Załącznik nr 3

Ocena skutków regulacji KSC 2.0 dla NASK-PIB w latach 2025–2034

Estymacja kosztów

1. Cel dokumentu

Niniejszy dokument ma na celu zaprezentowanie estymacji dodatkowych kosztów, jakie będzie ponosił NASK-PIB w latach 2025 – 2034 w związku z realizacją ustawowych obowiązków wynikających z projektu nowelizacji uKSC, w tym przepisów implementujących NIS2.

Na potrzeby estymacji kosztów przyjęto, że dotychczasowe i nowe obowiązki ustawowe będą podlegać ciągłemu procesowi rozwoju i doskonalenia. Zważywszy na ciągle rosnącą liczbę form cyberzagrożeń oraz faktycznych ataków, zapewnienie rozwoju i doskonalenia ww. procesów jest kluczowe dla istotnej poprawy cyberbezpieczeństwa w Polsce.

Estymacja kosztów przygotowana została w podziale na:

1. Zadania CSIRT NASK finansowane z dotacji podmiotowej (KSC)
2. Zadania w ramach projektu S46, finansowane z dotacji celowej

2. Założenia ogólne

Podczas szacowania kosztów przyjęto następujące założenia:

1. Rok bazowy – 2025.
2. Perspektywa kalkulacji – lata 2025 – 2034.
3. Wysokość kosztów ogólnych od sumy kosztów bezpośrednich – 25%.
4. Średni narzut na inflację w ujęciu rocznym – 6%.
5. Średni narzut na rozwój (współczynnik rozwoju) w ujęciu rocznym – 10%.

3. Estymacja kosztów dla KSC

3.1. Założenia

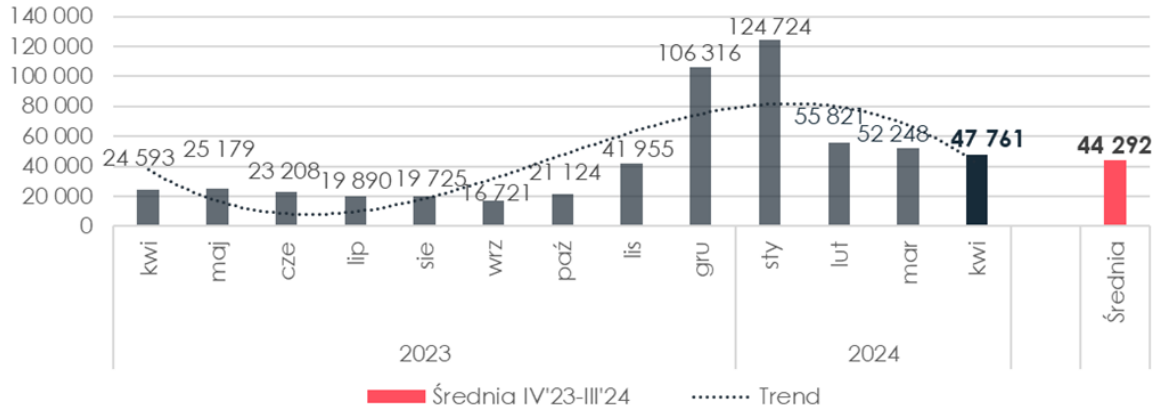
Podczas szacowania kosztów przyjęto następujące założenia:

1. Rok bazowy – 2025.
2. Perspektywa kalkulacji – lata 2025 – 2034.
3. Wysokość kosztów ogólnych od sumy kosztów bezpośrednich – 25%.
4. Średni narzut na inflację w ujęciu rocznym – 6%.
5. Średni narzut na rozwój (współczynnik rozwoju) w ujęciu rocznym – 10%.

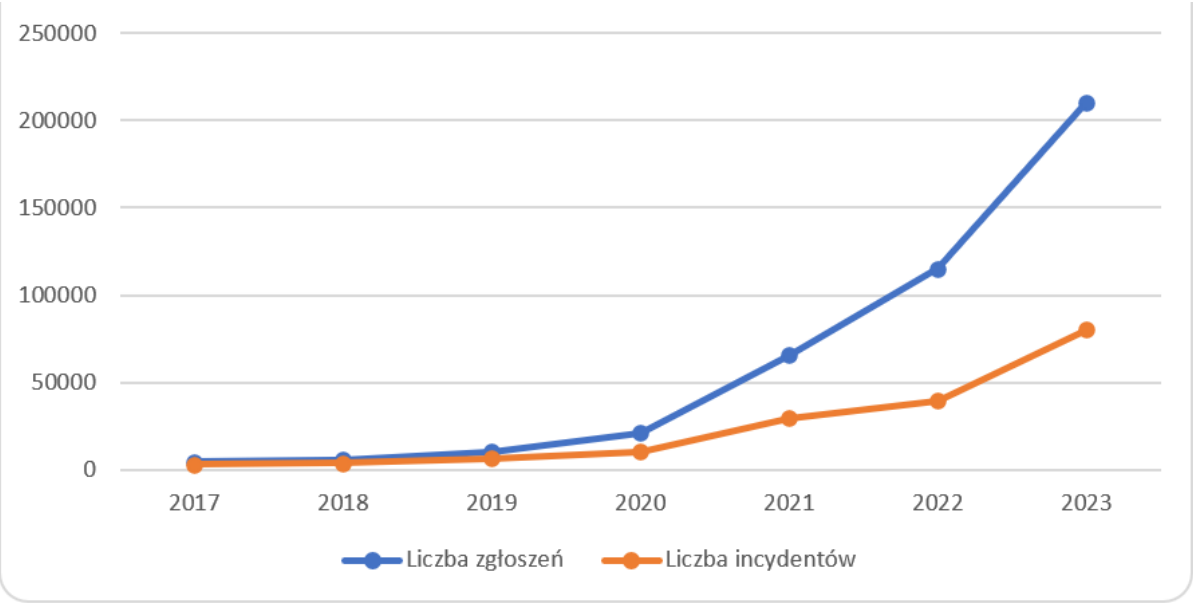
3.2. Opis zadań

W ramach szacowania skutków regulacji na funkcjonowanie CSIRT NASK poza nowymi zadaniami trzeba również wziąć pod uwagę szerszy zakres sektorów gospodarki, które będą objęte krajowym systemem cyberbezpieczeństwa. Zgodnie z aktualnie obowiązująca ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222), zwaną dalej „KSC", przybliżona liczba operatorów usług kluczowych i dostawców usług cyfrowych wynosi 400, natomiast przybliżona liczba podmiotów kluczowych i ważnych – 38 000. W projekcie nowelizacji KSC liczba sektorów wzrasta z 7 do 11, co bezpośrednio wpłynie na zwiększenie liczby podmiotów kluczowych i ważnych oraz liczbę operatorów usług kluczowych i dostawców usług cyfrowych.

