PARP
Grupa PFR

Mapa rozwoju rynku i technologii dla obszaru cyberbezpieczeństwa

Niniejsze opracowanie jest współfinansowane z Europejskiego Funduszu Rozwoju Regionalnego ze środków Programu Operacyjnego Inteligentny Rozwój 2014-2020.

Zamawiający

Polska Agencja Rozwoju Przedsiębiorczości

Wykonawca

PwC Advisory spółka z ograniczoną odpowiedzialnością sp.k.

Autorzy

Rozdziały 2.6 i 3.8 – adwokat, rzecznik patentowy Klaudia Błach-Morysińska
Pozostałe rozdziały – dr hab. inż. Jerzy Baranowski oraz Zespół Innowacji PwC Polska

Współpraca merytoryczna PARP

Dorota Frączek
Wojciech Sadowiec
Aleksandra Walczyk-Jansson

Niniejsze opracowanie jest rezultatem tzw. Procesu Przedsiębiorczego Odkrywania (PPO), prowadzonego przez Ministerstwo Rozwoju i Technologii w partnerstwie z Polską Agencją Rozwoju Przedsiębiorczości, w ramach projektu pozakonkursowego pn. *Monitoring Krajowej Inteligentnej Specjalizacji*.

Celem projektu pozakonkursowego jest monitorowanie i aktualizacja obszarów B+R+I priorytetowych dla rozwoju polskiej gospodarki, tzw. Krajowych Inteligentnych Specjalizacji (KIS). Lista tych obszarów ma charakter otwarty i jest aktualizowana stosownie do zachodzących zmian społeczno-gospodarczych.

Streszczenie

Niniejsze opracowanie stanowi ekspertyzę Business Technology Roadmap (BTR), tj. w przyjętym tłumaczeniu na język polski Mapę rozwoju rynku i technologii, podsumowującą cykl spotkań warsztatowych Smart Lab (SL) z udziałem przedstawicieli przedsiębiorstw, instytucji otoczenia biznesu oraz środowisk naukowych funkcjonujących w obszarze cyberbezpieczeństwa w Polsce. Celem ekspertyzy BTR jest określenie nisz technologicznych w interdyscyplinarnym obszarze cyberbezpieczeństwa, które stanowić mogą polskie specjalizacje i przewagi konkurencyjne względem podmiotów funkcjonujących na rynku globalnym. Wnioski płynące ze spotkań warsztatowych zostały pogłębione o wyniki własnych analiz autorów ekspertyzy, co pozwoliło na dokładniejsze oszacowanie potencjału oraz wyzwań dla tego obszaru.

Ekspertyza została sporządzona w ramach projektu pozakonkursowego Monitoring Krajowej Inteligentnej Specjalizacji. Projekt ten realizowany jest wspólnie przez Ministerstwo Rozwoju i Technologii oraz Polską Agencję Rozwoju Przedsiębiorczości.

Niniejszy dokument powstawał pomiędzy lipcem 2021 r. a styczniem 2022 r. W tym czasie przeprowadzono prace przygotowawcze oraz zorganizowano cztery spotkania warsztatowe Smart Lab - zgodnie z metodologią Procesu Przedsiębiorczego Odkrywania. W ramach prac przygotowawczych oraz realizowanych spotkań przeprowadzono szereg analiz, m.in. raportów rynkowych i publikacji powiązanych z tematem SL, materiałów z konferencji i wydarzeń targowych skupionych wokół analizowanego obszaru, a także posiłkowano się wiedzą ekspercką przedstawicieli podmiotów funkcjonujących w ramach obszaru cyberbezpieczeństwa. W trakcie spotkań SL jego uczestnicy dzielili się swoją wiedzą z zespołem ekspertów przy wykorzystaniu różnorodnych technik moderacji dyskusji i pracy, zarówno grupowej, jak i indywidualnej, m.in. z użyciem narzędzi Design Thinking oraz rozwiązań informatycznych dedykowanych współpracy w środowisku online. Kluczowe wnioski płynące z rezultatów wypracowanych przez uczestników spotkań SL zostały poddane krytycznej ocenie i agregacji przez zespół ekspertów PwC pod kierownictwem konsultanta-eksperta branżowego dr hab. inż. Jerzego Baranowskiego.

Efekty tych działań znalazły swoje odzwierciedlenie na kartach sporządzonej ekspertyzy BTR. W dokumencie można wyodrębnić trzy główne sekcje tematyczne. Sekcja pierwsza i druga zawiera wieloaspektową analizę obszaru cyberbezpieczeństwa, odpowiednio w kontekście globalnym i krajowym. Sekcja trzecia obejmuje swym zakresem opis scenariuszy rozwoju ww. obszaru i mapę BTR.

Pojęcie „cyberbezpieczeństwo”, stanowiące nazwę obszaru, wokół którego skupia się niniejsza ekspertyza, obejmuje interdyscyplinarny obszar technologiczny, w którym nie sposób prosto określić branże klienckie, na które technologie te oddziałują. Digitalizacja i popularyzacja Internetu spowodowała, że cyberbezpieczeństwo przenika przez niemalże wszystkie sektory gospodarki, a potencjał dywersyfikacji i zastosowania technologii z tego obszaru jest praktycznie nieograniczony. Mimo tego, że termin cyberbezpieczeństwo pojawił się w nomenklaturze branży

IT na przełomie lat 70 i 80 XX w., to akcelerację rozwoju tego obszaru i świadomości bezpieczeństwa IT przyniosły dopiero lata 90 XX w., kiedy to wraz z popularyzacją Internetu wśród indywidualnych użytkowników i pierwszych interakcji firma – klient czy firma – firma, pojawili się cyberprzestępcy (tzw. „hakerzy"), a cyberbezpieczeństwo stało się nie tylko profilaktyką, ale przede wszystkim odpowiedzią na coraz zuchwalsze cyberataki. Od tamtych czasów rynek cyberbezpieczeństwa zarówno na świecie, jak i z czasem również w Polsce, dynamicznie się rozwijał, a jego strategiczny charakter (w rozumieniu wpływu na bezpieczeństwo społeczne i gospodarcze) jest jednym z kluczowych motorów napędowych pozwalających utrzymywać ten pozytywny trend, mimo występujących cyklicznie kryzysów czy recesji gospodarczej.

W perspektywie długoterminowej cyberbezpieczeństwo pozostanie obszarem o strategicznym znaczeniu tak długo, jak technologicznym fundamentem funkcjonowania krajowej gospodarki i życia codziennego nadal będą technologie komputerowe oraz Internet. W perspektywie krótkoterminowej można wymienić szereg czynników, które wspierają rozwój tego rynku – wśród trendów horyzontalnych jest to przede wszystkim postępująca digitalizacja procesów biznesowych oraz interakcji z klientami, w tym wirtualizacja samej oferty produktowej i usługowej. Nie mniejsze znaczenie mają również trendy dotyczące samych branż – jak digitalizacja przemysłu (zgodnie z założeniami Przemysłu 4.0) czy administracji publicznej (w tym infrastruktura krytyczna, wymagająca szczególnych zabezpieczeń) oraz konkretnych technologii – jak Internet Rzeczy czy uwierzytelnianie wieloskładnikowe.

Krajowy rynek cyberbezpieczeństwa to jeden z najbardziej perspektywicznych sektorów całej branży IT – funkcjonuje na nim wiele innowacyjnych podmiotów, w tym zarówno korporacji o zagranicznym kapitale, jak i polskich przedstawicieli sektora MŚP. Na rozwój rynku równie mocno pracują również startupy, które swoimi unikalnymi technologiami rywalizują na krajowym i zagranicznym rynku. Polski obszar cyberbezpieczeństwa ogranicza jednak kilka ważnych barier, których mitygacja będzie miała fundamentalny wpływ na dynamikę jego dalszego rozwoju – wśród najważniejszych należy wymienić niski poziom świadomości rynku i społeczeństwa nt. zagrożeń czyhających w Internecie, mały udział sektora MŚP wśród klientów zainteresowanych rozwiązaniami z obszaru cyberbezpieczeństwa, braki kadrowe oraz relatywnie niski poziom sieciowości rynku i transferu wiedzy pomiędzy kluczowymi animatorami.

Po przeprowadzeniu spotkań warsztatowych w ramach SL i sporządzeniu dodatkowych analiz, wyselekcjonowano cztery scenariusze rozwoju dla obszaru cyberbezpieczeństwa. Stanowią one zagregowane rodziny potencjalnych projektów badawczo-rozwojowych i innowacyjnych, które mogą być realizowane w Polsce. Wyselekcjonowane scenariusze rozwoju obszaru cyberbezpieczeństwa przedstawiają się następująco:

- **Cyberbezpieczeństwo jako usługa (z ang. „Cybersecurity-as-a-Service")** – scenariusz skupiony wokół sektora usług z obszaru cyberbezpieczeństwa, z działaniami dotyczącymi m.in. wykrywania zagrożeń oraz usług osobistego uwierzytelniania.
- **Kryptografia, uwierzytelnianie i ochrona tożsamości** – scenariusz obejmujący nowoczesne rozwiązania z obszaru weryfikacji użytkowników i dodatkowych form ochrony danych

dostępowych. Planowane projekty zakładają m.in. pracę nad systemami odpornymi na technologie obliczeń kwantowych czy rozwój aplikacji do kontroli dostępu.

- **Cyberbezpieczeństwo instalacji procesowych** – scenariusz grupujący obszary technologiczne dotyczące instalacji procesowych, w tym powiązanych z Przemysłem 4.0 czy infrastrukturą krytyczną. Wśród planowanych projektów należy wymienić m.in. rozwój innowacyjnych technologii bezpieczeństwa procesów czy prace nad oprogramowaniem i narzędziami do obsługi i zarządzania systemami OT.
- **Cyberbezpieczeństwo dla sieci i IoT** – scenariusz skupiony na rozwiązaniach sieciowych i wykorzystujących technologie Internetu Rzeczy. Wśród projektów założono m.in. prace nad wydajnymi algorytmami szyfrowania oraz nowymi protokołami komunikacji urządzeń IoT.

Wypracowane scenariusze zakładają realizację 838 projektów w okresie najbliższych 7 lat, których budżety opiewają łącznie na kwotę 1 596 mln PLN.

Mając na uwadze zakres merytoryczny samego obszaru cyberbezpieczeństwa, jak również zakres projektów planowanych do realizacji w ramach poszczególnych scenariuszy, analizie poddano również obszary technologiczne wyszczególnione w ramach Krajowych i Regionalnych Inteligentnych Specjalizacji. Zarekomendowano szereg zmian, jednak wnioski z warsztatów Smart Lab oraz wiedza o charakterystyce rynku pozwoliła ustalić, że co do zasady wszelkie uruchamiane instrumenty pomocowe dedykowane obszarowi cyberbezpieczeństwa powinny być realizowane na poziomie krajowym i z tego powodu proponowane zmiany dotyczą wyłącznie Krajowych Inteligentnych Specjalizacji. Rekomendacje te dotyczą zarówno rozszerzenia obecnych działań o konkretne sformułowania i terminy, jak i utworzenia nowych działań rozszerzających obecne obszary technologiczne KIS.

Rekomendacje co do Krajowych Inteligentnych Specjalizacji nie są jednak jedynymi zaleceniami przedstawionymi w niniejszym dokumencie – w rozdziale pt. „Wnioski i rekomendacje" skupiono się również na innych aspektach funkcjonowania polskiego rynku cyberbezpieczeństwa, proponując zmiany, których implementacja miałaby ograniczyć negatywny wpływ barier rozwojowych. Wśród nich wymienić można zmiany o charakterze zarówno finansowym (m.in. wsparcie finansowania projektów badawczo-rozwojowych czy procesów komercjalizacyjnych), jak i niefinansowym (m.in. w zakresie wdrażania dobrych praktyk i efektywnych modeli transferu wiedzy i technologii).

Najważniejszym wnioskiem z przeprowadzonych analiz, warsztatów Smart Lab oraz dyskusji ekspertów podczas przygotowywania niniejszej ekspertyzy, pozostaje niezmiennie fakt, że polski rynek cyberbezpieczeństwa ma niezwykły potencjał rozwojowy i jego wsparcie może doprowadzić do realnych sukcesów gospodarczych na arenie międzynarodowej.

Summary

This document constitutes the Business Technology Roadmap (BTR) expertise, summarizing a series of workshop meetings with the representatives of enterprises, business environment institutions and scientific organization operating in the field of cybersecurity in Poland. The aim of BTR expertise is to define technological niches concerned with the cybersecurity, which may constitute Polish specialization and competitive advantages over entities operating globally. The conclusions from the workshop meetings were subjected to the in-depth analysis of experts, allowing for even more accurate estimation of potential and challenges of the cybersecurity area.

The expertise has been developed under the non-competitive project Monitoring of the National Smart Specialization, implemented by the Ministry of Development and Technology and Polish Agency for Enterprise Development.

This document has been developed between July 2021 and January 2022. During that time, preparatory work took place and four Smart Lab (SL) workshop meetings were held with nearly 50 participants, in accordance with the methodology of the “Entrepreneurial Discovery Process”, the essence of which is its’ strong business focus. This document has been prepared between August 2021 and January 2022. During this time, preparatory work has been carried out and four Smart Lab workshop meetings were held in accordance with the methodology of the Entrepreneurial Discovery Process. Within the preparatory work and meetings, various analyzes have been conducted, including the analysis of market reports and publications related to the Smart Lab topic, materials from conferences and events focused around the analyzed area, as well as the expert knowledge of representatives of entities and institutions operating within a given area has been utilized. During Smart Lab meetings, participants shared their knowledge with a team of experts using various techniques of moderating discussions and work (both – in groups and individually), including the use of Design Thinking tools and IT solutions dedicated to cooperation in the online environment. The key conclusions developed by the SL participants have been subject to a critical assessment and aggregation by an interdisciplinary team of PwC experts under the leadership of Jerzy Baranowski, DSc, PhD, Eng.

The expertise can be divided into 3 main sections: first and second contain a multi-faceted analysis of the cybersecurity area, in the global and national context, respectively. The third section covers the description of development scenarios for the above-mentioned area and BTR graphic map.

The term "cybersecurity" encompasses an extremely interdisciplinary technological area, in which it is impossible to simply define the client industries or areas affected by its products and services. Digitalization and popularization of the Internet has caused cybersecurity to permeate almost all sectors of the economy, and the potential for diversification and application of technologies from this area is practically unlimited. Although the term cybersecurity appeared in the nomenclature of the IT industry only at the turn of the 1970s and 1980s, it was not until the 1990s that the development of this area and awareness of IT security accelerated, when, with the popularization of the Internet among individual users and the first B2C and B2B interactions, cybercriminals

(so-called "hackers") emerged and cybersecurity became not only matter of prevention, but above all a response to increasingly daring hacking attacks. Since then, the cybersecurity market, both globally and over time in Poland as well, has developed dynamically, and its strategic nature (in terms of its impact on social and economic security) is still one of the key driving forces allowing this positive trend to continue despite cyclical crises and economic recessions.

In the long term, cybersecurity will remain an area of strategic importance as long as computers and internet connection remain the technological foundation of our economy and everyday life. In the short term, a number of factors can be mentioned that support the development of this market. Among the horizontal trends is the progressive digitalization of business processes and customer interactions, including the virtualization of the product and service offering itself. Of equal importance are also trends concerning the industries themselves, such as industry digitization (in line with the assumptions of Industry 4.0) or digitalization of public administration (including critical infrastructure, requiring special security measures), as well as specific technologies – such as the Internet of Things (IoT).

The domestic cybersecurity market is one of the most promising sectors of the entire IT industry – there are many innovative entities operating in it, including both corporations with foreign capital and Polish representatives of the SME sector. Startups are also working hard to develop the market, with their unique technologies competing on both domestic and foreign markets. The Polish market is, however, limited by several important barriers, the addressing of which will have a fundamental impact on the dynamics of its further development. Among the most important is the low level of awareness about the threats lurking on the Internet, a small share of the SME sector among customers for cyber security solutions, rising staff shortages and a relatively low networking among key market animators.

After conducting workshop meetings and preparing additional analyses, four Development Scenarios for the area of cybersecurity were selected:

- **Cybersecurity-as-a-Service** – a scenario focused on the service sector in the area of cybersecurity, with activities including threat detection and personal authentication services.
- **Cryptography, authentication and identity protection** – a scenario involving modern solutions in the area of user verification and additional forms of access data protection. Planned projects include work on systems resistant to quantum computing technologies or development of access control applications.
- **Cybersecurity of process installations** – a scenario grouping technological areas concerning process installations, including those related to Industry 4.0 or Critical Infrastructure. Planned projects include the development of innovative process security technologies/ software and tools to operate and manage OT systems.

- **Cybersecurity for networks and IoT** – a scenario focused on network solutions and technologies that use Internet of Things (IoT). The projects include work on efficient encryption algorithms and new communication protocols for IoT devices.

The developed scenarios assume the implementation of 838 projects over the next 7 years, with budgets totaling nearly PLN 1.59 billion.

Considering the substantive scope of the area of cybersecurity, as well as the scope of projects planned for implementation under different scenarios, the analysis also covered technological areas listed in the National (KIS) and Regional Smart Specializations (RIS). A number of changes were recommended, but the conclusions of the Smart Lab workshops and knowledge about the characteristics of the market made it possible to determine that, in principle, any launched assistance instruments dedicated to the area of cybersecurity should be implemented at the national level, and for this reason the changes apply only to National Smart Specializations (KIS). The recommendations concern both the extension of current actions mentioned in KIS with specific phrases and the creation of new actions extending the current KIS technological areas.

However, the recommendations concerning National Smart Specializations (KIS) are not the only ones presented in this document. Chapter 8 "Conclusions and recommendations" focuses also on other aspects of the Polish cybersecurity market, proposing changes the implementation of which would address key barriers to its development. These include both financial (e.g. support for financing of R&D projects or commercialization processes) and non-financial (e.g. implementation of good practices and effective models of knowledge and technology transfer) dimensions.

The most important conclusion from the conducted analyses, Smart Lab workshops and expert discussions, remains the fact that the Polish cybersecurity market has an extraordinary development potential and its support can lead to real economic success on the international market.

Spis treści

1. Cel i zakres BTR

Niniejsza ekspertyza Business Technology Roadmap (BTR) podsumowuje cykl spotkań Smart Lab z udziałem przedstawicieli przedsiębiorstw, instytucji otoczenia biznesu oraz środowisk naukowych funkcjonujących w obszarze cyberbezpieczeństwa. Jej celem jest określenie nisz technologicznych tego obszaru, które stanowić mogą polskie specjalizacje i przewagi konkurencyjne względem podmiotów funkcjonujących na rynku globalnym. Wiedza na temat potencjału analizowanego obszaru w Polsce może posłużyć do wsparcia procesów decyzyjnych instytucji publicznych w zakresie planowania i wdrażania mechanizmów wspierających rozwój polskiej gospodarki, w tym m.in. przez różnorodne instrumenty wsparcia finansowego dla projektów badawczo-rozwojowych i innowacyjnych.

Zakres niniejszej ekspertyzy obejmuje w szczególności:

- Charakterystykę globalnego oraz krajowego rynku cyberbezpieczeństwa, w tym m.in. przedstawienie rysu historycznego oraz analizę wielkości i dynamiki rynku;
- Analizę barier i trendów rynkowych oraz opis kluczowych podmiotów funkcjonujących na rynku z perspektywy globalnej oraz krajowej;
- Analizę otoczenia prawnego oraz w zakresie ochrony własności intelektualnej, z perspektywy globalnej oraz krajowej;
- Analizę oraz charakterystykę kierunków rozwoju technologii w Polsce w oparciu o wypracowane podczas warsztatów SL Scenariusze Rozwoju;
- Mapę Drogową, tj. uproszczony harmonogram prac i projektów B+R planowanych do realizacji i określonych jako kluczowe dla rozwoju cyberbezpieczeństwa w Polsce;
- Rekomendacje dotyczące działań, które należy podjąć w celu usprawnienia funkcjonowania przedsiębiorstw z segmentu cyberbezpieczeństwa w Polsce;
- Rekomendacje w zakresie potencjalnych zmian w Krajowych Inteligentnych Specjalizacjach w odniesieniu do usprawnienia opracowywania lub wdrażania technologii wymienianych w Mapie Drogowej.

2. Charakterystyka rynku globalnego

W rozdziałach od 2.1 do 2.7 zaprezentowana została charakterystyka rynku globalnego w obszarze cyberbezpieczeństwa, w tym przedstawiony został rys historyczny obszaru wraz z analizą dostępnych produktów i technologii. Przedstawiono podstawową analizę wielkości oraz dynamiki rynku, a także dokonano analizy cyklu życia produktów oraz barier rynkowych. Omówiono również profile kluczowych podmiotów funkcjonujących w tym obszarze oraz dokonano analiz otoczenia prawnego i związanej z nim ochrony własności intelektualnej. Całość zwieńczono przeprowadzeniem analizy trendów rozwojowych dla obszaru cyberbezpieczeństwa w skali globalnej.

2.1. Rys historyczny oraz analiza dostępnych produktów i technologii

Cyberbezpieczeństwo (ang. cybersecurity), jak każdy obszar z dziedziny informatyki, ma wiele definicji, w dużej mierze niewykluczających się, a najczęściej po prostu wzajemnie się uzupełniających. W zasadzie termin ten przedstawić można jako ogół technik, procesów i praktyk stosowanych w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem. Definicję tę dodatkowo rozszerza polskie prawodawstwo, które cyberbezpieczeństwem określa „ogólną odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”[1].

Cyberbezpieczeństwo jest jednocześnie obszarem, który, pomimo że jest nierozerwalnie związany z komputerami, sam wyprzedza powstanie komputerów osobistych. Przez prawie dwie dekady po zaprojektowaniu i złożeniu pierwszego na świecie komputera cyfrowego w 1943 r.[2], przeprowadzanie cyberataków było praktycznie niemożliwe. Wynikało to z dwóch powodów, po pierwsze dostęp do komputerów, stanowiących wówczas gigantycznych rozmiarów maszyny

[1] *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 22 lipca 2020 r. w sprawie ogłoszenia jednolitego tekstu ustawy o krajowym systemie cyberbezpieczeństwa.*

[2] *Colossus mark 1. Pierwszy elektroniczny programowalny komputer cyfrowy, opracowany dla zespołu Alana Turinga w laboratoriach Bletchley Park przez Tommy’ego Flowersa.*

elektroniczne, był ograniczony, po drugie nie były one połączone w sieć. Poza tym sama teoria dotycząca wirusów komputerowych została po raz pierwszy upubliczniona dopiero w 1949 r., kiedy pionier informatyki John von Neumann spekulował, że programy komputerowe mogą się „rozmnażać".

Ze względu na postępującą miniaturyzację i obniżanie kosztów produkcji komputerów, wiele dużych firm zainwestowało w technologie przechowywania danych i systemów oraz zarządzania nimi. Fizyczne ograniczenia dostępu stały się uciążliwe, ze względu na konieczność korzystania z komputerów przez coraz większą liczbę użytkowników. Z tego powodu zaczęto używać haseł.

Właściwe cyberbezpieczeństwo rozpoczęło się w 1972 r. od projektu badawczego ARPANET (The Advanced Research Projects Agency Network), protoplasty Internetu. Badacz Bob Thomas, pracujący w BBN[3], jednej z instytucji mających dostęp do ARPANET'u, stworzył program komputerowy o nazwie Creeper. Program ten mógł rozprzestrzeniać się w sieci ARPANET, zostawiając ślad w każdym miejscu w formie informacji: „I'm the creeper, catch me if you can"[4]. Ray Tomlinson – wynalazca poczty elektronicznej – napisał program Reaper, który ścigał i usuwał Creepera. Reaper był nie tylko pierwszym przykładem oprogramowania antywirusowego, ale także pierwszym samoreplikującym się programem, dzięki czemu stał się pierwszym w historii „robakiem" komputerowym.

Kwestionowanie luk w nowych technologiach stało się ważniejsze, ponieważ coraz więcej organizacji zaczęło używać telefonu do tworzenia zdalnych sieci. Każdy element podłączonego sprzętu stanowił nowy „punkt wejścia" i wymagał ochrony. Wraz ze wzrostem zależności od komputerów i sieci, dla decydentów stało się jasne, że bezpieczeństwo jest niezbędne, a nieautoryzowany dostęp do danych i systemów może być katastrofalny. W latach 1972-1974 nastąpił wyraźny wzrost zainteresowania tematem bezpieczeństwa komputerowego i był przedmiotem wielu dyskusji, głównie na łamach prasy akademickiej.

Tworzenie wczesnych zabezpieczeń komputerowych zostało podjęte przez konsorcjum ESD oraz ARPA, które pracowało nad opracowaniem projektu jądra bezpieczeństwa dla systemu komputerowego Honeywell Multics. Nad podobnymi projektami pracowały także UCLA i Stanford Research Institute. Projekt ARPA Protection Analysis badał bezpieczeństwo systemów operacyjnych identyfikując możliwe do automatyzacji techniki wykrywania luk w oprogramowaniu.

W połowie lat 70. XX w. koncepcja cyberbezpieczeństwa dojrzewała. W 1976 r. Theodore A. Linden w pracy „Struktury systemów operacyjnych do wspierania bezpieczeństwa i niezawodnego

[3] Oryginalnie Bolt Beranek and Newman Inc., obecnie Raytheon BBN Technologies.

[4] Ang. Jestem pełzaczem, złap mnie jeśli potrafisz.

oprogramowania”[5] stwierdził: „Bezpieczeństwo stało się ważnym i wymagającym celem w projektowaniu systemów komputerowych”.

Lata 80. XX w. przyniosły wzrost głośnych cyberataków, w tym na National CSS, AT&T i Los Alamos National Laboratory. Koncepcja cyberbezpieczeństwa przenikała także do kultury masowej. Film „Gry wojenne” z 1983 r, przedstawia włamanie do systemu komputerowego, który, bez świadomości młodego hakera, kontroluje arsenał nuklearny USA. W tym samym roku po raz pierwszy użyto terminów „koń trojański” i „wirus komputerowy”.

W czasie zimnej wojny ewoluowało zagrożenie cyberszpiegostwem. W 1985 r. Departament Obrony Stanów Zjednoczonych opublikował *Kryteria oceny zaufanych systemów komputerowych* (znane również jako Pomarańczowa Księga), które zawierały praktyczne porady dotyczące oceny stopnia zaufania, jakie można pokładać w oprogramowaniu przetwarzającym informacje niejawne lub inne poufne informacje oraz jakie środki bezpieczeństwa potrzebne są producentom do wbudowania w ich produkty komercyjne. Mimo to w 1986 r. niemiecki haker Marcus Hess użył bramki internetowej w Berkeley w Kalifornii, aby podłączyć się do ARPANET. Zhakował 400 komputerów wojskowych, w tym komputery mainframe w Pentagonie, z zamiarem sprzedawania informacji KGB.

Kwestie bezpieczeństwa zaczęły być traktowane przez użytkowników zarówno prywatnych, jak i instytucjonalnych z jeszcze większą powagą. Doświadczeni użytkownicy komputerów osobistych szybko nauczyli się monitorować rozmiar pliku command.com, zauważając, że jego wzrost był pierwszą oznaką potencjalnej infekcji. Środki bezpieczeństwa cybernetycznego uwzględniały to myślenie, a nagłe zmniejszenie ilości wolnej pamięci operacyjnej pozostaje oznaką ataku do dnia dzisiejszego.

W 1987 r. powstały pierwsze komercyjne programy antywirusowe - Ultimate Virus Killer (UVK) dla Atari ST, antywirus NOD oraz VirusScan Johna McAfee. Równolegle przeprowadzono jedną z pierwszych udokumentowanych akcji usuwania wirusa „na wolności”. Zostało to przeprowadzone przez Niemca Bernda Fixa, który zneutralizował niesławnego wirusa Vienna – wczesny przykład złośliwego oprogramowania, które rozprzestrzenia się i uszkadza pliki. Również w 1987 r. pojawił się po raz pierwszy zaszyfrowany wirus Cascade, który infekował pliki .COM. Wirus ten spowodował poważny incydent w belgijskim biurze IBM, służąc jako impuls do rozwoju produktu antywirusowego IBM. Wcześniej wszelkie rozwiązania antywirusowe opracowane w IBM były przeznaczone wyłącznie do użytku wewnętrznego. Do 1988 roku na całym świecie powstało wiele firm specjalizujących się w ochronie antywirusowej.

Pierwsze oprogramowanie antywirusowe składało się z prostych skanerów, które przeprowadzały wyszukiwanie kontekstowe w celu wykrycia unikalnych sekwencji kodu wirusa. Wiele z tych

---

[5] Theodore A. Linden. 1976. Operating System Structures to Support Security and Reliable Software. ACM Comput. Surv. 8, 4 (Dec. 1976), 409–445, https://doi.org/10.1145/356678.356682. Dostęp: 14.10.2021.

skanerów zawierało również „immunizatory", które modyfikowały programy, aby wirusy „myślały", że komputer jest już zainfekowany i ich nie atakowały. Ponieważ liczba wirusów wzrosła do setek, immunizatory szybko stały się nieskuteczne. Dla firm antywirusowych stawało się również jasne, że mogą reagować jedynie na istniejące ataki, a brak uniwersalnej i wszechobecnej sieci (internetu) utrudniał wdrażanie aktualizacji.

Wzrost świadomości istnienia wirusów komputerowych był impulsem do zorganizowania w 1988 roku pierwszego elektronicznego forum dyskusyjnego poświęconego bezpieczeństwu antywirusowemu – Virus-L. Lata 80-te XX w. to także początek prasy poświęconej tematyce antywirusowej. Powstały wówczas sponsorowane przez Sophos Virus Bulletin z siedzibą w Wielkiej Brytanii oraz Virus Fax International dr Solomona. Z kolei w 1989 r. IBM w końcu skomercjalizował swój wewnętrzny projekt antywirusowy, a IBM Virscan dla MS-DOS trafił do sprzedaży. Dekada zakończyła się pojawieniem kolejnych rozwiązań antywirusowych na rynku cyberbezpieczeństwa, w tym F-Prot, ThunderBYTE i Norman Virus Control.

Lata 90-te XX w. spotęgowały rozwój zagadnień związanych z cyberbezpieczeństwem. W roku 1990 powstał pierwszy wirus polimorficzny (rzeczywisty kod programu jest zaszyfrowany i za każdym uruchomieniem programu deszyfrowany, aby uniknąć wykrycia) o nazwie 1260. Był on demonstratorem technologii, która później się stała się bardzo popularna. W roku 1991 utworzono EICAR (Europejski Instytut Badań nad Antywirusami Komputerowymi), jako organizację mającą skupiać swe wysiłki nad opracowywaniem i zwiększaniem skuteczności oprogramowania antywirusowego. EICAR funkcjonuje do dziś i zajmuje się wszystkimi rodzajami złośliwego oprogramowania.

Problemem w latach 90-tych XX w. była także adaptacja rozwiązań zabezpieczających przez użytkowników. Wczesny program antywirusowy opierał się wyłącznie na sygnaturach, porównując pliki binarne w systemie z bazą danych „sygnatur" wirusów. Oznaczało to, że wczesny program antywirusowy generował wiele fałszywych alarmów i wykorzystywał dużo mocy obliczeniowej, co frustrowało użytkowników wraz ze spadkiem produktywności. Co więcej popularyzacja antywirusów sprawiła, że cyberprzestępcy zareagowali i w 1992 r. pojawił się pierwszy program antyantywirusowy. Do 1996 r. wirusy komputerowe posiadały w swoim arsenale wiele innowacyjnych rozwiązań. Obejmowało to między innymi zdolność ukrywania się, polimorfizm i powstanie tzw. „makrowirusów", stawiając nowe wyzwania dla producentów oprogramowania antywirusowego, którzy musieli stworzyć nowe możliwości wykrywania i usuwania złośliwego oprogramowania. Liczba nowych infekcji wirusami i złośliwym oprogramowaniem eksplodowała w latach 90 XX w. Jak na początku tej dekady były to tylko dziesiątki tysięcy, tak już w 2007 r. zarejestrowano ich ok. pięciu milionów. W połowie lat 90. XX w. było jasne, że cyberbezpieczeństwo musi być „produkowane" masowo, aby chronić społeczeństwo przed różnymi cyberatakami. Jeden z naukowców NASA opracował pierwszy program typu firewall, wzorując go na fizycznych strukturach, które zapobiegają rozprzestrzenianiu się rzeczywistych pożarów w budynkach. Wykrywanie heurystyczne pojawiło się również jako nowa metoda radzenia sobie z ogromną liczbą wariantów wirusów. Skanery antywirusowe zaczęły wykorzystywać sygnatury ogólne – często zawierające nieciągły kod i wykorzystujące znaki

wieloznaczne - do wykrywania wirusów, nawet jeśli zagrożenie zostało „ukryte” w bezsensownym kodzie.

Koniec lat 90-tych XX w. to popularyzacja poczty elektronicznej. E-maile, które miały zrewolucjonizować komunikację, otworzyły również nowy punkt wejścia dla wirusów. W 1999 r. pojawił się wirus Melissa, który infekował komputer użytkownika za pośrednictwem dokumentu Word, a następnie wysłał swoje kopie na pierwsze 50 adresów e-mail w programie Microsoft Outlook. Historycznie pozostaje on jednym z najszybciej rozprzestrzeniających się wirusów, a naprawa głównych szkód przez niego wyrządzonych kosztowała dotychczas około 80 milionów dolarów (stan na październik 2021 r.).

W 2001 roku pojawiła się nowa technika infekcji - użytkownicy nie musieli już pobierać plików – wystarczyło odwiedzić zainfekowaną witrynę, gdzie cyberprzestępcy zastąpili czyste strony zainfekowanymi lub „ukryli” złośliwe oprogramowanie na legalnych stronach internetowych. Wirusy zaczęły również atakować komunikatory internetowe oraz pojawiły się „robaki” zaprojektowane do rozprzestrzeniania się za pośrednictwem kanału IRC (Internet Chat Relay).

Rozwój ataków typu zero-day, które wykorzystują „dziury” w zabezpieczeniach dla nowego oprogramowania i aplikacji, oznaczał, że antywirus był coraz mniej skuteczny – nie można sprawdzać kodu pod kątem istniejących sygnatur ataków, chyba że wirus już istnieje w bazie danych. Magazyn komputerowy c't odkrył, że wskaźniki wykrywalności zagrożeń typu zero-day spadły z 40-50% w 2006 r. do zaledwie 20-30% w 2007 r.

Kluczowym wyzwaniem związanym z antywirusem jest to, że często może spowolnić działanie komputera. Jednym z rozwiązań tego problemu było przeniesienie oprogramowania z komputera do chmury. W 2007 r. Panda Security połączyła technologię chmury z analizą zagrożeń w swoim produkcie antywirusowym. W 2008 r. w jego ślady poszło McAfee Labs, dodając do programu VirusScan, opartą na chmurze, funkcję ochrony przed złośliwym oprogramowaniem. W następnym roku utworzono organizację Anti-Malware Testing Standards Organization (AMTSO), której celem było między innymi prowadzenie prac nad metodą testowania produktów w chmurze.

Kolejną nowością w zakresie cyberbezpieczeństwa, w pierwszej dekadzie XXI w. było bezpieczeństwo systemu operacyjnego. Twórcy oferowali cyberbezpieczeństwo wbudowane w system operacyjny, zapewniające dodatkową warstwę ochrony. Często obejmuje to przeprowadzanie regularnych aktualizacji poprawek systemu operacyjnego, instalowanie zaktualizowanych silników i oprogramowania antywirusowego, zapór i bezpiecznych kont z zarządzaniem użytkownikami. Wraz z rozprzestrzenianiem się smartfonów opracowano również program antywirusowy dla urządzeń mobilnych.

Na dokonujący się rozwój cyberbezpieczeństwa, cyberprzestępcy odpowiedzieli własnymi innowacjami, tj. atakami wielowektorowymi i socjotechniką. Wykorzystując zebrane doświadczenia sprawili, że program antywirusowy został zmuszony do odejścia od metod wykrywania opartych na sygnaturach na rzecz innowacji „następnej generacji”. Cyberbezpieczeństwo nowej generacji wykorzystuje różne podejścia, aby zwiększyć wykrywalność

nowych, bezprecedensowych zagrożeń, jednocześnie zmniejszając liczbę fałszywych alarmów. Zwykle obejmuje to:

- Uwierzytelnianie wieloskładnikowe (MFA).
- Network Behavioral Analysis (NBA) – identyfikację złośliwych plików na podstawie odchyleń behawioralnych lub anomalii.
- Analizę zagrożeń i automatyzację aktualizacji.
- Ochronę w czasie rzeczywistym – określaną również jako skanowanie przy dostępie, ochronę tła, ochronę rezydentną i automatyczną ochronę.
- Sandboxing – tworzenie izolowanego środowiska testowego, w którym można uruchomić podejrzany plik lub adres URL.
- Forensics (kryminalistyka) — analizowanie ataków tak, aby pomóc zespołom ds. bezpieczeństwa lepiej łagodzić przyszłe naruszenia.
- Kopie zapasowe i dublowanie.
- Zapory sieciowe aplikacji internetowych (WAF) — chroniące przed fałszowaniem między witrynami, wykonywaniem skryptów między witrynami (XSS), dołączaniem plików i wstrzykiwaniem SQL.

Dziś cyberbezpieczeństwo, będąc już dojrzałą, choć wciąż dynamicznie rozwijającą się dziedziną, funkcjonuje na rynku oferując szereg różnych produktów i usług, do których w szczególności należy zaliczyć:

Wsparcie bezpiecznego projektowania systemów – tzw. „security-by-design”, oprogramowanie zaprojektowane z myślą o jego bezpieczeństwie. Rozwiązania, które to wspomagają, to np. zasada ograniczonego dostępu, automatyczne dowodzenie twierdzeń, audytowanie, testowanie i rewizje kodu oraz wiele innych. Istnieje szereg firm świadczących usługi konsultingowe i outsourcingowe wspierające to podejście.

Różnego rodzaju środki bezpieczeństwa – szereg produktów z dziedziny oprogramowania mających na celu zwiększenie bezpieczeństwa systemów. Obejmują one w szczególności:

- Systemy kontroli dostępu.
- Firewalle.
- Systemy szyfrowania korespondencji i komunikacji.
- Systemy wykrywania naruszeń.
- Antywirusy.

- **Zarządzanie podatnościami** - obszar zarówno o charakterze usługowym, jak i produktowym. Oprócz wsparcia konsultingowego, udostępnia również różnego rodzaju skanery podatności, które analizują systemy w poszukiwaniu znanych rodzajów podatności, takich jak niezabezpieczone porty, niebezpieczne konfiguracje i ogólną podatność na złośliwe oprogramowanie. Takie skanery skupiają się prze wszystkim na nowo odkrytych podatnościach. Uzupełnieniem tego segmentu są metody testowania penetracyjnego, zlecane zewnętrznym audytorom bezpieczeństwa.

- **Mechanizmy kontroli autentykacji** - niezwykle szeroki segment dotyczący wielu dziedzin życia. Z jednej strony oczywista popularyzacja weryfikacji wieloetapowej, a innym aspektem jest wykrywanie automatycznych prób logowania (captcha). W wielu miejscach stosuje się skanery o charakterze biometrycznym – np. poprzez odcisk palca lub rozpoznawanie twarzy. Ważne są też mechanizmy inżynierii społecznej, które mają wytworzyć w użytkownikach zachowania nie zdradzające ich haseł.

- **Mechanizmy ochrony sprzętowej** - segment obejmujący wiele urządzeń, takich jak tokeny sprzętowe, dongle licencyjne i platformy urządzeń zaufanych. Dużą rolę odgrywają tu też rozwiązania fizycznej kontroli dostępu.

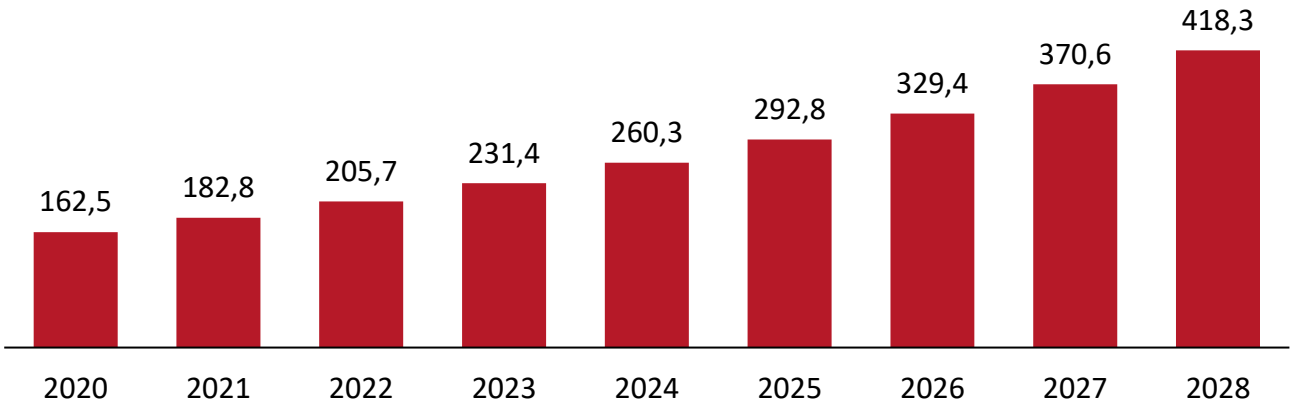
- **Kontrolę i bezpieczeństwo ruchu sieciowego** - mechanizmy zabezpieczania ruchu oraz ukrywania lokalizacji odgrywają ogromną rolę na rynku cyberbezpieczeństwa. Produkty w postaci VPN-ów (prywatne sieci wirtualne) oraz szyfrowanych komunikatorów i kont pocztowych. Segment ten cały czas się rozwija i na rynku dostępnych jest wiele produktów z nim związanych.

2.2. Podstawowa analiza wielkości i dynamiki rynku

Wartość światowego rynku cyberbezpieczeństwa w 2020 r., według szacunków Quince Market Research, wyniosła 162,5 miliarda USD i znajduje się obecnie w historycznym dla siebie okresie wzrostu, który co najmniej do 2028 r. powinien utrzymać się na poziomie ponad 12% (dokładne szacunki mówią nawet o 12,5% w skali roku). Tak wysoki CAGR nie tylko utrzymał się podczas recesji gospodarczej zapoczątkowanej w 2020 r. pandemią COVID-19, ale doznał on akceleracji (prognozy w 2019 r. wskazywały CAGR na poziomie 8-10%), głównie z uwagi na znacznie zwiększony popyt wśród branż, które zmuszone były do implementacji w pełni zdalnego lub hybrydowego trybu pracy. Jeśli prognozy te się sprawdzą, wartość rynku cyberbezpieczeństwa z 2020 r. podwoi się do 2026 r. (czyli w zaledwie 6 lat), a dwa lata później przekroczy 418 miliardów USD[6]. Wzrost ten zaprezentowany został na Rysunku 1.

[6] *Raport Cybersecurity Market, Quince Market Research, https://www.globenewswire.com/en/news-release/2021/03/17/2194254/0/en/Global-*

Rysunek 1. Wartość światowego rynku cyberbezpieczeństwa w roku 2020 i prognoza na lata 2021-2028 (mld USD)



Źródło: opracowanie własne na podstawie raportu Cybersecurity Market autorstwa Quince Market Research

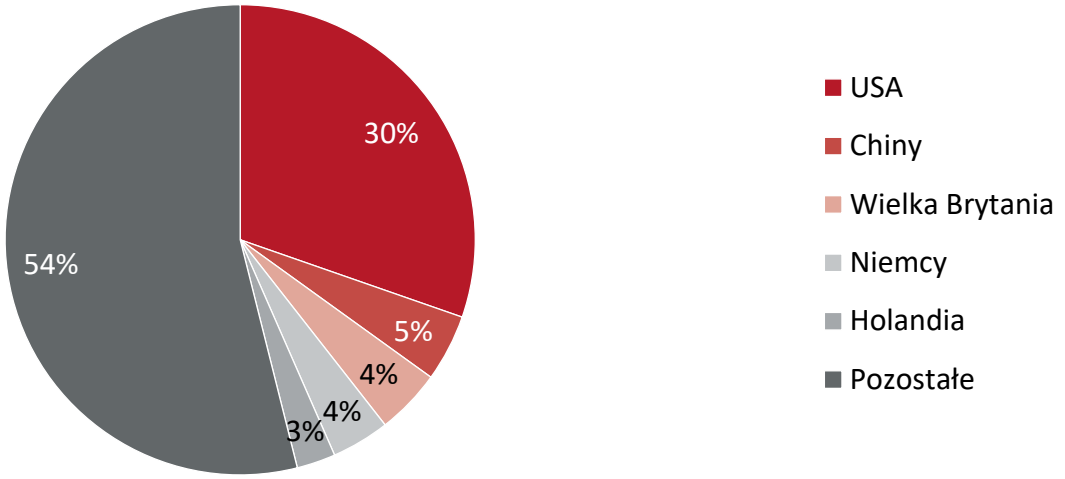
Niekwestionowanym liderem krajowym na rynku rozwiązań z obszaru cyberbezpieczeństwa są Stany Zjednoczone – segmentacja geograficzna wskazuje, że kraj ten odpowiadał w 2019 r. za niemalże 30% wartości całego globalnego rynku (48 mld USD). Pozycję wicelidera zajmują Chiny (7,35 mld USD), jednak wartość krajowego rynku Państwa Środka jest 6-krotnie niższa niż USA – należy mieć jednak na uwadze, że informacje z tego regionu są znacząco ograniczone, szczególnie jeśli chodzi o rozwiązania państwowe (można spodziewać się więc znaczących niedoszacowań co do wartości tego rynku krajowego). Pozostali liderzy, to przede wszystkim kraje europejskie, wśród których wyróżniają się te o najsilniejszych gospodarkach, z ważnymi międzynarodowo centrami finansowo-korporacyjnymi. Należą do nich: Wielka Brytania (7,17 mld USD), Niemcy (6,38 mld USD) oraz Holandia (4,26 mld USD)[7]. Segmentacja geograficzna przedstawiona została na Rysunku 2.

Wskazane kraje wyróżnia również najwyższy poziom świadomości ich społeczeństw co do zagrożeń płynących z cyberataków. Nawet jeśli poziom edukacji pojedynczych konsumentów w zakresie technologii zabezpieczających w IT pozostaje w nich względnie niski (analogicznie jak w przypadku całego światowego rynku), to nie brakuje w tych krajach aktywnych przedsiębiorców z unikatowymi technologiami z obszaru cyberbezpieczeństwa (od korporacji po startupy), jak i jednostek administracyjnych wyznaczających odpowiednie kierunki krajowej legislacji.

Cybersecurity-Market-Size-to-Grow-at-a-CAGR-of-12-5-from-2021-to-2028.html. Dostęp: 12.10.2021.

[7] *Raport The European Cybersecurity Market, Enterprise Ireland, https://globalambition.ie/cybersecurity-report-and-conference/. Dostęp: 07.10.2021.*

Rysunek 2. Procentowy udział kluczowych rynków krajowych w obszarze cyberbezpieczeństwa



Źródło: opracowanie własne na podstawie raportu The European Cybersecurity Market autorstwa Enterprise Ireland

Na rynku europejskim szczególnie duże znaczenie mają regulacje paneuropejskie (wprowadzane w ramach Unii Europejskiej), których zapisy kształtują bezpośrednio wymagania stawiane animatorom rynku (np. *The General Data Protection Regulation (EU) 2016/679* – wymagająca m.in. zgłaszania wszystkich incydentów w obszarze cyberbezpieczeństwa w przeciągu 72 godzin od zajścia)[8].

Oznacza to, że wartość rynku oraz popyt na nowoczesne rozwiązania z zakresu cyberbezpieczeństwa na najważniejszych geograficznie rynkach generowany jest nie tylko przez samych użytkowników, ale również przez wymagania legislacyjne, kampanie społeczne oraz incydenty powodowane aktywnościami cyberprzestępców – przy czym częstotliwość ataków (i ich dotkliwość) jest tym wyższa, im cenniejsze są dane możliwe do wykradzenia. Standardem rynkowym staje się więc szczególnie zainteresowanie obszarem bezpieczeństwa IT w największych gospodarczo krajach oraz wzrost popytu na produkty i usługi z zakresu cyberbezpieczeństwa w gospodarkach rozwijających się.

[8] *Artykuł o światowym i europejskim rynku bezpieczeństwa IT w perspektywie regulacji GDPR, Canalys, https://www.canalys.com/newsroom/it-security-market-europe-grow-16-2018-gdpr-legislation-kicks. Dostęp: 12.10.2021.*

2.3. Analiza cyklu życia produktów

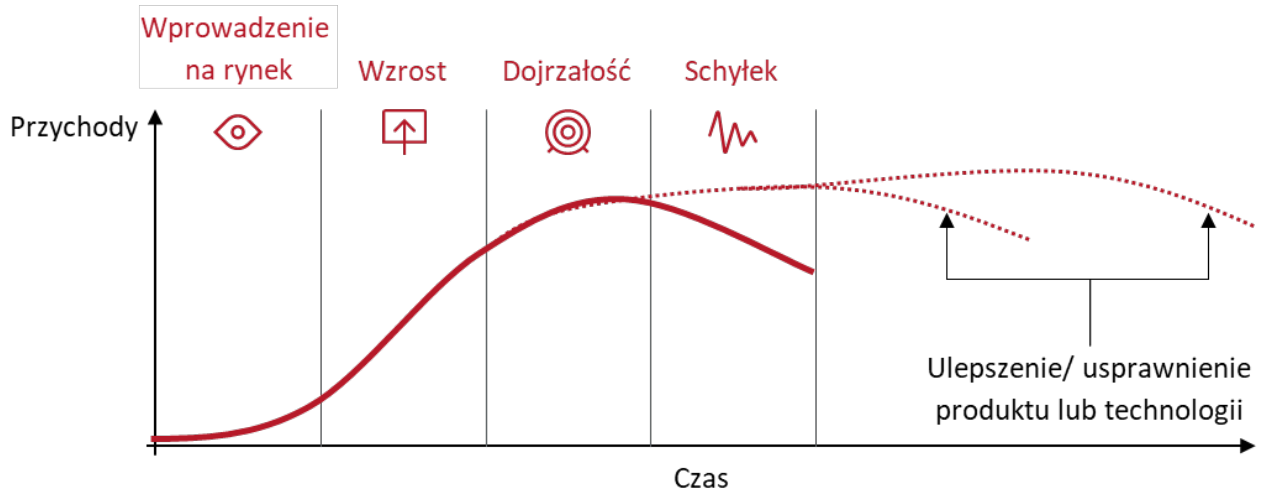
Standardowy cykl życia produktów lub technologii można podzielić na 4 główne fazy, zależnie od czasu, jaki dany produkt/ technologia istnieje na rynku oraz od generowanych przychodów:

- **Wprowadzenie na rynek** – produkt (lub technologia) jest nowością na rynku i został skomercjalizowany dopiero niedawno. Potencjalni nabywcy jeszcze „przekonują się" do niego. Następują wdrożenia pilotażowe, zarówno na zasadach niekomercyjnych (w celu uzyskania rzeczywistych danych na temat użycia lub pozyskania pierwszych referencji), jak i komercyjnych. Produkt zdobywa coraz więcej zaufania ze strony klientów, jednak przychody generowane są głównie przez tzw. *early adopters* – grupę użytkowników, która z chęcią i łatwością wdraża i wykorzystuje najnowocześniejsze technologie, aby zdobyć przewagę względem konkurencji.
- **Wzrost** – produkt zaczyna być dobrze znany i rozpoznawany na rynku, wskutek czego zaobserwować można tzw. *efekt kuli śnieżnej* – coraz większa skala wykorzystania produktu powoduje, że również znacząco rośnie rzesza jego nowych użytkowników. W odniesieniu do technologii, wraz ze wzrostem popularności, rośnie również potencjalnie jej zakres zastosowania (np. w różnych dziedzinach). Wdrożenia odbywają się niemal wyłącznie na zasadach komercyjnych. Na rynku zaczyna pojawiać się w tej fazie presja ze strony konkurencji, która stara się proponować swoje alternatywne wersje danego produktu czy technologii, podążając za trendem wzrostowym.
- **Dojrzałość** – produkt jest bardzo dobrze znany i powszechnie wykorzystywany na rynku. Nie jest już rozpatrywany jako innowacja czy przełom w kontekście technologicznym, staje się jednym z rynkowych standardów. Z jednej strony generowane przychody ze sprzedaży produktu notują „historyczne maksimum", jednak produkt jednocześnie musi liczyć się z silną konkurencją, gdyż rozwiązania konkurencyjne znajdują się w fazie wzrostu i przechodzą do fazy dojrzałości.
- **Schyłek** – z uwagi na fakt, że produkt lub technologia istnieje na rynku już od dłuższego czasu, dostępne stają się nowe lub ulepszone produkty i technologie o lepszych parametrach lub cechach użytkowych. Przychody ze sprzedaży spadają, gdyż klienci wybierają nowsze rozwiązania.

