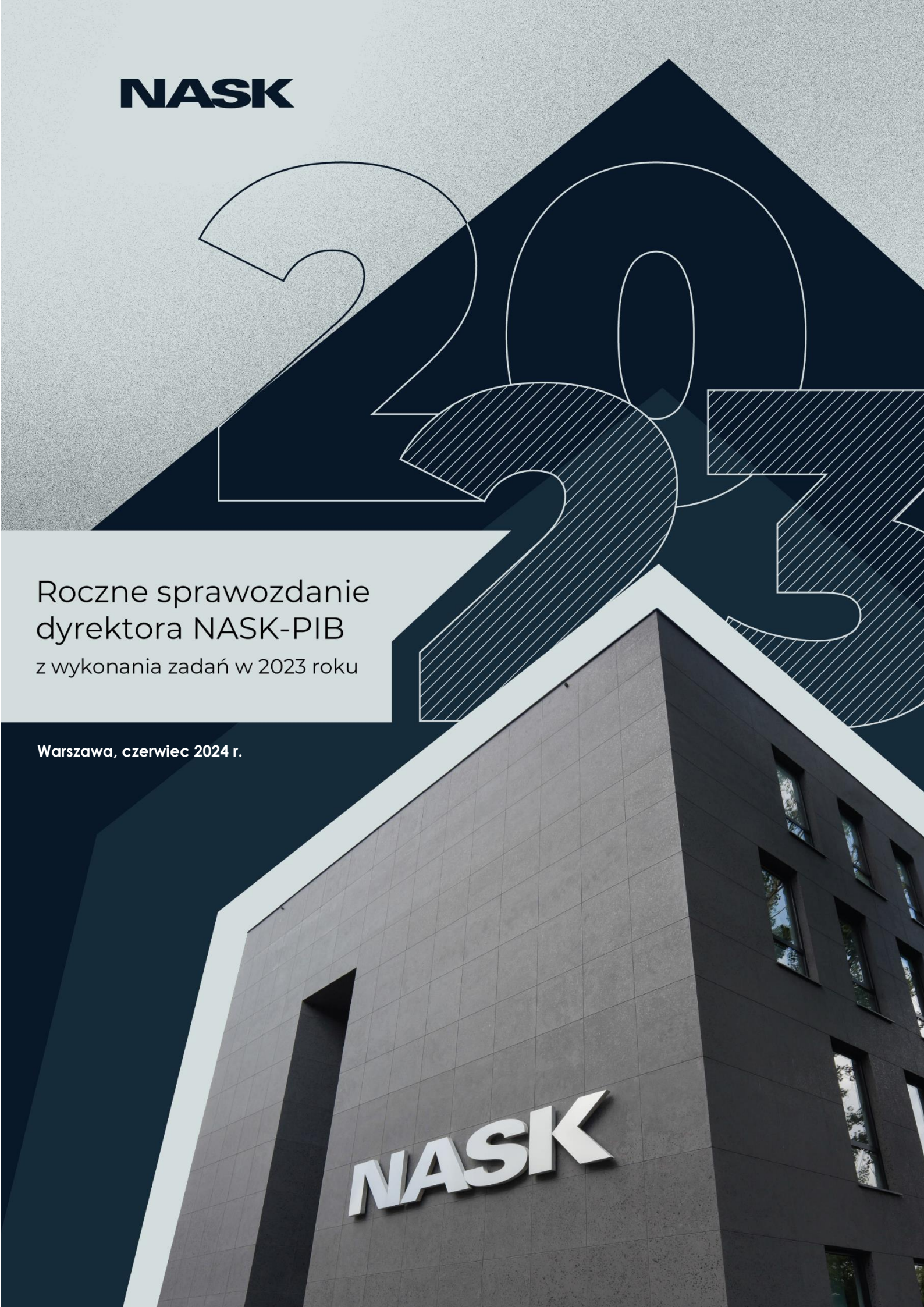
NASK

2023

Roczne sprawozdanie dyrektora NASK-PIB

z wykonania zadań w 2023 roku

Warszawa, czerwiec 2024 r.



Spis treści

Warszawa czerwiec 2024 r.

Wprowadzenie

Ponad 30 lat temu NASK podłączył Polskę do internetu, dziś działa na rzecz zapewnienia szerokiej dostępności oraz bezpieczeństwa internetu, realizując misję cyfryzacji i ochrony cyberprzestrzeni:

- wdraża projekty cyfryzacji kluczowych obszarów życia codziennego, administracji publicznej i gospodarki,
- reaguje na ogólnopolskie zgłoszenia incydentów cyberbezpieczeństwa,
- prowadzi badania naukowe służące rozwojowi technologii pomagającej w detekcji i tłumieniu wielowymiarowych zagrożeń cyberbezpieczeństwa,
- na bieżąco opracowuje raporty dotyczące cyberbezpieczeństwa , dezinformacji
- edukuje w zakresie bezpieczeństwa w sieci, szczególnie dzieci i młodzież.

Misja

Misją Instytutu jest cyfryzacja kraju, rozwój cyberbezpieczeństwa oraz najnowszych technologii poprzez badania, wdrożenia innowacyjnych produktów, działania społeczne i edukacyjne dla popularyzacji idei społeczeństwa informacyjnego. Istotne miejsce w jej realizacji zajmują badania z zakresu sztucznej inteligencji (AI).

Badania

NASK-PIB prowadzi zaawansowane badania naukowe o charakterze podstawowym (matematyka stosowana, informatyka techniczna) oraz interdyscyplinarne projekty badawczo-rozwojowe obejmujące zagadnienia przetwarzania tekstu i obrazu, a także analizy wielkich zbiorów danych (opisujących m.in. incydenty cyberbezpieczeństwa, ruch sieciowy oraz wpływ usług cyfrowych na społeczeństwo), w zastosowaniu do realnych problemów rzeczywistości cyfrowej.

Współpraca

NASK-PIB współpracuje z prestiżowymi ośrodkami naukowymi w Polsce i na świecie, w tym MIT CSAIL oraz University of Technology Sydney. Instytut posiada kategorię naukową A w dyscyplinie informatyka techniczna i telekomunikacja.

CSIRT NASK

Na mocy ustawy o Krajowym Systemie Cyberbezpieczeństwa w strukturach Instytutu działa CSIRT NASK, jeden z trzech zespołów CSIRT poziomu krajowego.

Innowacje

NASK funkcjonuje na styku nauki, biznesu oraz administracji publicznej, co pozwala nieustannie konfrontować innowacje z potrzebami rynku i społeczeństwa.

NASK-PIB oferuje innowacyjne rozwiązania teleinformatyczne dla środowisk akademickich, instytucji badawczych oraz klientów finansowych, biznesowych i administracji.

Domeny

NASK-PIB prowadzi także rejestr nazw w domenie .pl – utrzymując ponad 2,5 mln domen na rzecz ponad 1 mln abonentów.

OSE

W 2017 r. Instytut na mocy ustawy został operatorem Ogólnopolskiej Sieci Edukacyjnej (OSE) – programu, którego celem jest podłączenie wszystkich szkół w Polsce do szybkiego i bezpiecznego internetu.

NASK

1. O NASK-PIB

1.1. Podstawy prawne

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB) działa na podstawie:

- Ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (t.j., Dz. U. z 2024 r. poz. 534);
- Statutu uchwalonego przez Radę Naukową NASK-PIB w dniu 6 października 2023r., zatwierdzonego Decyzją Ministra Cyfryzacji nr 4 z dnia 31 października 2023 r. (Dziennik Urzędowy Ministra Cyfryzacji z dnia 6 listopada 2023 r. poz. 20).

Przedmiotem działania NASK-PIB jest prowadzenie prac badawczo-rozwojowych w szczególności w dziedzinie telekomunikacji, teleinformatyki, sieci i usług teleinformatycznych. Do podstawowej działalności Instytutu, według Polskiej Klasyfikacji Działalności (PKD), należy prowadzenie badań naukowych i prac rozwojowych w dziedzinie pozostałych nauk przyrodniczych i technicznych (PKD 72.19.Z) oraz prowadzenie badań naukowych i prac rozwojowych w dziedzinie nauk społecznych i humanistycznych (72.20.Z). NASK od 7 czerwca 2017 r. jest państwowym instytutem badawczym. Siedzibą NASK-PIB jest Warszawa. Instytut działa pod adresem 01–045 Warszawa, ul. Kolska 12.

Akta rejestrowe NASK-PIB przechowuje Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem 0000012938, REGON NASK-PIB: 010464542, NIP NASK-PIB : 521-04-17-157.

1.2. Struktura organizacyjna

Organami NASK-PIB są Dyrektor NASK-PIB oraz Rada Naukowa NASK-PIB.

Na wewnętrzną strukturę NASK-PIB składa się sześć centrów.

Stan zatrudnienia na dzień 31 grudnia 2023 roku

	Liczba pracowników
Centrum Badań i Rozwoju	103
Centrum Cyberbezpieczeństwa i Infrastruktury	303
Centrum Nowych Technologii dla Polityk Publicznych	204
Centrum Ogólnopolskiej Sieci Edukacyjnej	154
Centrum Procesów Administracyjnych	109
Centrum Zarządzania i Polityki Informacyjnej	314
Ogółem	1187 osób (1153,5 etatów)

Dyrekcja NASK-PIB*

dr inż. Radosław Nielek, Dyrektor NASK-PIB, Dyrektor ds. Zarządzania i Polityki Informacyjnej od 28.12.2023r.

Wojciech Pawlak, p.o. Dyrektora NASK-PIB, Dyrektor ds. Zarządzania i Polityki Informacyjnej do 28.12.2023r.

Adam Marczyński Zastępca Dyrektora NASK-PIB, Dyrektor ds. Cyberbezpieczeństwa i Innowacji

dr hab. inż. Michał Karpowicz, prof. instytutu Zastępca Dyrektora NASK-PIB, Dyrektor ds. Naukowych

Robert Król Zastępca Dyrektora NASK-PIB, Dyrektor ds. Nowych Technologii dla Polityk Publicznych

Magdalena Tarczewska- Szymańska Zastępca Dyrektora NASK-PIB, Dyrektor ds. Procesów Administracyjnych

Dominik Kopera Zastępca Dyrektora NASK-PIB, Dyrektor ds. Projektów Administracyjno-Edukacyjnych

Rada Naukowa NASK-PIB*

dr hab. inż. Joanna Jaworek-Korjakowska, Przewodnicząca Rady

dr hab. inż. Mariusz Kamola, profesor instytutu Zastępca Przewodniczącej Rady

dr Agnieszka Wrońska Sekretarz Rady

prof. dr hab. inż. Marek Amanowicz

prof. dr hab. inż. Katarzyna Kosek-Szott

prof. dr hab. inż. Jacek Mańdziuk

prof. dr hab. inż. Andrzej Pacut

dr hab. Dominik Batorski

dr hab. Joanna Kołodziej

dr hab. inż. Piotr A. Kowalski

dr hab. inż. Agnieszka Ławrynowicz

dr hab. inż. Marek Reformat

dr hab. inż. Piotr Sankowski

gen. bryg. dr inż. Mariusz Chmielewski

dr inż. Konrad Ciecierski

dr inż. Jacek Gondzio

dr inż. Anna Felkner

dr Jan Kołodyński

dr inż. Adam Kozakiewicz

dr inż. Mateusz Krzysztoń

dr inż. Michał Marks

dr inż. Katarzyna Musiał-Gabryś

dr Michał Sierakowski

dr Mateusz Koryciński

mgr inż. Paweł Kostkiewicz

mgr Piotr Nikel

mgr Marcin Wysocki

mgr Maciej Wyszoczarski

dr hab. inż. Michał Karpowicz, prof. instytutu Zastępca Dyrektora NASK-PIB, w trybie art. 30 Ustawy o instytutach badawczych

dr inż. Jerzy Greblicki przedstawiciel ministra właściwego do spraw szkolnictwa wyższego i nauki, w trybie art. 30 ust. 5 pkt 2 Ustawy o instytutach badawczych.

- Skład osobowy na 31 grudnia 2023 roku

Stan zatrudnienia NASK-PIB

NASK-PIB to stabilny pracodawca z ponad 30-letnią historią, który dysponuje doświadczoną i wysoko wykwalifikowaną kadrą naukową oraz inżynierską. Praca w NASK - PIB daje możliwość kreowania bezpiecznej cyberprzestrzeni w gronie światowej klasy ekspertów, uczestnictwa w badaniach naukowych, tworzenia nowoczesnych rozwiązań technologicznych i sztucznej inteligencji, a także budowania odpowiedzialnego społeczeństwa informacyjnego i szerokiego dostępu do Internetu w ramach Ogólnopolskiej Sieci Edukacyjnej. NASK-PIB zatrudnia również ekspertów z obszaru zarządzania projektami, edukacji, PR, marketingu, mediów społecznościowych i relacji z klientem, a wsparciem dla zespołów merytorycznych są pracownicy działów prawnych, finansowych, administracji, kadr oraz zakupów.

Stan zatrudnienia na dzień koniec grudnia 2023 wynosił 1187 osób (ogółem 1153, 5 etatów). W stosunku do roku poprzedniego zatrudnienie wzrosło o 230 pracowników. Dodatkowo 17 pracowników w 2023 roku podpisało umowę o rozpoczęciu pracy w NASK w 2024 roku.

Równość i Różnorodność w NASK

W NASK-PIB istotną wartością jest tworzenie przyjaznego środowiska pracy, które wspiera wszystkie osoby w pełnym wykorzystaniu ich potencjału. Dąży się do zapewnienia równości płci i unikania wszelkiej dyskryminacji, w szczególności ze względu na płeć, religię, orientację seksualną, narodowość, pochodzenie etniczne. W tym celu:

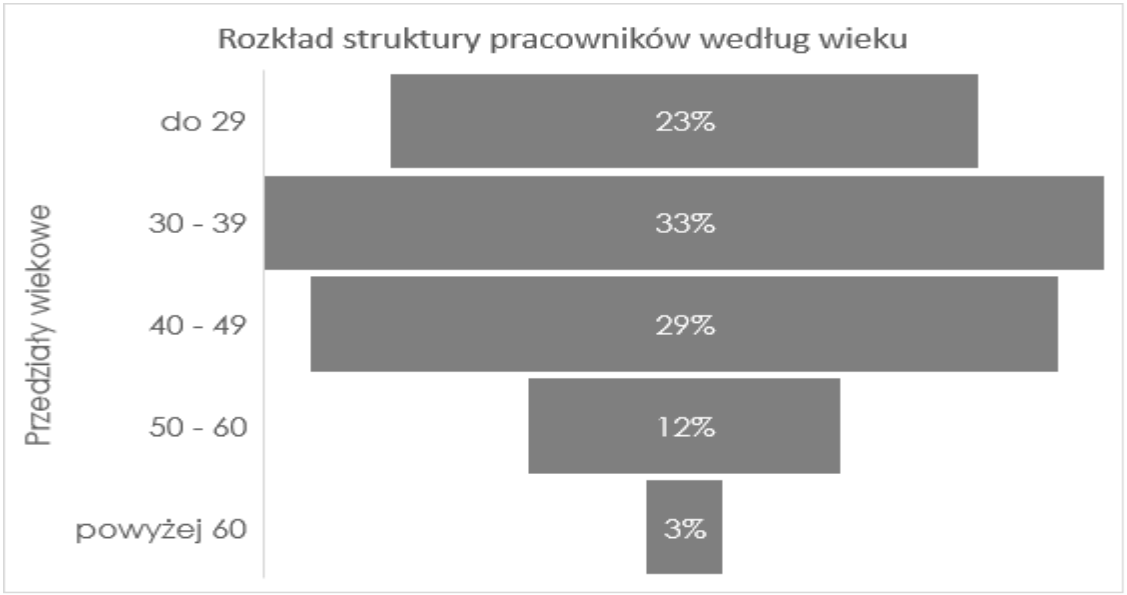
- W 2023 roku w NASK-PIB rozpoczęto realizację celów wyznaczonych w przyjętym pod koniec 2022 roku Planie równości płci.
- Powołano Zespół ds. Równości.
- Zorganizowano szkolenia nt. równości i neuroróżnorodności w miejscu pracy.
- Na stronie intranetowej NASK - PIB utworzono zakładkę, w której regularnie zamieszczane są treści edukacyjno-informacyjne.
- W połowie roku przyjęto nowy Regulamin pracy, na mocy którego dokonano rewizji obowiązków pracodawcy w zakresie przeciwdziałania dyskryminacji w zatrudnieniu ze względu na cechy prawnie chronione oraz wprowadzono szereg uprawnień pracowniczych związanych z rodzicielstwem, w tym prawo do elastycznej organizacji czasu pracy.

Statystyki dot. płci :

W 2023 roku w NASK-PIB zatrudnionych było 41% kobiet oraz 59% mężczyzn.

Statystyki dot. wieku:

Najmłodszy pracownik 19 lat – najstarszy pracownik 77 lat.



Statystyki dot. niepełnosprawności:

W 2023 roku w NASK-PIB zatrudniano 15 osób z orzeczoną niepełnosprawnością, co stanowiło **1,3%** wszystkich pracowników.

Etyka i wartości

W 2023 roku rozpoczęto prace nad Modelem wartości dla NASK-PIB. W proces ten zaangażowana była szeroka i zróżnicowana reprezentacja pracowników NASK-PIB, co wynikało z chęci wypracowania modelu w oparciu o dialog, uwzględniającego wartości, z którymi wszyscy pracownicy będą się identyfikować. Model wartości przyjęto w instytucie w grudniu 2023 roku. Jako kluczowe dla organizacji wskazuje on wartości, takie jak:

- Odpowiedzialność i sprawczość,
- Współpraca i relacje,
- Doskonalenie i otwartość.

W NASK-PIB przykłada się także dużą wagę do przeciwdziałania wszelkim nadużyciom, takim jak mobbing czy dyskryminacja. W tym celu:

- W instytucie obowiązuje Wewnętrzna polityka antymobbingowa.
- Regulamin pracy formułuje obowiązki pracodawcy w zakresie przeciwdziałania mobbingowi.
- Każdy pracownik ma obowiązek zapoznania się z przepisami dotyczącymi przeciwdziałania mobbingowi.
- Nowy Regulamin wynagradzania mówi, iż w przypadku stwierdzenia stosowania mobbingu przez pracownika, traci on prawo do premii, a także nagrody rocznej.

Dialog Społeczny

W NASK-PIB działa zakładowa organizacja związkowa o nazwie Związek Zawodowy Pracowników NASK NASK-PIB (ZZPN), która według stanu na 31 grudnia 2023 roku zrzeszała około 15% pracowników.

W 2023 roku nie było sporów zbiorowych, a prowadzone w tym czasie negocjacje nad zmianą Regulaminu pracy, Regulaminu wynagradzania oraz Regulaminu pracy zdalnej zakończyły się podpisaniem porozumień pracodawcy i strony społecznej. Pracodawca w poszanowaniu doniosłości pokoju społecznego konsultuje ze związkami zawodowymi także kwestie, które wykraczają poza jego obowiązki. Pracodawca odpowiada na pytania strony społecznej w trybie art. 28 ust.1 Ustawy o związkach zawodowych, a także wykonuje obowiązki z zakresu indywidualnego prawa pracy (konsultacje przyczyn wypowiedzeń w trybie art. 38 K.P.).

1.3. Infrastruktura NASK-PIB oraz spółek zależnych

Siedziba NASK-PIB

Własny budynek

ul. Kolska 12, Warszawa;

ul. Spokojna 13 A, Warszawa

Najem powierzchni biurowych

ul. Stawki 40, Warszawa;

al. Armii Ludowej 26 „FOCUS", Warszawa

Oddział Białystok

Najem powierzchni biurowych

ul. Łukowska 2, Białystok

INNE:

Najem powierzchni:

ul. 100-lecia Odzyskania Niepodległości 3, Gmina Moszczenica;

al. Grunwaldzka 413, Gdańsk;

ul. Strzegomska 2/4, Wrocław;

ul. Powstańców Śląskich 9, Wrocław;

ul. Kalwaryjska 33, Kraków

NASK S.A.

Adres siedziby:

ul. 11 Listopada 23, Warszawa

Centrum Przetwarzania Danych

„DC Praga Północ" (DC 11.11)

Powierzchnie biurowe:

ul. Wąwozowa 18, Warszawa

NASK 4 Innovation sp. z o.o. w likwidacji

Adres siedziby:

ul. Piękna 15 lok. 19, Warszawa

Infrastruktura telekomunikacyjna

Sieć telekomunikacyjna NASK-PIB (poza OSE rozdział 4b) składa się z ok. 89 węzłów, z czego ok. 37 jest poza aglomeracją warszawską, a jeden poza granicami Polski (Frankfurt). Sieć światłowodowa, zbudowana z ponad 550 km kabli optycznych i poza węzłami, łączy także lokalizacje klienckie. Sieć telekomunikacyjna NASK-PIB na podstawie odrębnej umowy utrzymywana jest przez NASK SA. W 2023 roku sieć działała stabilnie, oferując użytkownikom gwarantowane SLA. W stosunku do 2022 roku odnotowano wzrost ruchu o ok. 14,3%.

Sieć IP komercyjna

- zbudowana w oparciu o urządzenia Juniper serii MX.
- główne węzły sieci to WAW – UW, WAW – PW, WAW – LIM-2 oraz CPD11 - połączone linkami o przepustowości 100Gbps.
- ponad 4000 portów o łącznej przepustowości ok. 8,6 Tb/s.

Sieć IP naukowo - akademicka (WARMAN)

- technologie: IP, GE/10GE/100GE, MPLS, CWDM
- składa się z węzłów rozmieszczonych na terenie Warszawy, Płocka i Siedlec, co wynika z lokalizacji abonentów naukowych i akademickich
- ponad 1800 portów o łącznej przepustowości ok. 17 Tb/s
- w 2023 roku w projekcie PIONIER-LAB zakupiono nowe urządzenia – ok. 1750 portów o łącznej przepustowości 41,5 Tb/s.

W 1994 roku, na mocy porozumienia środowiskowego, NASK został wskazany jako Jednostka Wiodąca Miejskiej Sieci Komputerowej środowiska naukowo – akademickiego Warszawy – co dało początek budowie sieci WARMAN.

Od 2003 roku NASK-PIB jest członkiem Konsorcjum PIONIER tworzonego przez 23 jednostki z całej Polski, mającego na celu rozwijanie sieci o ustalonym standardzie.

Sieć WARMAN oferuje wszystkie usługi sieci PIONIER – w tym dostęp do internetu światowego (sieć PIONIER i WARMAN stanowią część ogólnoświatowej edukacyjnej sieci internetowej), a także usługi dodatkowe – w tym usługi dostępu do certyfikatów kwalifikowanych TCS, roamingu światowego WiFi – eduroam, PIONIER.TV oraz federacyjnej tożsamości PIONIER.Id (w konfederacji eduGAIN).

Z akademickiej sieci WARMAN korzystało w 2023 roku około 125 jednostek naukowych (większość – w tym wszystkie największe – instytuty i uczelnie aglomeracji warszawskiej).

Badawcza infrastruktura obliczeniowa

W ramach Laboratorium Obliczeniowego NASK-PIB dysponuje mocą obliczeniową zarówno procesorów CPU (ponad 1000 rdzeni obliczeniowych z przeszło 5TB pamięci RAM dla CPU), jak i GPU – kart nVidia V100 (8 sztuk 32GB RAM każda), nVidia A100 (8 sztuk z 40GB RAM każda oraz 8 sztuk z 80GB RAM każda) i nVidia T4 (20 sztuk 16GB RAM każda). Jako systemy składowania danych NASK-PIB wykorzystuje zarówno scentralizowane macierze (przeszło 250TB storage'u All-flash NVME + ponad 1PB storage'u na dyskach talerzowych) jak i wysokowydajne rozwiązanie rozproszone wykorzystujące system weka.io o pojemności ponad 200TB. Serwery obliczeniowe i systemy składowania danych połączone są redundantną siecią 100Gb wykorzystującą urządzania Juniper QFX. Na potrzeby zagadnień sztucznej inteligencji w środowisku obliczeniowym wdrożono między innymi system run.ai do szeregowania obliczeń w środowisku multi-tenant.

W 2023 roku Instytut realizował między innymi projekt wewnętrzny MLOps poświęcony adaptacji metodyki DevOps na potrzeby uczenia maszynowego.

1.4. Finanse

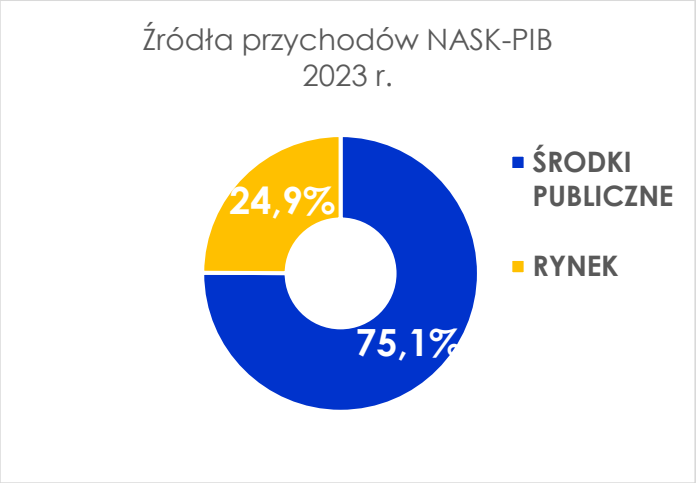
W ostatnich latach znacznie zmienił się charakter działalności i funkcjonowania Instytutu, w którym poza działalnością badawczo-naukową i rynkową (w tym DNS, usługi komercyjne i komercjalizacja), w coraz większym stopniu realizowane są projekty dotacyjne. W szczególności NASK-PIB realizuje coraz więcej zadań publicznych w obszarze cyberbezpieczeństwa i cyfryzacji kraju, jak również w zakresie dostępu do sieci, czy katalogu działań dla społeczeństwa. Wiąże się to też ze zmianą sposobu finansowania, ponieważ wiodącą rolę odgrywają dotacje ze środków publicznych, które z założenia nie mają charakteru komercyjnego i nie przynoszą zysku.

Struktura przychodów NASK-PIB

Źródła finansowania

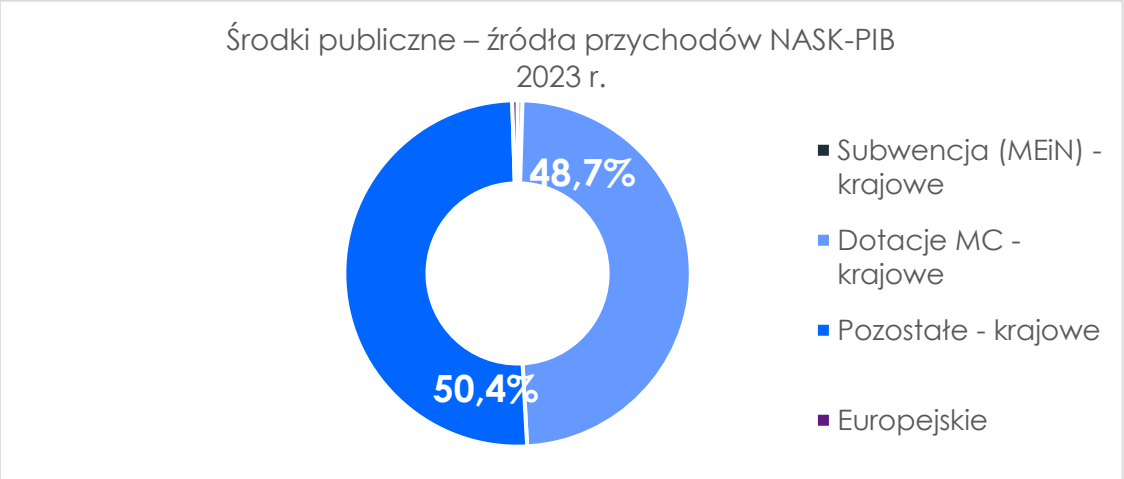
Finansowanie ze źródeł publicznych, w tym realizacja zadań publicznych, projektów inwestycyjnych i grantów B+R było w 2023 r. głównym źródłem przychodów Instytutu i stanowiło ponad 75%.

W porównaniu z rokiem 2022 udział środków publicznych w przychodach ogółem wzrósł z ok 67% do ponad 75%.

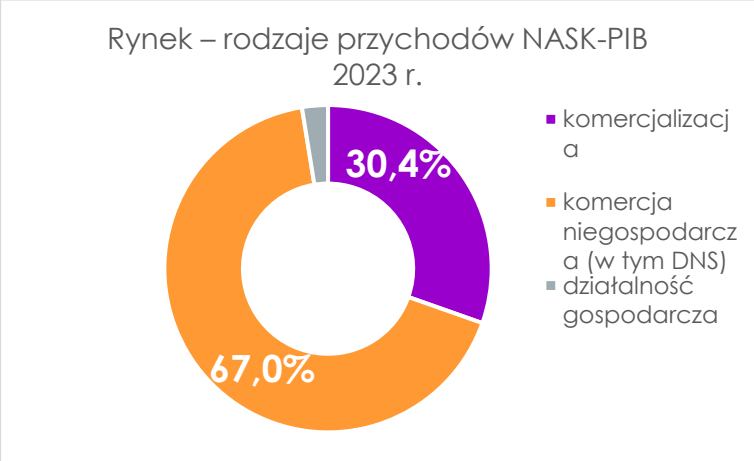


Dotacje, granty i subwencje przeznaczone były na pokrycie kosztów realizowanych projektów i działalności bieżącej, więc nie stanowiły źródeł marży, a w efekcie nie wpływały na wypracowywaną nadwyżkę finansową.

Środki publiczne przeznaczone na realizację zadań i działalność bieżącą NASK-PIB w 2023 r. pochodziły przede wszystkim z środków krajowych, w tym prawie w 49% z Ministerstwa Cyfryzacji.



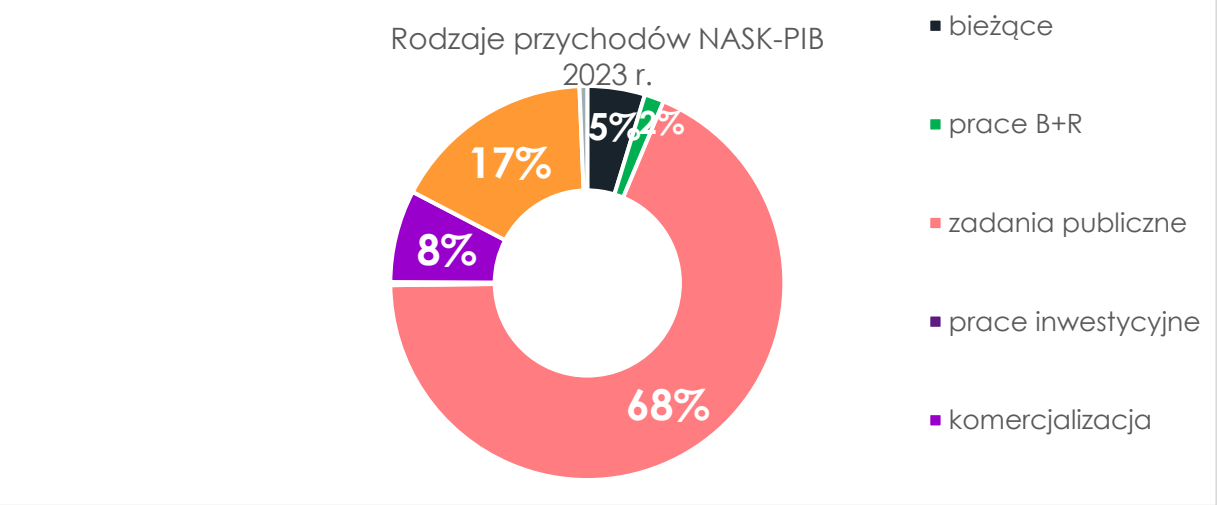
Stabilnym źródłem przychodów są przychody rynkowe, które w 2023 r. stanowiły niespełna 25% przychodów ogółem. Składają się na nie w dużej mierze przychody z usług komercyjnych – 67% i z komercjalizacji – 30%. Te najbardziej stabilne przychody to usługi Rejestru Domen Internetowych.



