Załącznik nr 2

do projektu Regionalnego Programu Strategicznego

w zakresie mobilności i komunikacji

REGIONALNY PROGRAM STRATEGICZNY
w zakresie mobilności i komunikacji

Uwarunkowania i diagnoza stanu w zakresie cyfryzacji

SPIS TREŚCI

Skróty:

4G – Sieci mobilne (komórkowe) czwartej generacji

5G - Sieci mobilne (komórkowe) piątej generacji

AI – Sztuczna inteligencja

B+R - Badania i rozwój

DC – Departament Cyfryzacji UMWP

DI – Departament Infrastruktury UMWP

DMW - Departament Majątku i Geodezji UMWP

DZ – Departament Zdrowia UMWP

EDM - Elektroniczna Dokumentacja Medyczna

Gb/s - Prędkość transmisji danych. Gigabity na sekundę.

GOZ - Gospodarka o obiegu zamkniętym

GUS – Główny Urząd Statystyczny

HPC – (ang. High-Performance Computing) obliczenia wielkiej skali

ICT - (ang. Information and communication technologies) technologie informacyjno-komunikacyjne

IoT – (ang. Internet of Things) Internet rzeczy

ISP – Inteligentne Specjalizacje Pomorza

ISP 2 - Inteligentna Specjalizacja Pomorza w zakresie „Technologii interaktywnych w środowisku nasyconym informacyjnie"

JST– jednostki samorządu terytorialnego

KE - Komisja Europejska

LAN – (ang. Local Area Network) lokalna sieć komputerowa

LTE – (ang. Long Term Evolution) technologia za pośrednictwem której odbywa się transmisja danych w sieci 4G

Mb/s – Prędkość transmisji danych. Megabity na sekundę.

NPS – Narodowy Plan Szerokopasmowy

OMG-G-S - Obszar Metropolitalny Gdańsk Gdynia Sopot

PSME - Pomorski System Monitoringu i Ewaluacji

RPS - Regionalny Program Strategiczny

SIP – System Informacji Przestrzennej

SRWP - Strategia Rozwoju Województwa Pomorskiego 2030

UE – Unia Europejska

UKE – Urząd Komunikacji Elektronicznej

UMWP - Urząd Marszałkowski Województwa Pomorskiego

UPS - (ang. Uninterruptible Power Supply) zasilacz awaryjny

VPN – (ang. Virtual Private Network) wirtualna sieć prywatna

WP – Województwo Pomorskie (Samorząd Województwa Pomorskiego)

ZWP - Zarząd Województwa Pomorskiego

1. Trendy i uwarunkowania zewnętrzne

Cyfryzacja, nazywana także transformacją cyfrową jest kluczowym zjawiskiem wynikającym z przemian i procesów społeczno-gospodarczych. Znajduje zastosowanie w wielu obszarach życia oraz stanowi elementarną część zdecydowanej większości działów gospodarki narodowej. Związana jest z rozwojem: technologii 5G, przemysłu 4.0, Internetu rzeczy (IoT), sztucznej inteligencji (AI), systemów wirtualnej oraz rozszerzonej rzeczywistości, systemów przetwarzających duże i złożone zbiory danych (big data), cyfrowej tożsamości, a także z postępującym upowszechnieniem e-usług (np. w zakresie transportu, zdrowia, edukacji, energetyki, bankowości czy turystyki). Wagę cyfryzacji podniesiono m.in. w Strategii na rzecz Odpowiedzialnego Rozwoju, w której podkreśla się, że gospodarka opierać się będzie na nowoczesnych sieciach telekomunikacyjnych (stacjonarnych i mobilnych). Cyfryzacja wyznacza również kierunek rozwoju w politykach miejskich. Współczesne inteligentne miasta wykorzystują technologie informacyjno-komunikacyjne (ICT) dla zarządzania oraz oferowania inteligentnych usług publicznych, co stawia przed nimi nowe wyzwania w obszarze społecznym, gospodarczym i środowiskowym[1].

Regionalny Program Strategiczny z zakresu mobilności i komunikacji jest silnie związany z europejską i krajową polityką rozwoju, które stanowią kluczowe uwarunkowania zewnętrzne. Dokumenty te z jednej strony definiują ramy rozwoju, a jednocześnie wskazują mechanizmy mogące wesprzeć realizację polityki na poziomie regionalnym.

Zgodnie z informacjami określonymi w dokumentach związanych z przygotowaniem nowych ram finansowania na lata 2021-2027 polityka rozwoju UE koncentrować się będzie na sześciu priorytetach, z których pod kątem niniejszej strategii, w szczególności należy wymienić:

- bardziej konkurencyjna i inteligentna Europa dzięki promowaniu innowacyjnej i inteligentnej transformacji gospodarczej;
- lepiej połączona Europa ze strategiczną infrastrukturą transportową i sieciami cyfrowymi;
- Europa o silniejszym wymiarze społecznym wdrażająca europejski filar praw socjalnych i inwestująca w wysokiej jakości zatrudnienie, edukację, umiejętności, integrację społeczną i równy dostęp do opieki zdrowotnej;
- Europa bliżej obywateli przez wspieranie oddolnych strategii rozwoju i zrównoważonego rozwoju obszarów miejskich w całej UE.

Głównym programem UE związanym z rozwojem cyfryzacji jest „Cyfrowa Europa”[2], z budżetem 9,2 mld euro. Jego celem jest przede wszystkim zwiększenie międzynarodowej konkurencyjności UE oraz rozwijanie i wzmacnianie strategicznej zdolności cyfrowej Europy. Wskazuje on na następujące kierunki rozwoju:

- wysokowydajne systemy obliczeniowe – superkomputery. Celem tego działania ma być opracowywanie i wzmacnianie superkomputerów i przetwarzania danych, co przełoży się na rozwój wielu obszarów, w tym opieki zdrowotnej i i cyberbezpieczeństwa.
- sztuczną inteligencja. W rezultacie tego działania nastąpi rozpowszechnianie sztucznej inteligencji w całej europejskiej gospodarce i społeczeństwie.
- cyberbezpieczeństwo i zaufanie do technologii. Celem tego działania ma być ochrona gospodarki cyfrowej, społeczeństwa i demokracji w UE poprzez budowanie cyberobrony i unijnego sektora cyberbezpieczeństwa, finansowanie najnowocześniejszych urządzeń i infrastruktury cyberbezpieczeństwa, a także wspieranie rozwoju niezbędnych umiejętności i wiedzy.

