnioskach, E – aktualizacja po zakończeniu pilotażu na podstawie badania beneficjentów).

## 4.4. Ryzyka

**Opóźnienia w zatwierdzaniu dokumentacji dotyczącej działań EDIH –** zastosowanie formuły pilotażu opartej na zaangażowaniu ośrodków EDIH wymaga uzyskania akceptacji ze strony Instytucji Zarządzającej. Proces zatwierdzania niezbędnej dokumentacji może ulec wydłużeniu, co może warunkować termin rozpoczęcia realizacji pilotażu. W celu ograniczenia ryzyka materializacji tego zagrożenia proces akceptacji będzie na bieżąco monitorowany przez jednostkę odpowiedzialną za wdrażanie pilotażu, tj. Departament Usług Proinnowacyjnych Polskiej Agencji Rozwoju Przedsiębiorczości.

**Nadmierne obciążenie ośrodków EDIH w okresie realizacji pilotażu –** ośrodki wyspecjalizowane w obszarze cyberbezpieczeństwa dysponują odpowiednim zapleczem eksperckim i organizacyjnym. Należy jednak uwzględnić, że obsługa pilotażu będzie stanowiła jedynie część ich bieżących zadań statutowych i projektowych. W związku z tym w niektórych okresach dostępność kluczowych ekspertów może być ograniczona, co może wpływać na tempo realizacji działań. Ograniczeniu tego ryzyka służyć będzie odpowiednie planowanie harmonogramu pilotażu oraz bieżąca koordynacja działań z zaangażowanymi ośrodkami EDIH.

**Ryzyko wyczerpania limitów usług audytowych oraz zakończenia działalności EDIH –** w toku procesu projektowego zwrócono uwagę na konieczność synchronizacji naboru uczestników pilotażu z dostępnością audytów realizowanych przez ośrodki EDIH. Ośrodki te dysponują bowiem określoną liczbą usług audytorskich zaplanowanych w swoich budżetach, które są świadczone na zasadach ogólnodostępnych. Okres ich realizacji jest ponadto ograniczony umowami finansowania sieci EDIH. Opóźnienia w uruchomieniu pilotażu mogłyby zatem stwarzać realne zagrożenie dla dostępności tych usług.

**Niejednorodna jakość usług świadczonych przez ośrodki EDIH** – metodyka świadczenia usług diagnostycznych i audytorskich pozostanie w gestii poszczególnych ośrodków EDIH, co może skutkować zróżnicowanym poziomem dopasowania stosowanych podejść do specyfiki pilotażu. W celu ograniczenia tego ryzyka kluczowe znaczenie będzie miało precyzyjne określenie wymagań dotyczących kwalifikacji osób realizujących usługi na rzecz uczestników pilotażu, a także bieżące monitorowanie jakości kluczowych produktów, ze szczególnym uwzględnieniem raportów diagnostycznych.

## 4.5. Kwestia wymagające doprecyzowania

W toku prac zespołu zidentyfikowano kilka obszarów wymagających pogłębionej analizy oraz podjęcia rozstrzygnięć na kolejnych etapach projektowania pilotażu.

### a) Kryteria rankingujące

W trakcie procesu projektowego nie podjęto ostatecznych decyzji dotyczących kryteriów rankingujących, które umożliwiałyby selekcję beneficjentów w sytuacji, gdy liczba przedsiębiorstw spełniających kryteria kwalifikacyjne przekroczy zakładaną liczbę uczestników pilotażu.

Niemniej jednak, w toku prac projektowych przyjęto założenie, że kryteria rankingujące powinny:

- opierać się na danych łatwo dostępnych, mierzalnych i porównywalnych,
- umożliwiać równą ocenę przedsiębiorców o zróżnicowanej specyfice działalności,
- nie wymagać przedkładania dodatkowych dokumentów ani przeprowadzania dodatkowych analiz eksperckich.

Wśród rekomendowanych podejść wskazano również możliwość zastosowania kryterium losowego doboru określonej liczby beneficjentów spośród puli przedsiębiorstw spełniających kryteria kwalifikacyjne. Rozwiązanie tego rodzaju jest stosowane w ramach interwencji publicznych, w szczególności w krajach anglosaskich, a jego zasadność jest szczególnie wysoka w przypadku interwencji o charakterze pilotażowym. Pilotaże pełnią bowiem funkcję działań o charakterze eksperymentalnym, w których losowy dobór uczestników uznawany jest za metodycznie pożądany standard.

Zastosowanie mechanizmu losowego doboru uczestników stanowi ponadto istotne uproszczenie procesu wdrażania pilotażu oraz ogranicza obciążenia organizacyjne po stronie jednostki odpowiedzialnej za jego realizację.