Biorąc pod uwagę stopniową zmianę charakteru działalności Instytutu oraz struktury jego finansowania można zaobserwować, że jeszcze w 2018 roku przychody z domen (DNS) stanowiły ponad 50% wszystkich przychodów przy 13% w 2023 roku.

Rodzaje przychodów NASK – PIB

Analizując wyniki finansowe za 2023 rok widać, jakie rodzaje działalności generowały najwyższe przychody. Największy udział w przychodach to realizacja zadań publicznych w ramach środków krajowych – 68%, usługi komercyjne (w tym DNS) – 17% i komercjalizacja (sprzedaż wyników badań, transfer wiedzy) – 8%.



Realizowane projekty

W roku 2023 Instytut realizował 58 projektów finansowanych z środków publicznych (krajowych i europejskich) na łączną kwotę 550 mln PLN.

PROJEKTY	liczba	przychody (mln zł)
Dotacje z MC	23	270,13
Programy operacyjne	14	246,84
Projekty krajowe	10	29,93
Projekty europejskie	10	2,71
KPO	1	0,73
	58	**550,34**

Omówienie wyników 2023 w porównaniu do planu i lat ubiegłych

Prognozowany w Planie finansowym zysk netto na rok 2023 wynosił 18,2 mln PLN natomiast wynik netto po wykonaniu roku i sporządzeniu Sprawozdania finansowego za 2023 wyniósł –6,2 mln PLN i jest o 24 mln PLN niższy niż planowany.

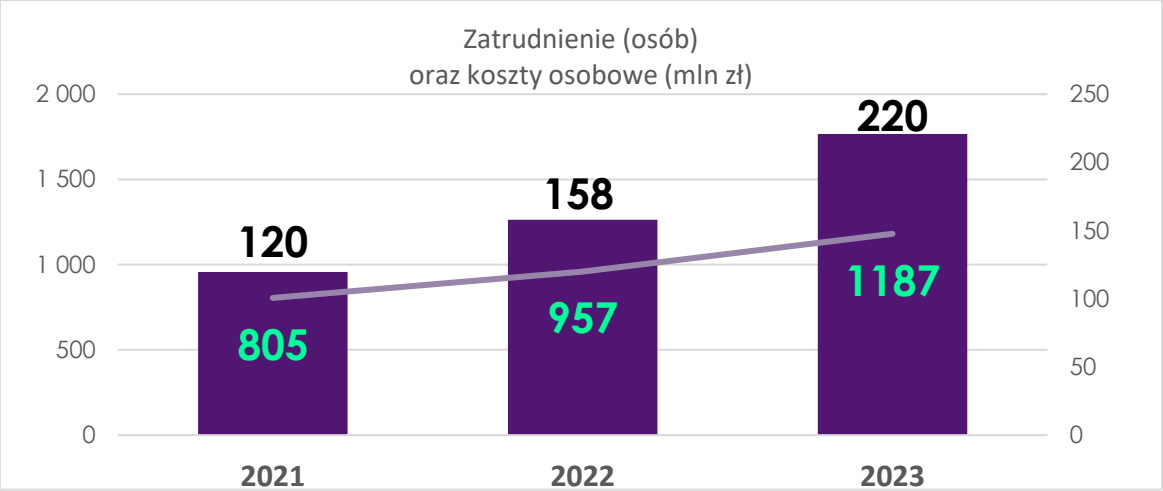
NASK-PIB (mln PLN)	Plan 2023	Wykonanie 2023	Różnica (W-P)
Przychody	**649,4**	**733,8**	**84,4**
Koszty bezpośrednie	**531,5**	**608,8**	**77,3**
Marża 1	117,9	125,0	7,1
marża 1 (%)	*18,2%*	*17,0%*	*-1,3%*
Koszy wydziałowe	**96,0**	**106,3**	**10,3**
Pozostałe przych. op	6,0	8,5	2,5
Pozostałe koszty op.	0,0	28,0	28,0
EBITDA	**28**	**-0,8**	**-28,8**
Amortyzacja	10,3	7,5	-2,8
Przych. finansowe	0,6	5,0	4,4
Koszty finansowe	0,0	1,2	1,2
WYNIK BRUTTO	18,2	-4,5	-22,7
Podatek dochodowy	0,0	1,7	1,7
WYNIK NETTO	**18,2**	**-6,2**	**-24,4**

Przychody ogółem (czyli suma przychodów z działalności podstawowej, pozostałych przychodów operacyjnych i przychodów finansowych) wyniosły 733,8 mln zł. i były wyższe o ponad 80 mln od planowanych.

Natomiast koszty bezpośrednie w porównaniu do planu wyniosły o prawie 80 mln więcej, a wydziałowe o ponad 10 mln. Koszty wydziałowe to przede wszystkim wynagrodzenia osobowe finansowane z własnych środków NASK – PIB.

Koszty wynagrodzeń osobowych wyniosły ok 220 mln zł. i wzrosły o ok 40% w stosunku do roku 2022.

Zatrudnienie na koniec 2023 było na poziomie 1187 pracowników i jest wyższe o 25% od roku poprzedniego.



Wzrost kosztów zatrudnienia w 2023 roku nie był współmierny ze wzrostem przychodów i przełożył się na obniżenie produktywności pracy. W roku 2022 wskaźnik ten wynosił 53,0 tys. zł przychodu na pracownika na miesiąc, a w roku 2023 mimo wzrostu przychodów spadł do 52,5 tys.

W 2022 i 2023 NASK-PIB dokonał wpłat na zewnętrzne Fundusze, w tym na Fundusz Cybezbezpieczeństwa i Fundusz CEPiK w łącznej kwocie 119,3 mln zł. Bardzo poważnie wpłynęło na stan środków pieniężnych i zachwiało zdolnością do samofinansowania Instytutu.

2. Nagrody i wyróżnienia

2.1. Osiągnięcia indywidualne pracowników

- Dr hab. Joanna Kołodziej,

profesor instytutu (Pion Obliczeń Chmurowych i Inteligentnych Sieci, CBiR) znalazła się na liście Top 2% najczęściej cytowanych badaczy na świecie wg Stanford University.

- Dr hab. Michał Oszmaniec,

profesor instytutu (kierownik Zakładu Obliczeń Kwantowych i Komunikacji Kwantowej, CBiR) Nagroda Naukowa PAN im. Stefana Pieńkowskiego w dziedzinie fizyki za osiągnięcie „Zastosowania pomiarów uogólnionych w komputerach kwantowych najbliższej przyszłości".

- Dr Weronika Gutfeter

adiunkt (Zakład Przetwarzania Obrazu, CBiR), wyróżnienie w konkursie na propozycję metody analizy biometrii behawioralnej pisania na klawiaturze w ramach Keystroke Verification Challenge 2023, zorganizowanego przy okazji konferencji IEEE International Conference on Big Data (IEEE BigData 2023)

- Dr Piotr Białczak, Mateusz Leśniak, Kacper Ratajczak

Nagrody w V jubileuszowej edycji konkursu Ministra Obrony Narodowej o nagrodę im. Mariana Rejewskiego na najlepszą pracę naukową poświęconą cyberbezpieczeństwu i kryptologii dla Piotra Białczaka (CERT, praca doktorska), Mateusza Leśniaka (Zakład Kryptologii, CBiR, praca magisterska) i Kacpra Ratajczaka (CERT, praca inżynierska)

Otrzymanie stopnia doktora przez 7 pracowników NASK-PIB:

- Piotr Białczak (CERT Polska), obrona rozprawy: „Wykorzystanie protokołu HTTP do identyfikacji i klasyfikacji złośliwego oprogramowania", Politechnika Warszawska,

- Sylwia Borowska-Kazimiruk (Biuro Rozwoju Nauki, CBiR), obrona rozprawy „Modernizacje widzenia. Władysław Heinrich, Wacław Berent a drogi rozwoju polskiej psychologii doświadczalnej (1890-1939)", Uniwersytet Warszawski,

- Weronika Gutfeter (Zakład Biometrii, CBiR), obrona rozprawy „Identyfikacja twarzy na podstawie obrazów wieloujęciowych z zastosowaniem głębokich sieci agregujących", Politechnika Warszawska

- Agnieszka Karlińska (Zakład Inżynierii Lingwistycznej i Analizy Tekstu, CBiR), obrona rozprawy „Psychiatria na wokandzie. Strategie dyskursywne w opiniowaniu sądowo-psychiatrycznym", Uniwersytet Warszawski,

- Antonina Krajewska (Zakład Algebry Liniowej, CBiR) obrona rozprawy „Efficient matrix completion for data recovery in data-driven IT applications", IBS PAN,

- Dorota Mularczyk (Zakład AI-MED, CBiR), obrona rozprawy „Termodynamiczne i strukturalne następstwa substytucji reszt aminokwasowych w rejonie kieszeni wiążącej β- laktoglobuliny", Uniwersytet Jagielloński w Krakowie,

- Marek Janiszewski (Zakład Bezpieczeństwa Informacji, CBiR), obrona rozprawy „Metodyka oceny wiarygodności systemów zarządzania zaufaniem i reputacją", Politechnika Warszawska.

2.2. Wyróżnione produkty

Nagroda Lider Bezpieczeństwa Państwa dla systemu ochrony bankowości mobilnej i internetowej Botsense.

2.3. Sukcesy w obszarach działalności

- CERT Polska, jako jedyna instytucja w kraju i jeden z 7 CERT-ów w Europie, od 1 sierpnia 2023 roku ma status CNA (CVE Numbering Authority), co pozwala na nadawanie identyfikatorów i publikowanie informacji o podatnościach w programie CVE.

- W ramach programu CVE CSIRT NASK w 2023r. koordynował ujawnienie 6 podatności – 3 z nich zostały odkryte w wyniku badań własnych CERT Polska oraz NASK-PIB.

- Odkrycie 5-ciu nowych podatności w urządzeniach IoT w ramach prac CBiR NASK-PIB w 2023 roku.

- Sukces NASK-PIB i CERT Polska w międzynarodowych ćwiczeniach Locked Shields 2023 organizowanych przez NATO Cooperative Cyber Defence Centre of Excellence CCDCOE. Polska zajęła 3. miejsce.

- Drugie miejsce drużyny „Poland Can Into Space" w 4. edycji konkursu „Hack-A-Sat" organizowanego przez amerykańskie wojsko. Członkami polskiego zespołu byli m.in. eksperci z CERT Polska.

- Sukces w European Cyber Security Challenge (ECSC) zorganizowanym przez ENISA. Polska drużyna, rekrutowana przez CERT Polska, zajęła 9. miejsce na 28 rywalizujących zespołów.

- W 2023 roku system ARAKIS został wyróżniony nagrodą Lider Bezpieczeństwa Państwa.

- Dyżurnet.pl uzyskał status tzw. buddy hotline, czyli zespołu wprowadzającego i wspierającego nowo utworzone zespoły reagujące na Słowacji (OCHRÁŇMA.sk) i w Ukrainie (Stop Crime Magnolia) w ramach stowarzyszenia INHOPE.

- Udział ekspertów Dyżurnet.pl w opracowaniu SCHEMA, międzynarodowego standardu klasyfikacji CSAM, ujednolicającego klasyfikację nielegalnych materiałów.

- Udział ekspertów Dyżurnet.pl w opracowaniu Krajowego Planu Przeciwdziałania Przestępstwom Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich na lata 2023–2026.

- Zwiększenie składu Rady Naukowej NASK-PIB do 28 osób o czołowych przedstawicieli nauki oraz biznesu, w tym z zagranicznych ośrodków naukowych.

- Utrzymanie certyfikatu normy ISO 9001:2015.Audyt nadzoru Systemu Zarządzania Jakością w zakresie rejestracji i utrzymywania domen .pl, zakończony pozytywnym wynikiem i utrzymaniem certyfikatu na zgodność systemu z wymaganiami normy ISO 9001:2015.

- Wyróżnienie dla NASK-PIB za 30-letnią współpracę z PIIT, okazji 30-lecia Polskiej Izby Informatyki i Telekomunikacji (PIIT) i 20-lecia Sądu Polubownego ds. Domen Internetowych przy PIIT.

2.4. Uzyskane patenty

- Zgłoszenie patentowe #P1349EP00 do europejskiego urzędu patentowego „Komputerowe narzędzie do klasyfikacji i sposób klasyfikacji sygnałów z mikroelektrody pobieranych podczas głębokiej stymulacji mózgu",

- Zgłoszenie patentowe 18412819 do urzędu patentowego USA „A computer implemented classification tool and method for classification of microelectrode re-cordings taken during a deep brain stimulation".

3. Działalność naukowo-badawcza

3.1. Główne obszary badań

Cyberbezpieczeństwo

Wykrywanie, modelowanie propagacji i tłumienie zagrożeń bezpieczeństwa cybernetycznego wymaga rozwoju technologii przetwarzania i analizy wielkich zbiorów danych. Kluczową rolę odgrywają w tym kontekście algorytmy obliczeniowe (m.in. randomizowanej algebry liniowej i uczenia maszynowego), mechanizmy inżynierii sieciowej oraz systemy analizy tekstu i obrazu wspierające analizę danych o incydentach cyberbezpieczeństwa. Ponadto ochrona informacji w cyberprzestrzeni w dużym stopniu oparta jest na komponentach kryptograficznych, które w przypadku prawidłowej implementacji w ekosystemie informacyjnym zapewniają m.in. poufność i integralność danych

oraz zarządzanie dostępem. Badania w obszarze cyberbezpieczeństwa skupiały się wokół następujących wyzwań:

- matematycznych podstaw detekcji, propagacji i tłumienia zagrożeń,
- technologii monitorowania sieci, systemów i usług cyfrowych,
- kryptoanalizy metodami wyżarzania kwantowego oraz kryptografii anamorficznej zapewniającej ochronę nawet w przypadku wymuszonego ujawnienia kluczy prywatnych,
- ochrony komunikacji w przypadku ekstremalnych ograniczeń natury fizycznej na kanał komunikacyjny,
- rozproszonych systemów cyberbezpieczeństwa,
- kwantowych systemów dystrybucji klucza (QKD) i generacji liczby losowych (QRNG),
- detekcji niebezpiecznych treści i dezinformacji.

Sztuczna inteligencja (AI)

Jednym z największych wyzwań naukowych naszych czasów jest zrozumienie natury inteligencji i świadomości, a także wyjaśnienie specyfiki i podatności procesów uczenia. Wokół tych wyzwań koncentrowały się badania nad matematycznymi podstawami uczenia maszynowego i inteligencji maszynowej, inżynierią mechanizmów uczenia i reprezentacji danych, a także nad interpretowalnością modeli. Badania obejmowały rozwój teorii metafaktoryzacji, teorii układów dynamicznych, metod analizy i reprezentacji treści, analizę struktur wielowarstwowych sieci neuronowych, zastosowaniu metod atencji w głębokich sieciach neuronowych, a także algorytmów optymalizacji. Głównymi nurtami badawczymi w tym obszarze były:

- matematyczne podstawy analizy danych,
- analiza procesów uczenia maszynowego i inteligencji maszynowej,
- inżynieria uczenia i reprezentacji danych,
- wyjaśnialność modeli (Explainable AI),
- etyka, ewolucja i bezpieczeństwo AI,
- analiza tekstu, obrazów, wideo i multimediów,
- AI w cyberbezpieczeństwie, medycynie, biometrii oraz humanistyce cyfrowej.

3.2. Główne osiągnięcia i odkryta wiedza

Nowe modele detekcji treści wrażliwych i szkodliwych w tekstach

Opracowane zostało nowe rozwiązania dla wyzwań związanych z identyfikacją treści wrażliwych i szkodliwych w danych tekstowych. Stworzono autorską wersję modelu BERTopic, która pozwala na efektywne wykrywanie tematów wrażliwych, takich jak: przemoc, zaburzenia odżywiania czy uzależnienia. Bazujący na danych z portalu Wykop.pl utworzono nowy model do wykrywania treści obraźliwych, który osiąga skuteczność na poziomie 94%. Jego architektura łączy warstwę wyjściową RoBERTy z wektorami StyloMetrix, a następnie kieruje wyniki do warstwy gęstej i decyzyjnej. Taka sama architektura została zastosowana w modelu detekcji treści drastycznych. Utworzono również BAN-PL, czyli pierwszy publicznie dostępny polskojęzyczny zbiór danych, który zawiera treści usunięte z sieci w procesie moderacji. Zbiór składa się z 24 000 zanonimizowanych postów i komentarzy z portalu Wykop.pl i jest w pełni zbalansowany.

Projekt powiązany: KOMTUR

Nowy model wykrywania szkodliwych treści erotycznych w tekstach narracyjnych

Opracowany został hybrydowy system łączący sieci neuronowe i reguły do identyfikacji treści erotycznych o charakterze szkodliwym, obejmujących m.in. CSAM i kazirodztwo. System wykorzystuje koreferencję, czyli związek między wyrażeniami w tekście odnoszącymi się do tej samej osoby lub rzeczy. Przeprowadzone testy wykazały dokładność 84% i czułość 80% w języku polskim, przewyższając metody oparte na modelach RoBERTa i Longformer. Wyniki te potwierdzają istotną rolę koreferencji w wykrywaniu szkodliwych treści erotycznych. Hybrydowy model może stanowić cenne narzędzie dla moderatorów w walce ze szkodliwymi treściami, wspierając ich w podejmowaniu świadomych decyzji a także umożliwiać lepszą wizualizację wyników,.

Projekt powiązany: APAKT

Odkryte podatności

W ramach prac PSC/CBiR w 2023 roku odkryto 5 podatności w urządzeniach IoT. Cztery z tych podatności zostały już opublikowane, jedna z nich ze względu na występowanie bezpośrednio w API nie uzyskała identyfikatora CVE. Podatność o najwyższym parametrze CVSS, w związku z prośbą producenta o wydłużenie czasu na naprawę, wciąż oczekuje na publikacje.

Odkryto następujące podatności:

- CVE-2023-3612, CVSS: 8.8 - HIGH – niezabezpieczony widok WebView,
- CVE-2023-6913, CVSS: 8.1 - HIGH, niezabezpieczony widok WebView i niezabezpieczony skaner kodów QR,
- CVE-2023-4617, CVSS: 9.4 - CRITICAL, niebezpieczna procedura parowania urządzeń, oczekuje na publikacje,
- CVE-2023-6998, CVSS: 7.4 - HIGH, niebezpieczny ekran blokady aplikacji,
- BRAK CVE, niebezpieczna procedura usuwania urządzeń z konta.

Metodykę badań pozwalającą na identyfikacje podatności w urządzeniach IoT przedstawiono na konferencjach branżowych The Hack Summit oraz Oh My H@ck, które odbyły się pod koniec 2023 roku.

Powiązany projekt: LaVA

Rozwój metod interpretowalnej lingwistycznej reprezentacji tekstu

StyloMetrix to otwarte wielojęzyczne narzędzie, które pozwala tworzyć interpretowalną dla człowieka i maszyny reprezentację wektorową danych tekstowych, opartą na statystykach lingwistycznych. Wektory StyloMetrix mogą być zarówno wejściem do modeli uczenia maszynowego, jak i źródłem informacji o wzorcach stylometrycznych analizowanego korpusu. Opracowane przez ekspertów statystyki pozwalają na analizę cech językowych tekstu związanych z częściami mowy, syntaktyką, fleksją, interpunkcją, leksyką i jej psycholingwistycznymi właściwościami, prozodią, kształtem graficznym i wzorcami deskryptywnymi. Narzędzie jest obecnie dostępne dla języków polskiego, angielskiego, ukraińskiego, rosyjskiego oraz niemieckiego.

Aplikacja do przetwarzania i analizy treści oraz stylu dokumentów tekstowych

NLP Toolkit to aplikacja webowa oferująca narzędzia do przetwarzania oraz analizy dokumentów tekstowych: od czyszczenia i anonimizacji, przez tworzenie streszczeń, po zaawansowaną analizę lingwistyczną. Umożliwia ona kompleksową pracę z tekstem osobom nieposiadającym kompetencji programistycznych. Przeprowadzone badanie rynku pozwoliło zidentyfikować dwie grupy odbiorców: osoby wykonujące zawody prawnicze oraz naukowców i naukowczynie. Na bazie aplikacji możliwe jest tworzenie modułowych zestawów narzędzi dla konkretnych grup użytkowników (on premise).

Opracowanie metody lokalizacji jądra niskowzgórzowego u pacjentów poddawanych chirurgicznemu leczeniu Choroby Parkinsona.

Opracowana metoda znajduje zastosowanie jako system wspomagania decyzji w operacyjnym leczeniu choroby Parkinsona. Leczenie takie stosowane jest w przypadku pacjentów, u których leki nie przynoszą pożądanego skutku. Zabieg polega na precyzyjnym umiejscowieniu elektrody stymulującej w jądrze niskowzgórzowym - niewielkiej strukturze znajdującej się wewnątrz mózgowia, która nie jest widoczna na obrazach tomograficznych czy MRI. Dla prawidłowego przebiegu zabiegu operacyjnego, oraz dla uzyskania maksymalnie korzystnego efektu terapeutycznego, wymagana jest niebywale duża precyzja w czasie umiejscowienia elektrody. Algorytm opracowany przez dr. inż. Konrada Ciecierskiego używa głębokiej sieci neuronowej opartej na modelu ResNet, który został wzbogacony w mechanizmy atencji działające w wymiarze czasowym. Na podstawie analizy aktywności tkanki mózgowej jest w stanie określić położenie docelowej struktury z ponad 90-procentową dokładnością, a także określić optymalny sposób umiejscowienia elektrody w obrębie tej struktury. Jest to nieoceniona pomoc dla neurochirurga, który bazując na swojej wiedzy i doświadczeniu jest w stanie zinterpretować wyniki działania algorytmu. Ponadto zastosowanie tego narzędzia umożliwiło znaczące skrócenie czasu zabiegu, co przyczynia się również do zmniejszenia dyskomfortu pacjenta, który w czasie zabiegu pozostaje przytomny.

Opracowana metoda Hy-Tract do uzyskiwania traktografii na podstawie wyników badania MRI DWT.

Hy-Tract to nowatorska metoda analizy danych dyfuzyjnych uzyskanych w wyniku eksperymentów MRI. Użyta hybrydowa technika łączy sieci neuronowe do analizy danych dyfuzyjnych z algorytmem wyszukiwania ścieżek wyznaczającym topologię włókien nerwowych na podstawie analizowanych danych. Proponowana metoda może znaleźć wiele zastosowań, w tym do określania topologii ścieżek neuronowych w pobliżu pola operacyjnego lub tworzenia map połączeń pomiędzy różnymi obszarami funkcjonalnymi mózgu. Neurochirurdzy i radiolodzy mogą wykorzystać pozyskiwaną dzięki niej wiedzę do planowania przedoperacyjnego i nawigacji śródoperacyjnej. Metoda zaprezentowana została na seminarium naukowym w Klinice Nowotworów Układu Nerwowego w NIO PIB.

APAKT - system do wykrywania treści przedstawiających seksualne wykorzystywanie dzieci (CSAM) oparty na AI.

W ramach projektu opracowano algorytmy rozpoznające niepożądane materiały, takie jak CSAM, w postaci obrazów oraz tekstów. Projekt był finansowany przez NCBR i realizowany przez konsorcjum złożone z NASK-PIB, Politechniki Warszawskiej oraz Enamor International.

Detekcja i analiza treści CSAM

W ramach realizacji projektu APAKT połączono w jeden system (tzw. pipeline) modele składowe detekcji CSAM: detekcja postaci, detekcja części ciała, klasyfikacja wieku, klasyfikacja aktywności seksualnej (oraz więcej modeli klasyfikacji umożliwiających klasyfikacje na podklasy CSAM). Na danych rzeczywistych dokonano porównania dokładności metody detekcji CSAM wykorzystującej jeden model end-to-end oraz systemu składającego się z wielu modeli cząstkowych. Opracowano także skrypty, służące do uzyskiwania predykcji wytrenowanych modeli w systemie stosowanym przez Dyżurnet.pl. Wraz z zespołem Dyżurnet.pl przeprowadzono testy użyteczności modeli w zagadnieniu priorytetyzacji nowych zgłoszeń.

Projekt powiązany: APAKT

System wczesnego wykrywania rejestracji domen phishingowych

Ataki phishingowe to podszywanie się pod jednostki, takie jak znane firmy czy banki w celu wyłudzenia informacji wrażliwych od użytkowników. W ramach przeprowadzonych prac stworzyliśmy system BadDomains do wczesnego wykrywania rejestracji domen phishingowych. Model LightGBM wykorzystuje dane z rejestru domen o nowo zarejestrowanych domenach połączone z wiedzą o aktualnej sytuacji phishingowej, taką jak informacje o najczęstszch celach cyberprzestępców, czy podejrzane informacje kontaktowe. Ocena systemu została przeprowadzona przy użyciu informacji z rejestru domen najwyższego poziomu .pl (TLD) połączonego z publiczną listą domen phishingowych CERT Polska. BadDomains zostało porównane z podobnym systemem wykrywania zaprojektowanym dla TLD .eu o nazwie Premadoma osiągając znacznie lepsze wyniki w zakresie precyzji i metryki F1. Projekt powiązany: DNS4EU

Interdyscyplinarny projekt badawczy Wykorzystywanie seksualne dzieci w cyberprzestrzeni

W 2023 roku trwały prace nad analizą pozyskanych danych w ramach interdyscyplinarnego projektu badawczego Wykorzystywanie seksualne dzieci w cyberprzestrzeni. Przeprowadzono analizę akt postępowań karnych ze szczególnym uwzględnieniem roli biegłych powoływanych w tych postępowaniach. Pierwsze tego rodzaju przedsięwzięcie badawcze odwoływało się do wiedzy z następujących dyscyplin naukowych: prawa, psychologii, seksuologii, antropologii, psychiatrii oraz informatyki. W ramach projektu powstał raport „Wykorzystywanie seksualne dzieci w cyberprzestrzeni. Analiza akt postępowań karnych ze szczególnym uwzględnieniem roli biegłych powoływanych w tych postępowaniach".

Badania społeczne i rynkowe

- „Kompetencje cyfrowe urzędników JST szczebla gminnego" – realizacja ogólnopolskich badań CAWI wśród urzędników gminnych JST na temat kompetencji cyfrowych urzędników JST szczebla gminnego.
- „Kompetencje cyfrowe urzędników JST szczebla powiatowego" - realizacja ogólnopolskich badań CAWI wśród urzędników powiatowych JST na temat kompetencji cyfrowych urzędników JST szczebla gminnego.
- ,,Nadzieje, obawy, wyzwania (NOW) – jak studenci postrzegają wpływ nowych technologii?" – Badanie PAPI wśród studentów na temat nowych technologii, ich nadziei (jakie szanse zawodowe i prywatne mogą im one przynieść) i obaw (w jaki sposób mogą mieć one negatywny wpływ na życie/plany studentów), wyzwań (jakie działania powinny zostać podjęte, aby zrealizować szanse i zapobiec obawom. Wyniki zostały opublikowane i zaprezentowane na IGF 2023.
- „Cyfrowe źródła informacji a procesy i struktury konstruowania wiedzy w okresie późnej adolescencji" - Analiza danych i redakcja raportu z ogólnopolskiego badania zrealizowanego w 2022. Raport jest rozpoznaniem cyfrowych źródeł informacji, wpływających i wywierających wpływ na proces konstruowania ogólnej wiedzy o świecie i postrzegania zjawisk społecznych przez młodych Polaków.
- „Nastolatki 3.0" - Analiza danych i redakcja raportu z V edycji badań będących kontynuacją pierwszej w Polsce, kompleksowej i systematycznej procedury obserwacji i pomiaru postaw nastolatków wobec internetu oraz rozwoju kompetencji cyfrowych nastolatków i cyfryzacji procesu nauczania. Badania CAWI zrealizowano wśród 4800 uczniów ze 160 szkół (podstawowych i ponadpodstawowych) oraz rodziców nastolatków biorących udział w badaniu (n=1000) z terenu całej Polski.
- „Aspiracje edukacyjne i zawodowe uczniów szkół średnich" - Badanie mające na celu określenie aspiracji edukacyjnych uczniów szkoły podstawowej i ponadpodstawowej, w tym uzyskanie informacji na temat planów edukacyjnych

i zawodowych uczniów. Badanie CAWI zrealizowane wśród 16800 uczniów szkół średnich.

- „Wzór osobowy internauty. Preferowane style interakcji cyfrowych w polskim społeczeństwie" – Raport z badania z zakresu pożądanych sposobów zachowań i interakcji w sieci (wzmacniających integralność, a w szczególności zaufanie i więź społeczną).
- „Silne hasła" – ogólnopolskie badania dotyczące Kampanii Edukacyjno - Informacyjnych mających na celu wzrost świadomości mieszkańców Polski w zakresie bezpieczeństwa w Internecie, zagrożeń takich jak waga ochrony danych oraz radzenia sobie z nimi (2 fale badania PRE i POST)
- „mObywatel" - ogólnopolskie badania dotyczące Kampanii Edukacyjno - Informacyjnych mających na celu wzrost świadomości mieszkańców Polski w zakresie korzystania z e-usług publicznych, w tym istnienia usług e-administracji oferowanych centralnie i przez samorządy; (2 fale badania PRE i POST)
- „Cyberzagrożenia" - ogólnopolskie badanie dotyczące Kampanii Edukacyjno - Informacyjnych mających na celu wzrost świadomości zagrożeń związanych z korzystaniem z Internetu; (badania PRE)
- „Fałszywe sklepy internetowe" ogólnopolskie badanie dotyczące Kampanii Edukacyjno - Informacyjnych mających na celu wzrost świadomości zagrożeń związanych z korzystaniem z Internetu w tym fałszywych sklepów internetowych (fala badania POST)
- „Szybkie płatności" ogólnopolskie badanie dotyczące Kampanii Edukacyjno - Informacyjnych mających na celu budowanie zaufania i pozytywnych postaw wobec usług e-administracji (fala badania POST)
- „Niebezpieczne załączniki" ogólnopolskie badanie dotyczące Kampanii Edukacyjno - Informacyjnych mających na celu wzrost świadomości mieszkańców Polski w zakresie bezpieczeństwa w Internecie, zagrożeń i radzenia sobie z nimi", (fala badania POST)
- „Fałszywe inwestycje" ogólnopolskie badanie dotyczące Kampanii Edukacyjno - Informacyjnych mających na celu wzrost świadomości cyberzagrożeń (fala badania POST)
- „Wiarygodność informacji" ogólnopolskie badanie dotyczące Kampanii Edukacyjno - Informacyjnych mających na celu wzrostu świadomości zagrożeń związanych z informacjami w mediach cyfrowych (fala badania POST)
- „FOMO 2022. Polacy a lęk przed odłączeniem" wspólne badanie badaczy z NASK-PIB, Wydziału Dziennikarstwa, Informacji i Bibliologii (WDIB UW) i Wydziału Psychologii Uniwersytetu Warszawskiego oraz Panelu Badawczego Ariadna dotyczące zjawiska FOMO.