1 Załącznik do uchwały nr 376/XXXI/21 Sejmiku Województwa Pomorskiego z dnia 12 kwietnia 2021 roku "Strategia Rozwoju Województwa Pomorskiego 2030"

2 Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające program „Cyfrowa Europa” na lata 2021–2027. Bruksela, dnia 6.6.2018 COM(2018) 434 final.

– zaawansowane umiejętności cyfrowe. Kierunek ten zakłada możliwość łatwego zdobywania zaawansowanych umiejętności cyfrowych poprzez kursy szkoleniowe oraz staże w trakcie pracy.

– wykorzystanie technologii cyfrowych. Działanie którego rezultatem ma być zapewnienie cyfrowej transformacji administracji publicznej i usług użyteczności publicznej oraz ich interoperacyjności w całej UE, a także ułatwienie wszystkim przedsiębiorstwom, dostęp do technologii i know-how. Kluczową formą będą tu ośrodki innowacji cyfrowych, które stanowić będą centra obsługi[3].

Z uwagi na wystąpienie pandemii wywołanej COVID-19 Komisja Europejska przedstawiła wniosek w sprawie kompleksowego planu odbudowy w formie narzędzia „Next Generation EU", wbudowanego w długoterminowy budżet UE. Środki zgromadzone przez Next Generation EU będą przekazywane za pośrednictwem programów UE na cele związane m.in. z wzmocnieniem jednolitego rynku i dostosowanie go do ery cyfrowej:

– inwestowanie w powszechniejszą i lepszą łączność, zwłaszcza w szybkie wdrożenie sieci 5G,

– silniejsza obecność przemysłu i technologii w sektorach strategicznych, w tym w dziedzinie sztucznej inteligencji, bezpieczeństwa cybernetycznego, superkomputerów i chmury obliczeniowej,

– budowanie gospodarki opartej na danych jako siły napędowej innowacji i tworzenia miejsc pracy,

– większa odporność w zakresie cyberbezpieczeństwa.

Technologie cyfrowe są obecnie niezbędne w pracy, nauce i w celu uzyskania dostępu do wszelkiego rodzaju usług – od świadczeń zdrowotnych po dostęp do kultury. Pandemia wyeksponowała również podatności istniejące w naszej przestrzeni cyfrowej, jej uzależnienie od pozaeuropejskich technologii oraz wpływ dezinformacji na nasze demokratyczne społeczeństwa[4].

1.1. Rozwój infrastruktury sieciowej

Jednym z podstawowych czynników ograniczających rozwój cyfrowy jest niewystarczająco rozwinięta infrastruktura telekomunikacyjna, co powoduje terytorialne ograniczenia w dostępności do Internetu szerokopasmowego. Dodatkowo w obliczu nierównomiernego poziomu infrastruktury ICT w jednostkach publicznych rozwój e-usług przez nie świadczonych staje się dużym wyzwaniem.

„Cyfrowy kompas 2030" – dokument określający wizję i kierunek transformacji cyfrowej w Europie stawia sobie za cel by do 2030 roku wszystkie europejskie gospodarstwa domowe zostały objęte siecią gigabitową, a wszystkie zaludnione obszary znalazły się w zasięgu sieci 5G. Pożądane jest także, by do 2025 roku Europa dysponowała pierwszym komputerem z przyspieszeniem kwantowym, co utoruje jej drogę do zajęcia czołowej pozycji w dziedzinie zdolności kwantowych do 2030 roku. Dokument wskazuje również, konieczność wzmocnienia infrastruktury i możliwości w zakresie chmury w Europie. Na potrzeby jej zastosowań niezbędne będą dedykowane połączenia gigabitowe oraz infrastruktura do przetwarzania danych. Takie technologie będą wykorzystywane w przedsiębiorstwach, ale też w szkołach czy podmiotach leczniczych na potrzeby e-edukacji i e-zdrowia[5].

3 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa" oraz uchylające decyzję (UE) 2015/2240

4 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Cyfrowy Kompas na 2030 r.: europejska droga w cyfrowej dekadzie

5 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Cyfrowy Kompas na 2030 r.: europejska droga w cyfrowej dekadzie

Rys. 1 Główne cele cyfrowe UE do 2030 roku określone w dokumencie „Cyfrowy kompas 2030".

W ślad za europejskimi wytycznymi w ramach krajowej polityki rozwoju opracowany został „Narodowy Plan Szerokopasmowy", który skupia się na zapewnieniu wszystkim gospodarstwom domowym dostępu do Internetu o przepustowości dla łącza "w dół" wynoszącej co najmniej 100 Mb/s, z możliwością modernizacji do przepustowości mierzonej w Gb/s. Plan zakłada również niezakłócony bezpieczny dostęp do sieci 5G na wszystkich obszarach miejskich i na wszystkich głównych szlakach komunikacyjnych, a także gigabitowy dostęp do Internetu dla wszystkich miejsc stanowiących główną siłę napędową rozwoju społeczno-gospodarczego, takich jak szkoły, węzły transportowe i główne miejsca świadczenia usług publicznych oraz przedsiębiorstw prowadzących szeroką działalność w Internecie[6].

1.2. Poszerzanie e-usług publicznych

Rozwój polskiej administracji publicznej przy wykorzystaniu nowoczesnych technologii cyfrowych, a w efekcie usprawnienie funkcjonowania Państwa oraz stworzenie warunków ułatwiających obywatelowi komunikację z administracją publiczną i wykorzystywanie zasobów informacyjnych i udostępnianych do jego potrzeb rozwiązań to podstawowe założenia działającego już Programu Zintegrowanej Informatyzacji Państwa[7]. Zakłada się w nim reorientację administracji publicznej na usługi zorientowane wokół potrzeb obywatela, implementację narzędzi horyzontalnych, wspierających działania administracji publicznej oraz rozwój kompetencji cyfrowych obywateli, pracowników administracji i specjalistów branży ICT. Realizacja programu wymaga ścisłej współpracy z samorządami, zarówno na poziomie regionalnym, jak i lokalnym, w celu zapewnienia komplementarności i efektywności wdrażanych rozwiązań. W każdym z obszarów związanych z wdrażaniem rozwiązań o charakterze horyzontalnym, które z założenia mają służyć rozwiązywaniu problemów systemowych, niezbędne są

6 Załącznik do uchwały nr 27/2020 Rady Ministrów z dnia 10 marca 2020 r. "Narodowy Plan Szerokopasmowy"
7 Załącznik do uchwały nr 109/2019 Rady Ministrów z dnia 24 września 2019 r. Program Zintegrowanej Informatyzacji Państwa"

uzgodnienia, aby zostały uwzględnione potrzeby podmiotów z każdego z poziomów i obszarów funkcjonowania państwa.

