CyberSecIdent „Cyberbezpieczeństwo i eTożsamość” – założenia Programu B+R [aktualizacja nr 4[1]

czerwiec 2024 r.

[1] Dokument jest zaktualizowaną wersją Założeń Programu CSI z 2016 r. Aktualizacja założeń dotyczy w szczególności: perspektywy czasowej określonej w celu głównym Programu (z roku 2023 na 2028 rok), harmonogramu Programu (dostosowanie zapisów do stanu faktycznego), uzupełnienie informacji o wartości docelowej we wskaźnikach rezultatu bezpośredniego, aktualizacja w zakresie dokumentów/strategii wskazanych w opisie otoczenia polityczno-prawnego, usunięcie odwołań do nieaktualnych procedur obowiązujących w NCBR zmiany redakcyjne pod względem poprawienia i doskonalenia tekstu, stylistyki i ogólnej spójności. „Streszczenie menadżerskie” i „Diagnoza stanu – Analiza PEST” – pozostają w brzmieniu z 2016 r. z korektami zaznaczonymi w tekście.

Streszczenie menadżerskie

CyberSecIdent jest programem badawczo – rozwojowym nakierowanym na podniesienie bezpieczeństwa cyberprzestrzeni RP poprzez zwiększenie dostępności rozwiązań sprzętowych i programistycznych.

Podstawą do przygotowania agendy badawczej, celów, wskaźników realizacji celów, sposobów interwencji oraz budżetu Programu była diagnoza stanu cyberbezpieczeństwa oraz cyfrowej tożsamości.

Na diagnozę stanu składają się wyniki analizy otoczenia polityczno-prawnego, ekonomicznego, społeczno–kulturalnego oraz technologicznego, wykonane zgodnie z metodyką PEST. W każdej z powyższych kategorii zidentyfikowano kluczowe czynniki, szanse jakie może stworzyć Program z punktu widzenia ustaleń w danym otoczeniu oraz ryzyka, jakie pozostaną w wypadku niepodjęcia działań.

W wyniku przeprowadzonej analizy określono cztery kluczowe zagadnienia oraz wynikające z nich potrzeby, które wskazano jako konieczne do uwzględnienia w celach Programu CyberSecIdent.

W otoczeniu polityczno – prawnym:

1. Zapewnienie adekwatnego do potrzeb i możliwości udziału Polski w działaniach Unii Europejskiej na rzecz wspólnych rozwiązań w zakresie cyberbezpieczeństwa oraz opracowywania i wdrażania bezpiecznych produktów lub usług teleinformatycznych w cyberprzestrzeni.

W otoczeniu ekonomicznym oraz otoczeniu społeczno-kulturalnym:

2. Zapewnienie skutecznego oddziaływania na poziom bezpieczeństwa cyberprzestrzeni jako środowiska działalności gospodarczej i społecznej.
3. Zapewnienie rozwiązań odpowiadających na obawy użytkowników w zakresie cyberbezpieczeństwa.

W otoczeniu technologicznym:

4. Konieczność zwiększenia nakładów i w konsekwencji zwiększenia liczby projektów B+R wspierających innowacyjność polskich produktów i usług teleinformatycznych w aspekcie bezpieczeństwa teleinformatycznego.

Na tej podstawie sformułowano następujące cele Programu:

Cel główny

Podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP przez zwiększenie dostępności narzędzi sprzętowo–programistycznych, do roku 2028.

Cele szczegółowe

1. Wdrożenie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości
2. Wdrożenie metod i technik identyfikacji i uwierzytelniania.

Program CyberSecIdent koncentruje się na rozwiązaniach technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości. Z Programu wyłączone są aspekty prawne i regulacyjne cyberbezpieczeństwa lub cyfrowej tożsamości oraz inne pośrednie działania wpływające na bezpieczeństwo, zwłaszcza w postaci podnoszenia świadomości oraz edukacji.

W zakresie cyfrowej tożsamości, w Programie zakłada się odniesienie jedynie do niektórych metod i technik identyfikacji i uwierzytelniania, nie obejmując rozwiązań o większym rozmiarze, takich jak platformy zarządzania cyfrową tożsamością.

Dla Agendy badawczej przyjęto następujące kryteria:

- Tematy, dla których istotność dla cyberbezpieczeństwa jest wysoka, a planowane nakłady pozwalają na osiągnięcie celów,
- Przedmiot badań, których efekty w jak najszerszym zakresie będą umożliwiać wiarygodną weryfikację bezpieczeństwa rozwiązań sprzętowo–programistycznych, mających zastosowanie w różnych sektorach gospodarki, ze szczególnym uwzględnieniem infrastruktury krytycznej.
- Innowacyjne komponenty, których opracowanie będzie w istocie decydować o bezpieczeństwie większych systemów.

W efekcie określono następujące tematy badawcze:

(i) Nowoczesne technologie i innowacyjne rozwiązania w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia,

(ii) Nowoczesne technologie i innowacyjne rozwiązania w zakresie tożsamości cyfrowej, z uwzględnieniem aspektów prywatności,

(iii) Metodyki, techniki i procesy w obszarze analizy cyberbezpieczeństwa i cyfrowej tożsamości oraz ich wdrożenia, w tym także analizy dostępnych rynkowo rozwiązań, mające na celu wybór optymalnych rozwiązań.

w których opisano także podtematy, precyzujące zakres i ograniczenia danego tematu.

Program jest adresowany do konsorcjów naukowych, składających się z jednostek naukowo – badawczych oraz przedsiębiorstw.

Zakłada się, że zadania będą realizowane w formie badań przemysłowych, prac rozwojowych oraz przygotowania wyników badań i prac rozwojowych do zastosowania w praktyce.

Zakładany budżet NCBR na realizację Programu wynosi 234 027 000 PLN.[2]

Struktury, których zadaniem będzie monitorowanie realizacji oraz nadzór nad Programem, będą obejmować Koordynatora Programu oraz Komitet Sterujący Programu. Tryb i proces wyłonienia Wykonawców określi Regulamin Programu.

Zakłada się, że monitorowanie realizacji Programu będzie wykonywane za pomocą zdefiniowanych wskaźników odpowiednio, produktu, rezultatu bezpośredniego (w odniesieniu do celów szczegółowych) oraz rezultatów długoterminowych (w odniesieniu do celu głównego).

[2] Na wniosek KS CyberSecIdent, Dyrektor Centrum wyraził zgodę na zwiększenie alokacji budżetu Programu z 212 000 000 PLN do 234 027 000 PLN.

Spis treści

Diagnoza sytuacji w obszarach nauki i gospodarki, które mają być objęte Programem

Wstęp

Pojęcia cyberbezpieczeństwa i cyfrowej tożsamości

Cyberprzestrzeń jest złożonym środowiskiem wynikającym z interakcji ludzi, oprogramowania i usług w Internecie za pośrednictwem urządzeń technicznych i dołączonych do nich sieci, które nie istnieje w fizycznej formie[3].

Przyjęta definicja cyberbezpieczeństwa to przeniesienie klasycznej definicji bezpieczeństwa rozumianego jako zachowanie poufności, integralności i dostępności informacji w cyberprzestrzeni[4]. Jednakże, w cyberprzestrzeni pojawiają się problemy bezpieczeństwa, dla których dotychczasowe rozwiązania bezpieczeństwa informacji, bezpieczeństwa sieciowego, bezpieczeństwa teleinformatycznego są niewystarczające. Wynika to z wielości separowanych – nie tylko logicznie, ale też geograficznie - domen bezpieczeństwa zarządzanych przez różne organizacje i dostawców usług, będących właścicielami urządzeń i dołączonych sieci, z których każdy kieruje się własnymi zasadami, ma swoje praktyki operacyjne oraz własne regulacje. Fragmentacja stanu bezpieczeństwa, innego dla każdej domeny, określa potrzeby wdrażania mechanizmów skutecznej współpracy między różnymi organizacjami i dostawcami usług, zwłaszcza w obszarze przeciwdziałania, identyfikowania i reagowania na incydenty naruszenia bezpieczeństwa.

Tożsamość jest definiowana ogólnie jako zbiór atrybutów związanych z jednostką[5]. Cyfrową tożsamością jest zatem informacja wykorzystana do określenia reprezentacji tej jednostki w systemie teleinformatycznym. Celem określenia cyfrowej tożsamości jest zdolność systemu do jednoznacznego odróżnienia każdej jednostki funkcjonującej w systemie. W zależności od zastosowania danego systemu, cyfrowa tożsamość może być budowana na podstawie różnych atrybutów: od danych opisujących fizyczne istnienie jednostki (np. data urodzenia, adres zamieszkania, lokalizacja geograficzna używanego urządzenia), przez dane opisujące historię jednostki (wykształcenie, kwalifikacje, zainstalowane aplikacje, konfiguracja urządzenia), dane określające, czym jednostka jest (np. dane biometryczne lub genetyczne), dane przypisane do jednostki (np. rola, podpis elektroniczny, numer ewidencyjny w systemie), do danych referencyjnych (np. numer paszportu, prawa jazdy, karty kredytowej).

Jak wskazano wcześniej, cechą charakterystyczną cyberprzestrzeni są rozdzielne domeny bezpieczeństwa. Z tego wynika, że w różnych domenach bezpieczeństwa wymagania na

[3] ITU-T X.1200 – X.1299, Series X: Data Networks, Open System Communications and Security, Telecommunication Security – Cyberspace security

[4] ISO/IEC 27032:2012: Information technology — Security techniques — Guidelines for cybersecurity

[5] ISO/IEC 24760-1:2011 Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts

cyfrową tożsamość oraz poziom wiarygodności prezentowanego zbioru atrybutów określającego tożsamość mogą być różne, w zależności od potrzeb danej domeny bezpieczeństwa.

Zdefiniowanie metod i technik przenoszenia cyfrowej tożsamości w cyberprzestrzeni, które zapewnią nie tylko odpowiedni poziom wiarygodności cyfrowej tożsamości, ale także odpowiedni poziom ochrony prywatności jednostki jest jednym z największych wyzwań dla cyberbezpieczeństwa.

Zakres przedmiotowy Programu CyberSecIdent

Program CyberSecIdent koncentruje się na rozwiązaniach technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości. Z Programu wyłączono aspekty prawne i regulacyjne cyberbezpieczeństwa oraz inne pośrednie działania wpływające na bezpieczeństwo, zwłaszcza w postaci podnoszenia świadomości oraz edukacji.

W zakresie cyfrowej tożsamości, w Programie założono odniesienie jedynie do niektórych metod i technik identyfikacji i uwierzytelniania nie obejmując rozwiązań o większym zakresie, takich jak platformy zarządzania cyfrową tożsamością.

Dla Agendy badawczej przyjęto następujące kryteria:

- Tematy, dla których istotność dla cyberbezpieczeństwa jest wysoka, a planowane nakłady pozwalają na osiągnięcie celów,
- Przedmiot badań, których efekty w jak najszerszym zakresie będą umożliwiać wiarygodną weryfikację bezpieczeństwa rozwiązań sprzętowo–programistycznych, mających zastosowanie w różnych sektorach gospodarki, ze szczególnym uwzględnieniem infrastruktury krytycznej,
- Innowacyjne komponenty, których opracowanie będzie w istocie decydować o bezpieczeństwie większych systemów.

Zakłada się, że program CyberSecIdent będzie uzupełnieniem dla programu strategicznego, wynikającego z potrzeb określonych w Krajowym Programie Badań [6] oraz Strategii Cyberbezpieczeństwa RP na lata 2019-2024, którego przygotowanie i uruchomienie jest przewidywane w 2019 roku. [7]

[6] Od 2022 roku KPB zostało zastąpione Polityką Naukową Państwa.

[7] W 2019 roku przyjęto Uchwałę nr 152 Rady Ministrów z dnia 22.10.2019 r. w sprawie Strategii Cyberbezpieczeństwa RP na lata 2019-2024. Uchwała jest dokumentem, który prezentuje strategiczne podejście administracji rządowej do kwestii szeroko rozumianego cyberbezpieczeństwa.

Diagnoza stanu - Analiza PEST

Wprowadzenie

W celu określenia problemów i wyzwań, na które będzie odpowiadać program CyberSecIdent, zastosowano makroekonomiczną metodę segmentacji otoczenia przez analizę zagadnień: polityczno-prawnych, ekonomicznych, społeczno–kulturalnych oraz technologicznych, znaną jako metodyka PEST[8].

Celem analizy jest zidentyfikowane kluczowych czynników Programu definiujących aktualne wyzwania. Zdefiniowanie kluczowych czynników pozwoli na sformułowanie podstaw dla celów Programu.

Otoczenie polityczno–prawne

Opis stanu

Kilkunastoletnie prace nad zintegrowanym systemem ochrony cyberprzestrzeni państw Unii Europejskiej zostały zwieńczone przyjęciem Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywa NIS).

Do najważniejszych kierunków działań Unii Europejskiej oraz Państw Członkowskich, wynikających z potrzeby wdrożenia Dyrektywy NIS do prawa krajowego[9] oraz dołączenia do ogólnoeuropejskiego systemu obrony cyberprzestrzeni, a jednocześnie zapewnienia skutecznego i bezpiecznego działania cyberprzestrzeni RP, należą:

- Wytworzenie mechanizmu współpracy między państwami członkowskimi i Komisją w celu przekazywania wczesnych ostrzeżeń w sprawie zagrożeń i incydentów, a także prowadzenia współpracy i organizowania regularnych ocen wzajemnych. Mechanizm jest, realizowany za pomocą sieci krajowych CSIRT-ów (*Computer Security Incident Response Team*),
- Zapewnienie rozwiązań uwzględniających zależności międzysektorowe oraz odporność infrastruktury teleinformatycznej operatorów świadczących tzw. usługi kluczowe[10] na ataki z cyberprzestrzeni, w tym zagwarantowanie skutecznej struktury raportowania poważnych incydentów bezpieczeństwa w takich środowiskach,
- Wspieranie standaryzacji i interoperacyjności umożliwiającej transfer danych oraz korzystanie z usług niezależnie od miejsca pobytu, nie tylko na terenie Unii Europejskiej, ale też w dowolnym miejscu świata,

[8] P (Political), E (Economical), S (Socio - cultural), T (Technological)

[9] W 2018 roku zakończył się w Polsce proces implementacji Dyrektywy NIS.W 2019 roku przyjęto Cybersecurity Act (2017/0225) - „Prawo o cyberbezpieczeństwie", opublikowany 28 czerwca 2018 r.