Seminaria naukowe

W 2023r. zorganizowano 28 seminariów naukowych. Celem było podnoszenie kwalifikacji, trening sztuki prezentacji , networking naukowy oraz otrzymanie informacji zwrotnej dotyczącej badań, publikacji. Część z tych seminariów była otwarta dla osób spoza instytutu, co umożliwiało szeroką dystrybucję wiedzy oraz sprzyjało nawiązywaniu współpracy między różnymi instytucjami i badaczami. Poniżej wybrane seminaria:

- 22 lutego – seminarium naukowe dr. Jana Kołodyńskiego z Politechniki Warszawskiej „Sensory kwantowe - perspektywy technologiczne vs motywacje naukowe"
- 1 marca – seminarium naukowe dr. Keatona Hamma z The University of Texas at Arlington „Getting more with less: matrix and tensor algorithms from subsampling modes"
- 29 marca – seminarium naukowe dr. Justina Solomona z Massachusetts Institute of Technology „ Machine Learning Using the Geometry of Datasets and Loss Functions"
- 12 lipca – seminarium naukowe z prof. dr. hab. Hanną Bogucką z Politechniki Poznańskiej „ Bezpieczeństwo otwartych radiowych sieci dostępowych 5G i 6G"
- 27 września – seminarium naukowe z dr. Amirem Patelem z Oxford University „Studying Cheetahs Through the Lens of Robotics"
- 4 października – seminarium naukowe z dr. hab. Tomaszem Wolakiem z Naukowego Centrum Obrazowania Biomedycznego w Światowym Centrum Słuchu „Sztuczna inteligencja a inteligencja biologiczna: podobieństwa, różnice i wyzwania"
- 11 października – seminarium naukowe z prof. dr. hab. Przemysławem Bieckiem z Politechniki Warszawskiej „Red-Teaming modeli AI, czyli jak i po co wykorzystywać XAI do analizy modeli predykcyjnych"

3.3. Publikacje naukowe

Artykuły w czasopismach naukowych

1. Elżbieta Burek, Krzysztof Mańk, Michał Wroński, *Searching for an Efficient System of Equations Defining the AES Sbox for the QUBO Problem*. Journal of Telecommunications and Information Technology, 2023, 4; 30-37. http://dx.doi.org/10.26636/jtit.2023.4.1340.
2. Konrad Ciecierski, Tomasz S. Mandat, *Classification of DBS microelectrode recordings using a residual neural network with attention in the temporal domain*. Neural Networks, 2024, 170; 18-31. Online first 2023. http://dx.doi.org/10.1016/j.neunet.2023.11.021.
3. Jacek Cichoń, Mirosław Kutyłowski, Patryk Stopyra, *Creating small ad hoc networks: Swift presence notification strategies.* Vehicular Communications, 2024, 45; 1-13. Online first 2023. https://doi.org/10.1016/j.vehcom.2023.100694.

4. Anna Felkner, *Źródła użytecznych informacji o zagrożeniach w internecie rzeczy*. Cybersecurity and Law, 2023, 1(9); 144-154. http://www.cybersecurityandlaw.com/pdf-169306-92123?filename=Zrodla%20uzytecznych.pdf.

5. Maciej Grzenda, Stanisław Kaźmierczak, Marcin Luckner, Grzegorz Borowik, Jacek Mańdziuk, *Evaluation of machine learning methods for impostor detection in web applications*. Expert Systems with Applications, 2023, 231. http://dx.doi.org/10.1016/j.eswa.2023.120736.

6. Agnieszka Karlińska, Paulina Czwordon-Lis, Maciej Maryl, *Korpus tekstowy jako narzędzie literaturoznawcze*, Teksty Drugie, 2023, 6.

7. Kamila Lis, Ewa Niewiadomska-Szynkiewicz, Katarzyna Dziewulska, *Siamese Neural Network for Keystroke Dynamics-Based Authentication on Partial Passwords*. Sensors, 2023, 23(15); 1-22. http://dx.doi.org/10.3390/s23156685.

8. Victor Mandat, Pawel R. Zdunek, Bartosz Krolicki, Krzysztof Szalecki, Henryk M. Koziara, Konrad Ciecierski, Tomasz S. Mandat, *Periaqueductal/periventricular gray deep brain stimulation for the treatment of neuropathic facial pain*. Frontiers in Neurology, 2023, 14; 1-8. http://dx.doi.org/10.3389/fneur.2023.1239092.

9. Inez Okulska, Anna Kołos, *A morpho-syntactic analysis of human moderated hate speech samples from Wykop.pl web service*, Półrocznik Językoznawczy Tertium. Tertium Linguistic Journal, 2023, 8(2).

10. Inez Okulska, Anna Kołos, Krzysztof Skibski, *Gra w klasy, czyli analiza lingwistycznych cech idiopoetyki na marginesie automatycznej klasyfikacji utworów poetyckich i ich parodii*, Biuletyn Polskiego Towarzystwa Językoznawczego 2023, LXXIX (79); 239-257. https://biuletynptj.com/resources/html/article/details?id=617965.

11. Jakub Skłodowski, Piotr Arabas, *Wykorzystanie drzew sufiksowych do efektywnej prezentacji podobieństw sesji z systemu pułapek honeypot*. Cybersecurity and Law, 2023, 1(9); 298-315.http://www.cybersecurityandlaw.com/pdf-169323-92138?filename=Wykorzystanie%20drzew.pdf.

12. Daniel Ziembicki, Karolina Seweryn, Anna Wróblewska, *Polish Natural Language Inference and Factivity – an Expert-based Dataset and Benchmarks*. Natural Language Engineering, 2023, 30(2); 1-32. http://dx.doi.org/10.1017/S1351324923000220.

13. Katarzyna Staciwa, *Wykorzystywanie seksualne dzieci w cyberprzestrzeni z perspektywy sprawcy – kto jest po drugiej stronie ekranu?,* Dziecko Krzywdzone. Teoria, badania i praktyka, vol 22, No 3 (2023), s. 94–113, https://dzieckokrzywdzone.fdds.pl/index.php/DK/article/view/886.

14. Ewa Niewiadomska-Szynkiewicz, Martyna Różycka, Katarzyna Staciwa, Katarzyna Nyczka, *System wspomagający wykrywanie treści wizualnych i tekstowych zagrażających bezpieczeństwu dzieci w cyberprzestrzeni*, Cybersecurity and Law 2023, 10 (2), s. 202–220, https://www.cybersecurityandlaw.com/Author-Katarzyna-Staciwa/250152.

15. Katarzyna Staciwa, The Metaverse, *Online Sexual Exploitation and Sexual Abuse of Children – a new challenge for today's global society?*, Prawo Nowych Technologii, nr 4/2022, s. 45–49.

16. Katarzyna Staciwa, *Krajowa koncepcja rozwiązań systemowych w obszarze zwalczania wykorzystywania seksualnego dzieci*, Problemy Kryminalistyki 314 (4) 2021, s. 18–28, https://clkp.policja.pl/clk/problemy-kryminalistyki/wydania-problemow-kryminalisty/2021/nr-3142021/katarzyna-staciwa-krajowa-kon/229761,Katarzyna-Staciwa-Krajowa-koncepcja-rozwiazan-systemowych-w-obszarze-zwalczania-.html.

17. Piotr Białczak, Wojciech Mazurczyk, *Malware Classification Using Open Set Recognition and HTTP Protocol Requests. In: Tsudik*, G., Conti, M., Liang, K., Smaragdakis, G. (eds) Computer Security – ESORICS 2023. ESORICS 2023. Lecture Notes in Computer Science, vol 14345. Springer, Cham. https://doi.org/10.1007/978-3-031-51476-0_12.

Publikacje pokonferencyjne i rozdziały w książkach

1. Przemysław Błaśkiewicz, Mirosław Kutyłowski, Anna Lauks-Dutka, *Darknet signatures*. 2023 International Conference on Data Security and Privacy Protection (DSPP), 2023; 232-237. https://doi.org/10.1109/DSPP58763.2023.10404582.

2. Dominik Bojko, Jacek Cichoń, Mirosław Kutyłowski, *Sliding Window Sampling over Data Stream – a Solution Based on Devil's Staircases*. 2023 IEEE 10th International Conference on Data Science and Advanced Analytics (DSAA), 2023; 1-9. http://dx.doi.org/10.1109/DSAA60987.2023.10302599.

3. Grzegorz Borowik, Michał Balicki, Michał Kasprzak, Piotr Cukier, *Improved Mesh Processing Using Distorted Pole Spherical Coordinates*. Advances in Systems Engineering, International Conference On Systems Engineering (ICSEng), Lecture Notes in Networks and Systems, vol. 761, red. Henry Selvaraj, Grzegorz Chmaj, Dawid Zydek, Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-40579-2_33.

4. Andrzej Karbowski, Przemysław Jaskóła, *A Markovian Model of Dynamic Cyber Risk Assessment Based on Questionnaires*. International Conference on Signal Processing and Communication Systems (ICSPCS) 2023; 1-6. https://dx.doi.org/10.1109/ICSPCS58109.2023.10261162.

5. Joanna Kołodziej, Mateusz Krzysztoń, Paweł Szynkiewicz, *Anomaly Detection in TCP/IP Networks. Communications of the ECMS, 37th Proceedings (ECMS)*, red. Enrico Vicario, Romeo Bandinelli, Virginia Fani, Michele Mastroianni, 2023, 37(1). https://doi.org/10.7148/2023-0542.

6. Mateusz Krzysztoń, *Weryfikacja wiarygodności systemów w erze uczenia maszynowego*. W: *Cyberbezpieczeństwo AI. AI w cyberbezpieczeństwie*, red. Aleksandra Szczęsna, Monika Stachoń, Warszawa: NASK-PIB, 2023: 45–58.

https://cyberpolicy.nask.pl/wp-content/uploads/2023/09/Cyberbezpieczenstwo-AI.-AI-w-cyberbezpieczenstwie.pdf.

7. Mirosław Kutyłowski, Giuseppe Persiano, Duong Hieu Phan, Moti Yung, Marcin Zawada, *Anamorphic Signatures: Secrecy from a Dictator Who Only Permits Authentication*. Advances in Cryptology (CRYPTO), Lecture Notes in Computer Science, vol. 14082, red. Helena Handschuh, Anna Lysyanskaya, Springer, Cham, 2023.; 759-790. https://doi.org/10.1007/978-3-031-38545-2_25.

8. Mirosław Kutyłowski, Giuseppe Persiano, Duong Hieu Phan, Moti Yung, Marcin Zawada, *The Self-Anti-Censorship Nature of Encryption: On the Prevalence of Anamorphic Cryptography*. Privacy Enhancing Technologies Symposium 2023; 170-183. https://doi.org/10.56553/popets-2023-0104.

9. Inez Okulska, Emilia Wiśnios, *Towards Harmful Erotic Content Detection through Coreference-Driven Contextual Analysis*. Proceedings of The Sixth Workshop on Computational Models of Reference, Anaphora and Coreference (CRAC), red. Maciej Ogrodniczuk, Vincent Ng, Sameer Pradhan, Massimo Poesio, Association for Computational Linguistics; 2023; 59-70. 10.18653/v1/2023.crac-main.8.

10. Daria Stetsenko, Inez Okulska, *The Grammar and Syntax Based Corpus Analysis Tool For The Ukrainian Language*. Communication Papers of the 18th Conference on Computer Science and Intelligence Systems, red. Maria Ganzha, Leszek Maciaszek, Marcin Paprzycki, Dominik Ślęzak. Annals of Computer Science and Information Systems 2023, 37; 303–311 http://dx.doi.org/10.15439/2023F7698.

11. Giuseppe Stragapede et al. (Weronika Gutfeter, Adam Baran, Mateusz Krzysztoń, Przemysław Jaskóła), *IEEE BigData 2023 Keystroke Verification Challenge (KVC)*. 2023 IEEE International Conference on Big Data (BigData), 2023; 6092-6100. https://dx.doi.org/10.1109/BigData59044.2023.10386557.

12. Piotr Szuster, Joanna Kołodziej, *Convective cells algorithm for storm data tracking*. Communications of the ECMS, 37th Proceedings (ECMS), red. Enrico Vicario, Romeo Bandinelli, Virginia Fani, Michele Mastroianni, 2023, 37(1). http://dx.doi.org/10.7148/2023-0535.

13. Joanna Wojciechowska, Mateusz Odrowaz-Sypniewski, Maria W. Smigielska, Igor Kaminski, Emilia Wiśnios, Bartosz Pieliński, and Hanna Schreiber. 2023. Deep Dive into the Language of International Relations: NLP-based Analysis of UNESCO's Summary Records. In *Proceedings of the 3rd Workshop on Computational Linguistics for the Political and Social Sciences*, pages 75–87, Ingolstadt, Germany. Association for Computational Lingustics.

14. Anna Wróblewska, Bartosz Pieliński, Karolina Seweryn, Sylwia Sysko-Romańczuk, Karol Saputa, Aleksandra Wichrowska, Hanna Schreiber, *Automating the Analysis of Institutional Design in International Agreements*. Computational Science – ICCS 2023, Lecture Notes in Computer Science, vol. 10475, red. Jiří Mikyška, Clélia de Mulatier, Maciej Paszynski, Valeria V. Krzhizhanovskaya, Jack J. Dongarra, Peter M.A. Sloot, Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-36024-4_5.

3.4. Współpraca instytucjonalna i międzynarodowa

Wysoka aktywność NASK-PIB w przedsięwzięciach krajowych i międzynarodowych skutkuje licznymi owocnymi kontaktami. Instytut nawiązał lub kontynuował współpracę z wieloma instytucjami i organizacjami (blisko 100) w ramach realizowanych projektów, wspólnych przedsięwzięć (nie tylko o charakterze naukowym), organizowanych wydarzeń na rzecz popularyzacji nauki oraz wiedzy o cyberbezpieczeństwie – m.in. organami administracji publicznej (samorządy, ministerstwa i inne), ośrodkami akademickimi i instytutami naukowymi, w tym zagranicznymi oraz wieloma stowarzyszeniami, izbami, fundacjami i innymi organizacjami, a także placówkami oświatowymi i mediami. Ponadto pracownicy NASK-PIB są członkami i przewodniczą kapitułom konkursowym, komitetom, radom programowym wielu konferencji oraz wydawnictw naukowych. W tym rozdziale zostaną przedstawione wybrane przedsięwzięcia, w których udział brał NASK-PIB:

MIT

W 2023 roku, w ramach współpracy pomiędzy NASK-PIB a MIT. w MIT w Computer Science & Artificial Intelligence Laboratory, z wykładami wystąpili Konrad Ciecierski oraz Mateusz Koryciński. Wykład Konrada Ciecierskiego „AI in medicine, applications in Deep Brain Stimulation", wykład Mateusza Korycińskiego „HyTract: A Hybrid Method for Tractography in Preoperative Planning".

UTS

W 2023 roku NASK-PIB nawiązał współpracę z University of Technology Sydney, która zaowocowała kilkudniowymi warsztatami w Behavioral Data Science lab w Sydney pod kierunkiem prof. Mariana-Andreia Rizoiu. Wymiana myśli i doświadczeń związana była z detekcją treści szkodliwych, mową nienawiści i strukturą anotacji danych. Badacze z UTS podzielili się m.in. swoim anotowanym zbiorem danych do wykrywania treści szkodliwych i mowy nienawiści w anglojęzycznych tweetach osób publicznych.

NATO NCIA

W 2023 roku NASK-PIB realizował prace badawcze w ramach współpracy z agencją NATO NCIA dotyczące lekkich schematów kryptografii postkwantowej w ramach zlecenia "Lightweight Post Quantum Security Schemes: Applicability to Underwater Scenario".

GCA (Global Cyber Alliance)

W 2023 roku była kontynuowana współpraca z Global Cyber Alliance. W ramach współpracy pozyskano dostęp do danych, które są wykorzystywane przez CBiR i CERT.

Shadowserver

Kontynuacja współpracy z Fundacją Shadowserver mająca na celu pozyskanie dostępu do danych z sieci honeypotów oraz wspólnych przedsięwzięć badawczych.

NIO PIB

W 2023 roku kontynuowano stałą współpracę naukową z Kliniką Nowotworów Układu nerwowego w Narodowym Instytucie Onkologii PIB. Pracownicy NASK-PIB (Konrad Ciecierski oraz Mateusz Koryciński) występowali na seminariach naukowych w Klinice Nowotworów Układu Nerwowego w NIO. W ramach stałej współpracy z NIO PIB Konrad Ciecierski jest członkiem zespołu operacyjnego przeprowadzającego operacje neurochirurgicznego leczenia choroby Parkinsona oraz dystonii.

UAM

NASK-PIB współuczestniczył w pracach nad wdrożeniem aplikacji INKAH (Internetowe Narzędzie do Kolaboratywnej Animacji i Hipertekstu) powstającej w ramach projektu Dariah.lab obejmującego nową infrastrukturę cyfrową dla humanistyki i nauk o sztuce na Uniwersytecie im. Adama Mickiewicza w Poznaniu. Narzędzie INKAH umożliwia tworzenie, odczyt oraz wizualizację kolektywnie tworzonego hipertekstu z możliwością badawczej analizy aktywności grup autorów.

EAB

NASK-PIB kontynuował swoją działalność na polu badań biometrycznych w organizacji EAB.

Makroklaster

Makroklaster to inicjatywa, która ma zapewnić poprawę bezpieczeństwa publicznego. Podmioty zrzeszone w Makroklastrze, reprezentujące środowiska nauki, przemysłu i administracji, współpracują w celu wzmocnienia bezpieczeństwa w przestrzeni społecznej, cyberprzestrzeni, środowisku naturalnym oraz infrastrukturze technicznej i energetycznej. NASK-PIB jest jednym z członków-założycieli Makroklastra.

Konsorcjum PLLuM

Pod koniec 2023 roku NASK-PIB wspólnie z Politechniką Wrocławską (lider), Ośrodkiem Przetwarzania Informacji Państwowym Instytutem Badawczym, Instytutem Podstaw Informatyki PAN, Uniwersytetem Łódzkim oraz Instytutem Slawistyki PAN zawiązał konsorcjum naukowe PLLuM. Celem konsorcjum jest realizacja projektu otwartego polskiego dużego modelu językowego.

CBZC (Centralne Biuro Zwalczenia Cyberbezpieczeństwa)

Porozumienie z CBZC podpisane 29 września 2023 roku pieczętuje istniejącą roboczą współpracę między instytucjami, realnie przyczyniając się do poprawy stanu cyberbezpieczeństwa w Polsce. Współpraca, o której mowa w porozumieniu ma być realizowana poprzez wymianę informacji o technikach i sposobach działań przestępców, a także skali ich występowania w zakresie spraw obsługiwanych przez CSIRT NASK, o ile nie są one objęte żadną ze znanych NASK-PIB tajemnic prawnie chronionych, wymianę doświadczeń i pomysłów w tworzeniu oraz użytkowaniu technologii informatycznych – sprzętowych i programowych oraz nieodpłatne użyczenie technologii informatycznych – sprzętowych i programowych, wspomagających pracę funkcjonariuszy

i pracowników CBZC. Ponadto obejmuje realizację wspólnych projektów i przedsięwzięć związanych ze zwalczaniem cyberprzestępczości, działaniami prewencyjnymi oraz szkoleń, a także podejmowanie wspólnych projektów edukacyjnych, profilaktycznych oraz informacyjnych, wynikających z bieżących potrzeb.

CENTR, ICCAN

Współpraca międzynarodowa w ramach CENTR (Council o European National Top-Level Domain Registries) oraz ICANN (Internet Corporation for Assigned Names and Numbers) dotyczy zaangażowania w prace grup roboczych, realizacji międzynarodowych inicjatyw i projektów z zakresu DNS oraz wymiany doświadczeń.

4. Cyberbezpieczeństwo i cyfryzacja

4.1. CSIRT NASK

Rola CSIRT NASK

Zgodnie z zapisami ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa NASK-PIB pełni funkcję CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym. CSIRT NASK prowadzi działania na poziomach:

- operacyjnym,
- analitycznym,
- badawczo-rozwojowym,
- informacyjno-edukacyjnym,

a także realizuje zadania wspierające oraz zadania z zakresu współpracy z innymi organami.

Monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym

Obsługa zgłoszeń, klasyfikacja incydentów oraz reagowanie odbywają się przez 24 godziny, 7 dni w tygodniu, przez 365 dni w roku. CSIRT NASK udziela również odpowiedzi na zapytania ze strony organów ścigania oraz wymiaru sprawiedliwości na temat zarejestrowanych incydentów lub analizowanych spraw.

W okresie od 1 stycznia do 31 grudnia:

Liczba raportów dobowych: **365**

Liczba raportów z analizy źródeł otwartych i wewnętrznych systemów CERT Polska: **126**

Liczba raportów tygodniowych CSIRT NASK: **51**

Klasyfikacja oraz obsługa incydentów

Od 1 stycznia do 31 grudnia 2023 r. CSIRT NASK zarejestrował **371 089** zgłoszeń oraz obsłużył aż **80 267** incydentów bezpieczeństwa. Wśród obsłużonych incydentów dominującą kategorią zagrożeń był phishing (oszustwa komputerowe).

TOP 10 Liczba incydentów w podziale na sektory gospodarki – 2023 roku.

Sektor gospodarki	Liczba incydentów
Handel hurtowy i detaliczny	19 253
Infrastruktura rynków finansowych	18 943
Media	10 191
Energetyka	9 196
Poczta i usługi kurierskie	5 319
Infrastruktura cyfrowa	5 101
Bankowość	2 481
Produkcja	2 353
Administracja publiczna	2 234
Osoby fizyczne	2 105

Tabela. Incydenty obsłużone przez CERT Polska w 2023 r. w podziale na sektory gospodarki (Top 10).

Rodzaje zagrożeń – 2023 roku.

Typy incydentów	Liczba incydentów
Oszustwa komputerowe	75 917
Szkodliwe oprogramowanie	1 650
Podatne usługi	964
Obraźliwe i nielegalne treści	584
Włamania	418
Dostępność zasobów	385
Próby włamań	205
Atak na bezpieczeństwo informacji	59
Inne	56
Gromadzenie informacji	29
Razem	**80 267**

Tabela . Incydenty obsłużone przez CERT Polska w 2023 roku w podziale na kategorie wg taksonomii eCSIRT.net mkVI.

Ustawa z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (UoKSC) reguluje kwestie związane ze zgłaszaniem incydentów poważnych, incydentów istotnych oraz incydentów w podmiocie publicznym do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. Liczba incydentów zgłoszonych w 2023 roku do CSIRT NASK została podana w poniższej tabeli.

Rodzaj incydentów	Liczba incydentów
Incydenty poważne	40
Incydenty istotne	0
Incydenty w podmiotach publicznych	2 184

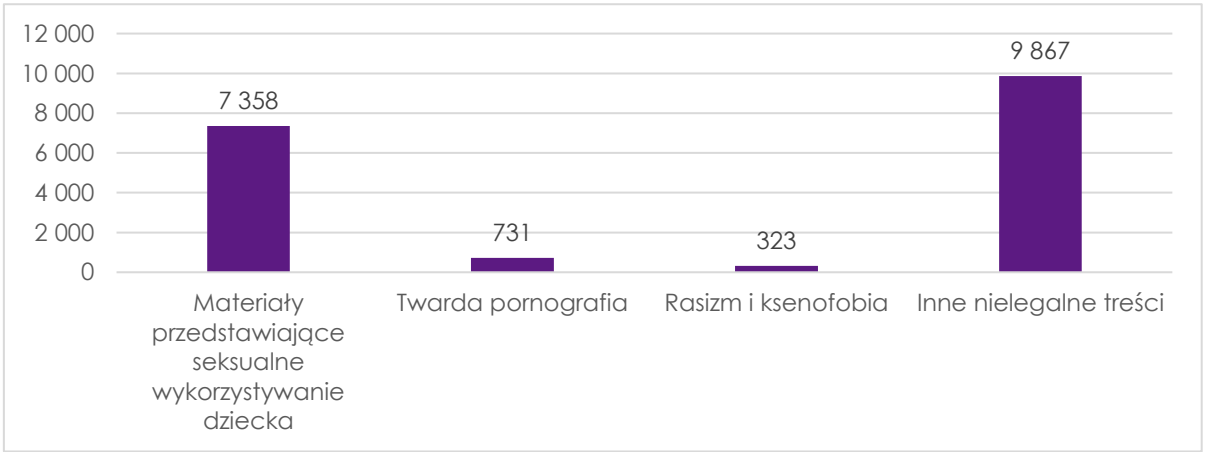
Tabela . Incydenty zgłaszane ustawowo do CERT Polska w 2023 roku.

Monitorowanie treści nielegalnych

DYŻURNET.PL

Oddzielną grupę stanowią incydenty związane z publikacją w internecie potencjalnie nielegalnych treści w, w szczególności chodzi o materiały przedstawiające seksualne wykorzystywanie dzieci lub inne szkodliwe treści skierowane przeciwko bezpieczeństwu małoletnich. Tego typu zagrożenia obsługiwane są przez zespół Dyżurnet.pl.

W 2023 roku Dyżurnet.pl obsłużył ponad **18 tys.** zgłoszeń, w tym aż **7 358** z kategorii CSAM, czyli materiałów zawierających pornografię dziecięcą, **731** zgłoszeń twardej pornografii, **323** zgłoszenia incydentów na tle rasistowskim i ksenofobicznym i aż **9 867** zgłoszeń dotyczących innych nielegalnych i szkodliwych treści.



Wykres . Liczba zgłoszeń otrzymanych przez Dyżurnet.pl – rodzaj potencjalnie nielegalnych treści (N=18 279).

Po przeprowadzeniu analizy treści 2 130 incydentów przekazano do innego zespołu hotline zrzeszonego w INHOPE, 300 incydentów do administratorów serwisu, 109 do dostawców usług (ISP), 4 do właściciela treści, 13 do innych instytucji/organizacji oraz 142 do policji.

Portal n6

przetworzył: **1 342 mln** zdarzeń bezpieczeństwa

90 mln zdarzeń dotyczących polskich sieci

1 265 uczestników platformy

Informowanie o zagrożeniach

Ostrzeżenia, rekomendacje, analizy publikowane są na stronie CERT Polska oraz w mediach społecznościowych, m.in.: Facebook, X (d. Twitter) oraz LinkedIn. Liczba publikacji w mediach społecznościowych w 2023 roku:

- w serwisie Facebook – **114**
- w serwisie X (d. Twitter) – **176**
- w serwisie LinkedIn – **118**

Poszukiwanie nowych podatności oraz wysyłanie ostrzeżeń i rekomendacji

W 2023 roku CERT Polska przekazał ostrzeżenia i informacje m.in. o:

- — podatnościach,
- — możliwych atakach DDoS,
- — przejętych dostępach w systemach,
- — błędach w konfiguracji stron internetowych,
- — wystawionych panelach logowania do usług wewnętrznych,
- — przejętych skrzynkach pocztowych,
- — wyciekach danych uwierzytelniających.

Zarządzanie wiedzą i raportowanie

Informacje na temat działalności CSIRT NASK oraz analizy dotyczące danych zgromadzonych i przetwarzanych przez CSIRT NASK zawarte są m.in. w sprawozdaniu z dotacji podmiotowej udzielonej na dofinansowanie CSIRT NASK w 2023 roku, raportach miesięcznych dla Pełnomocnika Rządu ds. Cyberbezpieczeństwa, a także innych zestawieniach wspomagających proces podejmowania decyzji.

Zwiększanie zasobów otwartych danych

Co tydzień na portalu dane.gov.pl NASK-PIB publikował ogólnodostępne informacje o liczbie incydentów zarejestrowanych oraz obsłużonych przez CERT Polska. Raz na

miesiąc publikowano dane na temat liczby szkodliwych domen wpisanych na listę ostrzeżeń CERT Polska.

Organizacja współpracy z podmiotami KSC

Do działań w tym zakresie można zaliczyć:

1. zarządzanie zgłoszeniami przesyłanymi do CSIRT NASK,

2. przekazywanie informacji dotyczących m.in. incydentów podmiotom krajowego systemu cyberbezpieczeństwa,

3. realizację zadań związanych z przystąpieniem jednostek samorządu terytorialnego do komunikatora Threema OnPrem,

4. wspieranie współpracy merytorycznej między podmiotami w celu budowania potencjału i zdolności w zakresie cyberbezpieczeństwa,

5. utworzenie Zespołu Cyberbezpieczeństwa w Sektorze Zdrowia,

6. udział w realizacji Programu Partnerstwo dla Cyberbezpieczeństwa (PdC).

Budowanie świadomości

Lista ostrzeżeń

W 2023 roku na listę ostrzeżeń CERT Polska trafiło ponad **79 tys.** domen, które prowadziły do 24,6 tys. różnych adresów IP lub które wskazywały na 24,6 tys. adresów IP. W praktyce oznacza to zablokowanie ok. **54 mln** prób wejścia na niebezpieczne strony z listy ostrzeżeń. Natomiast liczba zapytań o zawartość listy ostrzeżeń wysłanych do serwerów CERT Polska wyniosła w 2023 roku ok. **191 mln**.

Zgłoszenia SMS-ów

W 2023 roku liczba zgłoszeń fałszywych SMS-ów wyniosła: **119,8 tys**.

Współpraca z władzami centralnymi

Dyżurnet.pl

Dyżurnet.pl uczestniczył w pracach Zespołu do spraw przeciwdziałania przestępczości przeciwko wolności seksualnej i obyczajności na szkodę osób małoletnich. Zespół ten został powołany przez Ministra Sprawiedliwości we wrześniu 2021 roku, w celu analizy aktualnych rozwiązań oraz opracowania krajowego planu działania w tym obszarze, a także wypracowania propozycji legislacyjnych oraz propozycji zmian systemowych w ww. zakresie.

CERT Polska

W 2023 roku zakończyły się prace nad projektem ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. W zespole roboczym uczestniczyli pracownicy CERT Polska. Rezultatem tych działań jest Ustawa z 28 lipca 2023 roku (Dz. U. poz. 1703) o zwalczaniu nadużyć w komunikacji elektronicznej.

Cyberbezpieczeństwo w gminnych JST

W 2023 roku NASK-PIB przeprowadził badanie nt. poziomu świadomości cyberbezpieczeństwa oraz kompetencji cyfrowych w gminnych jednostkach samorządu terytorialnego. W badaniach łącznie wzięło udział 23 307 pracowników urzędów gmin z całej Polski. Jest to kontynuacja sondażu przeprowadzonego wśród pracowników urzędów powiatowych w 2022 roku.

Artemis

Artemis to narzędzie rozwijane przez zespół CERT Polska, a zapoczątkowane przez członków koła Politechniki Warszawskiej KN Cyber, służące do poszukiwania podatności bezpieczeństwa i błędów konfiguracyjnych stron internetowych. Uzyskane wyniki są niezwłocznie przekazywane administratorom. W ramach ponownych testów zespół CERT Polska sprawdza, czy niezbędne poprawki zostały wdrożone. Weryfikacji podlegają przede wszystkim podmioty znajdujące się w obszarze odpowiedzialności CSIRT NASK.

W 2023 roku łącznie przeskanowano ok. **50,6 tys.** domen i adresów IP oraz ok. **251,7 tys.** subdomen.

Skrócony numer 8080

W listopadzie 2023 roku CERT Polska uruchomił nowy, skrócony numer **8080** do zgłaszania podejrzanych wiadomości SMS. Uruchomienie skróconego numeru było związane z rozpoczęciem obowiązywania ustawy o zwalczaniu nadużyć w komunikacji elektronicznej.

Bezpieczna Poczta

W 2023 roku CERT Polska stworzył serwis **bezpiecznapoczta.cert.pl**, którego celem jest ochrona użytkowników poczty elektronicznej i ułatwienie instytucjom sprawdzenia poprawności konfiguracji mechanizmów podnoszących jej bezpieczeństwo. Serwis jest dostępny publicznie od sierpnia 2023 roku. Od tego czasu użytkownicy sprawdzili za jego pomocą prawie 19 tys. domen, a niemal 8 tys. zostało sprawdzonych więcej niż raz Z serwisu korzystają nie tylko instytucje publiczne, lecz także podmioty prywatne, np. firmy.

Snitch

Dostępność w internecie urządzeń OT/IoT może rodzić poważne konsekwencje dla cyberbezpieczeństwa instytucji, Snitch pozwala automatycznie monitorować taką ekspozycję z wykorzystaniem serwisów Shodan i Zoomeye, a następnie generuje raporty w formie wiadomości e-mail, wyszukuje adres kontaktowy (ang. abuse contact) dla danego adresu IP i wysyła wiadomość.

Platforma MWDB

MWDB to repozytorium informacji na temat złośliwego oprogramowania prowadzone i rozwijane przez CERT Polska. Próbki złośliwego oprogramowania są automatycznie wzbogacane dodatkowymi metadanymi pochodzącymi z wewnętrznych systemów analitycznych. W 2023 roku dodano do repozytorium ponad **300 tys.** próbek złośliwego oprogramowania.

W 2023 roku do projektu MWDB dołączyło **263** analityków z całego świata, a pod koniec roku liczba aktywnych kont wyniosła niemal **1,5 tysięcy.** Projekt jest udostępniany w formule open source.