Na potrzeby związane z wykorzystywaniem technologii cyfrowych przez samorządy dla zaspokojenia potrzeb mieszkańców powstał program „Cyfrowa Gmina". Mimo, że wiele urzędów z uwagi na pandemię już przeniosło swoje działanie do sieci, to jednak w wielu innych realizacja działań w formie cyfrowej nie zawsze jest możliwa. Program skupia się na dofinansowaniu zadań związanych z cyfryzacją urzędów gmin i powiatów, w tym jednostek im podległych poprzez nabycie sprzętu IT i oprogramowania, licencji niezbędnych do realizacji e-usług, pracy i edukacji zdalnej, edukację cyfrową w zakresie obsługi nabytego sprzętu oraz oprogramowania i licencji, a także analizą stanu cyberbezpieczeństwa, a także zapewnieniem cyberbezpieczeństwa samorządowych systemów informatycznych. Niezbędna jest jednak kontynuacja działań związanych cyfryzacją usług JST zarówno na poziomie rządowym jak i regionalnym, bowiem program "Cyfrowa Gmina" był niewystarczający do zaspokojenia wszystkich zdiagnozowanych potrzeb. Dodatkowo wyzwaniem dla JST jest wcześniej trudny do przewidzenia napływ uchodźców wojennych oraz konieczność zapewnienia ich obsługi administracyjnej

Sektor publiczny, o czym warto wspomnieć, posiada ogromne ilości cennych zasobów informacji, m.in. dane o mobilności, dane meteorologiczne, ekonomiczne, dane przestrzenne czy finansowe, które mogą być następnie wykorzystywane do tworzenia nowych, innowacyjnych produktów i usług z korzyścią dla społeczeństwa i gospodarki. Nieustające zwiększanie ilości danych sektora publicznego dostępnych do ponownego wykorzystania, w tym zwiększenie podaży danych wartościowych, będzie miało szereg pozytywnych skutków dla innowacyjności gospodarki i jakości życia społeczeństwa. Wszystkie te zagadnienia zostały szeroko poruszone w „Programie Otwierania Danych na lata 2021-2027"[8] i następnie w ustawie z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U.2021.1641).

Europejska strategia w zakresie danych zakłada budowę jednolitego rynku danych, oraz wspólnych, europejskich przestrzeni danych w kluczowych sektorach ale również wykorzystywanie danych pomiędzy różnymi sektorami gospodarki.

Pandemia uwidoczniła także potencjał wykorzystania telemedycyny i zdalnych rozwiązań w zakresie opieki i robotyki w celu zapewnienia zdalnej pomocy pacjentom będącym w swoich domach. Obywatele posiadając odpowiednie umiejętności cyfrowe będą mogli korzystać z narzędzi wspomagającymi ich w kontynuacji aktywności zawodowej, a pracownicy służby zdrowia będą mogli czerpać pełne korzyści z cyfrowych rozwiązań do realizacji świadczeń zdrowotnych[9]. W strategii na rzecz Odpowiedzialnego Rozwoju również duży nacisk położono na świadczenie usług z wykorzystaniem środków komunikacji elektronicznej. Jednym z flagowych projektów w ramach działań w obszarze zdrowia przewiduje się projekt Telemedycyna, który ma za zadanie stymulowanie rozwoju nowoczesnych usług i produktów medycznych wykorzystujących innowacyjne technologie komunikacyjne (planuje się przygotowanie innowacyjnych produktów - usługi i technologie, służących poprawie dostępu do specjalistycznych usług medycznych).

W rozwoju e-zdrowia, ale też wszędzie tam, gdzie przetwarzane są dane o istotnym znaczeniu dla realizacji zadań publicznych kluczowym znaczeniem są inwestycje w inteligentne przetwarzanie brzegowe (wzmocnienie infrastruktury ICT i możliwości w zakresie chmury). Takie rozwiązania przyniosą szereg korzyści w perspektywie długoletniej. W odniesieniu do danych dotyczących zdrowia i dokumentacji medycznej, da to możliwość znacznie szybszego gromadzenia tych danych na poziomie lokalnym[10]. Regionalne i lokalne administracje również powinny zwrócić szczególną uwagę na tego typu rozwiązania. Podniosą one zdolność przetwarzania danych do oczekiwanego w obecnych czasach poziomu. Ważnym elementem jest także w wzmocnienie współpracy administracji z przedsiębiorcami,

8 Uchwała nr 28 Rady Ministrów z dnia 18 lutego 2021 r. w sprawie Programu otwierania danych na lata 2021-2027

9 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Cyfrowy Kompas na 2030 r.: europejska droga w cyfrowej dekadzie

10 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Cyfrowy Kompas na 2030 r.: europejska droga w cyfrowej dekadzie

m.in.” poprzez wspieranie ich działalności, widoczności i dostępności w sieci jak np. w sferze oferty turystycznej i czasu wolnego.

1.3. Cyberbezpieczeństwo

Skutkiem ubocznym procesu cyfryzacji są nowe rodzaje zagrożeń, do których należy zaliczyć przestępstwa dokonywane w cyberprzestrzeni (cyberataki). Chęć przeciwdziałania tym skutkom wzmaga popyt w obszarze cyberbezpieczeństwa i w konsekwencji prowadzi do wysokich kosztów oprogramowania, systemów i usług z nim związanych, co w konsekwencji przyczynia się pośrednio do obniżenia poziomu bezpieczeństwa cyfrowego. Negatywną konsekwencją jest również uzależnienie od Internetu i życia w sieci.[11]

Cyberbezpieczeństwo stanowi obecnie integralny element bezpieczeństwa ludności. Obywatele muszą mieć pewność, że gdy korzystają z urządzeń podłączonych do Internetu, są chronieni przed cyberzagrożeniami. Społeczeństwo obecnie bardziej niż kiedykolwiek polega na bezpiecznych i niezawodnych narzędziach cyfrowych i łączności. Cyberbezpieczeństwo ma zatem zasadnicze znaczenie dla budowania odpornej infrastruktury i społeczności cyfrowej. Na poziomie europejskim aktualne kierunki działań związane z cyberbezpieczeństwem zostały określone w „Strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę”[12].