Rosnące zapotrzebowanie na dodatkowe etaty do realizacji dotychczasowych zadań obrazują też poniższe wykresy liczby incydentów oraz zgłoszeń. W skali rocznej można zaobserwować podwojenie liczby zgłoszeń incydentów (rys. 1), a od wejścia KSC w 2018 r. widać wzrost liczby zgłoszeń i incydentów odpowiednio: 44 krotnie i 25 krotnie (rys. 2). Jest to istotne również w kontekście obowiązku wypełniania przez CSIRT poziomu krajowego obowiązków CSIRTów sektorowych przez okres przejściowy trwający do 18 miesięcy od wejścia w życie projektowanej ustawy.



rys. 1. Liczba zgłoszeń i incydentów obsłużonych przez CERT Polska w okresie IV 2023 – IV 2024 z podziałem na miesiące.



rys. 2. Liczba zgłoszeń i incydentów obsłużonych przez CERT Polska w latach 2017–2023.

Kalkulacja dotyczy realizacji zadań wynikających z projektu nowelizacji KSC, które nie są ujęte w aktualnie obowiązującej ustawie i obejmuje realizację następujących zadań:

ID	Zakres zadania	Podstawa prawna
N.1	Zapewnienie wsparcia w obsłudze incydentów na zlecenie Pełnomocnika	art. 26 ust. 2 a nowelizacji
N.2	a) współpraca z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i ważnych oraz, w odpowiednich przypadkach, wymieniają z nimi stosowne informacje, b) współpraca z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich, w ramach której mogą wymieniać informacje w tym dane osobowe zgodnie z unijnymi przepisami o ochronie danych, c) udział we wdrażaniu bezpiecznych narzędzi wymiany informacji zgodnie z podmiotami kluczowymi i ważnymi oraz innymi odpowiednimi zainteresowanymi stronami,	art. 26 ust. 3 pkt 18–22 nowelizacji

ID	Zakres zadania	Podstawa prawna
	d) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności poprzez: – wykonywanie oceny bezpieczeństwa, – identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach, e) promowanie przyjmowania i stosowanie wspólnych lub znormalizowanych praktyk, systemów klasyfikacji i systematyki związanych z: – procedurami obsługi incydentu, – zarządzaniem kryzysowym, – ujawnianiem podatności.	
N.3	udział w procesie wzajemnej oceny państw członkowskich, o którym mowa w art. 19 dyrektywy NIS 2, jako ekspertów ds. cyberbezpieczeństwa (tu mogą być koszty delegacji, analiz, sprawozdań, itp.)	art. 26 ust. 12 nowelizacji
N.4	pełnienie funkcji koordynatora na potrzeby skoordynowanego ujawniania podatności	art. 26a ust. 1 nowelizacji
N.5	współpraca z Prezesem Urzędu Lotnictwa Cywilnego, Prezesem Urzędu Komunikacji Elektronicznej oraz Komisją Nadzoru Finansowego	art. 34 ust. 3 nowelizacji
N.6	dokonywanie ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa	Rozdział 6 – Ocena bezpieczeństwa – art. 36a–36d nowelizacji
N.7	wykonywanie ocen bezpieczeństwa w stosunku do podmiotów kluczowych na podstawie szacowania ryzyka na zlecenie organu właściwego do spraw cyberbezpieczeństwa	art. 53 ust. 2 pkt 3 nowelizacji
N.8	pozyskiwanie oraz analizowanie danych na potrzeby zasilania usługi online polegającej na możliwości sprawdzenia przez użytkownika czy jego dane zostały upublicznione w sieci internet w sposób nieuprawniony.	art. 26c
N.9	na wniosek przewodniczącego kolegium przeprowadzanie analiz dotyczących wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych	art. 65a nowelizacji

Tabela poniżej przedstawia opis/zakres działań w odniesieniu do zapisów z projektu nowelizacji. Projekt nowelizacji, oprócz nowych zadań, rozszerza również zakres zadań już realizowanych, stąd niektóre obowiązki wynikające z nowelizacji zostały w całości lub częściowo przypisane do tych zadań (zadania 1 do 10). Pozostałe zadania (od 11do 13) są zadaniami nowymi.

Lp.	Zadanie	ID zad. z nowelizacji	Opis zadania/Uwagi	Ilość planowanych etatów
1.	Prowadzenie zespołu	N1, N2, N.8,	Zadanie obejmuje ogół czynności polegających na przyjmowaniu, analizie, klasyfikacji i	