Powyższe cykle życia są fundamentem dla produktów i technologii tworzonych niemalże w każdej branży – jednak praktyka w każdej z nich odpowiednio dostosowuje niniejszą metodologię w taki sposób, aby w pełni efektywnie służyła własnym animatorom rynku. Taka personalizacja branżowa szczególnie widoczna jest w przypadku tych produktów, których cykl życia nie zakłada zamykania poszczególnych faz, a np. ich przedłużanie lub wręcz powrót do poprzednich. Dokładnie taka sytuacja ma miejsce w przypadku oprogramowania – czyli aktualnej podstawy produktów i usług oferowanych w branży cyberbezpieczeństwa.

Inżynieria oprogramowania wypracowała standard rynkowy, w którym to zdecydowana większość rozwiązań tworzona jest z myślą o stałym jej rozwijaniu i aktualizowaniu, co bezpośrednio wpływa na cykl życia produktu. W znakomitej większości przypadków oznaczać to będzie przedłużanie fazy wzrostu lub dojrzałości w taki sposób, aby produkt jak najpóźniej (docelowo nigdy, w praktyce jednak nie występują oprogramowania stosowane „bez końca") wszedł w fazę schyłkową, przy której przestaje on być konkurencyjny. Schemat takiego scenariusza przedstawiony został na Rysunku 3.

Rysunek 3. Uproszczony schemat obrazujący cykl życia produktu/ technologii oraz skutek wdrożenia ulepszonej lub nowej jego wersji



Źródło: opracowanie własne

Powyższy schemat nie jest jednak widoczny wyłącznie przy rozwiązaniach bazujących na oprogramowaniu, a tak naprawdę jest on docelowym założeniem przy znakomitej większości technologii, które z założenia mają być stale usprawniane. Nie oznacza to jednak, że rynek IT nie wypracował dotychczas żadnego schematu specyficznego wyłącznie dla oprogramowania – wręcz przeciwnie, w branży na co dzień wykorzystywany jest termin „cyklu życia oprogramowania", który definiuje nie tylko założenia odnośnie docelowego schematu funkcjonowania oprogramowania na rynku, ale również nakreśla metodologię jego tworzenia i aktualizowania. Z tego również powodu niemożliwe jest określenie jednego poprawnego schematu cyklu życia oprogramowania, a zamiast tego standardem rynkowym stało się dobieranie jego wariacji (zwanych modelami) ze względu na własne preferencje sposobu pracy oraz zamysłu technologicznego.

Obecnie wśród najpopularniejszych modeli cyklu życia oprogramowania możemy wymienić:

- **modele kaskadowe** (tzw. *waterfall*) – zakładające występowanie sześciu podstawowych faz tworzenia i rozwijania oprogramowania (od fazy planowania po fazę implementacji i testowania), pomiędzy którymi przejście następuje jedynie po ukończeniu poprzedniej i każda z nich ma fundamentalny wpływ na finalny produkt;

- **modele ewolucyjne** – rozwinięcie modelu kaskadowego, zakładającego bardziej elastyczne podejście do pracy, w której to fazy mogą być wykonywane symultanicznie, a powrót do poprzednich możliwy jest bez ograniczeń (jednym z najpopularniejszych modeli ewolucyjnych jest tzw. *agile software development*);
- **modele komponentowe** – zakładające tworzenie oprogramowania na bazie gotowych komponentów, a następnie jego rozwijania w bardzo ograniczonym zakresie (dużo mniejszy wpływ na dalsze fazy cyklu życia produktu);
- **modele przyrostowe** – zwane również iteracyjnymi, w ramach których prace nad oprogramowaniem zakładają ciągłe testowanie i weryfikowanie założeń, nawet po wprowadzeniu go na rynek (wykorzystuje się w nim m.in. prototypy czy założenia procesów spiralnych – tworzenia oprogramowania w ciągłej pętli powtarzanych czynności).

To, który cykl życia oprogramowania wykorzystywany jest przy konkretnej technologii zależne jest od samego zespołu jego twórców. Często decydują się oni na oparcie swojej pracy o założenia konkretnego modelu, jednocześnie jednak wdrażając w nim własne modyfikacje usprawniające prace.

Tak elastyczne podejście do cyklu życia produktu jest nie tylko analogicznie praktykowane w przypadku producentów oprogramowania z obszaru cyberbezpieczeństwa, ale również stało się obligatoryjne z uwagi na stale pojawiające się nowe technologie cyberprzestępców. Zjawisko to potwierdzili uczestnicy spotkań SL, którzy wspólnie zgodzili się, że produkty niezakładające ciągłego rozwoju i aktualizowania bardzo szybko stałyby się nieaktualne i (wykorzystując terminologię klasycznego cyklu życia produktów) pośpiesznie przeszły do fazy schyłkowej.

Elementem, który w unikalny sposób wpływa na rynek cyberbezpieczeństwa jest konieczność **działania reaktywnego**. W typowym oprogramowaniu możliwe jest poświęcenie czasu na przygotowanie rozwiązania zgodnie z opracowanym planem. W przypadku cyberbezpieczeństwa pojawia się konieczność wprowadzenia na rynek rozwiązania, które w natychmiastowy sposób zareaguje na nowy rodzaj zagrożenia (np. nowe złośliwe oprogramowanie) lub podatność (luki zero-day). Dlatego też, w niektórych przypadkach faza rozwoju produktu cyberbezpieczeństwa może być bardzo skrócona lub nawet poprzedzona natychmiastową reakcją z planem późniejszego rozwoju.

Warto również zwrócić uwagę, że w zakresie cyberbezpieczeństwa mamy do czynienia nie tylko z oprogramowaniem. Istotne segmenty rynku obejmują, m.in. urządzenia ochrony sprzętowej, takie jak klucze sprzętowe oraz systemy szyfrujące i ukrywające dane. Jest to np. popularne w branży OT. Cykl życia takich produktów, który nawet początkowo przypomina standardowy rozwój urządzeń, ma potencjalnie nieograniczoną żywotność w instalacjach procesowych. Urządzenia te często pracują latami bez żadnych aktualizacji, jako że ich aktualizacja byłaby bardzo kłopotliwa i kosztowna (np. konieczność zatrzymania pracy instalacji). Innym obszarem są komercyjne i przemysłowe urządzenia segmentu IoT. Bezpieczeństwo sieci Internetu rzeczy jest kluczowe i takie produkty jak bramki (interfejsy) tych sieci o podwyższonym poziomie

bezpieczeństwa stają się coraz częstsze. Cykl życia takich produktów należy porównywać z normalnymi urządzeniami infrastruktury sieciowej.

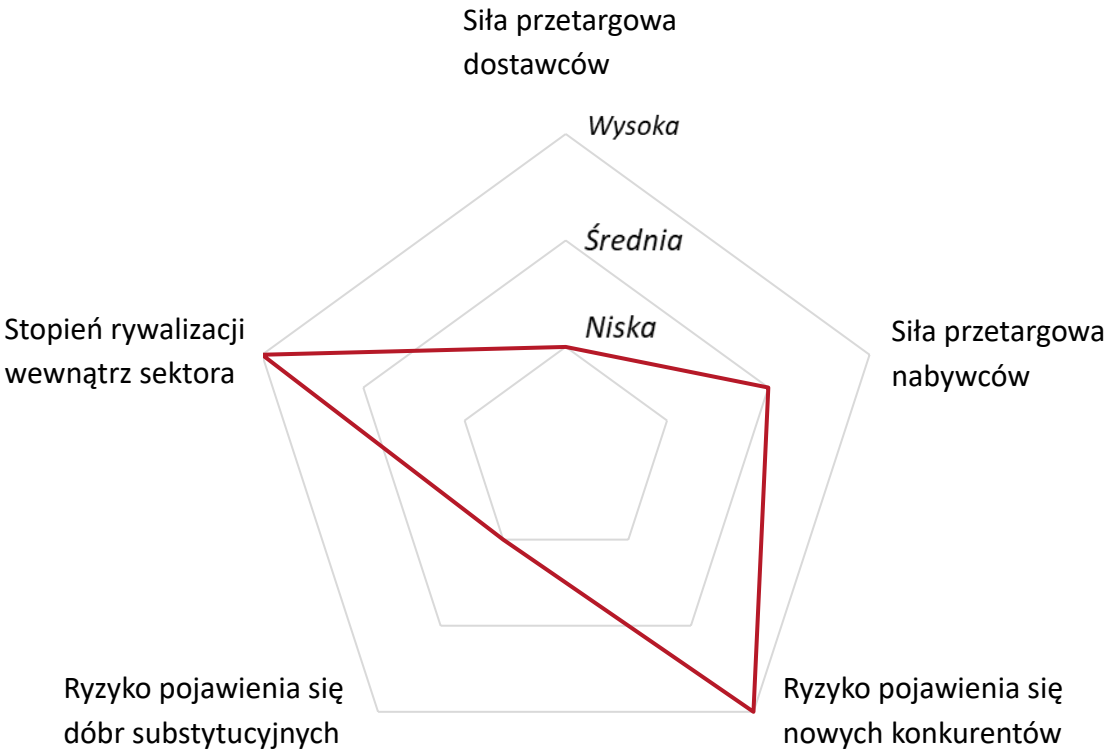
Z uwagi na mnogość rozwiązań informatycznych z obszaru cyberbezpieczeństwa nie jest możliwe określenie standardowego czasu trwania cyklu życia produktów tego typu. To co jest charakterystyczne dla tego typu rozwiązań (w szczególności bazujących na oprogramowaniu) to fakt, że ich cykl życia może być bardzo długi – raz wdrożone do sprzedaży rozwiązanie (np. antywirus dla klientów indywidualnych lub biznesowych) poddawane jest cyklicznym aktualizacjom, które pozwalają mu dalej pełnić swoją rolę, dostosowując się do coraz to nowych zagrożeń i przedłużając cykl życia w fazie dojrzałości takiego produktu. Warto zaznaczyć, że bez możliwości aktualizacji w obecnych czasach oprogramowanie mające zapewnić bezpieczeństwo w sieci przestałoby spełniać swoje zadanie w bardzo krótkim czasie z uwagi na pojawiające się stale nowe zagrożenia tworzone przez cyberprzestępców. Podobnie w przypadku zaawansowanych systemów cyberbezpieczeństwa w kluczowych sektorach gospodarki, takich jak np. bankowość, cykl życia produktów z obszaru cyberbezpieczeństwa jest relatywnie długi z uwagi na bariery oraz wyzwania związane ze zmianami już posiadanych systemów bezpieczeństwa. Widmo kapitałochłonnych, długich oraz ryzykownych dla bieżącej działalności infrastruktury IT wdrożeń nowych rozwiązań często skutecznie zniechęca korporacje do takich działań. Niebagatelny wpływ na żywotność rozwiązań z zakresu cyberbezpieczeństwa ma również samo zjawisko cyberprzestępczości, które co do zasady bazuje na dokładaniu kolejnych możliwych form ataku do już istniejących. Sprawia to, że konieczne jest nie tyle ciągłe zmienianie aktualnie dostępnych i używanych zabezpieczeń na zupełnie nowe, co dodawanie nowych funkcyjności i komponentów do już istniejących programów.

2.4. Analiza barier rynkowych

Bariery rynkowe globalnego obszaru cyberbezpieczeństwa przedstawione zostały dwutorowo – na początku cały sektor przenalizowano za pośrednictwem analizy „5 Sił Portera”, a następnie przytoczono bariery uzupełniające, które dopełniły obraz wyzwań, z którymi muszą mierzyć się interesariusze rynku.

Analiza „5 Sił Portera”, to miarodajne narzędzie pozwalające określić atrakcyjność otoczenia przez pryzmat pięciu głównych barier wpływających na możliwości rozwoju biznesu. Bariery te nazywamy siłami, do których zaliczamy: siłę przetargową dostawców (1) oraz nabywców (2), ryzyko pojawienia się nowych konkurentów (3) oraz substytutów (4) i stopień rywalizacji wewnątrz sektora (5). Na potrzeby niniejszej analizy każda z „sił” została oceniona w trójstopniowej skali (poziom oddziaływania niski, średni oraz wysoki). Na Rysunku 4 przedstawiono wynik analizy, a następnie argumentację oceny każdej z sił.

Rysunek 4. Uproszczona analiza „5 sił Portera” dla obszaru cyberbezpieczeństwa



Źródło: opracowanie własne

Oddziaływanie pierwszego z czynników, **siły przetargowej dostawców**, ocenione zostało jako **niskie**. Grupa dostawców obejmuje przede wszystkim właścicieli półproduktów i oprogramowań wykorzystywanych do pracy nad finalnymi rozwiązaniami, których na rynku IT jest bardzo dużo i nie zmienia się to w niszy cyfrowych zabezpieczeń. Tak duża różnorodność dostawców znacząco zmniejsza ich siłę oddziaływania na producentów, na co również wpływ miała łatwość ich ewentualnej zmiany przez klientów. Należy jednak zauważyć, że siła dostawców stopniowo rośnie, z uwagi na postępujące kroki nakierowane na „utrzymywanie klientów” – standardem rynkowym wśród renomowanych dostawców stało się podpisywanie długoterminowych umów ograniczających możliwość łatwej ich zmiany.

Siła przetargowa nabywców oceniona została jako **średnia**, jednak występują przesłanki świadczące o możliwym rozwoju w stronę sił wysokich, które dodatkowo uwidoczniły się podczas recesji gospodarki zapoczątkowanej przez pandemię COVID-19. Wyższą siłę klientów warunkuje przede wszystkim mnogość rozwiązań dostępnych na rynku i względna łatwość transferu pomiędzy nimi (w przypadku segmentu usługowego oraz rynku konsumentów indywidualnych).

Ryzyko pojawienia się nowych konkurentów ocenione zostało jako **wysokie**. Bariery wejścia są względnie niskie i obejmują w dużej mierze wydatki kapitałowe oraz dostosowanie rozwiązania do lokalnych wymogów regulacyjnych, co jednocześnie nie ogranicza znacząco możliwości

skalowania. Z uwagi na fakt, że rynek cyberbezpieczeństwa dynamicznie się rozwija, prezentuje się on jako atrakcyjny sektor dla nowych konkurentów – zarówno tych tworzących swoją działalność od zera (startupów), jak i dużych korporacji dywersyfikujących swoje portfolio produktowe. Należy jednak zaznaczyć, że tak jak samo ryzyko pojawienia się nowych konkurentów, którzy rozpoczną działalność w obszarze szeroko pojętego cyberbezpieczeństwa jest wysokie, to ryzyko pojawienia się nowych podmiotów, które osiągną sukces i zdobędą zaufanie klientów (w szczególności tych biznesowych), jest dużo niższe.

Odmiennie prezentuje się sytuacja **ryzyka pojawienia się dóbr substytucyjnych** – ocenione zostało ono na **niskie**, jednak na dobrą sprawę przy tak szerokiej definicji obszaru cyberbezpieczeństwa można byłoby uznać je za nieistniejące. Nie prognozuje się zmniejszenia aktywności cyberprzestępców na rynku, które mogłoby spowodować, że dobra substytucyjne zastępowałyby sektor cyberbezpieczeństwa, a jednocześnie nie ma przesłanek, które mogłyby przesądzać o np. zmniejszeniu znaczenia Internetu w działalności przedsiębiorstw czy codziennego życia społeczeństwa. Obecnie uznaje się, że obszar cyberbezpieczeństwa jest jednym z fundamentów rynku IT i niemożliwe jest jego zastąpienie.

Ostatni z czynników, **stopień rywalizacji wewnątrz sektora**, to ponownie siła oceniona na **wysoką**. Główny wpływ na taki stan rzeczy ma przede wszystkim mnogość konkurencji na rynku, względnie niskie bariery wejścia oraz trudność w tworzeniu unikalnych (w rozumieniu niepodrabialnych) przewag konkurencyjnych. Czynniki te powodują, że obszar ten cechuje się wysoką konkurencją, a dodatkowa trudność w długoterminowym utrzymaniu przewag konkurencyjnych bazujących na innowacji technologicznej pozwala sądzić, że sektor ten pozostanie obszarem zaciętej rywalizacji konkurentów.

Powyższe siły skutecznie zarysowują bariery rynkowe z perspektywy kluczowych uczestników rynku (twórców technologii, produktów oraz usług z obszaru cyberbezpieczeństwa oraz ich klientów i dostawców). Jednocześnie siły te podkreślają wyzwania z którymi zmierzyć się muszą podmioty myślące o rozpoczęciu działalności (lub dywersyfikacji już istniejącej) na rynku cyberbezpieczeństwa.

Oprócz barier wynikających z analizy „5 Sił Portera" warto nadmienić również **bariery będące kluczowymi wyzwaniami w skali makro takie jak**:

- **Poważne braki kadrowe** – obszar cyberbezpieczeństwa odczuwa globalnie (a w szczególności w obszarach geograficznych o mniejszej wartości rynku) znaczne braki kadrowe w postaci programistów, analityków i ekspertów, którzy posiadaliby wystarczające doświadczenie lub wiedzę w zakresie cyberbezpieczeństwa, ale również odpowiednie rozpoznanie w zakresie systemów operacyjnych, protokołów sieciowych czy pogłębionej matematyki, stosowanej m.in. w kryptografii. Cyberbezpieczeństwo to obszar wymagający holistycznej wiedzy, co znacząco potęguje wymagania stawiane zasobom ludzkim. Oznacza to, że zatrudnienie nowych pracowników wiąże się z reguły z długim procesem ich edukacji, a jednocześnie zasoby ludzkie dostępne na rynku albo preferują inne, dynamicznie rozwijające się branże IT (o np. mniejszych wymaganiach co do know-how) albo ich

specjalizacja jest na tyle wąska, że staje się ograniczeniem w tak interdyscyplinarnym obszarze jakim jest cyberbezpieczeństwo.

- **Niska świadomość klientów** – duża część odbiorców rozwiązań z obszaru cyberbezpieczeństwa nie jest świadoma jak bardzo ograniczone jest ich bezpieczeństwo w cyfrowym otoczeniu, co w szczególności widoczne jest wśród przedsiębiorców o mniejszej skali działalności (głównie MŚP), którzy często decydują się jedynie na najbardziej podstawowe zabezpieczenia, nie myśląc o cyberbezpieczeństwie jako poważnym czynniku wpływającym na ich działalność.

- **Wysoka zależność rynku od tradycyjnych rozwiązań** – największą penetrację w całym globalnym rynku mają producenci najprostszych rozwiązań z obszaru cyberbezpieczeństwa, takich jak antywirusy czy proste wtyczki do przeglądarek internetowych. Rozwiązania te są w dużej mierze znacząco ograniczone pod względem zaawansowania wykorzystywanych technologii, a brak odpowiedniej edukacji klientów powoduje, że złudnie czują się oni bezpieczni i nie widzą potrzeby korzystania z innych rozwiązań niż te najbardziej tradycyjne.

- **Nieaktualna legislacja** – na wielu rynkach geograficznych legislacja albo nie precyzuje jakie powinny być standardy cyberbezpieczeństwa reprezentowane przez przedsiębiorców (czy ogólnie podmioty przetwarzające jakiekolwiek dane w Internecie), albo robi to w sposób znacząco ograniczony, np. nie aktualizując wymogów mimo znaczących zmian w wykorzystywanych technologiach lub wręcz wykorzystując zapisy utrudniające implementację innowacji.

2.5. Kluczowi gracze rynkowi

Najważniejsze podmioty zajmujące się (w skali globalnej) tworzeniem, rozwijaniem oraz dystrybucją rozwiązań w zasadniczych obszarach cyberbezpieczeństwa wymieniono poniżej wraz z ich podziałem na specjalizacje branżowe:

Kluczowi gracze rynku systemów anti-malware

Ochrona antywirusowa stanowi podstawową, a jednocześnie jedną z najbardziej obligatoryjnych do poprawnego funkcjonowania w Internecie metod zabezpieczania urządzeń i sieci. Rozwiązania antywirusowe są na tyle spopularyzowaną formą zapewniania podstawowego bezpieczeństwa, że cieszą się one zainteresowaniem zarówno wśród klientów korporacyjnych, jak i instytucji otoczenia biznesu, administracji i indywidualnych użytkowników. Poniżej przedstawiono kluczowych graczy ww. rynku:

- **Avast Security A.S.** (Czechy) – jeden z liderów (obok Symantec) rynku antywirusów z rozwiązaniem opartym o formułę darmowej wersji podstawowej, możliwej do rozszerzenia po wykupieniu abonamentu. Wersja płatna zawiera nie tylko bardziej

rozszerzone opcje ochrony sieciowej, ale również dodatkowe moduły antywirusowe pozwalające chronić nie wyłącznie konkretne programy, ale również np. całą sieć wifi. Avast deklaruje ponad 165 milionów aktywnych użytkowników oraz ponad 1,5 mld blokowanych ataków na przestrzeni miesiąca. W ofercie przedsiębiorstwa widnieje technologia pozwalająca na zintegrowaną ochronę wszystkich użytkowników przed złymi kodami – jeśli algorytm antywirusa wykryje nieznany niebezpieczny kod, wysyła informację o nim do chmury i powiadamia o tym wszystkich pozostałych użytkowników.

Bitdefender (Rumunia) – firma założona w 2001 roku, która oprócz tradycyjnego oprogramowania antywirusowego zajmuje się również ochroną informacji (także tych wrażliwych) w sieci oraz strzeżeniem danych trzymanych w chmurze. Dodatkowo oferuje usługę VPN dla klientów prywatnych i korporacyjnych.

Cylance (USA) – organizacja angażująca systemy oparte o AI do ochrony sieci i podłączonych urządzeń. AI firmy wyposażone jest w algorytmy pozwalające wykryć wirusa nie znajdującego się jeszcze w bazie danych, co pozwala na skuteczniejszą ochronę.

ESET (Słowacja) – spółka działająca na rynku antywirusów już od 1987 roku. Oprogramowanie sprzedawane przez przedsiębiorstwo nagrodzone zostało w ponad 100 edycjach konkursu Virus Bulletin na program zapewniający największe bezpieczeństwo. W ramach swojej działalności sprzedaje ochronne oprogramowanie nie tylko dla użytkowników prywatnych i firm, ale też dla użytkowników systemu mobilnego Android. Oprócz podstawowych rodzajów oprogramowania w ramach droższych pakietów sprzedaje rozwiązanie chroniące bezpieczeństwo danych w chmurze.

McAffee (USA) – firma założona w 1987 roku przez programistę, od którego nazwiska pochodzi nazwa przedsiębiorstwa. W ofercie oprócz samego oprogramowania antywirusowego posiada także systemy ochrony prywatności i danych zamieszczanych w Internecie, wielokierunkową ochronę prywatności, a także usprawnienie dotyczące prędkości działania systemu operacyjnego w czasie, gdy oprogramowanie firmy jest aktywne.

Malwarebytes (USA) – kalifornijskie przedsiębiorstwo reklamujące się nowatorskim podejściem do ochrony urządzeń elektronicznych, stojącym w opozycji do tradycyjnych metod, zakładających protekcję na podstawie istniejących baz danych. Zamiast tego Malwarebytes wprowadza do komputera klienta 7-warstwową ochronę, zabezpieczającą go już na poziomie dostępu do sieci, a także wzmacniającą kody obronne aplikacji, na bieżąco badającą wrażliwość programów na ataki, weryfikującą zachowanie aplikacji oraz wykrywającą anomalie. Malwarebytes deklaruje blokowanie 8 milionów zagrożeń każdego dnia oraz 187 milionów skanów każdego miesiąca.

Safer-Networking (Irlandia) – właściciel marki Spybot Search&Destroy. Poza typowymi produktami antywirusowymi firma oferuje także oprogramowanie anti-beacon, które ma

chronić przed wyciekiem danych wrażliwych przez strony internetowe, a także przed pobieraniem szkodliwego oprogramowania przy okazji zapisywania plików cookies.

Symantec (USA) – jedna z największych firm sprzedających systemy ochrony przed złośliwym oprogramowaniem. Posiada ponad 13-procentowy udział w rynku globalnym (Statista 2020) oraz należy do listy Fortune 500. Swoje produkty wprowadza na rynek pod marką Norton. Jej główne segmenty to: ochrona w miejscu odbioru (Endpoint security), ochrona informacji (Information security) oraz bezpieczeństwo sieci (Web security), w ramach którego chroni zarówno przed dostaniem się złośliwego oprogramowania jeszcze na poziomie przeglądarki, jak i skanuje maile w poszukiwaniu zagrożeń.

Webroot (USA) – firma sprzedająca oprogramowanie antywirusowe dla różnych kategorii klientów – od klientów detalicznych, po przemysłowych, właścicieli portali e-commerce i duże korporacje. W dziedzinie ochrony danych oferuje również skanowanie sieci WiFi pod kątem zagrożeń. Firma deklaruje obsługiwanie ponad 286 milionów urządzeń.

Kluczowi gracze rynku ochrony danych w chmurze

Niektóre firmy zajmujące się tradycyjną ochroną antywirusową zajmują się również zabezpieczeniami chmury i danych w niej przetwarzanych. W tym przypadku opisane zostały jedynie te firmy, które nie zostały przedstawione w części dotyczącej systemów anti-malware. Poniżej przedstawiono kluczowych graczy ww. rynku:

CISCO (USA) – globalna korporacja o szczególnych osiągnięciach w rozwiązaniach typu wielochmurowych (tworzących system z więcej niż jednej chmury), jak i tworzeniem skutecznych powiązań między poszczególnymi ich modułami, optymalizacją kosztów w ramach zasobów pracy wirtualnej, a także automatyzacją procesów wdrażania, by wyeliminować „czynnik ludzki”.

CloudPassage (USA) – firmę wyróżniają przede wszystkim mechanizmy monitorowania dostępności plików dla użytkowników, przydatne szczególnie w sieciach korporacyjnych oraz do śledzenia czy wybrane pakiety danych nie wykraczają poza zasięg określony przez politykę firmy.

Palo Alto Networks (USA) – firma wyspecjalizowana w przejęciach innych graczy rynkowych, w celu adaptacji ich rozwiązań do własnego oprogramowania Prisma Cloud. System ten zapewnia pakiet zarządzania podatnością oraz ochronę w trakcie pracy. Firma deklaruje obsługiwanie ponad 85 tys. klientów i obecność w ponad 150 krajach i terytoriach.

Qualys (USA) – firma wyspecjalizowana w skanowaniu sieci połączeń pod kątem podatności na zagrożenia, ale też zgodności ze standardami bezpieczeństwa za pomocą modułu zgodności PCI-DSS.

Tenable (USA) – posiada w swojej ofercie usługi z zakresu skanowania aplikacji sieciowych, a także zarządzania zasobami elektronicznymi. Oprogramowanie firmy potrafi rozpoznawać ważne zasoby/ dane i przekładać na nie większe wysiłki ochronne, w tym również „na żywo”

podczas wykrycia ataku. Moduł naprawczy pozwala również na identyfikację potencjalnych błędów ludzkich (np. złego umieszczenia plików) i ich poprawę.

TrendMicro (Japonia) – firma oferująca kompleksową platformę integrującą procesy zarządzania nakładami pracy, bezpieczeństwa sieci, przestrzeni przechowawczej oraz weryfikacji zgodności z normami. Platforma ma również możliwość wykrywania i zabezpieczania luk w strukturach IT oraz szyfrowania konkretnych zasobów.

VMware (USA) – jeden z liderów rynku zarządzania chmurą, firma skupiająca się na rozwiązaniach zapewniających bezpieczeństwo chmur korporacyjnych o dużych zasobach danych. System rozwijany przez VMware rozpoznaje również niebezpieczeństwa związane z powiązaniem zasobów zapisanych w chmurze z zewnętrznymi systemami.

Zscale (USA) – firma wyspecjalizowana w rozwiązaniach typu „zero-trust" (nie przepuszczającej nikogo, ani żadnego kodu bez weryfikacji), a także w usługach z zakresu umożliwiania zarówno szybkiej, jak i bezpiecznej pod względem danych pracy zdalnej, modernizacji chmurowej infrastruktury, jak i całkowitego przeorganizowywania architektury bezpieczeństwa firm.

Kluczowi gracze rynku bezpieczeństwa Internetu Rzeczy (IoT)

Internet Rzeczy staje się coraz ważniejszym aspektem życia społecznego i gospodarczego. Poza rozwiązaniami dla gospodarstw domowych z sektora elektroniki użytkowej, w błyskawicznym tempie rozwijają się zastosowania przemysłowe, a także z dziedziny bezpieczeństwa, nadzoru nad miastami (tzw. Smart Cities) oraz danych w chmurze. Przykładowo firma Intel zaprojektowała systemy automatyzacji produkcji dla fabryk samochodów Audi, a IBM tworzy interfejsy do zarządzania posiadanymi przez użytkownika urządzeniami. Dla branży Internetu Rzeczy szczególnie istotne jest bezpieczeństwo tworzonych systemów, gdzie ewentualny udany atak zagraża nie tylko oprogramowaniu, ale także wszystkim podłączonym urządzeniom. Poniżej przedstawiono kluczowych graczy ww. rynku:

Forescout (USA) – firma projektująca systemy nieustannego skanowania i weryfikacji urządzeń w ramach Internetu Rzeczy, a także samo oprogramowanie chroniące kody urządzeń i ich powiązania. Poza tym w ofercie Forescout znajdują się rozwiązania z takich obszarów jak segmentacja sieci, kontrola dostępu czy ograniczanie widoczności poszczególnych urządzeń. Do produktów firmy należą: EyeSight, czyli działający w tle program badający wiarygodność podłączonych do sieci urządzeń, EyeInspect, klasyfikujący podłączone urządzenia pod kątem ryzyka naruszenia bezpieczeństwa oraz EyeSegment, rozdzielający sieci urządzeń na mniejsze systemy, by zredukować ryzyko ataku.

Mocana (USA) – firma wyspecjalizowana w trzech obszarach zabezpieczania Internetu Rzeczy, w każdym poprzez dedykowane oprogramowanie. Pierwszym z nich jest TrustCenter, które jest odporną na udział osób trzecich platformą chmurową dla pracy urządzeń IoT, zintegrowaną z procesami uwierzytelniania i certyfikacji. Oprócz powyższych, usługa daje także wygodny dla użytkownika interfejs i system zarządzania urządzeniami.

Kolejny produkt to TrustEdge, obserwuje w czasie rzeczywistym zachowanie oprogramowania IoT i samych urządzeń, szyfruje przepływy danych między nimi i prowadzi procesy uczenia maszynowego. Trzecim jest TrustCore, platforma dla developerów sieci IoT, pozwalająca na dostosowywanie mechanizmów prywatności, zabezpieczeń oraz zgodności, bez konieczności budowania całego systemu od podstaw.

Rapid7 (USA) – firma notowana na giełdzie NASDAQ, projektująca rozwiązania z dziedziny analizy zabezpieczeń chmury oraz integrująca proces wbudowywania zabezpieczeń już na etapie projektowania samych systemów IoT, tak by były one jak najlepiej zintegrowane z konkretną siecią urządzeń. Usługi Rapid7 skupiają się na procesie produkcyjnym urządzeń i systemów IoT.

Kluczowi gracze rynku cyberbezpieczeństwa infrastruktury krytycznej

Infrastruktura krytyczna reprezentuje urządzenia i sieci urządzeń, które umożliwiają konsumentom korzystanie z podstawowych dóbr i systemów ułatwiających im życie – wśród głównych należy wymienić m.in. rozdzielnie energetyczne, węzły wodociągowe, elektrociepłownie, elektrownie, systemy kanalizacji i uzdatniania wody, a także porty i stacje benzynowe. Wraz z coraz większą automatyzacją i uzależnieniem wszystkich tych niezbędnych elementów infrastruktury od systemów komputerowych, wzrastają obawy o ich bezpieczeństwo wobec ataków cyberprzestępców i działania wrogiego oprogramowania. Poniżej przedstawiono kluczowych graczy ww. rynku:

APC by Schneider Electric (USA) – firma założona w pierwszej połowie lat 80 XX w., zajmuje się rozwiązaniami infrastrukturalnymi z zakresu energetyki. APC opracowała system zarządzania infrastrukturą w przemyśle (wykorzystujący rozszerzoną rzeczywistość), działający pod marką EcoStruxure. Poza tym firma oferuje wielowarstwowy system ochrony przed zagrożeniami generowanymi przez złośliwe oprogramowanie i bezpośrednie ataki na centra przemysłowe – do czego wykorzystuje model Cybersecurity Lifecycle Portfolio, w którym na każdym etapie wdrażania technologii (i jej późniejszego wykorzystania) wykonywana jest ocena podatności na ataki w przestrzeni cyfrowej.

BAE Systems (Wielka Brytania) – głównym segmentem działalności firmy jest bezpieczeństwo infrastruktury, przy czym firma specjalizuje się przede wszystkim w zabezpieczeniach infrastruktury publicznej/ krytycznej. Poza usługami w rodzaju dostosowanego pod działalność klienta firewallu czy systemu zarządzania niepożądanymi zdarzeniami, firma oferuje także doradztwo w dziedzinie cyberbezpieczeństwa dla instytucji publicznych i administracyjnych. Ma w swojej ofercie także tzw. „wywiad zagrożeń", posiłkujący się bazą potencjalnie niebezpiecznych użytkowników cyfrowych i oceniający, które elementy infrastruktury mogą przyciągać cyberataki i dlaczego (analogicznie do wywiadów wojskowych) oraz testy penetracyjne, czyli wypuszczanie do systemu oprogramowania zachowującego się podobnie do faktycznego malware, by sprawdzić, jak system zareaguje i czy zachowa się odpowiednio do zagrożenia.

IronNet (USA) – firma wyspecjalizowana w zabezpieczeniach infrastruktury przemysłowej i publicznej. Głównym produktem IronNet jest system analizy ruchu w sieci, który pozwala na szybką odpowiedź na zagrożenie oraz informuje podobne placówki o ryzyku ataku. Współpracuje z konglomeratem Raytheon nad nowymi rozwiązaniami dla systemów OT/IT, czyli wiążących technologię operacyjną (produkcyjno-usługową) z technologią informacyjną.

Thales Group (Francja) – firma znana z wytwarzania systemów dla wojska i instytucji rządowych, zajmująca się równie profesjonalnie ochroną infrastruktury krytycznej. Do rozwiązań oferowanych przez spółkę należy otwarta platforma cyfrowa, dająca możliwość automatyzacji procesów ochrony infrastruktury oraz system zarządzania niepożądanymi zdarzeniami. Inną z usług jest odporna na ataki chmura z modułem analizy danych, która pozwala na skupienie narzędzi ochronnych w jednym miejscu.

Kluczowi gracze rynku bezpieczeństwa sieci

Sieci wewnętrzne firm, korporacji, agencji rządowych i pozarządowych są szczególnie narażone na ataki, ze względu na poufne dane przetrzymywane na lokalnych serwerach i dyskach. Narażone są także sieci komórkowe, przez które w ciągu doby przepływają miliony rekordów zawierających załączniki, metadane i hiperlinki. Oprócz sieci przemysłowych, korporacyjnych, wojskowych i rządowych, do podstawowych zaliczają się także sieci uniwersyteckie i szkolne. Poniżej przedstawiono kluczowych graczy ww. rynku:

Anam Technologies (Szwajcaria) – firma skupiająca swoją działalność na ochronie przesyłu wiadomości, w ramach sieci komórkowych. Świadczy usługi dla ponad 170 operatorów telefonii komórkowej. Posiada oprogramowanie zabezpieczające i analizujące pod kątem zagrożeń duże paczki danych, zawierające wiadomości SMS, MMS oraz dane użytkowników.

Cellusys (Irlandia) – analogicznie do Anam Technologies skupia się na ochronie wiadomości, zabezpieczając zarówno odbiorców, jak i podmioty/ sieć przez którą konkretna wiadomość dociera do adresatów. Oferowana przez firmę ochrona wykorzystuje protokół krzyżowy - poszczególne segmenty komunikują się ze sobą nawzajem, odsyłając dane do tego, który jest w stanie rozpoznać rodzaj zagrożenia.

TATA Communications (Indie) – firma informatyczno-telekomunikacyjna, spółka-córka technologiczno-przemysłowej grupy kapitałowej TATA. W ramach swoich usług przedsiębiorstwo oferuje zintegrowany pakiet ochronny, nakładający na sieci kilka warstw zabezpieczeń, w tym firewall, IDPS (system monitorujący ruch na stronie i na bieżąco sprawdzający go pod kątem potencjalnych zagrożeń) oraz filtrowanie sieciowe. Oprogramowanie firmy bazuje na polityce „zero trust", gwarantując, że każda dana przepływająca przez sieć jest poddawana weryfikacji pod kątem złośliwego kodu.

Przedsiębiorstwa wielobranżowe

Poniżej przedstawiono przedsiębiorstwa, których rozwiązania nie kwalifikują się wyłącznie do jednej z ww. specjalizacji w ramach cyberbezpieczeństwa. Część z nich to konglomeraty o silnej

dywersyfikacji portfela produktów i usług, pozostałe zaś w głównej mierze opracowały rozwiązania o szerszym zastosowaniu i z tego powodu niemożliwe jest ich zakwalifikowanie do wyłącznie jednego segmentu podmiotów. Poniżej przedstawiono kluczowych graczy tego typu:

- **Broadcom** (USA) – kolejna z firm projektujących zintegrowane rozwiązania zabezpieczeń. Jej „tarcza bezpieczeństwa" chroni przed zewnętrznymi i wewnętrznymi zagrożeniami za pośrednictwem zarówno wbudowanych w sprzęt modułów zabezpieczających, jak i ochrony urządzeń, danych, tożsamości, płatności, informacji i sieci za pośrednictwem oprogramowania.

- **CrowdStrike** (USA) – posiada w swojej ofercie oprogramowanie z zakresu bezpieczeństwa chmurowego, ochrony danych osobowych i wywiadu zagrożeń. Świadczy też usługi w dziedzinie rozpoznawania podatności oraz testów penetracyjnych.

- **Fortinet** (USA) – oferuje usługi zarówno dla małych, jak i dużych przedsiębiorstw. Świadczy je w segmentach ochrony sieci, automatyzacji oprogramowania w przedsiębiorstwach produkcyjnych, bezpieczeństwa chmury i aplikacji, zabezpieczeń dostępu, jak i analizy zagrożeń (w tym z wykorzystaniem AI).

- **KnowBe4** (USA) – firma oferująca szkolenia dotyczące bezpieczeństwa sieci, także w formie próbnych ataków czy uświadamiania na temat phishingu, jak również testów penetracyjnych na pracownikach oraz weryfikowania stopni zabezpieczenia sieci. Oferuje również narzędzia dla firm pozwalające weryfikować poziom świadomości pracowników o zagrożeniach w IT oraz sprawdza ich poziom gotowości na ewentualne ataki cyberprzestępców.

- **Okta** (USA) – zajmuje się głównie kwestiami dotyczącymi uwierzytelniania i zarządzania dostępem do sieci oraz poszczególnych danych. Oferuje produkty między innymi dotyczące bezpiecznej chmury, zaawansowanego dostępu do serwerów czy zarządzania danymi użytkowników. Posiada w swoim portfolio także rozwiązania ułatwiające bezpieczną pracę z domu, model dostępowy „zero-trust", integracji aplikacji czy modernizacji infrastruktury.

- **One Trust** (USA) – skupia swoją działalność na zarządzaniu prywatnością w Internecie, ale też ocenie ryzyka tkwiącego w zaangażowaniu osób trzecich, audytu systemów bezpieczeństwa, ochrony danych i zarządzania nimi. Świadczy także usługi z zakresu compliance światowych i regionalnych norm bezpieczeństwa sieciowego, prywatności i ochrony danych.

- **Splunk** (USA) – firma oferująca rozwiązania wielu problemów związanych z bezpieczeństwem w sieci, której oprogramowanie działa w formule ciągłego monitorowania bezpieczeństwa, wykrywania zagrożeń, ustalania zgodności ze standardami, badaniem niepożądanych zdarzeń i reakcji na nie. Oferta firmy skierowana jest do klientów korporacyjnych i dotyczy wszystkich aspektów ich działalności w Internecie, w tym rozwiązań chmurowych.

2.6. Otoczenie prawne i ochrona własności intelektualnej

W rozdziałach od 2.6.1 do 2.6.3 przedstawiona została analiza globalnego otoczenia prawnego, wstęp metodologiczny do analizy otoczenia patentowego oraz sama analiza otoczenia patentowego.

2.6.1. Analiza otoczenia prawnego

Wiele krajów stara się odpowiedzieć na ryzyka związane z cyberbezpieczeństwem tworząc odpowiednie regulacje. Zdecydowana większość jest jednak w fazie początkowej tego procesu. Jak podaje raport z badań Międzynarodowego Związku Telekomunikacyjnego z 2017 r., ze 193 państw członkowskich, 96 dopiero zaczyna wdrażać odpowiednie strategie dotyczące cyberbezpieczeństwa[9].

Międzynarodowym aktem związanym z cyberbezpieczeństwem jest Konwencja Rady Europy o Cyberprzestępczości z dnia 23 listopada 2001 roku[10]. Konwencja dotyczy przestępstw popełnianych za pośrednictwem Internetu i innych sieci komputerowych, w szczególności naruszeń praw autorskich, oszustw komputerowych, pornografii dziecięcej oraz naruszeń bezpieczeństwa sieci. Sygnatariuszami Konwencji są kraje europejskie, jak również kraje spoza Europy, w tym USA czy Japonia.

W USA już od wielu lat tworzone są akty prawne związane z cyberbezpieczeństwem. Jednym z najstarszych takich aktów jest the Federal Computer Fraud and Abuse Act z 1986 r.[11] (dalej: **CFFA**). W 2018 r. wydano Cyberstrategię Departamentu Obrony[12], gdzie podkreśla się, że USA są zaangażowane w długoterminową strategiczną konkurencję z Chinami i Rosją. Uznano, że państwa te, szczególnie aktywne w cyberprzestrzeni, stanowią ryzyko strategiczne dla USA i ich sojuszników. USA nie ma jednolitej i wspólnej dla całego kraju legislacji w zakresie cyberprzestrzeni, ponieważ obowiązuje równolegle prawo federalne, stanowe i miejscowe

---

[9] Global Cybersecurity Index (GCI) 2017, the International Telecommunication Union (ITU), ISBN 978-92-61-25071-3.

[10] Konwencja Rady Europy o cyberprzestępczości ratyfikowana w Polsce Ustawą o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. (Dz.U. z 2014 r. poz. 1514).

[11] The Federal Computer Fraud and Abuse Act, 1986, https://doi.org/10.1145/356678.356682. Dostęp: 27.10.2021.

[12] Departament of Defense, Cyber Strategy 2018, https://doi.org/10.1145/356678.356682. Dostęp: 27.10.2021.

wzbogacone o system precedensowy. Najpoważniejsze cyberprzestępstwa reguluje prawo federalne, a konkretnie CFAA. W ustawach szczegółowych zostały uregulowane kwestie bezpieczeństwa danych[13] czy ochrony praw konsumenta[14]. W obszarze incydentów cyberbezpieczeństwa popularne są rekomendacje NIST 800-61[15].

Federacja Rosyjska w maju 2009 r. zatwierdziła Narodową Strategię Bezpieczeństwa Federacji Rosyjskiej do 2020 r. Dokument wskazuje cele strategiczne w polityce krajowej i międzynarodowej i wymienia m.in. zagrożenia cybernetyczne w obszarze nowych technologii[16]. Podmioty wchodzące w skład rosyjskiej krytycznej infrastruktury informatycznej są zobowiązane do przestrzegania obowiązków w zakresie bezpieczeństwa cybernetycznego i informowania o naruszeniach. Wynika to z federalnej ustawy o bezpieczeństwie krytycznej infrastruktury informacyjnej Federacji Rosyjskiej (187-FZ z 2017 r.). Ustawa reguluje sposób ochrony danych przez krajowych i zagranicznych operatorów z sektora usług finansowych, telekomunikacji i wielu innych sektorów.

Chiny przyjęły 7 listopada 2016 r. ustawę o cyberbezpieczeństwie, która weszła w życie w czerwcu 2017 r. Uzasadnieniem tej ustawy miał być wzrost cyberzagrożeń, czyli włamań i terroryzmu[17]. Chińska ustawa zawiera liczne obowiązki cenzurowania informacji. Ustawa ogranicza anonimowość w cyberprzestrzeni przez nałożenie obowiązku podania prawdziwego imienia, nazwiska i danych osobowych. Ponadto ustawa nakłada na krytycznych operatorów infrastruktury informatycznej obowiązek zapisywania informacji osobistych i ważnych danych biznesowych w Chinach. Zgodnie z tym obowiązkiem firmy są zobowiązane monitorować i raportować dla rządu niezidentyfikowane incydenty bezpieczeństwa sieci oraz zapewnić nieokreśloną pomoc techniczną dla agencji obrony.

Ryzyka związane z cyberbezpieczeństwem dotyczą również danych osobowych. Nie ma globalnych regulacji w tym zakresie, stąd konieczna jest każdorazowa analiza krajowych regulacji prawnych przed rozpoczęciem działalności na danym terytorium. 27 września 2021 r. doszło do istotnej zmiany podstaw prawnych transferu danych osobowych do państwa trzeciego, tj. poza Europejski

---

[13] The Cybersecurity Information Sharing Act, 2015, https://www.congress.gov/bill/113th-congress/senate-bill/2588. Dostęp: 27.10.2021.

[14] The Consumer Privacy Protection Act of 2015, https://www.congress.gov/bill/114th-congress/senate-bill/1158/text. Dostęp: 27.10.2021.

[15] Rekomendacje National Institute of Standards and Technology, U.S. Department of Commerce, NIST 800-61, rev. 2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Dostęp: 27.10.2021.

[16] Russia's National Security Strategy to 2020, 12 maja 2009, nr 537, https://www.files.ethz.ch/isn/154915/Russia%E2%80%99s%20National%20Security%20Strategy%20to%202020%20-%20Rustrans.pdf. Dostęp: 27.10.2021.

[17] https://www.theguardian.com/world/2016/nov/07/chinas-new-cybersecurity-law-sparks-fresh-censorship-and-espionage-fears. Dostęp: 27.10.2021.

Obszar Gospodarczy, np. do USA. Z tym dniem przestały obowiązywać decyzje Komisji Europejskiej dotyczące transferów danych osobowych do państwa trzeciego, zastąpione decyzją Komisji UE nr 2021/914[18] z dnia 4 czerwca 2021 r. Oparcie transferów na podstawie klauzul dołączonych do tej decyzji umożliwia przekazanie danych osobowych do państwa trzeciego bez spełnienia dodatkowych wymogów.

Podstawowymi, międzynarodowymi aktami prawnymi dotyczącymi ochrony prawa własności przemysłowej i intelektualnej jest Konwencja paryska o ochronie własności przemysłowej[19] oraz Porozumienie w sprawie Handlowych Aspektów Praw Własności Intelektualnej (TRIPS)[20], które dają wytyczne do ochrony własności przemysłowej i intelektualnej. Międzynarodowa ochrona patentowa regulowana jest przez Układ o współpracy patentowej (PCT)[21], dzięki któremu dokonując jednego międzynarodowego zgłoszenia patentowego w ramach PCT zgłaszający mogą jednocześnie ubiegać się o ochronę wynalazku w ponad 150 krajach. Międzynarodowa ochrona znaków towarowych możliwa jest na podstawie madryckiego systemu ochrony znaków towarowych[22], dzięki któremu na podstawie jednego zgłoszenia można ubiegać się o uzyskanie ochrony w ponad 120 krajach. Natomiast haski system międzynarodowej rejestracji wzorów przemysłowych[23] zapewnia praktyczne rozwiązanie umożliwiające rejestrację wzorów w 92 krajach poprzez dokonanie jednego zgłoszenia międzynarodowego. Przed skorzystaniem z procedur

---

[18] Decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 4 czerwca 2021 r. (Dz. Urz. UE. L Nr 199, str. 31).

[19] Konwencja paryska o ochronie własności przemysłowej z dnia 20 marca 1883 r. zmieniona w Brukseli dnia 14 grudnia 1900 r., w Waszyngtonie dnia 2 czerwca 1911 r., w Hadze dnia 6 listopada 1925 r., w Londynie dnia 2 czerwca 1934 r., w Lizbonie dnia 31 października 1958 r. i w Sztokholmie dnia 14 lipca 1967 r. - Akt sztokholmski z dnia 14 lipca 1967 r. (Dz. U. z 1975 r. Nr 9, poz. 51).

[20] Porozumienie w sprawie Handlowych Aspektów Praw Własności Intelektualnej z dnia 22 grudnia 1994 r. (ang. Agreement on Trade-Related Aspects of Intellectual Property Rights, TRIPS) – załącznik do porozumienia w sprawie utworzenia Światowej Organizacji Handlu (WTO) (Dz. Urz. UE. L Nr 336, str. 214).

[21] Układ o współpracy patentowej sporządzony w Waszyngtonie dnia 19 czerwca 1970 r., poprawiony dnia 2 października 1979 r. i zmieniony dnia 3 lutego 1984 r. (Dz.U.1991.70.303).

[22] Porozumienie madryckie o międzynarodowej rejestracji znaków. 1891.04.14. (Dz.U.1993.116.514) oraz Protokół do Porozumienia madryckiego o międzynarodowej rejestracji znaków. Madryt dnia 27 czerwca 1989 (Dz.U.2003.13.129).

[23] Akt genewski Porozumienia haskiego w sprawie międzynarodowej rejestracji wzorów przemysłowych. Genewa.1999.07.02. (Dz.U.2009.198.1522 z dnia 2009.11.26)).

międzynarodowych konieczne jest dokonanie krajowego lub regionalnego zgłoszenia praw własności przemysłowej.

2.6.2. Wprowadzenie metodologiczne do analizy otoczenia patentowego

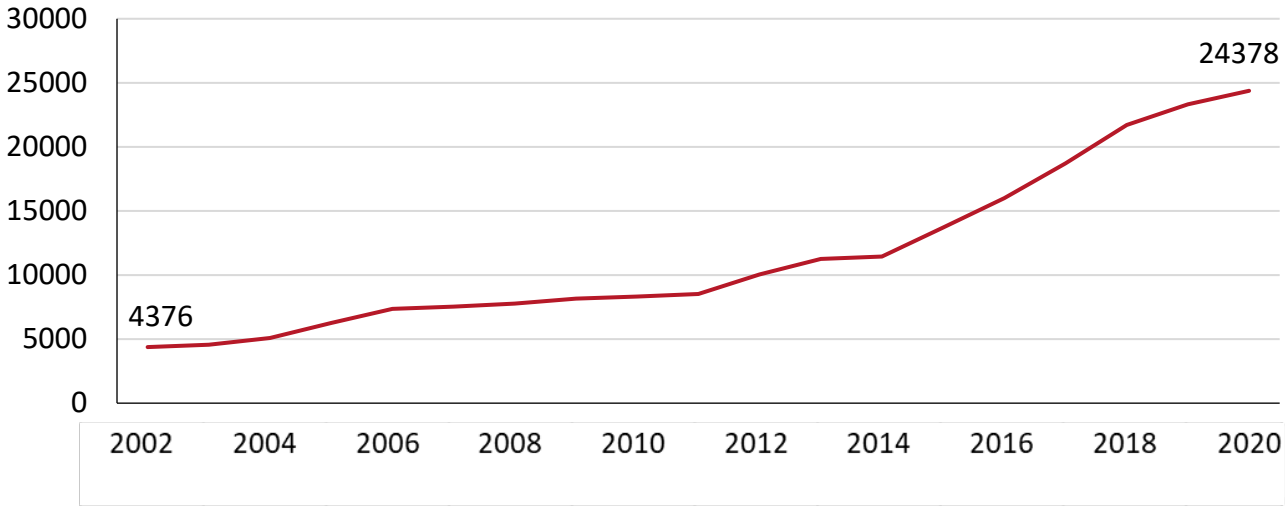
Aby przystąpić do analizy otoczenia patentowego, należy dokonać wprowadzenia metodologicznego. Źródłem prezentowanych danych jest badanie własne na podstawie danych z bazy Derwent Innovation[24]. Zgłoszenia patentowe publikowane są po 18 miesiącach od daty pierwszeństwa do uzyskania patentu, do tego czasu są tajne, o ile zgłaszający nie złoży wniosku o wcześniejszą publikację (co ma miejsce jedynie w nielicznych przypadkach). W związku z tym publikacje zgłoszeń patentowych np. w roku 2020 dotyczą zgłoszeń dokonanych w latach 2018 i 2019 (a zatem wynalazków dokonanych w tych latach).