Liczba urządzeń podłączonych do Internetu już teraz przewyższa liczbę mieszkańców na świecie, a przewiduje się, że do 2025 r. wzrośnie ona do 25 miliardów. Cyfryzacja modeli pracy nabrała tempa w związku z pandemią COVID-19, podczas której 40 % pracowników UE przeszło na pracę zdalną. Zwiększa to podatność na cyberataki. W przedmiotach podłączonych do Internetu, które trafiają do konsumentów, często występują stwierdzone podatności, co dodatkowo zwiększa możliwy zakres ataku w ramach szkodliwych działań w cyberprzestrzeni.

Kolejnym poważnym zagrożeniem są ataki na infrastrukturę krytyczną. Internet ma strukturę zdecentralizowaną, bez centralnego ośrodka, i zarządza nim wiele zainteresowanych stron. Skutecznie poradził sobie z gwałtownym wzrostem natężenia ruchu, będąc jednocześnie regularnym celem szkodliwych prób zakłócenia jego działania. Jednocześnie w zakresie komunikacji i hostingu, aplikacji i danych rośnie zależność od podstawowych funkcji globalnego i otwartego Internetu, takich jak system nazw domen (DNS), oraz podstawowych usług internetowych. Usługi te są w coraz większym stopniu skupione pod kontrolą kilku prywatnych przedsiębiorstw. Sytuacja ta powoduje, że europejska gospodarka i europejskie społeczeństwo są narażone na wstrząsy geopolityczne lub techniczne, które oddziałują na najważniejsze elementy Internetu lub na jedno z tych przedsiębiorstw lub większą ich liczbę. Wzrost korzystania z Internetu i zmiany wzorców spowodowane pandemią jeszcze bardziej obnażyły słabość łańcuchów dostaw, które polegają na tej infrastrukturze cyfrowej.

Obawy dotyczące bezpieczeństwa stanowią główny czynnik zniechęcający do korzystania z usług online. Około dwie piąte unijnych użytkowników napotyka problemy związane z bezpieczeństwem, a trzy piąte uważa, że nie jest w stanie uchronić się przed cyberprzestępczością. W ciągu ostatnich trzech lat jedna trzecia z nich otrzymała fałszywe wiadomości e-mail lub odebrała telefony z prośbą o podanie danych osobowych, ale 83% nigdy nie zgłosiło cyberprzestępstwa. Jedno na osiem przedsiębiorstw padło ofiarą cyberataków. Ponad połowa służbowych i prywatnych komputerów osobistych, które raz zostały zainfekowane złośliwym oprogramowaniem, została ponownie zainfekowana w ciągu tego samego roku. Każdego roku setki milionów zapisów wyciekają w wyniku naruszeń ochrony danych.

Usługi cyfrowe i sektor finansowy są jednymi z najczęstszych celów cyberataków, podobnie jak sektor publiczny i wytwórczy. W czasie pandemii szczególnie mocno ucierpiały organizacje i pracownicy opieki zdrowotnej. Ocenia się, że ponad dwie trzecie przedsiębiorstw nie ma doświadczenia w dziedzinie cyberbezpieczeństwa. Szacuje się, że w Europie 291 tysięcy stanowisk specjalistów w dziedzinie

11 Załącznik do uchwały nr 376/XXXI/21 Sejmiku Województwa Pomorskiego z dnia 12 kwietnia 2021 roku "Strategia Rozwoju Województwa Pomorskiego 2030"
12 Wspólny Komunikat do Parlamentu Europejskiego i Rady "Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę"

cyberbezpieczeństwa pozostaje nieobsadzonych. Zatrudnianie i szkolenie ekspertów do spraw cyberbezpieczeństwa to powolny proces, co naraża organizacje na zwiększone ryzyko w cyberprzestrzeni.

Poprawa cyberbezpieczeństwa jest zatem niezbędna, aby ludzie ufali innowacjom, łączności i automatyzacji, używali ich i czerpali z nich korzyści, a także aby zapewnić ochronę podstawowych praw i wolności, w tym prawa do prywatności i ochrony danych osobowych oraz wolności wypowiedzi i informacji. Cyberbezpieczeństwo jest niezbędne dla łączności sieciowej oraz globalnego i otwartego Internetu, które muszą stanowić podstawę transformacji gospodarki i społeczeństwa w latach 20. XXI wieku. Przyczynia się ono do podnoszenia kwalifikacji i zwiększania zatrudnienia, tworzenia bardziej elastycznych miejsc pracy, bardziej wydajnego i zrównoważonego transportu i rolnictwa oraz łatwiejszego i sprawiedliwszego dostępu do świadczeń zdrowotnych. Ponadto ma zasadnicze znaczenie dla międzynarodowego bezpieczeństwa i międzynarodowej stabilności oraz dla rozwoju gospodarek, demokracji i społeczeństw na całym świecie. Rządy, przedsiębiorstwa i osoby prywatne muszą zatem korzystać z narzędzi cyfrowych w sposób odpowiedzialny i ze świadomością kwestii dotyczących bezpieczeństwa. Świadomość i higiena w zakresie cyberbezpieczeństwa muszą stanowić podstawę transformacji cyfrowej codziennej działalności.

Krajowym dokumentem wyznaczającym kierunek w zakresie cyberbezpieczeństwa jest „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024”. Dokument ten określa strategiczne cele oraz odpowiednie środki polityczne i regulacyjne, które należy zrealizować, aby systemy informacyjne, operatorzy usług kluczowych, operatorzy infrastruktury krytycznej, dostawcy usług cyfrowych oraz administracja publiczna były odporne na cyberzagrożenia . Głównym celem Strategii jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym oraz promowanie wiedzy i dobrych praktyk wśród obywateli. W dokumencie określono pięć celów szczegółowych:

- rozwój krajowego systemu cyberbezpieczeństwa.
- podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.
- zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa w cyberprzestrzeni.
- budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa.
- zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

1.4. Rozwój kompetencji cyfrowych

Kolejnym problemem w upowszechnianiu e-usług są niewystarczające kompetencje cyfrowe obywateli, co w połączeniu z ograniczeniami w dostępie do szerokopasmowego Internetu prowadzi do wykluczenia cyfrowego. Problem ten eskalowało pojawienie się pandemii COVID-19. Konieczność korzystania z narzędzi do zdalnej komunikacji ujawniły ograniczenia w zakresie obecnej gotowości cyfrowej. Sprawa niedoboru umiejętności cyfrowych stała się również zauważalna, co w istocie rzeczy objawiło problem na dwóch płaszczyznach: brak wymaganych umiejętności cyfrowych oraz brak możliwości technicznych, aby z nich korzystać.