[10] Do podmiotów świadczących usługi kluczowe (*essential services*) należą operatorzy krytycznej infrastruktury teleinformatycznej w następujących sektorach: paliwowo-energetyczny, transportowy, bankowość, giełdy towarowe i platformy rozliczeniowe, opieka zdrowotna, zaopatrzenie w wodę, cyfrowa infrastruktura (węzły internetowe, usługi DNS, rejestry domen krajowych).

- Zwiększenie zaufania do bezpieczeństwa produktów i usług informatycznych, w tym w szczególności w wypadku stosowania technologii informatycznych w systemach związanych z zapewnieniem ochrony życia lub zdrowia ludzi lub infrastruktury krytycznej, takich jak automatycznie sterowany transport, systemy sterowania i automatyka przemysłowa czy inteligentne sieci elektroenergetyczne,
- Eliminowanie wykluczenia cyfrowego obywateli oraz mikro, małych i średnich przedsiębiorstw z powodu bariery cenowej dla bezpiecznych produktów i usług.

Szereg inicjatyw[11] wynikających z Dyrektywy NIS, jak też z innych regulacji przyjętych w Unii w 2016 r., takich jak Ogólne Rozporządzenie o Ochronie Danych, inaczej rozporządzenie o ochronie danych osobowych (*RODO)* [12],odnosi się do wskazanych wyżej kierunków (zob. część **Otoczenie technologiczne** poniżej). Wspomniane inicjatywy są podejmowane na poziomie europejskim, przez Komisję Europejską we współpracy z krajami członkowskimi oraz na poziomie krajowym, przez administrację państwową, w zakresie odpowiedzialności za bezpieczeństwo cyberprzestrzeni kraju w perspektywie krótkookresowej (do 2020 roku).

16 stycznia 2023 r. weszła w życie Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie UE nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (Dyrektywa NIS 2). Państwa członkowskie UE mają czas do 17 października 2024 r., aby zaimplementować przepisy Dyrektywy NIS 2 do porządku prawnego.

Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020[13] w dużej mierze odpowiada na wyzwania zidentyfikowane w dokumentach strategicznych Unii Europejskiej, a w szczególności Dyrektywie NIS. Jednym z trzech filarów elementów tej strategii, niezbędnych do realizacji celów, jest: *„współpraca z ośrodkami akademickimi, sektorem prywatnym oraz organizacjami pozarządowymi w celu zarządzania wiedzą i stymulowania innowacji w dziedzinie cyberbezpieczeństwa w Polsce”*.

5 lipca 2018 r. weszła w życie ustawa o krajowym systemie cyberbezpieczeństwa (tj. Dz. U. z 2023 r., poz. 913 ze zm.), która implementuje przepisy Dyrektywy NIS.

Jednym z fundamentów bezpieczeństwa świadczenia usług w cyberprzestrzeni – finansowych, publicznych oraz społecznych - jest cyfrowa tożsamość (e-Tożsamość).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji

[11] Com (2016) 410 final, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, Comhttps://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

[12] RODO zaczęło obowiązywać od 25 maja 2018 r.

[13] http://archiwum.mc.gov.pl/files/strategia_v_29_09_2016.pdf

elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE[14] (zwane też Rozporządzeniem eIDAS). Rozporządzenie eIDAS określa cyberprzestrzeń jako zbiór krajowych domen bezpieczeństwa, w którym zadaniem Krajów Członkowskich jest zbudowanie zaufania między tymi domenami w taki sposób, aby można realizować transgraniczne usługi on-line.

Rozporządzenie eIDAS w części odnosi do „środków identyfikacji elektronicznej"[15], stwarzając ramy do:

- znoszenia istniejących barier w transgranicznym stosowaniu środków identyfikacji elektronicznej stosowanych w państwach w celu uwierzytelniania w usługach dostarczanych on-line,
- notyfikowania krajowych środków identyfikacji elektronicznej,
- określenia minimalnych wymagań bezpieczeństwa (poziomów), niezbędnych dla wzajemnego uznawania środków identyfikacji elektronicznej, wskazując jednocześnie, że „*bezpieczeństwo systemów identyfikacji elektronicznej ma kluczowe znaczenie dla wiarygodnego transgranicznego wzajemnego uznawania środków identyfikacji elektronicznej*",
- dobrowolnego stosowania środków identyfikacji elektronicznej przez sektor prywatny, w wypadku usług on-line lub transakcji elektronicznych

Oczywiste potrzeby obywateli i przedsiębiorców przeniesienia znacznej części swojej działalności do wirtualnej rzeczywistości, rodzi jednak nowe ryzyka dla stabilności takiego ekosystemu, z uwagi na zupełnie inne modele zagrożeń dla bezpieczeństwa cyberprzestrzeni niż te, które istnieją w tradycyjnej terytorialnej organizacji państwa (przykład skoordynowanego ataku na cyberprzestrzeń kraju to zdarzenia z 2007 roku w Estonii), tradycyjnych sposobach świadczenia usług (np. rewolucja w usługach finansowych) oraz w tradycyjnych kontaktach społecznych (fenomen mediów społecznościowych)

Mechanizmy ochrony tożsamości w cyberprzestrzeni odnoszą się zatem do podstawowych potrzeb obywateli w zakresie ochrony prywatności i bezpieczeństwa oraz przedsiębiorców w zakresie bezpieczeństwa obrotu gospodarczego. Zapewnienie takich mechanizmów jest obowiązkiem Państwa.

20 maja 2024 r. zaczęło obowiązywać opublikowane 30 kwietnia 2024 r. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (eIDAS 2). Rozporządzenie to wprowadza Europejskie Portfele Tożsamości Cyfrowej, tj. osobiste portfele, które uznaje się powszechnie w całej Unii Europejskiej. Rozporządzenie eIDAS 2 kładzie również duży nacisk na ochronę danych osobowych i prywatności użytkowników portfeli. Kwalifikowane podpisy elektroniczne mają być dostępne w portfelach

[14] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0910

[15] "zgodnie z definicją z Rozporządzenia eIDAS, "środek identyfikacji elektronicznej" oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online, czyli odnosi się wprost do pojęcia instancji „cyfrowej tożsamości"

za darmo dla wszystkich, którzy będą ich używać do celów innych niż zawodowe. **Kluczowe czynniki**

A. Znaczne zintensyfikowanie działań w Unii Europejskiej na rzecz rozwiązań prawnych, organizacyjnych i technicznych, w tym opracowywania i wdrażania bezpiecznych produktów i usług informatycznych dostępnych w Internecie, spełniających potrzeby Europy w zakresie zidentyfikowanych wyzwań (zob. powyżej).
B. Weryfikacja bezpieczeństwa na podstawie jednolitych, obowiązujących w UE wymagań bezpieczeństwa dla produktów i usług z sektora ICT (certyfikacja, stosowanie i wymaganie odpowiednich norm bezpieczeństwa), jako istotny element jednolitego rynku.
C. Obowiązek Państwa zapewnienia obywatelom prywatności i bezpieczeństwa, a przedsiębiorcom bezpieczeństwa obrotu gospodarczego,
D. Obowiązek Państwa stworzenia instancji cyfrowych tożsamości o zweryfikowanym poziomie bezpieczeństwa, który umożliwia realizację transgranicznych usług on-line.

Szanse

- Działania wynikające z wdrożenia Dyrektywy NIS są aktualnie w fazie określania kierunków i wypracowywania rozwiązań. Na tym etapie jeszcze można wpływać na ich kształt i proponować innowacyjne rozwiązania, charakteryzujące się wysokim poziomem bezpieczeństwa teleinformatycznego.
- Powszechne zrozumienie wagi problematyki cyberbezpieczeństwa oraz cyfrowej tożsamości, co jest jednym z celów dokumentów strategicznych oraz regulacji unijnych, może przełożyć się na wzrost nakładów inwestycyjnych na bezpieczne rozwiązania teleinformatyczne, zarówno ze strony Unii Europejskiej, państw członkowskich UE, w tym Polski, jak i przedsiębiorców.
- Aktywne uczestnictwo polskich podmiotów w wypracowywaniu metod i technik weryfikacji bezpieczeństwa pozwoli na szybsze i tańsze udostępnianie polskich produktów i usług wyróżniających się na tle konkurencji wysokim poziomem bezpieczeństwa teleinformatycznego.
- Aktywizacja współpracy między ośrodkami akademickimi, sektorem prywatnym oraz organizacjami pozarządowymi w celu zarządzania wiedzą i stymulowania innowacji w dziedzinie cyberbezpieczeństwa w Polsce.

Ryzyka

- Ograniczone możliwości zastosowania polskich rozwiązań w systemach ogólnoeuropejskich, z uwagi na niedostatek interoperacyjności lub innowacyjności tych rozwiązań.
- Wprowadzając jednolite mechanizmy weryfikacji bezpieczeństwa produktów i usług informatycznych na terenie Unii Europejskiej, Komisja Europejska i państwa członkowskie dążą do wzrostu konkurencyjności swoich produktów i usług

informatycznych, nie tylko na rynku europejskim, ale także globalnym, właśnie z uwagi na walor zweryfikowanego poziomu bezpieczeństwa teleinformatycznego. Brak aktywności Polski w tym strumieniu działań spowoduje spadek konkurencyjności polskich rozwiązań teleinformatycznych na jednolitym rynku i brak możliwości ich stosowania w wielu obszarach, np. w zamówieniach publicznych, dla których będą formułowane wymagania oferowania produktów lub usług o weryfikowanym (certyfikowanym, zgodnym z normami) poziomie bezpieczeństwa teleinformatycznego.

- Utrzymanie rozproszonej aktywności ośrodków uczelnianych, badawczych oraz sektora prywatnego, a w konsekwencji brak synergii w działaniach na rzecz wprowadzania innowacyjnych rozwiązań w obszarze cyberprzestrzeni.

Cele Programu CyberSecIdent powinny uwzględniać następujące kluczowe zagadnienie i wynikające z nich potrzeby z otoczenia polityczno - prawnego:

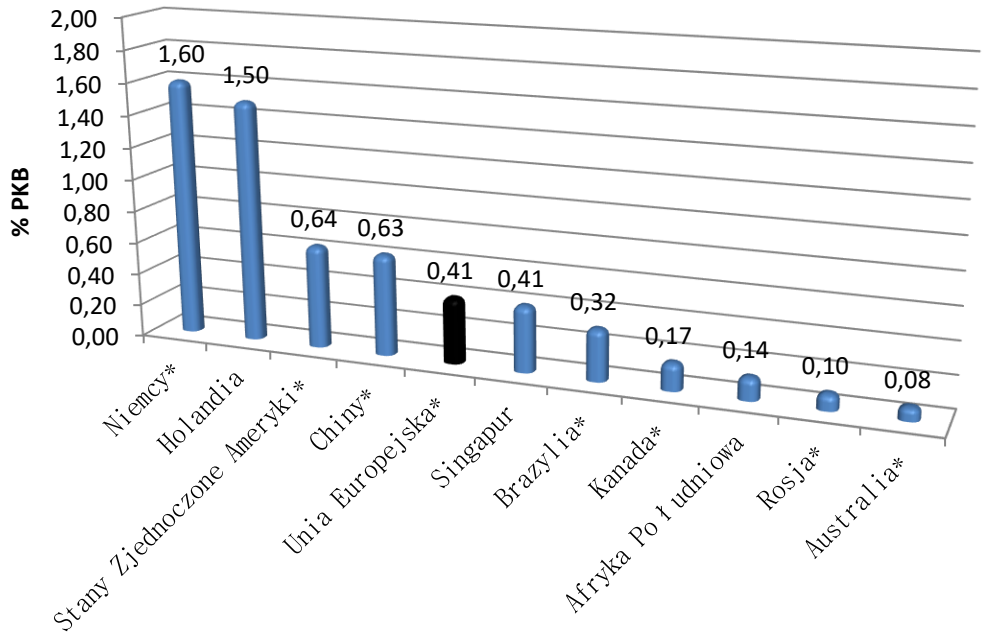
1. **Zapewnienie adekwatnego do potrzeb i możliwości udziału Polski w działaniach Unii Europejskiej na rzecz wspólnych rozwiązań w zakresie cyberbezpieczeństwa oraz opracowywania i wdrażania bezpiecznych produktów lub usług informatycznych w cyberprzestrzeni.**

Otoczenie ekonomiczne

Opis stanu

Rozwój technik informacyjnych zmienia gospodarkę światową. Wraz z nowymi usługami oraz wykorzystaniem nowych środków komunikacji do nowych sposobów realizacji procesów biznesowych i społecznych za pomocą nowych środków komunikacji, pojawiają się coraz większe problemy z bezpieczeństwem cyberprzestrzeni. Ten wpływ na ekonomię zaczął być mierzalny. Na poniższym rysunku zestawiono estymację wpływu cyberprzestępczości na produkt krajowy brutto (PKB) dla wybranych, przodujących gospodarek świata, oraz dodatkowo zbiorczo dla UE [16] . Jest to pierwszy, znany autorom, pomiar zjawiska cyberprzestępczości w ujęciu makroekonomicznym.

[16] Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, Center for Strategic and International Studies, June 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf



** kraje G20*

Rys. 1 Cyberprzestępczość wyrażona jako procent produktu krajowego brutto, dla wybranych krajów (McAffee, 2013)

Z powyższych zestawień wynika, że jeśli PKB dla Niemiec w 2013 roku wyniósł 3745 mld USD[17], to roczne straty gospodarki Niemiec z powodu cyberprzestępczości można oszacować na poziomie 59 mld USD.

Problemy z cyberbezpieczeństwem w wymiarze ekonomicznym dla przedsiębiorstw oznaczają przede wszystkim straty finansowe[18]. Z różnych dostępnych badań i ankiet adresowanych do przedsiębiorców, wynika, że straty z tytułu pojedynczego naruszenia bezpieczeństwa teleinformatycznego są z roku na rok większe.[19] Przykładowo, średnia roczna strata z tytułu naruszeń bezpieczeństwa teleinformatycznego przedsiębiorstwa w Niemczech, na podstawie ankietyzacji przeprowadzonej w 2016 roku, wynosiła 5 mln USD[20].