2.6.3. Analiza otoczenia patentowego

Analiza otoczenia patentowego w dziedzinie cyberbezpieczeństwa wskazuje na bardzo szybki przyrost liczby wynalazków w tej dziedzinie, szybszy niż średnia dla innych dziedzin techniki. Od 20 lat z każdym kolejnym rokiem rośnie ilość zgłoszeń patentowych względem poprzedniego roku. W urzędach patentowych na całym świecie można zaobserwować ogólny wzrost liczby zgłoszeń z zakresu cyberbezpieczeństwa. Rysunek 5 prezentuje liczbę publikacji nowych rodzin patentowych (w skład jednej rodziny patentowej może wchodzić kilka dokumentów patentowych (zgłoszeń patentowych lub patentów), z jednego lub więcej krajów, dotyczących tego samego wynalazku) opublikowanych na świecie w latach 2002-2020, które dotyczyły szeroko pojętego aspektu cyberbezpieczeństwa. Analiza została przeprowadzona przy zastosowaniu następujących haseł: computer, network, security, cryptography (komputer, sieć, bezpieczeństwo, kryptografia).

[24] *Strona internetowa Clarivate: https://clarivate.com/derwent/solutions/derwent-innovation/. Dostęp: 12.10.2021.*

Rysunek 5. Roczna liczba opublikowanych nowych rodzin patentowych na świecie dotyczących cyberbezpieczeństwa (2002-2020)



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Widoczny jest systematyczny wzrost liczby rodzin patentowych publikowanych w kolejnych latach. Rozwiązania z zakresu cyberbezpieczeństwa przedstawiane są w dokumentach patentowych w różnych kontekstach. Ochroną objęte są przede wszystkich rozwiązania z zakresu sieci telekomunikacyjnych (klasa patentowa H04L), przetwarzania danych cyfrowych (klasa patentowa G06F), sieci bezprzewodowych (klasa patentowa H04W), różnorodnych zastosowań komercyjnych (klasa patentowa G06Q) oraz systemów telewizyjnych (klasa patentowa H04N).

W niniejszym badaniu poświęcono szczególną uwagę czterem obszarom powiązanym ze scenariuszami rozwoju cyberbezpieczeństwa, przedstawionymi dokładniej w rozdziale 5 ekspertyzy BTR. Obszary te to: cyberbezpieczeństwo jako usługa, kryptografia, przemysł 4.0 oraz sieci komputerowe, a w szczególności Internet of Things – IoT (Internet rzeczy). Obszary te zostały wskazane jako szczególnie interesujące dla polskich podmiotów ze względu na dostępne kompetencje i możliwości techniczne do ich realizacji. Biorąc pod uwagę publikacje dokumentów patentowych, wskazanie akurat tych obszarów należy uznać za słuszne, gdyż widoczna jest w nich (poza specyficznym obszarem przemysłu 4.0) w ostatnich latach jeszcze wyższa dynamika wzrostu niż dynamika odnotowana dla cyberbezpieczeństwa w ujęciu ogólnym (są to więc główne obszary napędowe wzrostu liczby publikacji dokumentów patentowych dla całego cyberbezpieczeństwa).

W każdym z tych obszarów opublikowano na świecie w ostatnim roku setki lub tysiące dokumentów patentowych (zgłoszeń patentowych i patentów):

- cyberbezpieczeństwo jako usługa – ponad 600 dokumentów patentowych;
- kryptografia – ponad 18 000 dokumentów patentowych;
- przemysł 4.0 – ponad 300 dokumentów patentowych;
- sieci komputerowe, IoT (Internet rzeczy) – ponad 11 000 dokumentów patentowych.

Podobnie jak w wielu innych dziedzinach, wiodącą rolę pod względem liczby zgłoszeń patentowych dokonanych w ciągu ostatnich trzech lat pełnią podmioty z Chin, a w szczególności największe chińskie korporacje (m.in. Tencent, Ping An Insurance, State Grid Corporation, Baidu, Huawei). Podmioty te dokonują zgłoszeń patentowych głównie w chińskim urzędzie patentowym, który obecnie publikuje kilkukrotnie więcej dokumentów patentowych od każdego z pozostałych urzędów własności intelektualnej w jakimkolwiek państwie. Chińskie dokumenty patentowe stanowią zatem obecnie istotne źródło informacji o najnowszych rozwiązaniach ze stanu techniki. Bazy informacji patentowych (chociażby ogólnodostępne bazy Espacenet czy Google Patents) pozwalają już na dostęp do tłumaczeń maszynowych tych dokumentów na język angielski.

Większość patentowanych rozwiązań z zakresu cyberbezpieczeństwa, w perspektywie globalnej (ale tym samym również na rynku chińskim, jako że ma on fundamentalny na niego wpływ), dotyczy programów komputerowych (oprogramowania), które albo stanowią istotny element większego systemu (zwłaszcza w powiazaniu z rozwiązaniami dla przemysłu 4.0), albo też są samodzielnymi rozwiązaniami, niezależnymi od warstwy sprzętowej (zwłaszcza w przypadku rozwiązań z zakresu kryptografii). Należy mieć na uwadze, że co do zasady wszystkie programy komputerowe powiązane z bezpieczeństwem mają zdolność patentową w większości urzędów krajowych na całym świecie. Europejski urząd patentowy uznaje takie rozwiązania za posiadające charakter techniczny, a urząd patentowy w USA – za rozwiązania nieabstrakcyjne (służące rozwiązaniu konkretnego problemu), mają więc one zdolność patentową (mimo częstych dyskusji na temat możliwości patentowania oprogramowania). Co szczególnie ważne dla polskiego obszaru cyberbezpieczeństwa, ze względu na charakter techniczny tego typu rozwiązań, nawet realizowane wprost jako programy komputerowe, od 2020 r. mają one zdolność patentową również przed krajowym urzędem patentowym.

Poniżej przedstawione są wyniki analiz przeprowadzonych dla wybranych obszarów badania technologii cyberbezpieczeństwa.

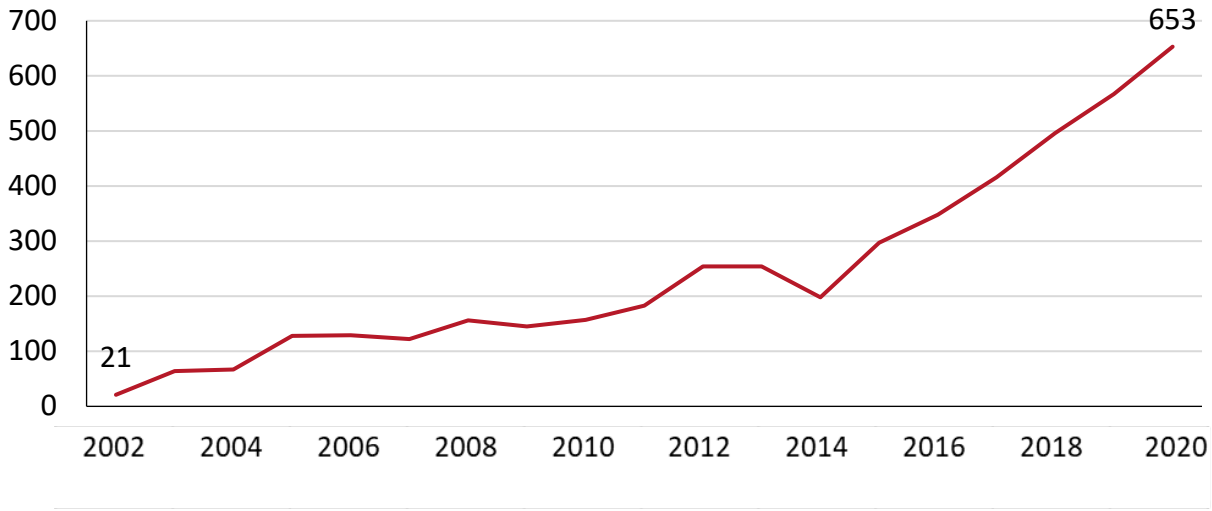
Obszar 1
Cyberbezpieczeństwo jako usługa

W ramach obszaru 1 wyselekcjonowano dokumenty patentowe (zgłoszenia patentowe i patenty), których skróty zawierały słowa „computer” (komputer), „security” (bezpieczeństwo) i „service” (usługa).

Zbadano dokumenty opublikowane w latach 2002-2020 (wcześniejsze nie mają istotnego znaczenia, gdyż ochrona ich już wygasła), nie ograniczając się przy tym terytorialnie – dokonano przeglądu dokumentów patentowych z całego świata.

Zidentyfikowano 7 829 dokumentów należących do 5 232 rodzin patentowych (w skład jednej rodziny patentowej może wchodzić kilka dokumentów patentowych, z jednego lub więcej krajów, dotyczących tego samego wynalazku). Liczba publikacji nowych rodzin patentowych w poszczególnych latach została zaprezentowana na Rysunku 6.

Rysunek 6. Roczna liczba publikowanych na świecie nowych rodzin patentowych w zakresie cyberbezpieczeństwa jako usługi (2002-2020)

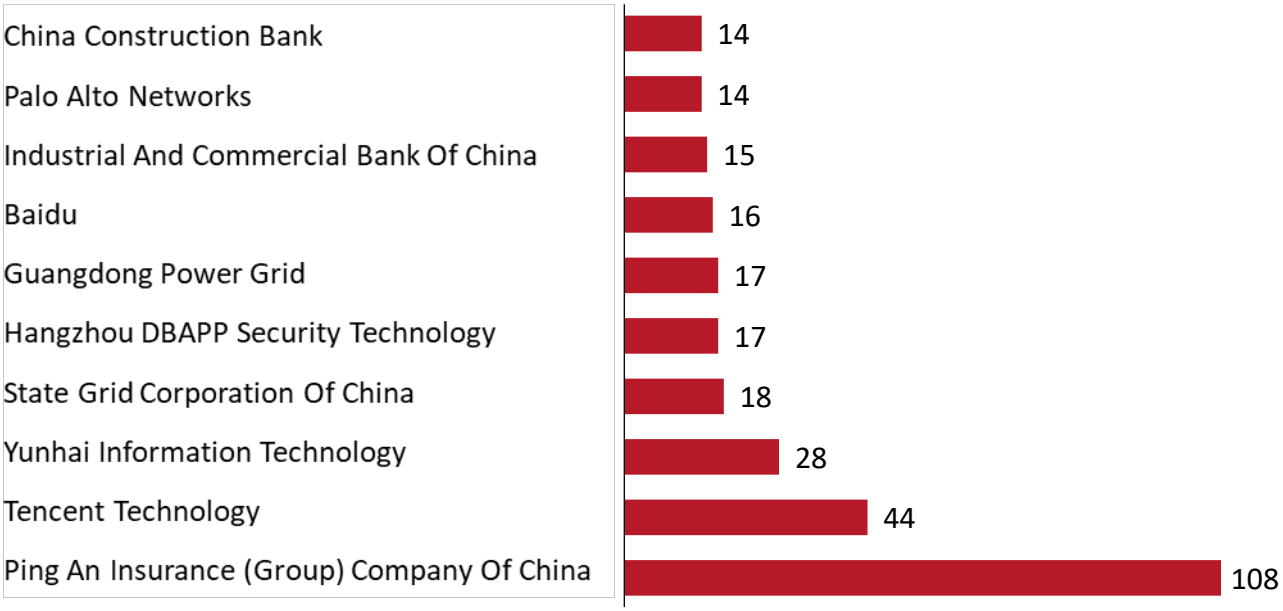


Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Z powyższego rysunku wynika, że badana dziedzina intensywnie się rozwija, widoczny jest stały coroczny przyrost liczby opracowywanych wynalazków.

Aby oszacować aktualne trendy w tej dziedzinie, przeanalizowano zgłoszenia patentowe dokonane i opublikowane w ciągu ostatnich 3 lat – grupa 1 328 publikacji rodzin patentowych. Najbardziej aktywne podmioty dokonujące zgłoszeń patentowych zostały zaprezentowane na Rysunku 7.

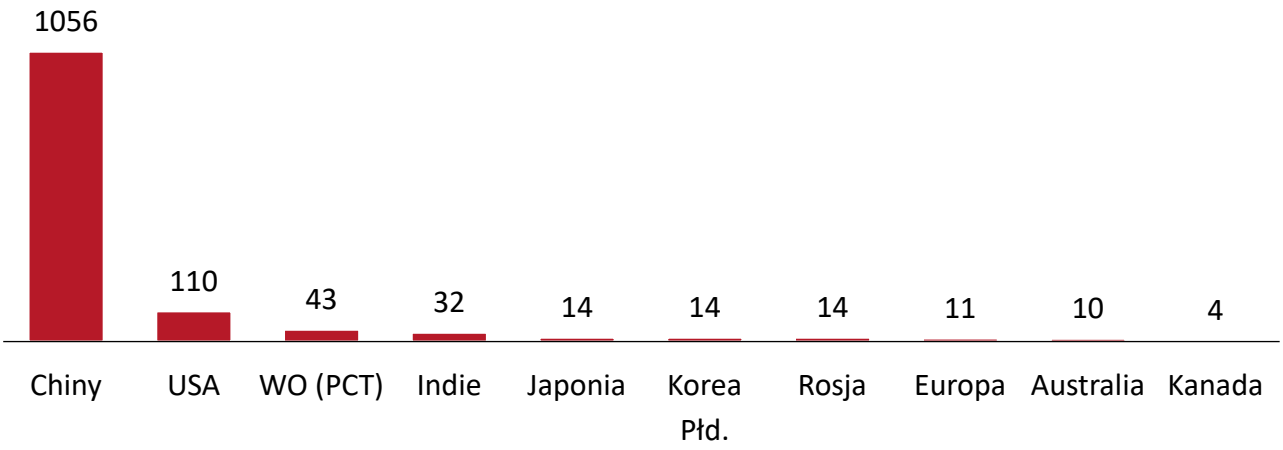
Rysunek 7. Podmioty z największą liczbą publikacji nowych rodzin patentowych w ciągu ostatnich 3 lat w zakresie cyberbezpieczeństwa jako usługi



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Liczba zgłoszeń patentowych dokonanych i opublikowanych w ciągu ostatnich 3 lat, w podziale na kraje, regiony lub zrzeszenia została zaprezentowana na Rysunku 8.

Rysunek 8. Kraje, regiony lub zrzeszenia z największą liczbą publikacji nowych rodzin patentowych w ciągu ostatnich 3 lat w zakresie cyberbezpieczeństwa jako usługi



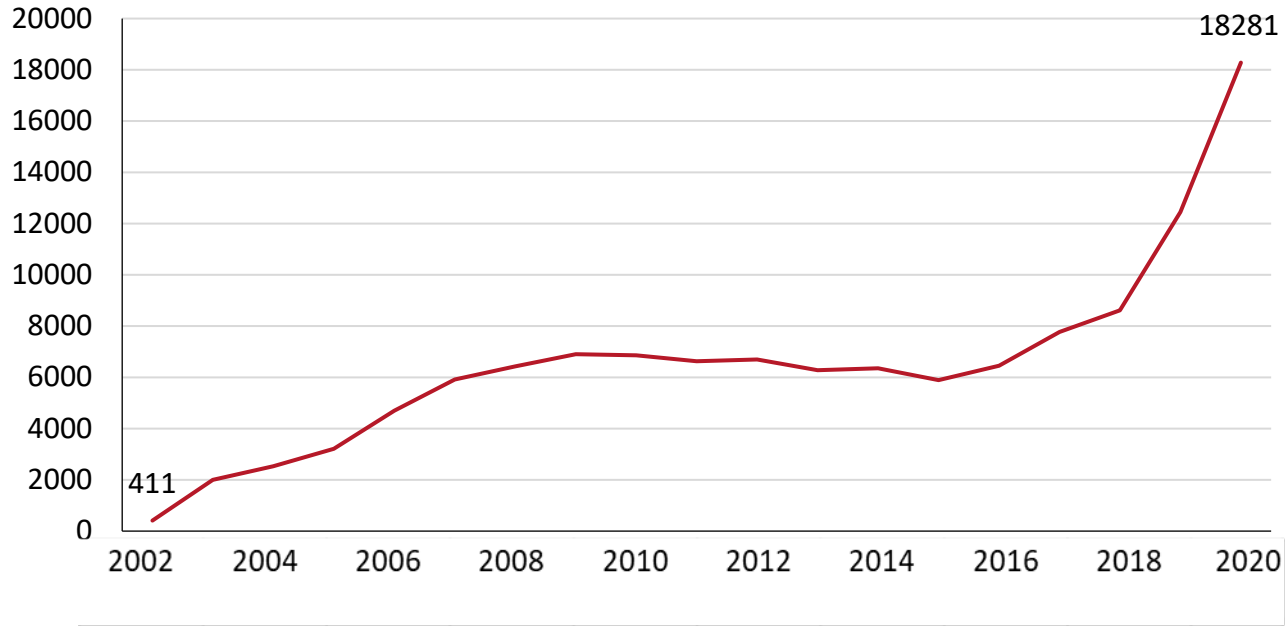
Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Obszar 2
Kryptografia

W ramach obszaru 2 wyselekcjonowano dokumenty patentowe (zgłoszenia patentowe i patenty) z klasy H04L9 (kryptografia). Zbadano dokumenty opublikowane w latach 2002-2020 (wcześniejsze nie mają istotnego znaczenia, gdyż ochrona ich już wygasła), nie ograniczając się przy tym terytorialnie – dokonano przeglądu dokumentów patentowych z całego świata.

Zidentyfikowano 393 552 dokumentów należących do 145 169 rodzin patentowych. Liczba opublikowanych nowych rodzin patentowych w poszczególnych latach została zaprezentowana na Rysunku 9 – który podkreśla, jak intensywnie rozwija się badana dziedzina, szczególnie w ostatnich latach (od 2016 roku).

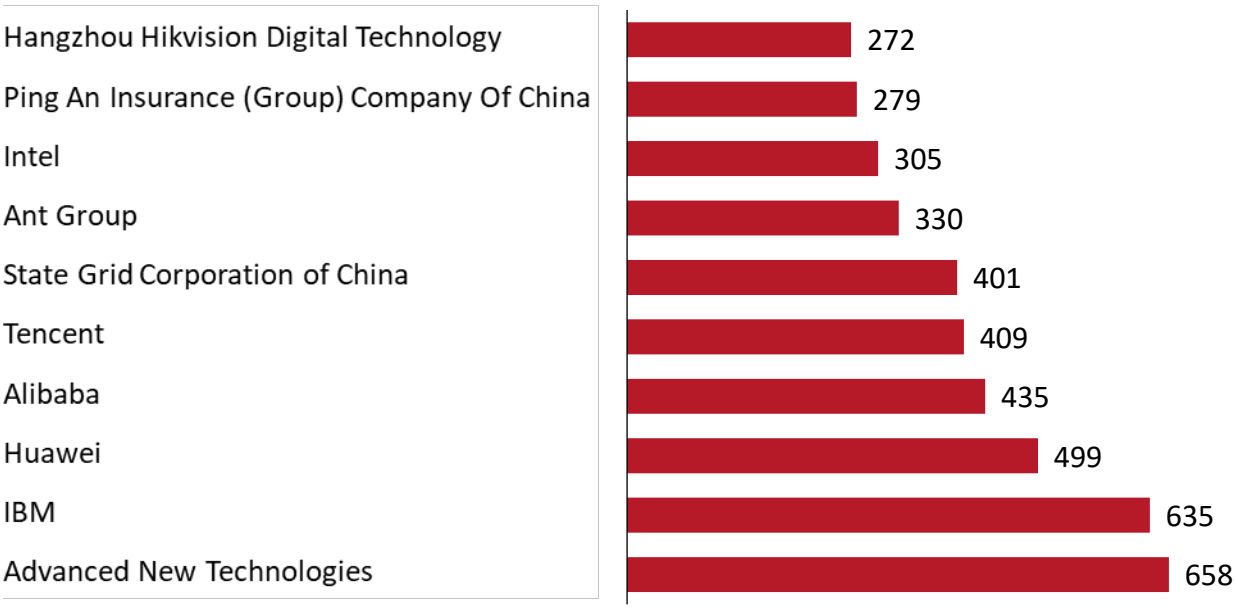
Rysunek 9. Roczna liczba publikowanych na świecie nowych rodzin patentowych w zakresie kryptografii (2002-2020)



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Aby oszacować aktualne trendy w tej dziedzinie, przeanalizowano zgłoszenia patentowe dokonane i opublikowane w ciągu ostatnich 3 lat – grupa 32 218 publikacji rodzin patentowych. Najbardziej aktywne podmioty dokonujące zgłoszeń patentowych zostały przedstawione na Rysunku 10.

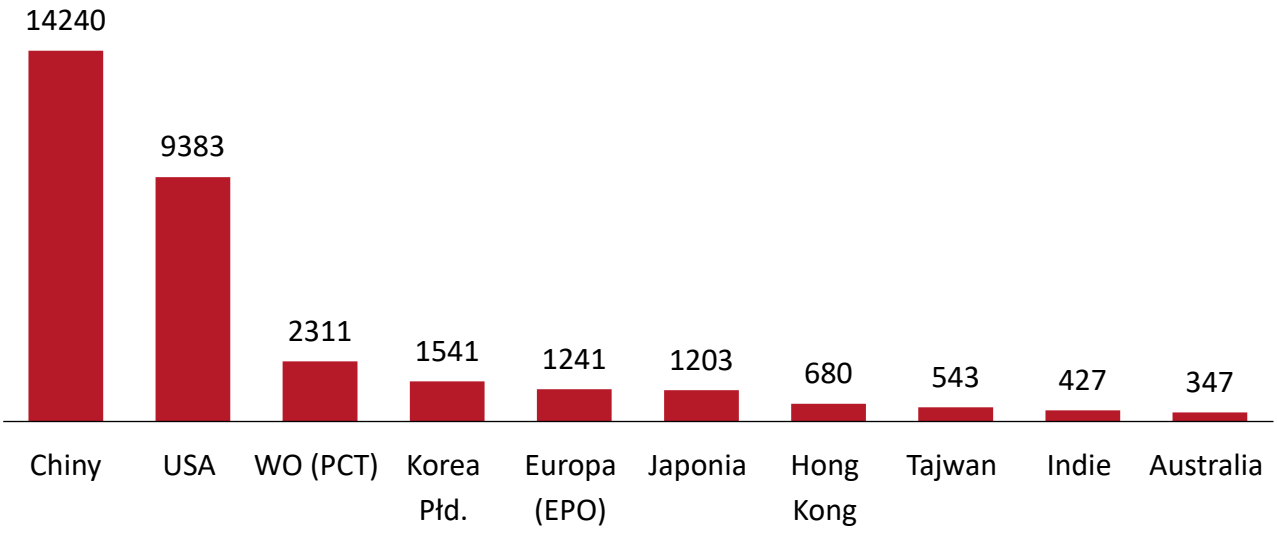
Rysunek 10. Podmioty z największą liczbą publikacji nowych rodzin patentowych w ciągu ostatnich 3 lat w zakresie kryptografii



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Liczba zgłoszeń patentowych dokonanych i opublikowanych w ciągu ostatnich 3 lat, w podziale na kraje, regiony lub zrzeszenia została zaprezentowana na Rysunku 11.

Rysunek 11. Kraje, regiony lub zrzeszenia z największą liczbą publikacji nowych rodzin patentowych w ciągu ostatnich 3 lat w zakresie kryptografii



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Obszar 3
Przemysł 4.0

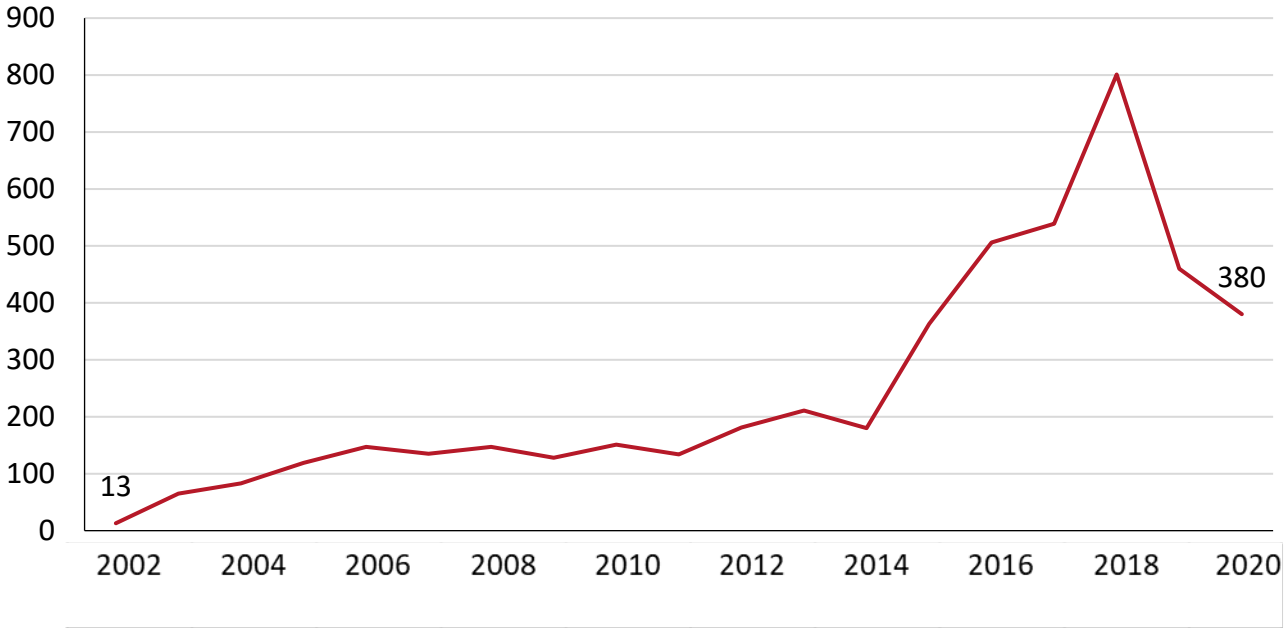
W ramach obszaru 3 wyselekcjonowano dokumenty patentowe (zgłoszenia patentowe i patenty), których skróty zawierają hasła computer, security (komputer, bezpieczeństwo) oraz następujące działy klasyfikacji patentowej: B (operacje, transport), C (chemia, metalurgia), D (tekstylia, papiernictwo), E (budownictwo), F (mechanika, oświetlenie). Dokumenty te dotyczą zatem kwestii bezpieczeństwa w różnych procesach przemysłowych.

Zbadano dokumenty opublikowane w latach 2002-2020 (wcześniejsze nie mają istotnego znaczenia, gdyż ochrona ich już wygasła), nie ograniczając się przy tym terytorialnie – dokonano przeglądu dokumentów patentowych z całego świata.

Zidentyfikowano 3 829 dokumentów należących do 3 074 rodzin patentowych. Liczba opublikowanych nowych rodzin patentowych w poszczególnych latach została zaprezentowana na Rysunku 12. W ostatnich latach trend wydaje się zanikać. Może to być związane z tym, że coraz więcej rozwiązań z zakresu cyberbezpieczeństwa projektowanych jest do wykorzystania

w szerokim zakresie i tak też jest chronionych – np. algorytmy kryptograficzne chronione są w zakresie zabezpieczania wszelkich danych, a nie tylko danych przemysłowych.

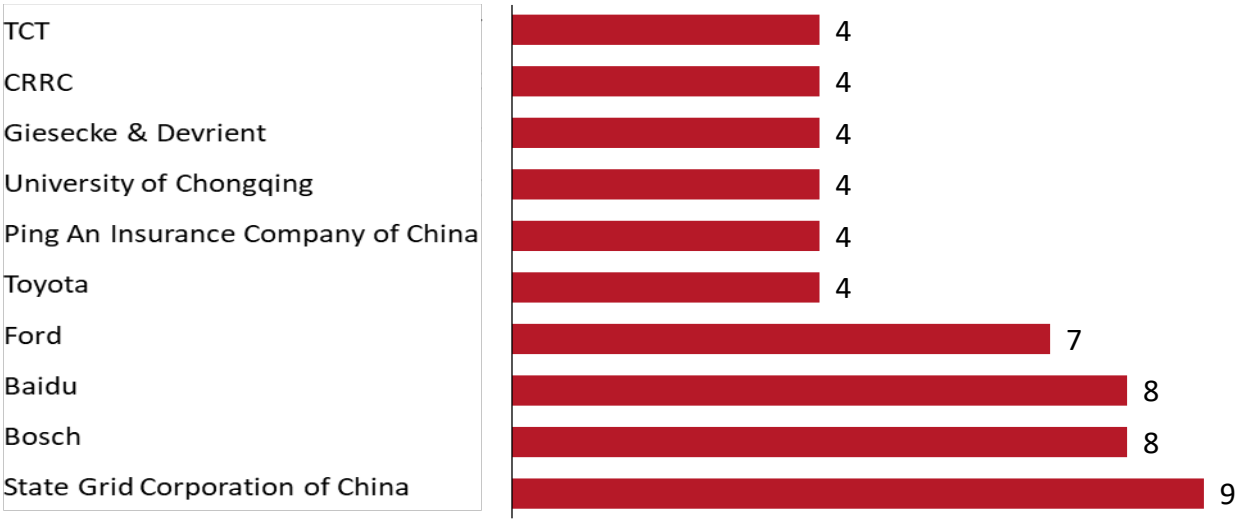
Rysunek 12. Roczna liczba publikowanych na świecie nowych rodzin patentowych w zakresie cyberbezpieczeństwa dla Przemysłu 4.0 (2002-2020)



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Aby oszacować aktualne trendy w tej dziedzinie, przeanalizowano zgłoszenia dokonane i opublikowane w ciągu ostatnich 3 lat – grupa 691 publikacji rodzin patentowych. Najbardziej aktywne podmioty dokonujące zgłoszeń patentowych zostały przedstawione na Rysunku 13.

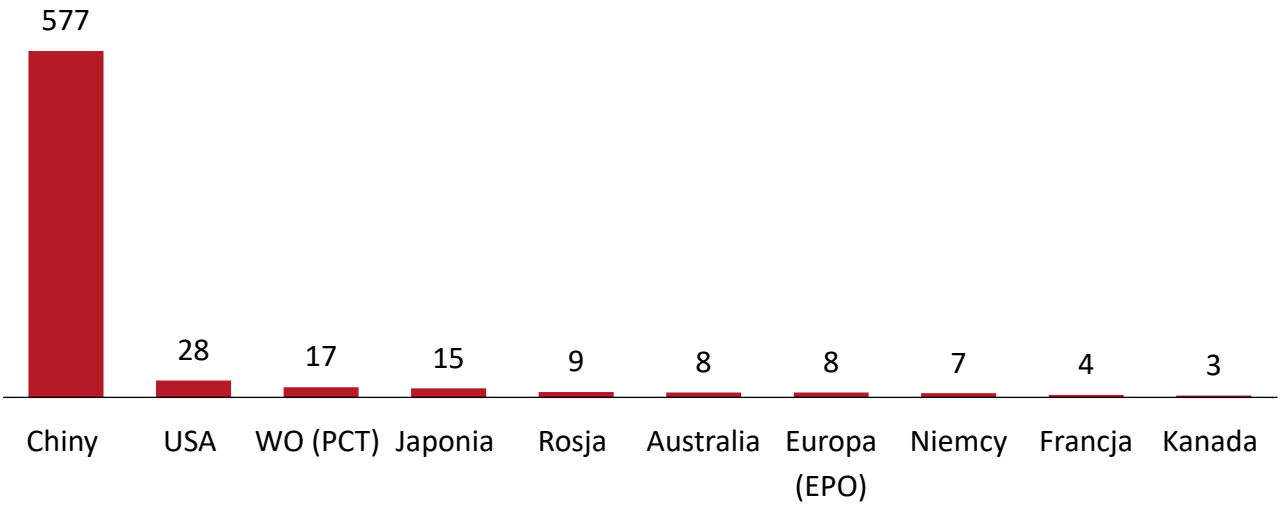
Rysunek 13. Podmioty z największą liczbą publikacji nowych rodzin patentowych w ciągu ostatnich 3 lat w zakresie cyberbezpieczeństwa dla Przemysłu 4.0



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Liczba zgłoszeń patentowych dokonanych i opublikowanych w ciągu ostatnich 3 lat, w podziale na kraje, regiony lub zrzeszenia została zaprezentowana na Rysunku 14.

Rysunek 14. Kraje, regiony lub zrzeszenia z największą liczbą publikacji nowych rodzin patentowych w ciągu ostatnich 3 lat w zakresie cyberbezpieczeństwa dla Przemysłu 4.0



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

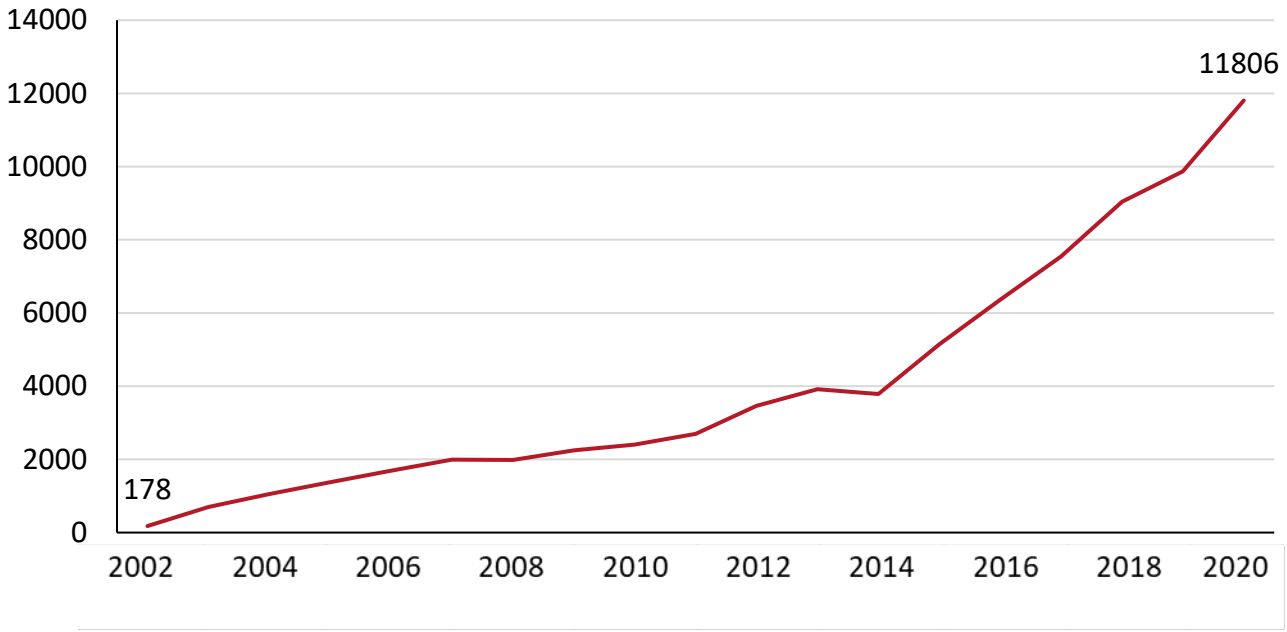
Obszar 4
Sieci komputerowe, IoT

W ramach obszaru 4 wyselekcjonowano dokumenty patentowe (zgłoszenia patentowe i patenty), których skróty zawierają słowa kluczowe: security, network/Internet (bezpieczeństwo, sieć/ Internet).

Zbadano dokumenty opublikowane w latach 2002-2020 (wcześniejsze nie mają istotnego znaczenia, gdyż ochrona ich już wygasła), nie ograniczając się przy tym terytorialnie – dokonano przeglądu dokumentów patentowych z całego świata.

Zidentyfikowano 138 617 dokumentów należących do 86 716 rodzin patentowych. Liczba opublikowanych nowych rodzin patentowych w poszczególnych latach została zaprezentowana na Rysunku 15.

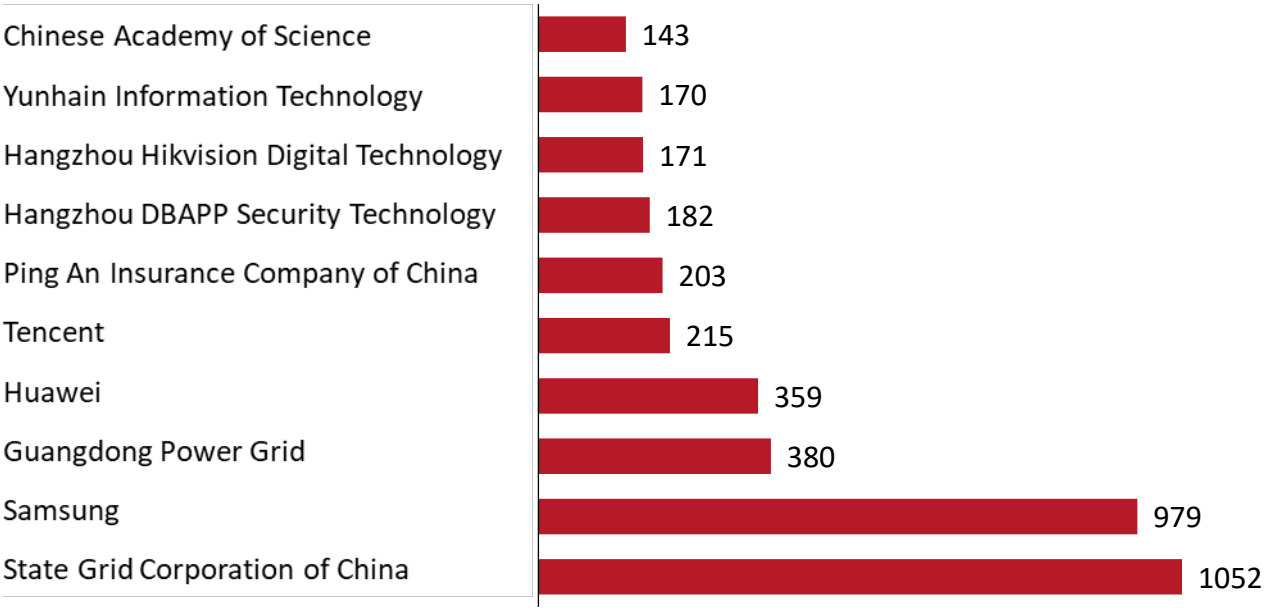
Rysunek 15. Roczna liczba publikowanych na świecie nowych rodzin patentowych w zakresie cyberbezpieczeństwa dla sieci komputerowych i IoT (2002-2020)



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Aby oszacować aktualne trendy w tej dziedzinie, przeanalizowano zgłoszenia patentowe dokonane i opublikowane w ciągu ostatnich 3 lat – grupa 22 688 publikacji rodzin patentowych. Najbardziej aktywne podmioty dokonujące zgłoszeń patentowych zostały przedstawione na Rysunku 16.

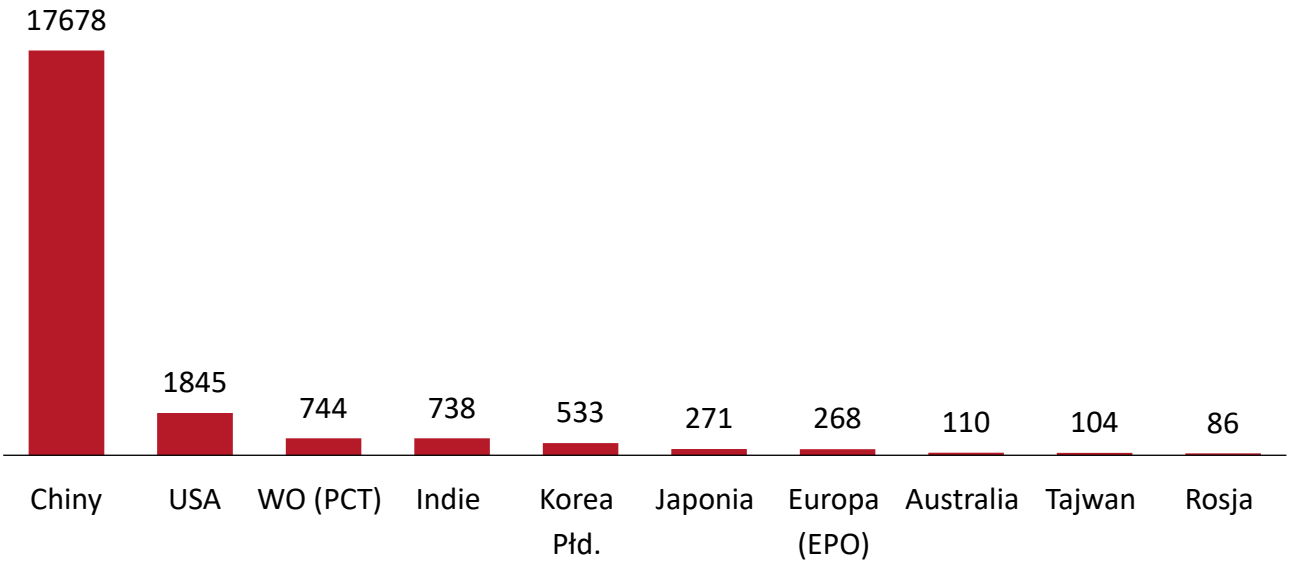
Rysunek 16. Podmioty z największą liczbą publikacji nowych rodzin patentowych w ciągu ostatnich 3 lat w zakresie cyberbezpieczeństwa dla sieci komputerowych i IoT



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Liczba zgłoszeń patentowych dokonanych i opublikowanych w ciągu ostatnich 3 lat, w podziale na kraje, regiony lub zrzeszenia została zaprezentowana na Rysunku 17.

Rysunek 17. Kraje, regiony lub zrzeszenia z największą liczbą publikacji nowych rodzin patentowych w ciągu ostatnich 3 lat w zakresie cyberbezpieczeństwa dla sieci komputerowych i IoT



Źródło: badanie własne na podstawie danych z bazy Derwent Innovation

Podsumowując, należy stwierdzić, że analiza otoczenia patentowego w dziedzinie cyberbezpieczeństwa wskazuje na szybki przyrost liczby wynalazków w tej dziedzinie, szybszy niż średnia dla innych dziedzin techniki. Co więcej, w badanym okresie, tj. w latach 2002 – 2020, z każdym kolejnym rokiem rośnie liczba zgłoszeń patentowych względem poprzedniego roku.

W ciągu ostatnich trzech lat większość zgłoszeń patentowych na świecie w dziedzinie cyberbezpieczeństwa dokonywana była przez podmioty z Chin, głównie do chińskiego urzędu patentowego. Systematycznie rośnie jednak liczba zgłoszeń patentowych dokonywanych przez podmioty chińskie w innych krajach, co dodatkowo podkreśla dominację chińskich patentów.

Badanie otoczenia patentowego potwierdza, że obszary tworzące fundament dla scenariuszy rozwoju, tj. scenariusza 1 (cyberbezpieczeństwo jako usługa), scenariusza 2 (kryptografia, uwierzytelnianie i ochrona tożsamości), scenariusza 3 (cyberbezpieczeństwo instalacji procesowych) oraz scenariusza 4 (cyberbezpieczeństwo sieci i IoT) dotyczą najbardziej innowacyjnych technologii w perspektywie całego rynku cyberbezpieczeństwa, w których obecnie prowadzone są na świecie intensywne działania badawczo-rozwojowe, czego efektem jest dynamiczny przyrost liczby rozwiązań zgłaszanych do ochrony patentowej. Potwierdza to duże zapotrzebowanie międzynarodowego rynku na dane technologie i ich rozwój w perspektywie

krajowej może przyczynić się do rozwoju nie tylko przedsiębiorstw (w tym ich możliwości eksportowych), ale całego polskiego rynku cyberbezpieczeństwa.

2.7. Analiza trendów rozwojowych

Trendy napędzające rozwój rynku IT mają przede wszystkim charakter technologiczny i w znakomitej większości wynikają z chęci usprawnień funkcjonujących już rozwiązań lub dywersyfikacji w stronę rewolucyjnych innowacji. Najczęściej jednak powodów ich powstawania trudno doszukiwać się w nierozwiązanych problemach uczestników rynku, a raczej wynikają one ze zidentyfikowanej szansy rynkowej, której wykorzystanie umożliwi dodatkowy zarobek, a jednocześnie zaspokoi potrzebę klientów, której równie dobrze mogli być nieświadomi. Oznacza to, że dużą część trendów technologicznych możemy nazwać usprawnieniami typu „nice-to-have" – czyli takich, których wykorzystanie przynosi korzyści, ale ich brak nie powodowałby problemów. Sytuacja ta znacząco jednak różni się w przypadku tych obszarów, które powstały na skutek realnej potrzeby rynkowej, której zaspokojenie jest konieczne, aby branża (lub cały rynek) mogła prawidłowo funkcjonować – tak właśnie jest w przypadku obszaru cyberbezpieczeństwa, w którym trendy rozwojowe mają charakter „must-to-have" (bez nich funkcjonowanie byłoby znacząco utrudnione lub niemożliwe), tzn. odpowiadają na konkretne i pilne potrzeby użytkowników.

Podstawowym czynnikiem rozwojowym, gwarantującym długoterminowość funkcjonowania całego obszaru cyberbezpieczeństwa, jest **konieczność zapewniania bezpieczeństwa w sferze wirtualnej** – technologie te stanowią fundament obecności wszystkich użytkowników w Internecie i bez nich jego wykorzystanie zarówno konsumenckie, jak i komercyjne, zwyczajnie nie byłoby możliwe. Bez odpowiednich zabezpieczeń popularyzacja Internetu nigdy nie osiągnęłaby obecnego pułapu, a brak rozwoju technologii z obszaru cyberbezpieczeństwa nie tylko doprowadziłaby do nieaktualności zapór, ale wcześniej czy później do załamania się obecnej struktury sfer wirtualnych (brak zaufania co do bezpieczeństwa, zaczynając od podstawowych danych i dokumentów, po wirtualne pieniądze w bankach).

Powyższy czynnik nie tylko gwarantuje długoterminową atrakcyjność sektora (konieczność jego funkcjonowania na rynku), ale jest również podstawą trendu, który warunkuje powstawanie wszystkich pozostałych trendów technologicznych w cyberbezpieczeństwie, a jest nim **nieustanny rozwój technologii wykorzystywanej przez cyberprzestępców**. To stałe pojawianie się nowych technologii, takich jak *ransomware* czy nowych technik *phishingu*, powoduje, że rynek cyberbezpieczeństwa nieustannie musi się rozwijać – nowe technologie powstają zarówno profilaktycznie, jak i jako bezpośrednie odpowiedzi na nowe zagrożenia. Z tego powodu rynek ten musi być niezwykle elastyczny i zawsze gotowy do transferu zasobów w kierunku, który aktualnie najbardziej zagraża *status quo* bezpieczeństwa sfer wirtualnych. Tak długo jak cyberprzestępcy będą poszukiwać nowych rozwiązań, tak długo rynek cyberbezpieczeństwa będzie pod presją ciągłego rozwoju.

Zwiększające się znaczenie wirtualnych zabezpieczeń oraz rosnąca świadomość klientów co do kluczowego ich charakteru, powoduje **wzrost zainteresowania technologiami z obszaru profilaktyki**. Coraz więcej użytkowników Internetu (w szczególności przedsiębiorcy i instytucje publiczne) inwestuje w technologie pozwalające wykrywać luki w zabezpieczeniach oraz proaktywnie przeszukiwać sieć w celu wykrywania nowych zagrożeń. Trend ten stał się podstawą rozwiązań typu *threat hunting*, wyspecjalizowanych w iteracyjnym skanowaniu otoczenia przedsiębiorstwa i analizie zagrożeń, które skutecznie omijają inne zabezpieczenia.

Jednocześnie jednak technologie z obszaru cyberbezpieczeństwa rozwijają się nie tylko poprzez aktualizacje czy pomniejsze poprawki uwzględniające najnowsze zagrożenia, ale również poprzez dodawanie nowych warstw zabezpieczeń, których złamanie wymaga przejścia każdej z nich. Trend ten jest następstwem coraz to większej popularności **technologii MFA/UW (uwierzytelniania wieloskładnikowego)**, czyli rozwiązań dostępowych wymagających co najmniej dwuetapowej weryfikacji użytkownika. W przypadku stosowania uwierzytelniania wieloskładnikowego, użytkownik oprócz podania identyfikatora oraz hasła musi (w kolejnych etapach) podać uzyskany kod lub frazę np. ze swojego przenośnego urządzenia internetowego (np. smartfon, tablet) lub poprzez przepisanie go z e-maila wysłanego przez serwis, na którym użytkownik próbuje się zalogować czy też za pomocą specjalnej karty/ wczytania linii papilarnych palca. Zainteresowanie tym sposobem zabezpieczenia staje się standardem rynkowym w kontekście coraz bardziej powszechnych wycieków haseł i kradzieży tożsamości.

Na rynku obserwowany jest również trend **rozwiązań bezpieczeństwa nowej generacji**:

- **XDR** – rozwiązania Extended Detection and Response (XDR) odpowiadają na wyzwania związane z bezpieczeństwem punktów końcowych, powstałe w wyniku przejścia na zdalną lub hybrydową pracę. XDR oferują proaktywną ochronę przed zagrożeniami cybernetycznymi, umożliwiając organizacji uzyskanie zwiększonej widoczności wielu wektorów ataków oraz poprawę produktywności dzięki zastosowaniu automatyzacji zabezpieczeń oraz scentralizowanego monitorowania i zarządzania zabezpieczeniami.
- **SASE** – rozwiązania Secure Access Service Edge (SASE) mają na celu konsolidację rozwiązań sieciowych i zabezpieczeń organizacji w jednym urządzeniu w chmurze. SASE wykorzystują definiowaną programowo funkcjonalność sieci WAN (SD-WAN) do optymalizacji routingu ruchu między punktami obecności SASE (PoP). Ponieważ punkty PoP integrują zabezpieczenia kompleksowo, SASE oferuje skonsolidowane monitorowanie i zarządzanie bezpieczeństwem w całej rozproszonej infrastrukturze organizacji.
- **ZTNA** – rozwiązania Zero-Trust Network Access (ZTNA) to alternatywa dla starszej sieci VPN dla bezpiecznego zdalnego dostępu. W przeciwieństwie do sieci VPN, która zapewnia pełny dostęp do sieci korporacyjnej uwierzytelnionym użytkownikom, ZTNA wdraża zasady zerowego zaufania i zapewnia dostęp do zasobów indywidualnie dla każdego przypadku. Wdrożenie ZTNA – znanego również jako programowalny obwód graniczny (SDP) – umożliwia organizacji bezpieczniejsze wsparcie zdalnych pracowników i ochronę przed próbami wykorzystania rozwiązań zdalnego dostępu.

Rozwój obszaru cyberbezpieczeństwa akcelerowany jest również przez czynniki zewnętrzne, w rozumieniu technologii i trendów pojawiających się w innych branżach, które docelowo korzystają również z rozwiązań zabezpieczających. Wśród takich branż należy wymienić m.in. sektory przemysłowe, które są obecnie pod silną presją automatyzacji i digitalizacji swojej działalności wraz z implementacją założeń **Przemysłu 4.0**. Trend ten warunkuje przeniesienie wielu aktywności do sfer wirtualnych, które dotychczas wykonywane były manualnie lub poza Internetem – co nakłada na przedsiębiorców wymagania wprowadzania dodatkowych zabezpieczeń, specyficznych dla Internetu. Przemysł 4.0 potęguje również znaczenie **rozwiązań IoT** które, aby poprawnie funkcjonować wymagają nie tylko zabezpieczeń urządzeń połączonych w ramach „Internetu Rzeczy", ale również zabezpieczeń bezpośrednio samej sieci pozwalającej na komunikację pomiędzy nimi – co znacząco zwiększa popyt na produkty z obszaru cyberbezpieczeństwa i wymaga od niego innowacyjnych rozwiązań. Ważnym trendem zewnętrznym jest również **przenoszenie coraz większej części działalności przedsiębiorstw do sfer wirtualnych**, zarówno w kontekście procesów sprzedażowych, jak i administracyjnych (*backoffice*). Z tego względu szczególnie ważnym elementem prowadzenia wirtualnej działalności stają się rozwiązania chmurowe, które wymagają dodatkowych zabezpieczeń, stworzonych specjalnie z myślą o nich.

Mimo tego, że wszystkie powyższe trendy mają silny charakter technologiczny, to nie wszystkie czynniki warunkujące rozwój rynku cyberbezpieczeństwa wywodzą się bezpośrednio z nowych technologii. Dotychczas czynniki pozatechnologiczne w głównej mierze sprowadzały się do **legislacji nakładającej nowe wymagania na użytkowników Internetu**, a w szczególności podmiotów komercyjnych przetwarzających dane konsumentów. Większość rynków krajowych na świecie posiada co najmniej fundament regulacyjny, który wymaga od przedsiębiorców stosowania rozwiązań z obszaru cyberbezpieczeństwa. Powoduje to, że popyt na takie rozwiązania generowany jest niemalże wszędzie, a możliwość jego zaspokojenia wymaga przede wszystkim znajomości lokalnych regulacji i wymogów.

Należy również wspomnieć o trendzie, którego znaczenie urosło wraz z pandemią COVID-19 i wprowadzanymi restrykcjami pracy w biurze, czyli **popularyzacji zdalnego trybu pracy**. Wielu przedsiębiorców nie było gotowych na taką skalę tego zjawiska, zarówno pod kątem administracyjnym, jak i posiadanych zabezpieczeń cyfrowych. Konieczność zapewnienia pracownikom analogicznego poziomu bezpieczeństwa struktur IT w pracy pozabiurowej, pozwoliło firmom z branży cyberbezpieczeństwa zmniejszyć negatywne skutki recesji gospodarczej.