Komisja zarekomendowała rozwiązania służące budowaniu bardziej zrównoważonej, odpornej i sprawiedliwej Europy:

- wspieranie zrównoważonej konkurencyjności: nabycie odpowiednich umiejętności pozwala pracownikom na bardziej efektywną pracę i korzystanie z zaawansowanych technologii, eliminuje główną przeszkodę, jaką zidentyfikowano dla inwestycji biznesowych, zapobiega niedopasowaniu

do rynku pracy i tworzy podstawy dla badań i rozwoju oraz innowacji opartych na przedsiębiorstwach. Ponad 70% przedsiębiorstw zgłasza brak pracowników o odpowiednich umiejętnościach cyfrowych jako przeszkodę dla inwestycji[13],

– zapewnienie sprawiedliwości społecznej: posiadanie odpowiednich umiejętności oznacza możliwość łatwiejszego utrzymania zatrudnienia i radzenia sobie w przypadku zmiany pracy. Wymaga to zapewnienia równego dostępu do dodatkowych możliwości podnoszenia kwalifikacji. Ponadto należy zapewnić taki dostęp wszędzie – od dużych miast po obszary wiejskie, przybrzeżne lub oddalone w całej Unii Europejskiej,

– budowanie naszej odporności: w ciągu ostatnich miesięcy wiele zawodów znalazło się pod silną presją. Dotyczy to w szczególności pracowników służby zdrowia i pracowników pierwszego kontaktu w handlu detalicznym, transporcie, usługach społecznych lub sanitarnych, a także nauczycieli i szkoleniowców. Dysponowanie wystarczającą liczbą wykwalifikowanych pracowników w tych strategicznych sektorach ma zasadnicze znaczenie dla zapewnienia obywatelom skutecznego dostępu do podstawowych usług zdrowotnych, społecznych lub edukacyjnych w czasie kryzysu.

Zasadą przewodnią tych dążeń powinno być zdobywanie umiejętności potrzebnych na danym stanowisku. Oznacza to, że punktem wyjścia jest identyfikacja i grupowanie zestawu umiejętności każdej osoby, zapewnienie ukierunkowanego szkolenia odpowiadającego konkretnym potrzebom w zakresie podnoszenia i zmiany kwalifikacji oraz pomoc w znalezieniu pracy, na którą jest popyt na rynku pracy[14].

Odpowiedzialność za politykę w zakresie umiejętności cyfrowych pozostaje na wielu szczeblach administracji państwa Na poziomie krajowym rozpoczęto prace nad ustanowieniem wieloletniego programu rządowego pod nazwą „Programu Rozwoju Kompetencji Cyfrowych" z terminem realizacji do 2030 r., który zakłada:

– Wzmocnienie zarządzania rozwojem kompetencji cyfrowych - zapewni schemat rozwoju kompetencji cyfrowych w Polsce.

– Rozwój edukacji cyfrowej - zapewni jednolite podejście do kształcenia kompetencji cyfrowych oraz wykorzystania zasobów i narzędzi w dydaktyce na wszystkich szczeblach kształcenia.

– Zapewnienie każdemu możliwości rozwoju kompetencji cyfrowych - zapewni dostęp do informacji, poradnictwa i szkoleń dla wszystkich, którzy chcą zbudować lub podnieść swoje kompetencje cyfrowe w Klubach Rozwoju Cyfrowego – lokalnych placówkach zorganizowanych w gminach na bazie istniejących instytucji. Działania promocyjne przyczynią się do wzrostu zainteresowania rozwojem kompetencji cyfrowych[15].

– Wsparcie kompetencji cyfrowych na rynku pracy - zapewni adekwatny do potrzeb napływ pracowników o oczekiwanych kompetencjach cyfrowych. Spowoduje większe wykorzystanie technologii cyfrowych w sektorze małych i średnich przedsiębiorstw a także wzrosną kompetencje cyfrowe pracowników instytucji publicznych.

[13] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Cyfrowy Kompas na 2030 r.: europejska droga w cyfrowej dekadzie

14 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów "Europejski program na rzecz umiejętności służący zrównoważonej konkurencyjności, sprawiedliwości społecznej i odporności"

15 Na poziomie europejskim w dokumencie „Europejski filar praw socjalnych - plan działania" przewiduje się, że docelowo 80% dorosłych będzie posiadało co najmniej podstawowe umiejętności cyfrowe w 2030 roku.

2. Cyfryzacja w województwie pomorskim

2.1. Dostęp do sieci Internet

Liczba gospodarstw domowych posiadających szerokopasmowy16 dostęp do sieci Internet rośnie systematycznie od kilkunastu lat. O ile dla makroregionu „Północnego" Polski (wg. NUTS-1) obejmującego województwo pomorskie dostęp do szerokopasmowego Internetu w 2010 roku posiadało jedynie 58,7% gospodarstw domowych, to w 2020 roku wskaźnik ten wynosił już 89,6%, w tym na obszarze województwa pomorskiego 90,2% (bez szerokopasmowego dostępu do Internetu pozostaje 80,9 tys. gospodarstw domowych z łącznej ich liczby 827,7 tys.). Poziom tego wskaźnika plasuje województwo pomorskie na 5 miejscu wśród innych województw. Spośród gospodarstw posiadających połączenie szerokopasmowe w województwie pomorskim, 78,5% dysponuje łączem stały, a pozostałe mobilnym. Dla całej Polski ten wskaźnik wynosi 75,6%. Poziom dostępności gospodarstw domowych do szerokopasmowego Internetu jest zróżnicowany w zależności od miejsca zamieszkania oraz liczby dzieci w gospodarstwie domowym. I tak, w miastach o liczbie mieszkańców powyżej 100 tys. wartość omawianego wskaźnika dla Internetu świadczonego za pomocą łącza stacjonarnego w 2020 roku dla całej Polski wynosiła 74,3%, ale dla wsi już tylko 60,1%. W 2020 roku aż 99,1% gospodarstwach domowych z dziećmi poniżej 16 roku życia posiadało dostęp do szerokopasmowego Internetu, natomiast w gospodarstwach domowych bez dzieci wskaźnik ten był znacznie mniejszy, bo wynosił jedynie 89,6%[17].