**b) Możliwość realizacji testów penetracyjnych przez EDIH**

Konieczne jest potwierdzenie czy ośrodki EDIH dysponują odpowiednimi zasobami, kompetencjami oraz infrastrukturą techniczną umożliwiającą realizację testów penetracyjnych jako elementu usług świadczonych w ramach pilotażu.

**c) Wypracowanie założeń promocji i komunikacji pilotażu**

Niezbędne jest podjęcie decyzji dotyczącej sposobu obsługi umów oraz prowadzenia komunikacji z grupą docelową, a następnie z beneficjentami pilotażu.

**d) Przygotowanie systemu informatycznego dla obsługi wniosków o dofinansowania i umów**

Beneficjenci działań pilotażowych nie są obecnie uwzględnieni w lokalnych systemach informatycznych Polskiej Agencji Rozwoju Przedsiębiorczości. W konsekwencji dane dotyczące obsługi umów gromadzone są w rozproszonych zbiorach, pozbawionych niezbędnej standaryzacji. Rozwiązanie to generuje istotny nakład dodatkowej pracy organizacyjnej, a jednocześnie negatywnie wpływa na jakość gromadzonych danych, utrudniając prowadzenie rzetelnych analiz oraz sprawne pozyskiwanie kluczowych informacji zarządczych.

W związku z powyższym zapewnienie dedykowanego, profesjonalnego systemu informatycznego do obsługi pilotażu powinno zostać uznane za jeden z kluczowych priorytetów poprzedzających jego wdrożenie.

# 5. Proces projektowy

## 5.1. Uczestnicy/czki procesu projektowego

Proces projektowy został przeprowadzony przez zespół projektowy Inno_LAB. W skład głównego zespołu projektowego weszły następujące pracownice/y PARP:

- Maciej Szałaj – Departament Analiz i Strategii
- Sylwia Rink – Departament Analiz i Strategii
- Dorota Węcławska – Departament Analiz i Strategii
- Martyna Maciaszczyk – Departament Analiz i Strategii
- Izabela Banaś – Departament Analiz i Strategii
- Hubert Pol – Departament Usług Proinnowacyjnych
- Elżbieta Koniuszewska – Departament Usług Proinnowacyjnych
- Michał Ciapara – Departament Usług Proinnowacyjnych

## 5.2. Metodologia

Proces prowadzony był wg metodologii *service design*. Ten tryb pracy został przyjęty z uwagi na potrzebę zrozumienia potrzeb użytkowników docelowych.

Wybrana metoda pracy charakteryzuje się koncentracją na realnych potrzebach, bolączkach i wyzwaniach użytkowników. W podejściu praktykowanym w ramach Inno_LAB jest ona zestawiana z pożądaną zmianą na poziomie gospodarki.

Rozpoznanie spektrum problemowego i jego zrozumienie jest punktem wyjścia do procesu wypracowywania rozwiązań. Prace projektowe odbywały się przede wszystkim w formule warsztatowej, dodatkowo miały miejsce spotkania robocze zespołu projektowego. Celem spotkań zespołu projektowego było analizowanie materiałów z przeprowadzonych badań i warsztatów, dopracowywanie rozwiązań projektowych oraz planowanie dalszych kroków w procesie.

Proces projektowy trwał około trzech miesięcy (październik - grudzień 2025 r.).

Spotkania odbywały się w formule zarówno zdalnej z wykorzystaniem narzędzi Teams oraz Mural, jak i w formie stacjonarnej.

Spotkanie i warsztaty, które odbywały się w ramach procesu, były facylitowane przez wykonawcę zewnętrznego – konsorcjum firm EGO-Evaluation for Government Organization S.C i missing dot studio Agnieszka Mróz (Zuzanna Popis, Agnieszka Mróz).

## 5.3. Definiowanie problemu i kierunki projektowe

Prace projektowe rozpoczęto od przeprowadzenia *desk research*. Kluczowe zagadnienia jakie zostały wytypowane do zbadania w obszarze cyberbezpieczeństwa to:

- regulacje krajowe i europejskie,
- dane statystyczne dot. zagrożeń,
- bariery i wyzwania stojące przed MSP,
- wsparcie systemowe w Polsce i dostępne instrumenty.

W dniu 07.10.2025 r. w siedzibie PARP odbyło się spotkaniu strategiczne. Uczestniczyły/li w nim przedstawicielki/e:

- NASK (2 os.),
- Ministerstwa Cyfryzacji (1 os.),
- Ministerstwa Rozwoju i Technologii, Departament Gospodarki Cyfrowej (4 os.),
- PARP (8 os.).