W społeczeństwie rośnie też **zainteresowanie prywatnością danych**. Użytkownicy coraz bardziej zdają sobie sprawę z zagrożeń, w szczególności dotyczących informacji o charakterze prywatnym lub obyczajowym. Stąd tendencje do ograniczania obecności w mediach społecznościowych lub skupianie się na technologiach UW. Trendy na rynku usług, to także usuwanie śladów po osobach prywatnych z Internetu i zapewnianie im na nowo anonimowości.

Istotnym obszarem, któremu poświęca się coraz więcej uwagi, jest **bezpieczeństwo systemów o długim czasie żywotności**. Dotyczy to między innymi przemysłu procesowego, infrastruktury

krytycznej, energetyki itp. Często modernizuje się takie systemy zamiast budować je na nowo, a zwiększanie bezpieczeństwa niekoniecznie idzie w parze z postępującą automatyzacją. Coraz więcej przedsiębiorców koncentruje się na zapewnieniu rozwiązań dedykowanych przemysłowi. Jest to szczególnie ważne w kontekście zapewnienia bezpieczeństwa łańcucha dostaw. Można znaleźć liczne przykłady skutecznych ataków na urządzenia należące do infrastruktury energetycznej lub procesowej. Najbardziej znanym przypadkiem jest atak na platformę monitorowania sieci Orion SolarWinds, który wywołał wstrząs na całym świecie.

Powyższy przykład wskazuje na ostatni, jednak nie mniej ważny, trend jakim jest **cyberwojna o charakterze międzynarodowym**. Największe światowe mocarstwa nie oszczędzają nakładów na własnych specjalistów od przeprowadzania i detekcji ataków. Działania te wchodzą w skład popularnego obecnie pojęcia „wojny hybrydowej", czyli działań militarnych realizowanych zarówno fizycznie, jak i w sferach wirtualnych. Mogą to być działania stricte wywiadowcze (kradzież informacji), ale też dezorganizacyjne - poprzez próby ataków na łańcuchy dostaw czy propagowanie nieprawdziwych informacji (z ang. tzw. fake news).

Analiza powyższych trendów podkreśla jak bardzo interdyscyplinarne jest oddziaływanie cyberbezpieczeństwa – technologie te mają wpływ zarówno na prawidłowe funkcjonowanie poszczególnych podmiotów i biznesów, jak i całej gospodarki oraz społeczeństwa.

3. Charakterystyka rynku krajowego

3.1. Rys historyczny i analiza dostępnych produktów i technologii

Historia cyberbezpieczeństwa w Polsce jest z naturalnych przyczyn dużo krótsza niż na świecie. Pomimo znanych przykładów sukcesów w zakresie kryptografii osiągniętych przez polskich matematyków (podwaliny pod złamanie Enigmy), dopiero nadejście informatyzacji pozwoliło na uzyskanie praktycznych rezultatów. W powojennej Polsce dostęp do komputerów był bardzo ograniczony. Lata 80-te XX w., to pojawienie się na polskim rynku mikrokomputerów. Początkowo ich źródłem był import własny, później Pewexy, aż w końcu pojawiły się w powszechnej sprzedaży.

Należy zwrócić uwagę na istotny element historii cyberbezpieczeństwa w Polsce jakim jest powstanie w 1987 r. MkS_Vir, jednego z pierwszych programów antywirusowych na świecie. Pierwotnie program był wykorzystywany jedynie na własne potrzeby autora, z prozaicznego powodu – dostępne wtedy programy nie spełniały jego oczekiwań. Po jego komercjalizacji, pierwsze wersje przeznaczone dla systemu DOS, dystrybuowane były na dyskietkach przez firmę Apexim (w której pracował autor programu), a aktualizacje (już wtedy istniała świadomość konieczności ich wdrażania, aby program był nadal aktualny) wydawane były w cyklu miesięcznym i dostarczane do klientów pocztą. Początkowo oprogramowanie było spersonalizowane – zawierało na głównym ekranie numer seryjny oraz dane właściciela licencji. Pomimo to często program użytkowany był bez licencji, a o jego popularności świadczy fakt powstawania „koni trojańskich" podszywających się pod nowe (niewydane jeszcze) aktualizacje programu.
W późniejszym okresie wraz z wersją płatną autor udostępniał wersję demonstracyjną programu z możliwością bezpłatnego korzystania z niej przez tydzień. W celach edukacyjnych program zawierał opisy działania niektórych wirusów (w tym demonstracje ich graficznych i dźwiękowych efektów), a od wersji 3.99 leksykon spotykanych w Polsce wirusów. W 1996 r. program został laureatem III edycji Konkursu „Teraz Polska". Historia programu zawiera wzloty i upadki – jego autor, Marek Sell w 1996 r. założył firmę MKS Sp. z o.o. specjalnie w celu rozwijania programu, jednak gdy w 2004 r. Sell zmarł, firma MKS miała trudności z utrzymaniem rentowności i finalnie zbankrutowała zaledwie 6 lat później. W 2011 r. znak towarowy mks_vir przejęła firma Arcabit Sp. z o.o., która ponownie skomercjalizowała produkt w formie darmowej aplikacji. Był on w jej ofercie do 2014 r. Od 2018 roku program antywirusowy mks_vir, w nowej odświeżonej wersji jest

produkowany i sprzedawany przez mks_vir Sp. z o.o. Firma ta jest jednym z założycieli klastra cyberbezpieczeństwa #CyberMadeInPoland.

Inne obszary rynku cyberbezpieczeństwa w Polsce nie posiadały aż tak spektakularnych produktów, jednak rozwój tych obszarów zdecydowanie postępował. Przemiany ustrojowe i pojawienie się nowych banków wytworzyły unikalną sytuację, w której system bankowy budowany jest już przy wykorzystaniu nowych technologii. Stąd też w polskim systemie bankowym funkcjonują wdrożone rozwiązania bezpieczeństwa, które nadal nie są powszechne nawet w bardziej dojrzałych gospodarkach rynkowych.

W Polsce dynamicznie rozwija się branża ochrony infrastruktury krytycznej i generalnie segmentu OT. Liczne produkty i usługi mają na celu zapewnienie bezpieczeństwa, zarządzanie ryzykiem i ochronę danych. Cykliczne konferencje i wsparcie ze strony państwa mają na celu zapewnienie bezpieczeństwa łańcuchom dostaw.

Ważnym elementem rynku jest również branża IoT, gdzie producenci rozproszonych systemów pomiarowych, układów automatyki domowej i monitoringu rozwijają technologie związane z bezpieczeństwem ich produktów. Opracowywane rozwiązania obejmują systemy szyfrowania i zabezpieczone bramki sieciowe.

Istotny segment, to także rozwiązania z obszaru potwierdzania tożsamości. W Polsce funkcjonuje kilka firm, które zajmują się stricte uwierzytelnianiem użytkownika. Stosowane są w tym zakresie np. techniki biometryczne lub metody uczenia maszynowego.

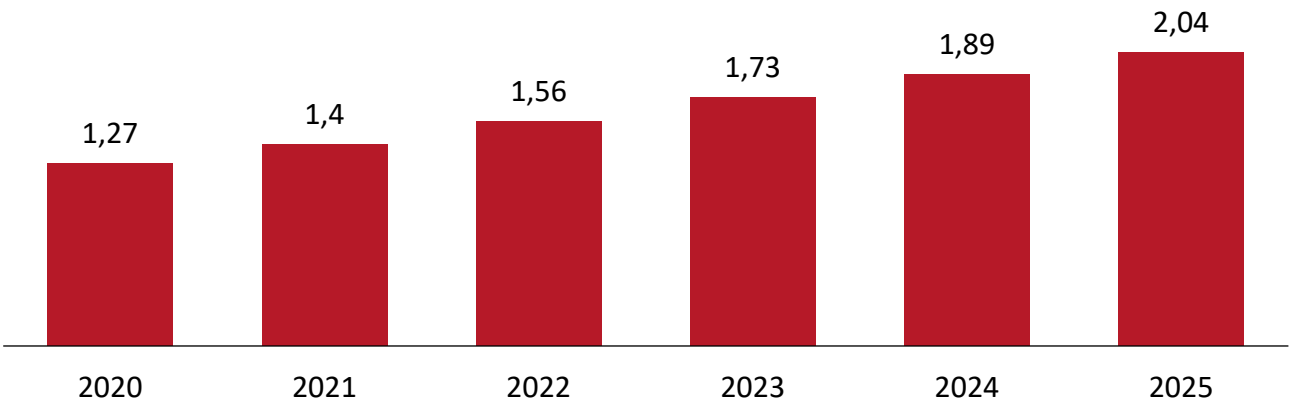
Podsumowując przeprowadzone analizy można wyciągnąć wniosek, że polski rynek cyberbezpieczeństwa, pomimo tego, że rozwija się krócej niż światowy i w mniejszej skali, to jednak zachowuje wysoki poziom technologiczny. Przedsiębiorcy wykazują dużą skłonność do rozwiązań innowacyjnych, a we wskazanych powyżej obszarach, takich jak ochrona OT, IoT czy autentykacja należy upatrywać szansy rozwoju polskich technologii. Ważnym jest jednak fakt, że w Polsce dostępne są również rozwiązania firm zagranicznych – dedykowane zarówno korporacjom (w zakresie np. rozwiązań ochrony danych w chmurze czy VPN-ów), jak i klientom indywidualnym (w zakresie chociażby programów antywirusowych czy VPN-ów). Zbudowanie solidnej i wiarygodnej marki w Polsce w odniesieniu do tego typu światowych i renomowanych produktów czy usług może być bardzo trudne i często nieopłacalne, szczególnie jeśli weźmie się pod uwagę istnienie innych obszarów technologicznych, które mogą mieć dużo większy potencjał i nie posiadać tak wielu barier czy wyzwań do pokonania.

3.2. Podstawowa analiza wielkości i dynamiki rynku

Wartość polskiego rynku cyberbezpieczeństwa w 2019 r. przekroczyła 1,3 mld USD, odnotowując jednocześnie historycznie rekordowy wzrost rok do roku w wysokości 14,3%. Na początku 2020 r. prognozy wskazywały, że tak dynamiczny trend wzrostowy zostanie co najmniej utrzymany, jednak zastój gospodarczy zapoczątkowany pandemią COVID-19 skutecznie utrudnił normalne

funkcjonowanie animatorom rynku i finalnie doprowadził do recesji również w obszarze cyberbezpieczeństwa – w 2020 r. wartość branży spadła do 1,27 mld USD, czyli o około 4,7%. Mimo zauważalnego spadku, nie był on dla obszaru cyberbezpieczeństwa tak odczuwalny jak można byłoby się tego spodziewać – popyt na zabezpieczenia cyfrowe nie tylko szybko (już w czwartym kwartale 2020 r.) ponownie wrócił do standardowych poziomów, a w niektórych branżach (szczególnie tych stawiających na pracę zdalną czy hybrydową) odnotowano wręcz znaczący jego wzrost. Najnowsze prognozy wskazują, że w ciągu najbliższych 5 lat na polskim rynku cyberbezpieczeństwa można podziewać się nawet 12% wzrostów rok do roku, a w 2025 roku wartość tego rynku może przekroczyć barierę 2 mld USD[25] – co przedstawione zostało na Rysunku 18.

Rysunek 18. Wartość rynku cyberbezpieczeństwa w Polsce w roku 2020 i prognoza na lata 2021-2025 (mld USD)



Źródło: opracowanie własne na podstawie The European Cybersecurity Market autorstwa Enterprise Ireland

Wzrost ten potęgowany jest również przez zwiększające się zainteresowanie polskim rynkiem wśród cyberprzestępców i (na tę chwilę) niewystarczającym średnim poziomem zabezpieczeń cyfrowych wśród przedsiębiorców – według rankingu Check Point Software, gotowość polskich przedsiębiorstw na ataki cyberprzestępców oceniana jest na 24 miejscu w Europie oraz 62 na świecie[26]. Względnie niska pozycja na tle regionu europejskiego podkreśla skalę wydatków, jakie muszą jeszcze ponieść polskie przedsiębiorstwa i instytucje publiczne, aby dorównać co najmniej średniej regionalnej.

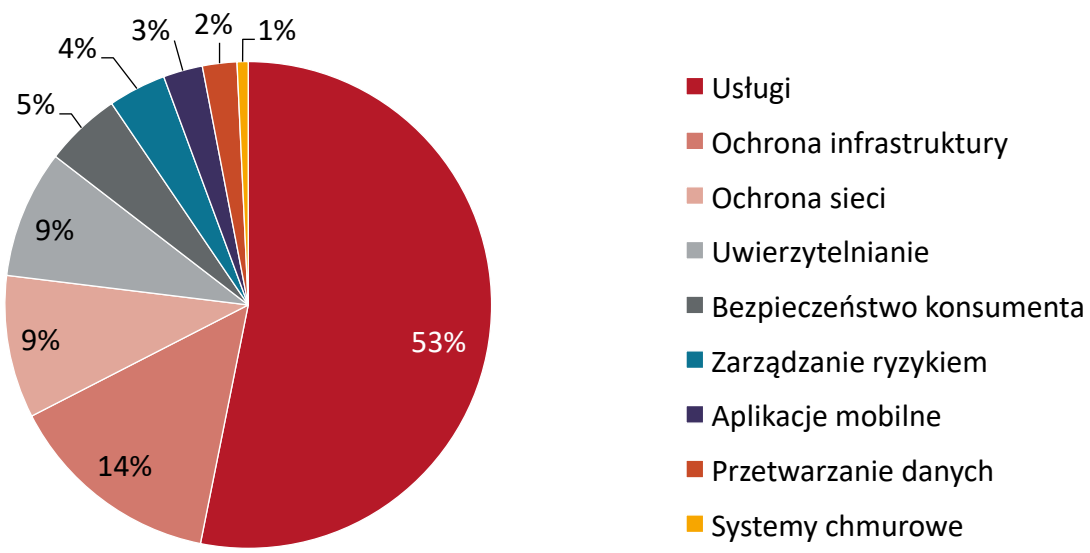
---

[25] Raport The European Cybersecurity Market, Enterprise Ireland, https://globalambition.ie/cybersecurity-report-and-conference/. Dostęp: 07.10.2021.

[26] Zestawienie Check Point Software dot. cyberbezpieczeństwa – artykuł ICT Market Experts, https://ictmarketexperts.com/en/news/poland-drops-in-the-ranking-of-cybersecurity/. Dostęp: 07.10.2021.

Największym segmentem krajowego rynku cyberbezpieczeństwa, pod względem wdrożeń i penetracji rynku, pozostaje od lat sektor usługowy, który w 2020 r. odpowiadał za prawie 65 tysięcy wdrożeń. Sektor ten pozostaje niekwestionowanym liderem, wyprzedzając ponad 3,5 krotnie sektor ochrony infrastruktury (17,5 tysiąca wdrożeń). Względnie podobne wartości osiągają również sektory: sprzętu do ochrony sieci (11,6 tys.) oraz oprogramowania do uwierzytelniania (10,4 tys.). Coraz większym zainteresowaniem cieszą się również oprogramowania zapewniające bezpieczeństwo konsumentom w sferze e-commerce (6,2 tys.), kompleksowe systemy do zarządzania cyfrowym ryzykiem (4,7 tys.), rozwiązania zabezpieczające aplikacje mobilne (3,2 tys.) oraz systemy bezpieczeństwa przetwarzania danych (2,8 tys.). Wzrost żadnego z powyższych segmentów nie był jednak tak duży (nie przekraczał 7% w skali roku), jak w przypadku najmniejszego z nich, tj. systemów bezpieczeństwa chmury (niecały tysiąc wdrożeń, jednak wzrost na poziomie 30% w skali roku)[27]. Udział powyższych segmentów zilustrowany został na Rysunku 19.

Rysunek 19. Udział kluczowych segmentów rynku cyberbezpieczeństwa w Polsce



Źródło: opracowanie własne na podstawie raportu Polski Rynek Cyberbezpieczeństwa: szanse i zagrożenia

Pierwsze prognozy na 2021 r. wskazują, że segmenty wewnątrz polskiej branży cyberbezpieczeństwa zareagowały na recesję gospodarczą spowodowaną pandemią COVID-19 analogicznie co ich zagraniczne odpowiedniki – te sektory, które dotychczas skupiały się

[27] *Raport Polski rynek Cyberbezpieczeństwa: szanse i zagrożenia, Venture INC, https://www.ventureinc.com/pl/blog/polski-rynek-cyberbezpieczenstwa-raport/. Dostęp: 07.10.2021.*

na rozwiązaniach fizycznych lub „biurowych" (jak np. ochrona sieci lokalnych, infrastruktura) odczuły brak popytu najmocniej (prognozuje się, że sam segment ochrony sieci może odnotować nawet 12% spadek), zaś te które dostarczały wartość niezależnie od lokalizacji i tym samym wspierały transformację w stronę pracy zdalnej, odnotowały wzrosty (z największymi widocznymi w sektorze bezpieczeństwa danych, aplikacji, chmury oraz uwierzytelniania). Podobnie jak w przypadku większości europejskich krajów, najmniej na nagłą konieczność prowadzenia działalności w formie zdalnej, a przez to wykorzystywania innych niż biurowe formy zabezpieczeń, przygotowany był sektor publiczny oraz MŚP – w tym w szczególności te o niskiej świadomości cyfrowej (dla których sfera wirtualna nadal pozostaje wsparciem biznesu, nie głównym narzędziem jego prowadzenia)[28].

W przypadku cyberprzestępczości szacuje się, że aż 78% wszystkich ataków przeprowadzanych w Polsce to *phishing* poprzez wiadomości e-mail. Szczególnie dużą popularnością wśród krajowych cyberprzestępców cieszą się również oprogramowania „udające" standardowe pliki (tzw. *trojany*), takie jak „Qbot" oraz „Trickbot". Wśród technologicznych liderów niebezpiecznego oprogramowania należy wyróżnić również narzędzia służące do wyłudzania informacji (szczególnie te nakierowywane na sektor bankowy), takie jak np. „Formbook" czy tzw. *keyloggery*. Wszystkie powyższe rozwiązania wpisują się w definicję tzw. *malware*, czyli złośliwego oprogramowania stworzonego z myślą o łamaniu zabezpieczeń cyfrowych i wykradaniu danych lub działania wbrew oczekiwaniom użytkowników[29].

Zdecydowanie pozytywnym trendem na polskim rynku jest stale zwiększające się wykorzystanie podstawowych narzędzi zapewniających bezpieczeństwo w sieci wśród użytkowników komercyjnych – szacuje się, że w 2020 r. aż 91% firm posiadało chociaż podstawową strukturę zarządzania infrastrukturą IT i około 85% stosowało oprogramowanie antywirusowe. Co więcej 76% z nich korzysta również z oprogramowań typu *VPN,* a 45% wszystkich firm wdrożyła lub planuje wdrożyć rozwiązania z obszaru *threat hunting* (z czego 54% z nich to duże przedsiębiorstwa)[30].

---

[28] Artykuł Cyberbezpieczeństwo w dobie pandemii, Grzegorz Juszczyk S&T, https://snt.pl/cyberbezpieczenstwo-w-dobie-pandemii-problem-globalny-towarzyszacy-przyspieszonej-cyfryzacji/. Dostęp: 07.10.2021.

[29] Raport Cyberbezpieczeństwo Polskich Firm 2021, Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, https://cybermadeinpoland.pl/raport-cyberbezpieczenstwo-polskich-firm-2021/. Dostęp: 07.10.2021.

[30] Raport Cyberbezpieczeństwo Polskich Firm 2021, Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, https://cybermadeinpoland.pl/raport-cyberbezpieczenstwo-polskich-firm-2021/. Dostęp: 07.10.2021.

3.3. Analiza cyklu życia produktów

Cykl życia technologii, usług i oprogramowania w obszarze cyberbezpieczeństwa nie jest zależny od regionu geograficznego, gdyż metodyki wytwarzania i komercjalizacji są względnie uniwersalne, a animatorzy rynku korzystają z tych samych fundamentów co ich odpowiednicy w innych krajach. Oznacza to, że produkty powstające w tym obszarze w Polsce cechują się analogicznym cyklem życia co ten opisany w kontekście rynku globalnego w rozdziale 2.3.

Co ważne w Polsce również cykl życia produktów powstających w ramach obszaru cyberbezpieczeństwa jest podobny niezależnie od branży, a zmienność ujawnia się głównie w metodykach pracy nad samym oprogramowaniem oraz długości trwania poszczególnych faz cyklu życia. W przypadku długości czasu trwania poszczególnych faz, polskim producentom przyświeca również podstawowy trend międzynarodowy, który propaguje podejście do prac oparte o stałe rozwijanie i aktualizowanie tworzonych rozwiązań, co powoduje celowe wydłużanie fazy wzrostu i dojrzałości w taki sposób, aby produkt jak najpóźniej wszedł w fazę schyłkową.

Naturalnie, jak w przypadku każdej technologii, projekty z obszaru cyberbezpieczeństwa również przechodzą przez klasyczne **fazy badawczo-rozwojowe (B+R)**, które jednak z uwagi na silnie niematerialny charakter większości produktów oraz popularność metodyk pracy opartych o szybką komercjalizację i testowanie prototypów z pierwszymi klientami, często nachodzą na siebie lub wykonywane są wręcz symultanicznie.

W celu ustandaryzowania czasu trwania poszczególnych faz projektów B+R w Polsce, przeanalizowano propozycje projektów wypracowanych przez uczestników warsztatów Smart Lab, co pozwoliło określić średni czas trwania każdej z faz w Polsce – przedstawiony w Tabeli 1.

Tabela 1. Średni przedział czasu trwania faz projektów B+R dla obszaru cyberbezpieczeństwa w Polsce

Faza projektu B+R	Średni przedział czasu trwania fazy w latach
Badania podstawowe	1–2
Badania przemysłowe	1–3
Prace rozwojowe	2–4

Źródło: opracowanie własne

Jak wcześniej podkreślono, w kontekście przytoczonych powyżej danych należy zwrócić szczególną uwagę na fakt, że sumaryczny czas realizacji projektów B+R w obszarze cyberbezpieczeństwa często nie będzie równy sumie długości trwania poszczególnych faz. Wynika to z faktu, że poszczególne fazy mogą być realizowane symultanicznie lub częściowo nachodzić na siebie (np. prace z obszaru badań przemysłowych mogą rozpocząć się jeszcze podczas trwania części

procesów z obszaru badań podstawowych). Widoczne jest to w przypadku projektów zaproponowanych przez uczestników warsztatów Smart Lab, które sumarycznie trwają na ogół od 4 do 7 lat.

W znakomitej większości przypadków faza badań podstawowych okazuje się najkrótsza (1-2 lata), zaś najwięcej czasu uczestnicy warsztatów spędzają (i planują spędzać) w fazie prac rozwojowych (średnio 2-4 lata), która w przypadku cyberbezpieczeństwa obejmuje zarówno prace przedwdrożeniowe i wdrożeniowe, jak i prace dotyczące aktualizacji oraz dalszego utrzymania oprogramowania.

Należy również mieć na uwadze, że podobnie jak w przypadku rynku globalnego, niemożliwe jest precyzyjne określenie czasu trwania cyklu życia produktu z obszaru cyberbezpieczeństwa już po zakończeniu prac B+R. Wynika to przede wszystkim z uwagi na dominujące wśród przedsiębiorców z sektora IT założenie co do ciągłego rozwoju oprogramowania (tj. praktycznie niekończącego się cyklu życia produktu) oraz stale rosnącej świadomości klientów o cyberbezpieczeństwie (co zwiększa popyt i stale otwiera nowe branże klienckie).

3.4. Analiza barier rynkowych

Bariery rynkowe dla podmiotów działających w obszarze cyberbezpieczeństwa w Polsce, w skali makro, są tożsame z przeanalizowanymi w rozdziale 2.4 dot. rynku globalnego. Animatorzy rynku polskiego mają jednak do czynienia ze specyficznymi barierami, które albo występują jedynie w skali najbliższego otoczenia (mikro), albo ich siła oddziaływania jest dodatkowo na polskim rynku spotęgowana. Bariery rynkowe zostały przeanalizowane wraz z uczestnikami warsztatów Smart Lab, a na bazie pozyskanej w ten sposób wiedzy wyłoniono te, które mają największy wpływ na funkcjonowanie krajowego rynku cyberbezpieczeństwa:

Niski poziom edukacji rynku i społeczeństwa – ogólny poziom wiedzy o niebezpieczeństwach czyhających w Internecie oraz możliwych skutkach stosowania nieodpowiednich (lub po prostu nieaktualnych) zabezpieczeń jest niski nie tylko wśród klientów detalicznych, ale również wśród niemalże wszystkich typów podmiotów biznesowych (oprócz największych organizacji, często z zagranicznym kapitałem) i podmiotów publicznych (w tym organizacji państwowych, administracyjnych czy edukacyjnych). Sytuacja ta tworzy realną barierę ograniczającą prawidłowy rozwój rynku i prowadzi do nadpodaży, kiedy to przedsiębiorcy posiadają najnowsze rozwiązania IT i gotowi są je wdrażać, jednak klienci wolą ograniczać się do rozwiązań podstawowych lub ignorują cały segment cyberbezpieczeństwa.

Postrzeganie cyberbezpieczeństwa jako jednorazowej inwestycji, nie procesu – zauważalna część polskiego rynku, w tym w szczególności sektor MŚP, interpretuje działania z zakresu cyberbezpieczeństwa jako „jednorazowy zakup technologii", który docelowo uchronić ma ich przed wszelkim wirtualnym niebezpieczeństwem. Klienci często nie mają świadomości, że nawet najlepsze obecnie rozwiązania staną się z czasem bezużyteczne, jeśli nie będą stale

rozwijane – technologie wykorzystywane przez cyberprzestępców stale ewoluują i analogiczny postęp muszą wykazywać rozwiązania mające je zwalczać. Jeśli się tak nie dzieje (co ma miejsce na polskim rynku w sektorze MŚP), tworzy to realną barierę rozwoju rynku. Co więcej, duża część przedsiębiorców polega wyłącznie na środkach technicznych (np. oprogramowaniu) – nie inwestując w szkolenia dla pracowników czy testy zgodności/ aktualności technologii.

Niski poziom zaufania MŚP do usług z obszaru cyberbezpieczeństwa – na krajowym rynku zauważalna jest niechęć do outsourcingu spraw dot. zabezpieczeń IT w przedsiębiorstwach, które często wolą pozostać przy swoich własnych, nieskutecznych rozwiązaniach niż korzystać z usług zewnętrznych (zarówno tych podstawowych, jak i kompleksowych systemów typu CSaaS). W sektorze MŚP, a w szczególności wśród firm mniej świadomych technologicznie, widoczny jest trend postrzegania usług dot. cyberbezpieczeństwa jako „informacji wychodzących poza przedsiębiorstwo i braku kontroli nad nimi". Tworzy to realną barierę dla przedsiębiorców oferujących rozwiązania usługowe.

Brak wpływu na międzynarodowe gremia decyzyjne – jedynie kilku przedstawicieli polskiej branży cyberbezpieczeństwa ma wystarczające relacje międzynarodowe, aby móc określić siebie jako członka gremiów decyzyjnych mających wpływ na cały rynek. Pozostali przedstawiciele krajowego rynku nie tylko mają znacząco utrudnioną możliwość decydowania o kluczowych regulacjach czy zawiązywania międzynarodowej współpracy, ale również mają problem z „trzymaniem ręki na pulsie" w kontekście kluczowych trendów, legislacji czy nowości technologicznych.

Niski stopień internacjonalizacji polskich rozwiązań – mimo tego, że rozwiązania z sektora IT cechują się względnie dużą skalowalnością, a ekspansja zagraniczna nie wiąże się z tak wysokimi barierami wejścia jak w przypadku większości branż technologicznych, to krajowe rozwiązania z obszaru cyberbezpieczeństwa mają duży problem z internacjonalizacją. Taka sytuacja występuje zarówno z uwagi na brak promocji polskiej technologii na arenie międzynarodowej, jak i brak ekosystemowych inicjatyw pozwalających skutecznie zmniejszać koszty takich działań czy nawiązywać relacje.

Brak lub przestarzałe standardy dot. bezpieczeństwa IT – obecnie zdecydowana większość segmentów biznesowych ma albo przestarzałe standardy bezpieczeństwa struktur IT lub w ogóle takie standardy nie funkcjonują w tych segmentach. Jedyne regulacje określające wprost wymagania w zakresie cyberbezpieczeństwa, to te wynikające z paneuropejskiej i krajowej legislacji, jednak ani nie jest ona „ruchoma" (czyli nie śledzi rozwoju technologicznego i nie napędza popytu na te najbardziej aktualne i bezpieczne rozwiązania), ani nie jest spersonalizowana pod zagrożenia w konkretnych branżach.

Braki kadrowe – jedną z głównych barier rozwoju polskiej technologii w obszarze cyberbezpieczeństwa są zauważalne i stale pogłębiające się braki kadrowe u większości animatorów rynku (od przedsiębiorców, po jednostki naukowe, a nawet instytucje otoczenia biznesu). Cyberbezpieczeństwo w Polsce, to jeden z najbardziej niedocenianych obszarów przez programistów i osoby decydujące się na rozwój kariery w IT – co powoduje trudności w pozyskaniu

specjalistów, zarówno na cały etat, jak i podwykonawców do konkretnych (ograniczonych czasowo) projektów.

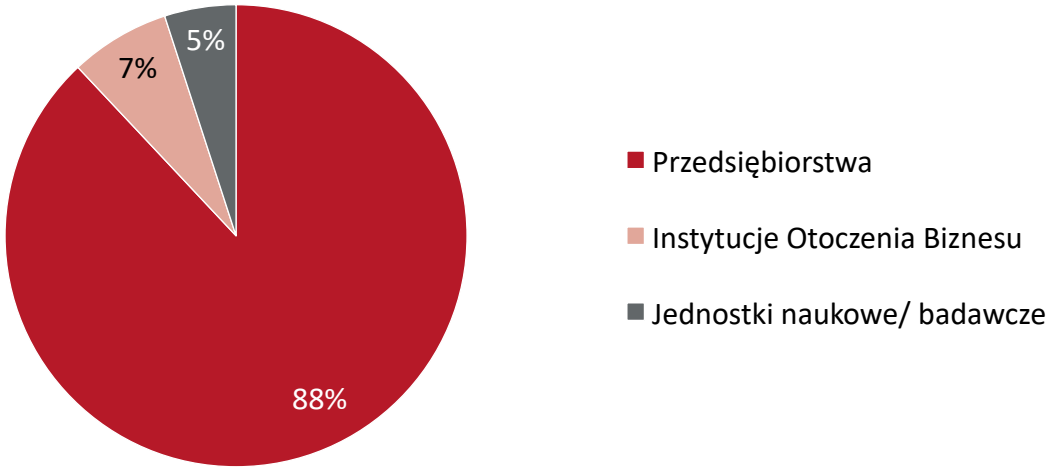
Brak doświadczenia w ochronie własności intelektualnej – polskie przedsiębiorstwa mają na ogół niewielkie doświadczenie w obszarze patentowania rozwiązań z obszaru cyberbezpieczeństwa, jak i ogólnie ochrony własności intelektualnej wykraczającej poza „tajemnicę przedsiębiorstwa". Sytuacja ta znacząco utrudnia ich konkurowanie na arenie międzynarodowej, na której często patenty są wręcz fundamentem prowadzenia rozmów o potencjalnej współpracy (zarówno bezpośrednio z potencjalnymi kontrahentami, jak i przy pozyskiwaniu zleceń na drodze przetargowej).

Relatywnie niski poziom sieciowości rynku, networkingu i transferu wiedzy – ograniczone zaufanie uczestników rynku oraz brak międzysektorowych inicjatyw zachęcających do nawiązywania relacji, doprowadziły do sytuacji, w której to krajowe przedsiębiorstwa mają bardzo ograniczone możliwości dzielenia się swoimi aktywnościami i wiedzą, co często powoduje, że, przedsiębiorcy, nawet w swoim najbliższym otoczeniu, nie wiedzą jakie technologie są obecnie opracowywane i z kim mogliby nawiązać współpracę. Bariera ta znacząco ogranicza możliwości czerpania korzyści z kooperacji i transferu wiedzy oraz pogłębia problem braku dostępu do najnowszych informacji dużej części branżowych animatorów. Należy jednak zaznaczyć, że istnieją wyjątki w postaci podmiotów animujących rynek (opisanych poniżej), które warto wspierać w ich staraniach dążących do zwiększania poziomu sieciowości całego rynku cyberbezpieczeństwa w Polsce.

3.5. Kluczowi gracze rynkowi

Podczas rekrutacji podmiotów do udziału w spotkaniach Smart Lab w obszarze cyberbezpieczeństwa zidentyfikowano blisko 150 podmiotów funkcjonujących w tym obszarze w Polsce. Spośród tej grupy prawie 88% stanowiły przedsiębiorstwa (zarówno z sektora MŚP, jak i duże) zajmujące się pracami B+R i komercjalizacją usług i produktów z obszaru cyberbezpieczeństwa. Blisko 7% z całkowitej liczby podmiotów stanowiły Instytucje Otoczenia Biznesu, zaś 5% stanowiły jednostki naukowe/ badawcze działające w obszarze cyberbezpieczeństwa. Udział procentowy poszczególnych grup interesariuszy, spośród których rekrutowano uczestników spotkań Smart Lab został przedstawiony na Rysunku 20. Część ze zidentyfikowanych podmiotów podczas rekrutacji była finalnie uczestnikami warsztatów Smart Lab.

Rysunek 20. Udział procentowy poszczególnych grup interesariuszy w całkowitej liczbie zidentyfikowanych podmiotów



Źródło: opracowanie własne

Poniżej wymieniono kluczowych graczy na polskim rynku w podziale analogicznym do powyższego, a więc uwzględniając przedsiębiorstwa, Instytucje Otoczenia Biznesu oraz jednostki naukowe. Są wśród nich zarówno uczestnicy spotkań SL, jak i inne zidentyfikowane podmioty, które finalnie nie wzięły udziału w warsztatach SL.

Przedsiębiorstwa

Do funkcjonujących na polskim i światowym rynku przedsiębiorstw prowadzących działalność w zakresie oprogramowania i usług z zakresu cyberbezpieczeństwa, pochodzących bądź mających główną siedzibę w Polsce można zaliczyć:

- **Arcabit** – jeden z największych polskich producentów oprogramowania anti-malware. Firma funkcjonuje od 2004 roku i od tego czasu wyrobiła sobie silną pozycję, zarówno wśród klientów biznesowych, jak i konsumentów detalicznych. Sprzedaje oprogramowanie ochronne dla domu, sieci organizacyjnych, a także dla jednostek edukacyjnych. Do produktów firmy należą również skanery sieci i przeglądarek oraz oprogramowanie ochronne serwerów.

- **Asseco Systems** – przedsiębiorstwo będące częścią grupy kapitałowej Asseco Group, czyli polskiego konglomeratu z branży IT, działającego globalnie. W zakresie cyberbezpieczeństwa firma posiada dwa segmenty: Centrum Danych, zapewniające miejsce w bezpiecznej chmurze UniCloud oraz Usługi Bezpieczeństwa i Zaufania, czyli działające pod marką Certum mechanizmy weryfikacji tożsamości i poprawności danych, opracowujące podpisy elektroniczne i cyfrowe pieczęci, ale też na przykład bezpieczne karty godzinowe dla pracowników, a nawet karty i czytniki procesorowe.

- **Blue Energy** – firma tworząca oprogramowanie prowadzące testy penetracyjne, chroniące aplikacje i badające słabości systemów ochrony w organizacjach. Świadczy również usługi

z zakresu Operacyjnych Centrów Bezpieczeństwa, zarządzania podatnością na zagrożenia oraz jakością infrastruktury IT, a także urządzeniami mobilnymi powiązanymi z siecią organizacji.

- **Comcert** – spółka działająca od 2011 roku, świadcząca usługi z zakresu identyfikacji zagrożeń, podnoszenia świadomości i umiejętności zespołów reagujących na nie, a także bezpośredniego wsparcia w przypadku wystąpienia incydentów. Usługi te wspierane są przez działania szkoleniowe i warsztaty dla pracowników klientów.

- **Cyberus Labs** – spółka oferująca innowacyjne rozwiązania z zakresu bezpieczeństwa w sieci, w tym „CyberKey" (elektroniczny klucz) likwidujący konieczność używania hasła przez użytkowników, co z kolei eliminuje czynnik ludzki. Działa on na zasadzie opartego w smartfonie systemu tokenowego, zbliżonego do tego znanego z banków. Równie aktywnie firma rozwija obecnie rozwiązania dedykowane Internetowi Rzeczy.

- **CyCommSec** – dynamicznie rozwijające się przedsiębiorstwo, prowadzące silnie zdywersyfikowaną działalność w niemalże wszystkich specjalizacjach cyberbezpieczeństwa. Prócz podstawowych segmentów, takich jak bezpieczeństwo sieci, aplikacji, urządzeń i danych, przedsiębiorstwo sprzedaje również oprogramowanie monitorujące wydajność i analizujące ruch w sieci pod kątem niebezpieczeństw, a także testy bezpieczeństwa aplikacji, infrastruktury IT oraz urządzeń. Świadczy również usługi doradcze i prowadzi szkolenia w dziedzinie zabezpieczeń danych i bezpiecznego poruszania się w przestrzeni cyfrowej.

- **Digital Core Design** – firma której głównym segmentem działalności jest produkcja hardware, w tym układów procesorowych i mikroczytników zintegrowanych z urządzeniami peryferyjnymi. Oprócz tego przedsiębiorstwo posiada oddział kryptograficzny, w ramach którego oferuje oprogramowanie szyfrujące, w protokołach DCRP1A, DSHA2-256 oraz DAES. Digital Core Design posiada również technologię jednokierunkowej bramy bezpieczeństwa, pozwalającą na konwersję danych prowadzoną symultanicznie z działaniem mechanizmów bezpieczeństwa.

- **Dsecure.me** – startup świadczący usługi doradcze i prowadzący szkolenia w dziedzinie bezpieczeństwa danych, rozwoju infrastruktury oraz zarządzania zasobami IT, a także sprzedający rozwiązania z zakresu sprawdzania bezpieczeństwa w organizacji czy to przez testy penetracyjne, czy audyty bezpieczeństwa, czy badania podatności na zagrożenia.

- **Dynacon** – firma zajmująca się rozwiązaniami z zakresu cyfrowego bezpieczeństwa przemysłowego (w tym dla operatorów usług kluczowych) i infrastruktury krytycznej. Główny zakres działalności w tej dziedzinie to monitorowanie technologii operacyjnych (czyli samych urządzeń produkcyjnych, podłączonych do sieci), rozpoznawanie niepożądanych zdarzeń i reagowanie na nie, ochrona infrastruktury razem z narzędziami i systemami za pomocą jednokierunkowej bramy bezpieczeństwa oraz zabezpieczania danych.

- **EXATEL** – duże przedsiębiorstwo, sprzedające rozwiązania z zakresu Centrów Operacyjnych Bezpieczeństwa, ochrony przed atakami DDoS (przeprowadzanymi symultanicznie z wielu lokalizacji IP), a także oferujące oprogramowanie firewall i anti-malware, chroniące również przed wyciekiem danych. Świadczy również usługi doradcze w dziedzinie bezpieczeństwa systemów IT.

- **Infradata** – polska firma z branży informatycznej, oferująca rozwiązania dla międzynarodowych przedsiębiorstw, operatorów telekomunikacyjnych czy dostawców usług. Infradata przede wszystkim dostarcza swoim klientom rozwiązania w zakresie Cloud-Networkingu, cyberbezpieczeństwa oraz automatyzacji.

- **Nethone** – firma działająca w branży bezpieczeństwa dla środowisk płatności. Nethone, za pomocą rozwiązań opartych na sztucznej inteligencji, pozwala sprzedawcom na całym świecie lepiej obsługiwać swoich klientów i zapobiegać kradzieżom internetowym.

- **Resilia** – spółka tworząca rozwiązania w obszarze zarządzania ryzykiem w przestrzeni cyfrowej, cyberbezpieczeństwa sieci w organizacjach (czy to korporacji, czy jednostek publicznych), bezpieczeństwa informacji i danych osobowych oraz mechanizmów reagowania na niepożądane zdarzenia. Prowadzi szkolenia w zakresie cyberbezpieczeństwa i odpowiedniego zabezpieczania się przed zagrożeniami.

- **SEQRED** – przedsiębiorstwo wykorzystuje najnowsze technologie, by zapewnić klientom bezpieczeństwo cyfrowe w różnych obszarach działalności. Do głównych usług SEQRED należą testy i audyty bezpieczeństwa, bezpieczeństwo infrastruktury krytycznej czy bezpieczeństwo inteligentnych budynków.

- **Xopero** – jeden z kluczowych dostawców oprogramowania do tworzenia kopii zapasowych na rynku europejskim. Przedsiębiorstwo, w ramach swoich usług, posiada szeroki wachlarz profesjonalnych aplikacji do zabezpieczania i przywracania krytycznych danych firmowych. Jednym z produktów firmy Xopero jest Xopero Backup, a więc narzędzie do backupu i szybkiego przywracania danych.

- **Zeto Software** – firma z historią działalności sięgającą lat 70 XX w. (jeden z pionierów przedsiębiorczości IT w Polsce). Dziś Zeto zajmuje się przede wszystkim oprogramowaniem dla administracji publicznej. Głównym projektem firmy jest platforma ePUMA, umożliwiająca wirtualne załatwianie spraw urzędowych, ze szczególnym naciskiem na bezpieczeństwo danych osobowych i innych informacji poufnych. Całościowo tworzenie systemów zaufanych profili urzędowych jest głównym segmentem działalności Zeto Software.

Instytucje Otoczenia Biznesu

Do zidentyfikowanych, głównych Instytucji Otoczenia Biznesu animujących rynek i wspierających w Polsce podmioty funkcjonujące w obszarze cyberbezpieczeństwa, zaliczyć można m.in.:

- **Polski Klaster Cyberbezpieczeństwa (#CyberMadeInPoland)** – organizacja zrzeszająca kluczowych animatorów rynku cyberbezpieczeństwa w Polsce, zarówno tych prywatnych, jak i publicznych. Działalność klastra opiera się na czterech filarach: (1) edukacji rynku, w ramach której prowadzone są szkolenia w zakresie obecnych i nadchodzących wyzwań, stojących przed branżą; (2) certyfikacji i regulacji, które mają za zadanie standaryzację metod oceny zgodności produktów i usług z normami (i samo ustalanie tych norm obowiązujących na terenie RP); (3) pomocy rozwijającym się przedsiębiorstwom poprzez nadanie im „znaku jakości", co ma zachęcić klientów, często niepewnych jakości wyrobów firm oraz wspomóc ekspansję zagraniczną; (4) pomoc w poszukiwaniu finansowania na innowacyjne projekty, zarówno ze strony sektora rządowego, jak i funduszy prywatnych, wspierając przy okazji proces nawiązywania kontaktów handlowych w ramach partnerstwa publiczno-prywatnego. Klaster publikuje także coroczne raporty dotyczące kondycji polskiego przemysłu cybersec.

- **Stowarzyszenie Instytut Kościuszki** – organizacja powstała w 2000 r. jako think tank mający na celu badanie różnych aspektów postępującej już wówczas integracji Polski z Unią Europejską. Później jednak, dostrzegając rosnący stopień transformacji gospodarki w kierunku ściślejszego powiązania każdego jej aspektu z Internetem, Instytut rozszerzył swoją działalność o gospodarkę cyfrową i bezpieczeństwo cybernetyczne. Od 2015 roku Instytut corocznie organizuje Europejskie Forum Cyberbezpieczeństwa, a w ramach struktur Unii Europejskiej i innych polityczno-gospodarczych powiązań międzynarodowych (Trójmorza oraz jego związku z USA) przewodniczy kilku panelom dotyczącym polityki w zakresie bezpieczeństwa cyfrowego. Prowadzi również projekt mający na celu skupienie w Krakowie dużej grupy przedsiębiorstw związanych z technologiami z dziedziny cyberbezpieczeństwa, co ma uczynić z tego miasta hub specjalizujący się w tych technologiach. Statutowo prowadzi również działalność doradczo-ekspercką, z której czerpie dochody na inne aktywności.

- **Polski Klaster IoT & AI SINOTAIC** – jeden z najważniejszych klastrów integrujących producentów technologii związanych z Przemysłem 4.0, Internetem Rzeczy i sztuczną inteligencją w Polsce, koncentrujący się na animacji ww. obszarów na terenie śląska. Do celów statutowych klastra należy m.in. integracja przedsiębiorców i instytucji otoczenia biznesu (w tym jednostek badawczych i naukowych), animacja współpracy przy pracach B+R i komercjalizacji nowych rozwiązań oraz wsparcie w internacjonalizacji i pozyskiwaniu strategicznych kontrahentów. Celem nadrzędnym klastra jest tworzenie nowych miejsc pracy, rozwój regionu oraz zwiększenie udziału śląskich przedsiębiorców na rynkach zagranicznych. W ramach klastra zrzeszonych jest ponad 25 członków oraz niemal 20 partnerów merytorycznych (organizatorów wydarzeń targowych, centrów przedsiębiorczości czy uczelni).

Instytucje naukowe

Do zidentyfikowanych głównych jednostek naukowych/ badawczych funkcjonujących w Polsce w obszarze cyberbezpieczeństwa zaliczyć można m.in.:

- **Centrum Cyberbezpieczeństwa AGH (CC AGH)** – centrum naukowe działające w ramach krakowskiej Akademii Górniczo-Hutniczej na Wydziale Informatyki, Elektroniki i Telekomunikacji. Centrum prowadzi współpracę zarówno z ekspertami w dziedzinie bezpieczeństwa cyfrowego z sektora prywatnego, jak i z absolwentami prowadzącymi badania w innych instytutach naukowych. Z Centrum współpracują: Laboratorium Informatyki Śledczej, Instytut Kościuszki oraz stowarzyszenie Polska Platforma Bezpieczeństwa Wewnętrznego.

- **NASK - PIB** – finansowany przez rząd instytut naukowo-badawczy oraz instytucja otoczenia biznesu, mający na celu opracowywanie rozwiązań z dziedziny rozwoju sieci teleinformatycznych, infrastruktury cyfrowej oraz cyberbezpieczeństwa. Oprócz tego prowadzi w tym zakresie działania operacyjne, a także wspiera edukację cyfrową dzieci i młodzieży tak, by społeczeństwo korzystało z Internetu z pełną świadomością wirtualnych zagrożeń. NASK jest również krajową instytucją odpowiedzialną za rejestrowanie niepożądanych zdarzeń i nowych niebezpieczeństw płynących z przestrzeni cyfrowej.

- **Polska Platforma Bezpieczeństwa Wewnętrznego** – organizacja powstała w ramach współpracy uczelni wyższych i instytutów badawczych z polską Policją, która z czasem rozszerzona została o współpracę z innymi krajowymi służbami mundurowymi i regionalnymi sądami. Platforma współprowadziła ponad 30 projektów finansowych ze środków NCBR oraz funduszy europejskich. Należały do nich między innymi projekt CYCLOPES, czyli forum wymiany doświadczeń między jednostkami zajmującymi się cyberbezpieczeństwem jako głównym segmentem działalności, a instytucjami publicznymi, które dostrzegają braki w bezpieczeństwie swojej infrastruktury IT, chciałyby poprawić zabezpieczenia i dostosować je do standardów europejskich i światowych. Oprócz tego Platforma prowadziła następujące projekty: EU-HYBNET - mający przeciwdziałać zagrożeniom hybrydowym, SPARTA – polegający na opracowaniu standardów i strategicznego planu działań w zakresie cyberbezpieczeństwa na terenie Unii Europejskiej, jak również projekt w zakresie opracowania standardów dotyczących bezpieczeństwa cyfrowego dla służb mundurowych i administracji publicznej.

- **Zakład Cyberbezpieczeństwa Politechniki Warszawskiej** – działający w ramach Instytutu Telekomunikacji wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej. Zakład prowadzi badania m.in. w ramach projektu „Zaawansowane Laboratorium Kryminalistyki Śledczej”, który ma na celu opracowanie metod działania w przypadku przestępstw popełnianych w przestrzeni cyfrowej. Innymi projektami są: Platforma Detekcji Anomalii Sieciowych (PDAS), system zabezpieczeń sieci informatycznej oparty na sztucznej inteligencji SEC-NET oraz projekt SIMARGL, mający podobny cel, jak PDAS, jednak zrzeszający badaczy z wielu krajów Unii Europejskiej.

3.6. Analiza powiązań kooperacyjnych

W kontekście omówienia licznych podmiotów odgrywających kluczowe role w obszarze cyberbezpieczeństwa w Polsce wskazane jest omówienie ich wzajemnych powiązań. Podobnie jak w innych wysokotechnologicznych branżach, również i cyberbezpieczeństwo trudno rozwijać w izolacji, stąd potrzeba współpracy między podmiotami. Podstawową formą współpracy rozwojowej, podobnie jak i w innych branżach, są doraźnie tworzone konsorcja lub podwykonawstwo w projektach B+R.

Projekty B+R, często finansowane ze źródeł publicznych (np. NCBR, PARP), realizowane są głównie w formie partnerstwa przemysłu z nauką. Środowiska naukowe są reprezentowane przez uczelnie wyższe (głównie techniczne) oraz przez instytuty badawcze. Należy jednak podkreślić, że profil instytutów wynikający z nazwy nie przesądza o zakresie posiadanych kompetencji, stąd w projektach kooperacyjnych dotyczących cyberbezpieczeństwa mogą brać udział instytuty branżowe zajmujące się np. górnictwem czy logistyką. Współpraca w realizacji projektów realizowana jest w dwóch głównych modelach. Z jednej strony mamy **tworzenie konsorcjów**, w których przemysł wspólnie z ośrodkiem badawczym podpisuje umowę o realizacji projektu. Jest to rozwiązanie pożądane z punktu widzenia wydatkowania środków publicznych, jako że przynajmniej część wypracowanej własności intelektualnej pozostaje na uczelniach czy w instytutach. Umożliwia to zwiększanie konkurencyjności także polskiej nauki. Rozwiązanie to ma jednak pewne znaczące wady, które powodują, że jednostki badawcze wolą uczestniczyć w projektach jako **podwykonawcy** dla przedsiębiorstw je realizujących. Powyższe wynika z następujących czynników:

- Podwykonawca przekazuje całe opracowane IP zamawiającemu co jest korzystne dla przedsiębiorcy.
- Wydatkowanie środków otrzymanych przez podmiot badawczy jako podwykonawcę jest bardziej elastyczne niż w przypadku konsorcjów, co pozwala płynnie zarządzać wysokością wynagrodzeń i łatwo przesuwać środki budżetowe. Łatwiejsze jest również naliczanie kosztów pośrednich przez podmiot badawczy.
- Premiowanie podwykonawstwa w systemie ewaluacji jednostek naukowych. Zgodnie z zasadami ewaluacji opracowanymi w tzw. Ustawie 2.0 - realizowanie zleceń dla przemysłu jest w ewaluacji warte 5 razy więcej punktów niż realizacja projektu w konsorcjum.

Takie mechanizmy zachęty powodują, że zamiast długotrwałych kooperacji realizacja projektów B+R ma bardziej charakter doraźnych usług.

Innym źródłem kooperacji przemysł-nauka lub przemysł-przemysł jest **sieć Hubów innowacji cyfrowych**. Tworzą ją obecnie pięć ośrodków skupionych wokół kilku technologicznych liderów: Krakowski Park Technologiczny, Politechnika Wrocławska, Fundacja UAM - Poznański Park Naukowo-Technologiczny, Voicelab.AI oraz Instytut Łączności – Państwowy Instytut Badawczy. Sieć składa się z następujących „hubów”:

- hub4industry (Kraków)
- Level 4.0 (Wrocław)
- DIH4Future (Poznań)
- dih4.ai (Gdańsk)
- DIH 5G (Warszawa)

Łączą one wiele podmiotów w celu wsparcia przedsiębiorców w rozwoju różnych technologii cyfrowych, m.in. cyberbezpieczeństwa.