Ważnym celem Europejskiej Agendy Cyfrowej[18] było zapewnienie, aby do 2020 r. wszyscy Europejczycy posiadali dostęp do Internetu o przepustowości min. 30 Mb/s i przynajmniej połowa europejskich gospodarstw domowych miała dostęp do połączeń o przepustowości przekraczającej 100 Mb/s. W celu oceny stopnia realizacji tych postanowień posługuje się wskaźnikiem penetracji lokalowej, rozumianym jako stosunek liczby lokali mieszkalnych w budynkach w zasięgu sieci min. 30 Mb/s lub 100 Mb/s (budynek w którym operatorzy deklarują możliwość świadczenia danych usług) do ogólnej liczby lokali mieszkalnych na analizowanym obszarze. Średnia penetracja lokalowa zasięgami Internetu stacjonarnego o przepustowości min. 30 Mb/s dla Polski na koniec 2020 roku wyniosła 75,9%, a w województwie pomorskim 79%. Mimo systematycznego wzrostu wartości tego wskaźnika, Polska w pod tym względem zajmuje jedno z ostatnich miejsc w Europie (gorszy wynik osiągnięto jedynie we Francji, Finlandii oraz na Łotwie). Średnia dla europejskich państw to 85,8%. Z danych Urzędu Komunikacji Elektronicznej wynika, że do końca 2023 roku, po zakończeniu realizacji wszystkich projektów budowy infrastruktury szerokopasmowej realizowanych z dofinansowaniem z Programu Operacyjnego Polska Cyfrowa, wskaźnik penetracji lokalowej zasięgami Internetu stacjonarnego o przepustowości min. 30 Mb/s dla Polski wzrośnie do 84%, a dla województwa pomorskiego do 85%.

W przypadku dostępu do stacjonarnego Internetu o przepustowości ponad 100 Mb/s sytuacja jest znacznie gorsza. Średnia penetracja lokalowa dla Polski na koniec 2020 roku wyniosła w tym przypadku 28,3%, przy średniej europejskiej 25,9%. Oznacza to jednak, że w tym przypadku Polska plasuje się powyżej europejskiej średniej. W zakresie penetracji lokalowej zasięgami Internetu stacjonarnego o przepustowości min. 30 Mb/s i 100 Mb/s na obszarze województwa istnieją duże dysproporcje terytorialne. W zdecydowanie lepszej sytuacji znajdują się gminy miejskie, w tym w szczególności: Gdańsk, Gdynia, Sopot czy Słupsk, gdzie wartość wskaźnika dla przepustowości min. 30 Mb/s przekracza 80,1%. Na drugim biegunie plasują się obszary wiejskie takie jak np. gminy Tuchomie i Borzytuchom,

16 Zgodnie z definicją przyjmowaną w badaniach statystycznych przez szerokopasmowy dostęp do Internetu należy rozumieć taki dostęp, który jest świadczony poprzez łącza światłowodowe, technologie z rodziny DSL, sieci telewizji kablowej (modem kablowy), telefony komórkowe 3/4/5G, łącza satelitarne i stałe połączenia bezprzewodowe (sieć radiowa) oraz które umożliwiają przekazywanie wysokiej jakości obrazów, filmów, oglądanie telewizji lub granie w gry internetowe, telefonowanie przez Internet z możliwością oglądania rozmówcy oraz pozwalają na korzystanie z różnorodnych zaawansowanych usług internetowych.

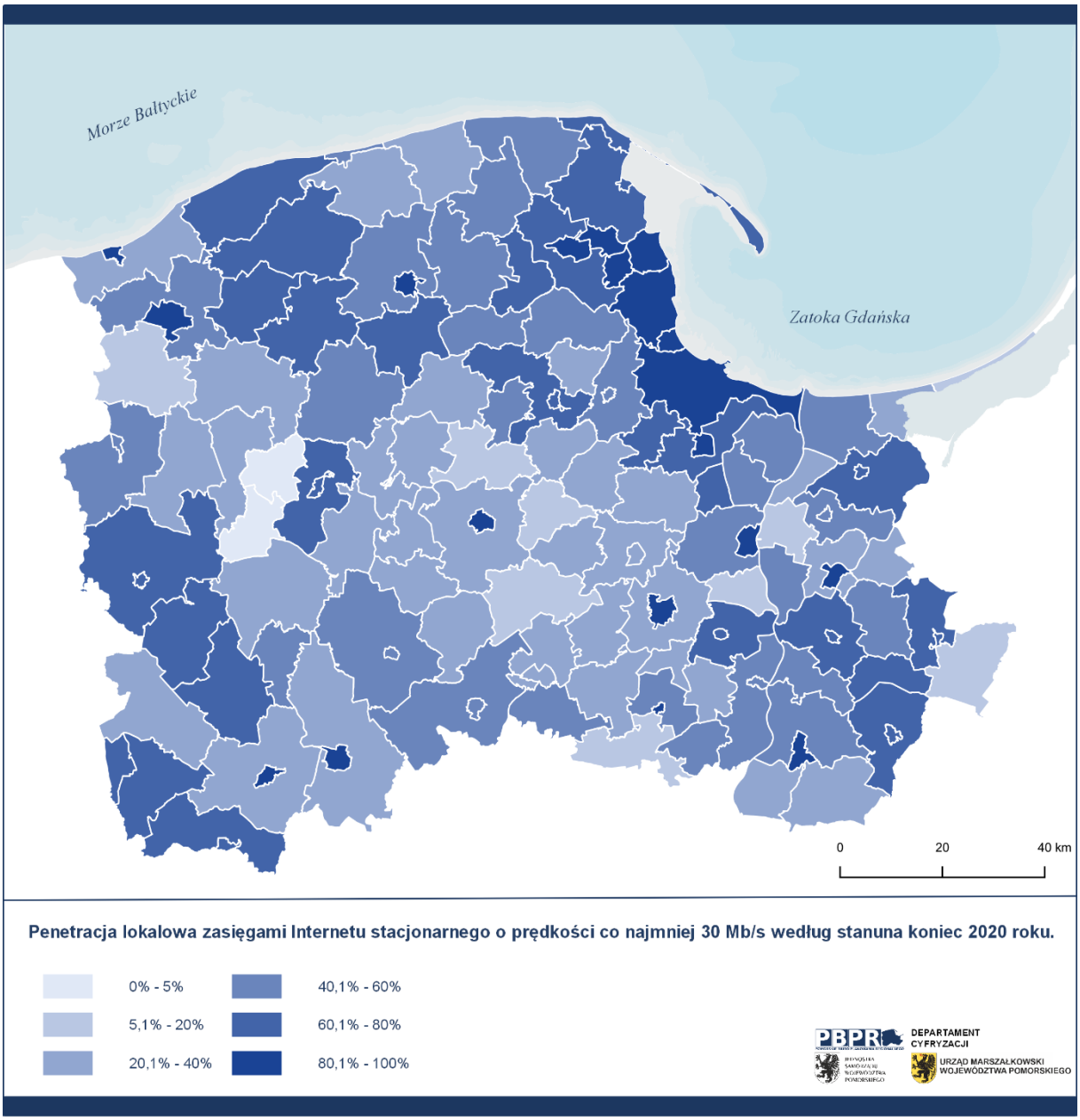
17 Na podstawie danych z raportu „Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej, przedsiębiorstwach i gospodarstwach domowych w 2020 roku". GUS.