Lp.	Zadanie	ID zad. z nowelizacji	Opis zadania/Uwagi	Ilość planowanych etatów
	reagowania na incydenty	N.9	reagowaniu na zgłoszone incydenty. Udzielanie pomocy w obsłudze incydentów na zlecenie Pełnomocnika, Rządu do Spraw Cyberbezpieczeństwa, współpraca z krajowymi zespołami reagowania na incydenty oraz większa liczba zgłoszeń od podmiotów zobowiązanych (wynikająca z rozszerzenia zakresu podmiotów zobowiązanych do wykonywania obowiązków w ramach uKSC) zwiększy nakład pracy. Wynika z tego konieczność zwiększenia liczby etatów w zespołach zajmujących się obsługą zgłoszeń w ramach CSIRT NASK oraz potrzeba automatyzacji możliwych elementów procesu.	23 etaty
2.	Monitorowanie zagrożeń cyberbezpieczeństwa	N.1, N.8, N.9	Działanie będzie realizowane w znacznie większym stopniu niż obecnie. Celem bardziej efektywnego wykorzystania gromadzonej wiedzy i danych konieczne jest zadbanie o ich właściwą analizę i jakość danych. Zwiększenie zasobów na to zadanie pozwoli na lepsze wykorzystanie wskaźników zbieranych przez podmioty KSC (dane systemów CERT Polska, IoC itp.). Zagregowane dane mogą być istotne podczas nowego zadania „dokonywanie ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa". Dodatkowe zadania pojawią się w związku z rosnącą liczbą podmiotów kluczowych i ważnych, obowiązkiem zapewnienia wsparcia w obsłudze incydentów na zlecenie Pełnomocnika, Rządu do Spraw Cyberbezpieczeństwa np. monitorowanie zagrożeń cyberbezpieczeństwa dla udzielenia wsparcia osobom będącym w zasięgu zainteresowań aktywnie działających grup APT.	21 etatów
3.	Przekazywanie inf. dot. zagrożeń podmiotom KSC	N.2	W związku ze zwiększającą się liczbą podmiotów kluczowych i ważnych większe będzie zapotrzebowanie na etaty osób z kompetencjami technicznymi, odpowiedzialnych za ostrzeganie użytkowników o zagrożeniach. Dodatkowo zacieśniona współpraca z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i ważnych będzie powodować zwiększenie częstotliwości przekazywanie informacji dotyczących zagrożeń podmiotom KSC.	2 etaty
4.	Wydawanie komunikatów o zidentyfikowanych zagrożeniach	N.1 N.2, N.8, N.9	Komunikacja zewnętrzna dotycząca zagrożeń odbywa się wieloma kanałami. W bieżącej pracy operacyjnej najskuteczniejszym kanałem komunikacji są media społecznościowe. Stosowne komunikaty opracowywane są przez ekspertów Zespołu Analiz Bieżących Zagrożeń oraz Zespół Obsługi Podatności i Poszukiwania Zagrożeń we współpracy ze specjalistami odpowiedzialnymi za popularyzację (recenzja pod kątem językowym i poziomem „trudności" przekazu dla wybranej grupy odbiorców). Konieczność wydawania komunikatów może wynikać ze zlecenia Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa lub współpracy z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i ważnych.	5 etatów
5.	Współpraca z OW, SZC, CSIRTs, OUK, DUC i PP oraz innymi z KSC	N.2, N.5	Poszerza się katalog podmiotów, które będą uznane ze kluczowe albo ważne, więc konieczne będzie utrzymanie aktywnej współpracy z całą grupą podmiotów w celu utrzymania wysokiej świadomości i bezpieczeństwa. Dodatkowo ważne jest uwzględnienie wsparcia specjalistów merytorycznych, którzy będą mogli tworzyć ostrzeżenia, prezentacje edukacyjne czy wypełniać inne tego typu zapotrzebowanie. Taką rolę w większym niż do tej	6 etatów

Lp.	Zadanie	ID zad. z nowelizacji	Opis zadania/Uwagi	Ilość planowanych etatów
			pory stopniu będzie spełniał m.in. Program Partnerstwo dla Cyberbezpieczeństwa, który wspiera efektywną komunikację z podmiotami KSC.	
6.	Prowadzenie zaawansowanych analiz szkodliwego oprogramowania i podatności	N.1	Zaawansowana analiza oprogramowania i poszukiwanie podatności są realizowane zarówno w procesie obsługi incydentów, kiedy oczekiwana jest szybka analiza i rekomendacje, jak i w trybie projektowym, kiedy urządzenia lub oprogramowanie poddawane są kompleksowej systematycznej analizie w celu poszukiwania podatności, które mogłyby spowodować istotne zagrożenie w przypadku użycia danego rozwiązania. Dodatkowe zadania wymagają zwiększenia ilości etatów w celu możliwości zapewnienia ich realizacji, zwłaszcza ze względu na bardzo szerokie constituency CSIRT NASK oraz rosnącą liczbę podmiotów, które będą uznane ze kluczowe albo ważne.	15 etatów
7.	Współpraca międzynarodowa	N.2, N.3	Realizacja zadania ma na celu rozwinięcie relacji międzynarodowych dla lepszej współpracy zarówno na poziomie techniczno-operacyjnym, jak i strategicznym. Efektem tych działań jest, z jednej strony, wzmocnienie istniejących kanałów wymiany informacji technicznych, a z drugiej wykorzystanie i udostępnianie materiałów budujących świadomość, tak aby dzielić się i korzystać z dorobku i doświadczeń innych państw.	5 etatów
8.	Współpraca z orangami ścigania i wymiary sprawiedliwości	N.1, N.2, N.6, N.9	Działania w ramach tego zdania mają na celu częstsze i szersze zakresowo wsparcie organów ścigania, wymiaru sprawiedliwości i służb specjalnych w realizacji ich ustawowych obowiązków. Wsparcie to udzielane jest zarówno na etapie operacyjno-rozpoznawczym, jak i procesowym. Współpraca z organami ścigania jest stałym elementem obsługi incydentów, zwłaszcza typu ransomware. Nowe obowiązki wynikające z konieczności wspierania podmiotów KSC w obsłudze incydentów czy dokonywania ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa będą wymagały również utrzymania aktywnej współpracy z organami ścigania i wymiarem sprawiedliwości.	2 etaty
9.	Testy aktywne	N.1, N.6	Realizacja zadania polega na aktywnej analizie bezpieczeństwa poszczególnych sektorów oraz dokonywanie ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa. Analizie poddawane mogą być różnego rodzaju usługi IT udostępniane przez podmioty danego sektora, począwszy od stron informacyjnych, poprzez udostępniane publicznie usługi web lub API po interfejsy urządzeń przemysłowych. Działania te przeprowadzane są w systemie projektowym, a każdy projekt kończy się raportem i, jeśli jest to uzasadnione, zestawem rekomendacji dla danego sektora/podsektora. Zadanie należy do kluczowych zarówno w kontekście zapewnienia wsparcia w obsłudze incydentów na zlecenie Pełnomocnika, jak i dokonywania ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa.	12 etatów
10.	Utrzymanie systemów i ciągłości funkcjonowania	N.2, N.6	Realizacja zadania ma na celu wzmocnienie procesu utrzymania i rozwoju systemów CSIRT używanych przez wszystkie linie wsparcia, w tym wzmocnienie zarządzania procesem ciągłości działania (BCM).Wymaga to zaangażowania nowych zasobów.	4 etaty