Najnowsze dostępne badania w odniesieniu do przedsiębiorstw, wskazują na problemy z bezpieczeństwem teleinformatycznym jako istotną przeszkodę w działalności gospodarczej. Warto, jednakże podkreślić, że w porównaniu do przedsiębiorstw z innych krajów UE (zob. Rys. 2), polskie przedsiębiorstwa przeważnie nie identyfikują lub nie informują o przypadkach naruszenia bezpieczeństwa informatycznego (procent polskich przedsiębiorców zgłaszających problemy cyberbezpieczeństwa jest dwa razy mniejszy niż średnia dla krajów UE i prawie trzy razy mniejszy niż dla Niemiec). Z danych analizowanych w rozdziale **Zagadnienia społeczno –**

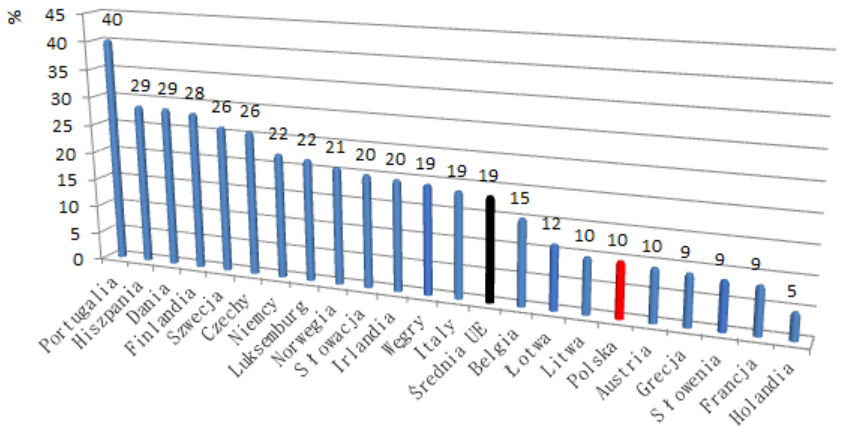
[17] http://data.worldbank.org/country/germany

[18] Zwykle w perspektywie krótkookresowej wskazuje się też na straty niewymierne, np. związane z utratą wizerunku, jednakże w ujęciu długoterminowym, także takie czynniki wylicza się w wartościach pieniężnych, zob. np. PN-ISO/IEC 27005:2013 Zarządzanie ryzykiem w bezpieczeństwie informacji

[19] Zob. http://www-03.ibm.com/security/data-breach/ 2016 Cost of Data Breach Study: Global Analysis

[20] Tamże

kulturalne wynika dodatkowo, że wśród polskich użytkowników Internetu skala identyfikacji problemów związanych z cyberbezpieczeństwem jest znacząco większa. Można sformułować tezę, że polskie przedsiębiorstwa nie nadążają z gotowością do obrony przed zagrożeniami z cyberprzestrzeni, skoro ich nie dostrzegają, a jeśli nawet je identyfikują, to nie informują o ich wystąpieniu.



Rys. 2 Procent przedsiębiorstw, które informowały o incydentach naruszenia bezpieczeństwa teleinformatycznego (Eurostat, 2010 r.)

Najnowsze badania statystyczne GUS w obszarze cyberbezpieczeństwa wykazują jednak zmianę tego stanu rzeczy i rosnące obawy polskich przedsiębiorców[21].

Mniej więcej co trzecie spośród wszystkich przedsiębiorstw (łącznie z sektorem finansowym), nie kupuje usług chmurowych ze względu na obawy związane z zagrożeniami naruszenia bezpieczeństwa. W 2014 roku było to 32,5% przedsiębiorstw[22], a rok później 33,4%[23].

Nieco mniejszy, ale także znaczący odsetek przedsiębiorstw napotyka problemy związane z bezpieczeństwem teleinformatycznym lub ochroną danych, które ograniczają lub wręcz uniemożliwiają im prowadzenie sprzedaży elektronicznej poprzez stronę internetową lub aplikacje mobilne. W 2014 roku tego typu problemy były raportowane przez 19,7% przedsiębiorstw (poza sektorem finansowym)[24], a dwa lata wcześniej ten odsetek wyniósł 18,4%.

[21] Z braku dostępnych danych nie ma możliwości porównania z innymi krajami UE.
[22] http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-telekomunikacyjnych-w-przedsiebiorstwach-i-gospodarstwach-domowych-w-2014-r-,3,12.html
[23] http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-telekomunikacyjnych-w-przedsiebiorstwach-i-gospodarstwach-domowych-w-2015-r-,3,13.html
[24] http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-telekomunikacyjnych-w-przedsiebiorstwach-i-gospodarstwach-domowych-w-2015-r-,3,13.html

Kluczowe czynniki

A. Cyberprzestępczość jest nowym rodzajem przestępczości, w tym gospodarczej, realizowanej nowymi środkami technicznymi, a ochrona przed nowymi zagrożeniami wymaga nowych metod i innowacyjnych rozwiązań.
B. Problemy cyberbezpieczeństwa przekładają się na wymierne straty finansowe dla przedsiębiorstw.
C. Problemy i obawy związane z cyberbezpieczeństwem mogą stać się czynnikiem hamującym popyt na nowoczesne rozwiązania teleinformatyczne (np. przetwarzania w chmurze), a tym samym wpłynąć na spowolnienie rozwoju gospodarki kraju.

Możliwości

- Rosnące potrzeby w zakresie bezpieczeństwa cyberprzestrzeni ze strony przedsiębiorstw mogą kreować popyt na produkty i usługi informatyczne gwarantujące wysoki i odpowiednio zweryfikowanym poziomie bezpieczeństwa. Usługi te mogą być dostarczane, zarówno przez przedsiębiorców prywatnych, jak i wyspecjalizowane jednostki administracji państwowej lub w modelu partnerstwa publiczno-prywatnego.
- Intensywny rozwój technik informacyjnych i komunikacyjnych może zwiększyć skłonność do inwestowania przedsiębiorców w nowe rozwiązania, jako pomysłu na zapewnienie bezpieczeństwa teleinformatycznego.
- Wyższy poziom bezpieczeństwa rozwiązań teleinformatycznych może sprzyjać unowocześnieniu gospodarki i inwestycjom w innowacje.

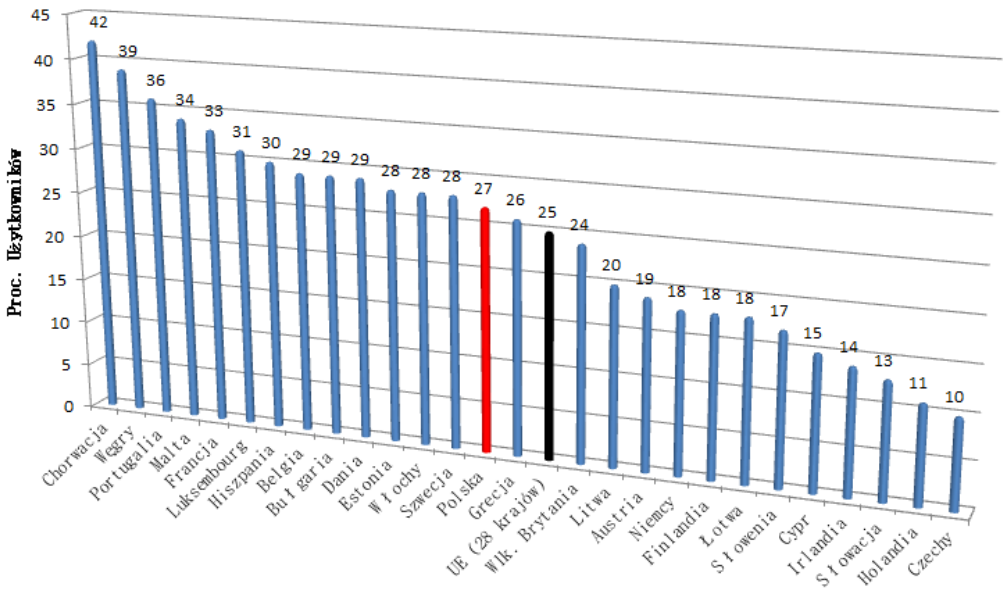
Ryzyka

- Brak skutecznych rozwiązań w zakresie cyberbezpieczeństwa, wobec rosnących obaw przedsiębiorstw, może skutkować spadkiem popytu na produkty i usługi teleinformatyczne i zahamowaniem wdrożeń nowych rozwiązań.
- Przy braku aktywnych działań, zarówno na poziomie UE, jak i w Polsce, wzrost cyberprzestępczości może stanowić istotną barierę wzrostu gospodarczego (zob. też część **Otoczenie społeczno – kulturalne**).

Otoczenie społeczno - kulturalne

Bezpieczeństwo cyberprzestrzeni jest nie tylko przedmiotem troski rządów i przedsiębiorstw, ale stanowi coraz większy problem dla użytkowników. W ostatnich latach rozległe badania statystyczne dotyczące bezpieczeństwa użytkowania usług w cyberprzestrzeni opublikował Eurostat [25] . Doświadczenia użytkowników w odniesieniu do bezpieczeństwa w cyberprzestrzeni w krajach UE zostały przedstawione na Rys. 3.

[25] http://ec.europa.eu/eurostat/documents/2995521/7151118/4-08022016-AP-EN.pdf/902a4c42-eec6-48ca-97c3-c32d8a6131ef

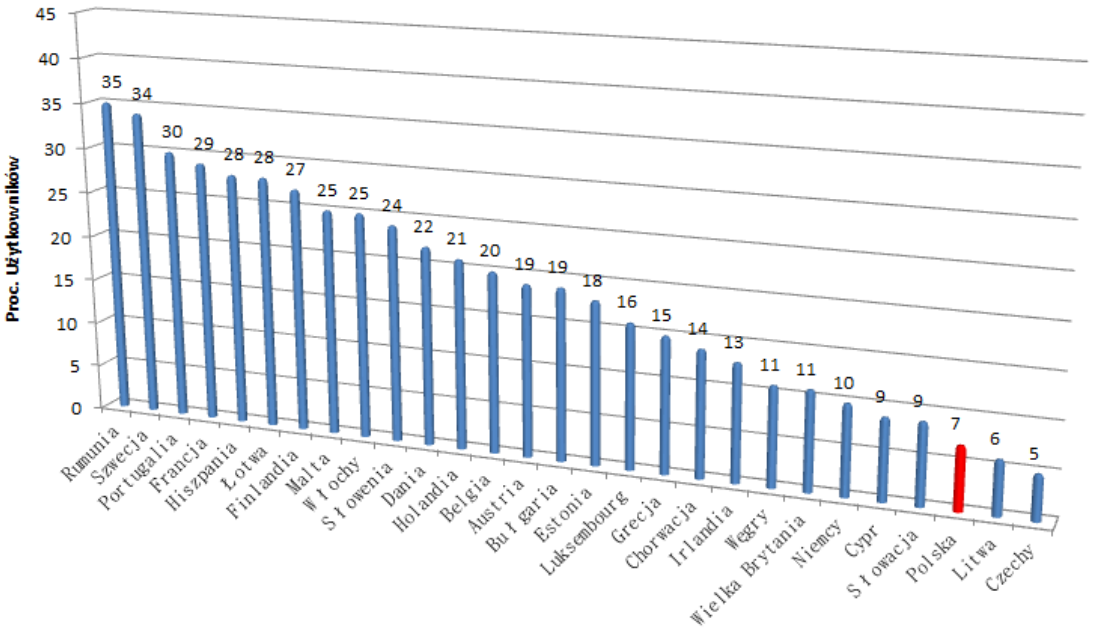


Rys. 3 Procent użytkowników Internetu w krajach członkowskich UE, którzy napotkali problemy związane z bezpieczeństwem[26] (Eurostat, 2015 r.)

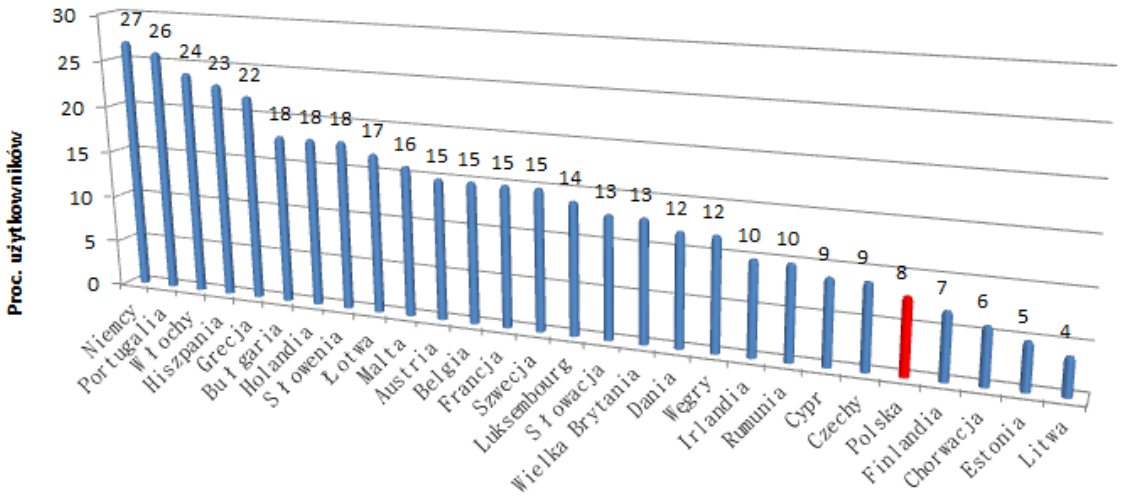
Z powyższych danych wynika, że średnio co czwarty użytkownik Internetu w UE doświadczył problemów związanych z bezpieczeństwem przy korzystaniu z usług dostępnych w Internecie. W Polsce odsetek ten jest nieznacznie większy i wynosi 27%.

Fakt odnotowania realnych problemów bezpieczeństwa przy korzystaniu z usług w Internecie, o czym świadczą przytoczone powyżej wyniki badań opublikowanych przez Eurostat, nie powoduje istotnego zmniejszenia zainteresowania tymi usługami w Polsce (zob. Rys. 4~~Rys. 4~~ i Rys. 5~~Rys. 5~~). Tylko mniej niż 10% polskich użytkowników Internetu, jako powód, dlaczego nie korzystają z usług on-line, podaje względy bezpieczeństwa. W innych krajach Unii ta percepcja jest odmienna. Przykładowo w Niemczech, gdzie szczególną wagę przykłada się do wysokiego bezpieczeństwa produktów i usług teleinformatycznych, jest wciąż najwyższy w Europie procent użytkowników, którzy nie korzystają z usług bankowości elektronicznej lub zakupów on-line.