Działania „hubów" koncentrują się na wielu obszarach. Zajmują się one informacją o potencjale transformacji przemysłowej i jej skutkach dla modeli biznesowych. Realizują działania demonstracyjne, dzięki którym przedsiębiorcy będą mogli w sposób praktyczny zapoznać się z procesami opartymi na technologiach cyfrowych wraz z możliwością wykorzystania ich w swojej firmie (symulacja procesów, wykonanie prototypów). Zajmują się edukacją i szkoleniami, których celem jest przekazanie przedsiębiorcom i ich (potencjalnym) pracownikom wiedzy z zakresu technologii cyfrowych i umiejętności ich stosowania. Podmioty te świadczą również doradztwo, które może polegać na wskazaniu przez Hub możliwości wprowadzenia optymalizacji lub innowacji w sposobie wytwarzania produktów lub świadczenia usług. Ponadto współpraca może zakończyć się przygotowaniem dla danego przedsiębiorcy **planu transformacji cyfrowej**. Oferowane są również inne działania, jak np. pomoc przy integracji i uruchamianiu nowych maszyn, urządzeń oraz oprogramowania. Program Hubów innowacji cyfrowej trwa do listopada 2021 roku (stan na moment przeprowadzenia analizy, tj. październik 2021 r.), przy czym przygotowywane jest jednak jego rozwinięcie w postaci programu **Europejskich Hubów Innowacji Cyfrowych (EDIH)**, których w Polsce ma być od 8 do 16.

Istotnym aspektem kooperacji w Polsce jest również działanie na poziomie rządowym. **Program Współpracy w Cyberbezpieczeństwie (PWCyber)** jest niekomercyjną inicjatywą o charakterze partnerstwa publiczno-prywatnego. Program jest zbieżny z celami Strategii Cyberbezpieczeństwa RP na lata 2019-2024. Strony porozumienia zobowiązują się do wymiany doświadczeń po to, by m.in. zwiększyć bezpieczeństwo cyfrowych procesów, produktów i usług. Do tej pory indywidualne porozumienia z rządem podpisały m.in. firmy: Samsung, Cisco, Ericsson, Nokia, Krypton, IBM, Thales, Dynacon, Dell, Mediarecovery i Smartech-IT. Podpisane porozumienia obejmują takie obszary jak: informacja, edukacja, szkolenia i testy oraz certyfikacja, w tym przede wszystkim:

- Podnoszenie kompetencji w zakresie świadomości zagrożeń oraz metod ataków w cyberprzestrzeni.
- Identyfikacja podatności i zagrożeń oraz wymiana informacji.
- Opracowywanie rekomendacji w zakresie konfiguracji urządzeń i oprogramowania.
- Przygotowanie i prowadzenie oceny oraz certyfikacji cyberbezpieczeństwa.

- Promowanie innowacyjnych rozwiązań i projektów w dziedzinie cyberbezpieczeństwa oraz budowanie partnerstwa z podmiotami Krajowego Systemu Cyberbezpieczeństwa.

Do tego porozumienia przystąpił również m.in. opisywany wcześniej Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland.

Na polskim rynku zidentyfikowano również inne inicjatywy wspierające kooperacje w zakresie cyberbezpieczeństwa. Można tu wspomnieć np. fundacje: Klaster Cyberbezpieczeństwa Przemysłowego Energii oraz Klaster Automatyki, Sztucznej Inteligencji i Robotyki; organizacje: Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego – ZIPSEE Cyfrowa Polska oraz Polskie Towarzystwo Informatyczne. Nie należy również zapominać o inicjatywach lokalnych, takich jak Polski Klaster IoT & AI SINOTAIC, zlokalizowany na śląsku.

Z przedstawionych wyżej informacji wynika, że kooperacja na rynku cyberbezpieczeństwa jest cały czas rozwijana. Oprócz wsparcia oferowanego przez różne instytucje i organizacje oraz programów dofinansowujących prace B+R mamy też wiele wydarzeń i inicjatyw umożliwiających nawiązywanie nowych relacji i współpracy. Należy podkreślić, że jest jeszcze sporo niewykorzystanego potencjału w zakresie kooperacji. Przyczyną takiego stanu rzeczy są m.in. skomplikowane relacje między sektorem nauki a przemysłem.

3.7. Najważniejsze cykliczne wydarzenia branżowe

Wydarzenia branżowe mają na celu zrzeszenie specjalistów reprezentujących konkretną dziedzinę, budowanie społeczności oraz rozpoczęcie dyskusji nt. obszaru wiedzy/ rynku powiązanym z daną branżą. Spotkania branżowe, konferencje i sympozja z zakresu cyberbezpieczeństwa skupiają się przede wszystkim na innowacyjnych technologiach oraz najnowszych trendach w branży, przyciągając specjalistów reprezentujących rozmaite segmenty klienckie. Interdyscyplinarność całego obszaru cyberbezpieczeństwa powoduje jednocześnie, że jedne wydarzenia skupiają się mocniej wokół konkretnych rozwiązań z zakresu bezpieczeństwa IT, gdy inne wagę przykładają bardziej do dyskusji o możliwościach rozwoju całej branży czy tworzeniu wokół niej społeczności. Warto nadmienić, że na branżowych wydarzeniach poruszana jest zarówno ogólna tematyka cyberbezpieczeństwa, jak i równie często poświęcane są one konkretnym zagadnieniom/ segmentom – takim jak Internet Rzeczy, sztuczna inteligencja czy cyberbezpieczeństwo w Przemyśle 4.0. W ten sposób wyróżnić możemy targi dotyczące całej branży, jak i wydarzenia dedykowane danej rodzinie produktowej (z reguły zauważalnie mniejsze, zrzeszające animatorów danego segmentu).

Do istotnych **organizowanych w Polsce** wydarzeń targowych oraz konferencji, popularnych wśród specjalistów ds. cyberbezpieczeństwa należą m.in.:

Tabela 2. Najważniejsze wydarzenia branżowe skupione wokół obszaru cyberbezpieczeństwa organizowane w Polsce

Nazwa wydarzenia	Opis wydarzenia
BSides Warsaw	Polska edycja międzynarodowego wydarzenia z serii Security BSides. Celem konferencji jest prowadzenie dialogu oraz stworzenie platformy dla wszystkich zainteresowanych cyberbezpieczeństwem. Tematy poruszane na konferencji to m.in. sztuczna inteligencja, cyberbezpieczeństwo oraz hacking. Wydarzenie organizowane jest w Warszawie.
CONFidence	CONFidence to międzynarodowa konferencja informatyczna zainicjowana w 2005 r. Główną ideą wydarzenia jest dostarczanie praktycznej, dogłębnej wiedzy technicznej dla specjalistów, programistów, menedżerów, przedstawicieli sektora bankowego oraz rządu. Wydarzenie organizowane jest w Krakowie.
CyberGOV	Konferencja poświęcona zagadnieniu cyberbezpieczeństwa w sektorze publicznym. Podczas wydarzenia poruszana jest tematyka Ustawy o Krajowym Systemie Cyberbezpieczeństwa, realiów funkcjonowania urzędów w Polsce czy obszarów technicznych i organizacyjnych administracji publicznej koniecznych do aktualizacji. Wydarzenie organizowane jest w Warszawie.
CyberSecForum	Wiodąca konferencja poświęcona strategicznym aspektom narodowego cyberbezpieczeństwa. Impreza podąża również za cyfrowymi megatrendami i ma swój udział w wyznaczaniu strategicznych kierunków rozwoju polskiego systemu cyberbezpieczeństwa oraz polityk publicznych. Wydarzenie organizowane jest w Katowicach.
InfraSEC Forum	Wiodąca konferencja o bezpieczeństwie systemów SCADA, rozwiązań klasy ICS oraz infrastruktury OT. Szczególny nacisk kładziony jest na praktyczne aspekty cyberbezpieczeństwa z wykorzystaniem najnowszych technologii i inteligentnych rozwiązań. Wydarzenie organizowane jest w Warszawie.
KSC Forum	Konferencja skoncentrowana ściśle na spełnieniu wymogów ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) na poziomie danego przedsiębiorstwa i instytucji. Wydarzenie obejmuje szerokie spektrum tematów dotyczących ustawy o KSC – od zagadnień prawnych, poprzez proces wdrożenia, współpracę, budowanie SOC, współpracę między

Nazwa wydarzenia	Opis wydarzenia
	przedsiębiorstwami, kontekst rozporządzeń i towarzyszących aktów regulacyjnych. Wydarzenie organizowane jest w Warszawie.
Oh My H@ck	Oh My H@ck to konferencja ITSEC, stworzona dla polskich inżynierów bezpieczeństwa (poprzednia nazwa: What The H@ck). Wydarzenie daje szansę na spotkanie się z najlepszymi ekspertami z zakresu cyberbezpieczeństwa, hakerami i przedstawicielami branży fintech, a także poznanie najbardziej aktualnych tematów z zakresu bezpieczeństwa. Odbywa się wyłącznie wirtualnie.
Polski Kongres Cyberbezpieczeństwa	Wydarzenie dotyczące ogólnej tematyki cyberbezpieczeństwa dla przedsiębiorstw i instytucji, skupiające się na dyskusjach o rozwoju całej branży i bezpieczeństwu Internetu w Polsce. Zagadnienia poruszane na konferencji to m.in. bezpieczeństwo urządzeń mobilnych, bezpieczeństwo infrastruktury sieciowej, a także bezpieczeństwo danych w chmurze. Wydarzenie organizowane jest w Warszawie.
Securak Hacking Party	Wydarzenie dotyczące głównie tematyki cyberbezpieczeństwa oraz hackingu organizowane przez portal Securak.pl. Wydarzenie organizowane jest w Krakowie.
Secure	Konferencja poświęcona tematyce cyberbezpieczeństwa. Tematy poruszane podczas wydarzenia to m.in.: wyłudzenia danych, przejęcia kont społecznościowych czy cyberataki typu DDoS. Wydarzenie organizowane jest w Warszawie.
Security Case Study (SCS)	Jedna z bardziej znanych konferencji z zakresu IT Security, poświęcona w całości cyberbezpieczeństwu. SCS skupia menedżerów i dyrektorów IT, szefów działów bezpieczeństwa, osoby odpowiedzialne za administrowanie sieciami i systemami IT oraz szefów działów audytu. Zagadnienia poruszane na wydarzeniu to m.in. Krajowy system cyberbezpieczeństwa, ale i najbardziej aktualne tematy branżowe. Wydarzenie organizowane jest w Warszawie.
Semafor	Jedno z najważniejszych wydarzeń dotyczących świata bezpieczeństwa informacji i audytu IT. Konferencja umożliwia zapoznanie się z bieżącymi zagrożeniami i ciekawymi studiami przypadku z zakresu cyberbezpieczeństwa. Wydarzenie organizowane jest w Warszawie.

Źródło: opracowanie własne

Odnosząc się z kolei do **globalnych** wydarzeń targowych, konferencji i sympozjów naukowych związanych w możliwie największym stopniu z cyberbezpieczeństwem, wymienić należy m.in.:

Tabela 3. Zestawienie wybranych międzynarodowych wydarzeń targowych, sympozjów i konferencji naukowych, w możliwie największym stopniu skupionych wokół obszaru cyberbezpieczeństwa

Nazwa wydarzenia	Opis wydarzenia
CA Day	Wydarzenie organizowane przez ENISA (European Union Agency for Cybersecurity) we współpracy z Komisją Europejską, skupiające się w największym stopniu na usługach zaufania. Forum ma na celu: dzielenie się doświadczeniami z zakresu wdrażania usług zaufania; omówienie najnowszych zmian dotyczących dostawców usług zaufania, w tym norm, aktów wykonawczych i wytycznych technicznych; wymianę poglądów na temat problemów związanych z wdrażaniem i obsługą usług zaufania; omówienie strategii promowania usług zaufania. Konferencja organizowana jest w Berlinie.
CA/ Browser Forum	Konferencja przeznaczona dla urzędów certyfikacji oraz dostawców oprogramowania organizowana w Nowym Jorku. Tematy poruszane na forum to m.in.: bezpieczeństwo sieciowe urzędów certyfikacji czy wytyczne branżowe dotyczące wydawania i zarządzania certyfikatami.
Chaos Communication Congress	Wiodąca konferencja organizowana przez Chaos Computer Club obejmująca różnorodne wykłady i warsztaty dotyczące zagadnień technicznych i politycznych związanych z bezpieczeństwem, kryptografią, prywatnością i wolnością słowa w Internecie. Wydarzenie organizowane jest co roku w Berlinie.
Cyber Defence Summit	Międzynarodowe wydarzenie dotyczące tematyki cyberbezpieczeństwa nastawione na łączenie ekspertów z branży. Konferencja poświęcona jest głównie zagadnieniom bezpieczeństwa w czasach zdalnej pracy oraz nauki. Forum organizowane jest w Waszyngtonie.
DEF CON	Jeden z najbardziej znanych na świecie kongresów z branży hakerskiej. Uczestnicy wydarzenia to przede wszystkim specjaliści od cyberbezpieczeństwa, dziennikarze, prawnicy, pracownicy rządu federalnego oraz badacze cyberbezpieczeństwa. Forum organizowane jest co roku w Las Vegas.

Nazwa wydarzenia	Opis wydarzenia
ENISA IoT Security Conference	Konferencja międzynarodowa, organizowana przez ENISA (European Union Agency for Cybersecurity), o tematyce cyberbezpieczeństwa w obszarze Internetu rzeczy. Wydarzenie organizowane jest co roku w innym, europejskim mieście.
ETSI Security Week	Flagowe wydarzenie ETSI poświęcone tematyce cyberbezpieczeństwa, gdzie omawiane są przede wszystkim nowości z branży w zakresie: bezpieczeństwa sztucznej inteligencji (AI), bezpieczeństwa Internetu rzeczy (IoT), wirtualizacji funkcji sieciowych (NFV), polityki bezpieczeństwa cybernetycznego, a także Multi Access Edge Computing (MEC). Konferencja organizowana jest w Nicei.
GITEX	Wiodące światowe wydarzenie technologiczne organizowane od 40 lat dot. m.in.: sztucznej inteligencji, analizy danych, a także cyberbezpieczeństwa. Wydarzenie organizowane jest w Dubaju.
Infosecurity	Największe spotkanie społeczności zajmującej się bezpieczeństwem informacji w Europie stworzone dla dużych firm oraz organizacji. Głównym tematem są innowacje i nowe technologie w zakresie cyberbezpieczeństwa. Wydarzenie organizowane jest w Londynie.
International Cybersecurity Forum	Wiodące, europejskie wydarzenie poświęcone tematyce cyberbezpieczeństwa, skupione na dyskusji wokół wizji europejskiego rynku bezpieczeństwa cyfrowego. Tematy poruszane na konferencji to m.in. cyberbezpieczeństwo dla przemysłu czy bezpieczeństwo e-konsumentów. Wydarzenie organizowane jest w Lille.
IoT Solutions World Congress	Globalna konferencja dla dyrektorów biznesowych i technicznych. Główne tematy poruszane na wydarzeniu to bezpieczeństwo (w tym cyberbezpieczeństwo), sztuczna inteligencja czy rozwiązania dla rynku łączności. Spotkanie organizowane jest w Barcelonie.
IP SoC Conference	Wiodące wydarzenie w obszarze własności intelektualnej oraz systemów elektronicznych opartych na IP. Tematy poruszane na konferencji, to między innymi: cyberbezpieczeństwo, sztuczna inteligencja czy też 5G. Wydarzenie o charakterze wirtualnym.

Nazwa wydarzenia	Opis wydarzenia
IT Nation Secure	IT Nation Secure, to hybrydowe wydarzenie poświęcone cyberbezpieczeństwu, stworzone, aby pomóc firmom zmniejszyć ryzyko związane z cyberatakami, a także by pomóc w przekształceniu i usprawnieniu świadczenia usług w zakresie rozwiązań cyberbezpieczeństwa dla klientów. Wydarzenie organizowane jest w Orlando.
KB4-CON	Największa międzynarodowa konferencja z zakresu świadomości cyberbezpieczeństwa. Wydarzenie pomaga organizacjom zająć się ludzkim czynnikiem w aspekcie cyberbezpieczeństwa poprzez podnoszenie świadomości na temat oprogramowania ransomware. Podczas forum prezentowane jest przede wszystkim nowe podejście do szkoleń w zakresie bezpieczeństwa cyfrowego. Wydarzenie od 2020 r. organizowane jest w formie zdalnej.
Mobile World Congress (MWC)	MWC Barcelona, to jedno z bardziej wpływowych wydarzeń na świecie dla branży mobilnej łączności. W konferencji biorą udział globalni operatorzy telefonii komórkowej, producenci urządzeń, dostawcy technologii, sprzedawcy i właściciele dużych firm branżowych. Tematy poruszane na forum to m.in.: 5G, bezpieczeństwo branży łączności czy Internet Rzeczy.
RSA Conference	Wiodąca i obecna na świecie od prawie 30 lat konferencja z zakresu cyberbezpieczeństwa. Główną ideą wydarzenia jest łączenie uczestników z doświadczonymi specjalistami i przekaz bieżących informacji dot. branży. Wydarzenie organizowane cyklicznie w różnych miastach USA, Wielkiej Brytanii, Japonii oraz Zjednoczonych Emiratów Arabskich.
Security BSides	Międzynarodowe wydarzenie zrzeszające specjalistów oraz początkujących w branży cyberbezpieczeństwa. Na konferencji, każdy, niezależnie od doświadczenia, ma szansę do zaprezentowania swojego projektu. Spotkanie organizowane jest w różnych miastach na całym świecie (m.in. Birmingham, Liverpool, Barcelona).
ZeroNights	Międzynarodowa konferencja poświęcona praktycznej stronie cyberbezpieczeństwa. ZeroNights skupia ekspertów, praktyków bezpieczeństwa informacji, analityków i hakerów z całego świata, by przedstawić nowe metody cyberataków oraz sposób obrony przed nimi. Wydarzenie organizowane jest w Moskwie.

Źródło: opracowanie własne

3.8. Otoczenie prawne i ochrona własności intelektualnej

Przygotowując się do inwestycji związanych z obszarem cyberbezpieczeństwa na rynku polskim również należy zapoznać się z aktami prawnymi regulującymi poszczególne obszary technologiczne i segmenty branżowe. Ze względu na fakt, iż Polska jest członkiem Unii Europejskiej, w rozdziale tym zostaną przedstawione zarówno polskie, jak i unijne regulacje.

Kluczowym aktem prawnym w Polsce dla rynku cyberbezpieczeństwa jest ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.[31] Ustawa ta wdraża do krajowego porządku prawnego Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[32]. Ustawa o Krajowym systemie cyberbezpieczeństwa określa organizację oraz sposób funkcjonowania krajowego systemu cyberbezpieczeństwa oraz sprawowania nadzoru i kontroli w zakresie stosowania jej przepisów; uzupełniająco ustawa normuje także zakres i tryb stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej[33].

Pod koniec 2020 r. Komisja Europejska zakończyła proces rewizji Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 i przedstawiła propozycję nowej, kompleksowej regulacji[34]. Przepisy te mają całkowicie zastąpić Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148, eliminując jej słabości i znaczące różnice w implementacji pomiędzy poszczególnymi państwami członkowskimi (wprowadzając jasne kryterium, kto jest nią objęty). Zgodnie z projektem Dyrektywy, kraje członkowskie powinny zapewnić, że podmioty objęte regulacją podejmą odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, które podmioty te wykorzystują przy świadczeniu swoich usług. Wdrożenie Dyrektywy wymagać będzie w dalszej perspektywie zmian

---

[31] Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r., tj. Dz.U. z 2020 r. poz. 1369, dalej jako KSC.

[32] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.Urz. UE L 194, s. 1.

[33] Aktualna przyjęta Uchwałą Nr 125 Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 z dnia 22 października 2019 r., M.P. z 2019 r. poz. 1037, dalej Strategia.

[34] Tekst projektu Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej Dyrektywę (UE) 2016/1148 z dnia 16.12.2020 COM (2020) 823 final, 2020/0359(COD) można znaleźć pod linkiem: https://eur-lex.europa.eu/legal-content/EN-PL/TXT/?from=EN&uri=CELEX%3A52020PC0823. Dostęp: 27.10.2021.

w polskim krajowym systemie cyberbezpieczeństwa, w którego skład wejdzie więcej podmiotów niż dotychczas.

W kwestiach cyberbezpieczeństwa i ochrony danych osobowych szczególnie istotne jest również przestrzeganie przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (dalej RODO)[35] oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[36]. Pomocne są również wskazówki i decyzje Prezesa publikowane na stronie Urzędu Ochrony Danych Osobowych.

Uczestnicy rynku zobligowani są również do zaprojektowania i wdrożenia systemu zarządzania incydentami – wykonany prawidłowo powinien opierać się na uznawanych, międzynarodowych standardach oraz zapewniać zgodność z wymogami RODO, Dyrektywą 2016/1148 oraz Ustawą o Krajowym systemie cyberbezpieczeństwa. W zakresie zarządzania incydentami naruszenia bezpieczeństwa danych osobowych powszechnie stosowanym standardem jest norma ISO 27035[37]. Podmioty świadczące usługi kluczowe są zobowiązane wdrożyć system zarządzania ciągłością działania w zakresie obsługi incydentu zgodny z normą ISO 22301[38].

Ważnym obszarem legislacyjnym związanym z cyberbezpieczeństwem jest również komunikacja elektroniczna. Zagadnienia te normowane są przez 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 elektronicznych na rynku wewnętrznym[39] oraz ustawę o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r.[40] Rozporządzenie 910/2014 wprowadziło obowiązek wzajemnego uznawania przez państwa członkowskie UE wydawanych środków identyfikacji elektronicznej, które mają stać się odpowiednikami tradycyjnych dokumentów tożsamości w świecie cyfrowym. Na początku czerwca 2021 r. pojawił

---

[35] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE.L 2016 Nr 119, str. 1).

[36] Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000 tj. Dz.U. z 2019 r. poz. 1781).

[37] Norma zawierająca najlepsze praktyki i wytyczne w zakresie wdrażania Systemu Zarządzania Incydentami Bezpieczeństwa Informacji, ISO 27035, https://www.iso.org/standard/60803.html. Dostęp: 25.11.21.

[38] Norma PN-EN ISO 22301:2014-11 „Bezpieczeństwo powszechne – Systemy zarządzania ciągłością działania – Wymagania".

[39] 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 elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, (Dz.Urz.UE.L Nr 257, str. 73).

[40] Ustawa o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. tj. Dz.U. z 2021 r. poz. 1797.

się również projekt zmian Rozporządzenia 910/2014[41], zgodnie z którym w ciągu 12 miesięcy od wejścia w życie nowelizacji każde państwo członkowskie UE będzie miało obowiązek wdrożyć tzw. Europejski Portfel Tożsamości Cyfrowej (dalej: **EPTC**). Przedsiębiorcy oraz osoby fizyczne będą miały możliwość załatwiania spraw przed organami publicznymi każdego z państw członkowskich za pomocą EPTC.

Od lat stopniowo zwiększane są kompetencje standaryzacyjne i regulacyjne Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (dalej: **ENISA**). Organ powołany w 2004 r. miał za zadanie ułatwiać współpracę i wymianę doświadczeń pomiędzy państwami członkowskimi[42]. Wraz ze wzrostem znaczenia unijnego projektu jednolitego rynku cyfrowego, rozszerzone zostały rola i kompetencje ENISA, zgodnie z przyjętą w 2016 r. Dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.[43] ENISA otrzymała nowe uprawnienia polegające na wydawaniu porad i wytycznych dotyczących standaryzacji mechanizmów bezpieczeństwa IT w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych na poziomie Unii. Kolejną zmianą było wejście w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych[44]. Na mocy tego Rozporządzenia ENISA otrzymała nowe kompetencje związane z procesem wydawania unijnych schematów certyfikacji w obszarze cyberbezpieczeństwa (European cybersecurity certification schemes).

W Polsce i Unii Europejskiej obowiązują również: Regulamin ONZ nr 155 z dnia 9 marca 2021 r. – Jednolite przepisy dotyczące homologacji pojazdów w zakresie cyberbezpieczeństwa i systemu zarządzania bezpieczeństwem [2021/387] (dalej: **Regulamin ONZ nr 155**)[45] oraz Regulamin ONZ

---

[41] Tekst propozycji nowelizacji Rozporządzenia 910/2014 można znaleźć pod linkiem: https://www.politico.eu/wp-content/uploads/2021/06/03/amdening-regulation.pdf. Dostęp: 25.11.2021.

[42] Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z 10.03.2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (Dz.Urz. UE L 77, s. 1).

[43] Dyrektywa 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, Dz.Urz.UE.L 2016 Nr 194, str. 1.

[44] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), z dnia 17 kwietnia 2019 r. (Dz.Urz.UE.L Nr 151, str. 15).

[45] Regulamin ONZ nr 155 - Jednolite przepisy dotyczące homologacji pojazdów w zakresie cyberbezpieczeństwa i systemu zarządzania bezpieczeństwem [2021/387] (Dz.U.UE.L.2021.82.30 z dnia 9 marca 2021 r.).

nr 156 z dnia 9 marca 2021 r. - Jednolite przepisy dotyczące homologacji pojazdów w zakresie aktualizacji oprogramowania i systemu zarządzania aktualizacjami oprogramowania [2021/388] (dalej: **Regulamin ONZ nr 156**)[46]. Wymienione akty określają np. w jaki sposób ubiegać się o homologację typu pojazdu w zakresie cyberbezpieczeństwa oraz jakie są wymagania systemu zarządzania cyberbezpieczeństwem (Regulamin ONZ nr 155) lub w jaki sposób ubiegać się o homologację typu pojazdu w zakresie procesów aktualizacji oprogramowania oraz wymagania dotyczące systemu zarządzania aktualizacjami oprogramowania producenta pojazdów (Regulamin ONZ nr 156).

W związku z rozwojem Internetu Rzeczy niewykluczone, że w najbliższym czasie konsumenci często będą słyszeć o zgodności produktów z normą ETSI EN 303 645[47]. Norma ta określa 13 przepisów dotyczących bezpieczeństwa urządzeń konsumenckich podłączonych do Internetu. Opracowana przez Komitet Techniczny ds. Cyberbezpieczeństwa Europejskiego Instytutu Norm Telekomunikacyjnych potwierdza, że dany produkt osiągnął wymagany podstawowy poziom bezpieczeństwa informacji. Pojawienie się i funkcjonowanie w obrocie normy ETSI EN 303 645 zwiększa świadomość konsumentów w zakresie cyberbezpieczeństwa.

Prawo własności przemysłowej chronione jest w Polsce na podstawie Ustawy prawo własności przemysłowej z dnia 30 czerwca 2000 roku[48] regulującej zagadnienia materialne i procesowe związane z uzyskiwaniem praw własności przemysłowej. Wspólną ścieżkę zgłaszania i udzielania patentów europejskich, obowiązujących w każdym z państw-członków Europejskiej Organizacji Patentowej (w tym w Polsce) wskazanych przez wnioskodawcę we wniosku o udzielenie patentu europejskiego ustala Konwencja o udzielaniu patentów europejskich[49]. Ochronę znaków towarowych na obszarze Unii Europejskiej reguluje Rozporządzenie Parlamentu Europejskiego

---

[46] Regulamin ONZ nr 156 - Jednolite przepisy dotyczące homologacji pojazdów w zakresie aktualizacji oprogramowania i systemu zarządzania aktualizacjami oprogramowania [2021/388] (Dz.U.UE.L.2021.82.60 z dnia 9 marca 2021 r.).

[47] Norma ETSI EN 303 645 Europejskiego Instytutu Norm Telekomunikacyjnych wydana w wersji v2.1.1 w czerwcu 2020 r. dostępna pod linkiem: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf. Dostęp: 25.11.2021

[48] Ustawa prawo własności przemysłowej z dnia 30 czerwca 2000 r. tj. Dz.U. z 2021 r. poz. 324.

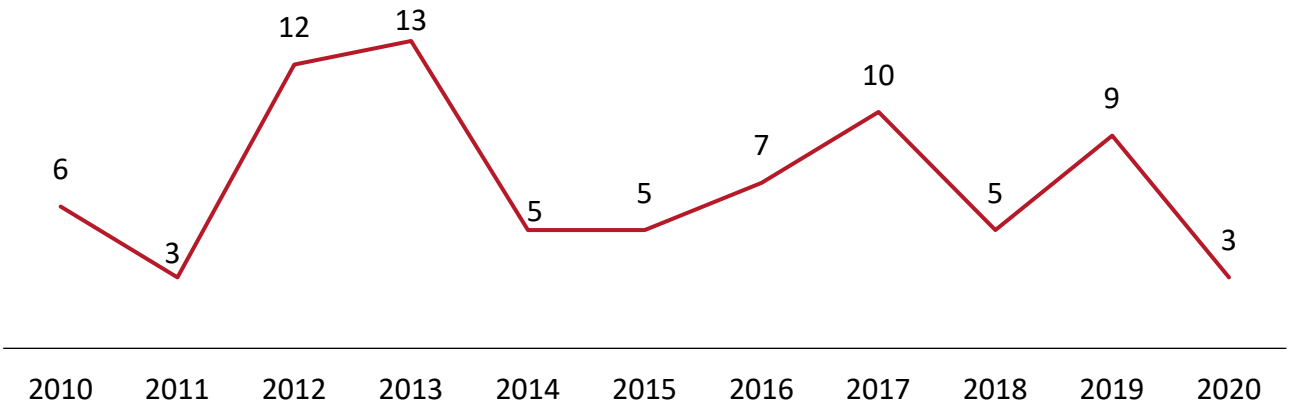
[49] Konwencja o udzielaniu patentów europejskich, sporządzona w Monachium dnia 5 października 1973 r., zmieniona aktem zmieniającym artykuł 63 Konwencji z dnia 17 grudnia 1991 r. oraz decyzjami Rady Administracyjnej Europejskiej Organizacji Patentowej z dnia 21 grudnia 1978 r., 13 grudnia 1994 r., 20 października 1995 r., 5 grudnia 1996 r. oraz 10 grudnia 1998 r., wraz z Protokołami stanowiącymi jej integralną część (Dz. U. z 2004 r. Nr 79, poz. 737), Akt z dnia 29 listopada 2000 r. rewidujący Konwencję o udzielaniu patentów europejskich, sporządzoną w Monachium dnia 5 października 1973 r. (Dz. U. z 2007 r. Nr 236, poz. 1736).

i Rady (UE) 2017/1001 w sprawie znaku towarowego Unii Europejskiej[50]. Ochronę wzorów wspólnotowych, które gwarantują ochronę wzorów na terenie Unii Europejskiej, reguluje Rozporządzenie Rady (WE) NR 6/2002 w sprawie wzorów wspólnotowych[51].

Analizując **otoczenie patentowe w Polsce** należy brać pod uwagę zarówno zgłoszenia patentowe i patenty polskie (udzielane przez Urząd Patentowy RP), jak również europejskie zgłoszenia patentowe i patenty europejskie udzielane przez Europejski Urząd Patentowy, które po przeprowadzeniu procesu walidacyjnego[52] uzyskują ochronę na terytorium Polski.

Jak widać na Rysunku 21, liczba publikacji polskich zgłoszeń patentowych dotyczących cyberbezpieczeństwa (kryterium wyszukiwania: hasła komputer, zabezpieczenie/ bezpieczeństwo w skrócie zgłoszenia patentowego, aby wskazać wprost tego typu rozwiązania) jest znikoma (biorąc pod uwagę, że corocznie jest dokonywanych kilka tysięcy zgłoszeń patentowych). Wynika to z faktu, że do czasu nowelizacji ustawy prawo własności przemysłowej z 2019 r. rozwiązania z zakresu programów komputerowych nie były uznawane za posiadające zdolność patentową.

Rysunek 21. Liczba polskich zgłoszeń patentowych dotyczących cyberbezpieczeństwa opublikowanych w latach 2010 - 2020



Źródło: badanie własne w bazie danych UPRP

[50] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1001 z dnia 14 czerwca 2017 r. w sprawie znaku towarowego Unii Europejskiej (Dz. Urz. UE. L 2017 Nr 154, str. 1).

[51] Rozporządzenie Rady (WE) nr 6/2002 z dnia 12 grudnia 2001 r. w sprawie wzorów wspólnotowych (Dz. Urz. UE. L 2002 Nr 3, str. 1).

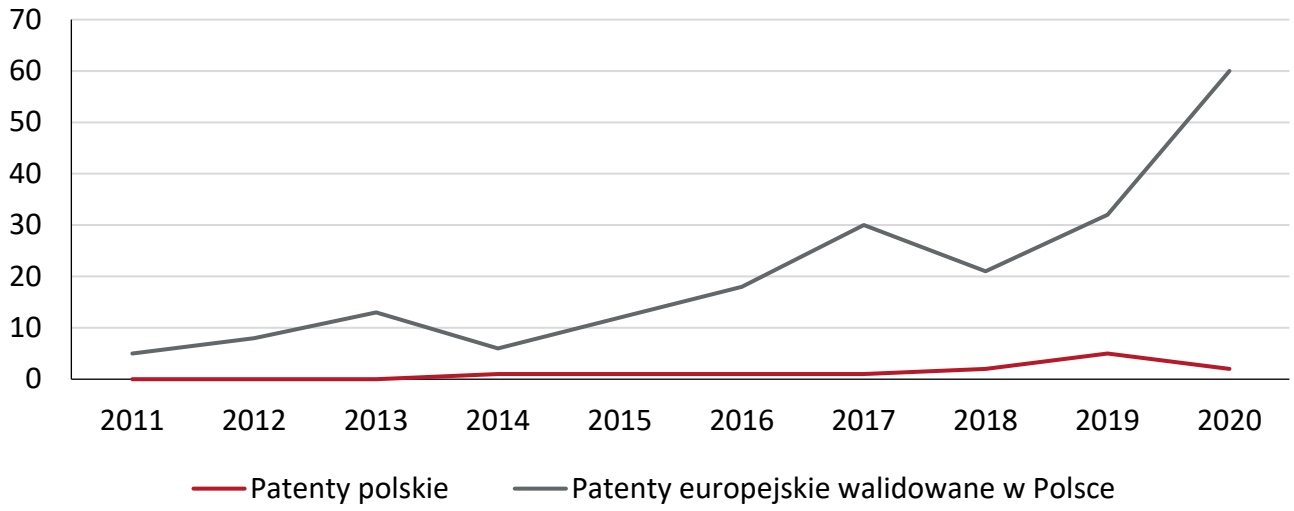
[52] Walidacja może zostać dokonana w ciągu 3 miesięcy od publikacji patentu. W Polsce do dokonania walidacji konieczne jest złożenie wniosku i tłumaczenia dokumentacji patentowej na język polski. UPRP bada jedynie kwestie formalne i nie przeprowadza badania merytorycznego. Walidowany patent europejski przyznaje właścicielowi taką samą ochronę, jak patent krajowy.

Zgłoszenia te dotyczyły zatem głównie rozwiązań z zakresu elektroniki, w szczególności rozwiązań do stosowania w przemyśle i z zakresu kryptografii. Zgłaszającymi te rozwiązania były zarówno uczelnie wyższe, jak i przedsiębiorstwa oraz osoby fizyczne.

Uzyskanie ochrony patentowej z zakresu cyberbezpieczeństwa w Polsce było więc możliwe w praktyce przede wszystkim za pośrednictwem Europejskiego Urzędu Patentowego, który traktuje rozwiązania z tej dziedziny jako posiadające charakter techniczny i udziela w tym zakresie patenty.

Rysunek 22 ilustruje liczbę patentów dotyczących cyberbezpieczeństwa w dziedzinie kryptografii (kryterium doboru: klasa patentowa H04L9), jako obiektywnie najprecyzyjniej możliwych do porównania, opublikowanych w latach 2011 - 2020, z podziałem na patenty polskie i patenty europejskie walidowane w Polsce (porównanie nie obejmuje zgłoszeń patentowych, gdyż liczba zgłoszeń europejskich jest około stukrotnie większa od liczby zgłoszeń polskich, lecz tylko część patentów jest walidowana w Polsce).

Rysunek 22. Liczba corocznych publikacji nowych patentów dotyczących cyberbezpieczeństwa wraz z liczbą patentów walidowanych w Polsce w latach 2011 – 2020



Źródło: badanie własne w bazie danych UPRP

Jak wynika z Rysunku 22, liczba nowych patentów polskich publikowanych co roku utrzymuje się na znikomym poziomie kilku sztuk (i dotyczy przede wszystkim rozwiązań sprzętowych), podczas gdy wyraźnie widać rosnący trend w liczbie patentów europejskich walidowanych w Polsce (dotyczących zarówno rozwiązań sprzętowych, jak i związanych z oprogramowaniem). Jest to zbieżne z ogólnym trendem co do rodzaju praw patentowych uzyskujących ochronę w Polsce – w 2020 r. uzyskało ochronę ok. 2 300 patentów polskich i ok. 13 000 patentów europejskich. W związku z powyższym, przy analizie stanu techniki dla nowo wdrażanych w Polsce projektów, w celu określenia czystości patentowej należy zwracać szczególną uwagę na patenty europejskie walidowane w Polsce przez podmioty zagraniczne.

Tak znikoma liczba publikacji polskich patentów w zakresie kryptografii (jak również praktyczny brak polskich patentów w innych dziedzinach cyberbezpieczeństwa, np. w zakresie zabezpieczeń sieciowych) wynika z tego, że są to w większości rozwiązania programowe, które do 2020 r. nie posiadały zdolności patentowej zgodnie z przepisami polskiej ustawy prawo własności przemysłowej. Dopiero po nowelizacji ustawy w 2019 r., od 2020 r. Urząd Patentowy RP może udzielać patentów na oprogramowanie na zasadach analogicznych do urzędu europejskiego.

W związku z powyższym nieliczne polskie patenty z zakresu cyberbezpieczeństwa dotyczą przede wszystkim rozwiązań elektronicznych, ewentualnie powiązania warstwy sprzętowej i programowej.

Pomimo braku możliwości uzyskania ochrony na rozwiązania informatyczne w Polsce, polscy przedsiębiorcy ubiegali się w niektórych przypadkach o ochronę zagraniczną. Przykładem mogą być patenty dotyczące bezpiecznej komunikacji pomiędzy urządzeniami (US10382208B2 - Olympus Sky Technologies S.A.), rejestracji danych w sieci blockchain (US10944548B2 - Confirm Blockchain Lab Sp. z o.o.), układ szyfrowania w systemie RSA (EP3561662B1 - ADIPS Sp. z o.o.) oraz zabezpieczanie transmisji w sieci LAN (EP3379794B1 - LINKK Sp. z o.o.).

Biorąc pod uwagę dużą aktywność podmiotów zagranicznych w zakresie ochrony patentowej swoich rozwiązań, w szczególności w zakresie obszarów powiązanych ze scenariuszami rozwoju, wskazane byłoby podjęcie przez podmioty z Polski intensywniejszych działań w zakresie ochrony swoich wynalazków za granicą.

3.9. Analiza trendów rozwojowych

Pomimo tego, że polski rynek cyberbezpieczeństwa jest relatywnie mały i nie jest silnie usieciowiony z rynkiem międzynarodowym, to kluczowe trendy na niego oddziaływujące nie różnią się znacząco od tych warunkujących prowadzenie biznesu w innych krajach. Ma on jednak szereg własnych uwarunkowań, które wynikają przede wszystkim z innego poziomu rozwoju branż klienckich – zacofanie jednych może powodować konieczność wdrażania bardzo tradycyjnych rozwiązań z zakresu cyberbezpieczeństwa, a inne branże mogą być na tyle rozwinięte, że konieczne będzie wdrażanie wyłącznie produktów o najwyższym poziomie skomplikowania i ochrony. Za przykład posłużyć może polski sektor bankowy, którego wysoki poziom rozwoju nawet na tle najbardziej zaawansowanych technologiczne gospodarek uwarunkował popyt na najbardziej wyspecjalizowane rozwiązania z zakresu cyberbezpieczeństwa.

Należy wyróżnić pewne tendencje, które mają charakter zdecydowanie dominujący na rynku polskim. Podstawowym zagadnieniem jest **szeroki zakres usług z obszaru cyberbezpieczeństwa**, które są świadczone przez polskie firmy. Usługi bezpieczeństwa stanowią podstawowy obszar działalności większości krajowych firm – sytuacja ta nie odbiega jednak od globalnej struktury rynku, na którym zdecydowana większość firm to właśnie podmioty usługowe. Klienci zwykle albo nie mają niezbędnego know-how lub dostępnych zasobów ludzkich, albo po prostu brakuje

im motywacji i chęci, aby poradzić sobie z tym problemem. Dlatego często decydują się na realizację kompleksowej usługi obejmującej szeroki zakres z wielu obszarów cyberbezpieczeństwa. Ponadto segment ten obejmuje również usługi wykonywane okresowo, takie jak testy penetracyjne, audyty bezpieczeństwa oraz compliance. Rozwój sektora usług jest tendencją, która będzie miała bardzo duże znaczenie w nadchodzących latach, szczególnie w kontekście pojawiania się zapotrzebowania na coraz to nowe rodzaje usług dedykowanych cyberbezpieczeństwu.

Drugi trend rozwojowy związany jest z zagadnieniami **bezpieczeństwa informacji i uwierzytelniania**. Wiele polskich firm odnotowało dotychczas znaczące sukcesy w zakresie biometrii, haseł jednorazowych, tokenów, a zagadnienia te stają się coraz bardziej istotne w kontekście nowych regulacji unijnych i nie tylko, wymagających wieloetapowego, bezpiecznego uwierzytelniania. Co więcej, także wydarzenia z życia codziennego jednoznacznie wskazują na konieczność zabezpieczeń. Warto również podkreślić silne tradycje polskiej nauki w zakresie kryptografii, która odnosiła sukcesy już przed drugą wojną światową. Stąd nadal silne ośrodki zajmujące się tą tematyką w Polsce. W kontekście zbliżającej się kwantowej rewolucji (lub co najmniej ewolucji) intensyfikują się prace nad tymi obszarami, zarówno w przedsiębiorstwach, jak też w ośrodkach badawczych. Dalszy rozwój oczywiście będzie wymagał inwestycji w te obszary.

Niezwykle dynamicznie na polskim rynku rozwijają się kwestie **bezpieczeństwa instalacji OT**, w tym procesowej i krytycznej. Istnieją już regulacje prawne dotyczące tego obszaru, a środowisko przedsiębiorców zajmujących się tymi instalacjami OT rozwija się bardzo dynamiczne. W Polsce odbywają się regularne konferencje poświęcone tej tematyce z udziałem przedstawicieli globalnych graczy, władz oraz wielu przedsiębiorców. Dalszy rozwój tego obszaru jest nieunikniony i jednocześnie bardzo wskazany w kontekście zapewnienia bezpieczeństwa łańcuchów dostaw i funkcjonowania krajowej gospodarki.

Ostatnim bardzo widocznym trendem na polskim rynku jest rozwój segmentu **urządzeń Internetu Rzeczy (IoT)**. W Polsce jest bardzo wielu producentów systemów IoT w takich obszarach jak automatyka domowa, czujniki zanieczyszczeń, sensory przemysłowe, systemy alarmowe, systemy monitoringu i wiele innych. Co więcej, bardzo szerokim zagadnieniem jest instalacja rozwiązań różnych technologii. W szczególności rynek zalewany jest produktami importowanymi bezpośrednio z Chin, mającymi bardzo niepewną strukturę bezpieczeństwa. Firmy świadczące usługi integracji systemów IoT muszą sobie jakoś z tym radzić, stąd coraz silniejsza presja na powstawanie nowych rozwiązań IoT zapewniających wysoki poziom cyberbezpieczeństwa. Firmy, które do tej pory tym zagadnieniem się nie interesowały, powoli zaczynają się rozwijać i w tym zakresie.

Wymienione powyżej cztery trendy są w tej chwili dominujące na polskim rynku cyberbezpieczeństwa. Oczywiście inne zagadnienia też są rozwijane, jak np. ochrona przed złośliwym oprogramowaniem i usługi chmurowe, jednak rozwój ten ma dużo mniejszą

intensywność i potencjał w kontekście rozwoju nisz technologicznych w obszarze cyberbezpieczeństwa w Polsce.

3.10. Analiza SWOT i PESTEL

Poniżej zaprezentowana została analiza silnych i słabych stron, szans i zagrożeń dla obszaru cyberbezpieczeństwa z perspektywy podmiotów operujących na polskim rynku – zwana **analizą SWOT**. Analiza pozwala na wyciągnie wniosków dot. całego obszaru w perspektywie głównych pozytywnych i negatywnych czynników oddziałujących na rynek, zarówno z perspektywy wewnętrznej (tej, na której strukturę uczestnicy mają wpływ – a więc silne i słabe strony), jak i zewnętrznej (tej niezależnej od samych animatorów, jednak które mogą wzmocnić silne strony lub pogłębić słabe – a więc szanse i zagrożenia). Przedstawione wnioski pochodzą od uczestników warsztatów Smart Lab.

Tabela 4. Analiza SWOT dla obszaru cyberbezpieczeństwa w Polsce

Silne strony	Słabe strony
• Niższe koszty produkcji niż w krajach zachodnich (oprócz kosztów zasobów ludzkich – które przez lata były niższe, jednak obecnie dynamicznie rosną i dorównują międzynarodowym stawkom, szczególnie w przypadku programistów). • Wysoka specjalizacja technologiczna przedsiębiorstw i ekspertów branżowych – technologie opracowywane w niektórych segmentach znacząco wyprzedzają rozwiązania komercjalizowane na rynkach zagranicznych. • Wykorzystywanie globalnych standardów i protokołów zgodności analogicznych do tych wymaganych przez zagranicznych kontrahentów. • Zdywersyfikowany popyt, generowany przez niemalże wszystkie branże produktowe i usługowe (a w szczególności te dostarczające dobra/ usługi w sferze wirtualnej).	• Niski poziom edukacji i wiedzy społeczeństwa oraz klientów biznesowych z sektora MŚP o zagrożeniach czyhających w wirtualnym środowisku oraz możliwych sposobach zabezpieczania się przed nimi. • Postrzeganie cyberbezpieczeństwa przez pryzmat „jednorazowej inwestycji", brak świadomości o konieczności ciągłego rozwijania oprogramowania i aktualizacji produktów, aby były skuteczne. • Brak promocji polskich produktów i usług na międzynarodowym rynku – potęgujący trudności w internacjonalizacji krajowych rozwiązań. • Niski poziom zaufania sektora MŚP dla usług z obszaru cyberbezpieczeństwa, błędne postrzeganie ich jako „informacji wychodzących poza przedsiębiorstwo". • Przestarzałe normy prawne i branżowe standardy regulujące wymagania odnośnie systemów cyberbezpieczeństwa – zarówno wśród przedsiębiorców świadczących

Silne strony	Słabe strony
• Istniejące laboratoria badawcze z wieloletnimi tradycjami i dużym doświadczeniem. • Duże zaangażowanie kluczowych animatorów w rozwój rynku – chęć współpracy, dzielenia się wiedzą i dyskusji na temat rozwoju całego krajowego obszaru cyberbezpieczeństwa. • Zaawansowana infrastruktura informatyczna i laboratoryjna (głównie w posiadaniu dużych przedsiębiorstw).	usługi w sferze wirtualnej, jak i tych jedynie przetwarzających w niej dane. • Niski poziom sieciowości rynku – funkcjonowanie jedynie kilku wyspecjalizowanych klastrów, które samodzielnie nie mogą zagwarantować odpowiedniego poziomu transferu wiedzy i animacji rynku. • Zauważalne braki kadrowe w obszarze cyberbezpieczeństwa, a w szczególności programistów/ analityków bez wąskiej specjalizacji branżowej. • Wysoka konkurencyjność podmiotów zagranicznych oraz ich przewaga w przetargach publicznych (z uwagi na międzynarodowe doświadczenie i sprawdzone technologie potwierdzone referencjami z ich wdrożeń). • Niskie zaufanie do polskich produktów i usług technologicznych na zagranicznych rynkach, znacząco utrudniające dotarcie do nowych klientów poza rynkiem krajowym. • Brak doświadczenia w ochronie własności intelektualnej rozwiązań z obszaru cyberbezpieczeństwa (dominacja „tajemnicy przedsiębiorstwa”). • Brak zdolności do budowy własnych układów mikroelektronicznych, jak i analizy bezpieczeństwa istniejących układów – co ogranicza możliwości wdrożeniowe w ważnym segmencie rynku.

Szanse	Zagrożenia
• Rozwinięty rynek IT (makro-rynek cyberbezpieczeństwa) z perspektywami dalszego dynamicznego rozwoju mimo recesji gospodarczej (spowodowanej pandemią COVID-19). • Wysoki potencjał wdrożeniowy dla rozwiązań z obszaru cyberbezpieczeństwa w wielu różnych sektorach gospodarki, w tym wszelkich nowych niszach czy branżach przechodzących przez proces cyfryzacji (obecnie szczególnie zauważalne w przypadku branż przemysłowych – w związku z wdrażaniem technologii i założeń z obszaru „Przemysłu 4.0"). • Duży potencjał rozwoju krajowego sektora cyberbezpieczeństwa z uwagi na wysoki udział potencjalnych klientów, którzy dotychczas posiadali jedynie znikome zabezpieczenia IT i w najbliższym czasie będą inwestować w nowe produkty. • Rosnąca świadomość strategicznego znaczenia cyberbezpieczeństwa wśród jednostek administracyjnych i publicznych (szansa na ogłoszenie nowych publicznych projektów, dofinansowań, zleceń dla jednostek publicznych). • Rosnąca penetracja technologii dodatkowo akcelerujących popyt na rozwiązania z obszaru cyberbezpieczeństwa – jak technologie z obszaru Internetu Rzeczy czy wdrażanie założeń Przemysłu 4.0. • Rozwijający się ekosystem startupowy powiązany z rosnącym popytem na innowacyjne rozwiązania.	• Stale rosnący „drenaż mózgów" z polskich uczelni do zagranicznych korporacji – trudność w utrzymaniu wysokokwalifikowanych zasobów ludzkich na krajowym rynku. • Pojawienie się regulacji ograniczających możliwości technologiczne wdrożeń (np. legislacja wymagająca konkretnej formy zabezpieczenia, która z czasem stanie się nieaktualna) – efekt „nienadążającej legislacji" za postępem technologicznym. • Utrzymująca się wysoka wrażliwość cenowa klientów detalicznych i biznesowych z sektora MŚP, utrudniająca wdrażanie rozwiązań faktycznie chroniących przed najnowszymi zagrożeniami.

Szanse	Zagrożenia
• Rosnąca popularność kierunków informatycznych w sektorze edukacyjnym (możliwe rozwiązanie problemu braków kadrowych). • Stale zwiększające się wsparcie finansowe dla różnych obszarów/ dziedzin gospodarczych ze strony państwa i Unii Europejskiej, a w tym dla cyberbezpieczeństwa. • Kontynuacja polityki wdrażania jednolitych norm legislacyjnych (np. eIDAS) dla wszystkich członków rynku (nakładających wymagania nawet na podmioty, które wcześniej niechętnie wprowadzały zabezpieczenia).	

Źródło: opracowanie własne

Poniżej zaprezentowana została **analiza PESTEL** – przedstawiająca makroekonomiczne uwarunkowania branży cyberbezpieczeństwa w odniesieniu do czynników politycznych, ekonomicznych, społecznych, technologicznych, środowiskowych oraz prawnych. Przedstawione wnioski pochodzą od uczestników warsztatów Smart Lab.

Czynniki polityczne

Głównym czynnikiem politycznym w Polsce mającym fundamentalny wpływ na funkcjonowanie całej krajowej branży cyberbezpieczeństwa, jest rosnąca świadomość jednostek rządowych i rozumienie strategicznego znaczenia bezpieczeństwa IT w kontekście prawidłowego rozwoju gospodarki i bezpieczeństwa całego narodu. Dzięki temu rosną wydatki na zwiększanie zabezpieczeń jednostek administracyjnych oraz wszystkich punktów publicznego dostępu do Internetu. Analogicznie pozytywnym czynnikiem jest również rosnąca digitalizacja interakcji publiczno-administracyjnych, co ujawnia się m.in. poprzez wdrażanie wirtualnych alternatyw dokumentów, jak e-dowód czy umożliwianie wykorzystania podpisu elektronicznego w relacjach z urzędami – w Polsce poprzez system ePUAP. Z racji przynależności Polski do Unii Europejskiej, szczególnie ważnym czynnikiem politycznym są również wszelkie dyrektywy, regulacje i dofinansowania inicjowane przez jednostki podległe Komisji Europejskiej, które warunkują również krajową sferę polityczną. Należy podkreślić jednocześnie, że krajowe i unijne polityki horyzontalne, takie jak polityka handlu zagranicznego, polityka podatkowa czy polityka społeczna, nie tworzą barier dla rozwoju rynku cyberbezpieczeństwa, a jednocześnie nie prognozuje się zagrożenia, że ewentualne w nich zmiany mogłyby tę sytuację odmienić. Wśród ważnych czynników na pograniczu

politycznych i ekonomicznych należy podkreślić również negatywny dla branży trend dofinansowywania przez krajowe i europejskie programy jedynie faz badawczych i rozwojowych, bez wsparcia beneficjentów w procesach wdrożeniowych, które w przypadku kompleksowych technologii z obszaru cyberbezpieczeństwa są wyjątkowo kapitałochłonne.