18 KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW „Europejska agenda cyfrowa". KOM(2010)245.

w których poziom ten kształtuje się poniżej 5%, a dla kolejnych 8 gmin mieści się w przedziale 5,1-20,0%. W przypadku wskaźnika dla przepustowości min. 100 Mb/s aż dla 19 pomorskich gmin poziom penetracji lokalowej nie przekracza 5%, choć w gminach miejskich: Gdańsk, Gdynia, Sopot czy Słupsk również przewyższa 80,1%[19]. Wskazuje to jednoznacznie, że infrastruktura zapewniająca dostęp do Internetu o wysokiej przepustowości poza terenami miejskimi wymaga dalszej rozbudowy.

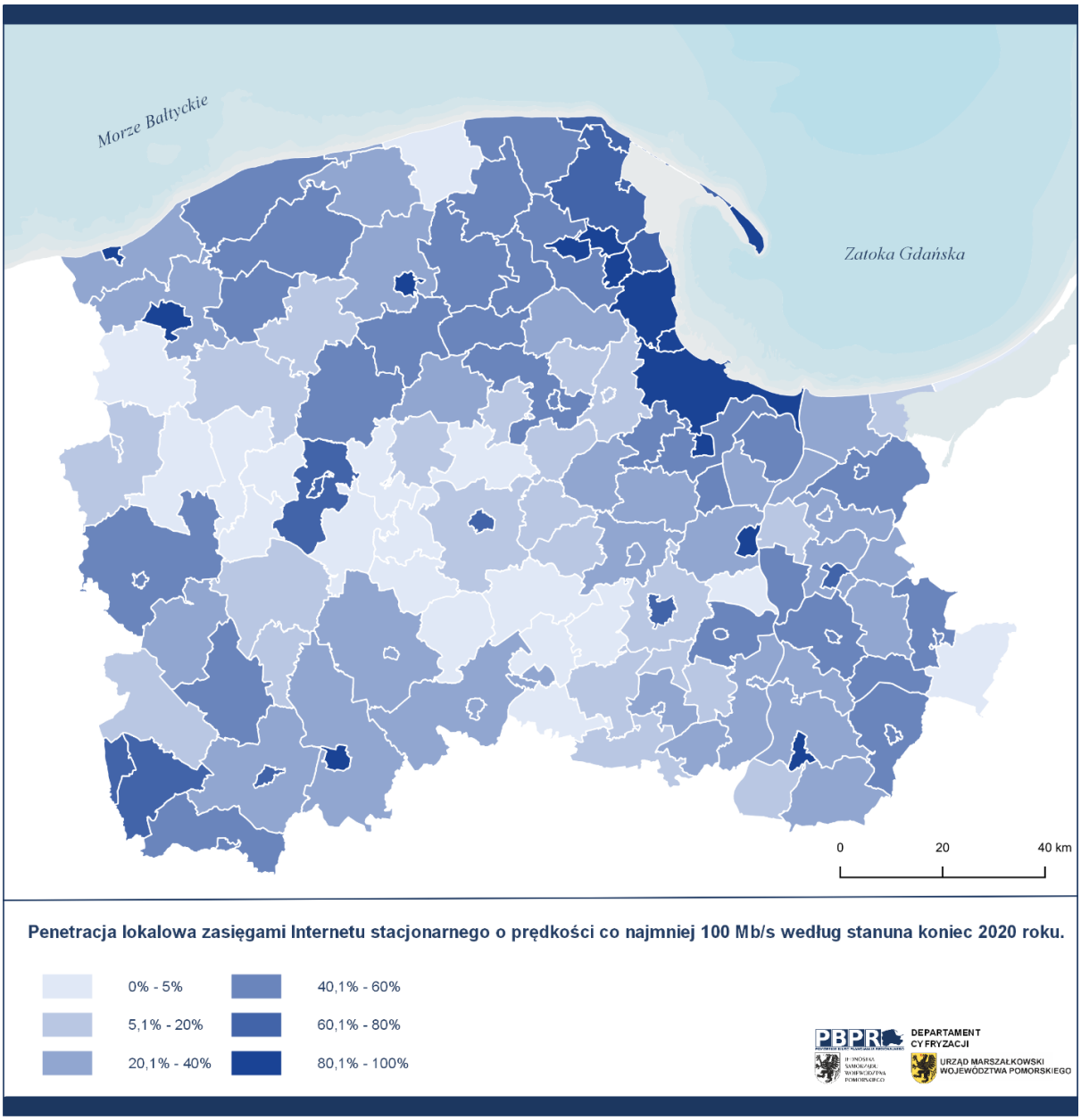
W województwie pomorskim w 2020 roku aż 98,7% przedsiębiorstw posiadało szerokopasmowy dostęp do połączeń internetowych (dla całej Polski średnia wyniosła 98,6%), jednak dostęp szerokopasmowy o przepustowości ponad 30 Mb/s posiadało już tylko 68,0% przedsiębiorstw. To blisko ogólnopolskiej średniej wynoszącej 69,2%. Wskaźnik ten był uzależniony od wielkości przedsiębiorstwa oraz rodzaju prowadzonej działalności. W skali Polski, dla małych przedsiębiorstw (zatrudniających 10-49 pracowników), uzyskano wartość 66,3%, a dla firm dużych (ponad 250 zatrudnionych) aż 92,4%. Prawie tak samo wysoka wartość (92,7%) wystąpiła dla firm prowadzących działalność informacyjno-komunikacyjną (ICT), natomiast np. dla branży budowniczej było to już tylko 61,3%, a przetwórstwa przemysłowego 64,7%[20].

19 Na podstawie danych z „Raportu o stanie rynku telekomunikacyjnego w Polsce w 2020 r.". UKE, czerwiec 2021 r.
20 Na podstawie danych z raportu „Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej, przedsiębiorstwach i gospodarstwach domowych w 2020 roku". GUS.



Rys. 2 Penetracja lokalowa zasięgami Internetu stacjonarnego o prędkości co najmniej 30 Mb/s według stanu na koniec 2020 roku.