Lp.	Zadanie	ID zad. z nowelizacji	Opis zadania/Uwagi	Ilość planowanych etatów
11.	Identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach	N.1, N.2, N.6, N.9	Zadanie nowe Zadanie obejmuje działania polegające na wykonywaniu ocen bezpieczeństwa w stosunku do podmiotów kluczowych, dokonywanie ocen bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa oraz prowadzenie i zarządzenie, procesem komunikacji z podmiotami. Ze względu na konieczność cyklicznego skanowania kilkudziesięciu tysięcy podmiotów w ramach constituency CSIRT NASK konieczne jest zwiększenie zasobów osobowych dedykowanych do rozwoju i obsługi stosownych narzędzi oraz procesu komunikacji.	9 etatów
12.	Pełnienie funkcji koordynatora na potrzeby skoordynowanego ujawniania podatności	N.4	Zadanie nowe Zadanie polegające na pełnieniu funkcji koordynatora na potrzeby skoordynowanego ujawniania podatności. W ramach wypełnienia tego obowiązku, konieczne będzie techniczne weryfikowanie zgłaszanych podatności oraz komunikacja i ewentualne mediacje między zgłaszającym a podmiotem (producentem), którego produktu dotyczy podatność.. Wraz z rosnącą skalą zgłoszeń konieczne będzie rozwijanie narzędzi, które usprawnią proces obsługi zgłoszeń podatności oraz rozbudowa i podniesienie poziomu roli takiej jak CNA.	8 etatów
13.	Wykonywanie ocen bezpieczeństwa w stosunku do podmiotów kluczowych na podstawie szacowania ryzyka na zlecenie organu właściwego do spraw cyberbezpieczeństwa	N.7	Zadanie nowe Zadanie polegające na wykonywaniu ocen bezpieczeństwa w stosunku do podmiotów kluczowych na podstawie szacowania ryzyka na zlecenie organu właściwego do spraw cyberbezpieczeństwa. Zależnie od sytuacji może to m.in. polegać na technicznym badaniu i ocenie infrastruktury podmiotu jak również na ocenie istniejących procedur reagowania na incydenty.	2 etaty

3.3. Analityka kosztowa

Estymację kosztów na lata 2025–2034 w podziale na poszczególne rodzaje kosztów przedstawia tabela poniżej. W pozycji *Koszty inne* uwzględniono inne wydatki niezbędne do realizacji zadań nie ujęte w pozostałych pozycjach w szczególności koszty organizacji wydarzeń.

Rodzaj kosztu	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034
Koszty osobowe	27 907 200,00	32 372 352,00	37 551 928,32	43 560 236,85	50 529 874,75	58 614 654,71	67 992 999,46	78 871 879,37	91 491 380,07	106 130 000,89
Delegacje	984 000,00	1 141 440,00	1 324 070,40	1 535 921,66	1 781 669,13	2 066 736,19	2 397 413,98	2 781 000,22	3 225 960,25	3 742 113,89

Usługi, koszty pośrednie, materiały i wydatki nisko cenne	492 000,00	570 720,00	662 035,20	767 960,83	890 834,57	1 033 368,10	1 198 706,99	1 390 500,11	1 612 980,13	1 871 056,95
Szkolenia personelu	9 802 050,00	11 370 378,00	13 189 638,48	15 299 980,64	17 747 977,54	20 587 653,94	23 881 678,58	27 702 747,15	32 135 186,69	37 276 816,56
RAZEM	**39 185 250,00**	**45 454 890,00**	**52 727 672,40**	**61 164 099,98**	**70 950 355,98**	**82 302 412,94**	**95 470 799,01**	**110 746 126,85**	**128 465 507,15**	**149 019 988,29**

Do celów wyliczenia kosztów osobowych przyjęto wartość średniej pensji na poziomie 20 400 złotych miesięcznie brutto przy szacowanej ilości etatów na poziomie 114 dla roku bazowego (2025). Należy zaznaczyć, że dotacja podmiotowa nie pokrywa kosztów inwestycyjnych powyżej 10 tys. zł kosztu jednostkowego. Oznacza to, że inwestycje infrastrukturalne, a także wydatki na systemy czy narzędzia, przekraczające 10 tys. zł kosztu jednostkowego, wymagają finansowania z projektów celowych lub dofinansowania unijnego.

3.4. Realizacja zadań nadzorczych na zlecenie Ministra właściwego ds. informatyzacji

Zgodnie z art. 41a ust. 5 nowelizacji minister właściwy do spraw informatyzacji może powierzyć realizację zadań nadzorczych nad podmiotami kluczowymi w sektorze administracji publicznej CSIRT NASK, ale środki na te czynności muszą się znaleźć w dotacji podmiotowej.

Z założeń zawartych w dokumencie z OSR nowelizacji KSC liczba podmiotów kluczowych i podmiotów ważnych z sektora administracji publicznej to 27905. Założenia sugerują prowadzenie kontroli w około 10% podmiotów rocznie, każda kontrola powinna być prowadzona przez zespół 3 osób, które mogą przeprowadzić 6 kontrole rocznie. Wynika z tego, że do wypełnienia założenia kontroli w 2790 podmiotach konieczne byłoby zatrudnienie 465 zespołów po trzy osoby, co przekłada się na 1395 etatów. Jednocześnie w założeniach wpisano, że maksymalna liczba etatów nadzorujących sektor to 40.

W związku z powyższym przyjęto założenie, że NASK-PIB zapewni 40 etatów, w ramach których będzie realizował powierzone zadania nadzorcze. Tabela poniżej przedstawia estymacje kosztów dla 40 etatów. Na potrzeby wyliczenia kosztów dla roku bazowego (2025) przyjęto następujące założenia:

1. Stawka miesięcznego wynagrodzenia – 20 400 zł.
2. Dzienna stawka delegacyjna – 500 zł.
3. Liczba dni delegacyjnych w skali miesiąca dla jednego etatu – 15.
4. Roczna kwota przeznaczona na szkolenia w ramach jednego etatu – 3 600 zł.
5. Inflacja rok do roku – 6%.