Do czynników ekonomicznych w największym stopniu wpływających na funkcjonowanie obszaru cyberbezpieczeństwa w Polsce zaliczyć należy przede wszystkim wszystkie te uwarunkowania, które przekładają się na atrakcyjność prowadzenia działalności w tym sektorze rynku. Wśród nich zdecydowanie najważniejszym jest stale rosnący popyt na rozwiązania zabezpieczające struktury IT, a w szczególności w sektorze administracyjnym i biznesowym. Ważnym czynnikiem jest również wysoka stabilność gospodarcza kraju i całego sektora IT, który na tle innych krajów wyjątkowo dobrze poradził sobie z recesją gospodarczą, co przedstawione zostało w ramach rozdziału 0 (powrót do wzrostów już w 2021 r.). Tempo rozwoju gospodarczego i PKB również rośnie, jednak niepokojąca (i finalnie mogąca stać się negatywnym czynnikiem ekonomicznym) staje się tendencja rosnącej inflacji oraz stóp procentowych. Do negatywnych czynników należy zaliczyć również stale rosnące podatki (zarówno dla pracowników etatowych, jak i tych pracujących jako kontraktorzy na umowach B2B), ceny energii oraz koszty wynagrodzeń dla krajowych programistów – których wyrównanie z poziomem zagranicznym zniweluje możliwość korzystania z efektu „przewagi kosztowej" przez polskich przedsiębiorców i wymusi podniesienie cen, zmniejszając przewagi konkurencyjne. Istotnym czynnikiem ekonomicznym o negatywnym oddziaływaniu na rynek są również zauważalne braki kadrowe, potęgowane przez nieustający „drenaż mózgów" wykwalifikowanych specjalistów, emigrujących głównie do krajów Europy Zachodniej oraz USA.

Podstawowy czynnik społeczny w obszarze cyberbezpieczeństwa, to jednocześnie jeden z elementów warunkujących prawidłowe funkcjonowanie tego rynku – jest nim świadomość społeczna zagrożeń ze strony cyberprzestępców oraz możliwych form zabezpieczania się przed nimi. W Polsce świadomość ta wyraźnie rośnie, jednak jak stwierdzili uczestnicy warsztatów Smart Lab podczas dyskusji, tendencja ta dotyczy głównie dużych aglomeracji miejskich – w mniejszych miejscowościach lub na terenach wiejskich utrudniony jest dostęp do nie tylko klientów indywidualnych, ale również do klientów biznesowych, nawet jeśli prowadzą oni względnie duże działalności gospodarcze. Mimo większej świadomości podmiotów z dużych aglomeracji, i tak w całym kraju widoczny jest trend negowania zagrożenia z uwagi na przeświadczenie o „nieatrakcyjności dla hakerów posiadanych przez siebie danych" lub wprost go ignorowanie wyłącznie z uwagi na spełnianie aktualnych regulacji co do wymaganych zabezpieczeń w przedsiębiorstwach (nawet jeśli są one zauważalnie przestarzałe). Na tle tego czynnika ważnym do podkreślenia jest inny, łączący się z zagadnieniami politycznymi – na krajowym rynku za mało jest akcji społecznych nakierowanych na zwiększanie świadomości społeczeństwa i edukację w zakresie podstawowych zagadnień dot. cyberbezpieczeństwa. Pozostałe czynniki społeczne mające horyzontalny wpływ na rynek cyberbezpieczeństwa są względnie pozytywne – poziom

wykształcenia stale rośnie, tak jak i zainteresowanie sektorem informatycznym, a stan adaptacji nowych technologii jest wysoki.

Czynniki technologiczne

Do głównych czynników technologicznych mających wpływ na funkcjonowanie branży cyberbezpieczeństwa należy rosnąca penetracja nowych technologii w różnych sektorach gospodarczych, które albo bezpośrednio powiązane są z cyberbezpieczeństwem (np. kryptografia), albo wymagają zabezpieczeń IT do prawidłowego i bezpiecznego funkcjonowania (np. Internet Rzeczy czy usprawnienia z obszaru Przemysłu 4.0). Absorpcja tych technologii i względna świadomość konieczności ich wdrażania (u największych korporacji - w sektorze MŚP nadal znacząco ograniczona) akceleruje jednocześnie rynek cyberbezpieczeństwa, zwiększając popyt na innowacyjne rozwiązania – co zdecydowanie zaliczyć należy do pozytywnych czynników technologicznych. Co więcej polski ekosystem informatyczny cechuje się wysokim poziomem technologicznym, zgodnością z normami jakości i regulacjami paneuropejskimi, a programy rządowe i europejskie wspierają rozwój technologicznych innowacji produktowych i usługowych.

Czynniki środowiskowe

Kluczowym czynnikiem środowiskowym, nie tylko w cyberbezpieczeństwie, ale we wszystkich branżach, jest stała presja na zmniejszanie negatywnego wpływu uczestników rynku na najbliższe otoczenie. W przypadku cyberbezpieczeństwa taki wpływ występuje przede wszystkim w przypadku wysokiego poziomu zużycia energii przez urządzenia wykorzystywane w pracach programistycznych, serwerowniach oraz ogólnego „hardware" do świadczenia usług i sprzedaży produktów. Polityka klimatyczna wymaga zmniejszania poboru energii i kluczowi animatorzy rynku są świadomi konieczności obniżania kosztów generowanych przez wykorzystanie energii – co potwierdzają uczestnicy warsztatów Smart Lab.

Czynniki prawne

Czynniki prawne w odniesieniu do obszaru cyberbezpieczeństwa są w dużej części spójne z czynnikami politycznymi, jak i łączą się z czynnikami ekonomicznymi, technologicznymi i środowiskowymi, gdyż stanowią często fundament zmian status quo w tych obszarach (np. polityka klimatyczna w obszarze środowiska czy legislacja zmieniająca warunki ekonomiczne). Legislacyjnie rynek cyberbezpieczeństwa jest mocno regulowany, co dzieje się za pośrednictwem zarówno krajowych, jak i zagranicznych aktów prawnych (omówionych szerzej w rozdziale 3.8 „Otoczenie prawne i ochrona własności intelektualnej"). Co więcej, duża część uwarunkowań prawnych ma charakter interdyscyplinarny, a więc wpływa na obszar cyberbezpieczeństwa analogicznie co na inne sektory gospodarki. Wśród takich czynników wymienić należy m.in. ulgi podatkowe i zachęty, takie jak „Ulga B+R" czy „IP Box". Zachęcają one do tworzenia i komercjalizacji rozwiązań opartych o własną technologię, docelowo przekładając się na opłacalność prowadzenia biznesu w kraju. Biorąc pod uwagę fakt, że Polska jest członkiem UE i w kraju dostępne są różnorodne instrumenty wsparcia, w tym ze środków unijnych, jako czynnik prawny wymienić należy również wytyczne w zakresie udzielania pomocy przedsiębiorcom - np. w postaci grantów na prace B+R. Istotną rolę pełni również Prawo Zamówień Publicznych, które precyzuje możliwy sposób zakupu produktów i usług. Jednocześnie jednak te horyzontalne czynniki mają stanowić realną barierę rozwoju

dla części uczestników rynku – w ten sposób np. przetargi oparte o Prawo Zamówień Publicznych często faworyzują w obszarze cyberbezpieczeństwa podmioty zagraniczne, wymagając od aplikantów międzynarodowego doświadczenia (podczas gdy większość podmiotów z branży skupia się na rynku krajowym). Ważnym czynnikiem prawnym jest również możliwość ochrony własności intelektualnej, która w Polsce jest analogicznie dostępna co w innych krajach Unii Europejskiej, jednak w obszarze cyberbezpieczeństwa wyjątkowo rzadko stosowana przez podmioty krajowe (niska świadomość oraz brak zaufania do procesu patentowania). Szczególnie ważnym czynnikiem o negatywnym oddziaływaniu na rynek, co wielokrotnie podkreślali podczas dyskusji uczestnicy warsztatów Smart Lab, jest brak horyzontalnych standardów bezpieczeństwa, zarówno dla podmiotów świadczących usługi lub sprzedających produkty w sferze wirtualnej, jak i dla tych którzy jedynie przetwarzają dane (tutaj głównym wyznacznikiem jest obecnie Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., czyli tzw. „RODO"). Należy zaznaczyć również względnie powolny proces legislacyjny w stosunku do regulacji rynkowych oraz certyfikacji technologii, co powoduje wystąpienie efektu prawa nienadążającego za zmianami technologicznymi i w rezultacie standaryzacja zamiast podnosić wymagania rynkowe powoduje wręcz odwrotny efekt. Ważnym czynnikiem o negatywnym charakterze jest też względnie niski poziom wykorzystania profesjonalnych sposobów ochrony własności intelektualnej, która w obszarze cyberbezpieczeństwa ogranicza się często jedynie do „tajemnicy przedsiębiorstwa". Z pozytywnych aspektów horyzontalnej legislacji należy wymienić m.in. obowiązywanie aktów prawnych regulujących całą branżę cyberbezpieczeństwa, takich jak Ustawa o Krajowym Systemie Cyberbezpieczeństwa z 2018 r. Sfera legislacyjna jednak nadal pozostaje, według uczestników warsztatów Smart Lab, elementem wymagającym rozwoju i ciągłej aktualizacji – tak, aby czynniki prawne aktywizowały rynek, a nie utrudniały funkcjonowanie na nim.

4. Przegląd dostępnych źródeł wsparcia niekomercyjnego

Oferta finansowa w zakresie przedsięwzięć związanych z cyberbezpieczeństwem jest dostępna głównie na szczeblu unijnym (w szczególności w ramach Horyzontu Europa i Europejskiego Funduszu Obronnego), tym niemniej na poziomie krajowym również występują programy, które mogą okazać się interesujące w tym zakresie.

Poniżej zaprezentowano szczegółowe informacje co do źródeł wsparcia dostępnych na moment przeprowadzenia analizy (październik 2021 r.) oraz planowanych w najbliższych miesiącach.

Tabela 5 prezentuje dane w odniesieniu do funduszy oferowanych na poziomie Komisji Europejskiej:

Tabela 5. Informacje odnośnie źródeł wsparcia oferowanych na poziomie Komisji Europejskiej

Nazwa programu/ źródła wsparcia	Opis
Horyzont Europa	Program oferuje różnorodne konkursy, w ramach których dofinansowanie mogą otrzymać przedsiębiorcy realizujący inicjatywy związane m.in. właśnie z cyberbezpieczeństwem. Wspierane są przedsięwzięcia m.in. z obszarów dotyczących infrastruktury i serwerów IT, pozyskiwania danych, automatyzacji i robotyzacji, sztucznej inteligencji czy też dotyczące instytucji publicznych (w tym administracji i opieki zdrowotnej). Szczególnie do udziału w konkursach zachęca się podmioty o statusie MŚP. Wsparciem objęte są m.in. poniższe zagadnienia: • identyfikacja i eliminacja zagrożeń oraz luk w obrębie urządzeń medycznych czy stworzenie schematów odnośnie analizy korzyści, ryzyka i możliwości dotyczących cyberbezpieczeństwa w branży medycznej (docelowo działania mają przyczynić się do wzmocnienia poziomu cyberbezpieczeństwa i zachowaniu wydajności wyrobów medycznych oraz poufności danych),

Nazwa programu/ źródła wsparcia	Opis
	• opracowanie, rozwój i weryfikacja nowych metodologii oraz zestawów narzędzi w celu zapewnienia cyberbezpieczeństwa w obrębie urządzeń medycznych już na etapie ich projektowania, • różnorodne badania i innowacje w obrębie cyberbezpieczeństwa infrastruktury cyfrowej celem wsparcia kategoryzacji i agregacji danych z różnych źródeł oraz automatycznego pozyskiwania danych i analizy incydentów bezpieczeństwa, • ulepszenie monitorowania zagrożeń czy też wykrywania ich w systemach i infrastrukturach cyfrowych, • rozwój i walidacja procesów oraz narzędzi wykorzystywanych do certyfikacji zwinnej produktów, usług i procesów ICT, • opracowanie metodologii, narzędzi i zabezpieczeń na potrzeby testowania potencjalnie podatnych na ataki, niezabezpieczonych komponentów sprzętowych i programowych. Jednym z instrumentów w ramach Programu Horyzont Europa jest również „EIC Accelerator Open". Instrument wspiera finansowanie MŚP i startupów, które opracowują przełomowe projekty innowacyjne o wysokim potencjale rozwojowym, charakteryzujące się dużym poziomem ryzyka. Przedsiębiorca ma dowolność pod kątem tematyki, gdyż w ramach Programu nie określono konkretnych obszarów wsparcia. Niemniej warunkiem koniecznym przy składaniu wniosku jest posiadanie prototypu oraz osiągnięcie co najmniej 5/6 poziomu gotowości technologicznej. Wsparcie przyjmuje formę dotacji (kwota dofinansowania do 2,5 mln euro – 70% kosztów kwalifikowalnych) lub bezpośrednich inwestycji kapitałowych (w wysokości od 0,5 do 17,5 mln euro). O wsparcie mogą aplikować samodzielni przedsiębiorcy (nie jest wymagane konsorcjum). Nabór wniosków wstępnych prowadzony jest w trybie ciągłym, a wnioski właściwe można składać w ramach dwóch rund określonych konkretnymi terminami dla każdego roku (np. w 2021 roku ostatnia runda została zamknięta 6 października). W kolejnym roku uruchomione zostaną następne nabory.
Europejski Fundusz Obronny (EFO)	W ramach EFO podejmowane są działania mające na celu wspieranie rozwoju konkurencyjnej i innowacyjnej bazy przemysłowej sektora

Nazwa programu/ źródła wsparcia	Opis
	obronnego oraz rozwój współpracy i zwiększenie efektywności wydatków państw członkowskich UE na stworzenie wspólnych zdolności obronnych. W ramach Programu występują konkursy przewidujące realizację przedsięwzięć dotyczących w szczególności badań produktów i technologii z dziedziny obronności, w tym również z obszaru cyberbezpieczeństwa. W obrębie wspomnianego obszaru wsparcie udzielane jest w szczególności na: • stworzenie zestawu narzędzi umożliwiających znaczący wzrost efektywności w realizacji procesu szkoleń i ćwiczeń cybernetycznych, przy zwiększeniu interoperacyjności cyberzakresów i efektywności kosztów, • stworzenie rozwiązań opartych na sztucznej inteligencji, które będą automatyzować większą część procesów związanych z zarządzaniem incydentami i cyberobroną, • opracowanie tzw. Proof of Concept potwierdzających słuszność koncepcji w zakresie zarządzania incydentami i cyberobroną w oparciu o algorytmy sztucznej inteligencji (w tym wykrywanie, łagodzenie skutków i reagowanie), • rozwój łączności satelitarnej, w tym technologii dotyczących bezpieczeństwa i odporności na potrzeby komunikacji satelitarnej wolnej od zagłuszeń, • opracowanie i testowanie cyfrowego systemu bezpiecznej i szybkiej wymiany informacji związanych z mobilnością wojskową. EFO jest realizowany za pomocą rocznych programów prac. W 2021 r. zaplanowano aż 23 nabory wniosków (11 zaproszeń dotyczących działań badawczych i 12 zaproszeń dotyczących działań rozwojowych) w ramach 15 różnych obszarów. Jedna z kategorii dedykowana jest wprost cyberbezpieczeństwu. Na przykład w obrębie wspomnianej kategorii realizowany jest konkurs „Poprawa cyberobrony i zarządzania incydentami za pomocą sztucznej inteligencji" (EDF-2021-CYBER-R-CDAI). Koncentruje się on wokół tworzenia rozwiązań opartych na sztucznej inteligencji, które umożliwią automatyzację procesów zarządzania incydentami i cyberobroną. Zadania konkursowe uwzględniają poniższe 3 obszary aktywności:

Nazwa programu/ źródła wsparcia	Opis
	• zwiększenie wiedzy o przedsiębiorstwach, procesach i podejmowaniu decyzji odnośnie zastosowania sztucznej inteligencji, • rozwój technik opartych na sztucznej inteligencji wspierających konkretne zadania operacyjne lub analityczne, • odkrycia i rozwój sztucznej inteligencji w kontekście podejmowania decyzji przy ograniczonych uprawnieniach w zakresie zarządzania incydentami i cyberobroną.

Źródło: opracowanie własne na podstawie publikacji Komisji Europejskiej [53, 54]

Tabela 6 prezentuje analogiczne informacje do wskazanych w Tabeli 5, jednak w odniesieniu wyłącznie do wsparcia dostępnego z instrumentów krajowych:

Tabela 6. Informacje odnośnie źródeł wsparcia oferowanych z instrumentów krajowych

Nazwa programu/ źródła wsparcia	Opis
Fundusze Europejskie na Rozwój Cyfrowy (FERC)	Program stanowi kontynuację Programu Polska Cyfrowa 2014-2020 i jego realizacja przewidziana jest na lata 2021-2027. Wsparcie udzielane będzie w formie dotacji. Budżet Programu to ok. 2 mld EUR. Wśród celów Programu należy wymienić w szczególności: • zapewnienie cyberbezpieczeństwa poprzez wsparcie w ramach nowego, dedykowanego obszaru interwencji, • rozwój gospodarki opartej na danych wykorzystujących najnowsze technologie cyfrowe, • rozwój współpracy na rzecz tworzenia cyfrowych rozwiązań problemów społeczno-gospodarczych, • wsparcie rozwoju zaawansowanych kompetencji cyfrowych.

[53] *Strona internetowa: https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/horizon-europe_en. Dostęp: 26.11.2021.*

[54] *Strona internetowa: https://ec.europa.eu/defence-industry-space/eu-defence-industry/european-defence-fund-edf_en. Dostęp: 26.11.2021.*

Nazwa programu/ źródła wsparcia	Opis
	Program obejmuje obszar dotyczący cyberbezpieczeństwa, co stanowi nowość tematyczną względem ubiegłej perspektywy finansowej. W tym zakresie oferta dotyczyć będzie np. zapobiegania atakom oraz incydentom zagrażającym bezpieczeństwu w sieci. Odbiorcami FERC będą m.in. przedsiębiorcy (głównie z branży telekomunikacyjnej), podmioty administracji publicznej oraz różnorodne instytucje (w tym instytucje kultury oraz systemu szkolnictwa wyższego i nauki). Konsultacje społeczne Programu zostały zakończone 25 maja 2021 r., trwają prace nad jego uszczegółowieniem, zatem uruchomienia naborów wniosków należy spodziewać się w 2022 r.
Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG)	Program stanowi kontynuację Programu Inteligentny Rozwój (POIR) i będzie realizowany w perspektywie 2021-2027. Jednocześnie FENG jest Programem komplementarnym z FERC. FENG będzie realizowany w ramach 3 priorytetów: • Wsparcie dla przedsiębiorców – dofinansowania m.in. w obszarach dotyczących prac badawczo-rozwojowych, rozwoju infrastruktury B+R, wdrożenia wyników badań (projekty inwestycyjne), wdrażania zielonych technologii w przedsiębiorstwach oraz cyfryzacji (związanej z transformacją w kierunku Przemysłu 4.0, w szczególności automatyki i robotyzacji oraz działania dotyczące cyberbezpieczeństwa). Pomoc publiczna udzielana będzie dla MŚP, small mid-caps i dużych przedsiębiorstw. Na realizację Priorytetu 1 zostanie przeznaczonych 55% alokacji programu, tj. ok. 4,5 mld EUR. • Środowisko przyjazne innowacjom – wspieranie projektów o strategicznym znaczeniu dla polskiej gospodarki, w tym m.in. rozbudowy publicznej infrastruktury badawczej czy wzmacnianie potencjału instytucji otoczenia biznesu. W tym obrębie wsparcie udzielane będzie organizacjom badawczym, podmiotom zajmującym się transferem technologii, zespołom badawczym, indywidualnym naukowcom i przedsiębiorcom. • Pomoc techniczna – zapewnienie systemowego wsparcia dla potencjalnych beneficjentów. W ramach Programu wspierane będą kompleksowe projekty składające się z poszczególnych modułów: obligatoryjnego, tj. moduł B+R (jego efektem powinno być opracowanie innowacyjnego rozwiązania możliwego

Nazwa programu/ źródła wsparcia	Opis
	do wdrożenia w działalności gospodarczej) lub moduł infrastruktura B+R (finansowanie kosztów w sprzęt, aparaturę i inną niezbędną infrastrukturę służącą prowadzeniu prac B+R), a także fakultatywnych: wdrożenie innowacji, kompetencje, inwestycje w zielone technologie w przedsiębiorstwach, cyfryzacja czy internacjonalizacja i współpraca międzynarodowa. Oferta Programu skierowana jest do: • przedsiębiorstw, • sektora nauki, • konsorcjów przedsiębiorców oraz konsorcjów przedsiębiorców z organizacjami badawczymi, • instytucji otoczenia biznesu, czyli ośrodków przedsiębiorczości, ośrodków innowacji, instytucji finansowych. Forma wsparcia: • dotacje, • instrumenty finansowe, • instrumenty kapitałowe oraz gwarancyjne, • instrumenty łączące finansowanie zwrotne i dotacyjne. Planuje się nabór wniosków w trybie ciągłym z wyznaczeniem konkretnych rund (z terminem zamknięcia danej rundy co 3 miesiące). Budżet Programu wynosi ok. 8 mld EUR.
Krajowy Plan Odbudowy (KPO)	KPO określa cele związane z odbudową i tworzeniem odporności społeczno-gospodarczej Polski po kryzysie wskutek COVID-19. Plan stanowi podstawę do skorzystania z Instrumentu Odbudowy i Zwiększenia Odporności, w ramach którego budżet przewidziany dla Polski to ok. 58 mld EUR (w tym blisko 24 mld EUR w formie dotacji). Wsparcie będzie udzielane na realizację przedsięwzięć w poniższych 5 komponentach: • odporność i konkurencyjność gospodarki, • zielona energia i zmniejszenie energochłonności, • transformacja cyfrowa,

Nazwa programu/ źródła wsparcia	Opis
	• dostępność i jakość ochrony zdrowia, • zielona i inteligentna mobilność. W ramach komponentu C „Transformacja cyfrowa” zakłada się m.in. następujące działania: • wzrost bezpieczeństwa w cyberprzestrzeni, zabezpieczenie infrastruktury przetwarzania danych oraz cyfryzacja infrastruktury służb odpowiedzialnych za bezpieczeństwo - celem inwestycji będzie głównie wzmocnienie cyberodporności systemów informacyjnych (IT i OT) wykorzystywanych w podmiotach wchodzących w skład krajowego systemu cyberbezpieczeństwa oraz zapewnienie wysoce wydajnych, energooszczędnych ośrodków obliczeniowych wraz z zabezpieczeniem ciągłości działania infrastruktury krytycznej zabezpieczającej dane na potrzeby świadczenia usług publicznych, • zwiększenie cyberbezpieczeństwa systemów informacyjnych, wzmocnienie infrastruktury przetwarzania danych. Na działania związane z realizacją komponentu C przeznaczonych zostanie łącznie 4,9 mld EUR (2,8 mld EUR z części grantowej i 2,1 mld EUR z części pożyczkowej), co stanowi 13,6% środków planowanych do wydatkowania w ramach KPO.

Źródło: opracowanie własne na podstawie dostępnych rządowych informacji o programie FERC[55], FENG[56] oraz KPO[57]

[55] *Strona internetowa: https://www.polskacyfrowa.gov.pl/strony/o-programie/fundusze-europejskie-na-rozwoj-cyfrowy-2021-2027/konsultacje-spoleczne-programu/. Dostęp: 26.11.2021.*

[56] *Strona internetowa: https://www.poir.gov.pl/strony/o-programie/fe-dla-nowoczesnej-gospodarki/. Dostęp: 26.11.2021.*

[57] *Strona internetowa: https://www.gov.pl/web/planodbudowy. Dostęp: 26.11.2021.*

5. Program rozwoju dla obszaru cyberbezpieczeństwa w perspektywie 7 lat

5.1. Scenariusze rozwoju obszaru cyberbezpieczeństwa

Poniżej przedstawiono scenariusze rozwoju obszaru cyberbezpieczeństwa oraz wpisujące się w nie konkretne działania/ projekty, które zostały zdefiniowane i przedyskutowane w ramach cyklu Spotkań Smart Lab. Prace nad scenariuszami odbyły się z grupą przedstawicieli obszaru cyberbezpieczeństwa w Polsce według metodyki zgodnej z koncepcją Procesu Przedsiębiorczego Odkrywania. Spotkania zaowocowały zdefiniowaniem czterech scenariuszy rozwoju technologii w obszarze cyberbezpieczeństwa. Opracowano dwa horyzontalne scenariusze: pierwszy poświęcony powstaniu na polskim rynku rozwiązań usługowych w zakresie bezpieczeństwa, drugi zaś dedykowany zagadnieniom rozwoju kryptografii, uwierzytelniania i ogólnej ochronie tożsamości (personalnej, jak i technicznej). Pozostałe dwa scenariusze mają charakter aplikacyjny, wynikający ze zidentyfikowanych potrzeb rynkowych. Pierwszy z nich dotyczy niezwykle ważnego obszaru instalacji procesowych i krytycznych, drugi obejmuje zapewnianie bezpieczeństwa w rozwiązaniach sieciowych, ze szczególnym uwzględnieniem urządzeń IoT.

Zidentyfikowane działania/ projekty w scenariuszach zostały podzielone ze względu na ich aktualny stan rozwoju oraz charakter na następujące fazy:

Faza I – Badania podstawowe i prace przygotowawcze
Działania/ projekty na poziomie gotowości technologicznej (TRL) I, czyli realizacja badań naukowych w celu wykorzystania technologii w przyszłych zastosowaniach. W ramach tej fazy działania przygotowawcze mogą również dotyczyć takich aspektów jak m.in. badania i weryfikacja rynku, opracowanie studium wykonalności czy analizy pod kątem dostępności niezbędnych do realizacji prac B+R partnerów oraz infrastruktury. Zakładany średni poziom dofinansowania projektów ze środków publicznych w tej fazie to 90-100%[58];

[58] *Wartości na bazie poziomów dofinansowania projektów B+R+I z Funduszy Europejskich w ramach perspektywy finansowej 2014-2020 oraz konsultacji z uczestnikami spotkań Smart Lab.*

Faza II – Badania przemysłowe

Działania/ projekty na poziomach TRL w zakresie II-VI, czyli opracowanie koncepcji zastosowania technologii, prowadzenie badań analitycznych i laboratoryjnych wybranych elementów technologii, badania opracowanej technologii w warunkach laboratoryjnych, w symulowanych warunkach operacyjnych oraz demonstracje prototypu technologii w warunkach zbliżonych do rzeczywistych. Zakładany średni poziom dofinansowania projektów ze środków publicznych w tej fazie to 60-80%[59];

Faza III – Prace rozwojowe, przedwdrożeniowe i wdrożeniowe

Działania/ projekty na poziomach TRL w zakresie VII-IX, czyli demonstracje prototypów technologii w warunkach operacyjnych, badania i demonstracje ostatecznej formy technologii oraz sprawdzenie funkcjonowania technologii w warunkach rzeczywistych. W ramach tej fazy działania przedwdrożeniowe oraz wdrożeniowe mogą również dotyczyć takich aspektów jak m.in. certyfikacja oraz ochrona własności intelektualnej wyników prac B+R, działania promocyjne oraz pierwsze wdrożenia komercyjne. Zakładany średni poziom dofinansowania projektów ze środków publicznych w tej fazie to 40-60%[60].

Poszczególne fazy realizacji projektów zostały umiejscowione na skali czasu i opatrzone ustalonym budżetem. Ilość faz w działaniu oraz ich czas trwania został zdefiniowany na bazie pierwotnej dojrzałości rozwijanej w działaniu/ projekcie technologii. Przewidywaną ilość projektów prowadzonych w danej fazie określonego działania, ich alokacje budżetowe i niezbędne zasoby określono na bazie wiedzy eksperckiej uczestników SL poddanej krytycznej ocenie przez zespół ekspertów opracowujący niniejszą ekspertyzę.

5.1.1. Scenariusz 1 – Cyberbezpieczeństwo jako usługa (z ang. „Cybersecurity-as-a-Service")

Rynek cyberbezpieczeństwa w Polsce cały czas się rozwija. Rozwój ten wynika w szczególności z szerokiego spektrum zagrożeń cyberbezpieczeństwa dla funkcjonowania polskich podmiotów gospodarczych i nie tylko. Dlatego też na rynku możemy zaobserwować dwa podejścia leżące

[59] *Wartości na bazie poziomów dofinansowania projektów B+R+I z Funduszy Europejskich w ramach perspektywy finansowej 2014-2020 oraz konsultacji z uczestnikami spotkań Smart Lab.*

[60] *Wartości na bazie poziomów dofinansowania projektów B+R+I z Funduszy Europejskich w ramach perspektywy finansowej 2014-2020 oraz konsultacji z uczestnikami spotkań Smart Lab.*

na przeciwległych biegunach. Z jednej strony popularne podejście to przeniesienie działalności cyfrowej do technologii chmurowych (np. AWS lub Azure). Dzięki temu kwestią bezpieczeństwa informacji oraz utrzymaniem funkcjonowania zajmuje się operator chmury. Rozwiązanie to niesie za sobą prostotę i często redukcję kosztów, ale pozbawia podmiot kontroli nad swoim bezpieczeństwem i ma ograniczoną możliwość odniesienia się do indywidualnych potrzeb.
Na przeciwległym biegunie znajduje się cyberbezpieczeństwo w tzw. formule „in-house" czyli wewnętrznie w organizacji. Model ten w znakomitej większości przypadków wiąże się z dużo wyższymi kosztami, głównie z uwagi na konieczność utrzymania personelu oraz infrastruktury. Zasoby te też są głównymi barierami rozwoju – chęć rozbudowy systemu cyberbezpieczeństwa wiąże się wtedy nie tylko z kosztami oprogramowania, ale również z szeregiem wydatków związanych z jego utrzymaniem. Pozwala on jednak na nieograniczoną indywidualizację rozwiązań i gdy zapory wdrażane są w odpowiedni sposób, zapewniają najwyższy poziom bezpieczeństwa.

W opinii uczestników Smart Labu na rynku jest miejsce na cały sektor usług dot. cyberbezpieczeństwa, które odpowiadałyby na różne potrzeby odbiorców leżące pomiędzy opisanymi powyżej dwoma biegunami. Umożliwiałoby to daleko idącą indywidualizację rozwiązań cyberbezpieczeństwa, jednocześnie pozwalając w przyszłości na ekspansję poza rynek krajowy z uwagi na fakt, że tego typu usługi o wysokim stopniu personalizacji są pożądane również na rynkach zagranicznych. Niejako przez analogię, do klasycznego już modelu SaaS (ang. Software-as-a-service, oprogramowanie jako usługa) zaproponowano nazwę scenariusza jako Cyberbezpieczeństwo jako usługa (z ang. „Cybersecurity-as-a-service", w skrócie „CaaS").
Aby scenariusz ten był możliwy do zrealizowania, należy przeprowadzić opisane niżej działania.

Działanie 1 - Wykrywanie zagrożeń, ocena ryzyka i inżynieria podatności

Działanie to ma dać zaczątek do powstania portfela usług z zakresu cyberbezpieczeństwa. Usługi te miałyby wypełnić istotną niszę na polskim rynku w opisanym powyżej zakresie.
W szczególności zapewnione mają być rozwiązania technologiczne pozwalające na oferowanie usług dotyczących wykrywania zagrożeń, oceny podatności na zagrożenia oraz zwiększania odporności odbiorców usług.

W jego wyniku mógłby powstać pełen pakiet usług lub innowacji produktowych i procesowych pozwalających na ich świadczenie. Obejmowałby on przykładowo aplikację do threat huntingu czy system umożliwiający automatyzację i nałożenie priorytetów dla ciągłych procesów zarządzania zasobami oraz zarządzania podatnościami. Odbiorcami wyników działania – w rozumieniu nowych usług – mogliby być operatorzy usług kluczowych, administracja, placówki naukowe, szpitale, przedsiębiorstwa, podmioty publiczne itp.

Działanie obejmuje prace we wszystkich 3 fazach:

Faza I | Faza II | Faza III

Przykładowe projekty/ działania, jakie mogłyby zostać zrealizowane w ramach fazy I to:

- Opracowanie algorytmów sztucznej inteligencji w zastosowaniu dla symulowania, przewidywania i wykrywania zaawansowanych ataków (APT).
- Opracowanie oprogramowania do zbierania danych o podatnościach na zagrożenia, dla istniejących w danym przedsiębiorstwie systemów i infrastruktury ICT.
- Prace nad wzajemną integracją i konwersją standardów CVSS 2.0 i CVSS 3.1.

Aby fazę I można było uznać za pomyślnie zakończoną, w wyniku jej realizacji powinny powstać: zdefiniowane wymagania funkcjonalne oraz opracowane założenia dla algorytmów AI, na których miałyby bazować nowe usługi, infrastruktura umożliwiająca symulację środowisk IT/ OT, algorytmy analizy ryzyka oraz koncepcje integracji oceny ryzyka z systemami zarządczymi.

Realizacja fazy I bazowałaby na wykwalifikowanej kadrze jednostek badawczych i przedsiębiorstw w obszarze elektroniki i bezpieczeństwa sieci. Wykorzystywane byłyby też środki trwałe (istniejące i nowo utworzone) oraz WNiP będące w posiadaniu uczelni i przedsiębiorstw. Projekty musiałyby w pewnych zakresach korzystać też z zakupu usług obcych np. dotyczących wykonywania układów elektronicznych na ich zlecenie.

Uczestnicy Smart Labu ocenili, że w ramach fazy I możliwe jest zrealizowanie 15 projektów. Projekty te powinny być relatywnie krótkie i zakończyć się w przeciągu 1 roku. Budżet fazy I oszacowano na 10 mln PLN.

Faza I | **Faza II** | Faza III

Faza II obejmująca badania przemysłowe, jest bezpośrednią kontynuacją prac zrealizowanych w fazie I. Dzięki zdobytej nowej wiedzy oraz opracowaniu niezbędnych analiz możliwe będzie wdrożenie nowych rozwiązań technologicznych w szerokim zakresie.

Przykładowe projekty/ działania, jakie mogłyby zostać zrealizowane w ramach fazy II to:

- Tworzenie prototypowych rozwiązań AI do wykrywania ataków.
- Tworzenie prototypów rozwiązań analizy ryzyka i ich testy, jak również integracja z rozwiązaniami do zarządzania podatnością.
- Testy prototypów oprogramowania i urządzeń w warunkach rzeczywistych i ich integracja z dostępnymi skanerami podatności i oprogramowaniem do inwentaryzacji IT.

Wynikiem fazy II miałyby być przetestowane prototypy rozwiązań, w oparciu, o które byłyby wdrażane finalne usługi.

Do realizacji przewidzianych prac niezbędne byłyby wykwalifikowane kadry (w obszarze bezpieczeństwa oprogramowania, systemów inteligentnych i elektroniki) oraz środki trwałe i WNiP powstałe w fazie I.

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 20 projektów. Projekty te powinny zakończyć się w przeciągu 2 lat. Budżet fazy II oszacowano na 75 mln PLN.

Faza I | Faza II | **Faza III**

Faza III działania miałaby na celu przejście od prototypów do wdrożeń.

Przykładowe projekty/ działania, jakie mogłyby zostać zrealizowane w ramach fazy III to:

- Wdrożenia testowe (np. w zakładach produkcyjnych i instytucjach publicznych) z komponentem personalizacji dla poszczególnych klientów.
- Wdrożenia platform usługowych w technologiach webowych.

Wynikiem działania powinno być finalne opracowanie oraz wdrożenie różnych usług w modelu „CaaS", szczególnie w ujęciu ich integracji z istniejącymi i rozwijanymi rozwiązaniami i technologiami z zakresu systemów bezpieczeństwa.

Kluczowymi zasobami dla fazy III powinny być zasoby ludzkie, w postaci ekspertów w przedsiębiorstwach, którzy posiadać będą wiedzę i umiejętności do przeprowadzenia wdrożeń oraz testów i dostosowania wypracowanych technologii u klientów.

Uczestnicy Smart Labu ocenili, że w ramach fazy III (ze względu na mnogość potencjalnych odbiorców) możliwe jest zrealizowanie 125 projektów. Projekty te powinny zakończyć się w przeciągu 3 lat. Budżet fazy III oszacowano na 225 mln PLN.

Podsumowując, działanie pierwsze ma stworzyć podwaliny pod sektor usług w proponowanym modelu CaaS. W ramach działania planowane jest zrealizowanie w okresie 6 lat łącznie 160 projektów z całkowitym budżetem wynoszącym 310 mln PLN.

Działanie 2 - Usługi osobistego uwierzytelniania

Celem działania jest rozwój, ukształtowanie i wzmocnienie segmentu usług cyberbezpieczeństwa w zakresie dotyczącym uwierzytelniania tożsamości. Usługi tego typu muszą być personalizowane ze względu na wymagania klientów i wymagają integracji różnych systemów cyberbezpieczeństwa.

Efektywne rozwiązania uwierzytelniania stanowią bardzo istotny aspekt rynku cyberbezpieczeństwa, a działanie to porusza jego interdyscyplinarne aspekty, wykorzystując m.in. założenia analizy behawioralnej czy biometrii. Rozpoznawanie użytkowników systemów musi być zarówno efektywne, jak i bezpieczne oraz - ze względu na wymogi prawne - wykorzystywać technologie wieloetapowe. Działanie to odpowiadać będzie na potrzeby branży oferując nowe, zintegrowane rozwiązania, zapewniające bezpieczeństwo wielopoziomowe. Odbiorcami usług z tego zakresu byliby m.in. przedsiębiorcy oferujący rozwiązania w zakresie uwierzytelniania tożsamości. Rozwiązania te szczególnie wysokim zainteresowaniem powinny cieszyć się w sektorze finansowym, jak również w sektorach produkcyjnych czy dotyczących infrastruktury krytycznej.

Działanie obejmuje prace w fazach II i III:

Faza II | Faza III

W wyniku prac w fazie II powstałyby zintegrowane prototypowe rozwiązania z zakresu uwierzytelniania tożsamości (wykorzystujące technologie biometryczne i/ lub elementy behawiorystyki). Należy liczyć się z tym, że nie wszystkie te projekty zakończą się sukcesem, gdyż, jak wszystkie projekty badawcze, są one obarczone dużym stopniem ryzyka. Stąd też tak ważne jest wsparcie ze środków publicznych. Sukces tego działania zaowocowałby jednak powstaniem technologii, które dawałyby polskiemu sektorowi cyberbezpieczeństwa możliwość rozszerzenia działalności na rynku lokalnym, a także skutecznej ekspansji zagranicznej.

Realizacja fazy II bazowałaby na wykwalifikowanej kadrze przedsiębiorstw wspieranych przez ekspertów (w obszarze kryptografii i bezpieczeństwa oprogramowania) z jednostek badawczych. Wykorzystywane byłyby też środki trwałe (istniejące i nowo utworzone) oraz WNiP będące w posiadaniu uczelni i przedsiębiorstw. Projekty musiałyby w pewnych zakresach korzystać też z zakupu usług obcych np. dotyczących wykonywania układów elektronicznych na zlecenie.

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 30 projektów. Projekty te powinny zakończyć się w przeciągu 2 lat. Budżet fazy II oszacowano na 60 mln PLN.

Faza II | **Faza III**

Faza III ma na celu realizację wdrożeń opracowanych technologii w ramach modelu CaaS. Mają powstać produkty (usługi) oferujące kompleksowe podejście do weryfikacji tożsamości użytkownika dostosowane do potrzeb danego segmentu odbiorców. Zaplanowano zarówno wdrożenia testowe, jak i pełne komercjalizacje w sektorze prywatnym i publicznym. W ramach tej fazy możliwe byłoby uzyskanie certyfikacji dla wypracowanych rozwiązań, zapewnianie ochrony IP, ale także wprowadzanie produktów na rynek w wersji produkcyjnej.

Kluczowymi zasobami dla fazy III powinny być zasoby ludzkie, w postaci ekspertów w przedsiębiorstwach, którzy posiadać będą wiedzę i umiejętności do przeprowadzenia wdrożeń oraz testów i dostosowania wypracowanych technologii u klientów.

Uczestnicy Smart Labu ocenili, że w ramach fazy III możliwe jest zrealizowanie 20 projektów. Projekty te powinny zakończyć się w przeciągu 3 lat. Budżet fazy III oszacowano na 70 mln PLN.

Podsumowując, działanie drugie skupia się na innowacyjnych rozwiązaniach z zakresu personalnego uwierzytelniania. Technologie te są już na etapie rozwoju i dojrzałości, która pozwala na ich odpowiednią adaptację i integrację, prowadząc do wdrożeń w formie usług. W ramach działania planowane jest zrealizowanie w okresie 5 lat łącznie 50 projektów z całkowitym budżetem wynoszącym 130 mln PLN.

Rysunek 23. Forma graficzna scenariusza 1

Źródło: opracowanie własne

5.1.2. Scenariusz 2 – Kryptografia, uwierzytelnianie i ochrona tożsamości

Drugi scenariusz odnosi się do zagadnień szczególnie aktualnych, zarówno w perspektywie rynku krajowego, jak i globalnego. Działania w nim zawarte odpowiadają na wyzwania pojawiające się zarówno w wyniku rozwoju technologii cyberataków, jak i globalnego ich nasilenia. Jednym z głównych czynników potęgujących na nie popyt są doniesienia dotyczące rozwoju komputerów kwantowych, w ramach których sugeruje się, że w niedługim czasie klasyczne metody kryptograficzne mogą okazać się niewystarczające. Co prawda technologia kwantowa jest w bardzo wczesnym stadium rozwoju i nie wyeliminowano do tej pory wszystkich związanych z nią problemów, jednak należy być przygotowanym na jej dalszy rozwój i finalną popularyzację. Potencjał tej technologii powoduje zainteresowanie tzw. metodami quantum resist, które oferują rozwiązania oparte o kryptograficzne zabezpieczenia, pozwalające skutecznie niwelować przewagę obliczeniową.

Innym obszarem wymagającym specjalnej uwagi są ogólnie rozumiane technologie uwierzytelniania, obejmujące nie tylko użytkownika w systemie, ale też komunikację międzysystemową i łączenie się poszczególnych urządzeń z systemem. Brak odpowiednich systemów zabezpieczających tworzy podatności, np. pozwalające na kradzież informacji lub atak na łańcuch dostaw. Obszar ten obejmuje zagadnienia kryptograficzne, w szczególności klucze jednorazowe (których wprowadzanie jest wymagane prawem UE), ale także np. tokeny sprzętowe dla uwierzytelniania urządzeń.

Tematem powiązanym, wchodzącym w zakres tego scenariusza, są usługi zaufania. Rozwój technologii blockchainowych i pokrewnych stwarza duży potencjał dla takich rozwiązań jak m.in. dokumenty cyfrowe czy szyfrowane archiwa. Zagadnienia te są perspektywiczne w Polsce zarówno ze względu na znaczny popyt wśród krajowych przedsiębiorców, jak również z uwagi na eksportowy charakter rozwiązań i ich względnie łatwą skalowalność.

W opinii uczestników SL konieczne jest podjęcie działań mających na celu zapewnienie technologicznych możliwości funkcjonowania w rozwijającym się paradygmacie zagrożeń. W szczególności wyróżniono trzy obszary jakimi są systemy quantum resist, zagadnienia uwierzytelniania i kontroli dostępu (w szczególności między systemami) oraz stworzenie oferty usług zaufania, z uwzględnieniem między innymi technologii blockchain. W ramach realizacji scenariusza przewidziano następujące działania:

Działanie 1 - Systemy odporne na technologie obliczeń kwantowych

Celem działania jest stworzenie bazy metod kryptograficznych i ich implementacji (aż do poziomu produktu) projektowanych od początku z myślą o kryptografii kwantowej. Technologie te dopiero wchodzą do użytku, jednak korzystając z wyników badań naukowych możliwe jest opracowanie technologii zabezpieczających.

W wyniku tego działania mogłyby powstać m.in.:

- Nowe metody, protokoły i technologie dla realizacji usług bezpiecznego pierwszego kontaktu w systemach uwierzytelniania.
- Urządzenia - FPGA, ASIC oraz biblioteki i programy, również na urządzenia mobilne, implementujące bezpieczny - odporny na znane podatności - protokół pierwszego kontaktu.
- System szyfrowania dostępny dla systemów i urządzeń IoT.

Konsekwentnie odbiorcami opracowanych rozwiązań byłyby wszystkie grupy odbiorców wymagających realizacji poufności i rozliczalności w przetwarzaniu informacji i danych. Pozwoliłoby to dostosować się do zapisów rozporządzenia wykonawczego komisji UE 2015/1502[61]

Dodatkowo należy uwzględnić regulacje dotyczące:

- Zastosowań w usługach zaufania – UE 2014/910 – eIDAS (ang. electronic Identification, Authentication and trust Services)[62].
- Ochrony danych osobowych - UE 2016/679- RODO[63].
- Transakcji e-bankingowych i w ogólnym fintech - UE 2015/2366 – PSD2 (ang. Payment Services Directive 2)[64].

W oczywisty sposób zaowocowałoby to szerokim zakresem produktów i usług dostępowych dla administracji, ochrony zdrowia, bankowości elektronicznej i Fintech, ePUAP, IoT oraz DLT, a także osób prywatnych i innych podmiotów chcących podnieść poziom zabezpieczeń.

---

[61] ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

[62] 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 elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

[63] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[64] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE.

Działanie obejmuje prace we wszystkich 3 fazach:

Faza I | Faza II | Faza III

Projekty fazy I miałyby dotyczyć opracowania koncepcji algorytmów kryptograficznych, architektury systemów ochrony, założeń funkcjonowania zabezpieczeń, możliwości implementacji rozwiązań bezpiecznych w kontekście prawnym i technicznym oraz komunikacji opartej na technologii kwantowej lub protokołów opartych na kryptografii z kluczami jednorazowymi o udowodnionym poziomie bezpieczeństwa bezwarunkowego.

Faza I zostanie uznana za zrealizowaną, gdy powstaną koncepcje architektur systemów bezpiecznych, koncepcji algorytmów i analizy podatności na cyberzagrożenia w kontekście obliczeń kwantowych, jak również będzie możliwe przedstawienie przewag konkurencyjnych wypracowanych koncepcji w stosunku do innych, już istniejących oraz wykazanie zgodności z wymaganiami prawnymi UE.

Realizacja fazy I bazowałaby na wykwalifikowanej kadrze jednostek badawczych i przedsiębiorstw dysponujących działami B+R mającymi doświadczenie w obszarze metod i technologii uznanych za bezpieczne. Wykorzystywane byłyby też środki trwałe (istniejące i nowo utworzone) oraz WNiP będące w posiadaniu uczelni i przedsiębiorstw. Projekty musiałyby w pewnych zakresach korzystać też z zakupu usług obcych np. dotyczących wykonywania układów elektronicznych na ich zlecenie lub też posiłkować się obliczeniami kwantowymi uzyskanymi w drodze wynajmu od podmiotów zagranicznych (USA, Chiny).

Uczestnicy Smart Labu ocenili, że w ramach fazy I możliwe jest zrealizowanie 11 projektów. Projekty te powinny być relatywnie krótkie i zakończyć się w przeciągu 1 roku. Budżet fazy I oszacowano na 25 mln PLN.

Faza I | **Faza II** | Faza III

Faza II ma na celu przejście od koncepcji teoretycznych do faktycznych produktów zapewniających bezpieczeństwo w post kwantowej kryptografii. Projekty tematycznie powinny dotyczyć narzędzi i urządzeń dla sprzętowego i programowego wsparcia uwierzytelniania peer-to-peer spełniających wymogi bezwzględnego bezpieczeństwa, w tym w szczególności wymogi „uwierzytelniania dynamicznego” zawarte w UE1502/2015, z uwzględnieniem prototypowania i certyfikacji. Zaplanowano również testy koncepcji w warunkach laboratoryjnych, testowe wdrożenia i testowe implementacje w oparciu o przynajmniej jeden obowiązujący standard technologiczny. Wynikiem fazy powinny być prototypowe rozwiązania wychodzące naprzeciw postawionym problemom.

Do realizacji przewidzianych prac miałyby być niezbędne wykwalifikowane kadry, w tym również praktycy specjalizujący się w zaawansowanych technologiach obliczeniowych oraz powstałe w fazie I środki trwałe (laboratoria) i WNiP, rozszerzane o nowe inwestycje w infrastrukturę obliczeń kwantowych, która jest kosztowna zarówno w pozyskaniu, jak i utrzymaniu.

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 13 projektów. Projekty te powinny zakończyć się w przeciągu 3 lat. Budżet fazy II oszacowano na 175 mln PLN.

Faza I | Faza II | **Faza III**

Rezultatami fazy III powinny być integracja i modyfikacja oraz dostosowanie systemów i aplikacji - np. dostosowanie protokołów do wymagań nowych rozwiązań oraz dostosowanie interfejsów użytkownika. Pożądane jest wdrożenie na przynajmniej jednym standardowym systemie/ środowisku funkcjonującym komercyjnie. Jest to też działanie, w którym powinny zostać zrealizowane prace w zakresie ochrony własności intelektualnej uzyskanych rozwiązań.

Do realizacji przewidzianych prac miałyby być niezbędne wykwalifikowane kadry innowacyjnych przedsiębiorców i jednostek badawczych oraz powstałe w fazie I oraz II środki trwałe (laboratoria) i WNiP.

Uczestnicy Smart Labu ocenili, że w ramach fazy III możliwe jest zrealizowanie 15 projektów. Projekty te powinny zakończyć się w przeciągu 2 lat. Budżet fazy III oszacowano na 35 mln PLN.

Podsumowując, w ramach działania planowane jest zrealizowanie, w ciągu 6 lat, 39 projektów z całkowitym budżetem wynoszącym 235 mln zł. Pozwoli to na rozwój w kierunku wprowadzenia rozwiązań charakteryzujących się odpornością na obliczenia kwantowe. Byłoby to istotnym wzmocnieniem polskiego sektora cyberbezpieczeństwa na międzynarodowym rynku.

Działanie 2 - Uwierzytelnianie i kontrola dostępu

Celem tego działania jest rozwój innowacji w sektorze cyberbezpieczeństwa, dotyczących kontroli dostępu i uwierzytelniania. Potencjalne rezultaty działania znacząco rozwiną polski sektor cyberbezpieczeństwa i obejmować mogą:

- Przygotowanie nowych metod, protokołów i technologii dla realizacji usługi bezpiecznego pierwszego kontaktu w systemach uwierzytelniania.
- Urządzenia w technologiach FPGA, ASIC oraz biblioteki lub programy (również na urządzenia mobilne) implementujące bezpieczny, odporny na znane podatności, protokół pierwszego kontaktu.
- Powstanie bezhasłowego systemu uwierzytelnienia niezależnego od rozwiązań zagranicznych, w pełni zgodnego z wymogami UE z przeznaczeniem dla wielu sektorów gospodarki (uniwersalnego).
- Powstanie systemu szyfrowania jako produktu komercyjnego dla systemów i urządzeń OT.
- Opracowanie warstwy elektronicznej rozwiązań umożliwiającej skuteczne i efektywne szyfrowanie/ deszyfrowanie danych, weryfikację tożsamości i uwierzytelnianie w formie drugiego składnika. Wpisują się w to również tokeny sprzętowe do uwierzytelniania zgodnie ze standardami FIDO Alliance, inteligentne dokumenty (Smart Card) i wiele innych.

Rezultaty działania skierowane są do wszystkich grup odbiorców wymagających realizacji poufności i rozliczalności w przetwarzaniu informacji i danych. Dotyczy to zwłaszcza spełniania wymogów zdefiniowanych w rozporządzeniu wykonawczym UE 2015/1502. Docelowe rozwiązania powinny być łatwe do implementacji i stosowania przez użytkowników końcowych w wielu sektorach gospodarki, takich jak: eCommerce, służba zdrowia, bankowość i fintech, administracja publiczna, usługi on-line oraz przez producentów urządzeń IoT i integratorów systemów IoT. Skuteczne narzędzia do bezhasłowego uwierzytelniania oraz uwierzytelniania dla systemów teleinformatycznych znajdą zastosowanie zarówno w polskich instytucjach finansowych, jak i administracji publicznej czy też w siłach zbrojnych RP.

Działanie obejmuje prace we wszystkich 3 fazach:

Faza I | Faza II | Faza III

W fazie I uczestnicy SL przewidują dużą aktywność podmiotów zarówno naukowych, jak i przemysłowych. Przewiduje się takie projekty jak:

- Opracowanie nowych innowacyjnych rozwiązań opartych o technologie kryptograficzne (w tym blockchain) pozwalających na integrację usług identyfikacji oraz systemów klasy Wallet.
- Opracowanie koncepcji systemu komunikacji i przedstawienie propozycji komunikacji między urządzeniami (i podsystemami) w środowiskach OT.
- Przeprowadzenie studiów wykonalności, dotyczących wprowadzania nowych systemów autentykacji.
- Badania nad koncepcjami nowych rozwiązań kryptograficznych, analizy podatności oraz wiele innych prac mających na celu wyodrębnienie nowych algorytmów, np. z wykorzystaniem kluczy jednorazowych.