Aktywność w mediach społecznościowych

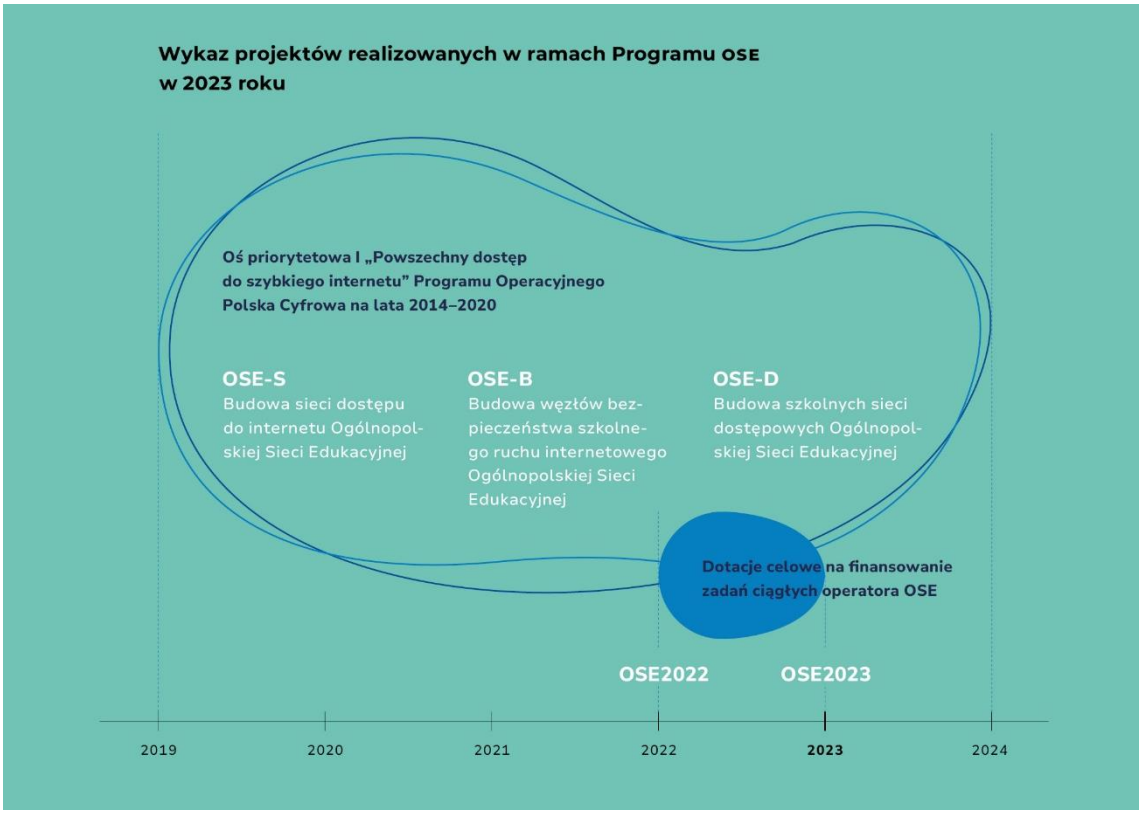
CERT Polska prowadził także działania edukacyjne w mediach społecznościowych. Na szczególną uwagę zasługują systematycznie wydawane ostrzeżenia. Dotyczą one największych kampanii oszustów i są publikowane równolegle na profilach CERT Polska na Facebooku, X (d. Twitter) oraz LinkedInie. Posty przygotowane przez ekspertów CERT Polska docierają nawet do kilkuset tysięcy odbiorców.

Ponadto eksperci z CERT Polska aktywnie działali w społeczności specjalistów

w zakresie cyberbezpieczeństwa, w tym wygłosili ponad 50 prelekcji na ważnych konferencjach branżowych, m.in.: Secure 2023, Confidence, Oh My Hack, Botconf 2023 czy 28th European Symposium on Research in Computer Security oraz uczestniczyli w międzynarodowych konkursach i ćwiczeniach (*patrz rozdział Konferencje i wydarzenia*).

4.2. Ogólnopolska Sieć Edukacyjna (OSE)

W 2023 roku w ramach projektów OSE-S, OSE-B oraz OSE-D realizowane były działania dodatkowe, będące odpowiedzią na nowe potrzeby pojawiające się w trakcie eksploatacji sieci i świadczenia usług OSE. Wykonane zostało podniesienie niezawodności w obszarze styków z siecią dostępową, realizowane na drodze budowy dodatkowych, wyniesionych poza lokalizacje węzłów OSE, punktów wymiany ruchu z operatorami dostarczającymi usługi transmisji danych do szkół. Zrealizowany został również drugi etap ochrony przez atakami DDoS, oparty o rozwiązania FLDX, będące implementacją własnego opatentowanego przez NASK-PIB rozwiązania.

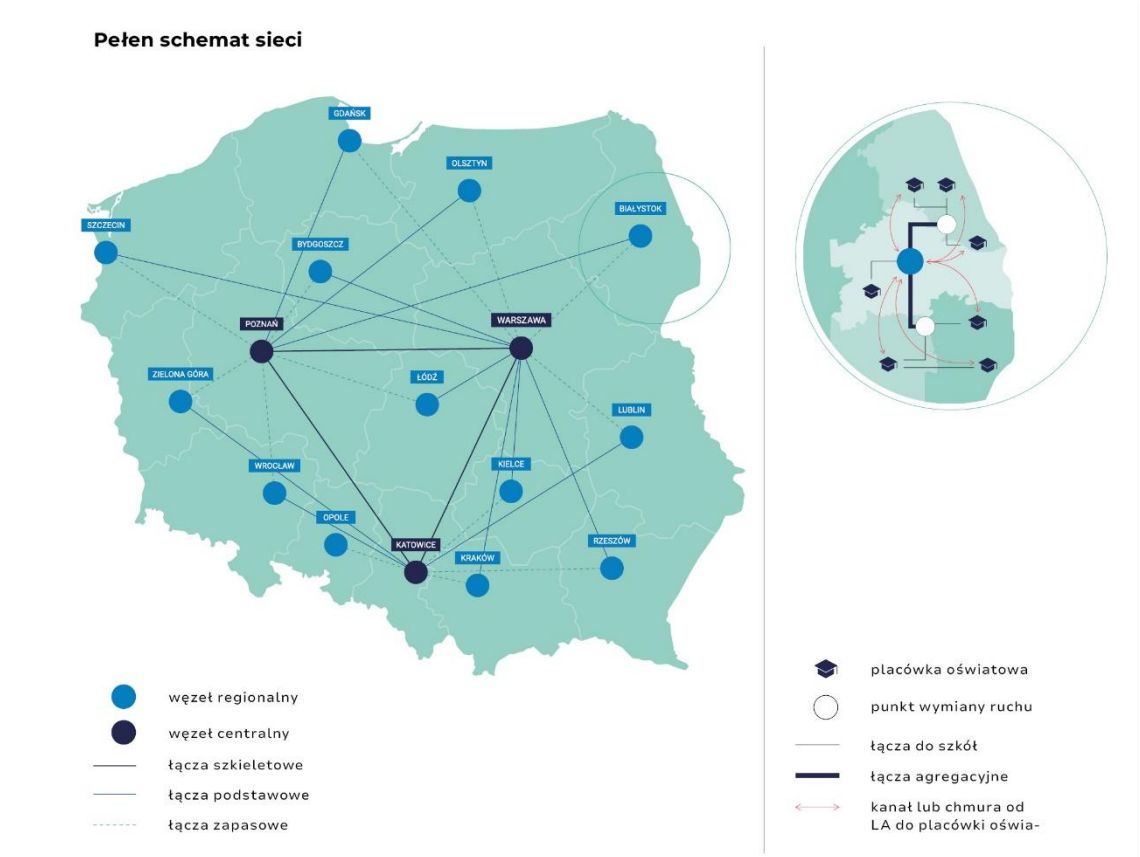


W obszarze usług bezpieczeństwa w 2023 roku zostały udostępnione raporty umożliwiające monitorowanie zachowań uczniów, korzystających z sieci OSE. Każdy dyrektor szkoły korzystający z zaawansowanych usług bezpieczeństwa OSE+ ma dostęp do raportu za okres minionych 30 dni z poziomu portalu MojeOSE.

Wraz z końcem listopada 2023 roku projekty OSE-S i OSE-B, realizowane ze środków POPC zostały zakończone. W ramach ww. projektów powstały węzły w 16 miastach wojewódzkich, które zapewniają możliwość świadczenia usług dla każdej szkoły podstawowej i ponadpodstawowej na terenie Polski. Wybudowana infrastruktura realizuje w pełni przyjęte założenia wydajnościowe i funkcjonalne, świadcząc usługi bezpiecznego i szerokopasmowego dostępu do sieci Internet w szkołach. Wraz z zakończeniem w/w projektów rozpoczął się 5-letni okres trwałości, który stawia przed NASK-PIB wyzwania związane z przedłużaniem wsparcia i odtwarzaniem wybudowanej infrastruktury.

W 2023 roku zakończył się również projekt OSE-D, w ramach którego został między innymi przeprowadzony pilotaż modernizacji szkolnych sieci LAN obejmujący 253 szkoły znajdujące się w 228 lokalizacjach.

Dla każdej ze szkół przeprowadzono indywidualny audyt badający ocenę potrzeb szkoły oraz przygotowano dedykowany projekt techniczny. Prace objęły 3579 sal dydaktycznych.



W szkołach została zmodernizowana infrastruktura kablowa oraz zainstalowano ponad 1800 urządzeń aktywnych (przełączniki i punkty dostępowe sieci WLAN). Wykorzystano ponad 32 000 m przewodu kategorii 6a, ponad 15 000 m światłowodu jednomodowego, 390 szaf RACK i ponad 62 000 m koryt kablowych.

Zainstalowana infrastruktura pasywna jest objęta 25-letnią gwarancją systemową producentów, natomiast urządzenia aktywne podlegają 5-letniej gwarancji.

Budowa szkolnych sieci dostępowych

Stan podłączeń (liczba szkoło-lokalizacji) na koniec 2023 roku przedstawia się następująco:

- każda szkoła w Polsce dla dzieci i młodzieży otrzymała możliwość zgłoszenia się do Programu OSE. Zgłoszenie nie jest obowiązkowe, niemniej jednak większość szkół zdecydowała się przystąpić do OSE;
- na 23,5 tysiąca szkoło-lokalizacji w Polsce (w tym szkoły w wielu lokalizacjach) 20 645 zgłosiło się do OSE (31.12.2023);
- umowę na świadczenie usług OSE zawarły 20 633 szkoły;
- do 31.12.2023 roku wyposażono w sprzęt OSE (OSE jest gotowe do podłączenia szkoły) **20 582** szkoło-lokalizacje. Z usługi OSE korzysta 20 541 szkoło-lokalizacji;

- operator OSE ze względu na brak możliwości technicznych świadczenia usługi docelowej może tymczasowo zastosować do lokalizacji rozwiązanie o obniżonych parametrach (najczęściej są to rozwiązania oparte o technologię LTE);
- 52 szkoło-lokalizacje korzystają z rozwiązania alternatywnego o obniżonych parametrach – te szkoły są systematycznie przełączane na pełną usługę OSE w momencie pojawienia się możliwości technicznych u operatora, który jest beneficjentem przetargu OSE w danej lokalizacji;
- 38 szkoło-lokalizacji korzysta z innej formy rozwiązania alternatywnego. Jest to refinansowanie usługi komercyjnej;
- 20451 szkoło-lokalizacji korzysta z pełnej usługi OSE, szkoły podłączane są do docelowej sieci OSE.

Stan podłączeń (liczba lokalizacji szkół) na koniec 2023 roku

- Pełna usługa OSE: 20451
- Usługa alternatywna: 52
- Refinansowanie: 38
- Pozostało do podłączenia: 92

Utrzymanie sieci OSE w liczbach

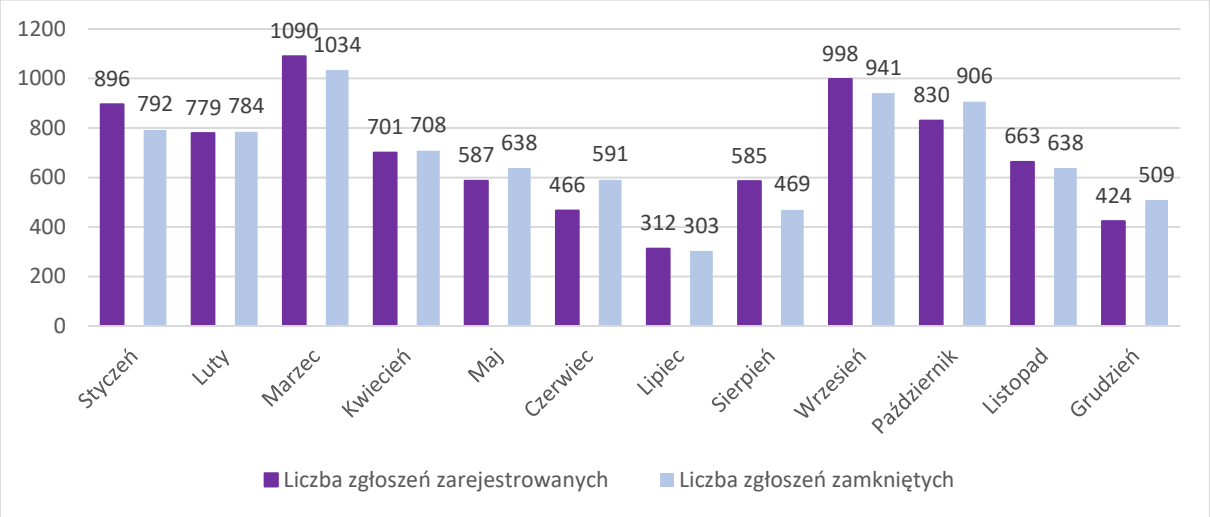
- **537 testów łączy** z operatorami przed uruchomieniem usług OSE w szkołach, 79.5% łączy działających podczas 1 weryfikacji;
- **150 lokalizacji szkolnych** (175 szkół) zostało przepiętych z łączy alternatywnych na docelowe łącza światłowodowe, 35.4% przepięć zostało wykonane metodą zdalnej rekonfiguracji przez pracowników OSE;
- **263 zaopiniowanych dokumentacji** powykonawczych ze szkół, 23.6% dokumentacji kierowanych jest do poprawy przez podwykonawców;
- **8313 obsłużonych zgłoszeń** technicznych ze szkół w procesach utrzymaniowych;
- **627 wizyt służb technicznych** operatora OSE w szkołach (bez techników operatorów trzecich);
- **3769 zgłoszeń** kierowanych do podwykonawców OSE w ramach obsługi serwisowej i gwarancyjnej, z czego 69.1% stanowiły zgłoszenia do operatorów łączy dostępowych;
- **123 zarejestrowanych zdarzeń typu DDOS**: dla 110 z nich uruchomiono mechanizmy oczyszczania ruchu, pozostałe 13 związane były z innymi zdarzeniami jak masowa aktualizacja oprogramowania w szkołach.

Prace rozwojowe w sieci OSE

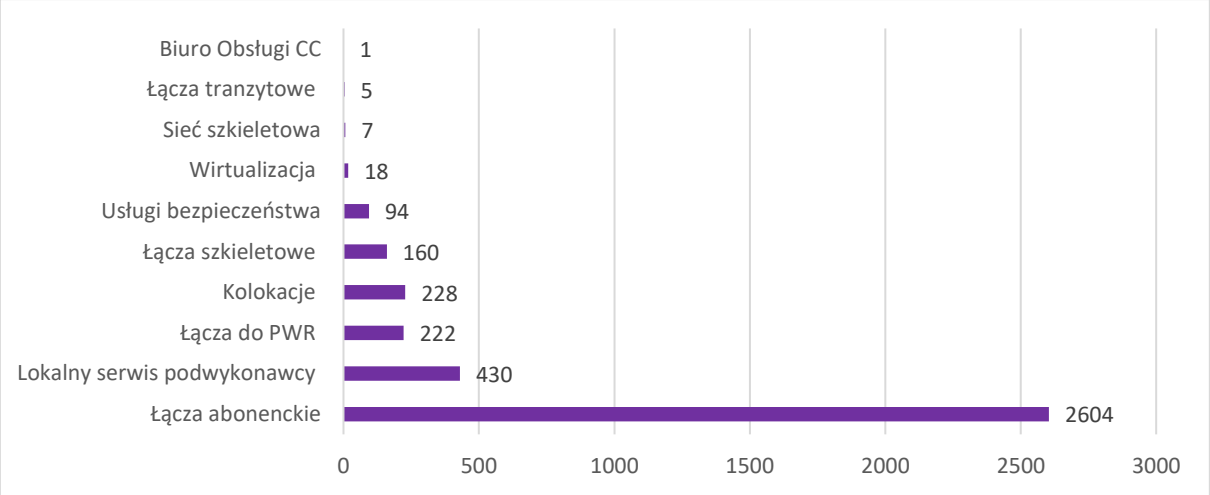
Rozpoczęto proces wymiany 2 300 urządzeń brzegowych w szkołach odpowiadając na rosnące potrzeby szkół w zakresie świadczonych usług.

Zostały również zrealizowane prace w zakresie rozbudowy łączy szkieletowych do 400 Gbps włącznie.

Zgłoszenia techniczne ze szkół



Zgłoszenia wsparcia według rodzaju



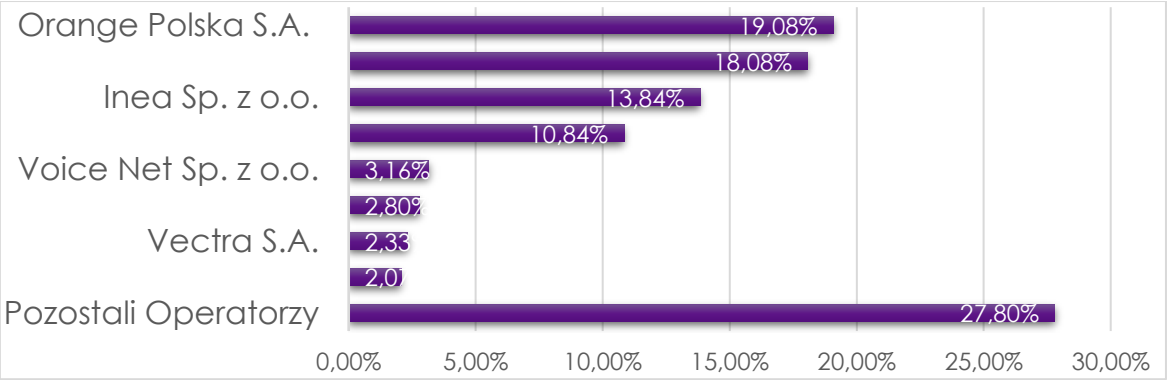
Współpraca z operatorami w zakresie pozyskania łączy na potrzeby OSE

Na koniec 2023 roku Operator OSE miał 521 zawartych umów z przedsiębiorcami telekomunikacyjnymi. Na bieżąco umowy są zmieniane, a zmian dotyczą w głównej mierze zmian administracyjnych adresów, rezygnacji z realizacji usługi w danej lokalizacji ze względu na brak możliwości technicznych, istniejące już usługi spełniające parametry usługi OSE lub likwidację szkoły pod danym adresem.

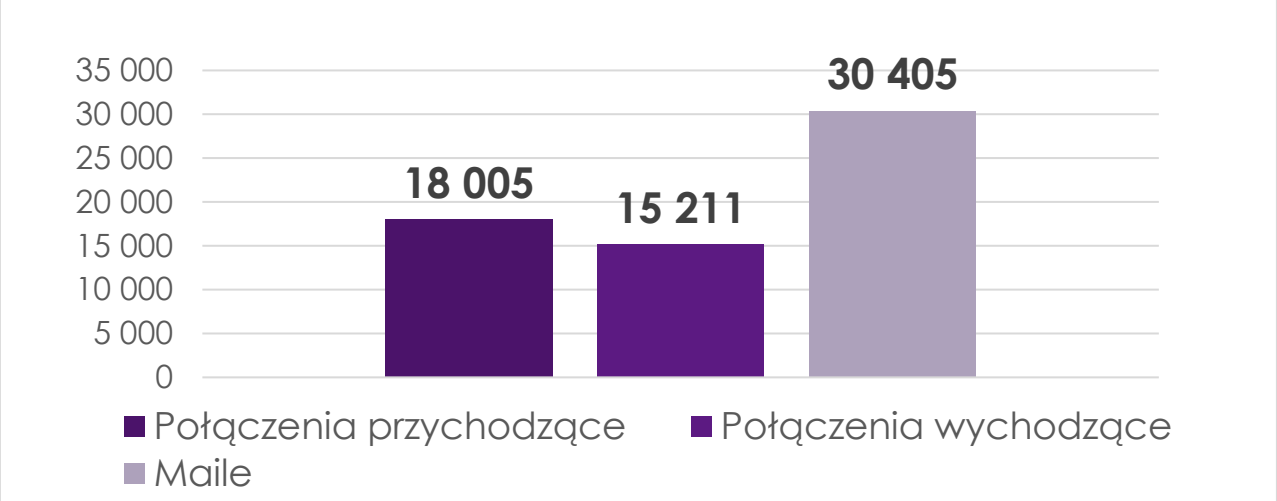
W 2023 roku w zakresie łączy dostępowych do szkół przeprowadzono 18 postępowań, zawarto 39 umów, w ramach obsługi umów podpisano 308 aneksów.

W zakresie łączy szkieletowych w wyniku wyboru najkorzystniejszych ofert podpisano z operatorami telekomunikacyjnymi 8 umów. W ramach podniesienia jakości świadczonych usług OSE rozstrzygnięto 6 postępowań na redundancyjne połączenia dla punktów styku sieci OSE z operatorami. Podpisano 8 umów. Kontynuacja tego zadania będzie prowadzona w 2024 roku.

Udział Operatorów w Programie OSE



OSE: obsłużone kontakty: 63 621; 96% skuteczności



Pozostałe projekty: obsłużone 75 845 kontaktów – 59891 połączenia, 17 954 maile.

ESA

- Połączenia: **3 420** /Maile: **1 735**

S46

- Połączenia: **512** /Maile: **537**

Cyberbezpieczny Samorząd

- Połączenia: **4 614**

Laptop Dla Ucznia

- Połączenia: **16 122**/Maile: **12 943**

LAN

- Połączenia: **305**

Niebieska Linia

- Połączenia: **9 538**

mOchrona

- Połączenia **77**/Maile: **52**

mLegitymacja

- Połączenia: **1 561**/Maile: **1 187**

CERT

- Połączenia: **2 737**

Kariera jutra

- Połączenia: **3 566**

Outbound

- Połączenia: **15 439**

PKC

- Maile: **1 500**

Inne przedsięwzięcia

Program Laptop dla Ucznia

NASK-PIB wspierał działania Centrum Rozwoju Kompetencji Cyfrowych w programie Laptop dla ucznia. W ramach działań zleconych NASK-PIB prowadziło obsługę zgłoszeń poprzez infolinię, uruchomiono portal wspierający użytkowników końcowych w zakresie eksploatacji, prowadzono kampanii marketingowych w mediach oraz zrealizowano proces relokacji laptopów wraz z obsługą magazynu sprzętu.

W trakcie trwania programu NASK-PIB dodatkowo przejął obsługę kontaktów z Organami Prowadzącymi Szkoły, w tym podpisywanie aneksów i umów. Duża skala rozbieżności w liczbach dostarczanych laptopów w stosunku do potrzeb spowodowało konieczność większego niż zakładano relokowania laptopów. Działania związane z relokacją będą kontynuowane w 2024 roku.

Do końca 2023 roku obsłużono łącznie 3117 zgłoszeń, w tym:

- nadmiary: 2020 zgłoszeń (łączna liczba 13449 laptopów),
- niedobory: 1097 zgłoszeń (łączna liczba 3677 laptopów),
- odebrano od OPS: 2817 laptopów,
- wysłano do OPS: 1953,
- podpisano 76 aneksów z OPS w związku z nadmiarami,
- podpisano 481 aneksów z OPS w związku z niedoborami.

Dodatkowo Eksperci OSE, w ramach programu „Laptop dla ucznia", przeprowadzili 7 warsztaty dla uczniów klas 4 szkół podstawowych, dotyczące zagadnień związanych ze szkodliwym korzystaniem z internetu i urządzeń cyfrowych.

4.3. Elektroniczne Zarządzanie Dokumentacją (EZD)

W 2023 roku osiągnięto wskaźniki założone w realizowanych projektach, w tym m.in.:

- **1226 podmiotów**
  przygotowanych do produkcyjnego uruchomienia EZD
  (737 podmioty – EZD RP, 489 podmioty – EZD PUW)
- **1127 szkoleń**
  zrealizowanych w jednostkach administracji publicznej
  (stacjonarnie: 737, on-line: 392)
- **95 402 uczestników szkoleń**
  zrealizowanych dla podmiotów wdrażających i użytkujących EZD
  (stacjonarnie: 13 935, on-line: 81 467)
- **54 000 użytkowników Demo EZD RP**
  usługa uruchomiona w połowie 2023 roku
  (do końca roku odnotowano 575 000 wyświetleń)
- **18 konferencji**
  na których eksperci NASK-PIB prezentowali i promowali system EZD RP

- **4 nowe wersje systemu**
  udostępnione wydania EZD RP oznaczone v.14, 15, 17, 19
- **4 nowe moduły**
  dodane funkcje: dziennik zdarzeń, chmurowy podpis cyfrowy, kolektor statystyk, obserwacje poprawności działania aplikacji.

Głównym celem działań skupionych wokół EZD RP – nowego, bezpłatnego systemu do elektronicznego zarządzania dokumentacją – jest cyfryzacja instytucji publicznych i tym samym zwiększanie transparentności, efektywności i jakości funkcjonowania podmiotów polskiej administracji rządowej i samorządowej.

Zrealizowane projekty

W 2023 roku system EZD RP rozwijany, wdrażany i utrzymywany był w ramach **dwóch kolejno realizowanych projektów**:

- Projekt **„Rozwój, wdrażanie i upowszechnianie systemu do elektronicznego zarządzania dokumentacją w podmiotach publicznych – Operator EZD" [EZDRP-OPERATOR]**
  Zadanie zlecone przez Ministra Cyfryzacji na podstawie Umowy dotacji celowej nr 3/DZS/2022/NASK z dnia 16.12.2022 r.
  Czas trwania projektu: 01.03.2022 r. do 31.03.2023 r.
- Projekt **„Upowszechnianie elektronicznego zarządzania dokumentacją w podmiotach publicznych (systemy EZD PUW i EZD RP) oraz nowe funkcje systemu EZD RP [akronim: EZD-POPC]"**
  Projekt EZD-POPC był dofinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz środków budżetu państwa w ramach II Osi priorytetowej „E-administracja i otwarty rząd" Programu Operacyjnego Polska Cyfrowa 2014-2020; umowa nr POPC.02.02.00-00-0046/23-00 z dnia 16.11.2023 r.
  Czas trwania projektu: od 01.04.2023 r. do 31.12.2023 r.

W ramach zadań zrealizowano działania mające na celu zwiększanie dostępności EZD RP, optymalizację wymagań sprzętowych, zwiększanie liczby funkcji systemu (m.in. dostosowywanie do zmieniającego się prawa, integracje z narzędziami wspierającymi e-administrację, reagowanie na potrzeby zgłaszane przez użytkowników) oraz usuwanie błędów zidentyfikowanych przez zespół NASK-PIB, oraz użytkowników EZD RP. W 2023 roku zostały udostępnione cztery nowe wersje systemu EZD RP oraz łącznie zaimplementowano w nich cztery nowe moduły funkcjonalne.

Istotną kwestią było utrzymanie i zapewnianie ciągłego dostępu do EZD RP w formule Software as a Service na wybudowanej infrastrukturze chmurowej na rzecz administracji rządowej i urzędów centralnych. W tym celu realizowane były zadania związane z administrowaniem infrastrukturą serwerową i sieciową, środowiskiem uruchomieniowym

aplikacji (klastry Kubernetes) oraz administrowaniem systemami bezpieczeństwa klasy UTM/NGFW.

Podejmowane przedsięwzięcia były kontynuacją działań w obszarach upowszechniania standardów w zakresie elektronicznego zarządzania dokumentacją oraz podnoszenia kompetencji pozwalających na cyfryzację procesów i procedur back office dla administracji rządowej.

Dostarczanie Usług wsparcia i materiałów edukacyjnych

W 2023 roku na rzecz Partnerów EZD świadczone były usługi **wsparcia szkoleniowego, wdrożeniowego oraz utrzymaniowego**. W tym czasie z pomocy we wdrożeniach skorzystało ponad 2000 podmiotów realizujących zadania publiczne. Efektem działań było uruchomienie produkcyjne systemu lub przygotowanie do finalizacji wdrożeń w pierwszych dniach kolejnego roku, w ponad 1200 podmiotach.

Równocześnie w ramach działań związanych z tworzeniem i udostępnianiem treści edukacyjnych i informacyjnych dla użytkownikówzaktualizowano 95,8% treści w Podręczniku użytkownika EZD RP (253 opisów realizacji zadań), rozbudowano Portal EZD RP, udostępniono 52 filmy edukacyjne oraz 2 kursy e-learningowe na platformie Ministerstwa Cyfryzacji (szkolenia.gov.pl). W listopadzie 2023 roku uruchomiono Forum użytkowników EZD RP – platformę dyskusyjną przeznaczoną do dzielenia się wiedzą i umiejętnościami związanymi z systemem elektronicznego zarządzania dokumentacją.

Pilotaż dla Dostawców SaaS EZD RP

W pierwszej połowie 2023 roku zrealizowany został pilotaż z udziałem podmiotów zainteresowanych świadczeniem SaaS EZD RP. Wzięło w nim udział 13 organizacji, z którymi podpisano listy intencyjne. Celem działania było nabycie przez podmioty trzecie umiejętności udostępniania systemu EZD RP w postaci usługi chmurowej. W ramach pilotażu wypracowano dobre praktyki i rekomendacje m.in. w zakresie bezpieczeństwa, a także zweryfikowano instrukcje instalacji i inne materiały edukacyjne EZD RP.

Integracjach aplikacji firm trzecich z EZD RP

W 2023 roku kontynuowana była współpraca z producentami oprogramowania w ramach tzw. Piaskownicy API EZD RP. Łącznie do końca roku podmioty trzecie przedstawiły osiem aplikacji zintegrowanych z EZD RP.

Automatyzacja procesów w EZD RP

W 2023 roku rozpoczęto prace wspierające cyfryzację procesów wewnętrznych NASK-PIB z wykorzystaniem automatyzacji procesów i technik low-code. Uruchomiono środowiska pełniące rolę szyny danych. Zintegrowano referencyjne źródła danych (JIRA, M365, TETA) z EZD RP w NASK-PIB. Pilotaż w zakresie wsparcia prac zespołów EZD RP dotyczył wykorzystania sztucznej inteligencji do usprawnienia obsługi zgłoszeń od użytkowników systemu (np. integracja LLM z systemami obsługowymi, CRM).

4.4. Ośrodek Standaryzacji i Certyfikacji (OSIC)

Ośrodek Standaryzacji i Certyfikacji odpowiada za działalność akredytowanej Jednostki Certyfikującej NASK-PIB i wykonuje certyfikację wyrobów (produktów) IT w obszarze bezpieczeństwa informatycznego (cyberbezpieczeństwa). Pion odpowiada jednocześnie za prace normalizacyjne (współpracę z instytucjami standaryzacyjnymi) oraz rozwój Laboratorium Badawczo-Eksperymentalnego AI/IT.

Pion OSiC prowadzi prace badawczo-rozwojowe w zakresie metod oceny zgodności i certyfikacji w obszarze cyberbezpieczeństwa i sztucznej inteligencji poprzez prowadzenie i udział w projektach badawczo-rozwojowych (m.in. kieruje projektem CyberBEAM, uczestniczy(ł) w projektach OptoCrypt, 5G-TACTIC, EPW).