Łącznie w warsztacie udział wzięło 15 osób.

Na spotkaniu omówiono:

- działania podejmowane albo planowane w najbliższych miesiącach przez administrację publiczną w obszarze cyberbezpieczeństwa,
- potrzeby firm,
- propozycje potencjalnych interesariuszy programu.

W dniu 9.10.2025 r. odbyło się spotkanie zespołu projektowego, na którym dodefiniowano grupę docelową, omówiono ograniczenia projektowe, pracowano nad teorią zmiany oraz wypracowano wyzwanie na warsztat kreatywny.

## 5.4. Prototypowanie

W ramach prac podczas warsztatu kreatywnego (20.10.2025) uczestnicy wypracowywali rozwiązania, będące odpowiedzią na wyzwanie projektowe:

- Jak moglibyśmy pomóc MŚP (z branży medycznej), w przejściu od działań ad hoc do kompleksowego zarządzania cyberbezpieczeństwem, tak aby zbudowały trwałą odporność na zagrożenia i osiągnęły gotowość do certyfikacji według norm NASK?

W warsztacie wzięło udział 14 osób, w tym:

- 2 przedstawicielki Ministerstwa Rozwoju i Technologii,
- 1 przedstawiciel Europejskich Hubów Innowacji Cyfrowych (European Digital Innovation Hub, EDIH),
- 5 firm specjalizujących się w obszarze cyberbezpieczeństwa.
- 6 przedstawicieli i przedstawicielek PARP.

Na spotkaniu powarsztatowym (21.10.2025 r.) zespół projektowy nadał ostateczną formę prototypowi.

## 5.5. Testowanie I

Pierwsza iteracja testów przeprowadzona została podczas warsztatu 30.10.2025.

Testy były realizowane w 2 turach: respondenci zapoznawani byli z prototypem - prezentacją graficzną przedstawiającą ścieżkę programu.

Głównym celem etapu była weryfikacja zdefiniowanych celów programu, odbiorców wsparcia oraz zakresu usług oferowanych w jego ramach. Jednocześnie uzupełniano też informacje dot. specyficznych potrzeb oraz wyzwań stojących przed użytkowniczkami/ami oraz postrzeganych korzyści z uczestnictwa w programie.

W testach wzięło udział 12 osób w tym:

- 2 przedstawicieli NASK,
- 2 przedstawicieli EDIH,
- 8 przedstawicielek i przedstawicieli przedsiębiorstw:
- 6 dostawców rozwiązań w obszarze cyberbezpieczeństwa

- 2 firmy z branży medycznej.

Wnioski z pierwszej rundy testów zostały zebrane oraz przeanalizowane przez zespół projektowy na spotkaniu 3.11.2025.

Najważniejsze wnioski z pierwszej rundy testowania

- pomysł ograniczenia wsparcia do określonej branży został odebrany pozytywnie, uczestnicy wielokrotnie wskazywali równocześnie, że definicja branży medycznej jest zbyt szeroka i niejednoznaczna,
- zwrócono uwagę, że wskazany cel: przygotowanie do procesu certyfikacji nie znajduje odzwierciedlenia w proponowanych działaniach;
- przedstawiony program oceniony został jako zbieżny z działaniami realizowanymi przez EDIH, jednak kładący większy nacisk na wdrożenie;
- element diagnozy/audytu oceniono jako bardzo istotny. Wskazywano także, że diagnoza i audyt to dwa zupełnie inne działania i lepszym rozwiązaniem byłoby w ramach programu zdecydowanie się na jedną z form, przy czym preferowaną była diagnoza;
- wskazano, że należy doprecyzować, co oznacza konieczność utrzymania systemów, aby beneficjenci byli świadomi koniecznych do poniesienia kosztów i zapewnienia odpowiednich zasobów;
- najwięcej dyskusji w zakresie usługi wzbudziła kwestia ubezpieczeń. Ubezpieczenie postrzegano nie jako kluczową wartość programu, ale element, który dodaje mu atrakcyjności, a jednocześnie uznano ją za konkretną, „namacalną" wartość programu i istotny motywator dla przedsiębiorców;
- jako wyróżnik wsparcia wskazywano możliwość pokrycia kosztów licencji i infrastruktury;
- w opinii osób uczestniczących w spotkaniu produkty programu powinny obejmować: zmapowane zasoby, dokumentację systemu zarządzania (z perspektywą użytkownika końcowego), procedury codziennego użytkowania i onboardingu, komponent *security-as-a-service* w fazie wdrożenia i utrzymania;
- podkreślono, że większość firm medycznych nie posiada administratora systemów IT, korzysta z outsourcingu.