Do realizacji projektów niezbędne będą wykwalifikowane kadry w obszarze kryptografii i bezpieczeństwa systemów oraz środki trwałe i WNiP jednostek akademickich i podmiotów dysponujących działami B+R mającymi doświadczenie w obszarze metod i technologii uznanych za bezpieczne.

Uczestnicy Smart Labu ocenili, że w ramach fazy I możliwe jest zrealizowanie 30 projektów. Projekty te powinny zakończyć się w przeciągu 1 roku. Budżet fazy I oszacowano na 71 mln PLN.

Faza I | **Faza II** | Faza III

Przykładowe projekty zaplanowane w fazie II to:

- Opracowanie urządzeń w technologiach półprzewodnikowych, mikroprocesorowych oraz kwantowych do generowania tożsamości oraz zarządzania tożsamością, z uwzględnieniem zaleceń dla kryptografii z kluczami jednorazowymi, w tym prototypowanie i certyfikacja.
- Opracowanie warstwy sprzętowej dla procesu uwierzytelniania dynamicznego w niewielkich układach scalonych, umożliwiających implementację podpisu cyfrowego czy algorytmów uwierzytelniania w oparciu o krzywe eliptyczne zarówno w kryptografii klucza publicznego, jak i z zastosowaniem kluczy jednorazowych.
- Opracowanie systemu bezpiecznego uwierzytelniania bez konieczności dodatkowych sterowników czy konieczności instalowania dodatkowego oprogramowania.

Faza II będzie mogła zostać uznana za zakończoną, jeżeli powstaną prototypowe technologie i urządzenia oraz biblioteki programistyczne dla integracji z usługami zarządzania tożsamością cyfrową i realizacji usługi „pierwszego kontaktu" dla systemów i usługi uwierzytelniania, autoryzacji oraz kontroli dostępu.

Projekty będą mogły być realizowane przez firmy posiadające działy B+R oraz innych przedsiębiorców przy udziale jednostek badawczych. Do realizacji przewidzianych prac miałyby być niezbędne wykwalifikowane kadry w obszarze kryptografii i bezpieczeństwa systemów oraz powstałe w fazie I środki trwałe (w tym laboratoria) i WNiP.

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 44 projektów. Projekty te powinny zakończyć się w przeciągu 2 lat. Budżet fazy II oszacowano na 120 mln PLN.

Faza I | Faza II | **Faza III**

Faza III ma posłużyć integracji i modyfikacji opracowanych w fazie II prototypów do zastosowań praktycznych i wdrożeń. W szczególności pożądane są wdrożenia z gotowością systemu na poziomie produkcyjnym w środowiskach webowych i mobilnych, w obszarach takich jak fintech, e-Commerce, e-Health, przy zachowaniu zgodności nowych rozwiązań i usług z wymaganiami eIDAS 2.0 oraz ich integracja z istniejącymi produktami i usługami na rynku.

Kluczowymi zasobami dla fazy III powinny być zasoby ludzkie, w postaci ekspertów w przedsiębiorstwach, którzy posiadać będą wiedzę i umiejętności do przeprowadzenia wdrożeń oraz testów i dostosowania wypracowanych technologii u klientów.

Uczestnicy SL oszacowali, że w ramach fazy III możliwe jest zrealizowanie 45 projektów w okresie 4 lat. Szacowany budżet wynosi 90 mln PLN.

Podsumowując, działanie 2 ma zwiększyć konkurencyjność polskiego rynku cyberbezpieczeństwa oraz w konsekwencji podnieść poziom cyberbezpieczeństwa w kraju w zakresie autentykacji. W ramach działania planowane jest zrealizowanie w okresie 7 lat łącznie 119 projektów z całkowitym budżetem wynoszącym 281 mln PLN.

Działanie 3 - Usługi zaufania

Celem tego działania jest wytworzenie produktów, takich jak zaawansowane kryptograficzne rozwiązania w zakresie usług zaufania jak np. ochrona zbiorów archiwalnych lub dokumenty cyfrowe. Do tego celu mogą posłużyć np. technologie blockchain. Opracowanie takich rozwiązań pozwoli na osiągnięcie wysokiego stopnia konkurencyjności na rynku polskim, jak i zagranicznym.

W wyniku działania powinny powstać nowe usługi zaufania zabezpieczające dokumenty i transakcje elektroniczne zgodnie z rozporządzeniem eIDAS 2.0. Usługi powinny również spełniać wymagania NIS2. Odbiorcami będą wszystkie branże zobowiązane na mocy eIDAS 2.0 do korzystania z kwalifikowanych usług zaufania (na mocy przepisów unijnych i polskich). Adresaci, to również rynek EU oraz rynki realizujące transakcje transgraniczne z EU (np. Szwajcaria, Norwegia, Ukraina, Turcja, UK).

Działanie obejmuje prace we wszystkich 3 fazach:

Faza I | Faza II | Faza III

W fazie I przeprowadzone zostaną prace mające na celu zdobycie nowej wiedzy potrzebnej do opracowania usług zaufania. Szczególnie w tym obszarze nacisk powinien być położony na kryptograficzne rozwiązania dotyczące archiwów cyfrowych. W tej fazie możliwe byłoby również przeprowadzenie analiz pozwalających na najlepsze zidentyfikowanie obszarów wymagających nowych usług zaufania. Rezultaty tej fazy pozwolą na płynną realizację późniejszych badań przemysłowych i prac rozwojowych.

Realizacja fazy I bazowałaby na wykwalifikowanej kadrze jednostek badawczych i przedsiębiorstw w obszarze kryptografii i bezpieczeństwa systemów. Wykorzystywane byłyby też środki trwałe (istniejące i nowo utworzone) oraz WNiP będące w posiadaniu uczelni i przedsiębiorstw. Projekty musiałyby w pewnych zakresach korzystać też z zakupu usług obcych np. dotyczących wykonywania układów elektronicznych na zlecenie.

Uczestnicy Smart Labu ocenili, że w ramach fazy I możliwe jest zrealizowanie 4 projektów. Projekty te powinny być relatywnie krótkie i zakończyć się w przeciągu 1 roku. Budżet fazy I oszacowano na 6 mln PLN.

Faza I | **Faza II** | Faza III

Faza II ma na celu przekształcić wyniki badań podstawowych i założeń powstałych w fazie I na technologie prowadzące do nowych produktów. W szczególności powinny powstać zarysy nowych produktów, potencjalnie w formie prototypów w skali laboratoryjnej/ pilotażowej. Realizacja prac powinna być przeprowadzona przez przedsiębiorstwa o ugruntowanej pozycji, tak aby możliwie szeroko zmobilizować rynek do działań w fazie III.

Do realizacji przewidzianych prac miałyby być niezbędne wykwalifikowane kadry oraz powstałe w fazie I środki trwałe i WNiP.

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 4 projektów. Projekty te powinny zakończyć się w przeciągu 1 roku. Budżet fazy II oszacowano na 12 mln PLN.

Faza I | Faza II | **Faza III**

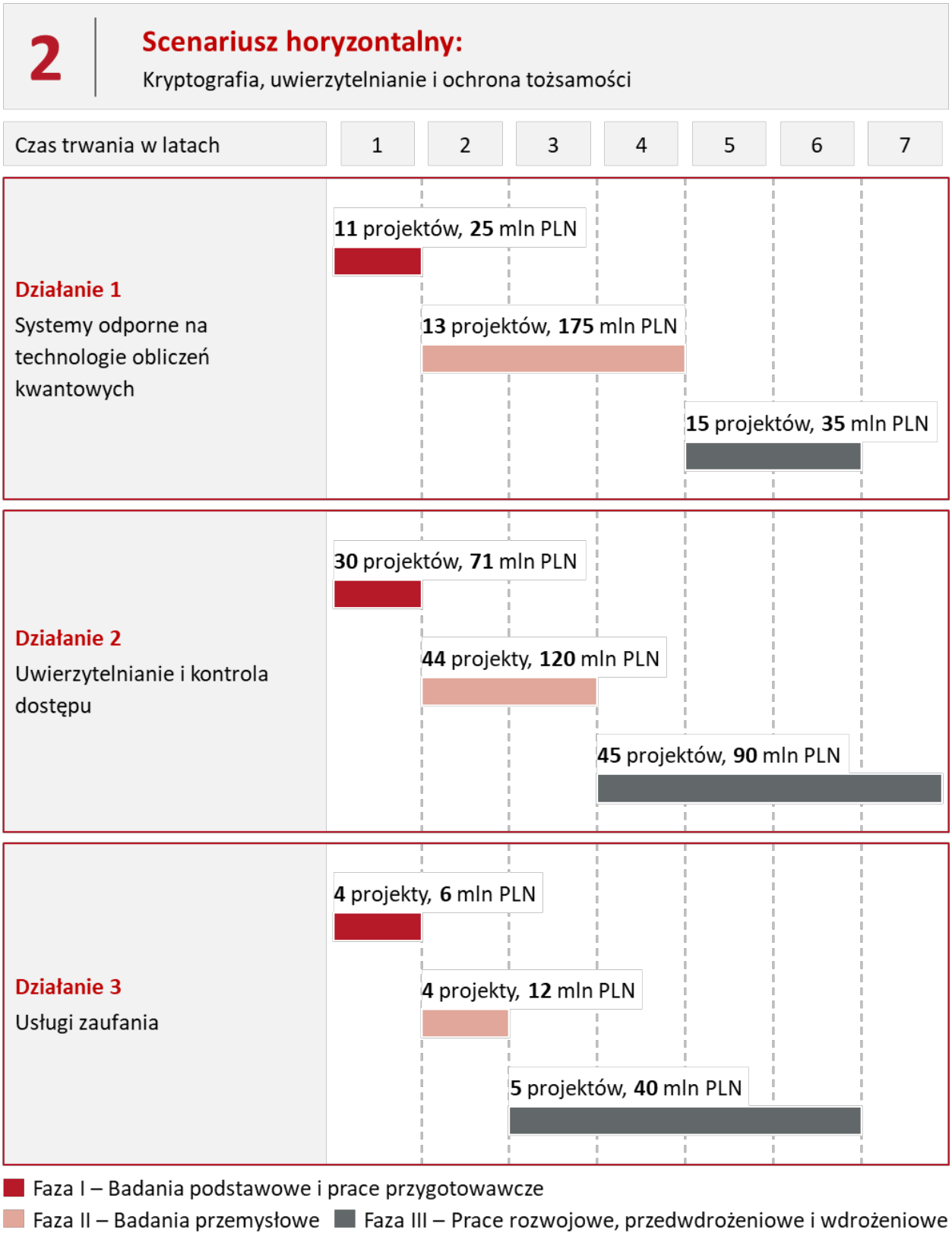
Faza III powinna być skupiona na dotarciu z nowymi usługami zaufania do odbiorców. W ramach fazy III należy przetestować rozwiązania w warunkach zbliżonych do rzeczywistych i dokonać wdrożeń pilotażowych. Ze względu na trudności np. w przeniesieniu danych do chronionych kryptograficznie archiwów, faza ta jest bardziej czasochłonna.

Kluczowymi zasobami dla fazy III powinny być zasoby ludzkie, w postaci ekspertów w przedsiębiorstwach, którzy posiadać będą wiedzę i umiejętności do przeprowadzenia wdrożeń oraz testów i dostosowania wypracowanych technologii u klientów.

Uczestnicy Smart Labu ocenili, że w ramach fazy III możliwe jest zrealizowanie 5 projektów. Projekty te powinny zakończyć się w przeciągu 4 lat. Budżet fazy III oszacowano na 40 mln PLN.

W ramach działania planowane jest zrealizowanie w okresie 6 lat łącznie 13 projektów z całkowitym budżetem wynoszącym 58 mln PLN. Jak wspomniano wcześniej, wprowadzenie opracowanych rozwiązań powinno przyczynić się do wsparcia procesów internacjonalizacji polskich przedsiębiorstw na rynkach europejskich i pozaeuropejskich.

Rysunek 24. Forma graficzna scenariusza 2



Źródło: opracowanie własne

5.1.3. Scenariusz 3 – Cyberbezpieczeństwo instalacji procesowych

W przeciwieństwie do poprzednich dwóch scenariuszy, scenariusz trzeci nie ma charakteru horyzontalnego, lecz skupia się na potrzebach jednego obszaru, jakim są systemy segmentu tzw. „Operational Technology" (OT), obejmującego m.in. infrastrukturę procesową i energetykę. Jest to w dużej mierze infrastruktura krytyczna (IK), pełniącą ważną rolę w łańcuchu dostaw. Jednocześnie, w przeciwieństwie do innych obszarów, mamy tu do czynienia z urządzeniami o wysokiej żywotności, wymagającej w rezultacie integracji z rozwiązaniami technologicznymi z różnych generacji, których wdrażanie i modyfikowanie nie może zakłócać podstawowej pracy systemów. Zwiększanie odporności infrastruktury na zagrożenia staje się więc niezwykle ważne, zarówno dla bezpieczeństwa danych, jak i samych urządzeń.

W ramach tego scenariusza uczestnicy SL skupili się na trzech aspektach. Pierwszym, najbardziej ukierunkowanym, jest zarządzanie ryzykiem systemów OT. Analiza wskazuje, że zapotrzebowanie na uaktualnienie paradygmatu kontroli bezpieczeństwa do współczesnych standardów jest bardzo duże. Drugi aspekt dotyczy rozwoju innowacyjnych technologii bezpieczeństwa OT, które ukończyły już fazę badań podstawowych i dojrzały do przekształcenia w konkretne produkty. Ostatni aspekt jest najbardziej perspektywiczny, ponieważ dotyczy stworzenia potencjału rozwojowego dla technologii bezpieczeństwa w Polsce poprzez utworzenie centrów badawczo-rozwojowych ukierunkowanych na potrzeby segmentu OT. Za każdy z tych aspektów odpowiada jedno dedykowane działanie.

Działanie 1 - Powstanie oprogramowania i narzędzi do obsługi i zarządzania systemów OT

Celem działania jest powstanie nowych produktów pozwalających na integrację i zarządzanie bezpieczeństwem infrastruktury zaliczanej do segmentu OT. W szczególności należy przewidzieć powstanie systemów zarządzania ryzykiem w zakresie cyberbezpieczeństwa dla infrastruktury krytycznej.

Wynikiem tego działania miałoby być oprogramowanie zbierające w jednym panelu informacje z wielu źródeł i na podstawie algorytmów przeliczające wartości ryzyka dla danych zasobów. Obecnie istnieją programy realizujące niektóre elementy, jednak brak jest między nimi integracji. Nowe rozwiązania w ramach tego działania mogłyby więc powstawać na różne sposoby – albo jako elementy systemu do integracji, albo jako rozwiązania integrujące. Dzięki zaistnieniu takich rozwiązań możliwe byłoby spełnienie wymagań prawnych dotyczących KSC, tj. Krajowego Systemu Cyberbezpieczeństwa, takich jak priorytetyzacja działań związanych z rozwojem obszaru cyberbezpieczeństwa OT czy szybka reakcja na pojawiające się ryzyka w sieci OT.

Potencjalnymi odbiorcami będą wszystkie spółki podlegające pod ustawę KSC, ale również duże zakłady przemysłowe i inne przedsiębiorstwa produkcyjne/ świadczące usługi oparte o infrastrukturę (wodociągi, PEC itp.), które posiadają rozległe sieci OT z dużą liczbą urządzeń.

Działanie obejmuje prace we wszystkich 3 fazach:

Faza I | Faza II | Faza III

Projekty realizowane w ramach fazy I będą prowadzić do opracowania koncepcji oprogramowania, które w sposób automatyczny i ciągły będzie analizować ryzyka a w szczególności pozwalać zarządzać wysokimi ryzykami. Zaplanowane bezpośrednie wyniki tej fazy obejmują np.:

- Opracowanie szczegółowej koncepcji oprogramowania.
- Identyfikacja źródeł do analizy ryzyka.
- Opracowanie algorytmów do analizy ryzyka.
- Opracowanie mechanizmów do automatycznej mitygacji ryzyka.

Realizacja fazy I bazowałaby na wykwalifikowanej kadrze jednostek badawczych i przedsiębiorstw w obszarze inżynierii procesowej, energetyce, obliczeń numerycznych oraz bezpieczeństwa systemów. Wykorzystywane byłyby też środki trwałe (w tym laboratoria z różnymi urządzeniami OT, istniejące i nowo utworzone czy istniejące oprogramowanie typu IDS) oraz WNiP będące w posiadaniu uczelni i przedsiębiorstw. Projekty musiałyby w pewnych zakresach korzystać też z zakupu usług obcych np. dotyczących wykonywania układów elektronicznych na ich zlecenie.

Uczestnicy Smart Labu ocenili, że w ramach fazy I możliwe jest zrealizowanie 5 projektów. Projekty te powinny być relatywnie krótkie i zakończyć się w przeciągu 1 roku. Budżet fazy I oszacowano na 5 mln PLN.

Faza I | **Faza II** | Faza III

Faza II ma na celu opracowanie interfejsów/ innych mechanizmów pozwalających na zebranie danych (pochodzących z różnych źródeł) dotyczących podatności i zagrożeń w środowisku OT. W tym celu konieczne będzie opracowanie funkcjonalnych prototypów oprogramowania, testowanie skuteczności mechanizmów integracyjnych oraz algorytmu do analizy ryzyka, jak również testowanie mechanizmów mitygacji ryzyka.

Do realizacji projektów potrzebni będą specjaliści z zakresu cyberbezpieczeństwa, a także z zakresu zarządzania ryzykiem oraz infrastruktura taka jak laboratoria, w których będzie można symulować opracowane algorytmy i tworzyć mechanizmy integracji. Ważnym aspektem będzie również współpraca z producentami narzędzi, która będzie źródłem do analizy ryzyka, np. w drodze usług

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 5 projektów. Projekty te powinny zakończyć się w przeciągu 2 lat. Budżet fazy II oszacowano na 5 mln PLN.

Faza III ma na celu uruchomienie i doskonalenie gotowych produktów w środowiskach produkcyjnych OT. Odbiorcami będą wszystkie jednostki podlegające pod IK i KSC (w tym spółki gazowe, energetyczne, producenci ciepła oraz firmy z branży wydobywczej) oraz duże zakłady produkcyjne. W ramach fazy III konieczne będzie testowanie stworzonych prototypów w środowiskach testowych i produkcyjnych w realnych warunkach funkcjonujących sieci OT oraz realizacja indywidualnych wdrożeń przy równoczesnym doskonaleniu mechanizmów integracji oraz algorytmów analizy ryzyka.

Kluczowymi zasobami dla fazy III będą zasoby ludzkie, w postaci ekspertów w przedsiębiorstwach, którzy posiadać powinni wiedzę i umiejętności do przeprowadzenia wdrożeń oraz testów i dostosowania wypracowanych technologii u klientów.

Uczestnicy Smart Labu ocenili, że w ramach fazy III możliwe jest zrealizowanie 60 projektów. Projekty te powinny zakończyć się w przeciągu 2 lat. Budżet fazy III oszacowano na 6 mln PLN.

Działanie 1 ma na celu doprowadzenie do powstania specjalistycznych narzędzi pozwalających na zarządzanie ryzykiem w środowiskach OT, począwszy od określenia potencjału, poprzez dopracowanie rozwiązania aż do jego wdrożenia. W ciągu 5 lat zostanie zrealizowanych 70 projektów z całkowitym budżetem 16 mln.

Działanie 2 - Rozwój innowacyjnych technologii bezpieczeństwa procesów

Celem działania jest umożliwienie efektywnego rozwoju innowacyjnych rozwiązań produktowych z zakresu cyberbezpieczeństwa OT, które osiągnęły już co najmniej trzeci poziom gotowości technologicznej (TRL). Przykładami takich rozwiązań są przemysłowa dioda danych, platformy bezpieczeństwa OT czy rozproszone korelatory procesowe.

Korzyści wynikające z tego działania to nowe produkty na rynku, które w innym przypadku pojawiłyby się na nim ze znacznym opóźnieniem. Systemy identyfikacji modułów logicznych będą pozwalały na łatwą identyfikację elementów instalacji i jednoczesną kontrolę dostępową. Przemysłowa dioda danych, to innowacyjne rozwiązanie zapewniające kontrolę kierunku przepływu danych określonymi kanałami. Platforma bezpieczeństwa OT pozwoli na integrację rozlicznych rozwiązań w centra zarządzania bezpieczeństwem operacyjnym. Natomiast korelatory procesowe pozwolą na bezpieczną detekcję zagrożeń w systemie. To jedynie przykłady rozwiązań, które przekroczyły już poziom gotowości technologicznej i potrzebują rozwinięcia w produkty rynkowe. Odbiorcami mogą być w dużej mierze wszystkie zakłady przemysłowe, w tym m.in. energetyczne, chemiczne, paliwowe, gazowe czy farmaceutyczne. Dodatkowe korzyści obejmują zwiększenie poziomu identyfikacji, bieżącego monitorowania systemów, zwiększenie poziomu bezpieczeństwa procesów technologicznych oraz zmniejszanie kosztów eksploatacyjnych. Dodatkową korzyścią będzie poprawne wprowadzanie danych agregacyjnych do platform cyberbezpieczeństwa poziomu krajowego.

Uczestnicy SL ocenili, że racjonalne jest w przypadku tej problematyki pominięcie fazy badań podstawowych i prac przygotowawczych, jako że wiedza podstawowa w tym zakresie jest dobrze ugruntowana.

Tak więc działanie obejmuje prace w fazach II i III:

Faza II Faza III

W ramach fazy II powinny zostać zrealizowane prace badawcze umożliwiające weryfikację koncepcji na rzecz wprowadzenia jej do testów w warunkach rzeczywistych, takie jak:

- Wsparcie dla rozbudowy funkcyjnej oraz strony kompatybilności aplikacyjnej i strumieniowej dla Diody Danych OT.
- Integracja systemu detekcji protokołów przemysłowych klasy Profinet i Ethernet/ IP.
- Testy bezpieczeństwa oraz stabilności predykcji i reakcji.

Rezultatem tej fazy będą rozwiązania prototypowe urządzeń i technologii bezpieczeństwa procesów.

Do realizacji fazy II potrzebne będzie zaplecze kadrowe obejmujące specjalistów z zakresu cyberbezpieczeństwa, inżynierii procesowej i algorytmiki. Przewidywane jest zaangażowanie zarówno sektora przemysłowego, jak i akademickiego.

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 16 projektów. Projekty te powinny zakończyć się w przeciągu 2 lat. Budżet fazy II oszacowano na 15 mln PLN.

Faza II **Faza III**

Faza III ma na celu integrację i modyfikację oraz dostosowanie systemów i aplikacji na potrzeby zapewnienia wdrożeń. W szczególności najważniejsza jest tu integracja opracowanych rozwiązań w systemach OT. Potencjał wdrożeń nowych rozwiązań jest bardzo duży, jako że wiele rezultatów fazy badań przemysłowych ma już docelowych odbiorców. Wynikiem będzie efektywne wdrożenie licznych rozwiązań z zakresu bezpieczeństwa infrastruktury OT.

Bazą do realizacji projektów będzie przemysł OT i specjaliści od cyberbezpieczeństwa.

Uczestnicy Smart Labu ocenili, że w ramach fazy III możliwe jest zrealizowanie 150 projektów. Projekty te powinny zakończyć się w przeciągu 4 lat. Budżet fazy III oszacowano na 15 mln PLN.

W ramach działania planowane jest zrealizowanie w okresie 6 lat łącznie 166 projektów z całkowitym budżetem wynoszącym 30 mln PLN. Wszystkie te projekty w sposób istotny odpowiadają na potrzeby środowiska OT i wpisują się w światowe trendy bezpieczeństwa infrastruktury i łańcuchów dostaw.

Działanie 3 - Perspektywiczne technologie rozwojowe w bezpieczeństwie procesów

Celem działania jest stworzenie potencjału badawczego i doprowadzenie do wdrożeń innowacyjnych układów samoświadomych (self aware) wchodzących w skład centrów bezpieczeństwa operacji (SOC). Będzie to wymagało powstania centrów B+R oraz pilotażowych systemów bezpieczeństwa.

Działanie to ma charakter inny od typowych, pojedynczych projektów B+R, gdyż jego celem jest budowa potencjału, poprzez tworzenie centrów badawczo rozwojowych i realizacji w nich projektów w ramach określonej z góry agendy badawczej, zgodnie z którą ma działać dane centrum. Działania tego typu były już w Polsce realizowane, a w ramach nich firmy otrzymywały środki na tworzenie centrów badawczo-rozwojowych w swojej dziedzinie. Przykładem może być działanie 2.1 Programu Operacyjnego Inteligentny Rozwój „Wsparcie inwestycji w infrastrukturę B+R przedsiębiorstw". Planowane do utworzenia centra będą się dynamicznie rozwijać, realizując jednocześnie projekty ze wszystkich trzech faz. Będzie to możliwe, ze względu na to, że część technologii wymagających wdrożenia już istnieje, część jest na zaawansowanym stopniu rozwoju, zaś część jest na wczesnym poziomie gotowości technologicznej, której podniesienie będzie wymagało dodatkowych nakładów.

Okres realizacji całego zakresu tego działania ma wynosić 5 lat. Dla zachowania spójności dokumentu i formy przedstawiania poszczególnych działań w ramach scenariuszy rozwoju poniżej przedstawiono rozbicie poszczególnych faz i projektów, jednak co do zasady ewentualne wsparcie finansowe w tym działaniu powinno obejmować projekty, które zakładać będą realizację wszystkich trzech faz prac równocześnie. Tym samym beneficjent powinien w ramach projektu przewidzieć zarówno część inwestycyjną związaną z utworzeniem i uruchomieniem centrum badawczo-rozwojowego, jak i agendę badawczą obejmującą projekty B+R w fazach I, II oraz III.

W rezultacie działanie obejmuje prace we wszystkich 3 fazach:

Faza I | Faza II | Faza III

W ramach fazy I głównym celem będzie powstanie centrów badawczo-rozwojowych specjalizujących się w cyberbezpieczeństwie środowisk OT, jak również pilotażowych rozwiązań testowo-weryfikacyjnych pozwalających na testowanie i tworzenie nowych technologii zabezpieczających. Takie centra miałyby być tworzone przez przedsiębiorców, z ewentualnym udziałem sektora naukowego.

Sukcesem fazy I będzie powstanie planowanych centrów B+R oraz rozpoczęcie w nich prac B+R przewidzianych dla tej fazy.

W ramach tej fazy zostaną wykorzystane zasoby ludzkie ze środowisk przemysłowych i akademickich, które będą wzmacniać potencjał kadrowy centrów. Konieczne będą również inwestycje w sprzęt, aparaturę, a także budynki o odpowiednich warunkach bezpieczeństwa i możliwościach energetycznych.

Uczestnicy Smart Labu ocenili, że w ramach fazy I możliwe jest zrealizowanie 5 projektów. Projekty te powinny zakończyć się w przeciągu 5 lat. Budżet fazy I oszacowano na 130 mln PLN.

Faza I | **Faza II** | Faza III

W ramach fazy II realizowane mają być prace związane z integracją centrów badawczo-rozwojowych z procesami badań i rozwoju przedsiębiorstw oraz ich laboratoriów. Powstać mają prototypy urządzeń (pomiarowych, zbierających dane, wykonawczych, predykcyjnych) i oprogramowania rozproszonego (zabezpieczeń, wizualizacji, komunikacji), których powstanie bez centrów nie byłoby możliwe.

Ponieważ faza II odbywa się równolegle do pozostałych i ma charakter badawczy, konieczne jest wykorzystanie zbliżonych zasobów przy jednocześnie zwiększonym zaangażowaniu przedsiębiorców.

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 4 projektów. Projekty te powinny zakończyć się w przeciągu 5 lat. Budżet fazy I oszacowano na 80 mln PLN.

Faza I | Faza II | **Faza III**

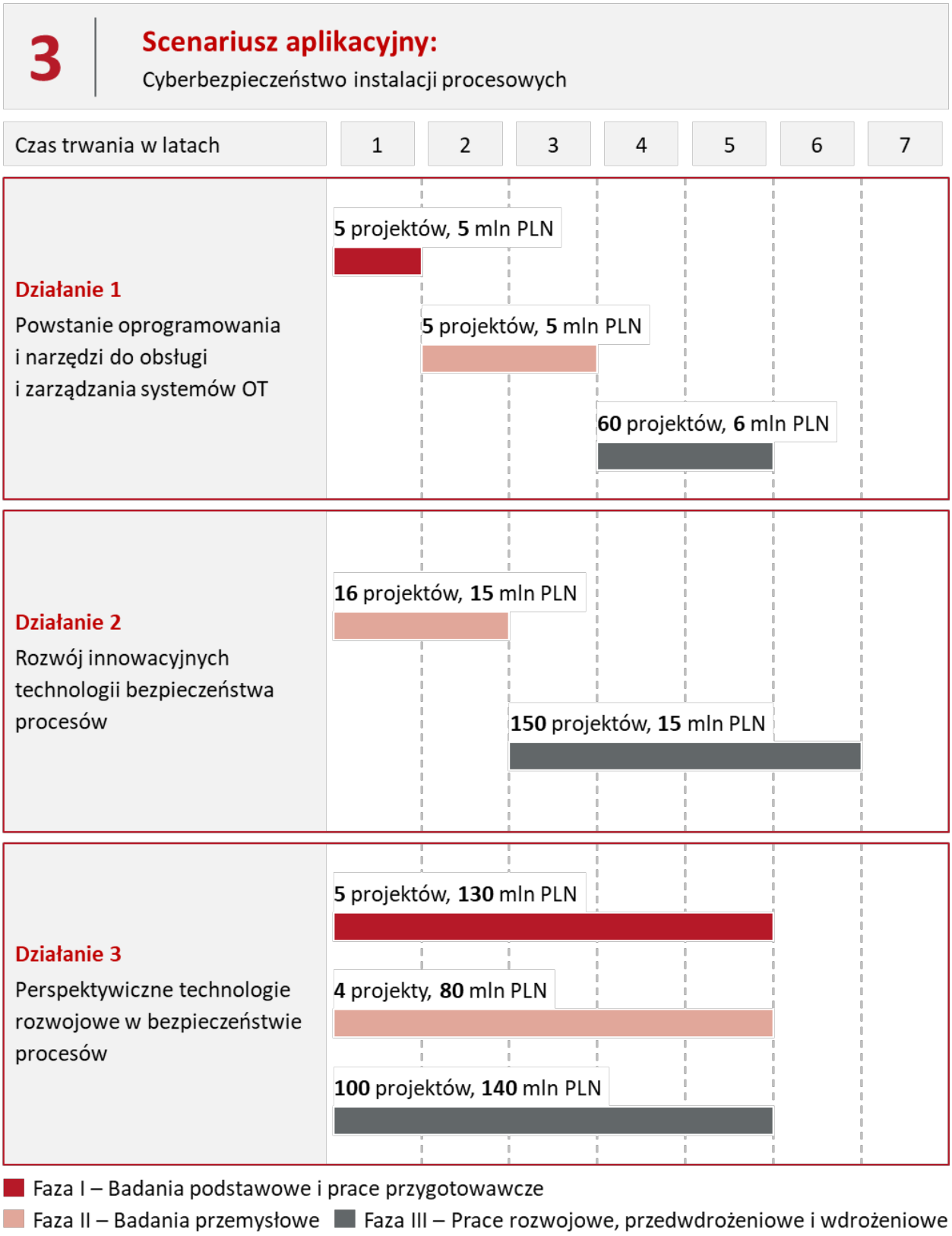
Faza III będzie polegać na sukcesywnym wdrażaniu u odbiorców przemysłowych rozwiązań opracowywanych i testowanych w centrach badawczo-rozwojowych i instalacjach pilotażowych. Projekty te mogą dotyczyć m.in. certyfikacji uzyskanych rozwiązań oraz wprowadzania systemów opracowanych w centrach badawczo-rozwojowych do łańcuchów decyzyjnych. Uzupełnieniem będą działania realizujące testy w warunkach rzeczywistych prowadzące do finalnego wdrożenia.

Kluczowymi zasobami dla fazy III powinny być zasoby ludzkie, w postaci ekspertów w przedsiębiorstwach, którzy posiadać będą wiedzę i umiejętności do przeprowadzenia wdrożeń oraz testów i dostosowania wypracowanych technologii u klientów.

Uczestnicy Smart Labu ocenili, że w ramach fazy III możliwe jest zrealizowanie 100 projektów. Projekty te powinny zakończyć się w przeciągu 5 lat. Budżet fazy III oszacowano na 140 mln PLN.

Działanie 3 wymaga dużych nakładów na część inwestycyjną związaną z powołaniem do życia centrów B+R. W ramach działania planowane jest zrealizowanie w okresie 5 lat (wszystkie trzy fazy zaplanowano do równoległej realizacji, a więc zaczynają się i kończą w tym samym okresie) łącznie 109 projektów z całkowitym budżetem wynoszącym 350 mln PLN.

Rysunek 25. Forma graficzna scenariusza 3



Źródło: opracowanie własne

5.1.4. Scenariusz 4 – Cyberbezpieczeństwo sieci i IoT

Urządzenia IoT stały się wszechobecne w codziennym życiu i zastosowaniach przemysłowych. Atrakcyjność rozproszonych rozwiązań sieciowych jest na tyle duża, że pomijane lub nawet ignorowane są wzrosty podatności na ataki. Z tego właśnie powodu scenariusz czwarty jest dedykowany rozwiązaniom z zakresu cyberbezpieczeństwa w systemach Internetu Rzeczy.

Działanie 1 - Wydajne algorytmy szyfrowania i nowe protokoły komunikacji urządzeń IoT oraz ich sprzętowe implementacje

Celem działania jest wprowadzenie na rynek nowości technologicznych o charakterze programowym i sprzętowym. Szczególny nacisk położony jest na rozwiązania kryptograficzne oraz nowe (lub ulepszone) protokoły komunikacyjne. Należy podkreślić, że w kontekście IoT nie można rozpatrywać tych kwestii bez analizy kwestii implementacyjnych zarówno w aspekcie prędkości wykonywania procesów, jak i redukcji zużycia energii.

Kontekst do podjęcia tego działania wynika z faktu, że w obecnym paradygmacie bezpieczeństwa sieci urządzenia IoT stanowią najsłabsze ogniwo. Są to urządzenia produkowane masowo, w niskich cenach i o małych możliwościach obliczeniowych, co naturalnie ogranicza sposoby ich zabezpieczania. Uczestnicy SL zdiagnozowali, że chcąc zwiększyć bezpieczeństwo sieci IoT, konieczne jest wprowadzenie technologii, która temu zaradzi. Rozwiązania tego problemu można poszukiwać w nowych algorytmach szyfrowania, dedykowanych elektronicznych układach bezpieczeństwa czy w nowych protokołach sieciowych. Wszystkie te rozwiązania muszą się jednak charakteryzować małym obciążaniem zasobów obliczeniowych urządzenia oraz małym zużyciem energii.

Działanie obejmuje prace we wszystkich 3 fazach:

Faza I | Faza II | Faza III

W fazie I przewiduje się, że będą realizowane prace nad takimi zagadnieniami jak:

- Wydajne algorytmy o niskim zużyciu energii.
- Analizy zdolności do adaptacji protokołów na rynku.
- Wydajne algorytmy kryptograficzne realizowane sprzętowo w układach elektronicznych z wykorzystaniem sprzętowych akceleratorów kryptograficznych.
- Lekkie (wymagające małej ilości zasobów obliczeniowych) algorytmy szyfrowania.

Wymagane zasoby i zakresy prac dla każdego projektu będą różne, głównie z uwagi na silnie interdyscyplinarny charakter działania (np. dla rozwiązań sprzętowych konieczne będzie projektowanie i produkcja eksperymentalnych układów elektronicznych, co znacząco podnosić będzie ich koszty). Projekty te mogą być realizowane przez uczelnie, jednostki badawczo-rozwojowe oraz firmy posiadające działy B+R.

Uczestnicy Smart Labu ocenili, że w ramach fazy I możliwe jest zrealizowanie 15 projektów. Projekty te powinny być relatywnie krótkie i zakończyć się w przeciągu 2 lat. Budżet fazy I oszacowano na 55 mln PLN.

Faza I | **Faza II** | Faza III

Faza II będzie dopełnieniem fazy I. Oprócz rozwijania opracowanych rozwiązań analizowane będą też rozwiązania budowane w oparciu o już obecnie istniejącą wiedzę. W szczególności tematem mogłaby być rozbudowa istniejących protokołów o elementy bezpieczeństwa, tak aby nowe, bezpieczne produkty były zgodne z istniejącymi sieciami. Konieczne będą implementacje nowych algorytmów, rozwiązań niskoenergetycznych i układów cybersecurity-on-chip. Powstaną prototypowe rozwiązania programowe/ biblioteki. Opracowane mogłyby zostać komponenty mikroelektroniczne do implementacji w układach scalonych w dowolnej lub jednej z wybranych technologii produkcji układów. Inne zagadnienia obejmują np. opracowanie projektu bezpiecznej szyfrowanej pamięci dla układów IoT lub opracowanie bezpiecznego bootloadera umożliwiającego szybkie szyfrowanie i deszyfrowanie w czasie rzeczywistym kodu programu układów IoT. Ważne jest zapewnienie efektywności szyfrowania umożliwiającej stosowanie bezpiecznych algorytmów przy ograniczonej mocy obliczeniowej i energochłonności rozwiązania.

Zasoby, podobnie jak w fazie I, będą się wyraźnie różnić pomiędzy projektami, głównie ze względu na ich materialny charakter (hardware), albo niematerialny (software). Jedne i drugie projekty potrzebują specjalistów z odpowiednich dziedzin: programistów, elektroników, automatyków, a do grona realizujących podmiotów mogą wejść producenci urządzeń i oprogramowania posiadający własne działy B+R lub we współpracy z konsorcjantami o odpowiednich kwalifikacjach.

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 15 projektów. Projekty te powinny zakończyć się w przeciągu 3 lat. Budżet fazy II oszacowano na 55 mln PLN.

Faza I | Faza II | **Faza III**

Faza III ma na celu wsparcie wdrożenia nowych rozwiązań. W ramach tej fazy powinny być realizowane projekty związane ze wsparciem w szczególności takich obszarów jak:

- Implementacja w urządzeniach na rynek.
- Uruchamianie produkcji systemów.
- Ochrona własności intelektualnej.
- Certyfikacje (CE, EMC, a także być może również certyfikaty opracowane w działaniu 3 niniejszego scenariusza).
- Wdrażanie produkcji układów elektronicznych.

Projekty w ramach fazy III powinny być realizowane zasobami głównie należącymi do producentów oprogramowania i sprzętu.

Uczestnicy Smart Labu ocenili, że w ramach fazy III możliwe jest zrealizowanie 25 projektów. Projekty te powinny zakończyć się w przeciągu 3 lat. Budżet fazy III oszacowano na 35 mln PLN.

W ramach działania planowane jest zrealizowanie w okresie 7 lat łącznie 55 projektów z całkowitym budżetem wynoszącym 145 mln PLN. Czas trwania działania jest krótszy niż suma czasu trwania poszczególnych jego faz z uwagi na fakt, że część prac fazy II można rozpocząć w trakcie realizacji prac fazy I. Całe działanie powinno doprowadzić do uzyskania nowych, konkurencyjnych technologii pozwalających na produkcję bezpiecznych urządzeń zaliczanych do segmentu IoT.

Działanie 2 - Sieci IoT i ich rozbudowa

Celem działania drugiego jest rozwiązanie problemu jakim jest obecność na rynku wielu niezabezpieczonych lub niewiadomego pochodzenia urządzeń. Urządzenia te, ze względu na swoje atrakcyjne ceny są szeroko wykorzystywane i w związku z tym generują podatności na ataki. Potrzebne jest więc zabezpieczenie rozwiązań z tego segmentu poprzez odpowiednie integracje nowych i starych technologii, w sposób umożliwiający ich niskokosztową modernizację. W wyniku działania powinny powstać wieloprotokołowe interfejsy sieciowe (tzw. bramki), nowe struktury chmurowe oraz metody wirtualnej i fizycznej segmentacji sieci, które zapewnią bezpieczne użytkowanie niepewnych urządzeń.

Działanie obejmuje prace we wszystkich 3 fazach:

Faza I | Faza II | Faza III

W fazie I uczestnicy SL przewidzieli dwa projekty. Pierwszym projektem jest analiza potencjalnych nowych mediów komunikacyjnych, które mogą być wykorzystane do poprawy bezpieczeństwa. W tym celu potrzebne jest przebadanie sposobów połączenia oraz wirtualnych podziałów sieci urządzeń, tak aby zapewnić odpowiednie poziomy bezpieczeństwa. Drugi projekt dotyczy poziomu świadomości użytkowników w zakresie bezpieczeństwa otaczających ich urządzeń, ponieważ dopiero świadomy użytkownik będzie zdawał sobie sprawę z czyhających go zagrożeń. W tym celu konieczne jest przeprowadzenie stosownych diagnoz społecznych.

Wyniki tej fazy określą możliwości kierunków rozwoju w fazie II, które na tę chwilę nie są w pełni zdefiniowane.

Bazą do realizacji projektów będą wykwalifikowane kadry. W szczególności powinny obejmować specjalistów z zakresu telekomunikacji oraz IoT, a także psychologów, socjologów i analityków.

Uczestnicy Smart Labu ocenili, że w ramach fazy I możliwe jest zrealizowanie 2 projektów. Projekty te powinny zakończyć się w przeciągu 1 roku. Budżet fazy I oszacowano na 2 mln PLN.

Faza I | **Faza II** | Faza III

Faza II ma połączyć istniejącą wiedzę z tą zdobytą w fazie I, aby stworzyć nowe produkty.

Planowane projekty miałyby obejmować przede wszystkim rozwój:

- Bezpiecznej platformy urządzeń IoT (np. dedykowanej pod urządzenia medyczne).
- Rozwiązań z obszaru bezpiecznej integracji dla protokołów legacy (w urządzeniach już istniejących).
- Bezpieczeństwa bramek, koncentratorów oraz serwerów w kontekście sieci IoT.

Realizacja projektów będzie wymagała m.in. specjalistów z zakresu elektroniki, automatyki, informatyki, cyberbezpieczeństwa (zarówno z przemysłu, jak i świata nauki), urządzeń do testów, wsparcia odbiorców technologii oraz dostępu do technologii wytwarzania prototypowych urządzeń i oprogramowania, w formie infrastruktury lub usług obcych.

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 5 projektów. Projekty te powinny zakończyć się w przeciągu 2 lat. Budżet fazy II oszacowano na 10 mln PLN.

Faza I | Faza II | **Faza III**

Celem fazy III będzie implementacja opracowanych rozwiązań w urządzeniach przeznaczonych na rynek, uruchamianie produkcji systemów, ochrona własności intelektualnej, certyfikacja i szeroko pojęte wdrożenia, którym towarzyszyć powinna promocja. Beneficjentami projektów byliby wszyscy odbiorcy technologii, począwszy od sieci przemysłowych po użytkowników domowych.

W realizację projektów zaangażowane powinny być m.in. takie zasoby jak podwykonawcy produkcyjni, własna infrastruktura produkcyjna, działy programistyczne, działy DevOps, infrastruktura serwerowa i działy QA.

Uczestnicy Smart Labu ocenili, że w ramach fazy III możliwe jest zrealizowanie 20 projektów. Projekty te powinny zakończyć się w przeciągu 2 lat. Budżet fazy III oszacowano na 10 mln PLN.

W ramach działania planowane jest zrealizowanie w okresie 5 lat łącznie 27 projektów z całkowitym budżetem wynoszącym 22 mln PLN. Rozwiązania opracowane w tym działaniu będą miały szereg zalet w kontekście zapewniania bezpieczeństwa sieciom i ich rozbudowy bez generowania podatności.

Działanie 3 - Usługi certyfikacji cyberbezpieczeństwa IoT

Celem trzeciego działania jest stworzenie podstaw pod system certyfikacji urządzeń IoT w kontekście cyberbezpieczeństwa. Mechanizmy certyfikacji urządzeń elektronicznych, takie jak CE albo EMC, mają obecnie charakter deklaratywny, nieweryfikowany w zewnętrznych laboratoriach. Należy jednak podkreślić, że wykazanie niespełnienia norm przy wcześniejszej

deklaracji jest podstawą do nałożenia wysokich kar. W kontekście cyberbezpieczeństwa takie mechanizmy certyfikacyjne nie są popularne. Dlatego uczestnicy SL zaproponowali działanie, w którym wytworzony zostanie cały segment usługowy i certyfikacyjny, dzięki któremu zarówno producenci, jak i odbiorcy, będą mogli rozpoznać produkty o wysokim poziomie bezpieczeństwa.

W wyniku tego działania powinny być zrealizowane dwa cele. Po pierwsze powinien zostać wypracowany standard usługi oraz rekomendacje najlepszych praktyk. Po drugie powinien powstać sektor usług pozwalających firmom sprawdzać sprzęt pod kątem cyberbezpieczeństwa. Potencjalnymi odbiorcami będą zarówno producenci urządzeń IoT, jak i pośrednio ich odbiorcy. Sam system certyfikacji daje też możliwość ekspansji międzynarodowej w drodze do propagowania standardów.

Działanie obejmuje prace we wszystkich 3 fazach:

Faza I | Faza II | Faza III

Faza I ma na celu stworzenie bazy pod segment usługowy. Każdy z realizowanych w jej ramach projektów mógłby odpowiadać na poszczególne elementy procesu certyfikacji. Obejmowałoby to badania podstawowe w zakresie podatności urządzeń, układów mikroelektronicznych i protokołów, opracowanie standardu usługi i dobrych praktyk rynkowych ze wsparciem legislacji oraz zbudowanie systemu oceny jakości usług. W opinii uczestników SL najlepszym sposobem organizacji tych projektów byłoby wyłonienie (np. w drodze konkursu) jednego operatora, który odpowiadałby za integrację projektów i podział środków. W ten sposób wynikiem fazy byłby uporządkowany system certyfikacji bazujący na szeregu interdyscyplinarnych badań.

Bazą do realizacji projektów będą wykwalifikowane kadry. W szczególności powinny obejmować specjalistów z dziedzin pokrewnych cyberbezpieczeństwu.

Uczestnicy Smart Labu ocenili, że w ramach fazy I możliwe jest zrealizowanie 20 projektów. Projekty te powinny zakończyć się w przeciągu 1 roku. Budżet fazy I oszacowano na 4 mln PLN.

Faza I | **Faza II** | Faza III

W fazie II należy skupić się na zaprojektowaniu modelu usługi, wykonaniu prototypu (100% kluczowych funkcjonalności) oraz pilotażowych realizacji. Celem tych projektów byłyby próby certyfikowania różnych docelowych rozwiązań IoT w kontekście cyberbezpieczeństwa. Konieczne byłoby również wytworzenie nowych urządzeń i oprogramowania pozwalającego na analizę podatności i bezpieczeństwa urządzeń IoT. Posiadając prototypy usług certyfikacyjnych przetestowane na „żywym organizmie” będzie można przejść do fazy III działania.

Zasobami potrzebnymi do realizacji fazy II byłyby laboratoria z urządzeniami i sprzętem testowym oraz specjaliści z sektorów przemysłowych, wspierani przez środowisko badawcze.

Uczestnicy Smart Labu ocenili, że w ramach fazy II możliwe jest zrealizowanie 5 projektów. Projekty te powinny zakończyć się w przeciągu 1 roku. Budżet fazy II oszacowano na 10 mln PLN.

Faza I | Faza II | **Faza III**

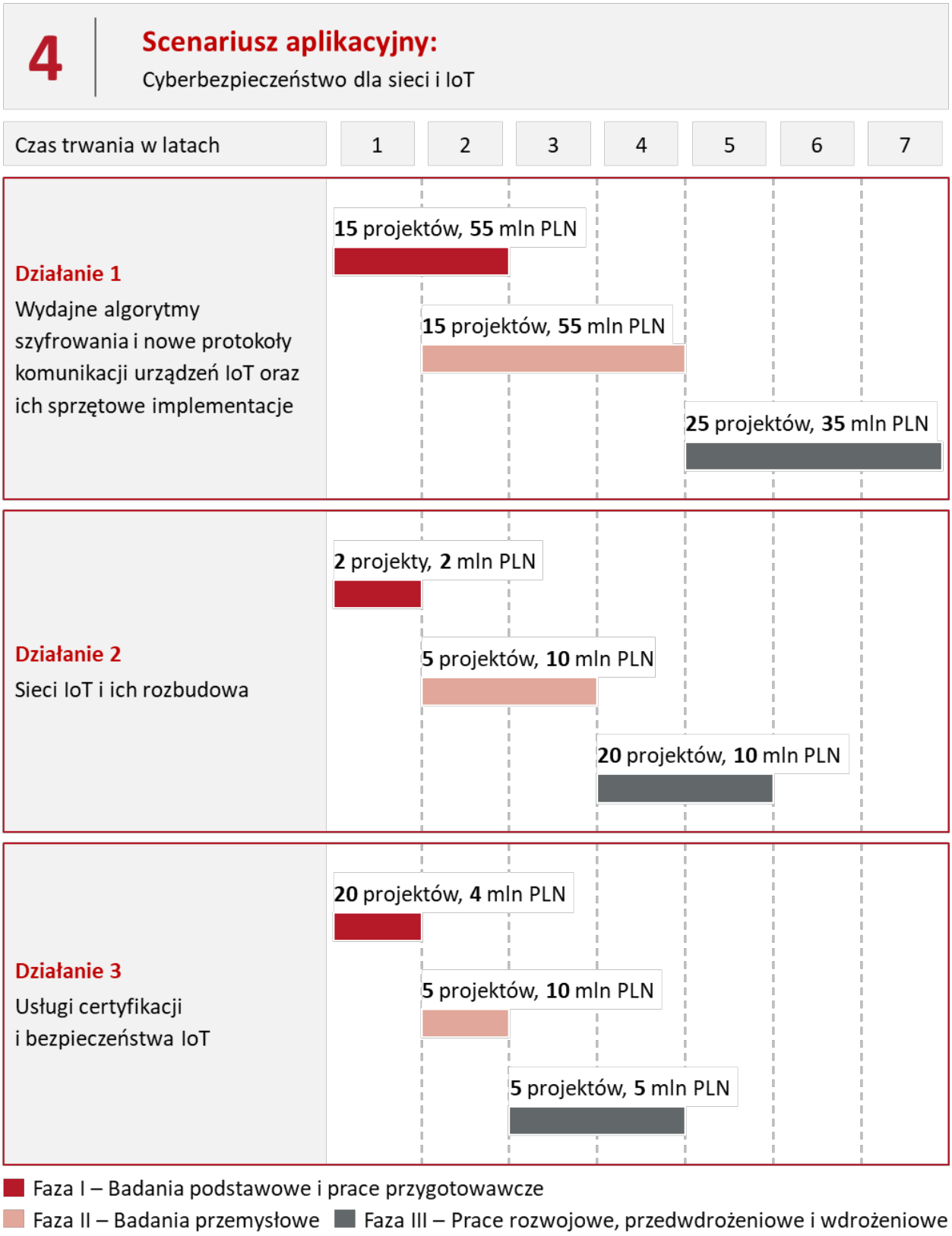
Faza III miałaby na celu wdrożenie usług zgodnie z wypracowanym modelem przez jednostki w różnych obszarach rynku. Można to traktować jako powstanie nowych podmiotów certyfikujących, dla których projekty umożliwiłyby wdrożenie swoich usług. Mogłyby być one umocowane zarówno w jednostkach przemysłowych, jak i badawczych, które wykorzystałyby opracowane w ramach fazy II prototypy do wdrożenia. Możliwe też byłoby zrealizowanie działań promujących certyfikację, zarówno marketingowych, jak i lobbingowych w celu zapewnienia instytucjonalnego wymogu posiadania wybranych certyfikatów.

Zasobami potrzebnymi do realizacji tej fazy byłyby laboratoria z urządzeniami i sprzętem testowym oraz specjaliści z sektorów przemysłowych, wspierani przez środowisko badawcze.

Uczestnicy Smart Labu ocenili, że w ramach fazy III możliwe jest zrealizowanie 5 projektów. Projekty te powinny zakończyć się w przeciągu 2 lat. Budżet fazy III oszacowano na 5 mln PLN.

W ramach działania planowane jest zrealizowanie w okresie 4 lat łącznie 30 projektów z całkowitym budżetem wynoszącym 19 mln PLN. Ostatecznym wynikiem działania 3 byłoby posiadanie na rynku polskim systemu certyfikacji urządzeń IoT pod kątem cyberbezpieczeństwa.

Rysunek 26. Forma graficzna scenariusza 4



Źródło: opracowanie własne

5.2. Mapa drogowa

Mapa technologii w obszarze cyberbezpieczeństwa prezentuje graficznie zagregowane cztery scenariusze rozwoju oraz działania/ projekty B+R, które zostały zdefiniowane i przedyskutowane w ramach cyklu Spotkań Smart Lab z grupą przedstawicieli obszaru cyberbezpieczeństwa w Polsce.