Eksperci OSIC biorą udział w pracach grup roboczych, komitetów zarządzających i technicznych w ramach inicjatyw krajowych i międzynarodowych. Poddawane są analizie, komentowane i współtworzone dokumenty kryterialne stanowiące podstawę do oceny zgodności; w tym krajowe, europejskie oraz publikowane przez Państwa Członkowskie UE oraz kraje związane umowami partnerskimi i konsorcjami (m.in. USA, Kanada, Japonia).

Jednostka Certyfikująca autoryzuje i nadzoruje działalność laboratoriów badawczych wykonujących ocenę w ramach Programu oceny i certyfikacji bezpieczeństwa IT.

Nowe zrealizowane inicjatywy pionu OSiC w roku 2023 to m.in. uruchomienie we współpracy z Ministerstwem Rozwoju i Technologii programu edukacji i certyfikacji „Firma Bezpieczna Cyfrowo" skierowanego do sektora MŚP, dołączenie NASK-PIB do grona pełnoprawnych uczestników ETSI (europejska instytucja normalizacyjna). Rozpoczęto prace rozwojowe nad programem certyfikacji osób zajmujących się CSAM, przeciwdziałaniem dezinformacji w sieci. Zainicjowano program certyfikacji dla kadry zarządzającej podmiotami Krajowego Systemu Cyberbezpieczeństwa.

4.5. Przeciwdziałanie dezinformacji

W ramach realizowanej dotacji celowej przygotowano 247 raportów porannych i 247 raportów popołudniowych wysyłanych bezpośrednio do KPRM. W okresie 01.01-31.12.2023 przygotowano 44 raporty tygodniowe w języku polskim i języku angielskim. W tym samym okresie opracowano 33 analizy problemowe, które przetłumaczono na język angielski. W 2023 roku zespół przygotował również 20 raportów specjalnych, wynikających z bieżących wydarzeń i obserwowanych wzrostów w liczbie publikacji szkodliwych.

W ramach dodatkowych zadań, przygotowano 86 raportów na temat dezinformacji zagranicznej: chińskiej, niemieckiej i rosyjskiej.

W kwietniu 2023 roku grono sygnatariuszy Kodeksu Dobrych Praktyk powiększyło się o kolejne podmioty: Fundacja "Przeciwdziałamy Dezinformacji", Instytut Kościuszki, Centrum

Badań nad Współczesnym Środowiskiem Bezpieczeństwa, Wojownicy Klawiatury (Fundacja Geremka).

W okresie lipiec- grudzień 2023, równolegle do zadań w projekcie DEEPMNTRNG, prowadzono prace w projekcie OKW23 i serwisie www.bezpiecznewybory.pl. Projekt realizowany był z inicjatywy Działu Przeciwdziałania Dezinformacji we współpracy z CERT Polska oraz partnerami: Google, Meta i TikTokiem. W weekend wyborczy 13-15 października 2023 roku wpłynęło 214 zgłoszeń materiałów o potencjale dezinformacyjnym. Ponadto w ramach bieżącego monitoringu prowadzonego przez specjalistów przekazano bezpośrednio 71 dodatkowych zgłoszeń do instytucji odpowiedzialnych za rozpatrywane sprawy: Krajowego Biura Wyborczego, Policji, Państwowej Komisji Wyborczej oraz CSIRT GOV. W ramach przeciwdziałania dezinformacji NASK-PIB podjął w 2023 r. szereg aktywności ukierunkowanych na uświadamianie istnienia zjawiska dezinformacji, umiejętność jej rozpoznawania, a wreszcie reagowania i zwalczania pojawiających się w przestrzeni mediów społecznościowych treści o charakterze dezinformacyjnym. Aktywności edukacyjne prowadzone były w formie szkoleń, webinarów, warsztatów, wystąpień na różnorodnych wydarzeniach skierowanych do różnych grup odbiorców. Działalność edukacyjna była prowadzona zarówno w odpowiedzi na potrzeby wybranych jednostek administracji rządowej i samorządowej, w ramach działań własnych NASK-PIB i współpracy międzydziałowej, jak i sformalizowanych współprac zewnętrznych, np. z Warszawskim Instytutem Bankowości. W szkoleniach udział wzięło około 35 tys. osób. Dodatkowo prowadzono kampanie społeczne (patrz rozdział Kampanie i projekty społeczne).

4.6. Paszportyzacja żywności

W 2023 roku zakończył się pilotażowy projekt badawczy zrealizowany na zlecenie Krajowego Ośrodka Wsparcia Rolnictwa – Paszportyzacja Polskiej Żywności, mający na celu sprawdzenie i przetestowanie możliwości zbierania i potwierdzenia autentyczności danych w całym okresie produkcji rolnej, weryfikację określonych funkcjonalności oraz przygotowanie rekomendacji dla Docelowego Systemu Paszportyzacji Polskiej Żywności. W projekt zaangażowanych było około 90 podmiotów (uczestnicy pilotażu, urzędy administracji publicznej, jednostki naukowe, dostawcy rozwiązań). W trakcie prac przygotowano kompleksową dokumentację opisującą szczegółowo rynek ziemniaka, wieprzowiny i wołowiny w Polsce i Europie.

Przygotowana dokumentacji zawierała:

82 modele procesowe AS-IS, 13 referencyjnych modeli TO-BE, 108 analiz symulacyjnych,

- rozpoznane potrzeby i oczekiwania podmiotów biorących udział w badaniu,
- uzgodniony zakres danych do paszportu (opracowany wspólnie z zewnętrznymi ekspertami i organizacjami branżowymi),

- przeanalizowane systemy i rejestry administracji publicznej, zidentyfikowane dane,
- przeanalizowany system prawny dotyczący obszaru pilotażu,
- zinwentaryzowany poziom technologiczny podmiotów, biorących udział w badaniu,
- opracowane rekomendacje, dotyczące automatycznej identyfikacji (ADC),
- oszacowane korzyści z wdrożenia paszportu żywności (na podstawie symulacji procesowych),
- zidentyfikowane potencjalne rozwiązania technologiczne, możliwe do wykorzystania w projekcie,
- analizę dotycząca możliwości współpracy i współdziałania w zakresie wykorzystania danych w administracji,
- analizę wykorzystania metod genetycznych w procesie potwierdzania autentyczności produktów,
- identyfikację miejsc i sposobów podniesienia efektywności realizowanych procesów w tym ograniczenie obciążeń administracyjnych,
- analizę kwestii dotyczących „zero-emisyjności",
- analizę wykorzystania technologii blockchain,
- raport końcowy zawierający rekomendacje dla Docelowego Systemu Paszportyzacji

Rozstrzygnięte zostały konkursy na dostawców rozwiązań branżowych do obsługi procesów paszportyzacji w ramach gospodarstw rolnych. Wdrożono ostateczne rozwiązanie pilotażowe wraz z symulacją integracji z administracją publiczną oraz z systemami dostawców wyłonionych w konkursach przygotowanych i przeprowadzonych podczas prac pilotażowych. W ramach projektu przygotowano również pełną dokumentację dotyczącą przetargu na realizację Docelowego Systemu Paszportyzacji Polskiej Żywności – Szczegółowy Opis Przedmiotu Zamówienia oraz wstępną wersję umowy na budowę, wdrożenie i utrzymanie Docelowego Systemu Paszportyzacji Polskiej Żywności wraz z załącznikami.

4.7. Architektura Informacyjna Państwa (AIP)

NASK-PIB realizował w 2023 roku zadanie zlecone przez Ministerstwo Cyfryzacji objęte umową dotacji na „Rozwinięcie i utrzymanie Architektury Informacyjnej Państwa".

AIP jest szczegółowym opisem zorganizowania wszystkich dziedzinowych systemów informacyjnych państwa, wraz z obsługującymi je systemami teleinformatycznym, warstwą danych, organizacyjną oraz prawną. Zawiera elementy niezbędne do skutecznego zarządzania cyfryzacją państwa: pryncypia, standardy, modele i procesy zarządzania obejmujące też interakcję systemów z otoczeniem. Wiedza ta jest kluczowa dla wszystkich jednostek administracji publicznej rozwijających istniejące i budujących nowe systemy informacyjne. Jest ona kluczowa w kontekście zachowania interoperacyjności pomiędzy poszczególnymi komponentami AIP, również dla optymalizacji kosztów modernizacji lub wdrożeń nowych rozwiązań teleinformatycznych oraz w kontekście finansowania takich rozwiązań przy wykorzystaniu europejskich środków finansowych.

Wybrane zadania:

- przeprowadzenie I Fazy Studium AIP – szkolenia dla jednostek administracji centralnej poświęcone teoretycznym i praktycznym aspektom AIP. Przeszkolono 583 osoby w ramach 5 spotkań informacyjnych,

- rozpoczęcie II Fazy Studium AIP – 6 dniowe spotkania warsztatowe dot. m.in. podstaw teoretycznych oraz koncepcji zarządzania AIP, sposobu budowy repozytorium oraz stosowanych notacji uświadamiania, w jaki sposób organizacje uczestniczące w szkoleniach współuczestniczą w budowie architektury informacyjnej Państwa. W 4 kwartale 2024 roku przeszkolono 104 osób,

- wykłady w ramach Akademii Zarządzania IT Administracji Publicznej. Omówiono m.in. podejście architektoniczne w kontekście racjonalnego rozwoju cyfrowego państwa, przedstawiono wizję Architektury Informacyjnej Państwa, przedstawiono kontekst wykorzystania AIP w kontekście cyberbezpieczeństwa,

- wsparcie eksperckie prac Rady Architektury IT przy KRMC w zakresie realizacji zadań związanych z oceną propozycji nowych projektów teleinformatycznych. W 2023 roku Rada opiniowała 46 tego typu inicjatyw,

- wsparcie Ministerstwa Cyfryzacji w zakresie utrzymania i rozwoju Systemu do Inwentaryzacji Systemów Teleinformatycznych Państwa (SIST) oraz repozytorium AIP poprzez tworzenie nowych obiektów i modeli architektonicznych w zgodzie z wytycznymi Rady Architektury,

- prowadzenie asysty, konsultacji i wsparcia dla jednostek administracji publicznej w praktycznym wdrażaniu rozwiązań opartych na AIP – wizji stanu docelowego rejestrów, usług, środowiska IT, wyznaczanie kierunków i przygotowanie propozycji działań i planów. W 2023 roku świadczona była asysta architektoniczna dla Urzędu Transportu Kolejowego. Prace prowadzone były w czterech głównych zakresach: wizji, strategii i planowanych działań umożliwiających wdrożenie zasad związanych z AIP, architektury informacyjnej UTK wpisującej się w wizję AIP, zdefiniowanie ramowego planu działań dla projektów cyfrowej transformacji obszaru działania UTK oraz wsparcia w formie konsultacji w zakresie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w oparciu o normę ISO 27001.

4.8. System S46

Cel projektu: Rozwój i utrzymanie systemu teleinformatycznego S46 dla dwukierunkowej bezpiecznej wymiany informacji i danych pomiędzy podmiotami KSC.

Realizacja zadania prowadzona była w trybie ciągłym w oparciu o umowę dotacji i projekt POPC pod nazwą S46-REACT. System S46, o którym mowa w art. 46 ust. 1 ustawy o KSC, wdrożono 01.01.2021, zgodnie z art. 89 tej ustawy. Obsługiwane są CSIRT-y poziomu krajowego, Pełnomocnik Rządu ds. Cyberbezpieczeństwa, UKE, Organy Właściwe (OW) oraz operatorzy usług kluczowych (OUK) – w sumie 157 podmiotów.

W 2023 roku realizowano standardowe procesy utrzymaniowe (zapewnienie sprawności systemu, podłączanie, szkolenia, monitorowanie, naprawy awarii, helpdesk). Wdrożono nowe, tańsze sposoby podłączania nowych uczestników do systemu. W obszarze rozwoju opracowano kolejne wydania systemu, których głównym celem była optymalizacja pod kątem podłączania dużej liczby użytkowników oraz przygotowanie na zmiany w ustawie o KSC (nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa) w związku z dyrektywą NIS2). Prowadzone były prace rozwojowe zmierzające do wprowadzenia nowych funkcjonalności wymaganych proponowaną nowelizacją KSC – w tym rejestru podmiotów KSC z funkcją samorejestracji oraz związane z udostępnieniem systemu dla 40 tysięcy podmiotów w modelu SaaS, raportowaniem audytów, nowym – prostszym – modelem analizy ryzyka itp.

4.9. Ochrona ADDoS podmiotów istotnych z punktu widzenia bezpieczeństwa RP

Cel projektu: zapewnienie usługi ochrony przed atakami DDoS – Distributed Denial of Service dla podmiotów realizujących zadania publiczne oraz podmiotów istotnych z punktu widzenia bezpieczeństwa RP.

Od 2022 roku wdrożono usługi ochrony przed atakami na infrastrukturę (warstwa L3 i L4) oraz aplikacyjnymi (L7) w oparciu o usługi dostawcy zewnętrznego. W 2023 r. objęto ochroną 65 podmiotów (kolejnych ok. 50 – w przygotowaniu). Obejmowanie ochroną często miało charakter interwencyjny – związany z trwającymi atakami. W ramach projektu prowadzone były instruktaże oraz konsultacje dla podłączanych podmiotów. Dzięki zindywidualizowanemu podejściu jednostki objęte działaniem projektowym dodatkowo uzyskały wsparcie w poprawie bezpieczeństwa podłączenia do internetu.

4.10. Projekty związane z siecią telekomunikacyjną NASK-PIB

Światłowody 2020

Cel projektu: Rozbudowa sieci światłowodowej WARMAN w części szkieletowej oraz wykonanie podłączeń światłowodowych dla 15 jednostek naukowych i budowa szkieletu do Jabłonnej.

Wykonanie projektu rozpoczęto w 2020 roku. Do końca 2023 roku wykonano podłączenie 14 jednostek oraz relację szkieletową. Złożono raport końcowy. Podłączenie Domu Zjazdów i Konferencji PAN w Jabłonnej nastąpi w 2024 r. ze środków własnych.

Światłowody 2023

Cel projektu: Rozbudowa sieci światłowodowej WARMAN w części szkieletowej (Wilanów – most południowy – Anin - Otwock) oraz wykonanie podłączeń światłowodowych dla 5 jednostek naukowych.

Wykonanie projektu rozpoczęto w sierpniu 2023 r. Wykonano podłączenie 3 jednostek i rozpoczęto budowę relacji szkieletowej. W 2024 r. finalizowane będzie podłączanie 2 jednostek i relacji szkieletowej.

PIONIER-LAB – Krajowa Platforma Integracji Infrastruktur Badawczych z Ekosystemami Innowacji

Celem projektu, którego NASK-PIB jest uczestnikiem, jest budowa 8 „laboratoriów" – struktur świadczących usługi dla nauki i gospodarki: sieć, precyzyjny sygnał zegarowy i czasu, smart Campus, „żywe laboratoria" – przestrzeń prac AV/VR/AR, obliczenia chmurowe, obliczenia wieloskalowe, e-learning, preinkubator (z przestrzeniami prototypowania IoT, wideokonferencji itp.).

Wykonanie projektu, dofinansowanego z POIR, rozpoczęto w 2021 roku. W roku 2023 zakończono projekt, kompletując wyposażenie wszystkich laboratoriów. Od 2024 roku planowane są praktyczne zastosowania zakupionej aparatury i oprogramowania – udostępnienie sieci, precyzyjnego sygnału zegarowego i czasu oraz wyposażenia AV/VR/AR, badań UX, prototypowania IoT. Planowane jest także pełne udostępnienie nowych usług sieci PIONIER (w tym obliczeń, e-learningu).

4.11. Krajowe Centrum Przetwarzania Danych (KCPD)

W ramach wzmacniania bezpieczeństwa cybernetycznego zasobów administracji rządowej do połowy 2026 roku planowane jest powstanie KCPD. Projekt realizowany jest przez Ministerstwo Cyfryzacji, NASK-PIB oraz Centralny Ośrodek Informatyki. Inwestycja finansowana jest ze środków KPO i ma wartość ponad 829 mln zł netto. KCPD to zespół obiektów budowlanych, które składają się na sieć ośrodków obliczeniowych i będą połączone łączami światłowodowymi wraz z infrastrukturą techniczną niezbędną do ich funkcjonowania. Inwestycja obejmować będzie początkowo 3 ustandaryzowane i efektywne energetycznie centra przetwarzania danych zlokalizowane na terenie województwa mazowieckiego. Ośrodki będą zasilane w części energią pochodzącą z alternatywnych źródeł zasilania. KCPD będzie umożliwiał przetwarzanie danych w systemach teleinformatycznych w sposób zapewniający ciągłość przepływu oraz bezpieczeństwo danych na potrzeby systemów teleinformatycznych wykorzystywanych w administracji publicznej przez operatorów usług kluczowych lub dostawców usług cyfrowych oraz państwowe osoby prawne, jak również spółki realizujące misję publiczną.

4.12. Cyberbezpieczny Samorząd

Projekt Cyberbezpieczny Samorząd jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Celem projektu jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Beneficjentem projektu jest Centrum Projektów Polska Cyfrowa w partnerstwie z NASK-PIB.

Realizacja projektu poprzez wsparcie grantowe jednostek samorządowych, przyczyni się do:

- wdrożenia lub aktualizacji w JST polityk bezpieczeństwa informacji (SZBI),
- wdrożenia w JST środków zarządzania ryzykiem w cyberbezpieczeństwie,
- wdrożenia w JST mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni,
- podniesienia poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie,
- przeprowadzenia w JST audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia.

Grupą docelową projektu jest administracja publiczna: jednostki samorządu terytorialnego (JST) wraz z jednostkami podległymi (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia).

W naborze, który trwał od 19.07.2024 do 14.12.2023 r. upoważnionych do udziału było 2807 jednostek, z czego 2517 jednostek złożyło wnioski, w tym 2202 gmin, 300 powiatów i 15 województw. Podczas oceny wniosków 2 jednostki samorządu terytorialnego zrezygnowały z udziału, a 4 wnioski zostały ocenione negatywnie.

Łączny budżet projektu wynosi 1 762 235 453 zł, w tym:

- budżet UE 1 465 303 702 zł
- budżet państwa 296 931 751 zł

Łącznie wykorzystanie środków, po ocenie wniosków, zaplanowane jest

na 1 492 367 874,66 zł.

4.13. Inne przedsięwzięcia

Węzeł Transgraniczny (WT)

Cel projektu: Pełnienie roli operatora węzła eIDAS przez NASK-PIB.

W 2023 roku przeprowadzone prace przyczyniły się do zwiększenia poziomu integracji węzła eIDAS z węzłami innych państw UE umożliwiając transgraniczne logowanie polskimi notyfikowanymi środkami identyfikacji elektronicznej (tj. profil zaufany, profil osobisty) do usług 17 państw w EU i portali Unii Europejskiej poprzez integrację z EU login oraz logowanie obywatelom z 19 państw EU do polskiego transgranicznego portalu biznes.gov.pl. NASK-PIB zapewnił bezpieczny dostęp w modelu SasS do środowisk testowo-integracyjnego i produkcyjnego oraz wykonał prace analityczne, rozwojowe i integracyjne węzła eIDAS. W ramach utrzymanie ciągłości działania polskiego węzła transgranicznego zapewnione zostały zasoby chmury obliczeniowej oraz monitorowanie i skanowanie podatności infrastruktury udostępnionych środowisk, kolokacja urządzeń WT (urządzenia HSM), usługa ADDoS, oraz usługa II linii wsparcia. Przeprowadzono czynności audytowe pozwalające na utrzymanie certyfikacji ISO 27001 a w ramach działań rozwojowych przeprowadzono prace przygotowawcze do wdrożenie nowej wersji 2.6 węzła eIDAS, które są kontynuowane w 2024 roku.

Organ Cyfrowej Tożsamości (OCT)

Cel projektu: Wsparcie w funkcjonowaniu Organu ds. Cyfrowej Tożsamości w Ministerstwie Cyfryzacji.

W 2023 roku osiągnięto planowane rezultaty umowy dotacji. Zapewniono wsparcie w pracach grup Cooperation Network i eIDAS Technical Subgroup działających w obszarze identyfikacji elektronicznej oraz merytoryczną komunikację w serwisie gov.pl w zakresie informacji wspierających użycie przez obywateli polskich środków identyfikacji elektronicznej w procesie identyfikacji i uwierzytelnienia w ruchu transgranicznym. Ponadto zapewniono wsparcie w prowadzeniu nadzoru nad PSIE, dostarczono zmodyfikowany wzór ankiety dla dostawców usług online w zakresie PBI Węzła Krajowego, KRI oraz opracowano „Raport z badania dostawców usług on-line". Przeanalizowano 1066 ankiet dotyczących zintegrowanych z Węzłem Krajowym systemów świadczących usługi online. Przeprowadzono analizę przekazanych projektów dokumentów stanowiących Politykę bezpieczeństwa informacji dla węzła krajowego (PBI WK) i zaproponowano zmiany mające wpływ na funkcjonowanie systemu Węzła Krajowego.

Eksperymentalna Platforma Walidacyjna (EPW)

Cel projektu: Przygotowanie eksperymentalnej platformy do automatycznej weryfikacji i walidacji algorytmów oraz protokołów kryptograficznych.

W 2023 roku osiągnięto planowane rezultaty umowy dotacji. Zakończono prace nad platformą w wersji on-line i off-line EPW. Zakupiono wszystkie niezbędne elementy infrastruktury. Zakończono także założenia dockerów dostarczanych przez konsorcjantów i sposób komunikacji, zainstalowano repozytorium do przekazywania dockerów, uruchomiono platformę współdziałającą z dockerami dostarczonymi przez konsorcjantów, przeprowadzono testy integracyjne i bezpieczeństwa platformy. Wykonano także analizę komercjalizacji platformy.

ChatBot dla CERT Polska

Cel projektu: Przygotowanie w formie ChatBota, dodatkowego, częściowo zautomatyzowanego kanału przyjmowania zgłoszeń o incydentach cyberbezpieczeństwa. System będzie zintegrowany z ekosystemem CERT Polska oraz wykorzystywać będzie mechanizmy sztucznej inteligencji. Uruchomienie pierwszej, podstawowej wersji produkcyjnej planowane jest na połowę 2024 roku. System będzie stanowić część strony https://www.cert.pl. Projekt finansowany jest ze środków KSC, istnieje potencjalna możliwość kontynuacji ze środków UE.

AK NASK to wdrożenie i utrzymanie wysokiej jakości architektury korporacyjnej wspierającej proces długofalowego planowania strategicznego oraz wpływającej na kluczowe decyzje dotyczące rozwoju i modyfikacji systemów informatycznych NASK-PIB, a co za tym idzie optymalizacji kosztów związanych z tymi pracami.

W ramach prac w 2023 roku:

- opracowano projekt zarządzenia Dyrektora NASK-PIB w sprawie regulaminu tworzenia, aktualizacji i zarządzania architekturą korporacyjną Instytutu. Zarządzenie ustanawia rolę Rady Architektury jako organu kolegialnego właściwego do opiniowania wniosków dot. propozycji zmian dla inicjatyw modyfikujących funkcjonujące procesy biznesowe, dane, aplikacje lub elementy infrastruktury Instytutu,

- opracowano zasady tworzenia (metamodel) oraz sposób organizacji i zarządzania repozytorium AK NASK,

- przygotowano koncepcję tworzenia zawartości repozytorium i rozpoczęto przenoszenie i porządkowanie domen biznesowej, aplikacyjnej, danych oraz infrastruktury.

Wytworzenie i uruchomienie Bazy Strat Wojennych na rzecz MKDNiS

Cel projektu: zaprojektowanie oraz wytworzenie systemu „Baza strat wojennych".

W roku 2023 NASK-PIB rozpoczął współpracę z Ministerstwem Kultury i Dziedzictwa Narodowego w obszarze budowy rozwiązania do obsługi zbioru danych o dziełach utraconych w wyniku wojen. Projektowany system zapewni wsparcie procesów biznesowych w tym obszarze jak również będzie stanowił kanał dostępu do skatalogowanych obiektów muzealnych dla obywateli i badaczy. Finalizacja prac przewidziana jest na rok 2025.

Kontynuacja projektu proof-of-concept Resolver DNS

Przedmiotem projektu jest dostarczenie bezpiecznego narzędzia, Resolver DNS, chroniącego użytkowników internetu przed witrynami zawierającymi złośliwe oprogramowanie, phishing oraz w przypadku których istnieje duże prawdopodobieństwo, że są fałszywe lub stanowią wyłudzenie danych.

Cel projektu: zapewnienie bezpiecznej przestrzeni cyfrowej dla użytkowników Internetu, korzyści wizerunkowe z dostarczenia nowej wysokiej jakości usługi o znaczeniu strategicznym dla zapewnienia bezpiecznego Internetu w Polsce

W 2023 roku wykonano następujące prace:

- zainstalowano na serwerach wirtualnych oprogramowanie Resolver DNS wraz z dodatkowymi narzędziami,
- opracowano i dopasowano skrypty aktualizujące listy domen blokowanych przez resolver,
- opracowano „landing page" dla zablokowanych domen,
- zkonfigurowano oprogramowanie serwera HTTP(s) oraz zainstalowano narzędzia monitorujące oraz zbierające logi z systemu,
- wykonano testy wydajnościowe,
- udoskonalono konfigurację o DoT oraz DoH,
- przebadano zachowanie oraz wykorzystanie zasobów Resolverów DNS, po skonfigurowaniu serwera domeny NASK-PIB, tak aby użytkownicy w NASK-PIB korzystali pośrednio z Resolverów DNS,
- nawiązano współpracę z Warszawską Wyższą Szkołą Informatyki i podpisano umowę określającą warunki realizacji Usługi testowej Resolver DNS,
- opracowano regulamin świadczenia usługi testowej Relosver DNS,
- rozpoczęto działania komercjalizacyjne Resolver DNS w zakresie wyjścia z produktem na rynek.

Projekt APLIK „Człowiek w kryzysie – platforma wiedzy i komunikacji"

Cel projektu: Projekt cyfryzacyjny, usprawniający i wspierający udzielanie pomocy osobom w kryzysie emocjonalnym, psychologicznym czy społecznym.

Głównym partnerem projektu jest podmiot obsługujący numer 116 123 – Niebieska Linia. W ramach projektu NASK-PIB dostarcza nowoczesne rozwiązania techniczne do obsługi wszystkich kanałów komunikacji (infolinia, formularz kontaktowy, czat), tj. system contact center, co pozwala udzielić pomocy większej liczbie osób w kryzysie.

5. Nowe technologie i usługi cyfrowe

5.1. BOTSENSE

Obszar zastosowań i potencjalny odbiorca:

Wersja webowa — bankowość — instytucje rządowe

Wersja mobilna — bankowość — wydawcy aplikacji mobilnych — mObywatel

Opis Usługi:

System BotSense wykrywa aktywność złośliwego oprogramowania wykorzystywanego przeciwko użytkownikom bankowości elektronicznej na platformach stacjonarnej i mobilnej, co pozwala na ochronę jej użytkowników przed próbami kradzieży środków lub danych wrażliwych.

Dostępny jest w dwóch wersjach:

BotSense Web

Oprogramowanie rozwijane od 2014 roku, którego celem jest wykrywanie zmian treści serwisów internetowych wyświetlanych w przeglądarkach WWW użytkowników aplikacji klienta. Oprogramowanie BotSense jest oparte o mechanizm zarządzania sygnaturami oraz dynamicznej analizy struktury DOM pod kątem zachowań wykraczających poza normalną funkcjonalność webowych serwisów internetowych użytkownika.

Kluczowe działania w 2023 roku:

1. Moduł Trojan Checker, którego kluczową funkcjonalnością jest wykrywanie webinjectów na komputerach użytkownika serwisu klienta ukierunkowanych na inne polskie podmioty (np. banki lub sklepy internetowe) na podstawie bazy sygnatur BotSense przygotowywanych przez NASK-PIB.

2. Moduł Password Checker, wykorzystujący analizę behawioralną sposobu wprowadzania przez użytkownika hasła do bankowości elektronicznej. Moduł wspiera proces uwierzytelniania w operacjach bankowych. W module szczególną uwagę zwrócono na metody analizy tzw. hasła maskowanego – składającego się z losowo wybranych znaków hasła pełnego.

3. Remote Checker, służy do wykrywania wykorzystania oprogramowania do obsługi zdalnego pulpitu typu AnyDesk lub Team Viewer w trakcie sesji logowania w serwisie internetowym za pomocą dwuetapowej weryfikacji: analizy dostępności portów oraz analizy dynamiki ruchów kursora myszy.

4. Analiza behawioralna - moduł przy pomocy sztucznej inteligencji analizuje specyficzny sposób, w jaki użytkownik wchodzi w interakcję ze swoim urządzeniem. Jest pasywną metodą uwierzytelniania, ponieważ nie wymaga od klienta żadnych dodatkowych działań, a wprowadza dodatkową warstwę bezpieczeństwa. Analiza odbywa się na urządzeniu końcowym użytkownika, a dane nie są przesyłane na serwer BotSense, sprawdzana jest jedynie integralność.

Kluczowe dane 2023 rok

- 12 dużych banków
- 2 filie zagraniczne
- 16 banków spółdzielczych
- ponad 16 milionów kont bankowości internetowej

BotSense Mobile

Oprogramowanie BotSense Mobile jest biblioteką programistyczną służącą do oceny stanu bezpieczeństwa urządzenia mobilnego pracującego pod kontrolą systemu operacyjnego Android w wersji API 19 (Android 4.4) lub wyższej oraz pod kontrolą systemu iOS w wersji 12.4 lub wyższej.

Kluczowe działania w 2023 roku

Malware Hunter AI nowatorski systemem wykorzystującym metody AI i heterogeniczne źródła danych do oceny zagrożenia bezpieczeństwa urządzeń mobilnych generowanego przez zainstalowane aplikacje, będący biblioteką programistyczną dla aplikacji pracującej na systemie operacyjnego Android w wersji API 19 (Android 4.4) lub wyższej.

BotSense Mobile Threat Defense

BotSense MTD to zaawansowane narzędzie do monitorowania i śledzenia urządzeń mobilnych oraz ich aktywności. Centralny serwer pełni kluczową rolę w zbieraniu, analizowaniu i zarządzaniu danymi pochodzącymi z urządzeń mobilnych, co umożliwia administratorom śledzenie i zarządzanie flotą urządzeń w czasie rzeczywistym.

BotSense MTD służy do identyfikowania i reagowania na różnego rodzaju zagrożenia bezpieczeństwa mobilnych urządzeń, w tym:

- na złośliwe oprogramowania (malware), ataki hakerskie, phishing czy próby naruszenia prywatności użytkowników,

- na potencjalnie ryzykowne aktywności, na przykład próby ingerencji w system lub dostęp nieautoryzowany do danych,

- pozwala sprawdzić połączenia sieciowe i monitorować ruch w celu wykrywania niebezpiecznych aktywności sieciowych lub ataków.

Kluczowe dane 2023 rok

Aktualne wdrożenia BotSense Mobile:

- 4 duże banki
- 1 instytucja rządowa
- 16 banków spółdzielczych
- ponad 20 milionów użytkowników aplikacji mobilnych

5.2. FLDX

Obszar zastosowań

Infrastruktura IT, sieci komputerowe, aplikacje

Potencjalni odbiorcy

Administracja centralna, służby mundurowe, podmioty infrastruktury krytycznej, operatorzy usług kluczowych, dostawcy usług cyfrowych, inne podmioty utrzymujące systemy informatyczne.

Opis produktu

FLDX to autorski, opatentowany w Polsce system NASK-PIB do ochrony przed atakami wolumetrycznymi DDoS. FLDX to adaptacyjny system wczesnej detekcji oraz tłumienia wolumetrycznych ataków DDoS, który w bezpieczny, szybki i niezwykle skuteczny sposób zapewnia ochronę dostępności usług w sieci – niezależnie, czy źródłem zagrożenia jest atak wolumetryczny DDoS czy nagły wzrost natężenia aktywności użytkowników.