## 5.4. Prototypowanie II

W oparciu o wnioski z testowania, poprawiono prototyp podczas spotkania zespołu projektowego, które miało miejsce 3.11.2025.

Kluczowe zmiany w prototypie wypracowane na podstawie wyników pierwszej iteracji testów:

- podjęto decyzję o konieczności zawężenia grupy docelowej: jako jedno z kluczowych kryteriów wejścia do programu wskazano konieczność gromadzenia przez podmiot danych medycznych;
- w drugiej iteracji testów testowana będzie opcja 20% wkładu własnego;
- cel przygotowania firmy do certyfikacji w wyniku udziału w programie został usunięty;
- zaproponowano, aby audyty były realizowane przez EDIH-y, które wyrażą chęć udziału w programie;
- EDIH-y będą mogły stosować swoją metodykę, sprecyzowane zostanie jednak jakie produkty mają dostarczyć;
- działania szkoleniowe dedykowane będą administratorom, a nie lekarzom/pracownikom administracji;
- uznano, że ubezpieczenie może być istotnym elementem oferty, dlatego w drugiej turze testów zdecydowano się pogłębić temat, aby zdobyć informacje, które pozwolą doprecyzować w jakiej formie wsparcie to może być realizowane.

## 5.7. Testowanie II

Druga iteracja testów prowadzona była w okresie 12.11. - 02.12.2025 r. Plan testowania i scenariusze wywiadów testujących opracowane zostały przez przedstawicieli Sekcji Projektowania Pilotaży Departamentu Analiz i Strategii PARP.

Celem testów była weryfikacja poprawionej koncepcji instrumentu wsparcia.

Testowanie prowadzone było w formie zdalnych, indywidualnych wywiadów pogłębionych lub diad, w trakcie których respondenci zapoznawani byli z prototypem - prezentacją graficzną przedstawiającą schemat programu.

Testowanie koncentrowało się na weryfikacji poprawionych w trakcie warsztatu elementach prototypu.

W testach wzięło udział 10 podmiotów, w tym:

- 3 EDIH-y,
- 2 dostawców usług cyberbezpieczeństwa,
- 1 dostawca rozwiązań w zakresie zarządzania dokumentami i procesami,
- 4 podmioty świadczące usługi ochrony zdrowia.

Wyniki testowania zebrano i przeanalizowano podczas spotkania Zespołu projektowego w dniu 4.12.2025.

## 5.8. Prototyp III: spis najważniejszych zmian po testach

Zespół projektowy podjął m.in. następujące decyzje dotyczące projektowanego programu na tym etapie:

- EDIH, który w programie przygotowuje diagnozę, nie może być wykonawcą wdrożenia (ani lider EDIH, ani żaden z partnerów);
- w raporcie diagnostycznym powinny znaleźć się informacje o warunkach, jakie powinien spełniać wykonawca wdrożenia, wskazywać typy/funkcje oprogramowania, ale nie powinno się wskazywać konkretnych dostawców;
- testy penetracyjne kwalifikowane będą jako opcjonalna usługa doradcza, nie jako element obowiązkowy;
- jako kryterium wejścia do programu dodano konieczność posiadanie zasobów/gotowość do ich zapewnienia (osoby pełniącej rolę administratora danych) do wdrożenia i utrzymania systemu.

## 5.9. Planowanie wdrożenia

Warsztat wdrożeniowy odbył się 10.12.2025 roku. W warsztacie, poza członkami/-iniami zespołu projektowego, uczestniczył zastępca dyrektora Departamentu Projektów Proinnowacyjnych.

Kluczowe prace zrealizowane podczas warsztatu:

- odtworzono ścieżkę użytkownika i działania w zakresie *frontstage* i *backstage;*
- zidentyfikowano ryzyka na każdym jej etapie;
- opracowano podstawowe założenia odnośnie budżetu programu;
- wypracowano założenia dot. wskaźników produktu i rezultatu;

- przedyskutowano i rozstrzygnięto kwestie dotyczące grupy docelowej programu (posiadanie przez MSP danych medycznych poza rozwiązaniami chmurowymi) oraz wyłączenia z kosztów kwalifikowanych środków trwałych (zakup podstawowego sprzętu IT jest standardowym kosztem prowadzenia działalności i nie powinien być finansowany ze środków publicznych);
- zebrano i podsumowano kwestie, które wymagają dopracowania w trakcie dalszych prac nad pilotażem (m.in. kryterium rankingujące projekty, system informatyczny niezbędny do obsługi beneficjentów).