Wypracowane scenariusze zakładają realizację, w okresie najbliższych 7 lat, 838 projektów, których budżety opiewają łącznie na kwotę 1 596 mln PLN.

Rysunek 27. Mapa BTR dla obszaru cyberbezpieczeństwa

Źródło: opracowanie własne

6. Ocena potencjału obszaru cyberbezpieczeństwa w kontekście KIS oraz RIS

Analiza aktualnych dokumentów dot. KIS oraz RIS pozwoliła stwierdzić, że co do zasady konkursy i inicjatywy dedykowane obszarowi cyberbezpieczeństwa powinny być realizowane na poziomie krajowym. Z tego powodu rekomendacje odnośnie zmian zostały poświęcone w pełni Krajowym Inteligentnym Specjalizacjom, tak aby nie wykluczać animatorów rynku z żadnego regionu geograficznego kraju. Poniżej przedstawiono wynikające z przeprowadzonych analiz **rekomendacje zmian w ramach KIS**:

KIS 1. ZDROWE SPOŁECZEŃSTWO
DZIAŁ II – DIAGNOSTYKA I TERAPIA CHORÓB
III. TELEMEDYCYNA

Rekomenduje się modyfikację punktów 1 oraz 2 w następującej formie:

Punkt 1.

- **Aktualne brzmienie:**
  „Tworzenie rozwiązań, technologii, produktów, narzędzi, aplikacji, algorytmów, które poprzez wykorzystanie nowoczesnych technologii informacyjnych i komunikacyjnych, udoskonalą już istniejące, ale przede wszystkim stworzą nowe metody akwizycji, analizy, archiwizacji oraz bezpiecznej wymiany informacji o stanie zdrowia pacjenta zarówno pomiędzy pacjentem, a profesjonalistą branży medycznej („PBM"), jak i grupami profesjonalistów branży medycznej, które to podmioty znajdują się w odległych od siebie geograficznie miejscach. Bezpośrednim celem tworzonych w tym modelu rozwiązań winno być wsparcie procesów diagnostycznych i terapeutycznych związane z bezpieczną transmisją danych i informacji medycznych, poprzez analizę tekstu, dźwięku, obrazu lub innych form niezbędnych do diagnozowania, leczenia i monitorowania pacjentów oraz wymiany informacji pomiędzy PBM lub grupami PBM."

- **Rekomendowane nowe brzmienie:**
  „Tworzenie rozwiązań, technologii, produktów, narzędzi, aplikacji, algorytmów, które poprzez wykorzystanie nowoczesnych technologii informacyjnych i komunikacyjnych, udoskonalą już istniejące, ale przede wszystkim stworzą nowe metody akwizycji, analizy, archiwizacji oraz

bezpiecznej wymiany informacji o stanie zdrowia pacjenta zarówno pomiędzy pacjentem, a profesjonalistą branży medycznej („PBM"), jak i grupami profesjonalistów branży medycznej, które to podmioty znajdują się w odległych od siebie geograficznie miejscach. Bezpośrednim celem tworzonych w tym modelu rozwiązań winno być wsparcie procesów diagnostycznych i terapeutycznych związane z bezpieczną transmisją danych i informacji medycznych, poprzez analizę tekstu, dźwięku, obrazu lub innych form niezbędnych do diagnozowania, leczenia i monitorowania pacjentów oraz wymiany informacji pomiędzy PBM lub grupami PBM. Rozwiązania ICT odpowiadające na te potrzeby powinny charakteryzować się wysokim stopniem zabezpieczeń przed cyberatakami, ze szczególnym uwzględnieniem wieloetapowego uwierzytelniania."

Punkt 2.

- **Aktualne brzmienie:**
  „Opracowanie innowacyjnych rozwiązań opartych o technologie informacyjne i komunikacyjne (ICT) wykorzystywanych jako metody nieinwazyjnego i bezpiecznego gromadzenia i wymiany na odległość informacji o stanie zdrowia pomiędzy systemem opieki zdrowotnej a osobą chorą lub zdrową. Proponowane rozwiązania powinny mieć zastosowanie w: diagnostyce; terapii, w tym zabiegach inwazyjnych wykonywanych na odległość; profilaktyce; rehabilitacji medycznej; opiece skoordynowanej; monitorowaniu stanu zdrowia przy pomocy urządzeń, czujników i akcesoriów; rejestracji i analizie sygnałów biologicznych o istotnym znaczeniu dla zdrowia; poprawie przestrzegania zaleceń, w tym trzymania się planu terapeutycznego; rehabilitacji pozabiegowej i pourazowej; rekreacyjnej aktywności fizycznej; edukacji chorych i zdrowych z promowaniem prozdrowotnych zachowań; poprawie jakości życia chorych i/ lub osób w trakcie diagnozy; profesjonalnym kształceniu pracowników opieki medycznej; tworzeniu dużych baz danych medycznych; integracji i unifikacji rozproszonych systemów danych zdrowotnych z systemami Elektronicznych Danych Medycznych. Ważnym celem innowacyjnych działań w zakresie telemedycyny winno być opracowanie i wykorzystanie rozwiązań ICT i wyrobów medycznych pomagających obniżyć koszty opieki zdrowotnej i/ lub poprawić jakość udzielanych świadczeń i/lub wyrównać różnice oraz ułatwić i skrócić dostęp do systemu opieki zdrowotnej i/lub zapewnić bezpieczeństwo zdrowotne osobom w wieku podeszłym, z przewlekłymi chorobami i inwalidztwem oraz wygodę i prostotę ich stosowania przez końcowych użytkowników."

- **Rekomendowane nowe brzmienie:**
  „Opracowanie innowacyjnych rozwiązań opartych o technologie informacyjne i komunikacyjne (ICT) wykorzystywanych jako metody nieinwazyjnego i bezpiecznego gromadzenia i wymiany na odległość informacji o stanie zdrowia pomiędzy systemem opieki zdrowotnej a osobą chorą lub zdrową. Proponowane rozwiązania powinny mieć zastosowanie w: diagnostyce; terapii, w tym zabiegach inwazyjnych wykonywanych na odległość; profilaktyce; rehabilitacji medycznej; opiece skoordynowanej; monitorowaniu stanu zdrowia przy pomocy urządzeń, czujników i akcesoriów; rejestracji i analizie sygnałów biologicznych o istotnym znaczeniu dla zdrowia; poprawie przestrzegania zaleceń, w tym trzymania się planu terapeutycznego;

rehabilitacji pozabiegowej i pourazowej; rekreacyjnej aktywności fizycznej; edukacji chorych i zdrowych z promowaniem prozdrowotnych zachowań; poprawie jakości życia chorych i/ lub osób w trakcie diagnozy; profesjonalnym kształceniu pracowników opieki medycznej; tworzeniu dużych baz danych medycznych; integracji i unifikacji rozproszonych systemów danych zdrowotnych z systemami Elektronicznych Danych Medycznych. Ważnym celem innowacyjnych działań w zakresie telemedycyny winno być opracowanie i wykorzystanie rozwiązań ICT i wyrobów medycznych pomagających obniżyć koszty opieki zdrowotnej i/ lub poprawić jakość udzielanych świadczeń i/lub wyrównać różnice oraz ułatwić i skrócić dostęp do systemu opieki zdrowotnej i/lub zapewnić bezpieczeństwo zdrowotne osobom w wieku podeszłym, z przewlekłymi chorobami i inwalidztwem oraz wygodę i prostotę ich stosowania przez końcowych użytkowników. Rozwiązania ICT odpowiadające na te potrzeby powinny charakteryzować się wysokim stopniem zabezpieczeń przed cyberatakami, ze szczególnym uwzględnieniem wieloetapowego uwierzytelniania."

KIS 9. ELEKTRONIKA I FOTONIKA,
DZIAŁ VII. ZAGADNIENIA APLIKACYNE

Rekomenduje się rozszerzenie listy zagadnień o nowy punkt:

Punkt 17.

- **Rekomendowane dodanie punktu:**
  „Cyberbezpieczeństwo sieci sensorowych."

Wynika to z faktu, że sieci sensorowe są niezwykle ważnym i silnie rozwijanym obszarem, którego potencjał aplikacyjny jest nieograniczony. Jednocześnie stają się one potencjalnym celem ataków, które mogą mieć na celu kradzież informacji, zaburzenie łańcuchów dostaw, a nawet ataki przeciw ludziom (sieci sensorów medycznych). Rozwój cyberbezpieczeństwa w tym obszarze wynika w naturalny sposób z ustaleń SL.

KIS 10. INTELIGENTNE SIECI I TECHNOLOGIE INFORMACYJNOKOMUNIKACYJNE ORAZ GEOINFORMACYJNE, DZIAŁ I. TECHNOLOGIE INTERNETU PRZYSZŁOŚCI, TECHNOLOGIE INTERNETU RZECZY, SYSTEMY WBUDOWANE

Rekomenduje się rozszerzenie listy zagadnień o dwa nowe punkty:

Punkt 8.

- **Rekomendowane dodanie punktu**:
  „Cyberbezpieczeństwo sieci."

Punkt 9.

- **Rekomendowane dodanie punktu:**
  „Cyberbezpieczeństwo urządzeń Internetu Rzeczy."

W świetle wzrostu popularności rozwiązań sieciowych, sieci 5G i masowości urządzeń IoT włączenie tych zagadnień do KIS jest bardzo potrzebne, a funkcjonowanie jedynie wydzielonego obszaru cyberbezpieczeństwa jest niewystarczające w kontekście potrzeby specjalizacji powstających technologii.

KIS 10. INTELIGENTNE SIECI I TECHNOLOGIE INFORMACYJNOKOMUNIKACYJNE ORAZ GEOINFORMACYJNE,
DZIAŁ IV. ZARZĄDZANIE INFORMACJĄ W INTELIGENTNYCH SIECIACH

Rekomenduje się rozszerzenie listy zagadnień o nowy punkt:

Punkt 14.

- **Rekomendowane dodanie punktu:**
  „Bezpieczne mechanizmy uwierzytelniania."

Obszar zidentyfikowany w jednym ze scenariuszy opracowanych w ramach warsztatów Smart Lab. Uwierzytelnianie, zwłaszcza wieloetapowe, stanowi kluczowy element ochrony danych i zarządzania nimi, jak również jest wymagane przez unijne regulacje.

KIS 12. AUTOMATYZACJA I ROBOTYKA PROCESÓW TECHNOLOGICZNYCH,
DZIAŁ I. PROJEKTOWANIE I OPTYMALIZACJA PROCESÓW

Rekomenduje się rozszerzenie listy zagadnień o nowy punkt:

Punkt 7.

- **Rekomendowane dodanie punktu:**
  „Systemy cyberbezpieczeństwa procesów."

Rekomendacja ta wynika bezpośrednio z wniosków, jakie pojawiły się po warsztatach Smart Lab oraz z projektów planowanych do realizacji w ramach jednego ze scenariuszy.

KIS 13. INTELIGENTNE TECHNOLOGIE KREACYJNE,
DZIAŁ II. GRY

Rekomenduje się rozszerzenie listy zagadnień o nowy punkt:

Punkt 7.

- **Rekomendowane dodanie punktu:**
  „Cyberbezpieczeństwo w grach."

Obszar ten powinien uwzględniać uwierzytelnianie w grach komputerowych, bezpieczeństwo danych graczy oraz bezpieczeństwo płatności w mikro transakcjach.

7. Wnioski i rekomendacje

Cyberbezpieczeństwo to niezwykle interdyscyplinarny obszar technologiczny, którego produkty i usługi wykorzystywane są w niemalże wszystkich sektorach gospodarki. Z uwagi na tak rozpowszechnioną obecność rozwiązań z zakresu bezpieczeństwa IT i różne warunki kształtujące każdy z takich obszarów wdrożeniowych, niemożliwe jest wysnucie wniosków kompleksowo dla każdego z nich – szczególnie, że rosnąca popularność Internetu w życiu społecznym i procesach biznesowych powoduje nieustanne pojawianie się nowych nisz gospodarczych zainteresowanych wdrożeniami z obszaru cyberbezpieczeństwa. Z tego powodu zdecydowano się na uproszczenie, polegające na wyciąganiu wniosków horyzontalnych, dotyczących całej branży. Efektem tego podejścia są poniższe wnioski i rekomendacje, które powstały na bazie wiedzy pozyskanej od uczestników warsztatów Smart Lab oraz wiedzy eksperckiej autorów niniejszego dokumentu. Wdrożenie niżej wymienionych rekomendacji powinno przyczynić się do rozwoju obszaru cyberbezpieczeństwa w Polsce.

Pierwsza rekomendacja, o charakterze horyzontalnym, wynikająca bezpośrednio z dyskusji prowadzonych podczas warsztatów Smart Lab oraz przeprowadzonych analiz krajowego rynku przez ekspertów przygotowujących Ekspertyzę BTR, dotyczy **uruchomienia dedykowanych programów wsparcia skupionych wokół projektów, technologii i produktów wymienionych w Scenariuszach Rozwoju**, wskazanych i opisanych w rozdziale 5.1. Programy te powinny mieć charakter ogólnokrajowy i powinny być dostępne dla każdego rodzaju podmiotu – za podjęciem takich działań wypowiadała się zdecydowana większość uczestników warsztatów Smart Lab, którzy reprezentowali różne regiony geograficzne kraju oraz znajdowali się na różnym etapie rozwoju własnych organizacji (od startupów, po średnie przedsiębiorstwa i korporacje). Do głównych obszarów wsparcia, które powinny być objęte takimi programami należą:

- **Procesy przedwdrożeniowe i komercjalizacyjne** – szczególnie dużą bolączką dla przedsiębiorców starających się doprowadzić do pierwszych wdrożeń nowych rozwiązań z obszaru cyberbezpieczeństwa jest ich wysoki poziom kapitałochłonności dla klientów, którzy (z uwagi na brak odpowiednich regulacji czy standardów rynkowych) traktują profesjonalne produkty i usługi z zakresu bezpieczeństwa IT jako inwestycje typu „nice-to-have”, a nie „must-to-have”. Wsparcie w formie dotacji, dofinansowania czy ulgi podatkowej dla biznesowych klientów w sektorze cyberbezpieczeństwa zwiększyłoby nie tylko popyt na bardziej zaawansowane rozwiązania, ale również świadomość klientów jak bardzo uproszczone (i niebezpieczne) były dotychczas wykorzystywane przez nich rozwiązania.

- **Działalność B+R i innowacyjna** – wsparcie w zakresie prac B+R, w szczególności w fazie badań przemysłowych i prac rozwojowych, które zachęciłoby przedsiębiorców do realizacji projektów wysokiego ryzyka w obszarze cyberbezpieczeństwa i próby realizacji i komercjalizacji innowacyjnych produktów i technologii (które finalnie mogłyby przyczynić się do rozwoju krajowego rynku i jego ekspozycji na arenie międzynarodowej). W ramach fazy prac rozwojowych warto też zaplanować możliwość dofinansowania kosztów ochrony IP – np. przy programach pomocowych zagadnienie to powinno być przedstawiane przez wnioskodawców na etapie składania wniosków o dofinansowanie w formie wyników analizy czy efekty produktów prac B+R będą możliwe do ochrony w formie np. patentów albo dlaczego taka ochrona nie jest opłacalna w konkretnym przypadku. Inwestowanie w cyberbezpieczeństwo powinno być również dodatkowo premiowane, szczególnie w przypadku tych przedsiębiorstw, które wcześniej ograniczały się jedynie do tradycyjnych, mało skutecznych rozwiązań. Podstawową formą zachęty, np. dla przedsiębiorstw z sektora MŚP, mogłyby być mechanizmy fiskalne, w tym odpisy podatkowe i dopłaty inwestycyjne oraz nieodpłatne wsparcie we wdrażaniu innowacyjnych rozwiązań związanych z cyberbezpieczeństwem.
- **Działalność marketingowa** – polskie MŚP odczuwają na rynku efekt faworyzowania dostawców korporacyjnych przez podmioty publiczne i większość klientów biznesowych, w szczególności w odniesieniu do ich międzynarodowego doświadczenia – które może, ale nie musi warunkować wyższej jakości samego produktu lub usługi. Rekomendowane jest rozważenie uruchomienia programu, który umożliwiłby przedsiębiorcom z sektora MŚP zwiększenie wydatków na promocję w mediach branżowych, krajowych targach i konferencjach oraz intensyfikować wydatki na pozycjonowanie w Internecie.
- **Internacjonalizacja działalności** – z uwagi na zidentyfikowane trudności w samodzielnym prowadzeniu przez przedsiębiorców działań z zakresu ekspansji zagranicznej, rekomendowane jest wsparcie wprowadzania polskich rozwiązań na rynki zagraniczne, w tym dofinansowanie stoisk/ uczestnictwa w branżowych targach i konferencjach, organizacji wizyt handlowych oraz działalności marketingowej nakierowanej na nowe rynki docelowe. Rekomendowane jest rozważenie uruchomienia takiego programu dedykowanego obszarowi cyberbezpieczeństwa, aby zwiększyć jego efektywność w kontekście całej branży i ograniczyć konieczność rywalizacji w procesie naboru wniosków z przedstawicielami innych, mniej strategicznych branż w znaczeniu wpływu na gospodarkę i życie społeczne.

Jedną z kluczowych barier rozwoju polskiego rynku cyberbezpieczeństwa jest niski poziom świadomości przedsiębiorców i społeczeństwa odnośnie zagrożeń czyhających w sferze wirtualnej oraz możliwych sposobów zabezpieczania się przed nimi. Z tego powodu rekomendowane jest wsparcie rynku poprzez **inicjowanie programów społecznych nakierowanych na edukację rynku**, zarówno w odniesieniu do odbiorców indywidualnych, jak i podmiotów komercyjnych (przedsiębiorców, szczególnie z sektora MŚP). Takie programy społeczne powinny docelowo:

- Poszerzyć wiedzę klientów końcowych, pośredników i wszelkich innych uczestników rynku na temat zagrożeń wynikających z cyberataków oraz potrzebnego zakresu i dostępnych sposobów ochrony.
- Zmienić nastawienie społeczne do bezpieczeństwa w Internecie i uczynić wiedzę o cyberbezpieczeństwie jednym z fundamentów przekazu społecznego.
- Zmienić wizerunek cyberbezpieczeństwa z „jednorazowej inwestycji" na „obszar ciągłego rozwoju", w szczególności w sektorze MŚP, gdyż jedynie takie podejście pozwala utrzymać wysoki poziom skuteczności wykorzystywanych produktów.
- Zmienić sposób postrzegania usług z zakresu cyberbezpieczeństwa wśród podmiotów z sektora MŚP – aby kompleksowe wsparcie w formie outsourcingu procesów bezpieczeństwa IT nie było kojarzone z „informacjami wychodzącymi poza przedsiębiorstwo".

  Wsparciem dla takich programów społecznych mogłyby być ogólnopolskie konferencje z udziałem międzynarodowych podmiotów i gremiów decyzyjnych w obszarze cyberbezpieczeństwa oraz wydarzenia typu „hackaton" dla programistów, a w szczególności tych na początku swojej kariery, decydujących o specjalizacji i ciągle mogących poświęcić się tematowi cyberbezpieczeństwa.

Polscy przedsiębiorcy z obszaru cyberbezpieczeństwa mają szczególny problem z internacjonalizacją swojej działalności – oprócz programów dotacyjnych czy dofinansowań, rekomendowane jest zainicjowanie działań horyzontalnych polegających na **promocji polskich technologii z zakresu cyberbezpieczeństwa na arenie międzynarodowej**.

Jedną z kluczowych konkluzji w ramach warsztatu podsumowującego cały cykl spotkań Smart Lab był brak ogólnokrajowych standardów bezpieczeństwa, które dotyczyłyby całego rynku – z tego powodu rekomenduje się **zainicjowanie prac nad wdrożeniem standardów bezpieczeństwa IT**, obejmujących zarówno podmioty świadczące usługi lub oferujące produkty w sferze wirtualnej, jak i podmiotów jedynie przetwarzających w niej dane lub digitalizujące wewnętrzne procesy. Standardy te powinny cechować się jednocześnie wysokim stopniem elastyczności, tak aby mogły podążać za rozwojem technologicznym i aby spełnianie standardów zawsze gwarantowało dostateczny poziom bezpieczeństwa.

Ważnym czynnikiem negatywnie wpływającym na możliwości dynamicznego rozwoju branży cyberbezpieczeństwa w Polsce są poważne braki kadrowe oraz nadmierny „odpływ specjalistów". Z tego powodu rekomenduje się, aby polskie uczelnie, w szczególności techniczne, rozważyły **utworzenie nowych kierunków edukacyjnych dedykowanych cyberbezpieczeństwu** lub **dofinansowanie szkoleń wspierających proces przebranżowienia ekspertów** z innych obszarów gospodarczych. Obecnie braki kadrowe odczuwalne są u niemalże wszystkich rodzajów animatorów rynku (od przedsiębiorców, po jednostki naukowe i instytucje otoczenia biznesu), a najbardziej perspektywiczne zasoby ludzkie często decydują się rozwijać swoją karierę poza granicami kraju.

Dla wielu przedsiębiorstw z sektora MŚP, a szczególnie tych najmniejszych, uczestnictwo w programach dotacyjnych jest dużym obciążeniem administracyjnym, które często skłania firmy do ograniczania albo wręcz nie korzystania z tego rodzaju wsparcia. Do rozważenia jest zatem **uproszczenie procedur formalnych w programach dotacyjnych**, w aspektach które nie są ograniczone wymaganiami instytucji nadrzędnych względem polskich instytucji dystrybucyjnych środki pomocowe. Należy jednak pamiętać, że duża część stosowanych procedur jest przełożeniem formalnych wymagań nakładanych na krajowe jednostki odgórnie, a przez to na które nie mają one żadnego wpływu.

Polskie przedsiębiorstwa posiadają na ogół niewielkie doświadczenie w zakresie ochrony własności intelektualnej. Odnośnie samej tematyki ochrony patentowej funkcjonuje na rynku również dużo niejasności i mitów. Potencjalnie rozwiązaniem dla takiego stanu rzeczy może być **dofinansowywanie specjalistów w zakresie IP**, którzy będą nie tylko uświadamiać animatorów rynku o zaletach różnych form ochrony własności intelektualnej, ale również będą mieli za zadanie doradzać jakiego typu produkty/ procesy powinny być w konkretnym przedsiębiorstwie dodatkowo chronione. Potencjalnie takie funkcje mogłyby też być finansowane w jednostkach naukowych/ badawczych lub IOB, które pomagałyby również rozwijać współpracę między firmami i jednostkami badawczymi na wczesnych etapach rozwoju danej technologii.

Branża cyberbezpieczeństwa w Polsce cechuje się szczególnie niskim poziomem sieciowości jak na jeden z kluczowych (w kontekście bezpieczeństwa państwa) sektorów gospodarczych. Z tego powodu duża część animatorów rynku nie jest świadoma jakie technologie rozwijane są w ich najbliższym otoczeniu i nie ma możliwości nawiązania relacji, które mogłyby spowodować zawiązanie współpracy czy ramowego partnerstwa w obszarze prac B+R. Z tego powodu rekomenduje się **wsparcie rynku w zakresie tworzenia nowych klastrów (i innych inicjatyw networkingowych) lub promowania obecnych**, tak aby umożliwić animatorom rynku swobodną wymianę wiedzy, transfer technologii i korzystanie z pozytywnych efektów kooperacji.

8. Metodyka

Ekspertyza Business Technology Roadmap dla obszaru cyberbezpieczeństwa została sporządzona w ramach projektu pozakonkursowego pn. Monitoring Krajowej Inteligentnej Specjalizacji, który realizowany jest przez Ministerstwo Rozwoju i Technologii oraz Polską Agencję Rozwoju Przedsiębiorczości.

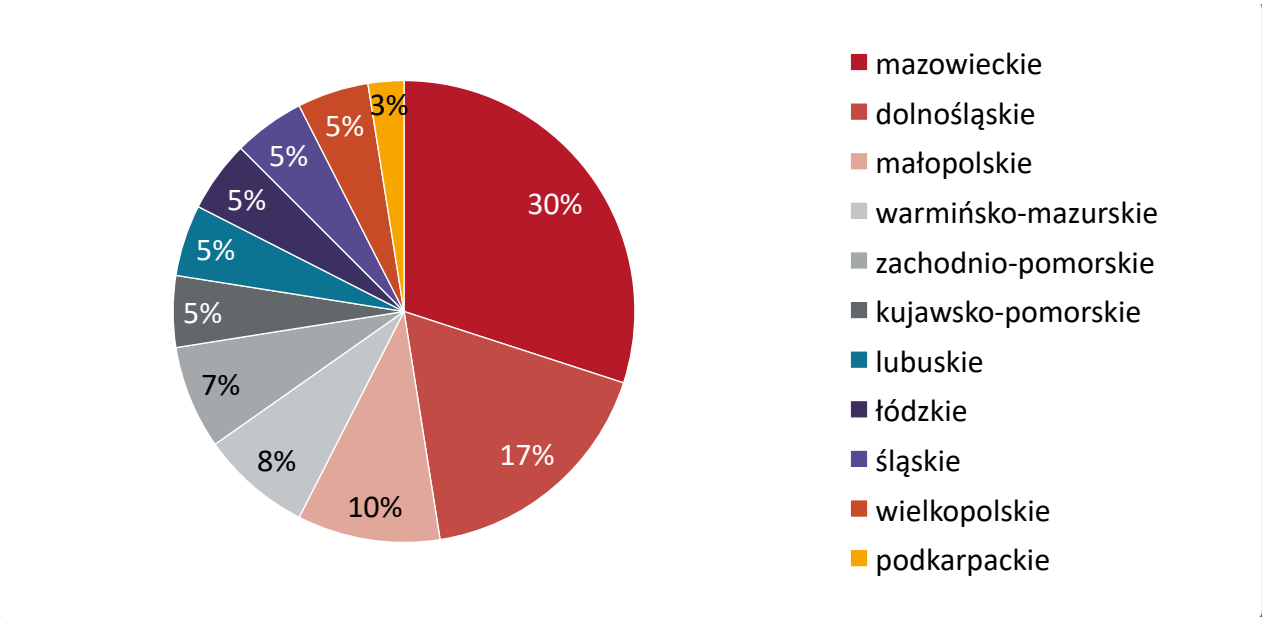
Krajowe Inteligentne Specjalizacje są dokumentem strategicznym, określającym priorytetowe kierunki rozwoju technologii w Polsce, które stanowić mogą nisze technologiczne będące przewagą konkurencyjną polskich przedsiębiorstw.

Proces monitoringu Krajowej Inteligentnej Specjalizacji realizowany jest w ramach metodologii określanej mianem Procesu Przedsiębiorczego Odkrywania (PPO). Zakłada ona wypracowywanie wniosków, spostrzeżeń i rekomendacji dotyczących konkretnych działań technologicznych niezbędnych do rozwoju danego obszaru technologicznego podczas dedykowanych warsztatów Smart Lab, w których uczestniczą przedstawiciele przedsiębiorstw, jednostek naukowych/ badawczych oraz Instytucji Otoczenia Biznesu, a także, w roli obserwatorów, reprezentanci jednostek administracji publicznej i instytucji dystrybuujących środki unijne.

W efekcie zrealizowanego projektu, istnieje możliwość aktualizacji Krajowych Inteligentnych Specjalizacji lub Regionalnych Inteligentnych Specjalizacji o nowe obszary, co może stanowić podstawę dla instytucji publicznych do planowania zakresu merytorycznego i budżetu nowych lub zaktualizowanych instrumentów wsparcia.

Ekspertyza BTR dla obszaru cyberbezpieczeństwa została przygotowana przy współudziale naukowców i przedsiębiorców funkcjonujących w różnych sektorach rynku i pracujących zarówno nad produktami dla klientów detalicznych, jak i tych biznesowych. W efekcie ich rozwiązania wpisują się w różne branże, od sektora usługowego po przemysł i infrastrukturę krytyczną. Właśnie z uwagi na interdyscyplinarny charakter całego obszaru, szczególną uwagę poświęcono różnorodności uczestników warsztatów Smart Lab – celowo reprezentowali oni różne typy podmiotów, o różnej wielkości oraz pochodzili z różnych regionów kraju. Rysunek 28 prezentuje strukturę uczestników w podziale na województwa.

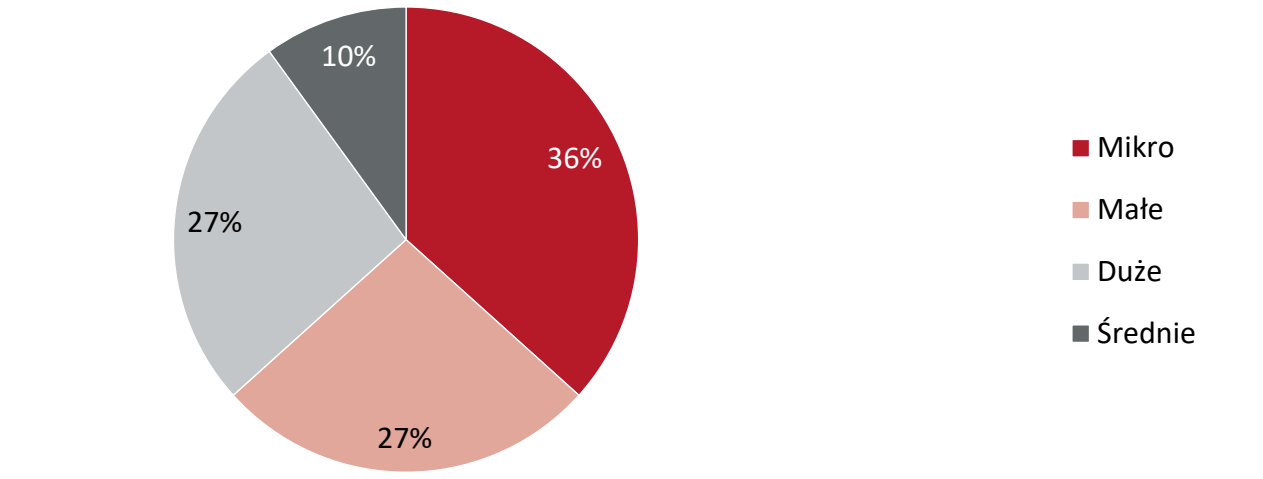
Rysunek 28. Struktura uczestników spotkań Smart Lab w obszarze cyberbezpieczeństwa w podziale na województwa



Źródło: opracowanie własne

Rysunek 29 prezentuje strukturę uczestników w podziale na wielkość przedsiębiorstwa.

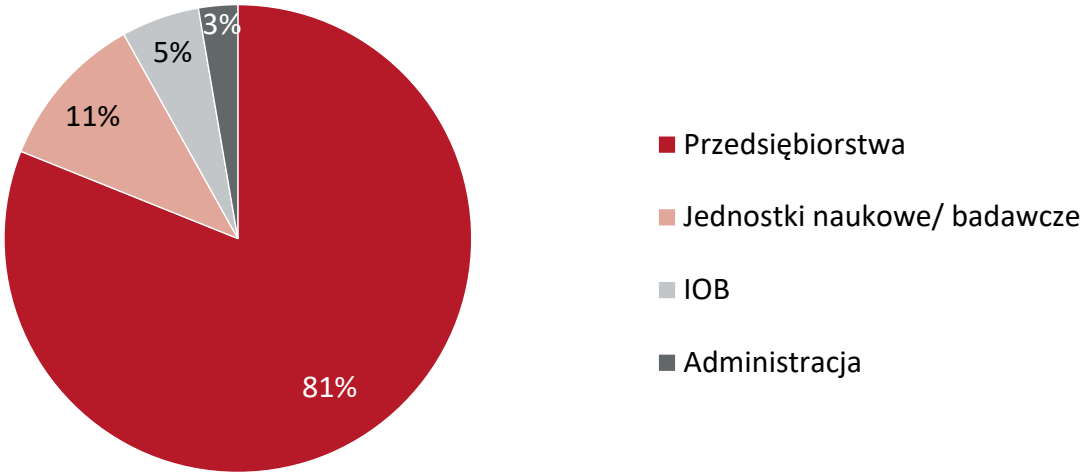
Rysunek 29. Struktura uczestników spotkań Smart Lab w obszarze cyberbezpieczeństwa w podziale na wielkość przedsiębiorstwa



Źródło: opracowanie własne

Rysunek 30 prezentuje strukturę uczestników w podziale na typ podmiotu.

Rysunek 30. Struktura uczestników spotkań Smart Lab w obszarze cyberbezpieczeństwa w podziale na typ podmiotu



Źródło: opracowanie własne

Kluczowe elementy i treści ekspertyzy BTR zostały wypracowane kolektywnie przez wszystkich uczestników spotkań SL, pod nadzorem merytorycznym dr. hab. inż. Jerzego Baranowskiego oraz przy współudziale zespołu ekspertów PwC.

Cztery spotkania SL realizowane były w formule zdalnej w dniach od 01.09.2021 r. do 05.10.2021 r. Podczas spotkań uczestnicy pracowali zarówno samodzielnie, jak i w grupach, korzystając przy tym z różnych narzędzi IT, od systemów konferencyjnych po platformy kolaboracyjne z edytowalnymi na żywo współdzielonymi planszami i interaktywnymi ćwiczeniami. Za ich pośrednictwem uczestnicy pracowali m.in. nad określeniem:

- Scenariuszy rozwoju obszaru cyberbezpieczeństwa.
- Silnych i słabych stron obszaru cyberbezpieczeństwa w Polsce.
- Trendów rynkowych wpływających na funkcjonowanie animatorów rynku cyberbezpieczeństwa w Polsce.
- Barier utrudniających funkcjonowanie i rozwój obszaru cyberbezpieczeństwa w Polsce.
- Czynników wyznaczających granice funkcjonowania obszaru cyberbezpieczeństwa w odniesieniu do aspektów politycznych, ekonomicznych, prawnych, społecznych, technologicznych oraz środowiskowych.
- Najważniejszych oraz najbardziej atrakcyjnych krajowych i międzynarodowych wydarzeń targowych, konferencji, sympozjów skupionych wokół obszaru cyberbezpieczeństwa.

- Potencjału obszaru cyberbezpieczeństwa w kontekście KIS i RIS.
- Rekomendacji w zakresie dostosowania różnorodnych praktyk czy polityk, które docelowo mają zwiększyć efektywność funkcjonowania obszaru cyberbezpieczeństwa w Polsce.

Gotowość uczestników spotkań do dzielenia się swoją wiedzę, doświadczeniem, dobrymi praktykami oraz przede wszystkim planami biznesowymi zaowocowała stworzeniem listy działań, które nakreślają zakres merytoryczny planowanych przez nich do realizacji w najbliższych latach, ambitnych projektów badawczo-rozwojowych w obszarze Cyberbezpieczeństwa. Działania te zostały finalnie zintegrowane w ramach czterech tzw. Scenariuszy Rozwoju, które stanowiły podstawę do opracowania mapy graficznej BTR.

Spotkania Smart Lab prowadzone były w sposób warsztatowy, mający na celu zapewnienie jak największej zgodności ze zwinnymi metodykami zarządzania projektami. Jednocześnie wiele starań przykładanych było do zapewnienia możliwie najbardziej indywidualnego podejścia do każdego z uczestników, aby zapewnić, że dokument w sposób wiarygodny odzwierciedla wszelkie kwestie poruszane przez uczestników spotkań. Również poza samymi spotkaniami zespół ekspertów realizujący projekt przeprowadził wiele rozmów telefonicznych i konwersacji email z uczestnikami, aby na bieżąco zaspokajać najbardziej naglące i dyskusyjne kwestie. W efekcie wypracowane przez uczestników materiały tworzone były przyrostowo i ulegały licznym zmianom. Ekspertyza BTR jest więc żywym dokumentem, który iteracyjnie wyewoluował do formy jaka prezentowana jest obecnie. Uproszczony schemat prezentujący metodykę prac nad BTR dla obszaru cyberbezpieczeństwa został zaprezentowany na Rysunku 31.

Rysunek 31. Uproszczona metodyka prac nad BTR dla obszaru cyberbezpieczeństwa

Źródło: opracowanie własne

9. Słownik pojęć/ wykaz skrótów

- **Adres IP** (*Internet Protocol Adress*, z ang. Adres protokołu internetowego) - niepowtarzalny adres sieci urządzeń, najczęściej pojedynczego urządzenia lub sieci WiFi.
- **AI** (*Artificial Intelligence*, z ang. Sztuczna inteligencja) - oprogramowanie stale uczące się akcji zachodzących w systemach i sieciach, ćwiczące analityczne „myślenie" w ich kierunku.
- **APT** (*Advanced Persistent Threat*, z ang. Zaawansowane ciągłe zagrożenie) - zaawansowane technologicznie zagrożenie o charakterze ciągłym, najczęściej umotywowane politycznie lub gospodarczo i związane z rządami krajów wrogich.
- **ARPA** (od 1996 DARPA: *Defence Advanced Research Projects Agency*, z ang. Agencja Obronnych Zaawansowanych Projektów Badawczych) - wydział amerykańskiego departamentu obrony, którego zadaniem jest opracowywanie technologii dla armii USA.
- **ARPANET** - system łączący komputery w sieci, utworzony w czasie Zimnej Wojny przez armię USA na własne potrzeby.
- **ASIC** (*Application-Specific Integrated Circuit*, z ang. Specjalizowany układ scalony) - układ zaprojektowany do realizacji z góry określonego zadania. Cechą szczególną ASIC jest zastępowalność układów ogólnego przeznaczenia, przez co jest tańszy, szybszy, efektywniejszy i zużywa mniej energii.
- **B+R** (Badania i Rozwój) - Badania i Rozwój, Prace Badawczo-Rozwojowe.
- **B+R+I** (Badania, Rozwój i Innowacje) - prace obejmujące badania, rozwój i innowacje.
- **Backoffice** - część organizacji odpowiadająca za jej prawidłowe funkcjonowanie (nie współpracująca z klientem), często nazywana „administracyjną".
- **Blockchain** - jedna z technologii rozproszonego rejestru (DLT), działająca na zasadzie współużytkowanego i niezmienialnego rejestru, który upraszcza proces zapisywania i śledzenia zasobów w sieci. Blockchain wykorzystywany jest przede wszystkim w procesach transakcyjnych i stał się podstawą kryptowalut.
- **Bootloader** - program odpowiedzialny za uruchomienie systemu operacyjnego w komputerze.
- **BTR** (*Business Technology Roadmap*, z ang. Mapa Rozwoju Technologii) - opracowanie zawierające opis sytuacji technologiczno-rynkowej wraz z mapą rozwoju technologii i planowanymi projektami B+R w danej dziedzinie.

- **CAGR** (*Compund Annual Growth Rate*, z ang. Skumulowany roczny wskaźnik wzrostu) - wskaźnik wykorzystywany do obliczeń średniego rocznego wzrostu danej wielkości w badanym okresie.
- **Captcha** - narzędzie służące do rozpoznawania czy użytkownik, chcący uzyskać dostęp do strony internetowej jest fizycznym człowiekiem, czy oprogramowaniem udającym człowieka. Sprawdza umiejętność czytania tekstu nieujętego w znane czcionki.
- **CC** (*Common Criteria*, z ang. Wspólne kryteria) - międzynarodowo uznawany system certyfikacji, oznaczany charakterystycznym logo.
- **Chromebook** - laptop produkcji firmy Google, oparty na jej oprogramowaniu.
- **CSaaS** (*Cybersecurity-as-a-service*, z ang. Cyberbezpieczeństwo jako usługa) - model oferowania cyberbezpieczeństwa w formie usług, często kompleksowych, opartych o konkretne oprogramowania/systemy/czynności outsourcingowe.
- **CSO** (*Chief Security Officer*, z ang. Szef działu bezpieczeństwa IT) - skrót wykorzystywany głównie w krajach anglojęzycznych oraz na arenie międzynarodowej.
- **Cybersecurity-on-chip** (z ang. Cyberbezpieczeństwo w chipie) - podzespół z wbudowanymi mechanizmami obrony.
- **DDoS** (*Distributed denial of service*, z ang. Rozproszona odmowa usługi) - przychodzący z wielu kierunków atak na sieć ofiary, powodujący przeciążenie jej mocy przerobowych i odbierający możliwość wykonania jakiegokolwiek pożądanego działania.
- **DevOps** - zbiór rozwiązań pozwalających na skrócenie czasu tworzenia nowych wersji systemów informatycznych.
- **DLT** (*Distributed Ledger Technology*) - zdecentralizowana baza danych.
- **Dongle** - rodzaj przejściówki kablowej.
- **DOS** (*Disk Operating System*, z ang. Dyskowy system operacyjny) - pierwszy przenośny system operacyjny w mikrokomputerach, powstały w latach 80 XX wieku.
- **eCommerce** - handel internetowy.
- **eHealth** - usługi dotyczące ochrony zdrowia, udzielane za pośrednictwem Internetu.
- **eIDAS** (*Electronic IDentification, Authentication and Trust Services*, z ang. Elektroniczna identyfikacja, uwierzytelnianie i usługi zaufania) - regulacja Unii Europejskiej, określająca wymagania dotyczące autoryzacji w systemach komputerowych.
- **EMAG** - Instytut Technik Innowacyjnych Oddział w Białymstoku.
- **EMC** - system certyfikacji obowiązkowy na rynkach większości krajów rozwiniętych.
- **ePUAP** - rządowa platforma dostępu obywatelskiego.

- **ESD** (*Earth Sciences Division*, z ang. Wydział nauk o ziemi) - program amerykańskiej agencji kosmicznej NASA, mający na celu mapowanie powierzchni kuli ziemskiej.
- **Ethernet** - sieć połączonych przewodami komputerów.
- **Fintech** (*Financial Technology*, z ang. Technologia finansowa) - technologie komputerowe, stosowane w organizacjach związanych ze światem finansów.
- **Firewall** - system ochrony sieci, broniący jej przed nieautoryzowanym logowaniem i przesyłem nieautoryzowanych danych.
- **FPGA** (*Field Programable Gate Array*, z ang. Programowalna macierz bramek) - jeden z rodzajów programowalnego układu logicznego, którego cechą szczególną jest możliwość wielokrotnego programowania bez demontażu.
- **Haker** - termin określający osobę wyszukującą i intencjonalnie wykorzystującą luki w zabezpieczeniach oprogramowania, głównie w celu kradzieży lub modyfikacji danych.
- **Hakowanie/ hacking** - czynność intencjonalnego łamania zabezpieczeń oprogramowania pochodząca od terminu „haker".
- **Hardware** - fizyczny sprzęt komputerowy.
- **HMI/ HIS** (*Human-Machine Interface/ Human Interface System*, z ang. Interfejs człowiek-maszyna) - urządzenie/ system umożliwiające komunikację między człowiekiem a innymi urządzeniami.
- **Hyperlink** - termin określający interaktywną frazę, której aktywacja (poprzez np. kliknięcie) powoduje otworzenie powiązanej z nią witryny internetowej.
- **ICS** (*Industrial Control System*, z ang. Przemysłowy system sterowania) - termin opisujący rozmaite systemy kontroli i sterowania w ramach zakładów przemysłowych.
- **ICT** (*Information and Communications Technology*) - technologie informacyjno-komunikacyjne/ teleinformatyczne.
- **ID(P)S** (*Intrusion Detection (and Prevention) System*, z ang. System wykrywania i zapobiegania włamań) - system wykrywający i odmawiający dostępu do komputera lub sieci podejrzanemu oprogramowaniu albo użytkownikowi.
- **Industry 4.0** (z ang. Przemysł 4.0) - koncepcja tzw. „czwartej rewolucji przemysłowej", w ramach której następuje szeroko pojęta cyfryzacja, automatyzacja i autonomizacja przemysłu.
- **Infrastruktura Krytyczna (IK)** - infrastruktura niezbędna do funkcjonowania państwa i społeczeństwa: elektrownie, wodociągi itd.
- **In-house** - działania wykonywane wewnątrz organizacji (wewnętrznie, własnymi zasobami).

- **Interface/ Interfejs** - wizualne narzędzie do obsługi oprogramowania lub urządzeń przez użytkownika.
- **IoT** (*Internet of Things*, z ang. Internet Rzeczy) - rozwiązania i technologie tzw. Internetu Rzeczy.
- **IRC** (*Internet Chat Relay*, z ang. Przekaźnik czatu internetowego) - jeden z pierwszych komunikatorów internetowych.
- **ITSEC** (*Information Technology Security Evaluation Criteria*, z ang. Kryteria oceny bezpieczeństwa technologii informatycznych) - zestaw norm określających jakość ochrony systemów komputerowych.
- **Keylogger** - program zapisujący wszystkie znaki zapisane za pomocą klawiatury, poszukujący loginów i haseł dostępu.
- **KIS** (Krajowe Inteligentne Specjalizacje) - obszary uznane za strategiczne dla Polski w kontekście rozwoju technologicznego oraz rozwoju gospodarczego. Pełna, aktualna lista Krajowych Inteligentnych Specjalizacji dostępna jest na stronie smart.gov.pl
- **KSC** (Krajowy System Cyberbezpieczeństwa) - funkcjonujący w Polsce od 2018 r. system ochrony cyfrowych usług publicznych, oparty na Ustawie o Krajowym Systemie Cyberbezpieczeństwa.
- **MEC** (*Multi-Access Edge Computing*, z ang. Wielodostępowe przetwarzanie brzegowe) - kod przenoszący dane i zachodzące procesy z wnętrza chmury na jej krawędź, bliżej użytkownika tak, by ograniczyć czas oczekiwania na odpowiedź i usprawnić działanie.
- **Mechanizmy compliance** (z ang. Mechanizmy zgodności) - mechanizmy ustalania zgodności z normami obowiązującymi w branży lub prawnymi.
- **Metadane** - dane zawarte w pliku, określające jego parametry, np. lokalizację wykonania zdjęcia.
- **MFA/ UW** (*multi-factor authentication*, z ang. uwierzytelnianie wieloskładnikowe) - co najmniej dwuskładnikowa weryfikacja użytkownika przed nadaniem dostępu.
- **Model Agile** (*agile software development model*) - jeden z najpopularniejszych obecnie modeli cyklu życia oprogramowania, opartego na iteracyjno-przyrostowym procesie pracy, w którym to produkt jest stale rozwijany.
- **MŚP** (Małe i Średnie Przedsiębiorstwa) - skrót odnoszący się do mikro, małych oraz średnich przedsiębiorstw.
- **National CSS** - nieistniejąca już firma, zajmująca się wynajmowaniem komputerów na określony czas.
- **NCBR** - Narodowe Centrum Badań i Rozwoju.

- **NFV** (*Network Function Virtualization*, z ang. Wirtualizacja funkcji sieciowych) - rodzaj architektury sieci, mający na celu wirtualizację zachodzących w niej procesów i istniejących powiązań.
- **NIS** - dyrektywa UE dotycząca cyberbezpieczeństwa.
- **Oprogramowanie anti-beacon** - oprogramowanie mające przeciwdziałać zbieraniu danych na temat użytkownika przez nawet teoretycznie przyjazne programy (jak np. system operacyjny Windows 10).
- **Oprogramowanie anti-malware** - oprogramowanie chroniące przed oddziaływaniem malware, np. antywirus.
- **Oprogramowanie malware** - każdy rodzaj oprogramowania szkodliwego dla komputera bądź sieci odbiorcy.
- **OT** (*Operational Technology*, z ang. Technologia operacyjna) - sprzęt/ oprogramowanie, które wykrywa lub powoduje zmianę poprzez bezpośrednie monitorowanie i/lub kontrolę fizycznych urządzeń, procesów i zdarzeń w przedsiębiorstwie.
- **PARP** - Polska Agencja Rozwoju Przedsiębiorczości.
- **PESTEL** (*Political, Economic, Social, Technological, Environmental, Legal*, z ang. Polityczne, Ekonomiczne, Społeczne, Technologiczne, Środowiskowe, Prawne) - analiza biznesowa służąca do badania otoczenia przedsiębiorstwa lub rynku w kontekście uwarunkowań politycznych, ekonomicznych, społecznych, technologicznych, środowiskowych oraz prawnych.
- **Phishing** (z ang. Wyłudzanie informacji) - sposób nawiązywania kontaktu, mający na celu wyłudzenie wrażliwych danych od osoby, która odpowie na próbę kontaktu, zazwyczaj naśladującą wiarygodnego maila.
- **PPO** (Proces Przedsiębiorczego Odkrywania) - mechanizm diagnozy, identyfikacji, aktywizacji i integracji firm z potencjałem do rozwijania działalności innowacyjnej (z udziałem przedstawicieli środowiska nauki i otoczenia biznesu) w oparciu o wyniki prac badawczo-rozwojowych. Celem procesu jest wypracowanie mechanizmu współpracy finansowej i niefinansowej przedsiębiorców, której efektem ma być ilościowy i jakościowy wzrost nowych lub ulepszonych produktów/ technologii wdrażanych na rynku polskim i eksportowanych na rynki zagraniczne.
- **Profinet** - standard komunikacji danych między urządzeniami.
- **Przemysłowa Dioda Danych** - urządzenie z zastosowaniem w przemyśle, przepuszczająca informacje tylko w jedną stronę.
- **Quantum Resistant Methods** - dopiero projektowane metody obrony przed złamaniem szyfrowania przez komputery kwantowe.

- **Ransomware** - wrogie oprogramowanie szyfrujące pliki na komputerze lub w całej sieci ofiary do poziomu braku używalności. W zamian za odszyfrowanie, autorzy oprogramowania żądają okupu – ransom.
- **Rozwiązania chmurowe** (*Cloud technologies*, z ang. Chmury obliczeniowe) - rozwiązania pozwalające na przechowywanie danych poza fizycznym dyskiem komputera, z którego są przesyłane.
- **SCADA** (*Supervisory Control and Data Acquisition*, z ang. Kontrola nadzorcza i akwizycja danych) - system łączący elementy oprogramowania i hardware, mający zastosowanie w różnych gałęziach przemysłu, a pozwalający na kontrolę zachodzących procesów fizycznych i przepływu danych.
- **Smart City** - koncepcja tzw. inteligentnych miast zarządzanych z wykorzystaniem wysokich technologii.
- **SL** (Smart Lab) – jeden z etapów PPO obejmujący spotkania grup przedsiębiorców, z udziałem przedstawicieli nauki, otoczenia biznesu i administracji, moderowane przez doświadczonych konsultantów – ekspertów branżowych. Celem SL jest inicjowanie i rozwijanie inicjatyw projektowych w obszarach/ dziedzinach zidentyfikowanych w trakcie etapu PPO, tzw. Smart Panelu oraz zweryfikowanie potencjału tych obszarów jako ewentualnych nowych specjalizacji.
- **SOC** (*Security Operation Center*, z ang. Operacyjne Centrum Bezpieczeństwa) - system agregujący informacje w jednym miejscu, by dzięki zwiększonej bazie danych, można było skutecznie bronić się przed zagrożeniami płynącymi z sieci.
- **SWOT** (*Strengths, Weaknesses, Opportunities, Threats*, z ang. Mocne strony, Słabe strony, Szanse, Zagrożenia) - analiza biznesowa przedstawiana w formie matrycy 2x2, uwzględniająca czynniki wewnętrzne: silne i słabe strony oraz czynniki zewnętrzne: szanse i zagrożenia.
- **Think Tank** - podmiot zajmujący się bieżącymi sprawami społecznymi, gospodarczymi, politycznymi, technologicznymi czy też kulturalnymi.
- **Threat hunting** - iteracyjne, proaktywne systemy wyszukiwania nowych, nieznanych zagrożeń dla systemów komputerowych.
- **Token** - urządzenie lub program generujący kod jednorazowego użytku. Użyteczny szczególnie w bankowości elektronicznej i uwierzytelnianiu logowań.
- **TRL** (*Technology Readiness Level*, z ang. Poziom gotowości technologicznej) - metodologia pozwalająca na zdefiniowanie stopnia zaawansowania danej technologii, przez co możliwe jest porównanie poziomu zaawansowania prac nad różnymi technologiami.
- **Trojan** - program wkradający się do systemu i wykradający dane udając w pełni bezpieczne oprogramowanie.

- **USD** (*United States Dollar*, z ang. Dolar amerykański) - waluta Stanów Zjednoczonych
- **UPRP** - Urząd Patentowy Rzeczypospolitej Polskiej.
- **VPN** (*Virtual private network*, z ang. Wirtualna sieć prywatna) - bezpieczne, szyfrowane połączenie komputera lub sieci komputerów z resztą światowego Internetu. Uniemożliwia ono zobaczenie przez postronnych prawdziwego adresu IP użytkownika, a także odczytanie przesyłanych danych.
- **WNiP** (Wartości Niematerialne i Prawne) - część sumy aktywów przedsiębiorstwa, najczęściej odnosząca się do posiadanych patentów i opłacanych licencji.
- **ZML** (*Zoho Markup Language*, z ang. Język znaczników Zoho) - jeden z języków sieciowych, używany do tworzenia stron w systemie Zoho Creator.

10. Spis tabel

11. Spis rysunków

PARP
Grupa PFR

Infolinia: 801 332 202
kontakt@parp.gov.pl