[26] Użytkownicy mogli wskazać: zainfekowanie komputera złośliwym oprogramowaniem, które spowodowało utratę danych lub czasu, nieuprawnione użycie danych osobowych na portalach społecznościowych, straty finansowe w wyniku oszustw (np. phishing), straty finansowe wynikające z nieautoryzowanych płatności, dostęp dzieci do niewłaściwych stron lub kontakt dzieci z niewłaściwymi osobami nawiązany przez Internet.



Rys. 4 Procent użytkowników Internetu w krajach członkowskich UE, którzy NIE korzystają z usług zakupów on-line ze względów bezpieczeństwa (Eurostat, 2015 r.)



Rys. 5 Procent użytkowników Internetu w krajach członkowskich UE, którzy NIE korzystają z usług bankowości internetowej ze względów bezpieczeństwa (Eurostat, 2015 r.)

To konserwatywne podejście do usług on-line w części krajów członkowskich może znajdować potwierdzenie w badaniach opinii publicznej, zleconych przez Komisję Europejską w ramach inicjatywy Eurobarometr, w specjalnym wydaniu poświęconym problematyce cyberbezpieczeństwa[27]. W raporcie opisano stan cyberbezpieczeństwa na podstawie badań

[27] Special Eurobarometr 423 on Cybersecurity, 2015, http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

przeprowadzonych na jesieni 2014 roku. Ponieważ analogiczne badanie było przeprowadzone rok wcześniej[28] to można formułować wnioski porównawcze.

Badano zarówno **obawy** użytkowników odnoszące się do zagrożeń istniejących w cyberprzestrzeni, jak i **zdarzenia**, które wystąpiły i zostały odnotowane.

Analizując naruszenia bezpieczeństwa cyberprzestrzeni, część z nich odnosi się, bezpośrednio lub pośrednio, do cyfrowej tożsamości. Poniżej (zob. Tab. 1~~Tab. 1~~) zestawiono obawy i rzeczywistość dla różnych rodzajów naruszeń bezpieczeństwa w cyberprzestrzeni. Zdarzenia, które były związane z utratą lub przejęciem cyfrowej tożsamości, zaznaczono w tabeli brązową czcionką.

Rodzaj zdarzenia	Obawy - Polska	Obawy - wzrost w porównaniu do stanu z 2013 roku	Obawy - średnia UE	Obawy - wzrost w porównaniu do stanu z 2013r	Zgłoszenia - Polska	Zgłoszenia - wzrost w porównaniu do stanu 2013r	Zgłoszenia - średnia UE	Zgłoszenia - wzrost w porównaniu dostanu z 2013r
kradzież tożsamości	**62%**	**+7**	**68%**	**+16**	**8%**	**-**	**7%**	**+1**
oszustwa transakcji z użyciem kart płatniczych lub w bankowości internetowej	**62%**	**+11**	**63%**	**+14**	**7%**	**+1**	**8%**	**+1**
przejęcie konta poczty elektronicznej lub w mediach społecznościowych	**57%**	**+11**	**60%**	**+15**	**9%**	**+1**	**12%**	**-**
złośliwe oprogramowanie na swoim urządzeniu	67%	bd	66%	+3	43%	bd	47%	bd
oszustwa w usługach on-line	51%	bd	56%	+12	19%	+7	16%	+6
próba wyłudzenia za pośrednictwem poczty elektronicznej lub połączeń telefonicznych	56%	+6	57%	+14	19%	+2	30%	-5
przypadkowe natrafienie na pornografię dziecięcą	56%	+6	52%	+8	13%	bd	7%	bd
przypadkowe natrafienie na treści o charakterze rasistowskim, mowy nienawiści itp.	49%	+7	46%	+11	22%	+7	14%	-
brak dostepności usług on-line z powodu cyberataku	58%	+12	50%	+13	14%	+6	14%	+2
okup za za odzyskanie kontroli nad urządzeniem	54%	bd	47%	bd	9%	bd	8%	bd
bd - brak danych								

Tab. 1 Procent użytkowników wyrażających obawę w odniesieniu do różnych kategorii naruszeń bezpieczeństwa w cyberprzestrzeni oraz procent użytkowników, którzy zgłosili takie naruszenia (Eurobarometr, 2014-2015]

Z badań Eurobarometru wynika wzrost obaw użytkowników w odniesieniu do bezpieczeństwa cyberprzestrzeni, we wszystkich kategoriach. Niemniej jednak, w kategoriach związanych z cyfrową tożsamością te wzrosty są bardziej widoczne, zwłaszcza porównując dane z Polski z średnią dla UE.

Należy wskazać, że najwięcej użytkowników (68%) obawia się kradzieży tożsamości (wzrost obaw w tej kategorii odnotowano też w badaniach przeprowadzonych w 2012 roku). Dopiero na drugim miejscu (66%) znalazła się obawa związana ze zidentyfikowaniem złośliwego oprogramowania na swoim urządzeniu. Co więcej, dla obawy kradzieży tożsamości zanotowano największy przyrost (16 %), w porównaniu do badań przeprowadzonych w 2013

[28] http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

roku. Największy odsetek użytkowników wyrażających swoje obawy co do kradzieży tożsamości odnotowano we Francji (80%) oraz w Hiszpanii (79%). Polska z wynikiem 62% znajdowała się w grupie krajów o najniższym poziomie takiej obawy.

Jednakże, analizując zgłoszenia kradzieży tożsamości okazuje się, że odsetek użytkowników, którzy padli ofiarą tego typu zdarzenia, jest podobny we wszystkich Krajów Członkowskich UE, przy czym średnia wynosi 7%, a najwyższy poziom zgłoszeń odnotowano w Rumunii i na Węgrzech (po 11%). Wartość dla Polski (8%) była nieznacznie wyższa niż średnia UE.

Należy oczekiwać, że ten stan może dość szybko się zmienić, jeśli odnotowano tak znaczny odsetek użytkowników wyrażających obawy w tej kategorii naruszeń bezpieczeństwa (efekt samospełniającej się prognozy).

Kluczowe czynniki

A. Jedną z przyczyn dysproporcji między postrzeganiem problemów a nie dostrzeganiem ryzyka jest niski poziom świadomości i uwrażliwienia polskich użytkowników Internetu na problemy bezpieczeństwa cyberprzestrzeni, przy jednoczesnym realnym, bardzo niskim poziomie ochrony cyberprzestrzeni RP.
B. Jednocześnie, użytkownicy w całej UE wyrażają obawy w odniesieniu do potencjalnych zdarzeń naruszenia bezpieczeństwa cyberprzestrzeni, a zwłaszcza w odniesieniu do cyfrowej tożsamości, co może przekładać się na potrzeby zapewnienia ochrony przed niepożądanymi zjawiskami.

Możliwości

- Masowość użytkowania usług w cyberprzestrzeni, potrzeby wynikające z obaw co do bezpieczeństwa, mogą przełożyć się na znaczny wzrost popytu na rozwiązania charakteryzujące się jednocześnie, niskim kosztem i jednocześnie zweryfikowanym poziomem bezpieczeństwa. Oczekiwanym skutkiem powinien być rozwój istniejących i powstawanie nowych firm z obszaru nowych technologii, wzrost gospodarczy kraju, eksport na rynki międzynarodowe innowacyjnych rozwiązań i pojawienie się nowych miejsc pracy.

Ryzyka

- Rozdźwięk między potrzebami polskich użytkowników a faktycznym poziomem bezpieczeństwa w Internecie może spowodować gwałtowny spadek zaufania do usług świadczonych on-line, spowodowany incydentami o znacznych konsekwencjach dla osób fizycznych, nie tylko o charakterze finansowym.

Cele Programu CyberSecIdent powinny uwzględniać następujące kluczowe zagadnienia oraz wynikające z nich potrzeby z otoczenia ekonomicznego oraz społeczno – kulturalnego:

2. **Zapewnienie skutecznego oddziaływania na poziom bezpieczeństwa cyberprzestrzeni jako środowiska działalności gospodarczej i społecznej.**
3. **Zapewnienie rozwiązań odpowiadających na obawy użytkowników w zakresie cyberbezpieczeństwa.**

Otoczenie technologiczne

Opis stanu

W strategii UE w zakresie cyberbezpieczeństwa[29], jak również w strategii jednolitego rynku cyfrowego[30], zapisano potrzebę wspierania wzrostu podaży produktów i usług ze strony unijnego sektora cyberbezpieczeństwa. Zadanie to będzie realizowane przez Komisję Europejską i przybierze postać nowatorskiego europejskiego programu badań naukowych i innowacji w zakresie bezpieczeństwa cyberprzestrzeni[31] na rzecz większej konkurencyjności, w formule partnerstwa publiczno – prywatnego. Na dzień aktualizacji dokumentacji aktualna jest strategia UE w zakresie unii bezpieczeństwa z 24 lipca 2020 r.[32]

Planując dalsze, intensywne działania w kierunku podniesienia bezpieczeństwa cyberprzestrzeni, Komisja Europejska zakłada też szerokie wykorzystanie wyników prac badawczo - rozwojowych prowadzonych w Europie w ramach poprzedniej perspektywy budżetowej[33]. Z danych przedstawionych przez Komisję Europejską wynika, że w latach 2007-2014, w ramach programów 7. Programu Ramowego oraz CIP (*Competitiveness and Innovation Programme*), zrealizowano 101 projektów naukowo -badawczych dotyczących cyberbezpieczeństwa w na łączną kwotę 340 mln euro. W poniższej tabeli zestawiono liczbowo udział organizacji z poszczególnych krajów UE w projektach FP7.

[29] JOIN (2013) 1 final JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

[30] COM (2015) 192., COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe

[31] Aktualizacja w ramach ujednolicenia terminologii

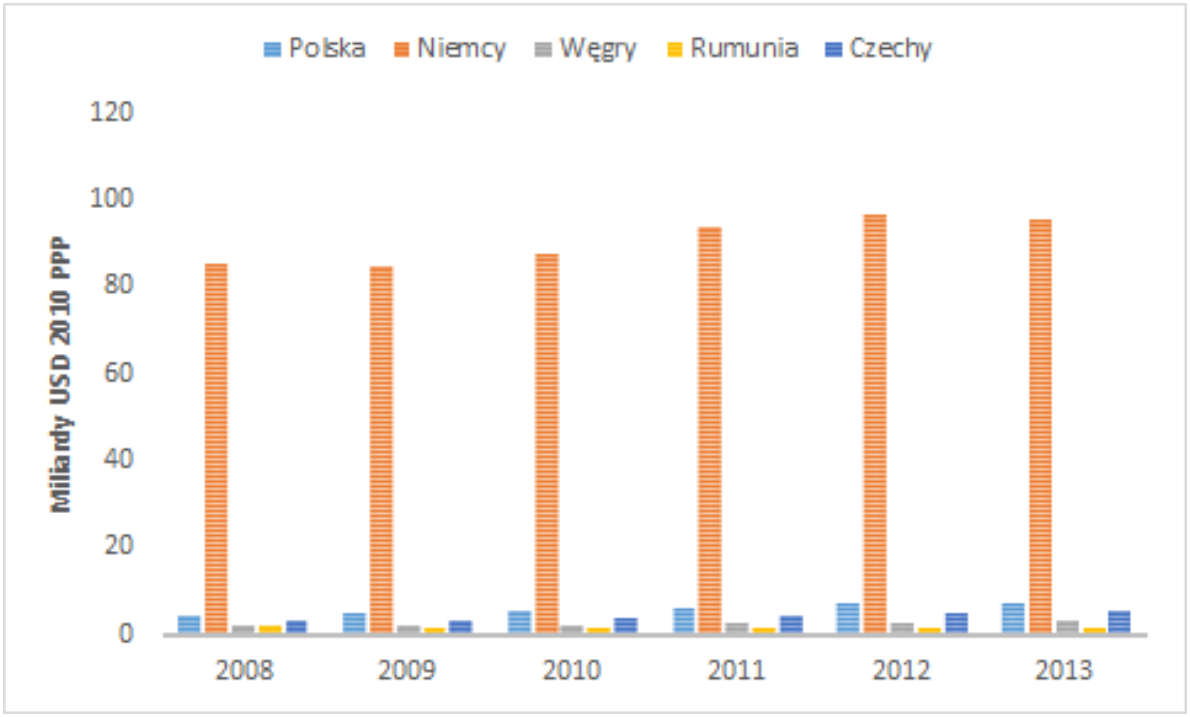
[32] COM (2020) 605 final, COMMUNICATION FROM THE COMMISSION on the EU Security Union Strategy

[33] SWD (2016) 210 final, an assessment of the implementation and participation in the EU Trust and Cybersecurity RTD and innovation programme funded by FP7 and CIP grants (2007 - 2013)