Kluczowe działania w roku 2023

System FLDX wykorzystywany jest do ochrony wielu podmiotów, w tym sieci OSE (Ogólnopolska Sieć Edukacyjna), czy klientów korzystających z łączy NASK-PIB. W oparciu o badanie rynku oraz potrzeby klientów, w 2023 roku rozpoczęto prace nad rozwojem systemu. Rozwój FLDX ukierunkowany jest na wytworzenie nowych modeli wdrożeniowych, pozwalających na ochronę większej liczby podmiotów. Ponadto rozpoczęto pracę nad modernizacją stosu technologicznego i rozszerzeniem funkcjonalności FLDX, np. przez wytworzenie portalu klienta.

W roku 2023 poza ochroną m.in. sieci OSE, NASK-PIB, czy kilku podmiotów państwowych, zrealizowano prace pilotażowe z potencjalnymi interesariuszami rządowymi i komercyjnymi.

5.3. Usługa CTI

Obszar zastosowania

cyberbezpieczeństwo, e-usługi

Potencjalni odbiorcy

Podmioty infrastruktury krytycznej, operatorzy usług kluczowych, bankowość i finanse, podmioty publiczne, potencjalni odbiorcy, podmioty infrastruktury krytycznej w tym banki, operatorzy usług kluczowych.

Opis usługi

Usługa Collective Threat Intelligence (CTI) obejmuje działania z zakresu monitorowania i wczesnego ostrzegania o zewnętrznych zagrożeniach mogących mieć wpływ na bezpieczeństwo teleinformatyczne chronionej organizacji.

Specjaliści zespołu NIRT na bieżąco monitorują i analizują wiele źródeł informacji o cyberzagrożeniach mogących mieć wpływ na integralność i dostępność systemów teleinformatycznych chronionych Organizacji oraz ich Klientów. Analiza zagrożeń wykonywana jest w oparciu o wiele własnych źródeł danych jak Darknet, honeypot, sinkhol, spampot,

samtrap oraz innych otwartych i zamkniętych źródeł monitorowania nieindeksowanych warstw Internetu (Deep i Dark Web). Dostarczane dane oraz kompetencje ekspertów NIRT stanowią istotny element procesu ochrony organizacji przed nowymi i celowanymi atakami tworząc kolejną linie wsparcia dla wewnętrznych zespołów bezpieczeństwa, oraz istotne źródło danych zewnętrznych automatycznie zasilających systemy ochrony bezpieczeństwa sieci jak SIEM, IPS, EDR itp.

Usługa Collective Threat Inteligence (CTI) obejmuje działania z zakresu monitorowania i wczesnego ostrzegania o zewnętrznych zagrożeniach mogących mieć wpływ na bezpieczeństwo teleinformatyczne chronionej organizacji. Specjaliści zespołu NIRT na bieżąco monitorują i analizują wiele źródeł informacji o cyberzagrożeniach mogących mieć wypływ na integralność i dostępność systemów teleinformatycznych chronionych Organizacji oraz ich klientów. Analiza zagrożeń wykonywana jest w oparciu o wiele wlanych źródeł danych jak Darknet, honeypot, sinhol, samtrap oraz wiele innych otwartych i zamkniętych źródeł monitorowania nieindeksowanych warstw Internetu (Deep i Dark Web). Dostarczane dane oraz kompetencje ekspertów NIRT stanowią istotny element procesu ochrony organizacji przed nowymi i celowanymi atakami tworząc kolejną linię wsparcia dla wewnętrznych zespołów bezpieczeństwa oraz istotne źródło danych zewnętrznych automatycznie zasilających systemy ochrony bezpieczeństwa sieci jak SIEM, IPS,EDR itp.

Usługa zbudowana jest z następujących modułów:

- Incident response

Moduł wsparcia zespołów bezpieczeństwa w reagowaniu na incydenty.

- Brand protection

Moduł ma na celu monitorowanie i wykrywanie złośliwych działań w cyberbezpieczeństwie oraz reakcji na wykryte przez zespół NIRT incydenty.

- Vulnerability scan

Moduł wpierający wzmacnianie odporności na cyberzagrożenia.

- Fraud prevention(for banks only)

Moduł zapobiegający nadużyciom finansowym w kanale bankowości elektronicznej.

- Feed as service (FaaS)

Moduł służący do zwiększania poziomu bezpieczeństwa systemów ochrony, automatycznie zasilając je w aktualną informację o obserwowanych zagrożeniach w polskiej cyberprzestrzeni.

- CTI Awareness

Moduł ma na celu budowanie świadomości sytuacyjnej cyberzagrożeń na rynku polskim i zagranicznym.

Kluczowe dane za 2023

- Liczba klientów: 17
- Próbki malware: 7 845
- Próbki mobilny malware: 47 162
- Phishing łącznie: 126 254
- Phishing w sektorze finansowym w Polsce: 3 557

Kluczowe działania w roku 2023

2023 rok to czas prac nad usprawnieniem usługi CTI NASK i projektowaniem aplikacji klasy platform CTI. TI BOX będzie automatyzował dostarczanie informacji o cyberzagrożeniach do klientów objętych pakietem CTI/TI BOX, a także wprowadzi graficzną wizualizację dostarczanych wiadomości. Zakres zmian i nową aplikację opracowano na podstawie wywiadów ze specjalistami od cyberbezpieczeństwa oraz menedżerami odpowiedzialnymi za obszar cyberbezpieczeństwa i IT. TI BOX integruje w sobie dotychczasowe wyniki prac NASK-PIB (m.in. projekt VARIoT). Aplikacja ma wspierać pracę specjalistów ds. cyberbezpieczeństwa w czterech obszarach:

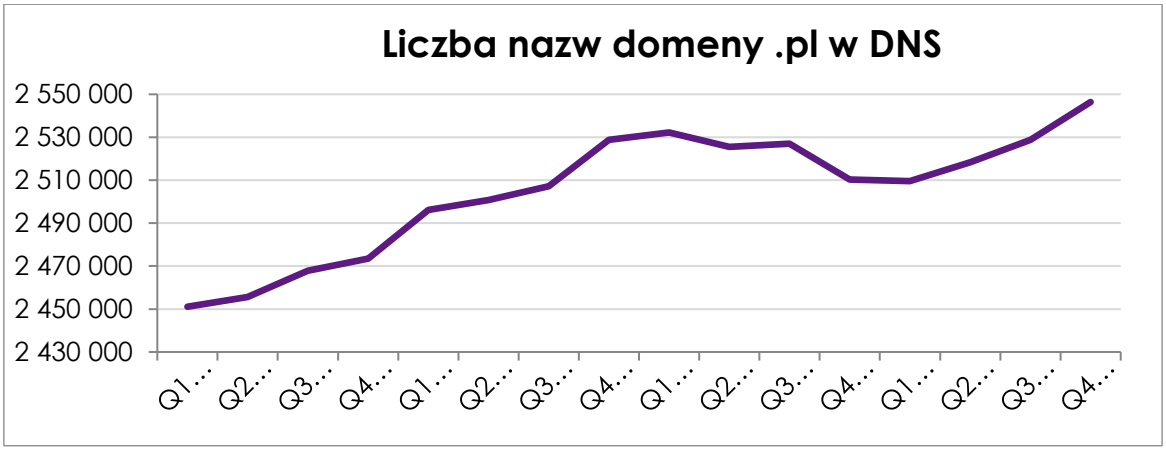
1. automatyzacja procesów,
2. wiarygodneźródła informacji,
3. priorytetyzacja cyberzagrożeń,
4. bieżące informowanie o pojawiających się cyberzagrożeniach.

5.4. Domeny

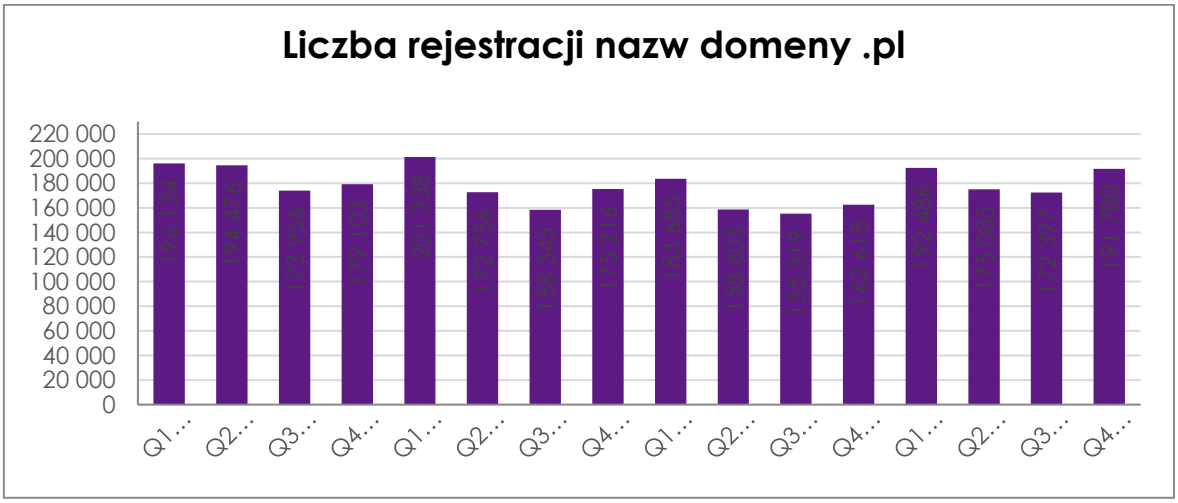
Wielkość rynku domeny .pl na koniec 2023 roku

W Rejestrze domeny .pl na koniec 2023 roku znajdowało się 2 546 407 aktywnych nazw domeny .pl utrzymywanych na rzecz 1 131 332 abonentów. Bezpośrednio w domenie .pl zarejestrowanych było 2 095 051 nazw, w domenach funkcjonalnych (np. .com.pl, .net.pl) 374 944, zaś w domenach regionalnych (np. .waw.pl, .wroclaw.pl) 76 412 nazw.

Liczba utrzymywanych nazw z narodowymi znakami diakrytycznymi, tzw. IDN (ang. Internationalized Domain Names), na koniec 2023 roku wyniosła 25 288 i stanowiła 0,99% wszystkich aktywnych nazw w DNS.



W 2023 roku do rejestru wprowadzono 731 748 nowych nazw domeny .pl, z czego 8 639 nazw zawierało narodowe znaki diakrytyczne.



Uruchomienie projektu: Generator Nazw Domen

Generator nazw domen to usługa umożliwiająca wyszukiwanie wolnych nazw domen zbliżonych znaczeniowo do wskazanych w procesie rejestracji nazwy domeny słów kluczowych lub kontekstu.

Cel projektu: potencjalnie zwiększenie liczby rejestrowanych nazw domen, udostępnienie nowej funkcjonalności umożliwiającej klientowi pozyskanie alternatywnej nazwy domeny jeżeli ta, której poszukuje jest już niedostępna, korzyści wizerunkowe z dostarczenia nowej usługi wspierającej/stymulującej proces rejestracji (sprzedaży) nazw domen.

Prace wykonane w 2023 roku:

- Opracowanie własnego modelu językowego rekomendacji nazw w miejsce pierwotnego modelu regałowego. Prowadzenie prac nad poprawą jego działania, które pozwolą na opracowanie procedury systematycznego aktualizowania

modelu na podstawie bieżących danych o rejestracjach zarekomendowanych nazw domen,

- Implementacja w Pythonie web-serwisu generatora opartego na słowniku synonimów,
- Udostępnienie demonstracyjnego interfejsu webowego do testowania generatora,
- Implementacja alternatywnego generatora opartego na regułach i formularzach,
- Trening modelu Llama2 i HerBert na domenach i metadanych „zescrapowanych" stron internetowych,
- Implementacja generatora opartego na modelu Llama2 (przez narzędzie llama.cpp) i modelu HerBERT,
- Implementacja obsługi sprawdzania dostępności domen przez WHOIS, DNS i przez protokół EPP w rejestrze domeny .pl. ,
- Implementacja bramki do sprawdzania dostępności dla wariantu uruchomienia z wieloma procesami generatora,
- „Dokeryzacja" aplikacji,
- Uruchomienie generatora na środowisku testowym dns.pl. ,
- Uruchomienie narzędzia LabelStudio na serwerze VPS, udostępnienie dla części pracowników NASK-PIB, adnotacja/ocena wyników generatora w celu pozyskania danych uczących,
- Nawiązanie współpracę z Cyber_Folks S.A., podpisanie umowy określającej warunki realizacji Usługi testowej – Generator Nazw Domen,
- Wystawienie API dla partnera (Cyber_Folks S.A.),
- Sprawdzenie wielu metod generowania nazw. Ostatecznie najbardziej obiecujący okazał się model HerBERT. Model po wytrenowaniu daje satysfakcjonujące wyniki. API udostępnione dla partnera wykorzystuje model HerBERT.

Rozwój Registry

W obszarze technicznym kluczową i krytyczną rolę w Rejestrze odgrywają: infrastruktura DNS oraz system Registry. System Registry zawiera m.in. bazę wszystkich utrzymywanych nazw domen, ich delegacje i dane abonentów, za jego pośrednictwem odbywa się zasilanie danymi plików stref domen zarządzanych przez NASK-PIB i publikowanie wpisów na serwerach DNS. System Registry obsługuje różne grupy interesariuszy poprzez liczne zintegrowane aplikacje wspomagające obsługę nazw domeny .pl, .gov.pl, .mil.pl.

W 2023 wprowadzono produkcyjnie zmiany w systemach Registry:

- zmiana sposobu komunikacji aplikacji Rejestru z bazą danych, użycie Oracle Universal Connection Pool;
- wdrożenie nowej aplikacji Registry Web 2.0.0 do testowego wysyłania komend EPP (narzędzie dla Partnerów). Aplikacja względem wersji poprzedniej wzbogacona o została o szereg funkcjonalności ułatwiających korzystanie;
- wdrożenie aktualizacji bezpieczeństwa oraz poprawek bezpieczeństwa likwidujących podatności wykryte podczas audytów.

Ukończono przygotowanie następujących rozwiązań, które na koniec 2023 roku oczekiwały na produkcyjne uruchomienie:

- integracja aplikacji Registry z kanałem szybkich płatności PayPal v2;
- integracja aplikacji Registry z nową usługą banku Santander Bank Polska S.A. w celu automatycznego zasilenia kont pre-paid Partnerów w Registry;
- automatyzacja weryfikacji poprawności danych abonentów usług Rejestru (RCV: Registry Contact Validation). Rozwiązanie weryfikuje dane)m.in. na podstawie bazy kodów pocztowych Poczty Polskiej) i wystawia Partnerom raporty z błędami do poprawy;
- W ramach działań na rzecz bezpiecznego Internetu w 2023 roku zostało zablokowanych 3357 domen phishingowych. Przygotowano nową usługę do obsługi administracyjnego nakładania blokad na nazwy domen z uwagi na nadużycia zidentyfikowane przez CERT (funkcjonalność dodana do aplikacji RAT tj. Registry Administration Tool). Dzięki wprowadzonemu rozwiązaniu, proces blokowania nazw domen, uznanych za złośliwe, uległ znaczącemu skróceniu;
- zmiany w aplikacjach portalu www.dns.pl usuwające dług technologiczny (aktualizacja CMS Drupal do wersji 9.x z mechanizmem migracji danych w wersji skonteneryzowanej oraz aktualizacja frameworka Symfony do wersji 4.x).

Ponadto prowadzono prace analityczne i deweloperskie w następujących obszarach:

- opracowanie rozwiązań dot. wdrożenia wymagań NIS 2 w systemach Rejestru;
- kontynuowano przygotowania do wdrożenia w Rejestrze nowego protokołu dostępu do danych abonentów RDAP i nowych aplikacji WHOIS;
- przygotowanie zmian w szacie graficznej i funkcjonalnościach portalu www.dns.pl;
- opracowanie wymagań i współpraca z innymi komórkami NASK-PIB przy implementacji nowego Panelu Partnerskiego;

- dalsze dokumentowanie procesów systemowych, przypadków użycia i innych elementów aplikacji, które przejęliśmy w 2022 roku do rozwoju.

W 2023 roku realizowano działania mające na celu dostosowanie funkcjonowania Rejestru do wymagań prawnych wynikających z regulacji europejskich. Dokonano zmian organizacyjnych, usprawniających działanie Rejestru, zapewniając m.in. obsługę punktu kontaktowego, umożliwiającego organom Państw Członkowskich oraz Komisji i Radzie Usług Cyfrowych komunikację elektroniczną bezpośrednio z Rejestrem, na potrzeby stosowania DSA. Podjęto działania w obszarze wdrożenia nowych regulacji: Digital Services Act, NIS2, Data Governance Act, Data Act, mających bezpośredni wpływ na funkcjonowanie DNS. Jednym z działań było zorganizowanie punktu kontaktowego odpowiedzialnego za realizowanie nakazów dotyczących podejmowania działań przeciwko nielegalnym treściom zgodnie z art. 9 DSA.

Prowadzono aktywną działalność edukacyjną w obszarze roli systemu domen w środowisku cyfrowym, poprzez organizację szkoleń i cyklu warsztatów. W ramach działalności popularyzatorskiej, przygotowano czasopismo naukowe dot.pl., którego celem jest przyczynianie się do rozwoju krytycznych badań nad Internetem w różnych jego aspektach – społecznym, politycznym, ekonomicznym, jak również prawnym.

Infrastruktura techniczna

W obszarze infrastruktury technicznej Rejestru ukończono kluczowe prace modernizacyjne, których celem było podniesienie poziomu bezpieczeństwa i zwiększenie stabilności systemów informatycznych i usług. Zakres prac obejmował wdrożenia dedykowanych dla systemów Rejestru:

- sieci LAN (ang. Local Area Network),
- sieci SAN wraz macierzami dyskowymi (ang. Storage Area Network),
- ochrony aplikacji webowych WAF (ang. Web Application Firewall),
- systemu kopii zapasowych,
- podniesienie wersji silnika bazodanowego bazy danych Rejestru ze wsparciem dla szyfrowania danych,
- przeprowadzenie migracji systemów do nowej sieci LAN i SAN.

Uruchomiono również nową sieć sześciu autorytatywnych serwerów DNS w technologii anycast oraz zakończono modernizację systemu DNSSEC.

Prace modernizacyjne prowadzone były również w obszarze systemów wspierających, m.in. innymi uruchomiono nowe klastry wirtualizacyjne oraz wdrożono nowe systemy uwierzytelniania, monitoringu, CMDB, wiki oraz system zgłoszeń.

5.5. Audyty bezpieczeństwa teleinformatycznego (ASB)

Obszar zastosowania

cyberbezpieczeństwo, cyfryzacja, e-usługi

Potencjalni odbiorcy

administracja centralna, służby mundurowe, podmioty infrastruktury krytycznej, operatorzy usług kluczowych, dostawcy usług cyfrowych, inne podmioty krytyczne dla funkcjonowania państwa

Opis usługi

NASK-PIB realizuje badania bezpieczeństwa infrastruktury technicznej oraz badania bezpieczeństwa proceduralno-organizacyjnego obszaru przetwarzania informacji. Badania infrastruktury technicznej opierają się na opracowanych przez NASK-PIB wewnętrznych metodykach. Celem świadczenia usług jest podnoszenie poziomu odporności na cyberataki systemów teleinformatycznych dostarczających istotne usługi w cyberprzestrzeni RP.

Zakres oferowanych badań to m. in.:

- Obszar techniczny:
  - ocena podatności infrastruktury;
  - testy penetracyjne aplikacji;
  - badanie bezpieczeństwa kodu źródłowego;
  - testy penetracyjne styku sieci wewnętrznej z siecią internet oraz sieci wewnętrznych;
  - analiza architektury IT;
  - audyt bezpieczeństwa konfiguracji urządzeń sieciowych i topologii sieci;
  - test penetracyjny sieci bezprzewodowej Wi-Fi;
  - analiza bezpieczeństwa środowiska mobilnego;
  - testy odporności infrastruktury na ataki DDoS;
- Obszar formalno-proceduralny:
  - audyt zgodności z obowiązującymi regulacjami lub przepisami prawa w tym m.in. KSC, KRI;
  - dostosowanie organizacji do spełnienia wymogów zawartych w Rozporządzeniu KRI oraz Ustawie o KSC;
  - doskonalenie SZBI, w tym przegląd dokumentacji bezpieczeństwa.

Kluczowe działania wykonane w 2023 roku:

Oferta usług audytowych NASK-PIB jest przygotowana i dostosowana do potrzeb obsługiwanego przez NASK-PIB segmentu rynku, tj. podmiotów o kluczowym znaczeniu dla funkcjonowania państwa i cyberprzestrzeni RP, takich jak administracja centralna, służby mundurowe, podmioty infrastruktury krytycznej, dostawcy usług kluczowych, dostawcy usług cyfrowych.

W roku 2023 roku zrealizowano prace, m. in. dla: KPRM, PKP, ZUS, Urząd Miejski w Łomiankach, SoftNet.

5.6. Program Transformacji Cyberbezpieczeństwa (PTC)

Obszar zastosowania

cyberbezpieczeństwo, cyfryzacja, e-usługi

Potencjalni odbiorcy

administracja centralna, służby mundurowe, podmioty infrastruktury krytycznej, operatorzy usług kluczowych, dostawcy usług cyfrowych, inne podmioty krytyczne dla funkcjonowania państwa

Opis usługi

Celem realizacji Programu Transformacji Cyberbezpieczeństwa (PTC) jest istotna i długotrwała poprawa odporności klienta na zagrożenia cybernetyczne w korelacji z jego celami biznesowymi. Ze względu na swój charakter i zakres, projekty integratorskie realizowane przez NASK-PIB są obejmowane ochroną informacji. PTC jest działaniem długookresowym, o dużej złożoności organizacyjnej i technicznej. Realizowany jest w ścisłej współpracy z klientem, w oparciu o unikalne kompetencje oraz autorskie rozwiązania i metodyki NASK-PIB. Obejmują one działania analityczne, ewaluacyjne i weryfikacyjne, a także organizacyjne i techniczne w obszarze modernizacji środowiska IT, w tym niwelowanie długu technologicznego. Koncentrują się one również na obszarze bezpieczeństwa, w tym bezpieczeństwa administracyjno-proceduralnego, budowaniu kompetencji i transferu wiedzy w oparciu o inżynierię programu i zarządzanie programem, a także na budowie i rozwoju architektury cyberbezpieczeństwa. Realizacja PTC przez NASK-PIB zapewnia spójność i interoperacyjność wszystkich działań projektowych dla wdrażanych technologii cyberbezpieczeństwa, opracowywanych procesów i procedur oraz budowy wiedzy i kompetencji pracowników.

Kluczowe działania wykonane w 2023 roku

W 2023 roku prace wykonywane były między innymi dla: Zakładu Ubezpieczeń Społecznych, Komendy Głównej Straży Granicznej, PKP Polskich Linii Kolejowych S.A.

5.7. Węzeł Blockchain (WB)

Rozwój węzła blockchain oraz aplikacji wykorzystujących tę technologię odbywa się w ramach powiązanych ze sobą projektów – dotacyjnego WB-BIW oraz dofinansowanych z funduszy UE – EBSI-NE, EBSI-VECTOR i EBSI-DC4EU

Projekt WB-BIW

Cel projektu: pełnienie roli operatora węzła EBSI POLSKA dla zapewnienie bezpiecznego i niezawodnego funkcjonowania, jako punktu przyłączenia.

NASK-PIB, na podstawie porozumienia z 17.03.2022 roku z Ministrem Cyfryzacji, pełni rolę operatora w środowiskach pilotażowym pre-produkcyjnym i produkcyjnym. Polski węzeł jest jednym z węzłów walidacyjnych. Wdrażane są działania, pozwalające rozwijać zdolności integracyjne, oprogramowanie przypadków użycia oraz scenariusze zastosowań. Dla węzła funkcjonującego w środowisku chmurowym uzyskano certyfikat cyberbezpieczeństwa ISO27001. NASK-PIB realizuje ustalenia, wynikające z uczestnictwa w pracach grup roboczych European Blockchain Partnership (EBP). Partnerstwo Polski w ramach w EBP wspiera interoperacyjność i szerokie wdrażanie usług transgranicznych opartych na technologii blockchain oraz oferuje środowisko do rozwoju, w pełni zgodne z przepisami UE, politykami UE oraz modelami zarządzania, które pomagają rozwijać infrastrukturę i usługi blockchain w kraju oraz w całej Europie, podnosząc poziom zaufania i bezpieczeństwa cyfrowych usług administracji publicznej. W ramach projektu NASK-PIB będzie rozwijał zdolności kompetencyjne i badawcze w sprawie cyberbezpieczeństwa blockchain i zastosowań blockchain do wzmacniania odporności i cyberbezpieczeństwa AI.

Projekt EBSI-NE

Cel projektu: rozwój węzłów produkcyjnych EBSI i świadczenia usług wsparcia dla sieci EBSI na poziomie europejskim.

Projekt dofinansowany grantem DEP jest realizowany w ramach międzynarodowego konsorcjum EBSI-NE, rozbudowującego produkcyjną sieć EBSI z zachowaniem niezbędnych wymogów cyberbezpieczeństwa i świadczącego w sposób skoordynowany usługi wsparcia i centra kompetencji oferujące usługi w lokalnych ekosystemach blockchain EBSI. W ramach zadania przewidziany jest wypracowanie dobrych praktyk na poziomie europejskim, w tym rozwój dokumentacji technicznej EBSI i wypracowanie dobrych praktyk i standaryzacji w zakresie cyberbezpieczeństwa EBSI, w tym zasad działania dla wdrożonej certyfikacji ISO 27001.

Projekt EBSI-VECTOR

Cel projektu: zapewnienie weryfikowalnych poświadczeń i rejestrów zaufanych organizacji w EBSI wymiarze europejskim.

Projekt VECTOR dofinansowany grantem DEP jest realizowany w ramach międzynarodowego konsorcjum 52 partnerów z 20 krajów. Umożliwiając weryfikację poświadczeń

zgodnych EBSI dla tożsamości suwerennej, pozwala wykorzystać je w sektorach szkolnictwa wyższego i sektorze zabezpieczenia społecznego. Projekt zmieni cyfrową interakcję studiujących i pracujących obywateli w Europie oraz uprości w sposób zdecentralizowany niektóre złożone procesy weryfikacji dyplomów, uprawnień do leczenia oraz organizacji wydających poświadczenia. Kluczowym celem projektu jest zdefiniowanie i realizacja strategii zwiększania możliwości EBSI i wdrażania usług transgranicznych w różnych krajach z udziałem wielu zaangażowanych uczelni, a także podmiotów w sektorze ubezpieczeń społecznych. Projekt stworzył okazję dla rozwoju zdolności kompetencyjnych i badawczych NASK-PIB w sprawach tożsamości suwerennej.

Projekt EBSI-DC4EU

Cel projektu: zastosowanie blockchain jako ram cyfrowego poświadczenia dla Europy.

Projekt DC4EU dofinansowany grantem DEP jest realizowany w ramach międzynarodowego konsorcjum 80 podmiotów z 23 państw. Ramy zaufania nowego rozporządzenia eIDAS2 są jednym z filarów Unii Europejskiej dla tożsamości i zaufania w świecie cyfrowym. Powstaną ramy dla europejskiego portfela tożsamości cyfrowej jako nowej usługi zaufania. Celem projektu jest opracowanie i przetestowanie środków technicznych, procesów i procedur tworzenia ram zaufania w wybranych obszarach sektorowych. W zgodności z wymaganiami eIDAS2 testowane są wybrane scenariusze wydawania mobilnych dokumentów PDA1 i europejskiej karty ubezpieczenia zdrowotnego (EKUZ) w sektorze zabezpieczenia społecznego. Europejski portfel tożsamości cyfrowej (EUDIW) jest kluczowym elementem hybrydyzacji międzysektorowych i transgranicznych przypadków użycia (tożsamość, podpis, poświadczenia edukacyjne w sektorze szkolnictwa wyższego i zabezpieczenia społecznego). Projekt stworzył okazję dla rozwoju zdolności kompetencyjnych i badawczych NASK-PIB w sprawach usług zaufania, poświadczeń tożsamości i portfeli tożsamości zgodnych z wymogami eIDAS.

5.8. Inne

Projekt Bank danych syntetycznych na potrzeby obliczeń AI i Zaufana Trzecia Strona dla anonimizacji danych

Realizacja i rozliczenie II Etapu projektu pn. „Bank danych syntetycznych na potrzeby obliczeń AI i Zaufana Trzecia Strona dla anonimizacji danych" w ramach dotacji celowej nr 4/WPI/DTC/2022. Efektem realizacji zadania jest m.in. udostępnianie publicznie pod adresem: https://anonimizator.eadministracja.nask.pl, nieodpłatnego demo serwisu do anonimizacji dokumentów w języku polskim.

6. Edukacja i budowanie świadomości

6.1. Kampanie i projekty społeczne

NASK-PIB w 2023 roku zorganizował liczne kampanie edukacyjne i informacyjne oraz działania na rzecz szeroko rozumianego cyberbezpieczeństwa skierowane do różnych grup odbiorców.

Kampania podnosząca świadomość na temat cyberzagrożeń

Kampania organizowana przez Ministerstwo Cyfryzacji oraz NASK-PIB i CERT Polska była współfinansowana ze środków Unii Europejskiej i realizowana w internecie, telewizji, radiu oraz prasie od połowy czerwca do połowy grudnia 2023 roku. Miała formę pięcioodcinkowego serialu. W każdym spocie przedstawiano wybrane cyberzagrożenie i kilka praktycznych wskazówek dla osób, które mogą się znaleźć w podobnej sytuacji.

Kampania Promocja numeru 8080

Kampania podkreślająca zasadność przesyłania do CERT Polska podejrzanych SMS-ów. Kampania rozpoczęła się w 2022 roku, a pod koniec roku 2023 została wznowiona i wzbogacona o informację o nowym, bezpłatnym numerze 8080, na który można przesłać podejrzaną wiadomość.

Europejski Miesiąc Cyberbezpieczeństwa – 11. edycja kampanii

Europejski Miesiąc Cyberbezpieczeństwa (ECMS) to ogólnoeuropejska kampania edukacyjna organizowana przez agencję ENISA (European Union Agency for Cybersecurity) z inicjatywy Komisji Europejskiej, mająca na celu budowanie świadomości cyberzagrożeń i promowanie odpowiedzialnego korzystania z internetu wśród wszystkich jego użytkowników, a także dzielenia się dobrymi praktykami w obszarze cyberhigieny. W Polsce projekt koordynowany jest przez NASK-PIB. Motywem przewodnim 2023 roku były zagadnienia związane z inżynierią społeczną (socjotechniką), czyli wykorzystaniem przez przestępców różnych technik manipulacji stosowanych w kampaniach phishingowych wycelowanych w użytkowników internetu. Hasło przewodnie ECSM 2023 to „Bądź mądrzejszy niż oszust" – zachęcające do mądrego i rozważnego korzystania z internetu. W trakcie trwania polskiej edycji kampanii zgłoszone zostały 81 inicjatywy, które dotarły do ponad 1,5 miliona osób. Publikacja: https://bezpiecznymiesiac.pl/ oraz https://www.nask.pl/pl/aktualnosci/5310,Ponad-15-miliona-odbiorcow-i-rekordowa-liczba-inicjatyw-za-nami-11-edycja-Europe.html

Kampania „Rozsądek online" - jak się nie dać oszukać w sieci!

Kampania promująca bezpieczne zachowania i sposoby na rozpoznawanie i unikanie zagrożeń. W opracowanych przez NASK-PIB materiałach opisane zostały metody stosowane przez oszustów oraz podstawowe zasady weryfikacji informacji. Publikacja: https://bezpiecznymiesiac.pl/bm/baza-wiedzy/1200,quotRozsadek-onlinequot-jak-sie-nie-dac-oszukac-w-sieci.html

Kampania #Halo! Tu cyberbezpieczny Senior

Kampania edukacyjna podnosząca świadomość seniorów na temat oszustw internetowych. Realizowana przez NASK-PIB przy współpracy z Centralnym Biurem Zwalczania Cyberprzestępczości oraz Warszawskim Instytutem Bankowości. W ramach kampanii przygotowano i udostępniono materiały edukacyjne w formie ulotki, plakatu i infografik. Publikacja: https://bezpiecznymiesiac.pl/bm/baza-wiedzy/1181,Halo-Tu-cyberbezpieczny-Senior.html

Kampania Światowy Dzień Backupu

Mini kampania dotycząca tworzenia kopii zapasowych plików. Jak przygotować kopię zapasową, jak często ją wykonywać, gdzie przechowywać? Odpowiedzi na te pytania zostały zawarte w infografice przygotowanej przez NASK-PIB.