Rodzaj kosztu	Rok									
	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034
Koszty osobowe	9 792 000,00	10 379 520,00	11 002 291,20	11 662 428,67	12 362 174,39	13 103 904,86	13 890 139,15	14 723 547,50	15 606 960,35	16 543 377,97
Delegacje	3 600 000,00	3 816 000,00	4 044 960,00	4 287 657,60	4 544 917,06	4 817 612,08	5 106 668,80	5 413 068,93	5 737 853,07	6 082 124,25
Szkolenia	144 000,00	167 040,00	193 766,40	224 769,02	260 732,07	302 449,20	350 841,07	406 975,64	472 091,74	547 626,42
Razem	**13 536 000,00**	**14 362 560,00**	**15 241 017,60**	**16 174 855,30**	**17 167 823,52**	**18 223 966,13**	**19 347 649,02**	**20 543 592,07**	**21 816 905,16**	**23 173 128,64**

Koszty projektu Bezpiecznedane.gov.pl

W ramach dotacji podmiotowej przewiduje się sfinansowanie projektu https://bezpiecznedane.gov.pl/.

Rodzaj kosztu	Od 2025
Bezpieczne dane – Wynagrodzenia osobowe	1 696 962
Bezpieczne dane – Usługi obce	129 900
Bezpieczne dane – Licencje/oprogramowanie	104 000
Bezpieczne dane – Razem koszty	1 930 862
Bezpieczne dane - Koszty pośrednie	482 716
SUMA	4 344 440,09 zł

4. Estymacja dla projektu S46

4.1. Utrzymanie i rozwój systemu S46

4.1.1. Wprowadzenie

System S46, dalej określany również jako „S46", jest systemem teleinformatycznym, o którym mowa w art. 46 KSC. System został uruchomiony zgodnie ze wskazanym terminem ustawowym w dniu 01.01.2021. Realizacja S64 bazowała na dorobku projektów NPC i NPCNet, które były dofinansowane przez NCBiR. Dostosowanie produktów ww. projektów, do przepisów KSC, zostało zrealizowane przez NASK-PIB w wyniku realizacji zadania publicznego „Rozwój systemu teleinformatycznego S46".

W kolejnych latach NASK-PIB realizował zadania publiczne, których celem było utrzymanie i rozwój systemu teleinformatycznego S46. W obszarze utrzymania finansowane były elementy takie jak obsługa administratorska, linie wsparcia, korekty błędów oraz niezbędne do działania systemu zakupy. Obszar rozwoju obejmował ulepszanie funkcjonalności systemu, niezbędną rozbudowę infrastruktury oraz podłączanie nowych użytkowników. Zwiększenie skali podłączeń instytucji do systemu S46 zostało również osiągnięte przy wykorzystaniu środków z Unii Europejskiej finansowanego z inicjatywy REACT-EU. Środki pozyskane z Unii Europejskiej pozwoliły również na zwiększenie odporności S46 na katastrofy.

Ze względu na wzrastającą rolę systemu S46, wynikającą w nowelizacji ustawy o KSC, konieczne jest zapewnienie dalszego finansowania zarówno w obszarze utrzymania, jak i rozwoju systemu S46.

4.1.2. Streszczenie managerskie

Aktualnie przyjęta Ustawa o krajowym systemie cyberbezpieczeństwa (Ustawa o KSC), przewiduje w ramach OSR kwoty na utrzymanie i rozwój systemu o którym jest mowa w art. 46 KSC.

Analiza wykazała, że do rozwoju i utrzymania systemu jest konieczne przeznaczenie większych środków od tych, które zostały uwzględnione w ramach OSR dla KSC.

Poniższa tabela ilustruje potrzeby w zakresie zwiększania kwot na utrzymanie i rozwój systemu S46.

rok	Bieżące	majątkowe	Suma	OSR2018	zwiększenie kosztów
2025	22 624 317,00 zł	12 214 576,50 zł	34 838 893,50 zł	9 500 000,00 zł	**25 338 893,50 zł**
2026	25 660 615,68 zł	2 344 995,00 zł	28 005 610,68 zł	9 500 000,00 zł	**18 505 610,68 zł**
2027	22 436 552,14 zł	6 571 680,90 zł	29 008 233,04 zł	9 500 000,00 zł	**19 508 233,04 zł**
2028	30 246 145,93 zł	8 893 638,00 zł	39 139 783,93 zł	9 500 000,00 zł	**29 639 783,93 zł**
2029	32 063 937,62 zł	18 450 000,00 zł	50 513 937,62 zł	9 500 000,00 zł	**41 013 937,62 zł**
2030	37 095 769,70 zł	27 749 230,50 zł	64 845 000,20 zł	9 500 000,00 zł	**55 345 000,20 zł**
2031	44 076 677,03 zł	1 815 480,00 zł	45 892 157,03 zł		**45 892 157,03 zł**
2032	49 566 936,42 zł	7 876 932,30 zł	57 443 868,72 zł		**57 443 868,72 zł**
2033	59 889 994,58 zł	12 874 410,00 zł	72 764 404,58 zł		**72 764 404,58 zł**
2034	68 007 369,59 zł	27 675 000,00 zł	95 682 369,59 zł		**95 682 369,59 zł**

Tabela 1 Potrzeby w zakresie finansowania utrzymania i rozwoju S46

Zwiększenie nakładów na utrzymanie i rozwój S46 jest związane z czynnikami wymienionymi poniżej:

1. W szacunkach do OSR KSC 2018, uwzględniono koszty wynikające z sukcesywnego podłączania podmiotów krajowego systemu cyberbezpieczeństwa. Założono dynamikę podłączeń na poziomie około stu uczestników rocznie. Nowelizacja KSC w znaczący sposób zwiększa liczbę podmiotów, które będą korzystać z systemu S46, aż do poziomu ponad 10 tysięcy. Zwiększona o dwa rzędy wielkości liczba uczestników przekłada się na koszty obsługi systemu, zarówno jeśli chodzi o wsparcie oferowane przez poszczególne linie wsparcia, jak również w zakresie wsparcia merytorycznego. Brak zwiększenia środków wygeneruje problemy z wykorzystaniem systemu, który w projekcie nowelizacji jest systemem obowiązkowym.
2. Projektowana nowelizacja przewiduje uruchomienie rejestru podmiotów krajowego systemu cyberbezpieczeństwa zapewniającego podmiotom mechanizm samorejestracji za pośrednictwem sieci Internet i mechanizmów węzła krajowego. Uruchomienie bezpiecznego mechanizmu samorejestracji, oraz wsparcie podmiotów podłączanych do S46, wymaga nakładów w stosunku do planowanych w OSR 2018
3. W zestawie założeń przyjętych w OSR KSC 2018 założono dostęp do S46 dla kilkuset podmiotów poprzez sieć wydzieloną. Powodowało to konieczność finansowania urządzenia końcowego dedykowanego dla danego partnera. Takie podejście nie jest możliwe do dalszego stosowania przy konieczności obsługi kilkudzisi ęciu tysięcy podmiotów. W związku z tym została podjęta decyzja o uruchomieniu dostępu do S46 w trybie SaaS. Jedynie w przypadku szczególnie istotnych podmiotów (CSiRTy, OW itp.) oraz już podłączonych jednostek, pozostawiony zostanie dostęp przez sieć wydzieloną. Dzięki takiemu podejściu, nie będzie konieczne zapewnienie dodatkowych urządzeń końcowych użytkownikom S46. Konieczne jest natomiast utrzymanie i zapewnienie wsparcia dla aktualnie użytkowanych końcówek.
4. W trakcie realizacji zadań związanych z utrzymaniem, okazało się konieczne powołanie zespołu analitycznego zdolnego do zauważania zależności, analizowania spójności modeli i ryzyk itp. W założeniach do KSC 2018 funkcje takie nie były znane i przewidywane, a zatem nie mogły być też wycenione. Należy wziąć pod uwagę również zatrudnienie specjalistów specjalizujących się w nowych technologiach, takich jak AI. Podniesienie nakładów umożliwi organizację zespołu analitycznego, który będzie mógł realizować analizy wspomagając działanie wszystkich CSRIT'ów.
5. Doświadczenia dotyczące utrzymania i rozwoju systemu wskazują, że konieczne jest zapewnienie ciągłego doskonalenia funkcjonalności S46. Planowany wzrost liczby użytkowników powoduje, że konieczne staje się utrzymanie stałego zespołu deweloperskiego, dedykowanego do ciągłego doskonalenia systemu, oraz wprowadzania poprawek. Zwiększenie liczby personelu dedykowanego do rozwoju systemu S46, umożliwi obsługę zwiększającej się skali i poziomu złożoności systemu. Brak dodatkowych nakładów w obszarze zespołów rozwojowych mógłby spowodować drastyczne wydłużenie okresu wprowadzania poprawek i dostosowywania systemu do wymagań użytkowników.
6. Doświadczenia z eksploatacji systemu S46 wskazują, że należy przewidzieć intensywny rozwój w zakresie technologii do analizy danych. Przewidując zapotrzebowanie w tym zakresie, zaplanowano w okresie 10-cio letnim wykorzystanie stosownych narzędzi, w tym narzędzi opartych o sztuczną inteligencję. Brak inwestycji w narzędzia do analizy danych może wydłużyć czas reakcji na zagrożenia w obszarze cyberbezpieczeństwa.

4.1.3. Założenia

Podczas szacowania kosztów przyjęto następujące założenia, które adresują zagadnienia opisane w ramach streszczenia managerskiego:

1. Perspektywa kalkulacji – lata 2025–2034.
2. Wysokość kosztów ogólnych od sumy kosztów bezpośrednich – 20% (z wyłączeniem usług obcych).

3. Narzut na inflację w ujęciu rocznym – 6%.
4. Współczynnik rozwoju – 10%.
5. Koszty zakupów liczono z uwzględnieniem 23% VAT.
6. Nie przewiduje się zakupu dedykowanych końcówek dla systemu S46. Uczestnicy mogą korzystać z już zakupionych urządzeń będących w dyspozycji Operatora S46, lub mogą zakupić urządzenia we własnym zakresie.
7. Koszty transmisji już podłączonych uczestników, za pomocą dedykowanych urządzeń końcowych są refundowane przez skarb państwa.

4.1.4. Metodyka kalkulacji

Podczas szacowania kosztów przyjęto założenia przedstawione w rozdziale 1.3. Szacowanie przeprowadzono osobno w rozbiciu na:

1. Koszty osobowe.
2. Koszty inwestycji.

Wyniki kalkulacji przedstawiono w podziale na lata i następujące kategorie kosztowe:

1. Sprzęt.
2. Materiały.
3. Usługi obce.
4. Wynagrodzenia.
5. Delegacje.
6. Koszty pośrednie.

Koszty osobowe

Koszty oszacowano w głównych obszarach: utrzymania i rozwoju.

W obszarze **utrzymania** rozróżniono działania związane z utrzymaniem na poziomie aplikacyjnym oraz działaniami na poziomie sieci i zasobów obliczeniowych. Ze względu na prognozowane zwiększenie liczby podmiotów korzystających z systemu, przewiduje się, że monitorowanie, reagowanie na awarie oraz rozwiązywanie zgłoszeń użytkowników będzie wymagać zwiększonego wysiłku. Ze względu na czas życia systemu konieczne będzie również zaangażowanie zespołów w zadania związane z modernizacją systemu.

W pierwszych latach, od wejścia w życie nowelizacji KSC szacuje się zwiększone obciążenie związane z przyjmowaniem użytkowników do systemu, oraz związanych ze wsparciem w zakresie korzystania systemu ale przede wszystkim w zakresie operacyjnym i szkoleń.