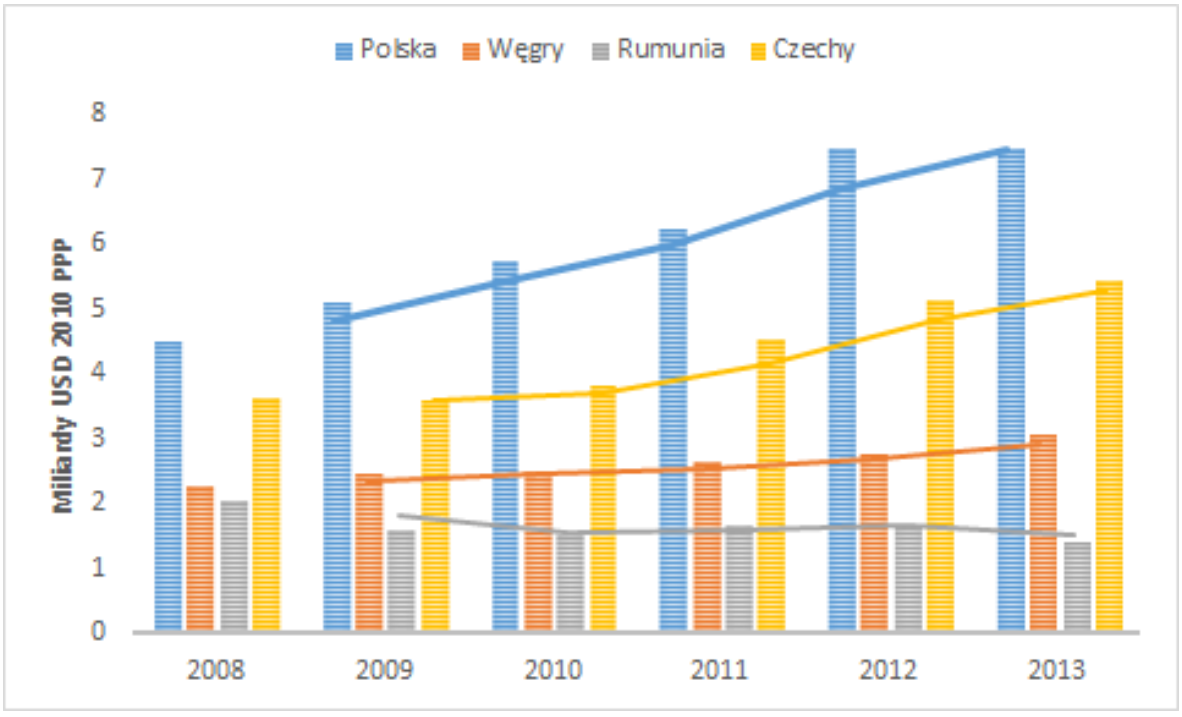
Kraj UE	Jedn. nauk. bad.	Przedsiębiorstwa	Inne	Razem
Niemcy	55	44	2	**101**
Włochy	42	36	4	**82**
Francja	31	39	4	**74**
Hiszpania	20	33	7	**60**
Wlk. Brytania	18	21	2	**41**
Austria	20	10	5	**35**
Holandia	14	15	2	**31**
Grecja	18	10	2	**30**
Belgia	11	10	5	**26**
Szwajcaria	9	15	1	**25**
Szwecja	8	6	7	**21**
Portugalia	5	10	0	**15**
Norwegia	12	2	0	**14**
Finlandia	7	5	0	**12**
Dania	6	4	0	**10**
Irlandia	5	5	0	**10**
Rumania	4	3	1	**8**
Czechy	1	6	0	**7**
Polska	1	4	0	**5**
Węgry	1	3	0	**4**
Bułgaria	2	0	1	**3**
Estonia	0	3	0	**3**
Luksemburg	1	0	1	**2**
Słowenia	0	2	0	**2**

Tab. 2 Udział organizacji z poszczególnych krajów UE w 7. Programie Ramowym oraz CIP

Analizując nakłady na prace B+R na przestrzeni kilku ostatnich lat, należy wskazać szereg czynników wskazujących na niski potencjał Polski w tej dziedzinie, o czym świadczą poniższe dane. Aby lepiej zaprezentować pozycję Polski, do porównania wybrano potęgę gospodarczą (Niemcy) oraz kraje „nowej Unii" (Czechy, Węgry, Rumunia).



Rys. 6 Nakłady na prace B+R w wybranych krajach UE, z uwzględnieniem parytetu siły nabywczej (OECD, 2014 r.)



Rys. 7 Nakłady na prace B+R w wybranych krajach UE (bez Niemiec), z uwzględnieniem parytetu siły nabywczej (OECD, 2014 r.)

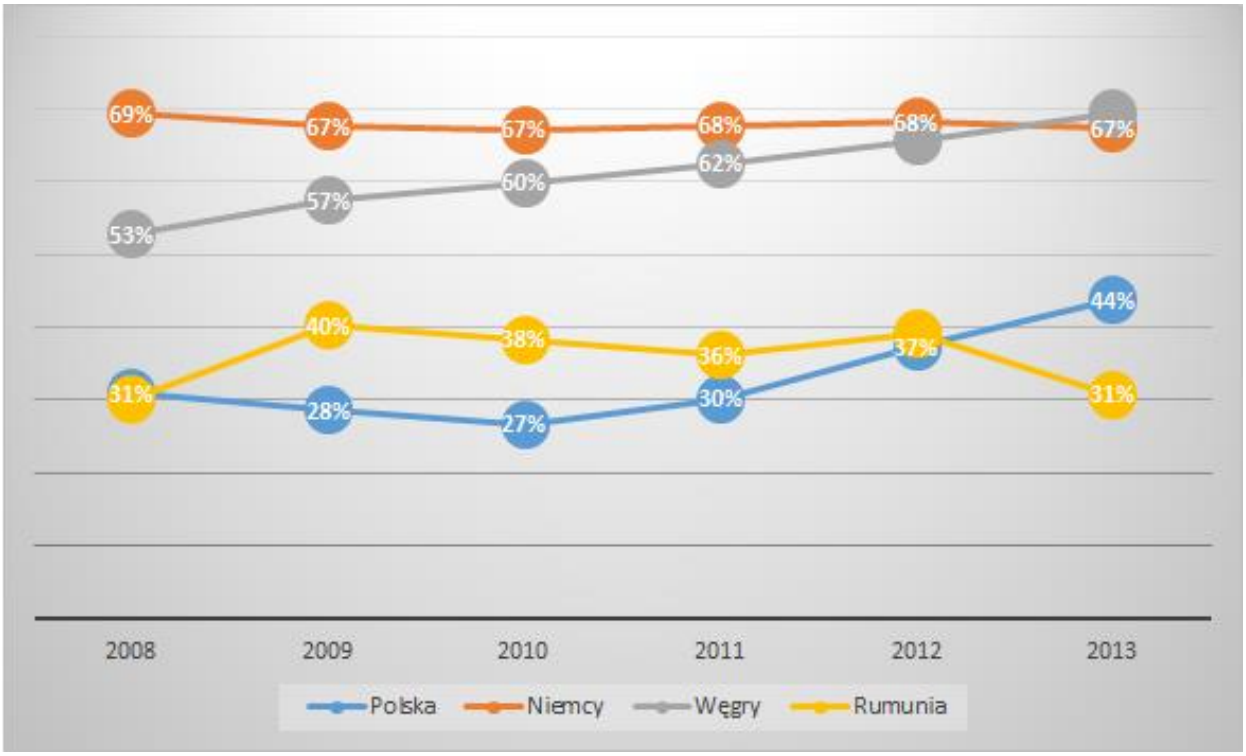
W liczbach bezwzględnych (zob. Rys. 6 oraz Rys. 7), nakłady Niemiec na działalność B+R są na przestrzeni analizowanych lat ok. 10 razy większe niż Polski. Warto podkreślić, że trend rosnący dla Polski w tej kategorii makroekonomicznej jest większy niż dla innych krajów „nowej Europy" (zob. Rys. 7).

Całości obrazu ogólnego potencjału B+R w skali kraju dopełnia odniesienie wydatków na działalność B+R do produktu krajowego brutto (zob. Tab. 3~~Tab. 3~~Tab. 2). Wynika z niej, że jakkolwiek trend jest rosnący, to na tle innych krajów UE, nakłady na działalność B+R są ciągle niskie.

Czechy	Niemcy	Węgry	Polska	Rumunia
2,00%	2,87%	1,37%	**0,94%**	0,38%

Tab. 3 Wydatki na działalność B+R jako% PKB (Bank Światowy, 2013)[34]

Dodatkowo, analizując ogólnie potencjał sektora prywatnego jako udział w wydatkach na prace B+R, należy wskazać na niską wartość tego wskaźnika na tle innych krajów UE, jakkolwiek można zaobserwować silny trend rosnący. (zob. Rys. 8).



Rys. 8 Udział sektora prywatnego w wydatkach na B+R w wybranych krajów UE w latach 2008-2013 (OECD, 2014 r.)

W odniesieniu bezpośrednio do zagadnień B+R związanych z cyberbezpieczeństwem, w Krajowym Programie Badań (określany dalej jako KPB) [35] ,sformułowano strategiczne kierunki badań naukowych i prac rozwojowych. Program CyberSecIdent wpisuje się w dwa z wymienionych kierunków:

- zaawansowane technologie informacyjne, telekomunikacyjne i mechatroniczne,

[34] Wydatki na działalność B+R jako % PKB do 2016 r. dostępne na stronie: https://data.worldbank.org/indicator/gb.xpd.rsdv.gd.zs?end=2016&start=2013

[35] http://www.bip.nauka.gov.pl/krajowy-program-badan/; Od 2022 roku KPB zostało zastąpione Polityką Naukową Państwa.

- bezpieczeństwo i obronność państwa.

Analizując zapisy dotyczące rozwiązań z obszaru technik informacyjnych i komunikacyjnych, określanych jako TIK, cyberbezpieczeństwu poświecono tylko jeden akapit:

„Mimo bardzo istotnych korzyści związanych z rozwojem technologii i społeczeństwa informacyjnego należy także zwrócić uwagę na zagrożenia wynikające ze stosowania i demokratyzacji sieci, w tym na cyberterroryzm lub dostęp cyberprzestępców do danych wrażliwych, poufnych czy tajnych."

Należy podkreślić, że powyższe stwierdzenie – zgodnie z analizą przeprowadzoną przez Autorów – nie przełożyło się na jakikolwiek odrębny program zdefiniowany i realizowany w ramach działalności NCBR (zob. Tab. 4~~Tab. 4~~). Jednocześnie, kierunek strategiczny „zaawansowane technologie informacyjne, telekomunikacyjne i mechatroniczne" tylko w niewielkim stopniu odnosi się do problemów bezpieczeństwa cyberprzestrzeni RP w zakresie, w jakim zostały one wskazane w Dyrektywie NIS oraz, w konsekwencji, w dokumencie „Strategia Cyberbezpieczeństwa RP na lata 2016-2020" (zob. część **Otoczenie polityczno – prawne**). Od 31 października 2019 r. obowiązuje Strategia Cyberbezpieczeństwa RP na lata 2019-2024. Głównym celem strategii jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i komunikacyjnym.

Kierunek strategiczny „bezpieczeństwo i obronność państwa" zawiera odniesienie do zagadnień związanych z tematyką programu CyberSecIdent, jednakże należy podkreślić, że bezpieczeństwo i obronność państwa jest ważnym, ale nie jedynym aspektem bezpiecznego funkcjonowania cyberprzestrzeni RP. W agendzie badawczej programu CyberSecIdent uwzględniono niektóre kierunki badań sformułowane w tym rozdziale KPB.

Brak wyraźnych kierunków prac B+R w odniesieniu do bezpieczeństwa cyberprzestrzeni przełożył się na bardzo niewielki udział projektów w tym obszarze, w porównaniu do liczby oraz nakładów w programach operacyjnych oraz strategicznych, realizowanych przez NCBR (zob. Tab. 4).

Nazwa progamu	Wartość przekazanego dofinansowania - ogółem [mln PLN]	Liczba realizowanych projektów związanych z cyber-bezpieczeństwem	Okres realizacji	Wartość dofinansowania projektu [mln PLN]	Udział dofinansowania projektów związanych z cyberbezpieczeństwem w odniesieniu do poziomu dofinansowania całego Programu
Program Operacyjny Innowacyjna Gospodarka	49 836,54	2	2007-2014	74,07	0,15%
Programy i Projekty rozwojowe - obronność bezpieczeństwo	3 360,17	5	2011-2015	32,04	0,95%
INNOTECH	1 774,00	2	2012-2015	7,18	0,40%

Tab. 4 Nakłady na projekty związane z bezpieczeństwem cyberprzestrzeni w programach NCBR (opracowanie własne)

W odniesieniu do potencjału ludzkiego należy wskazać, że w latach 2014 i 2015 tylko na jednej uczelni w Polsce (Wojskowa Akademia Techniczna) uruchomiono i kształcono na kierunku, którego zakres był bezpośrednio poświęcony tematyce cyberbezpieczeństwa. Na kierunku „Kryptologia i cyberbezpieczeństwo" studiowało 106 osób w 2014 roku[36] i 170 w 2015 roku.[37]

Kluczowe czynniki

A. Na podstawie powyższych danych można sformułować tezę, że innowacyjność rozwiązań teleinformatycznych w aspekcie bezpieczeństwa teleinformatycznego, których podstawą muszą być prace B+R, w Polsce miała i ma nadal niewielkie systemowe wsparcie.
B. Jednostki naukowo–badawcze, a także przedsiębiorstwa, mają ograniczone doświadczenie i kompetencje w opracowywaniu i wdrażaniu innowacyjnych rozwiązań w dziedzinie cyberbezpieczeństwa.
C. Powstaje europejski program badań naukowych i innowacji w zakresie cyberbezpieczeństwa na rzecz większej konkurencyjności, w formule partnerstwa publiczno – prywatnego, w którym udział Polski powinien być większy niż w podobnych programach poprzednich perspektyw budżetowych.

Możliwości

- Zwiększenie nakładów B+R na programy strategiczne może dać impuls w postaci podaży produktów w odpowiedzi na przewidywany wzrost popytu na innowacyjne rozwiązania charakteryzujące się potwierdzonym poziomem bezpieczeństwa teleinformatycznego.
- Podniesienie kompetencji i uzyskanie doświadczenia w zakresie B+R pozwoli na większy udział polskich jednostek naukowo – badawczych w ogólnoeuropejskich programach B+R, w ramach wybranych specjalności.
- W wyniku realizacji projektów B+R o wysokim poziomie gotowości technologicznej (VIII lub IX) powinny powstać produkty i usługi IT, które znajdą zastosowanie na rynku krajowym i zagranicznym oraz podniosą konkurencyjność polskiej gospodarki.

Ryzyka

- Brak polskich rozwiązań w zakresie cyberbezpieczeństwa jako efekt braku nakładów na programy B+R w obszarze bezpieczeństwa cyberprzestrzeni, może skutkować całkowitym uzależnieniem od rozwiązań zagranicznych.

[36] http://stat.gov.pl/obszary-tematyczne/edukacja/edukacja/dane-wstepne-dotyczace-szkolnictwa-wyzszego-2014-r-,8,2.html
[37] W roku 2019 sytuacja uległa radykalnej zmianie. Kierunki związane z cyberbezpieczeństwem zostały uruchomione na wielu uczelniach.

- Niedostatek kompetencji i doświadczenia jednostek naukowo – badawczych oraz przedsiębiorstw w realizacji projektów B+R z poziomem technologii umożliwiającym wdrożenie produkcyjne może spowodować, że polskie rozwiązania będą nieinnowacyjne, a przez to niekonkurencyjne w stosunku do rozwiązań europejskich.
- Efektem braku doświadczenia w budowaniu konsorcjów naukowo-przemysłowych oraz prowadzeniu prac B+R będzie utrzymanie niskiej skuteczności polskich zespołów w pozyskiwaniu europejskiego finansowania na badania i prace rozwojowe.