Kampania dot. bezpiecznych płatności bezgotówkowych

Kampania NASK-PIB realizowana we współpracy z CSIRT KNF i Centralnym Biurem Zwalczania Cyberprzestępczości dotycząca podstawowych aspektów bezpieczeństwa finansowego użytkowników internetu, zwłaszcza w obszarze

płatności bezgotówkowych. W ramach kampanii opracowano pięć bloków tematycznych: bezpieczne korzystanie z płatności online, e-portfel, karty płatnicze, płatności mobilne i biometria. Każdy z materiałów obejmuje część informacyjną oraz praktyczną sekcję poradniczą.

Publikacja: https://bezpiecznymiesiac.pl/bm/baza-wiedzy/1152,Kampania-dot-bezpiecznych-platnosci-bezgotowkowych.html

Kampania CyberBHP-Cyberbezpieczeństwo w mikro, małych i średnich przedsiębiorstwach

Kampania kierowana do użytkowników biznesowych omawiająca tematykę cyberzagrożeń, ochrony przed atakami typu ransomware, zgłaszania incydentów, cyberhigieny i bezpieczeństwa w miejscu pracy. W ramach kampanii opracowano i opublikowano na stronie Bezpieczny Miesiąc pakiet sześciu broszur.

Publikacja: https://bezpiecznymiesiac.pl/bm/baza-wiedzy/1046,CyberBHP-Cyberbezpieczenstwo-w-mikro-malych-i-srednich-przedsiebiorstwach.html

Kampania CYBERbezpieczne Święta

Mini kampania podnosząca świadomość cyberzagrożeń i bezpiecznego korzystania z urządzeń, skierowana do dorosłych użytkowników internetu. W jej ramach przedstawiono zbiór porad tzw. 6 kroków do CYBERbezpiecznych Świąt.

Publikacja: https://bezpiecznymiesiac.pl/bm/aktualnosci/1204,6-krokow-do-cyberbezpiecznych-Swiat.html

Kampania „Chill w relau – moje korzyści z bycia offline"

Kampania edukacyjno-informacyjna skierowana do uczniów w wieku 13 – 17 lat, promująca świadome kontrolowanie czasu spędzonego w sieci.

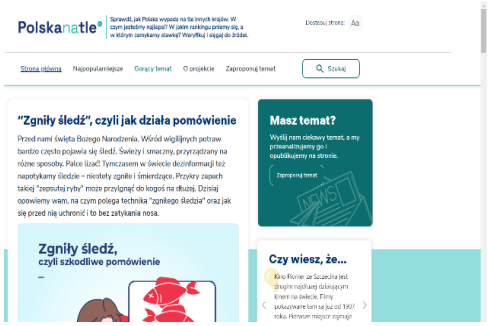
Projekt I kampania Make It Clear – educating young people against disinformation online

(Projekt MIC2022 współfinansowany ze środków Komisji Europejskiej Creative Europe)

Projekt Komisji Europejskiej realizowany przez konsorcjum NASK-PIB, Latvian Internet Association oraz Save the Children Romania, którego celem jest rozwój kompetencji informacyjnych, a także świadomego i krytycznego podejścia młodzieży do treści udostępnianych online. Projekt obejmuje m.in. organizację międzynarodowego creathonu dla młodzieży i międzynarodowej konferencji dla nauczycieli, realizację kampanii informacyjno-edukacyjnej, a także przygotowanie materiałów edukacyjnych w 5 wersjach językowych (PL, EN, RO, LV, UA): 18 modułów lekcji, materiału dydaktycznego dla nauczycieli, edukacyjnej gry planszowej. Więcej: www.makeitclear.edu.pl.

Kampania „Mierzymy się ze smogiem"

Kampania edukacyjno-informacyjna pod hasłem „Mierzymy się ze smogiem" przeprowadzona w mediach o zasięgu ogólnopolskim: w telewizji, na portalach internetowych i Facebooku. Kampania miała na celu zachęcenie Polaków do regularnego sprawdzania stanu powietrza i chronienia w ten sposób swojego zdrowia. Zasięg: 4,5 mln odbiorców.



Serwis internetowy Polska na tle

Serwis internetowy, którego celem jest popularyzowanie korzystania ze źródeł i weryfikowania informacji, a co za tym idzie – prebunkingowe ostanianie społeczeństwa przed dezinformacją. Projekt wspierany merytorycznie przez: **PIE, KOWR, WIB oraz serwis #FakeHunter**.

Kampania w mediach społecznościowych „Włącz Weryfikację na platformach Facebook i X".

Działania w mediach społecznościowych miały regularny charakter. Alerty oraz ważne informacje były tworzone na podstawie aktualnego monitoringu infosfery, a posty edukacyjne publikowane według media planu. Wpisy publikowane na profilach „Włącz Weryfikację" były udostępniane (podawane dalej) zarówno przez prywatnych użytkowników, jak instytucje, m. in. lokalne komendy policji, ministerstwa czy urzędy takie jak Zakład Ubezpieczeń Społecznych. W 2023 roku uzyskano:

- Ponad **8 mln** zasięgu publikacji w mediach społecznościowych;
- Ponad **12 tys.** obserwujących na Facebooku;
- Ponad **26 tys**. na platformie X.

Projekt i kampania Bezpieczne Wybory

Projekt ukierunkowany na zapewnienie bezpieczeństwa informacyjnego i ochrony przed cyberzagrożeniami związanymi z wyborami parlamentarnymi. Strona bezpiecznewybory.pl zawierała materiały edukacyjne i formularze do zgłaszania incydentów. W ramach działań edukacyjnych zorganizowano spotkanie edukacyjne dla przedstawicieli wszystkich komitetów wyborczych.

W ramach działania przeprowadzono szeroko zakrojoną kampanię informacyjną online i offline. Organicznie publikowano posty o projekcie w kanałach społecznościowych NASK-PIB i Włącz Weryfikację. Przeprowadzono aktywności z zakresu media relations (informacja prasowa z komentarzem dyrektora NASK-PIB oraz wypowiedziami przedstawicieli Google, Meta i TikToka). W ramach działań płatnych zrealizowano kampanię online i offline. Bannery informacyjne kierujące do serwisu www.bezpiecznewybory.pl pojawiły się w mediach społecznościowych oraz w internecie w ramach Google Display Network a także na wybranych stronach internetowych w ramach współpracy Działu Komunikacji i PR z domem mediowym. Film wideo promujący serwis pojawił się online oraz w komunikacji miejskiej w wybranych miastach w całej Polsce. Dodatkowo banner informujący o projekcie zamieszczony był na wybranych paczkomatach InPost na terenie całej Polski.

Kampania online przyniosła prawie 75 mln zasięgu.
Kampania offline miała prawie 18 mln zasięgu

Kampania Sprawdź zanim udostępnisz

Kampania zrealizowana we współpracy z **Ministerstwem Cyfryzacji i brytyjskim Cabinet Office Government Communication Services Internationa (UK GCSI)**. W ramach działania powstała strona internetowa sprawdzam.info, która w pigułce przekazuje zasady dotyczące weryfikacji treści w internecie. Zasięg kampanii online zakupionej przez Ministerstwo Cyfryzacji (poprzez dom mediowy) **wyniósł 24 mln wyświetleń** (dane domu mediowego). Zasięg działań media relations przeprowadzonych przez Dział Komunikacji i PR oszacowano na **4 mln** i **422 wzmianki** (dane IMM).

Kampania „fałszywe smsy"

Kampania „Fałszywe SMSy" miała na celu poinformowanie wszystkich użytkowników telefonów komórkowych o zagrożeniu w postaci fałszywych SMSów i drodze ich zgłaszania pod nowy numer 8080. Kampania kierowała na stronę www.polskanatle.pl, gdzie przygotowano artykuły dotyczące tego zagrożenia, zawierające porady dla użytkowników telefonów czy porównania skali wyłudzeń poprzez tę metodę oszustwa.

Gra paragrafowa z CD-Action:
Projekt dotyczył walki ze zjawiskiem dezinformacji w mediach społecznościowych. W ramach kampanii stworzono grę paragrafową oraz opracowano cykl materiałów edukacyjnych na www.cdaction.pl dotyczącą zjawiska dezinformacji w sieci. Komunikacja w kampanii została wsparta m.in. przez influencerów: Izak, Jakub Ćwiek, Przemek Staroń (Szkoły Staronia), Adrian Bruździak.

6.2. Działania edukacyjno-szkoleniowe w obszarze cyberbezpieczeństwa

NASK-PIB realizuje szereg projektów o charakterze edukacyjnym i szkoleniowym, na rzecz bezpieczeństwa użytkowników internetu oraz podnoszenia poziomu świadomości i kompetencji cyfrowych. Działania te związane są z realizacją zapisów ustawy o Krajowym Systemie Cyberbezpieczeństwa, zgodnie z którą do zadań CSIRT NASK należy m.in. wspieranie podmiotów krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa oraz prowadzenie działań z zakresu budowania świadomości na temat cyberbezagrożeń. Szkolenia swoim zakresem obejmują przede wszystkim podstawowe zasady cyfrowej higieny.

Działania w liczbach:

- blisko **300 wystąpień** ekspertów NASK-PIB na konferencjach naukowych, edukacyjnych i wydarzeniach branżowych,
- ponad **3300 szkoleń** dla różnych grup odbiorców,
- ponad **450 000 uczestników** szkoleń i konferencji.

W 2023 roku zrealizowano:

- Szkolenia dla podmiotów krajowego systemu cyberbezpieczeństwa realizowane m.in. we współpracy z ministerstwem cyfryzacji (29 szkoleń, 9 685 osób).
- Szkolenia w ramach umowy dotacyjnej „Działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa w 2023 roku – podnoszenie odporności Rzeczypospolitej Polskiej na zagrożenia w przestrzeni cyfrowej" – 2 959 szkoleń stacjonarnych (5 288 osób), w większości indywidualnych lub kilkuosobowych. Szkolono pracowników wysokiego szczebla administracji państwowej i samorządowej, a także m.in. pracowników podstawowej opieki zdrowotnej i Krajowego Biura Wyborczego.
- Szkolenia dla szkół oraz uczelni wyższych –zdalne lub stacjonarne (13 szkoleń, 1 278 osób),
- Szkolenia dla policjantów z oddziałów prewencji i profilaktyki – 2 szkolenia dla w sumie 165 osób,
- Międzynarodowe wysokospecjalistyczne warsztaty cyberbezpieczeństwa dla sektora energii – zorganizowane przez ministerstwo cyfryzacji i NASK w dniach 10-12 stycznia 2023 roku, przeprowadzone przez amerykańskich wykładowców (US Department od Energy/Idaho National Lab) dla 50 uczestników z Ukrainy, Holandii, Litwy, Niemiec, Słowacji, Czech i Polski,

- Szkolenia dla różnych grup wiekowych i społecznych dot. zjawiska dezinformacji – w formule warsztatów, szkoleń, webinarów – 70 wydarzeń dla ok. 35 000 osób.
- Warsztaty regulacyjne dot. obszaru domen internetowych – 4 spotkania dla łącznie 260 osób,
- Szkolenie (online) z cyberhigieny dla studentów pierwszego roku śląskich uczelni (PŚ, UŚ, UEwK, Akademia WSB w Dąbrowie Górniczej) w ramach Cyber Science, który ukończyło ok. 6 000 studentów,
- European Cybersecurity Challenge – coroczne zawody europejskie cyberbezpieczeństwa w formule CTF (Capture The Flag) – koordynacja projektu w Polsce, organizacja kwalifikacji krajowych oraz przygotowania polskiej drużyny do międzynarodowych zawodów. W 2023 r zawody odbyły się w dniach 24-27 października w Norwegii. Polska drużyna zajęła 9 miejsce na 33 startujące drużyny,
- Organizacja i współorganizacja przez NASK-PIB wielu konferencji i różnych wydarzeń oraz udział ekspertów NASK-PIB w wydarzeniach organizowanych przez inne podmioty. (patrz rozdział Konferencje i wydarzenia).

Webinary CYBERTEMATYCZNIE

Cykl webinarów skierowany do użytkowników internetu poruszający tematykę cyberbezpieczeństwa i przeciwdziałania dezinformacji, rozwoju nowych technologii i budowania społeczeństwa informacyjnego. Publikacja: https://bezpiecznymiesiac.pl/bm/baza-wiedzy/1037,CYBERTEMATYCZNIE.html

Działania edukacyjno-informacyjne prowadzone w ramach OSE

Portale OSE
W 2023 roku na bieżąco rozbudowywane były portale OSE: ose.gov.pl i OSE IT Szkoła. W ramach bieżącej obsługi administracyjnej m.in. publikowano artykuły (łącznie 170 unikalnych aktualności), aktualizowano treści na podstronach i uruchamiano nowe zakładki. Dodatkowo na platformie e-learningowej OSE IT Szkoła zostały wdrożone produkcyjnie końcowe moduły kursu „Internetowa szkoła słonia Spacjusza" oraz „Kurs podstawowy nauki gry w szachy – część 3" Na platformie pojawiło się także 6 nowych publikacji edukacyjnych.

ose.gov.pl – 227 tys. użytkowników, 646 tys. wyświetleń
OSE IT Szkoła – 77 tys. użytkowników, 1,08 mln wyświetleń, 2 nowe kursy, 6 nowych publikacji edukacyjnych

Projekt OSEhero
Do udziału w projekcie po raz kolejny zgłosili się nauczyciele z całej Polski, którzy zdobywają i przekazują swoim uczniom wiedzę na temat cyberbezpieczeństwa.

W edycji 2022/2023, której podsumowaniem był Zlot OSEhero, tytuły i certyfikaty zdobyło 363 uczestników. We wrześniu 2023 r. rozpoczęła się edycja 2023/2024, do której zgłosiła się rekordowa liczba nauczycieli – aż 1795 osób. Do zakończenia edycji w czerwcu 2024 roku uczestnicy projektu będą brać udział w szkoleniach i „spotkaniach przy kawie" oraz organizować w swoich szkołach inicjatywy związane z cyberbezpieczeństwem.

edycja 2022/2023
4 szkolenia, 7 „spotkań przy kawie", 757 uczestników, 363 osób z tytułem OSEhero, 992 zorganizowane w szkołach inicjatywy związane z cyberbezpieczeństwem
Statystyki – edycja 2023/2024
1795 uczestników, w planach: 5 szkoleń, 28 „spotkań przy kawie"

Projekt Bezpieczni w sieci (BWS)
Na platformie e-learningowej bezpieczniwsieci.edu.pl nauczyciele, uczniowie klas 7–8 szkół podstawowych i szkół ponadpodstawowych mogą skorzystać z e-kursów, scenariuszy i materiałów pomocniczych w zakresie zagrożeń online. W 2023 r. trwały prace nad kolejnym modułem dotyczącym cyfrowej higieny.

Treści w sześciu modułach tematycznych – 18 kursów, 12 scenariuszy zajęć
55 tys. aktywowanych kont
W 2023 r. ponad 200 tys. wyświetleń, 9,1 tys. użytkowników

Pracownia Kompetencji Cyfrowych
W 2023 roku odbył się konkurs „Pracownia Kompetencji Cyfrowych" dla wszystkich szkół w Polsce. Uczniowie podzieleni na kategorie wiekowe mieli zrealizować wskazany kurs e- learningowy i przygotować pracę zgłoszeniową. Celem było zaangażowanie jak największej liczby uczniów w szkole oraz poszerzenie wiedzy z zakresu bezpieczeństwa w sieci i wykorzystanie jej w kreatywny sposób. Realizacja działań szkoleniowych oraz konkursu finansowana była ze środków POPC w ramach III osi priorytetowej Cyfrowe kompetencje społeczeństwa, Działanie 3.2 Innowacyjne rozwiązania na rzecz aktywizacji cyfrowej.

Ponad 3000 zgłoszeń
Nagrody: 832 mobilne pracownie komputerowe uzupełnione o interaktywny ekran, dostarczane do szkół,

Mistrzowie Energii
W 2023 roku został rozstrzygnięty ogłoszony w 2022 roku konkurs „Mistrzowie Energii", w którym zadaniem uczniów było zorganizowanie dowolnej szkolnej inicjatywy dotyczącej oszczędzania energii.

448 zgłoszeń
Nagrody: 50 kart podarunkowych o wartości 2000 zł każda, do wykorzystania na cele edukacyjne

W projekcie „Mistrzowie Energii" prowadzone były również działania edukacyjne:
– opracowanie scenariuszy lekcji na temat oszczędzania energii przygotowanych przez ekspertów dla wszystkich poziomów szkoły podstawowej, publikacja materiałów na platformie eduESA;
– kampania świadomościowa na Facebooku – seria postów tematycznych na temat oszczędzania energii, zasięg: blisko 22 tys. odbiorców.

Wydarzenia dla nauczycieli, dyrektorów szkół, ale też uczniów i rodziców, m.in. przybliżających zagadnienia związane z cyberbezpieczeństwem i programowaniem

Kongres OSE: 2,2 tys. uczestników (stacjonarnie i online), liczba wyświetleń transmisji: 3,5 tys.
Szachowe Grand Prix OSE: 846 uczestników – uczniów szkół podstawowych z całej Polski
Wielkie Święto Programowania – łącznie ponad 3 tys. uczestników

Meta VR & AR dla Edukacji
Od kwietnia do grudnia 2023 roku we współpracy z firmą Meta oraz VRheroes organizowane były bezpłatne szkolenia dla nauczycieli ze szkół podstawowych i ponadpodstawowych, dotyczące wykorzystania wirtualnej rzeczywistości w szkole. Po stronie NASK-PIB znalazła się część szkolenia dotycząca bezpiecznego korzystania z rozwiązań VR i AR w edukacji.

36 szkoleń
Przeszkolonych ponad 1000 nauczycieli

Dodatkowo eksperci OSE brali udział w działaniach edukacyjnych w mediach (m.in., występowali w audycjach radiowych i telewizyjnych), brali udział w zewnętrznych konferencjach oraz akcjach edukacyjnych dla nauczycieli, rodziców i uczniów.

Edukacyjna Sieć Antysmogowa (ESA)

Ogólnopolski program edukacyjno-informacyjny, który łączy edukację ekologiczną z budowaniem kompetencji cyfrowych dzieci i dorosłych.

ESA w liczbach:

- **2256** placówek edukacyjnych w programie ESA
- **1729** stacji pomiarowych
- **700 tys.** uczestników programu ESA
- **4,5 mln** odbiorców kampanii „Mierzymy się ze smogiem"
- **43,5 tys.** użytkowników platformy eduESA
- **4,7 tys.** uczestników Olimpiady ESA

Projekt „Wykorzystanie technologii cyfrowych dla podniesienia kompetencji społeczeństwa w walce ze SMOGiem w Polsce"

Projekt: „Wykorzystanie technologii cyfrowych dla podniesienia kompetencji społeczeństwa w walce ze SMOGiem w Polsce" współfinansowany ze środków europejskich w ramach Programu Operacyjnego Polska Cyfrowa, skierowany do środowisk szkolnych oraz szerokiej opinii publicznej. Na projekt składały się:

- konkurs dla szkół podstawowych i ponadpodstawowych, w którym do zdobycia był sprzęt do prowadzenia pomiarów jakości powietrza i cyfrowej edukacji ekologicznej;

- instalacja w zwycięskich placówkach 1600 wewnętrznych ekranów edukacyjnych oraz 100 mierników jakości powietrza i tablic informacyjnych LED;

- działania edukacyjne: webinary dla nauczycieli (ok. 1000 przeszkolonych nauczycieli), dostęp do cyfrowych materiałów edukacyjnych na platformie eduESA;

-kampania edukacyjno-informacyjna pod hasłem „Mierzymy się ze smogiem" przeprowadzona w mediach o zasięgu ogólnopolskim: w telewizji, na portalach internetowych i Facebooku. Kampania miała na celu zachęcenie Polaków do regularnego sprawdzania stanu powietrza i chronienia w ten sposób swojego zdrowia. Zasięg: 4,5 mln odbiorców.

Ogólnopolska Olimpiada Antysmogowa

Zorganizowana została II edycja ogólnopolskiego konkursu wiedzy dla uczniów klas 7 i 8 w formule online. Tematyka koncentrowała się wokół zagadnień związanych z ochroną powietrza i zmianą klimatu. Do udziału w tej edycji konkursu zgłosiło się niemal 4700 uczniów. Konkurs znalazł się w wykazie konkursów punktowanych przy rekrutacji do szkół ponadpodstawowych 14 kuratoriów oświaty w Polsce.

Technikon ESA

Konkurs z zakresu zanieczyszczenia powietrza i zmiany klimatu dla szkół technicznych. Uczniowie w 5-osobowych drużynach pod opieką nauczyciela tworzyli projekty, w których wykorzystywali branżową wiedzę zdobywaną w szkole oraz cyfrowe, innowacyjne rozwiązania do budowania praktycznych rozwiązań przyszłości. W 2024 roku konkurs odbędzie się w formule ogólnopolskiej.

Cyberprofilaktyka NASK (poprzednio Akademia NASK)

Odpowiada na wyzwania, jakie niesie ze sobą rozwój nowych technologii cyfrowych. Działania profilaktyczne koncentrują się na szeroko rozumianej tematyce bezpieczeństwa w sieci dzieci i młodzieży. Podejmowane są aktywności związane z kształtowaniem świadomości społecznej w zakresie bezpieczeństwa w sieci dzieci i młodzieży poprzez m.in. prowadzenie lekcji oraz szkoleń, udział w konferencjach oraz merytoryczne opracowanie materiałów edukacyjnych. W ramach marki redagowana jest edukacyjna strona internetowa wraz blogiem eksperckim oraz prowadzone są profile w mediach społecznościowych na platformie Facebook oraz YouTube.

W 2023 roku przeprowadzono następujące działania edukacyjne:

- **Uczniowie szkół podstawowych i ponadpodstawowych**

  7 lekcji online – 39 300 uczniów

  65 lekcji stacjonarnych – 2 225 uczniów

- **Nauczyciele i osoby pracujące z dziećmi**

  12 spotkań (webinary, szkolenia, prelekcje) – 1 500 uczestników
- **Rodzice**

  22 spotkania (online i stacjonarnie) – 650 uczestników

Cyberlekcje 3.0

Projekt jest inicjatywą Ministerstwa Cyfryzacji i NASK-PIB, skierowaną głównie do nauczycieli szkół podstawowych i ponadpodstawowych. Jego celem jest wspieranie nauczania o bezpiecznym korzystaniu z internetu poprzez dostarczenie gotowych narzędzi dydaktycznych do prowadzenia zajęć. Dostosowano 9 z 18 scenariuszy Cyberlekcji do nauczania problemowego (metoda Project Based Learning). Scenariusze dla szkół podstawowych i średnich wraz z kartami pracy są dostępne w bazie wiedzy na gov.pl praz na Zintegrowanej Platformie Edukacyjnej.

Rada Doradcza Rodziców

We wrześniu 2022 roku utworzono Radę Doradczą Rodziców, której członkami są eksperci NASK, blogerzy parentingowi oraz rodzice uczniów z C.P.U. Młodzieżowego Panelu Doradczego. W maju 2023 roku przeprowadzono konsultacje online w formie webankiety z rodzicami i opiekunami, których celem była diagnoza potrzeb rodziców w zakresie bezpieczeństwa dzieci i młodzieży online. W II półroczu 2023 roku w nowym cyklu „Cyfrowe wieczory dla rodziców" przeprowadzono 4 eksperckie webinary.

4 Webinary z cyklu „Cyfrowe wieczory dla rodziców"

- Bezpieczeństwo dzieci w erze internetu.
- Co rodzice powinni wiedzieć o mediach społecznościowych, ale wstydzą się zapytać?
- 100% sok z pomarańczy czy napój owocowy? Czyli jak rodzic może pomóc swojemu dziecku uniknąć konsumpcji dezinformacji.
- Cyfrowa higiena dla najmłodszych, czyli jak wprowadzić dobre nawyki od dzieciństwa.

„Rodzic 3.0"

Celem partnerstwa merytorycznego w projekcie Warszawskiego Centrum Innowacji Edukacyjno-Społecznych i Szkoleń (WCIES) „Rodzic 3.0" jest podnoszenie świadomości dotyczącej cyberbezpieczeństwa wśród dzieci i młodzieży, poprzez edukację

rodziców i opiekunów. Przeprowadzono **6 webinarów** dla rodziców z udziałem ekspertów NASK-PIB.

- Jak chronić dzieci przed zagrożeniami w sieci (cyberprzemoc, pornografia i inne, część I i II),
- Ochrona prywatności własnej i cudzej w sieci, zagrożenia związane z brakiem dbałości o własną prywatność ,
- Jak radzić sobie z hejtem/mową nienawiści w internecie w mediach społecznościowych? (Część I. II. III).

Ostrożni w sieci

Celem partnerstwa merytorycznego w projekcie EY „Ostrożni w sieci" było podnoszenie świadomości dotyczącej cyberbezpieczeństwa wśród dzieci i młodzieży, poprzez edukację rodziców i opiekunów. Nagrano 4 webcasty z udziałem ekspertów z NASK-PIB oraz opracowano 4 broszury dla rodziców, które dostępne są na stronie Ostrożni w sieci | EY Polska.

Cykle edukacyjne na FB oraz YT

- Granie w gry online i uzależnienie – porady dla rodziców – 6 filmików,
- „Bezpieczne wakacje" porady dla rodziców – 6 filmików.

Polskie Centrum Programu Safer Internet

saferinternet.pl

Projekt PSIC2022 współfinansowany ze środków Komisji Europejskiej Digital Europe) Konsorcjum PCPSI tworzą NASK-PIB oraz Fundacja Dajemy Dzieciom Siłę. Centrum realizuje działania edukacyjne i uświadamiające, podnoszące bezpieczeństwo dzieci i młodzieży w internecie, jak również działania pomocowe polegające na reagowaniu na nielegalne treści w internecie oraz udziela wsparcia poprzez telefony zaufania 116 111 oraz 800 100 100. Centrum należy również do międzynarodowych sieci INSAFE i INHOPE (opisane w części Współpraca Międzynarodowa). Przy PCPSI działają ciała doradcze – Komitet Konsultacyjny (przedstawiciele różnych instytucji i organizacji), Młodzieżowy Panel Doradczy oraz Rada Doradcza Rodziców. Więcej: www.saferinternet.pl.

W ramach Polskiego Centrum Programu Safer Internet w 2023 r. NASK-PIB zorganizował:

Obchody Dnia Bezpiecznego Internetu (DBI) 2023 pod hasłem „Działajmy razem!"

3000 uczestników gali DBI

4 674 inicjatyw DBI

1,5 mln uczestników obchodów DBI

1500 wzmianek medialnych w trakcie trwania kampanii DBI 2023

32 lekcje online

276 000 uczniów

19 webinarów dla profesjonalistów

4300 profesjonalistów sektora edukacyjnego

17. edycja Międzynarodowej Konferencji „Bezpieczeństwo dzieci i młodzieży w internecie"

- 4 dni spotkań
- 400 uczestników w formule stacjonarnej
- 1895 uczestników w formule online
- 15 sesji plenarnych
- 8 warsztatów prowadzonych w językach PL i ANG
- 32 ekspertów z Polski i zagranicy

Cyfrowa Przyszłość Ucznia (CPU) - Młodzieżowy Panel Doradczy

Młodzieżowy panel doradczy działa przy NASK-PIB od 2011 roku. Celem CPU jest konsultowanie i testowanie z młodzieżą nowych materiałów edukacyjnych, wypracowywane są hasła promujące bezpieczeństwo w internecie, młodzież dzieli się także swoimi doświadczeniami w zakresie ich aktywności online, a także internetowych trendów. W 2023 r. przedstawiciele CPU wzięli udział w 4 spotkaniach w formule warsztatowej (w tym jednym wyjazdowym), a także reprezentowali Polskę podczas Safer Internet Forum w Brukseli.

- 60 uczniów w wieku 13- 17 lat
- 11 szkół zlokalizowanych na terenie całej Polski

Spektakle dla dzieci „Dzieci Sieci – Plik i Folder na tropie internetowych kłopotów"

- 90 tys. uczestniczących dzieci oraz 10 spektakli online dla klas I – III, IV – VI

6.3. Szkolnictwo wyższe

Szkoła Doktorska TIB PAN

W 2023 roku NASK-PIB kontynuował działania w ramach Szkoły Doktorskiej Technologii Informacyjnych i Biomedycznych Instytutów PAN. W związku z uzyskaniem przez NASK-PIB, zgodnie z art. 198 ust. 5 ustawy z dnia 20 lipca 2018r. Prawo o szkolnictwie wyższym i nauce, uprawnień do prowadzenia szkoły doktorskiej, na mocy aneksu do umowy o utworzeniu i prowadzeniu Szkoły Doktorskiej Technologii Informacyjnych i Biomedycznych Instytutów PAN, w dniu 18.05.2023 roku status NASK-PIB uległ zmianie z Jednostki Współpracującej na Jednostkę Prowadzącą Szkołę. Przedstawicielem NASK-PIB w Radzie Dyrektorów był dr hab. inż. Michał Karpowicz, a członkami Rady Szkoły - dr hab. inż. Szymon Łukasik oraz dr hab. Joanna Kołodziej. Funkcję lokalnego koordynatora Szkoły w NASK-PIB pełnił dr hab. inż. Szymon Łukasik.

W 2023 roku kształcenie w Szkole Doktorskiej kontynuowało 5 doktorantów z NASK-PIB:

- mgr Mateusz Koryciński (temat: „System wspomagania decyzji w zabiegach neurochirurgicznych, identyfikujący na podstawie badań fMRI ośrodki elokwentne kory mózgowej odpowiedzialne za mowę", promotor: prof. dr hab. inż. E. Niewiadomska-Szynkiewicz (NASK-PIB/PW), promotor pomocniczy: dr inż. Konrad Ciecierski (NASK-PIB)),
- mgr inż. Kamila Lis (temat: "Sensitive applications user profiling using machine learning methods", promotor: prof. dr hab. inż. E. Niewiadomska-Szynkiewicz (NASK-PIB/PW), promotor pomocniczy: dr inż. A. Sikora (NASK-PIB)),
- mgr inż. Karolina Seweryn (temat: „Object and Event Identification in Video Guided with Natural Language Processing of Video Content Description", promotor: dr hab. inż. Szymon Łukasik (NASK-PIB), promotor pomocniczy: dr inż. Anna Wróblewska (PW)),
- mgr Daria Stetsenko (temat: „Automated Harmful Content Detection Using Grammar-Focused Representations of Text Data", promotor: dr hab. inż. Szymon Łukasik (NASK-PIB), dr Inez Okulska (NASK-PIB)),
- mgr inż. Michał Koźbiał (temat: „Anatomical and behavioral silhouette biometrics for age and activity determination with application to detection of illegal internet contents", promotor: prof. dr hab. inż. Andrzej Pacut (NASK-PIB)).

W ramach rekrutacji na rok akademicki 2023/2024 zgłoszono 8 tematów badawczych, a Zespół Rekrutacyjny NASK-PIB na posiedzeniach w dniu 07.07.2023 r. oraz 15.09.2023 r. przeprowadził rozmowy kwalifikacyjne z kandydatami i rekomendował przyjęcie do Szkoły Doktorskiej TIB PAN 4-ech doktorantów:

- mgr inż. Joannę Gajewską (temat: „Integration of video analysis and multimodal fusion techniques to detect visual and covert anomalies in synthetic materials such as deepfakes", promotor: Xin Yu, PhD (The University of Queensland), promotor pomocniczy: dr inż. Ewelina Bartuzi-Trokielewicz (NASK-PIB)),

- mgr inż. Mateusza Bursiaka (temat: „Robustness of machine learning models considering adversarial conditions", promotor: dr hab. J. Kołodziej (NASK-PIB), promotor pomocniczy: dr inż. M. Krzysztoń (NASK-PIB)),

- mgr inż. Jakuba Postępskiego (temat: „Neurosurgical Support System for Craniofacial Access Procedures", promotor: dr hab. inż. G. Borowik (NASK-PIB), promotor pomocniczy: dr inż. K. Ciecierski (NASK-PIB)),

- mgr inż. Dipendrę Kumara Singh (temat: "Study on the behavior of third-generation neural network models in NLP applications", promotor: dr hab. inż. G. Borowik (NASK-PIB)).