W obszarze **rozwoju** oszacowano potrzeby związane z utrzymaniem i rozwojem aplikacji oraz utrzymaniem i rozwojem zasobów obliczeniowych. Spodziewany jest duży nacisk na dostosowywanie systemu i rozwój nowych funkcjonalności. Działania w obszarze rozwoju będą wymagać dużego zaangażowania zespołów deweloperskich i skrócenia czasu realizacji wydań, stąd konieczność zwiększenia zasobów.

Lata	2025	2026	2027	2028	2029	2030
rozwój	**18**	**18**	**19**	**19**	**19**	**19**
utrzymanie i rozwój aplikacji	12,5	12,5	18	18	18	18
utrzymanie i rozwój sieci i zasobów obliczeniowych	5,5	5,5	1	1	1	1
utrzymanie	**48,23**	**51,45**	**33,63**	**33,63**	**29,63**	**33,63**
onboarding	12,4	12,19	3,09	3,09	3,09	3,09
szkolenia	3,21	5,67	4,54	4,54	4,54	4,54
utrzymanie i rozwój aplikacji	2	2	2	2	2	2
wspólne	1	1	1,54	1,54	1,54	1,54
analizy między CSIRT	19,62	20,59	8,46	8,46	8,46	8,46
utrzymanie i rozwój sieci i zasobów obliczeniowych	10	10	14	14	10	14
Suma końcowa	**66,23**	**69,45**	**52,63**	**52,63**	**48,63**	**52,63**

Po przyjęciu szacunkowych stawek kosztów osobowych, z uwzględnieniem narzutów koszty osobowe rozkładają się w następujący sposób:

Lata	2025	2026	2027	2028	2029	2030
	19 077 120,00 zł	**23 222 736,00 zł**	**19 707 011,71 zł**	**24 658 285,78 zł**	**28 603 612,02 zł**	**33 180 192,00 zł**
rozwój	**5 652 000,00 zł**	**6 556 320,00 zł**	**8 525 721,60 zł**	**9 889 837,06 zł**	**11 472 210,58 zł**	**13 307 765,18 zł**
utrzymanie i rozwój aplikacji	4 068 000,00 zł	4 718 880,00 zł	8 138 188,80 zł	9 440 299,01 zł	10 950 746,40 zł	12 702 866,69 zł
utrzymanie i rozwój sieci i zasobów obliczeniowych	1 584 000,00 zł	1 837 440,00 zł	387 532,80 zł	449 538,05 zł	521 464,18 zł	604 898,50 zł
utrzymanie	**13 425 120,00 zł**	**16 666 416,00 zł**	**11 181 290,11 zł**	**14 768 448,72 zł**	**17 131 401,44 zł**	**19 872 426,82 zł**
analizy między CSIRT	5 650 560,00 zł	6 878 707,20 zł	3 278 527,49 zł	3 803 091,89 zł	4 411 586,93 zł	5 117 441,28 zł
adaptacja pracowników	3 250 080,00 zł	3 717 475,20 zł	1 089 936,00 zł	1 264 325,76 zł	1 466 617,96 zł	1 701 276,86 zł
szkolenia	924 480,00 zł	1 894 233,60 zł	1 759 398,91 zł	2 040 902,74 zł	2 367 447,36 zł	2 746 239,17 zł
utrzymanie i rozwój aplikacji	720 000,00 zł	835 200,00 zł	968 832,00 zł	1 123 845,12 zł	1 303 660,22 zł	1 512 245,95 zł
utrzymanie i rozwój sieci i zasobów obliczeniowych	2 592 000,00 zł	3 006 720,00 zł	3 487 795,20 zł	5 843 994,62 zł	6 779 034,14 zł	7 863 679,87 zł
wspólne	288 000,00 zł	334 080,00 zł	596 800,51 zł	692 288,59 zł	803 054,83 zł	931 543,68 zł
Suma końcowa	**19 077 120,00 zł**	**23 222 736,00 zł**	**19 707 011,71 zł**	**24 658 285,78 zł**	**28 603 612,02 zł**	**33 180 192,00 zł**

Oraz w kolejnych latach:

Lata	2031	2032	2033	2034
o	**38 489 021,38 zł**	**44 647 266,24 zł**	**51 790 827,17 zł**	**60 077 360,68 zł**
rozwój	**15 437 007,79 zł**	**17 906 929,92 zł**	**20 772 038,30 zł**	**24 095 564,50 zł**
utrzymanie i rozwój aplikacji	14 735 325,60 zł	17 092 978,56 zł	19 827 854,78 zł	23 000 311,58 zł
utrzymanie i rozwój sieci i zasobów obliczeniowych	701 682,19 zł	813 951,36 zł	944 183,52 zł	1 095 252,91 zł
utrzymanie	**23 052 013,59 zł**	**26 740 336,32 zł**	**31 018 788,87 zł**	**35 981 796,18 zł**
analizy między CSIRT	5 936 231,34 zł	6 886 028,51 zł	7 987 792,58 zł	9 265 839,64 zł
adaptacja pracowników	1 973 481,05 zł	2 289 238,04 zł	2 655 516,07 zł	3 080 398,78 zł
szkolenia	3 185 637,15 zł	3 695 339,17 zł	4 286 593,18 zł	4 972 448,22 zł
utrzymanie i rozwój aplikacji	1 754 205,41 zł	2 034 878,40 zł	2 360 458,94 zł	2 738 132,35 zł
utrzymanie i rozwój sieci i zasobów obliczeniowych	9 121 868,06 zł	10 581 367,10 zł	12 274 385,47 zł	14 238 287,71 zł

wspólne	1 080 590,58 zł	1 253 485,09 zł	1 454 042,62 zł	1 686 689,48 zł
Suma końcowa	**38 489 021,38 zł**	**44 647 266,24 zł**	**51 790 827,17 zł**	**60 077 360,68 zł**

Należy również zauważyć, iż założono że w latach, w których przewidziano finansowanie zgodne z OSR do KSC (do roku 2030), odpowiednia cześć z oszacowanych wydatków będzie uwzględniona w kwotach aktualnie wpisanych do OSR projektu nowelizacji KSC. Zestawienie rozbicia poszczególnych kosztów na koszty majątkowe i bieżące, z uwzględnieniem poszczególnych kwot, zostały wskazane w rozdziale „koszty całościowe".