Cele Programu CyberSecIdent powinny uwzględniać następujące kluczowe zagadnienie oraz wynikająca z nich potrzebę z otoczenia technologicznego:

4. **Konieczność zwiększenia nakładów i w konsekwencji zwiększenia liczby projektów B+R wspierających innowacyjność polskich produktów i usług teleinformatycznych w aspekcie bezpieczeństwa teleinformatycznego.**

Cel główny i cele szczegółowe realizacji Programu

Przesłanki określenia celów Programu

Rzeczywisty poziom bezpieczeństwa, który też wyraża pewność i zaufanie obywateli i przedsiębiorców do rozwiązań teleinformatycznych, mierzony wskaźnikami statystycznymi, powinien znacząco wzrosnąć w porównaniu do stanu początkowego.

Ponadto, wzrost konkurencyjności i innowacyjności polskich produktów informatycznych z uwzględnieniem aspektów bezpieczeństwa teleinformatycznego będzie służył rzeczywistemu podniesieniu bezpieczeństwa cyberprzestrzeni, globalnie, w wymiarze europejskim oraz w szczególności cyberprzestrzeni RP.

Wreszcie, innowacyjność polskich rozwiązań teleinformatycznych, polegająca na zastosowaniu wyników badań B+R do wdrożeń w obszarze bezpieczeństwa teleinformatycznego pozwoli, nie tylko reaktywnie, ale również proaktywnie oddziaływać na bezpieczeństwo cyberprzestrzeni.

Powyższe przesłanki pozwalają na sformułowanie celów Programu CyberSecIdent.

Cel główny Programu

Podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP przez zwiększenie dostępności narzędzi sprzętowo–programistycznych, do roku 2028

Cele szczegółowe Programu

1. Wdrożenie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości

2. Wdrożenie metod i technik identyfikacji i uwierzytelniania.[38]

Agenda badawcza

Przesłanki do określenia tematów badawczych

1. Krajowy Program Badań (KPB)2[39], ustanowiony przez Radę Ministrów w formie uchwały (art. 4 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (Dz. U. z 2014 r. poz. 1620 oraz Dz. U. z 2015 r. poz. 249), określa cel rozwoju polskiej nauki oraz wskazuje strategiczne dla państwa kierunki badań i prac rozwojowych.

Zakres tematów badawczych programu CyberSecIdent jest związany z jednym ze strategicznych, interdyscyplinarnych kierunków badań naukowych i prac rozwojowych rozwoju nauki określonym jako „Bezpieczeństwo i obronność państwa". W tym obszarze zdefiniowano przedstawione poniżej priorytetowe obszary rozwoju technologii w sferze bezpieczeństwa wewnętrznego:

1) Nowoczesne technologie i innowacyjne rozwiązania w zakresie wykrywania, zwalczania i neutralizacji zagrożeń,
2) Technika kryminalistyczna,
3) Indywidualne środki ochrony i wyposażenia,
4) Profilaktyka społeczna, wiktymologia, kryminologia oraz badania społeczne,
5) Organizacja i zarządzanie,
6) Nowoczesne technologie lub rozwiązania innowacyjne w sferze bezpieczeństwa teleinformatycznego, ochrony informacji w systemach i sieciach teleinformatycznych oraz narodowej kryptografii.

2. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, która określa:
   a. organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;
   b. sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;
   c. zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

[38] Z wyłączeniem rozwiązań o większym rozmiarze, takich jak platformy zarządzania cyfrową tożsamością.

[39] Od 2022 roku KPB zostało zastąpione Polityką Naukową Państwa.

3. Uchwała nr 125 Rady Ministrów z 22 października 2019 wraz ze Strategią Cyberbezpieczeństwa RP na lata 2019-2024.

   Strategia Cyberbezpieczeństwa RP na lata 2019-2024 określa w szczególności:

   - Cel główny: Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.
   - Cel szczegółowe:
     - Rozwój krajowego systemu cyberbezpieczeństwa.
     - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.
     - Zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni.
     - Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa.
     - Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

Zakres tematyczny Programu jest wystarczający dla wsparcia celów Strategii w zakresie związanym głównie z ochroną cyfrowej tożsamości.

4. „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020”[40],

W dokumencie tym przewiduje się znaczący wkład sektora B+R w bezpieczeństwo cyberprzestrzeni RP (zob. rozdział 6.3):

„(..) *Do głównych zadań w tym zakresie należy zaliczyć m.in. badanie i opisywanie sposobów i metod ataków, cyberprzestępstw, cyberterroryzmu, a także opracowywanie skutecznych metod przeciwdziałania. Zakłada się opracowanie rozwiązań umożliwiających:*

a) szybką identyfikację zagrożeń,
b) usprawnienie systemu informowania o zagrożeniach,
c) podniesienie efektywności zabezpieczeń proceduralno-organizacyjnych i technicznych,
d) skuteczne informowanie użytkowników cyberprzestrzeni o zagrożeniach,
e) podnoszenie wiedzy informatycznej użytkowników cyberprzestrzeni,
f) wypracowanie metod obrony przed zmasowanymi atakami z cyberprzestrzeni”

[40] https://mc.gov.pl/files/strategia_v_29_09_2016.pdf

Tematy badawcze[41]

(i) Technologie i rozwiązania w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia na poziomie państwa:
   a. Skuteczne monitorowanie i szybka identyfikacja zagrożeń,
   b. Metody i techniki wizualizacji zagrożeń w cyberprzestrzeni,
   c. Metody i techniki obrony przed zmasowanymi atakami z cyberprzestrzeni oraz ochrony prywatności,
   d. Metody i techniki dla postępowania po incydencie,
   e. Dynamiczne i statyczne metodyki szacowania ryzyka,
   f. Rozwiązania z zakresu technicznych metod identyfikacji nieprzyjaznych operacji dezinformacyjnych w cyberprzestrzeni, prowadzonych w oparciu o narzędzia teleinformatyczne,
   g. Techniki i metody przeciwdziałania nowym, zaawansowanym atakom na infrastrukturę dostępową i aplikacje w sieci 5G.

(ii) Technologie i rozwiązania w zakresie tożsamości cyfrowej, z uwzględnieniem aspektów prywatności:
   a. Dedykowane rozwiązania sprzętowe w technologiach nowej generacji, wykorzystujące układy mikroelektroniczne, w tym specjalizowane układy scalone ASIC oraz układy programowalne FPGA,
   b. Techniki uwierzytelniania z wykorzystaniem systemów i rozwiązań biometrycznych,
   c. Aplikacje do cyfrowej tożsamości, w tym oparte o przeglądarki internetowe,
   d. Zabezpieczenia i deidentyfikacja danych,
   e. Rozwiązania sprzętowo – programowe zapewniające realizację zasady bezpieczeństwa E2E (end to end), w tym nowe komponenty z wbudowanymi elementami bezpieczeństwa, takie jak (U)SIM, odporne na manipulacje urządzenia abonenckie obsługowe i bezobsługowe, zdolne do ochrony tożsamości sieciowej w systemach zarządzania tożsamością.

(iii) Metodyki, techniki i procesy w obszarze analizy cyberbezpieczeństwa i cyfrowej tożsamości oraz ich wdrożenia:
   a. Metody i techniki weryfikacji bezpieczeństwa dla różnych warstw struktur sprzętowo – programistycznych opartych na międzynarodowych standardach takich jak ISO 15408 oraz opracowanie krajowego schematu certyfikacji,
   b. Metody i techniki weryfikacji bezpieczeństwa modułów kryptograficznych,
   c. Metody i wzorce projektowe security by design dla danych przetwarzanych w systemach teleinformatycznych administracji publicznej,
   d. Metody i wzorce projektowe privacy by design dla danych przetwarzanych w systemach teleinformatycznych administracji publicznej,

[41] Aktualizacja zgodnie z Agendą Badawczą dla III konkursu oraz zakresem tematycznym

e. Metody i techniki efektywnego testowania integralności urządzeń na etapie wdrażania i eksploatacji (zarówno komponentów sieci, jak i urządzeń końcowych), w tym w sieci 5G,
f. Metody i techniki ewaluacji bezpieczeństwa i prywatności urządzeń Internetu Rzeczy (IoT - Internet of Things) i Internetu Pojazdów (IoV - Internet of Vehicles), smart cities, telemedycyny, aplikacji mobilnych, komponentów sieci 5G, w tym oprogramowania wirtualizacyjnego funkcji sieciowych,
g. Narzędzia do analizy zagrożeń w cyberprzestrzeni, ze szczególnym uwzględnieniem monitorowania infrastruktury wykorzystywanej do ataków oraz szkodliwego oprogramowania,
h. Stworzenie polskiego, nowoczesnego systemu oceny i certyfikacji bezpieczeństwa produktów i usług ICT, funkcjonującego w europejskich ramach certyfikacji z wyłączeniem standardu normy ISO 15408.

Krótka charakterystyka tematów badawczych

Ad (i)

Proponowany temat badawczy dotyczy prac B+R, których celem jest opracowanie nowych metod monitorowania, analizy i przetwarzania różnych strumieni danych w celu identyfikacji w czasie rzeczywistym zagrożeń oraz opracowania skutecznych technik obrony przed takimi atakami sieciowymi.

Uwaga powinna koncentrować się na metodach wykrywania i analizy zdarzeń niepożądanych występujących, zarówno w sieciach teleinformatycznych pracujących w protokole sieciowym TCP/IP, jak i w przemysłowych sieciach automatyki przemysłowej i systemów sterowania, w sieciach bezprzewodowych, a także w Internecie Rzeczy. Zakłada się objęcie badaniami metod wykrywania szerokiego zakresu cyberataków realizowanych z wykorzystaniem różnych technik i sposobów użytych do uzyskania nieautoryzowanego dostępu do systemu komputerowego lub urządzenia sieciowego, w celu przejęcia nad nim kontroli, bądź wydobycia informacji. Rozważane będą różne źródła, cele, profile i wektory ataku, w tym DDoS (*Distributed Denial of Service*), kampanie *spamowe* i inne. Szczególne znaczenie w tym kontekście ma opracowanie skutecznych metod i technik w odniesieniu do automatycznie generowanych ataków, które stanowią obecnie jedno z najpoważniejszych rodzajów zagrożeń w cyberprzestrzeni.

Istotnym elementem badawczym powinno być uzyskanie kompletności podejścia do zagadnienia, w tym metody i techniki realizacji działań ex-ante (zapobieganie incydentom), jak i ex-post (postępowanie po incydencie).

Nowatorski charakter badań powinien wynikać z opracowania, a następnie wykorzystania narzędzi sprzętowych i programistycznych do identyfikacji modeli ataków na podstawie obserwacji sieci teleinformatycznych, wykrywania ich potencjalnych celów, prognozowania trendów oraz dostarczania charakterystyk pozwalających na prowadzenie działań obronnych.

Badania powinny mieć charakter interdyscyplinarny (metody statystyczne, techniki sztucznej inteligencji itd.) i obejmować mechanizmy przetwarzania strumieni informacji uzyskiwanych z różnych źródeł, w tym, że sfederowanych systemów monitorujących krajową cyberprzestrzeń[42]. Istotnym aspektem wpływającym na szybkość i skuteczność detekcji zagrożenia jest odpowiednia wizualizacja sytuacji w cyberprzestrzeni. Badania powinny obejmować opracowanie skutecznych rozwiązań pozwalających na wielowymiarowe obrazowanie zjawisk występujących w cyberprzestrzeni[43], m.in. uwzględniające różnorodność typów informacji, przynależność sektorową i geograficzną, a także stopień krytyczności.

Podsumowaniem wykonanych badań powinny być gotowe do wdrożenia najistotniejsze komponenty kompleksowego systemu ochrony cyberprzestrzeni charakteryzującego się:

- dostępem do informacji niezbędnych do poprawnej analizy, oceny sytuacji oraz określenia pożądanego stanu bezpieczeństwa, realizowanych w czasie rzeczywistym lub prawie rzeczywistym,
- możliwościami korelacji zdarzeń zachodzących w różnych miejscach, symultanicznie lub w różnym czasie,
- możliwościami koordynacji realizowanych procesów i procedur reagowania na incydenty komputerowe, na poziomie krajowym oraz w układzie transgranicznym,
- możliwości zamknięcia incydentu, z odpowiednimi procesami, procedurami technikami po incydencie.

Nie przesądzając, jaki model współdziałania ośrodków typu CERT/CSIRT lub SOC (Security Operation Center) jest najodpowiedniejszy - scentralizowany, rozproszony, hierarchiczny, czy sfederalizowany - pożądane jest opracowanie i przygotowanie do wdrożenia jednego lub więcej takich modeli.

W obszarze tematu badawczego mieszczą się systemy wspomagające dla CERT/CSIRT lub SOC. Przykładem takiego systemu może być system bezpiecznej dystrybucji oraz monitorowania czasu.

Ad(ii)

Obszar badawczy obejmuje opracowanie zintegrowanego układu scalonego o podwyższonym poziomie bezpieczeństwa, przeznaczonego do zastosowań w systemach identyfikacji elektronicznej. Procesor aplikacyjny powinien charakteryzować się m.in. podwyższoną odpornością na błędy, opierać swe działanie na „prawdziwym" generatorze liczb losowych, posiadać bezpieczne obszary pamięci nieulotnej, w szczególności wyposażone w mechanizmy wykrywania i reagowania na próby nieautoryzowanego dostępu, jak również bloki wspomagające wykonywanie funkcji kryptograficznych. Procesor powinien spełniać funkcje identyfikacji i uwierzytelniania, realizowalne w czasie rzeczywistym, (np. z wykorzystaniem fizycznie nieklonowalnych funkcji PUF - Physical Unclonable Function)), zapewniać wsparcie dla wbudowanych programów operacyjnych, jak również być wyposażony w odpowiednie peryferia cyfrowe, oraz interfejsy (zgodne z realizowana

[42] Aktualizacja w ramach ujednolicenia terminologii
[43] Aktualizacja w ramach ujednolicenia terminologii

funkcjonalnością) oraz czujniki i układy monitorujące środowiskowe warunki pracy układu scalonego (np. temperatura, napięcie zasilania, częstotliwość sygnału zegarowego).