Na posiedzeniu w dniu 06.09.2023 r. Komisja Oceny Śródokresowej w składzie:

- dr hab. inż. Szymon Łukasik (NASK-PIB) – przewodniczący,
- dr hab. inż. Mariusz Kamola, prof. instytutu (NASK-PIB),
- dr hab. inż. Piotr Gawrysiak, prof. uczelni (Politechnika Warszawska),

pozytywnie oceniła realizację indywidualnego planu badawczego przez doktorantkę mgr. inż. Kamilę Lis.

W semestrze letnim roku akademickiego 2022/2023 pracownicy NASK-PIB przeprowadzili wykłady:

- "Introduction to cybersecurity" – dr inż. Adam Kozakiewicz,

- "Artificial Intelligence Methods in Distributed Computing Systems (AlinDC)" – dr hab. Joanna Kołodziej,

a w semestrze zimowym 2023/2024:

- "Advanced tools of cryptanalysis" – dr inż. Michał Wroński.

Szkoła Doktorska NASK-PIB

W 2023 roku w NASK-PIB podjęte zostały prace nad utworzeniem samodzielnej szkoły doktorskiej prowadzonej przez instytut. W ich ramach przygotowany został projekt programu kształcenia i zasad rekrutacji. Szkoła Doktorska NASK-PIB powołana została Zarządzeniem Dyrektora NASK-PIB z 29 listopada 2023 roku.

OSA UW

W semestrze letnim 2023/2024 pracownicy Centrum Badań i Rozwoju NASK-PIB prowadzili w Ośrodku Studiów Amerykańskich Uniwersytetu Warszawskiego zajęcia dla studentów studiów II stopnia p.t. "Practical Project: AI - Science and Ethics (Projekt praktyczny: Sztuczna Inteligencja - nauka i etyka)". W ciągu całego semestru studenci i studentki opracowywali praktyczne projekty związane ze sztuczną inteligencją, których kontekst merytoryczny stanowiły spotkania z naukowcami i naukowczyniami Pionu Sztucznej Inteligencji NASK-PIB.

Studia podyplomowe

NASK-PIB z Politechnika Śląską, Uniwersytetem Śląskim oraz Uniwersytetem Ekonomicznym w Katowicach powołał konsorcjum naukowe – Śląskie Centrum Inżynierii Prawa, Technologii i Kompetencji Cyfrowych „Cyber Science". W 2023 roku, w ramach „Cyber Sciene", 90 studentów ukończyło pierwszą edycję studiów podyplomowych, w tym 53 osób specjalność Zarządzanie Cyberbezpieczeństwem, a 37 specjalność Tokenizacja i automatyzacja w gospodarce cyfrowej, aspekty prawne techniczne i ekonomiczne. W kolejnej edycji studiów w roku akademickim 2023/24 realizowane są dwa kierunki:

- Zarządzanie Cyberbezpieczeństwem (prowadzony przez Politechnikę Śląską),
- Tokenizacja i automatyzacja w gospodarce cyfrowej, aspekty prawne techniczne i ekonomiczne (prowadzony przez Uniwersytet Śląski).

Liczba studentów obu specjalności to 80 osób, a zajęcia sprowadzone są m.in, przez 10 wykładowców z NASK-PIB.

6.4. Praktyki i programy stażowe

W NASK-PIB prowadzone są praktyki i programy stażowe. W latach 2022 - 2023, NASK-PIB zrealizował jeden z największych programów stażowych w Polsce – „Kariera Jutra", którego celem była trwała integracja osób młodych na rynku pracy.

Projekt realizowany był w 3 turach, w latach 2022-2023, we współpracy z Google i SGH. Wartość projektu to 12.954.419,72 zł. Skierowany był do osób w wieku 18–30 lat, które nie miały stałego zatrudnienia, w szczególności kobiet z terenów wiejskich i małych miejscowości, a także osób z niepełnosprawnościami . Kandydaci uczestniczyli w 2 edycjach 8-tygodniowego szkolenia „Umiejętności Jutra" w dziedzinie marketingu internetowego. Łącznie w szkoleniach wzięło udział 17.163 osoby. Zrekrutowano 2493 mikro, małe i średnie przedsiębiorstwa oraz organizacje pozarządowe. Po ukończonym szkoleniu i egzaminie kandydaci odbierali certyfikaty i mogli aplikować na wybraną ofertę stażową. W trakcie projektu podpisano 1002 umowy stażowe. 975 osób ukończyło 3-miesięczne staże. Część z absolwentów kontynuowało współpracę z organizacjami, w których odbywali staż.

Ogółem w 2023 roku w programach wzięło udział łącznie 714 osób.

Rozwój i dobrostan Pracowników NASK-PIB

NASK-PIB realizuje programy kształtujące politykę kadrową oraz rozwój i budowanie marki instytutu, jako pracodawcy. W 2023 roku w NASK-PIB prowadzone były programy rozwojowe, organizowano szkolenia wewnętrzne, a także inicjatywy pracownicze, których celem było zadbanie o dobrostan pracowników. W NASK-PIB w 2023 roku miały miejsce wydarzenia dla wszystkich pracowników instytutu, takie jak: impreza

integracyjna, Dzień Dziecka i Mikołajki dla dzieci pracowników, akcje krwiodawstwa, spływy kajakowe oraz wieczory planszówek.

Dbając o dobrostan pracowników NASK-PIB zapewnia się dostęp do programów opieki medycznej, kart sportowych, grupowego ubezpieczenia na życie i programu Pracowniczych Planów Kapitałowych. Ważnym elementem wspierającym pracowników jest możliwość skorzystania ze środków Zakładowego Funduszu Świadczeń Socjalnych w postaci wypłaty tzw. „wczasów pod gruszą", dofinansowania do zakupu literatury i sztuki, wsparcie socjalne dla pracowników w postaci zapomogi losowej i niskooprocentowanych pożyczek.

6.5. Konferencje i wydarzenia

W 2023 roku NASK-PIB brał udział w licznych wydarzeniach związanych z obszarem działalności instytutu, a szczególnie z szeroko rozumianym cyberbezpieczeństwem i wypełnianiem przez NASK-PIB roli jednego z sektorowych CSIRT-ów. Najważniejsze konferencje i wydarzenia branżowe, w których instytut był organizatorem, współorganizatorem lub partnerem:

Styczeń

- 26 stycznia - CENTR & LACTLD joint webinar – prezentacja Rejestru .pl „Moving from direct registrations to registry-registrar model, udział merytoryczny przedstawicieli NASK-PIB

Luty

- 7 lutego -Dzień Bezpiecznego Internetu, NASK-PIB współorganizatorem
- 8 lutego - 56th CENTR Administrative workshop – NASK-PIB Panelistą na warsztatach
- 9 lutego -Konferencja pod hasłem „Zwalczanie dezinformacji w czasie wojny – doświadczenia Europy, Polski i Ukrainy" w Parlamencie Europejskim w Brukseli, udział merytoryczny przedstawicieli NASK-PIB
- 22 lutego – seminarium naukowe dr Jana Kołodyńskiego z Politechniki Warszawskiej „Sensory kwantowe - perspektywy technologiczne vs motywacje naukowe", NASK-PIB organizatorem

Marzec

- 1 marca – seminarium naukowe dr Keatona Hamma z The University of Texas at Arlington „Getting more with less: matrix and tensor algorithms from subsampling modes", NASK-PIB organizatorem
- 14-15 marca – Forum Gospodarcze TIME, NASK-PIB Partnerem, udział merytoryczny przedstawicieli NASK-PIB
- 15 marca – NCC Network Meeting, NASK-PIB gospodarzem
- 16-17 marca – 4th Governing Board Meeting ECCC (European Cybersecurity Competence Centre), NASK-PIB gospodarzem
- 29 marca – seminarium naukowe dr Justina Solomona z Massachusetts Institute of Technology „Machine Learning Using the Geometry of Datasets and Loss Functions", NASK-PIB organizatorem

Kwiecień

- 18–19 kwietnia – XXVI Konferencja SECURE 2023 pod hasłem „Bezpieczeństwo w dobie zmian", NASK-PIB organizatorem

Maj

- 8 maja – Seminarium eksperckie „co jest grane? Jak zadbać o bezpieczeństwo młodych graczy?" NASK-PIB współorganizatorem
- 10-11 maja – Kongres IMPACT 2023, NASK-PIB Partnerem, udział merytoryczny przedstawicieli NASK-PIB
- 18-19 maja – Konferencja CYBERGov, NASK-PIB Partnerem merytorycznym, udział merytoryczny przedstawicieli instytutu
- 29-31 maja – Globalne Forum Bezpieczeństwa Globsec Bratysława, udział merytoryczny przedstawicieli NASK-PIB
- 30 maja – Konferencje „Szanse, wyzwania, zagrożenia – wprowadzenie do problematyki bezpieczeństwa dzieci i młodzieży online", NASK-PIB organizatorem
- 31 maja – CENTR Jamboree 2023 udział merytoryczny przedstawicieli NASK-PIB

Czerwiec

- 6 czerwca – Konferencje „Szanse, wyzwania, zagrożenia – wprowadzenie do problematyki bezpieczeństwa dzieci i młodzieży online", NASK-PIB organizatorem
- 6 czerwca – Konferencja „Uwaga smartfon!" – NASK-PIB partnerem, udział merytoryczny przedstawicieli instytutu

- 13 czerwca – Konferencja z Partnerami Rejestru Domeny .pl, NASK-PIB organizatorem
- 19-21 – czerwca forum EURODIG Tampere, Finlandia. NASK-PIB Współorganizatorem panelu, udział merytoryczny przedstawicieli NASK-PIB
- 25-26 czerwca – Mistrzostwa Polski Szkół Średnich w Programowaniu Zespołowym, NASK-PIB Partnerem
- 28-29 listopada – Kongres CyberTrust, NASK-PIB partnerem merytorycznym, udział merytoryczny przedstawicieli instytutu
- 29-30 czerwca – Zlot OSEhero; NASK-PIB organizatorem

Lipiec

- 12 lipca – seminarium naukowe z prof. dr hab. Hanną Bogucką z Politechniki Poznańskiej „Bezpieczeństwo otwartych radiowych sieci dostępowych 5G i 6G", NASK-PIB organizatorem

Wrzesień

- 5-7 września - V Forum Cyberbezpieczeństwa w Karpaczu organizowane przez Ministerstwo Cyfryzacji oraz NASK-PIB w ramach XXXII Forum Ekonomicznym w Karpaczu
- 11 września - Gala z okazji 30-lecia Polskiej Izby Informatyki i Telekomunikacji (PIIT) i 20-lecia Sądu Polubownego ds. Domen Internetowych przy PIIT. NASK-PIB patronem
- 13 września – Konferencja Security Case Study, NASK-PIB partnerem merytorycznym, udział merytoryczny przedstawicieli instytutu.
- 13 września – Finał CyberTwierdzy, NASK-PIB partnerem merytorycznym
- 11-13 września – „Letnia Szkoła Cyberbezpieczeństwa" organizowane we współpracy MON z Morskim Centrum Cyberbezpieczeństwa AMW. NASK-PIB współorganizatorem warsztatów
- 13-15 września – Ogólnopolskie wydarzenie Krynica Forum 2023, udział merytoryczny przedstawicieli NASK-PIB
- 21-22 września – Forum Teleinformatyki, NASK-PIB partnerem, udział merytoryczny przedstawicieli instytutu.
- 24-25 września - Festiwal Nauki NASK-PIB Współorganizatorem
- 28 września – Walne Zgromadzenie CISO Poland, NASK-PIB gospodarzem

- 26-29 września – Międzynarodowa Konferencja Bezpieczeństwo dzieci i młodzieży online, NASK -PIB Współorganizatorem
- 25-26 września – 69TH CENTR LEGAL & REGULATORY WORKSHOP, NASK-PIB panelistą i uczestnikiem grupy roboczej przedstawicieli NASK-PIB
- 27 września – seminarium naukowe z dr Amirem Patelem z Oxford University "Studying Cheetahs Through the Lens of Robotics", NASK-PIB organizatorem
- 28 września – 57th CENTR Administrative workshop, NASK-PIB panelistą i uczestnikiem grup roboczych

Październik

- 4 października – Konferencja IGF Polska 2023, NASK-PIB współorganizatorem
- 4 października – seminarium naukowe z dr hab. Tomaszem Wolakiem z Naukowego Centrum Obrazowania Biomedycznego w Światowym Centrum Słuchu „Sztuczna inteligencja a inteligencja biologiczna: podobieństwa, różnice i wyzwania", NASK-PIB organizatorem
- 7 października – Wielkie Święto Programowania w Olsztynie, Augustowie i Wrocławiu, NASK-PIB Organizatorem
- 7 oraz 21 października – Szachowe Grand Prix OSE (dwa turnieje półfinałowe – we Wrocławiu i Bydgoszczy), NASK-PIB Organizatorem
- 8-12 października – 18th Internet Governance Forum pod hasłem „The Internet We Want – Empowering All People, Kioto, Japonia, NASK-PIB wystawcą, organizatorem warsztatów, udział merytoryczny przedstawicieli NASK-PIB
- 10 października – Noc Innowacji w NASK
- 11 października – seminarium naukowe z prof. dr hab. Przemysławem Bieckiem z Politechniki Warszawskiej „Red-Teaming modeli AI, czyli jak i po co wykorzystywać XAI do analizy modeli predykcyjnych", NASK-PIB organizatorem
- 21 października – 2023 ICANN 78 Annual General Meeting, NASK-PIB uczestnikiem grup roboczych
- 7 oraz 21 października – Szachowe Grand Prix OSE (dwa turnieje półfinałowe – we Wrocławiu i Bydgoszczy), NASK-PIB organizatorem
- 21 października – Wielkie Święto Programowania w Bydgoszczy, NASK-PIB organizatorem

Listopad

- 3-5 listopada – XXVII Akademickie Mistrzostwa Polski w Programowaniu Zespołowym, NASK-PIB Partnerem Strategicznym
- 4 listopada – Szachowe Grand Prix OSE, turniej finałowy w Warszawie, NASK-PIB organizatorem
- 8 listopada 2023 – 38TH CENTR MARKETING WORKSHOP NASK-PIB panelistą i uczestnikiem grupy roboczej
- 14 listopada – Konferencja CommonSign, NASK-PIB współorganizatorem
- 16 listopada – Konferencje „Szanse, wyzwania, zagrożenia – wprowadzenie do problematyki bezpieczeństwa dzieci i młodzieży online", NASK-PIB organizatorem
- 17 listopada – Konferencja „Pierwsza polska strategia walki z przemocą seksualną wobec dzieci – geneza i wdrażanie", NASK-PIB współorganizatorem
- 20 listopada – Warsztaty regulacyjne Rejestru domeny .pl, dla Partnerów, NASK-PIB organizatorem
- 29 listopada – Konferencja „Państwo Blockchain", NASK-PIB organizatorem

Grudzień

- 5 grudnia – Kongres OSE, NASK-PIB Organizatorem
- 5 grudnia – Konferencja Oh My Hack 2023, udział merytoryczny przedstawicieli NASK-PIB
- 4-8 grudnia Child Sexual Abuse Reduction Research Network/2023 ANZSOC National Conference, udział merytoryczny przedstawicieli NASK-PIB

6.5. Wydawnictwa

Książki, poradniki

- Anna Borkowska „*Uczeń w cyfrowym świecie, Jak projektować działania profilaktyczne w szkole i przedszkolu*", Warszawa: NASK Państwowy Instytut Badawczy, 2023, ISBN: 978-83-65448-54-5
- Anna Kwaśnik, Magdalena Melka-Roszczyk, *Internetowe love Poradnik – jak zadbać o swoje cyberbezpieczeństwo w relacjach online*. ", Warszawa: NASK Państwowy Instytut Badawczy, 2023,
- Anna Kwaśnik, Zuzanna Polak, Katarzyna Koletyńska *Cyber bezpieczne wakacje"* Warszawa: NASK Państwowy Instytut Badawczy, 2023,
- *#Antysmogowi* – interaktywna e-lekcja dla szkół ponadpodstawowych opublikowana na platformie eduESA

- *Cyberbezpieczny Samorząd. Poradnik*, Warszawa: NASK Państwowy Instytut Badawczy, 2023,
- Cykl 5 kursów nt. zmiany klimatu powstałych we współpracy z CNK: „*Prawda o klimacie", „Migracje klimatyczne", „Co dwa kółka, to nie cztery", „Czy planeta nas wyżywi?" oraz „Bioróżnorodność: po co nam komary?";*
- Cykl „Mistrzowie Energii": „*Skąd się bierze prąd w gniazdku elektrycznym?" (kl. 1-3); „Jak wyglądałby Twój dzień, gdyby nie było prądu?"* (kl. 4-6); „O co tyle hałasu z tym prądem?" (kl. 7-8)
- „Metawersum. Zagrożenia, szanse, wyzwania", Dyżurnet.pl, NASK-PIB, 2023 https://dyzurnet.pl/uploads/2023/09/Metawersum-zagrozenia-szanse-wyzwania.pdf
- „*Miasteczko Ekomoko"* – karty pracy dla uczniów kl. 1-3 - scenariusze lekcji wraz z kartami pracy i prezentacjami na temat oszczędzania energii w ramach kampanii
- „(Nie)widzialne ślady online. Poradnik Polskiego Centrum Programu Safer Internet" , NASK-PIB, (2023) https://www.saferinternet.pl/pliki/publikacje/cyfrowy-slad-PUBLIKACJA_03_281123.pdf
- OUCH! – tłumaczenie i edycja 12 numerów biuletynu bezpieczeństwa OUCH! https://www.cert.pl/ouch/
- Pakiet scenariuszy stworzony na potrzeby akcji edukacyjnej #stopfpmo, prowadzonej w ramach promocji projektu „FOMO 2022. Polacy a lęk przed odłączeniem":
    - Anna Borkowska „FOMO a relacje w mediach społecznościowych", Warszawa: NASK Państwowy Instytut Badawczy, 2023 [online: https://it-szkola.edu.pl/publikacje,plik,92]
    - Anna Borkowska „FOMO i nadużywanie smartfona", Warszawa: NASK Państwowy Instytut Badawczy, 2023 [online: https://it-szkola.edu.pl/publikacje,plik,93]
    - Anna Borkowska „FOMO i przymus bycia na bieżąco", Warszawa: NASK Państwowy Instytut Badawczy, 2023 [online: https://it-szkola.edu.pl/publikacje,plik,94]
    - Marta Witkowska „FOMO a wielozadaniowość", Warszawa: NASK Państwowy Instytut Badawczy, 2023 [online: https://it-szkola.edu.pl/publikacje,plik,95]
    - Marta Witkowska „FOMO, smartfony i ryzykowne zachowania… w realu", Warszawa: NASK Państwowy Instytut Badawczy, 2023 [online: https://it-szkola.edu.pl/publikacje,plik,96]

- „Patrol Smogowy wkracza do akcji!" – zadania dla przedszkoli z naklejkami
- Seria edukacyjna „*Mierzymy się ze smogiem*" – cykl 5 plakatów i ulotek

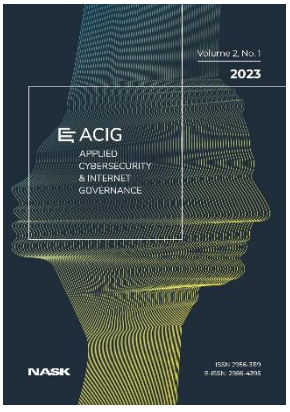
Raporty

- Rafał Lange, Agnieszka Wrońska, Agnieszka Ładna, Karol Kamiński, Mariola Błażej, Anna Jankiewicz, Katarzyna, *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców,* NASK Państwowy Instytut Badawczy, Warszawa 2023

ISBN 978-83-65448-56-9 (wersja elektroniczna), ISBN 978-83-65448-57-6 (wersja drukowana)

- Zuzanna Polak (red.), *Kompetencje Cyfrowe Pracowników JST Szczebla Powiatowego. Raport z badań.* Warszawa: NASK Państwowy Instytut Badawczy, 2023,. ISBN: 978-83-65448-70-5
- *Raport roczny z działalności CERT Polska 2023,* Warszawa: NASK Państwowy Instytut Badawczy, 2023 https://cert.pl/uploads/docs/Raport_CP_2023.pdf
- Raport opracowany przez CSIRT NASK, Służbę Kontrwywiadu Wojskowego (SKW) oraz partnerów zagranicznych o wykrytych szkodliwych działaniach grupy APT29 powiązanej z Rosyjską Służbą Wywiadu Zagranicznego (SVR) https://cert.pl/posts/2023/12/apt29-teamcity
- Raporty kwartalne dot. rynku domeny .pl, Warszawa: NASK Państwowy Instytut Badawczy, 2023 https://www.dns.pl/raporty
- Raport na temat domen internetowych – publikacja specjalna NASK-PIB i PIIT https://www.dns.pl/sites/default/files/2023-09/Raport-30-lecie-PIIT-20-lecie-Sadu.pdf
- Dyżurnet.pl, *Raport 2022,* Warszawa: NASK Państwowy Instytut Badawczy, 2023 https://dyzurnet.pl/publikacje
- Dyżurnet.pl, *Od zgłoszenia do reakcji. Raport z badania szkodliwych treści w serwisach internetowych,* Warszawa: NASK Państwowy Instytut Badawczy, 2023 https://dyzurnet.pl/uploads/2023/12/Od_zgloszenia_do_reakcji.pdf

Czasopisma



Applied Cybersecurity & Internet Governance (ACIG)

W 2023 roku opublikowano drugi numeru anglojęzycznego, międzynarodowego czasopisma naukowego „Applied Cybersecurity & Internet Governance" wydawanego przez NASK-PIB. Funkcję redaktorki naczelnej pełni dr hab. Aleksandra Gasztold, prof. UW. ACIG 2023 vol 1, zawiera 14 artykułów naukowych, związanych z tematyką cyberbezpieczeństwa, nowych technologii i sztucznej inteligencji. Przedstawiciele zagranicznych ośrodków naukowych i instytucji stanowią przeważającą liczbę twórców i recenzentów: 80% autorów reprezentuje zagraniczne ośrodki naukowe, 50%

recenzentów to eksperci zagraniczni. Ogółem artykuły napisało 24 autorów, w tym 20 autorów z zagranicy i 4 z Polski. Ich prace były recenzowane przez 27 recenzentów w procesie recenzyjnym double blind peer review. Wszystkie artykuły opublikowane zostały na podstawie zasady online-first w otwartym dostępie (open access) na stronie www.acigjournal.com. Łączna liczba wyświetleń artykułów z dwóch numerów czasopisma ACIG, w okresie sprawozdawczym, to ponad 17 500. Czasopismo jest obecne w następujących bazach: Directory of Open Access Journals /DOAJ/, Central and Eastern European Online Library /CEEOL/, Crossref, EBSCO Information Services, ERIH Plus; Semantic Scholar.Sherpa Services, International Standard Serial Number /The ISSN Portal/, BazTech Arianta, Academic Journals – Czasopisma naukowe (academic-journals.eu, Polska Bibliografia Naukowa/ PBN/POL-Index/; ICI Journals Master List / ICI World of Journals. Ponadto w 2023r. ogłoszono nabory do kolejnego numeru czasopisma oraz do numeru specjalnego poświęconego konfliktowi w Ukrainie –ACIG 2024, Volume 3, No.1 – numer specjalny „The Russian-Ukrainian War: Effects on Global Cybersecurity and Digital Infrastructure". Do końca 2023r. zostało pozytywnie zrecenzowanych i przyjętych 6 artykułów. Zamknięcie numeru specjalnego planowane jest w 2Q 2024roku.

7. NASK-PIB w mediach

Najważniejsze wydarzenia medialne 2023 roku

- **Kampania edukacyjno-informacyjna CYBER w ramach KEI** – „Pan Krzyś" prowadzona z Ministerstwem Cyfryzacji od czerwca do grudnia 2023 r. Seria 5 spotów edukowała na temat cyberzagrożeń i przekazywała porady, jak być bezpiecznym w sieci. Tematy podjęte w kampanii obejmowały: bezpieczne hasła i logowanie, fałszywe sklepy online, fałszywe prośby o szybki przelew, niebezpieczne załączniki w mailach i fałszywe inwestycje w sieci. Kampania zachęcała do odwiedzenia strony cert.pl. Kampania pojawiła się w telewizji, radiu, internecie, prasie oraz w kinach, na dworcach, peronach. Kampania telewizyjna dotarła do 76% grupy docelowej, a reklama internetowa wygenerowała ponad 1,8mln kliknięć.

- **Kampania informacyjna platformy pomocowej 116sos.pl**, która oferuje bezpłatne wsparcie dla osób dorosłych w trudnej sytuacji życiowej, realizowana była w listopadzie i grudniu 2023 roku. Obejmowała podcasty w serwisie radiowym, reklamę w komunikacji miejskiej w całej Polsce z liczbą wyświetleń na poziomie 5,5 mln, a także w prasie.

- **Kampania informacyjna „Bezpieczne wybory**", prowadzona od września do listopada 2023 roku. Projekt „Bezpieczne Wybory" miał na celu krótko i długoterminowe działania osłonowe, informacyjne i edukacyjne w kontekście wyborów parlamentarnych. Główną platformą działań wokół projektu jest strona bezpiecznewybory.pl. Kampania obejmowała działania głównie online o zasięgu ponad 15 mln oraz OOH, takie jak paczkomaty czy ekrany LCD w pociągach i komunikacji miejskiej.

- **Kampania Edukacyjnej Sieci Antysmogowej – „Mierzymy się ze smogiem**" trwała od października do grudnia 2023 roku. Nadrzędnym celem promowanego projektu był wzrost świadomości społecznej dotyczącej problemu smogu i zbudowanie zdrowych

nawyków związanych z ochroną powietrza przy wykorzystaniu technologii cyfrowych. Treści edukacyjne promowane były w social mediach, w serwisach informacyjnych, a także w telewizji śniadaniowej. Kampania w telewizji obejmowała dwukrotny felieton oraz wejścia pogodowe, a także działania dodatkowe online.

- **Kampania informacyjna dotycząca nowego numeru zgłaszania fałszywych SMSów** do CERT Polska – 8080. Realizowana była w okresie wzmożonej aktywności cyberprzestępców – przed świętami Bożego Narodzenia, informowała użytkowników internetu o zagrożeniu w postaci fałszywych SMSów. Wszystkie działania skupione były w internecie, obejmowały emisję spotu w social mediach oraz serwisach informacyjnych i telewizyjnych, wygenerowały prawie 6 mln odsłon.

- **Premiera najnowszego raportu Ogólnopolskiej Sieci Edukacyjnej „Aspiracje edukacyjne i zawodowe uczniów szkół średnich".**

- **Kampania informacyjno-edukacyjna Rejestru Domeny .pl.** Kampania emisję miała w grudniu 2023 roku. Miała na celu poinformowanie odbiorców i zbudowanie świadomości, że domena .pl jest gwarancją bezpieczeństwa i stabilności. Spot popularyzował ideę, że własna strona internetowa jest wirtualną przestrzenią do rozwoju, wzrostu i samorealizacji, która chroni i zabezpiecza najważniejsze sprawy w cyfrowym świecie, a własna domena „.pl" to gwarancja bezpieczeństwa i niezależności od zewnętrznych nagłych zmian, regulacji, regulaminów. Działania kampanijne obejmowały emisję w internecie zapewniając ponad 2,7 mln odsłon, w kinach niezależnych z widownią sięgającą prawie 480 tys., w radiu z zasięgiem ponad 1,7 mln, a także w telewizji ogólnopolskiej.

- **Premiera raportu z ogólnopolskiego badania uczniów i rodziców Nastolatki 3.0**. o tym co robią nasze dzieci w sieci.

- Pracownia Kompetencji Cyfrowych – **konkurs dla wszystkich szkół w Polsce** (podłączonych do OSE i nie tylko) – pozwalający poszerzyć wiedzę z zakresu bezpieczeństwa w sieci i wykorzystać ją w kreatywny sposób.

- **Projekt OSEhero** skierowany jest do wszystkich nauczycieli, a także dyrektorów, pedagogów, psychologów i bibliotekarzy ze szkół OSE, którzy chcą aktywnie działać w zakresie upowszechniania wiedzy na temat bezpieczeństwa w internecie.

- **Szachowe Grand Prix OSE** - pierwsza edycja ogólnopolskich, bezpłatnych rozgrywek dla uczniów ze szkół podstawowych popularyzująca gry w szachy wśród dzieci i młodzieży szkolnej – jako aktywności, która jest wsparciem wszechstronnego rozwoju.

W 2023 r. polityka informacyjna NASK-PIB realizowana była poprzez bieżące treści zamieszczane na stronie internetowej NASK-PIB oraz w mediach społecznościowych (Facebook, Twitter i LinkedIn, Instagram, YouTube) oraz kontakty z dziennikarzami.

Instytut realizował stałą współpracę z mediami, podejmował działania na rzecz promocji NASK-PIB i udzielał odpowiedzi na zapytania prasowe.

Na podstawie danych z monitoringu mediów IMM odnotowano w 2023 roku **199 676 przekazów.**

Podsumowanie

NASK-PIB odgrywa kluczową rolę w cyfryzacji kraju i cyberbezpieczeństwie, realizując zadania wynikające z Ustawy o Krajowym Systemie Cyberbezpieczeństwa, zapewniając infrastrukturę Ogólnopolskiej Sieci Edukacyjnej i rozwijając system elektronicznego zarządzania dokumentami oraz rejestr domen internetowych.

Rok 2023 był dla NASK-PIB okresem wyzwań i transformacji organizacyjnych oraz dynamicznego rozwoju. Finansowanie ze źródeł publicznych, w tym realizacja zadań publicznych, projektów inwestycyjnych i grantów B+R było w 2023 roku głównym źródłem przychodów Instytutu i stanowiło ponad 75%. Instytut realizował 58 projektów finansowanych z środków publicznych (krajowych i europejskich) na łączną kwotę 550 mln PLN. Zatrudnienie wzrosło o 25% w porównaniu do roku poprzedniego.

Naukowo-badawcza działalność NASK-PIB była zgodna ze strategią rozwoju nauki, i opierała się o współpracę z czołowymi ośrodkami na świecie oraz rozwój kadry naukowej. Badania obejmowały kryptografię, obliczenia kwantowe, algorytmy uczenia głębokiego, przetwarzanie języka naturalnego, obrazu i dźwięku oraz matematyczne podstawy uczenia maszynowego.

W 2023 roku Instytut odniósł znaczące sukcesy. System Botsense zdobył nagrodę - Lider Bezpieczeństwa Państwa, a CERT Polska uzyskał status uzyskał status CNA (CVE Numbering Authority), jako jedyna instytucja w kraju i jedna z siedmiu w Europie. Dyżurnet.pl został „buddy hotline": w stowarzyszeniu INHOPE. Polskie drużyny zajęły czołowe miejsca w międzynarodowych ćwiczeniach i konkursach, takich jak Locked Shields, Hack-A-Sat i European Cyber Security Challenge.

NASK-PIB prowadził również działalność komercyjną, oferując cenione na rynku produkty i usługi, w tym system BotSense, CTI i audyty bezpieczeństwa teleinformatycznego. Instytut przeprowadził blisko 3300 szkoleń, seminariów, warsztatów i konferencji dla ponad 450 000 uczestników, prowadził kampanie społeczne, a także wspierał szkolnictwo wyższe poprzez współpracę z uczelniami i współorganizację studiów podyplomowych i Szkoły Doktorskiej.

Zapewniono istotną dla dalszego rozwoju rozpoznawalność medialną i dbano o, wizerunek budując silną markę i prowadząc spójną komunikację w mediach społecznościowych.