Koszty całościowe

Podczas szacowania kosztów utrzymania rozwoju i działania systemu S46 oprócz kosztów osobowych, uwzględniono również koszty inwestycyjne ponoszone w związku z zakupem sprzętu oraz oprogramowania, koszty usług obcych, materiałów i przedmiotów niskocennych oraz delegacji. Koszty te są ponoszone zarówno w związku z rozbudową, modernizacją jak i utrzymaniem infrastruktury, aplikacji i zdolności analitycznych.

Podsumowanie kosztów w poszczególnych kategoriach z podziałem na koszty inwestycyjne i koszty bieżące przedstawia poniższa tabela:

Lata	2025	2026	2027	2028	2029	2030
Bieżące	**22 624 317,00 zł**	**25 660 615,68 zł**	**22 436 552,14 zł**	**30 246 145,93 zł**	**32 063 937,62 zł**	**37 095 769,70 zł**
Rozwój	**5 652 000,00 zł**	**6 556 320,00 zł**	**8 525 721,60 zł**	**9 889 837,06 zł**	**11 472 210,58 zł**	**13 307 765,18 zł**
Osobowe	5 652 000,00 zł	6 556 320,00 zł	8 525 721,60 zł	9 889 837,06 zł	11 472 210,58 zł	13 307 765,18 zł
Utrzymanie	**16 972 317,00 zł**	**19 104 295,68 zł**	**13 910 830,54 zł**	**20 356 308,87 zł**	**20 591 727,04 zł**	**23 788 004,51 zł**
Delegacje	71 340,00 zł	82 754,40 zł	95 995,10 zł	111 354,32 zł	129 171,01 zł	149 838,37 zł
Materiały	170 970,00 zł	162 655,20 zł	188 680,03 zł	813 297,09 zł	253 887,85 zł	294 509,91 zł
Osobowe	13 425 120,00 zł	16 666 416,00 zł	11 181 290,11 zł	14 768 448,72 zł	17 131 401,44 zł	19 872 426,82 zł
Usługi obce	3 304 887,00 zł	2 192 470,08 zł	2 444 865,29 zł	4 663 208,74 zł	3 077 266,74 zł	3 471 229,42 zł
Inwestycje	**12 214 576,50 zł**	**2 344 995,00 zł**	**6 571 680,90 zł**	**8 893 638,00 zł**	**18 450 000,00 zł**	**27 749 230,50 zł**
Rozwój					**18 450 000,00 zł**	
Sprzęt					18 450 000,00 zł	
Utrzymanie	**12 214 576,50 zł**	**2 344 995,00 zł**	**6 571 680,90 zł**	**8 893 638,00 zł**	**0,00 zł**	**27 749 230,50 zł**
Sprzęt	10 787 776,50 zł	2 344 995,00 zł	6 571 680,90 zł	8 893 638,00 zł	0,00 zł	25 609 030,50 zł
Oprogramowanie	1 426 800,00 zł		0,00 zł	0,00 zł	0,00 zł	2 140 200,00 zł
Suma końcowa	**34 838 893,50 zł**	**28 005 610,68 zł**	**29 008 233,04 zł**	**39 139 783,93 zł**	**50 513 937,62 zł**	**64 845 000,20 zł**

W kolejnych latach koszty rozkładają się następująco:

Lata	2031	2032	2033	2034
Bieżące	**44 076 677,03 zł**	**49 566 936,42 zł**	**59 889 994,58 zł**	**68 007 369,59 zł**
Rozwój	**15 437 007,79 zł**	**17 906 929,92 zł**	**20 772 038,30 zł**	**24 095 564,50 zł**
Osobowe	15 437 007,79 zł	17 906 929,92 zł	20 772 038,30 zł	24 095 564,50 zł
Utrzymanie	**28 639 669,23 zł**	**31 660 006,50 zł**	**39 117 956,27 zł**	**43 911 805,09 zł**
Delegacje	173 812,51 zł	201 622,52 zł	233 882,12 zł	271 303,26 zł
Materiały	396 106,99 zł	259 705,36 zł	1 131 508,22 zł	421 966,42 zł
Osobowe	23 052 013,59 zł	26 740 336,32 zł	31 018 788,87 zł	35 981 796,18 zł
Usługi obce	5 017 736,14 zł	4 458 342,30 zł	6 733 777,07 zł	7 236 739,23 zł
Inwestycje	**1 815 480,00 zł**	**7 876 932,30 zł**	**12 874 410,00 zł**	**27 675 000,00 zł**
Rozwój				**27 675 000,00 zł**
Sprzęt				27 675 000,00 zł
Utrzymanie	**1 815 480,00 zł**	**7 876 932,30 zł**	**12 874 410,00 zł**	**0,00 zł**
Sprzęt	1 815 480,00 zł	7 876 932,30 zł	12 874 410,00 zł	0,00 zł
Oprogramowanie	0,00 zł	0,00 zł	0,00 zł	0,00 zł
Suma końcowa	**45 892 157,03 zł**	**57 443 868,72 zł**	**72 764 404,58 zł**	**95 682 369,59 zł**

Koszty inwestycyjne w obszarze utrzymania są związane z wymianą aktualnie użytkowanej infrastruktury. Usługi obce w tym obszarze obejmują przedłużanie subskrypcji na oprogramowanie, opłaty za kolokację i łączność, opłaty serwisowe oraz opłaty za usługi chmurowe. W przypadku rozwoju planuje się poniesienie kosztów związanych z uruchomieniem części niejawnej S46.

Należy zwrócić uwagę, że koszty wdrożenia nowych usług w ramach nowelizacji UKSC w latach 2024–2026 roku ponoszone będą w dużej części z dofinansowaniem z funduszy Krajowego Planu Odbudowy i Rozwoju, w ramach projektu S46-KPO Te wydatki rozwojowe są ujęte w przedstawionych tu kalkulacjach w latach 2025 i 2026.

Ich podsumowanie wygląda następująco (wydatki poniższe są częścią wydatków przedstawionych wyżej):

Lata	KPO
2025	23 375 236,19 zł
2026	8 223 208,10 zł