Wykonany prototyp w technologii krzemowej, zapewniający pełną kontrolę sprzętową uniemożliwiającą zdalne lub lokalne, sprzętowe lub programowe, przejęcie kontroli nad układem elektronicznym (proces rozwoju powinien zapewniać eliminację tzw. *backdoors)*, powinien zostać przygotowany w taki sposób, aby wyprodukowana na jego podstawie produkcyjna wersja układu scalonego mogła przejść pomyślnie certyfikację bezpieczeństwa zgodnie z normą PN-ISO/IEC PN – ISO/IEC 15408 (*Common Criteria)* z poziomem uzasadnienia pewności wyższym niż EAL4.

Metody rozpoznawania i uwierzytelniania biometrycznego wykorzystują specyficzne cechy ludzkie: fizjologiczne (odcisk palca, obraz twarzy, obraz tęczówki, geometria dłoni, obraz naczyń krwionośnych dłoni lub palca i inne) albo behawioralne (głos, rytm klawiatury, rytm chodu etc.). Istniejące rozwiązania biometryczne - stają się powszechnie dostępnymi, „normalnymi" elementami smartfonów, niemniej jednak pracują w układzie lokalnym, uwierzytelniając użytkownika do jego urządzenia.

Mobilne uwierzytelnianie biometryczne stawia przed badaczami wyzwania w postaci konieczności przystosowania czujników, algorytmów, wymagań bezpieczeństwa, architektury systemu, protokołów wielu innych elementów, natomiast zdalne uwierzytelnianie dodatkowo wprowadza istotne elementy zapewniające prywatność danych sensytywnych, które muszą być chronione przed ujawnieniem komukolwiek innemu niż ich posiadacz.

W tym kontekście istotne jest opracowanie i przygotowanie do wdrożenia polskiego układu scalonego zapewniające bezpieczeństwo danych biometrycznych służących do uwierzytelniania oraz metod biometrycznych uwzględniających specyficzne własności urządzeń mobilnych. Agenda badawcza obejmuje analizę możliwości zastosowania różnych technik biometrycznych do uwierzytelniania z wykorzystaniem powszechnie dostępnych urządzeń mobilnych oraz opracowanie nowych, niezawodnych rozwiązań zapewniających zachowanie prywatności danych biometrycznych i umożliwiających dostosowywanie poziomu bezpieczeństwa do aktualnych wymagań. Dla spełnienia wymogów bezpieczeństwa tworzonego rozwiązania badania powinny koncentrować się na najnowszych architekturach i systemach komunikacji spełniających odpowiednie normy. Konieczne jest uwzględnienie możliwości rozbudowy systemu i jego adaptacji do wymagań użytkownika. W wyniku prowadzonych badań powinny powstać przygotowane do wdrożenia komponenty krajowego systemu tożsamości cyfrowej.

Ad (iii)

Temat badawczy obejmuje opracowanie i przygotowanie do wdrożenia zaawansowanych metod, technik, procesów i procedur weryfikacji bezpieczeństwa rozwiązań sprzętowo-programistycznych, które mogą być konieczne do przeprowadzenia oceny bezpieczeństwa, a następnie przeprowadzenia certyfikacji na zgodność z wymaganiami bezpieczeństwa.

Ogólna metodyka przeprowadzenia ocen bezpieczeństwa produktów i usług teleinformatycznych zgodna z normą ISO/IEC 15408 *(Common Criteria)* zakłada, że dla wyższych poziomów uzasadnionej pewności weryfikacji należy opracować testy, które mają cechy charakter penetrującego ataku, tak jakby to wykonał intruz określany zwykle jako atakujący.

W obszarze badań powinny być metody, techniki, procesy i procedury charakterystyczne dla testów różnego typu, w tym:

- powierzchnie ataku na różne warstwy struktur sprzętowo – programistycznych,
- ataki na prezentację biometryczną,
- nieinwazyjne metody zaawansowanego testowania modułów kryptograficznych
- metody i testy weryfikacji losowości generatorów bitów losowych,
- testy fizycznego zabezpieczenia (tzw. *tamper proof*) modułów kryptograficznych,
- ataki na funkcje typu PUF (fizycznie nieklonowalne) w modułach kryptograficznych,
- testy weryfikacji bezpieczeństwa w różnych warstwach modelu sieciowego OSI lub podobnych modeli teleinformatycznych.

Obszar badawczy obejmuje opracowywanie i projektowanie procesów, procedur i testów weryfikacji bezpieczeństwa z uwzględnieniem wymagań bezpieczeństwa dla różnych rozwiązań sprzętowo – programistycznych, w tym przykładowo takich kategorii jak:

- Infrastruktura krytyczna (programowalne sterowniki, VPN, sieci bezprzewodowe),
- Infrastruktura informatyczna (IPSec, moduły kryptograficzne, systemy wykrywania wtargnięć, systemy antywirusowe),
- Energetyka (inteligentne liczniki),
- Administracja publiczna (paszporty, prawa jazdy),
- Zdalna identyfikacja i uwierzytelnienie (podpis elektroniczny, pieczęć elektroniczna, uwierzytelnianie biometryczne),
- Opieka zdrowotna (karty lekarza i pacjenta),
- Systemy transportowe (tachografy),
- Specjalizowane karty dla użytkowników telefonii komórkowej (USIM),

Obszar badawczy obejmuje także projektowanie procesów i procedur oceny bezpieczeństwa i certyfikacji produktów i usług teleinformatycznych, umożliwiających opracowanie i zapewnienie operacyjnej gotowości polskiego schematu oceny i certyfikacji, w oparciu o normę wiodącą PN-ISO/IEC 15408 (*Common Criteria*).

Sposoby interwencji

Program, którego podstawą ustanowienia jest art. 30 ust. 1 pkt 2 ustawy z dnia 30 kwietnia 2010 r. o Narodowym Centrum Badań i Rozwoju (Dz. U. 2022, poz. 2279 tj. z późn. zm.) będzie wdrażany, zgodnie z art. 36 ust. 1 ww. ustawy - wybór wykonawców projektów nastąpi

w drodze konkursu ogłaszanego przez Dyrektora, którego szczegółowy tryb realizacji w zakresie składania wniosków oraz kryteriów oceny zostanie określony w Regulaminie.

Sposób interwencji	Wartość
Odniesienie do zadań NCBR	Realizacja zadań określonych w art. 30 ust 1 pkt 2 ustawy z dn. 30 kwietnia 2010 r. o NCBR
Zakładany budżet NCBR na realizację Programu	**234 027 000** [44] **PLN**
Wnioskodawcy	Konsorcja naukowe w rozumieniu *Ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (Dz. U. z 2016 r., poz. 2045 tj. ze zm.)*[45] *(dalej ustawa o zasadach finansowania nauki)* - grupa jednostek organizacyjnych, w której skład wchodzi co najmniej jedna jednostka naukowa oraz co najmniej jeden przedsiębiorca, albo co najmniej dwie jednostki naukowe.
Rodzaje zadań w ramach projektu	**badania przemysłowe** - zgodnie z definicją zawartą w art. 2 pkt. 3c ustawy o zasadach finansowania nauki – badania mające na celu zdobycie nowej wiedzy oraz umiejętności w celu opracowywania nowych produktów, procesów i usług lub wprowadzania znaczących ulepszeń do istniejących produktów, procesów i usług; badania te obejmują tworzenie elementów składowych systemów złożonych, szczególnie do oceny przydatności technologii rodzajowych, z wyjątkiem prototypów objętych zakresem prac rozwojowych.
	prace rozwojowe - zgodnie z definicją w art. 2 pkt. 4 ustawy o zasadach finansowania nauki – nabywanie, łączenie, kształtowanie i wykorzystywanie dostępnej aktualnie wiedzy i umiejętności z dziedziny nauki, technologii i działalności gospodarczej oraz innej wiedzy i

[44] Na wniosek KS CyberSecIdent, Dyrektor Centrum wyraził zgodę na zwiększenie alokacji budżetu Programu z 212 000 000 PLN do 234 027 000 PLN.

[45] Ustawa o zasadach finansowania nauki, obowiązująca w dniu ogłoszenia Programu została uchylona z dniem 1 października 2018 r. Obecnie obowiązująca ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2023 r., poz. 742 tj.) nie definiuje pojęcia konsorcjum naukowego, a badania naukowe i prace rozwojowe definiuje następująco: *art. 4 ust. 2 Badania naukowe są działalnością obejmującą: 1) badania podstawowe rozumiane jako prace empiryczne lub teoretyczne mające przede wszystkim na celu zdobywanie nowej wiedzy o podstawach zjawisk i obserwowalnych faktów bez nastawienia na bezpośrednie zastosowanie komercyjne; 2) badania aplikacyjne rozumiane jako prace mające na celu zdobycie nowej wiedzy oraz umiejętności, nastawione na opracowywanie nowych produktów, procesów lub usług lub wprowadzanie do nich znaczących ulepszeń.; art. 4 ust. 3 Prace rozwojowe są działalnością obejmującą nabywanie, łączenie, kształtowanie i wykorzystywanie dostępnej aktualnie wiedzy i umiejętności, w tym w zakresie narzędzi informatycznych lub oprogramowania, do planowania produkcji oraz projektowania i tworzenia zmienionych, ulepszonych lub nowych produktów, procesów lub usług, z wyłączeniem działalności obejmującej rutynowe i okresowe zmiany wprowadzane do nich, nawet jeżeli takie zmiany mają charakter ulepszeń.*

Sposób interwencji	Wartość
	umiejętności do planowania produkcji oraz tworzenia i projektowania nowych, zmienionych lub ulepszonych produktów, procesów i usług.
	Przygotowanie wyników badań i prac rozwojowych do zastosowania w praktyce, obejmujące w szczególności: – sporządzenie dokumentacji niezbędnej do wdrożenia produktu, – opracowanie procedur związanych z wykorzystywaniem przyszłego produktu będącego wynikiem badań naukowych lub prac rozwojowych, – uzyskanie certyfikatu zgodności upoważniającego do oznaczenia wyrobu znakiem zgodności z normą krajową lub ponadnarodową, – certyfikację w rozumieniu ustawy z dnia 30 sierpnia 2002 r. *o systemie oceny zgodności* (Dz. U. z 2023 r., poz. 215t.j., z późn. zm.), – działania bezpośrednio związane z postępowaniami dotyczącymi przyznania praw własności przemysłowej
Instrumenty i intensywność wsparcia	**Jednostki naukowe** - dofinansowanie badań przemysłowych, prac rozwojowych - do 100% kosztów kwalifikowanych, dofinansowanie prac przygotowawczych do wdrożenia - do 90% kosztów kwalifikowanych
	Przedsiębiorcy - pomoc publiczna na badania przemysłowe, prace rozwojowe oraz prace przygotowawcze do wdrożenia, zgodnie z rozporządzeniem w sprawie warunków i trybu udzielania pomocy publicznej za pośrednictwem NCBR[46] <u>na badania przemysłowe:</u> małe/ mikroprzedsiębiorstwa - maks. 80%, średnie przedsiębiorstwa - maks. 75% duże przedsiębiorstwa - maks. 65% <u>na prace rozwojowe:</u> małe/ mikroprzedsiębiorstwa - maks. 60%, średnie przedsiębiorstwa - maks. 50% duże przedsiębiorstwa - maks. 40% <u>na prace przygotowawcze do wdrożenia:</u> maks. 90% kosztów kwalifikowalnych (pod warunkiem nieprzekroczenia pomocy *de minimis*)

Sposób monitorowania i oceny stopnia osiągania celu

[46] zastąpione rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 19 sierpnia 2020 r. w sprawie udzielania pomocy publicznej za pośrednictwem Narodowego Centrum Badań i Rozwoju (Dz. U. poz. 1456, ze zm.)

głównego i celów szczegółowych programu

Informacje wstępne

Ocena, na ile cel główny i cele szczegółowe Programu CyberSecIdent „Cyberbezpieczeństwo i eTożsamość" zostały zrealizowane, jest dokonywana poprzez mierzenie szeregu wskaźników. Część z nich służy monitorowaniu realizacji Programu i mierzeniu postępu względem celów (przede wszystkim są to tzw. wskaźniki produktu). Inne służą weryfikacji tego, czy cele realizacji Programu zostały osiągnięte i czy zakończył się on sukcesem.

Zarówno cele, jak i służące mierzeniu ich realizacji wskaźniki, powinny spełniać kryteria SMART, to znaczy powinny być *konkretne*, *mierzalne*, *dostępne*, *realistyczne* i *określone w czasie*. Dobre wskaźniki spełniają kryteria **RACER** (z ang. Relevant, Accepted, Credible, Easy and Robust), to znaczy, że są: *odpowiednie*, tj. ściśle powiązane z wyznaczonymi celami, *akceptowane*, np. przez zainteresowane strony, *wiarygodne* dla laików, a więc jednoznaczne i łatwe w interpretacji, *dające* się w prosty sposób monitorować, *miarodajne* i odporne na manipulację.

Wskaźniki produktu[47]

Wskaźniki produktu opisują rozwiązania i produkty powstałe w toku realizacji Programu i są podstawowymi wskaźnikami monitorowania jego realizacji. Dlatego też ich pomiar odbywa się w okresie realizacji Programu i nie powinien wykraczać poza przyjęty termin jego zakończenia. Wskaźniki produktu będą mierzone w trakcie i po zakończeniu realizacji projektów finansowanych w ramach Programu, na podstawie raportów okresowych oraz raportów końcowych dostarczonych przez Wykonawców. Wykonawca będzie zobowiązany do dostarczenia raportów z zapisami umowy o dofinansowanie danego projektu.

Wskaźniki produktu			
Źródło: Wskaźniki produktu są raportowane przez Wykonawców Czas pomiaru: w trakcie realizacji projektów w raportach okresowych oraz po ich zakończeniu w raportach końcowych.			
L.p.	Opis	Wartość bazowa	Wartość docelowa
1.	Liczba produktów opracowanych podczas realizacji Programu, gotowych do wdrożenia lub certyfikacji bezpieczeństwa, zgodnie z Dyrektywą NIS w tym:	0	20
1a	nowych	0	10
1b	Znacząco ulepszonych	0	10
2.	Liczba prototypów nowych produktów przeznaczonych do zastosowań w systemach identyfikacji elektronicznej	0	8

[47] Wskaźniki we wszystkich tabelach (produktu, rezultatu bezpośredniego i długoterminowego) zaktualizowane adekwatnie do zmian planu finansowego oraz zakresu tematycznego III konkursu

Wskaźniki produktu			
Źródło: Wskaźniki produktu są raportowane przez Wykonawców Czas pomiaru: w trakcie realizacji projektów w raportach okresowych oraz po ich zakończeniu w raportach końcowych.			
L.p.	Opis	Wartość bazowa	Wartość docelowa
3.	Liczba opracowanych metod monitorowania bezpieczeństwa teleinformatycznego, pozwalających na identyfikację zagrożeń w czasie rzeczywistym.	0	15
4.	Liczba opracowanych technik obrony przed atakami sieciowymi	0	16
5.	Liczba opracowanych i przygotowanych do wdrożenia zaawansowanych metod, technik, procesów i procedur weryfikacji bezpieczeństwa rozwiązań sprzętowych, programistycznych lub sprzętowo-programistycznych	0	10

Wskaźniki rezultatów bezpośrednich i długoterminowych

Wskaźniki rezultatu bezpośredniego mierzą bezpośrednie efekty działań podjętych w ramach Programu, które są odczuwalne także po ich zakończeniu. Opisują zmiany, jakie zajdą w wyniku wdrażania efektów Programu. Wskaźniki rezultatu powinny być logicznie powiązane ze szczegółowymi celami Programu. Wskaźniki rezultatu będą mierzone po zakończeniu Programu, a przed upływem 3 lat, częściowo na podstawie informacji dostarczonych przez Wykonawców. Wykonawca będzie zobowiązany do dostarczenia informacji z zapisami umowy o dofinansowanie danego projektu.

1. Wdrożenie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości
2. Wdrożenie metod i technik identyfikacji i uwierzytelniania.

Wskaźniki rezultatu bezpośredniego			
Źródło: Informacje dostarczone przez Wykonawców Czas pomiaru: Przed upływem 3 lat od zakończenia projektów.			
L.p.	Opis	Wartość bazowa	Wartość docelowa
1) *Wdrożenie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości*			
1	Liczba wdrożonych produkcyjnie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa	0	20
2	Liczba wdrożeń komponentów mających zastosowanie w systemach teleinformatycznych związanych z cyfrową tożsamością	0	6

Wskaźniki rezultatu bezpośredniego			
Źródło: Informacje dostarczone przez Wykonawców Czas pomiaru: Przed upływem 3 lat od zakończenia projektów.			
L.p.	Opis	Wartość bazowa	Wartość docelowa
3	Przychód beneficjentów z wdrożonych rozwiązań technologicznych w zakresie koordynacji działań między domenami cyberbezpieczeństwa	0	90 396 181,00[48]
4	Udział rozwiązań opracowanych w ramach Programu, w zakresie koordynacji działań między domenami cyberbezpieczeństwa generujących przychody w stosunku do liczby wdrożonych rozwiązań	0	50%
2) *Wdrożenie metod i technik identyfikacji i uwierzytelniania*.			
1	Liczba wdrożonych metod i technik identyfikacji i uwierzytelniania	0	6
2	Przychód beneficjentów z wdrożonych metod i technik identyfikacji i uwierzytelniania	0	0[49]
3	Udział rozwiązań opracowanych w ramach Programu w zakresie metod i technik identyfikacji i uwierzytelniania generujących przychody w stosunku do liczby wdrożonych rozwiązań	0	50%
4	Liczba dokonanych zgłoszeń patentowych złożonych w wyniku realizacji Programu	0	4

Wskaźniki rezultatu długoterminowego (wpływu) mierzą efekty Programu w dłuższej perspektywie czasu i pokazują trwałe zmiany, jakie Program spowodował w otoczeniu społecznym i gospodarczym. Tym samym, wskaźniki wpływu można uważać za miernik stopnia realizacji celu głównego Programu: *Podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP przez zwiększenie dostępności narzędzi sprzętowo–programistycznych, do roku 2028*.

Pomiar dokonywany jest na zakończenie okresu trwałości, tj. w 2028 roku, w ramach ewaluacji ex-post.

Wskaźniki rezultatu długoterminowego (wpływu)			
Źródło: Informacje dostarczone przez Wykonawców, ewaluacja ex-post. Czas pomiaru: Po 3 latach od zakończenia Programu.			
L.p.	Opis	Wartość bazowa	Wartość docelowa

[48] Wartość docelową wskaźnika podano na podstawie informacji przedstawionych przez Beneficjentów w raportach okresowych/końcowych/z wdrożenia.

[49] Wartość docelową wskaźnika podano na podstawie informacji przedstawionych przez Beneficjentów w raportach okresowych/końcowych/z wdrożenia.

1.	Liczba wprowadzonych do użytku egzemplarzy produktów, powstałych w wyniku wdrożenia rezultatów Programu.	0	250 000
2.	Liczba sprzedanych usług, powstałych w wyniku wdrożenia rezultatów Programu.	0	30
3.	Liczba certyfikatów bezpieczeństwa produktów lub usług, wydanych z wykorzystaniem metodyk opracowanych w Programie.	0	6

Ryzyka dla osiągnięcia celu głównego i celów szczegółowych Programu oraz ryzyk związanych z zarządzaniem i realizacją Programu

Ryzyka obiektywne:

- specyfika badań i rozwoju ze swej natury obarczone wysokim ryzykiem polegającym na niemożności przewidzenia wyników badań naukowych,

Ryzyka subiektywne:

- tempo zmian technologicznych w obszarze objętym programem - ryzyko, iż rozwiązania opracowywane w ramach projektów mogą okazać się mało konkurencyjne;
- pojawiające się nowe zagrożenia – ryzyko, iż rozwiązania opracowywane w ramach projektów mogą okazać się nieskuteczne;

Dla minimalizacji ww. ryzyk przewiduje się następujące działania:

- zapewnienie właściwego monitorowania realizacji i osiągania celów programu na poziomie poszczególnych projektów – zobowiązanie Beneficjenta w umowie do okresowego raportowania o postępie w realizacji projektu oraz jego wynikach, w przypadku oceny negatywnej możliwość wstrzymania realizacji projektu oraz rozwiązania umowy, uprawnienie do wystąpienia o zwrot środków wykorzystanych nieprawidłowo;
- identyfikacja zmian zachodzących w otoczeniu programu w kontekście jego celów;
- możliwość wprowadzania zmian w projektach i w programie jako reakcja na rozwój technologii oraz nowe zagrożenia.

Harmonogram realizacji Programu

Szczegółowy harmonogram realizacji Programu jest przygotowywany przez Koordynatora **Programu** i opiniowany przez **Komitet Sterujący** z uwzględnieniem budżetu Centrum na rok bieżący oraz kolejne lata realizacji Programu.

Mając na względzie powyższe, ramowy harmonogram realizacji Programu, w odniesieniu do dnia zaopiniowania projektu Programu przez Radę NCBR przedstawiono poniżej.

Ramowy harmonogram realizacji Programu

Termin	**Działanie**
21.12.2016	Zaopiniowanie Programu przez Radę NCBR, ustanowienie Programu
19.01.2017	Powołanie Koordynatora Programu I Komitetu Sterującego
21.02.2017	Przygotowanie harmonogramu realizacji Programu przez Koordynatora Programu i zaopiniowanie przez Komitet Sterujący
I konkurs	
13.03.2017 31.03.2017	Ustalenie zakresu tematycznego konkursów i określenie alokacji środków przez Komitet Sterujący, Ogłoszenie I konkursu
11.04.2017 – 05.06.2017	Przeprowadzenie i rozstrzygnięcie konkursu
05.06.2017 – 28.06.2017	Analiza wyników I konkursu – wnioski do dalszego wdrażania programu
04.07.2017 – 31.05.2025	Finansowanie i nadzór nad realizacją projektów z I konkursu
II konkurs	
28.06.2017 17.07.2017	Ustalenie zakresu tematycznego konkursów i określenie alokacji środków przez Komitet Sterujący Ogłoszenie II konkursu
01.08.2017 – 07.12.2017	Przeprowadzenie i rozstrzygnięcie konkursu
07.12.2017 – 04.06.2018	Analiza wyników II konkursu – wnioski do dalszego wdrażania programu
09.04.2018 – 31.09.2022	Finansowanie i nadzór nad realizacją projektów z II konkursu
III konkurs	
21.11.2018 19.07. 2019	Ustalenie zakresu tematycznego konkursów i określenie alokacji środków przez Komitet Sterujący Ogłoszenie III konkursu
23.08. 2019 – 15.01.2020	Przeprowadzenie i rozstrzygnięcie konkursu
I kw 2020	Analiza wyników III konkursu – wnioski do dalszego wdrażania programu

II, III, IV kw. 2020 – IV kw. 2024	Finansowanie i nadzór nad realizacją projektów z III konkursu
IV konkurs	
I kw. 2020 II kw. 2020	Ustalenie zakresu tematycznego konkursów i określenie alokacji środków przez Komitet Sterujący Ogłoszenie IV konkursu
II-IV kw. 2020	Przeprowadzenie i rozstrzygnięcie konkursu,
IV kw. 2020 – I kw. 2021	Analiza wyników IV konkursu – wnioski do dalszego wdrażania programu
II kw. 2021 – I kw. 2025	Finansowanie i nadzór nad realizacją projektów z IV konkursu
2017-2030	Monitoring i ewaluacja programu

Plan finansowy Programu, w tym źródła finansowania

Projekty w ramach Program będą finansowane z dotacji celowej na realizację strategicznych programów badań naukowych i prac rozwojowych, innych zadań Centrum oraz na realizację badań naukowych i prac rozwojowych na rzecz obronności i bezpieczeństwa państwa, o której mowa w art. 46 ust. 1 pkt 1 Ustawy o NCBR, środków prywatnych (środki przedsiębiorców) oraz – potencjalnie - środków innych instytucji działających w obszarach Programu.

Koszty zarządzania Programem tj. w szczególności wynagrodzenia pracowników NCBR zaangażowanych we wdrażanie Programu, koszty oceny wniosków o dofinansowanie wykonywanych przez niezależnych ekspertów, koszty związane z działalnością Komitetu Sterującego, koszty związane z kontrolą projektów oraz ewaluacją programu **będą pochodziły z dotacji podmiotowej** na pokrycie bieżących kosztów zarządzania realizowanymi przez Centrum zadaniami, o której mowa w Art. 46 ust. 1 pkt 2 Ustawy o NCBR.

Środki NCBR przeznaczone **na realizację projektów to 234 027 000 [50] PLN**. Zakłada się również, że dodatkowe **koszty zarządzania Programem nie przekroczą 3% budżetu** NCBR przeznaczonego na finansowanie projektów w ramach Programu.

Szczegółowy system realizacji i zarządzania Programem

[50] Na wniosek KS CyberSecIdent, Dyrektor Centrum wyraził zgodę na zwiększenie alokacji budżetu Programu z 212 000 000 PLN do 234 027 000 PLN.

Nadzór nad realizacją Programu sprawuje Dyrektor NCBR lub osoba przez niego upoważniona. Prace związane z wdrażaniem Programu realizuje wskazany przez Dyrektora Dział NCBR.

Realizacja Programu obejmuje m.in. wybór i finansowanie projektów obejmujących badania naukowe, prace rozwojowe oraz działania związane z przygotowaniem wyników badań i prac rozwojowych do zastosowania w praktyce. Wykonawcy projektów są wybierani w drodze konkursu ogłaszanego przez Dyrektora zgodnie z art. 36 ust. 1 Ustawy o Narodowym Centrum Badań i Rozwoju. Procesy wyboru projektów, nadzoru nad ich wykonaniem i finansowaniem oraz monitoringu programu będą prowadzone w oparciu o procedury obowiązujące w NCBR.

Kluczowe znaczenie dla zarządzania realizacją programu ma **Komitet Sterujący** i **Koordynator Programu**. Zakłada się, że powołany przez Dyrektora Centrum Komitet Sterujący będzie składał się z 5 osób: 2 przedstawicieli Ministerstwa Cyfryzacji, 2 osób wskazanych przez Dyrektora NCBR oraz 1 osoby wskazanej przez Radę NCBR.

Do zadań **Komitetu Sterującego** należy w szczególności:

- uszczegółowienie zakresu tematycznego programu;
- określenie zakresów tematycznych konkursów;
- określenie adekwatnych do zakresów tematycznych konkursów warunków realizacji projektów (w tym ewentualnych maksymalnych kwot dofinansowania projektów), udziału środków pozabudżetowych;
- opiniowanie harmonogramu realizacji konkursów;
- monitorowanie realizacji Programu, mając w szczególności na uwadze osiągnięcie jego celów;
- identyfikacja zmian zachodzących w otoczeniu programu oraz proponowanie zmian w programie / projektach w szczególności w kontekście celów programu.

Zakres zadań oraz tryb ich realizacji zostanie w sposób szczegółowy określony w Regulaminie pracy Komitetu Sterującego.

Do zadań **Koordynatora Programu** należy w szczególności:

- przygotowanie projektu harmonogramu realizacji konkursów;
- przygotowanie projektów wszelkich dokumentów opiniowanych przez Komitet Sterujący Programu i zatwierdzanych przez Dyrektora Centrum, w tym dokumentacji konkursowej;

- koordynacja działań związanych z realizacją konkursów na projekty – wyborem wykonawców projektów oraz procesem podpisywania umów o wykonanie i finansowanie projektów;
- monitorowanie realizacji Programu

Koordynator Programu będzie wspierany w swoich działaniach przez pracowników Działu wdrażającego Program. Bieżący bezpośredni nadzór nad realizacją zadań Koordynatora będzie spoczywał na osobach kierujących komórką organizacyjną odpowiedzialną za realizację programu. Inne Działy NCBR będą udzielały wsparcia w zakresie swoich kompetencji określonych w Regulaminie Organizacyjnym oraz wewnętrznych procedurach NCBR.

W trakcie realizacji Programu będzie prowadzona jego ewaluacja w szczególności w celu rozstrzygnięcia, czy kontynuacja programu prowadzi do osiągnięcia celów Programu.

Po zakończeniu realizacji Programu, przeprowadzona będzie ewaluacja mająca na celu w szczególności ocenę stopnia osiągnięcia jego celów, a w przypadku nieosiągnięcia celów Programu określenie przyczyn niepowodzenia.

Proces ewaluacji będzie realizowany zgodnie z obowiązująca w NCBR ***Procedurą dotyczącą ewaluacji programu***.