Źródło: UKE.

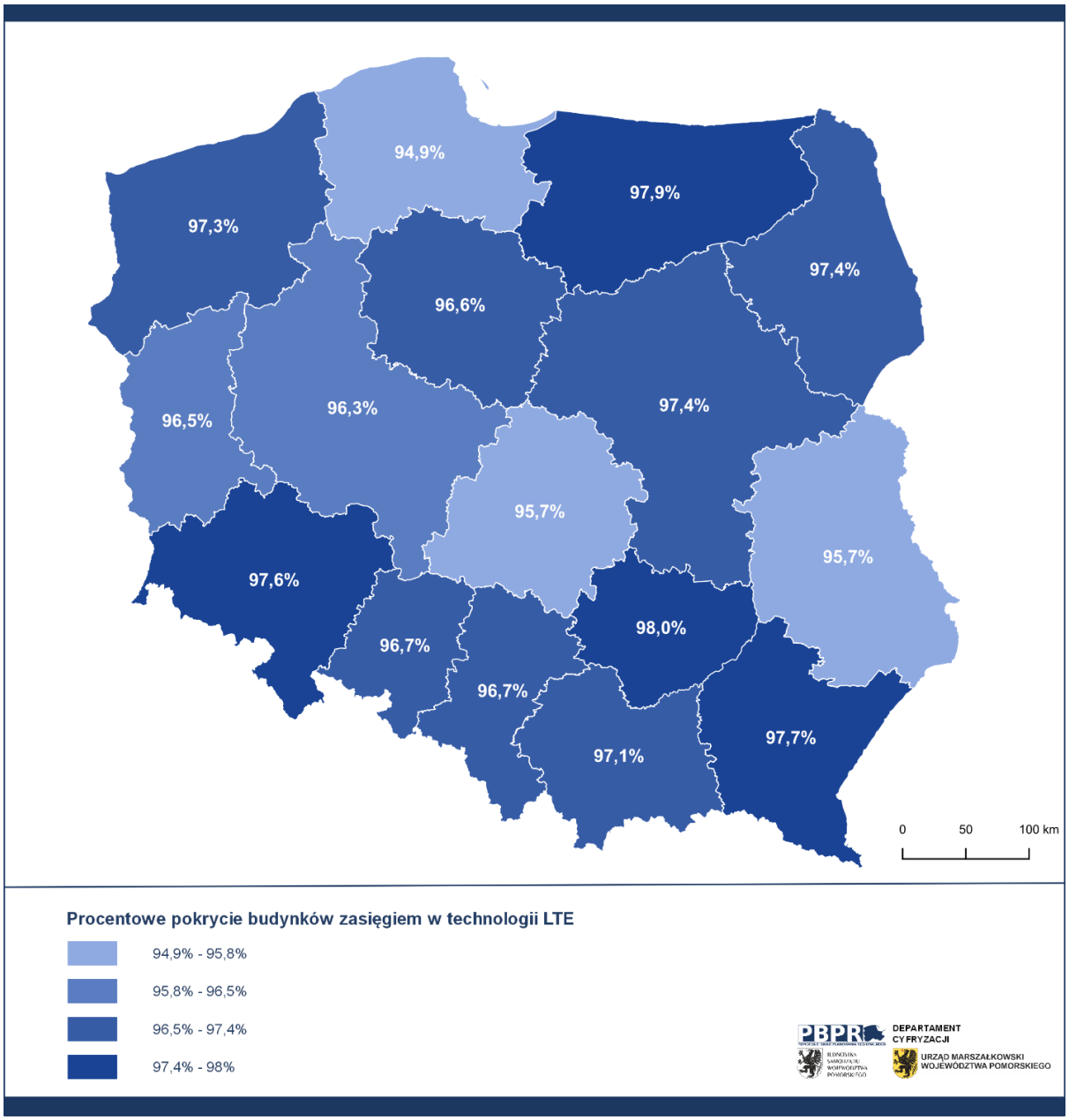


Rys. 3 Penetracja lokalowa zasięgami Internetu stacjonarnego o prędkości co najmniej 100 Mb/s według stanu na koniec 2020 roku.

Źródło: UKE.

W 2020 r. niemal wszystkie jednostki administracji publicznej korzystały z dostępu do Internetu poprzez stałe łącze. W przypadku 83% jednostek z województwa pomorskiego jest to łącze o przepustowości ponad 30 Mb/s (średnia dla Polski to 87,7%)[5]. Natomiast z przeprowadzonego przez UMWP badania21 wynika natomiast, że w przypadku pomorskich JST, jedynie 57,8% z nich korzysta z dostępu do Internetu z wykorzystaniem połączenia światłowodowego, 31,2% ze stałego łącza ale z wykorzystaniem kabla miedzianego (np. DSL, VDSL), a 10,1% (11 jednostek) nadal jako główne połączenie z Internetem wykorzystuje łącze radiowe. Niepokojące jest również, że aż 43% objętych badaniem pomorskich JST nie posiada zapasowego łącza do sieci Internet (co najmniej 43 jednostki), a z tych co posiadają, 14,7% (16 jednostek) wykorzystuje do tego celu łącze sieci mobilnej (komórkowej).

21 Badanie przeprowadzone w 2021 roku w którym wzięło udział 78% urzędów powiatowych i gminnych z obszaru województwa pomorskiego.



Rys. 4 Procentowe pokrycie budynków zasięgiem w technologii LTE

Źródło: UKE.

Pod względem nasycenia usługami Internetu mobilnego Polska w 2020 roku utrzymała się na pierwszym miejscu spośród wszystkich państw Unii Europejskiej z wynikiem 190,3%[22]. Średnia unijna w tym zakresie wynosi 107%, a w najniższą penetrację usługami dostępu mobilnego do Internetu odnotowano na Węgrzech, gdzie wyniosła ona 75,2%. Główną technologią wykorzystywaną obecnie do świadczenia usług Internetu mobilnego jest 4G, której udział stanowi 96,2%, natomiast udział technologii 5G w 2020 roku to jak na razie jedynie 3,3%. Wśród użytkowników urządzeń dedykowanych do Internetu coraz większą cześć zajmują użytkownicy urządzeń mobilnych 4G. Analysys Mason przewiduje, że ich udział w 2021 r. wyniesie 92%, a w kolejnych latach będzie malał na korzyść dostępu 5G, z którego w 2025 r. korzystać będzie 66% użytkowników. Procentowe pokrycie budynków zasięgiem w technologii LTE (4G)

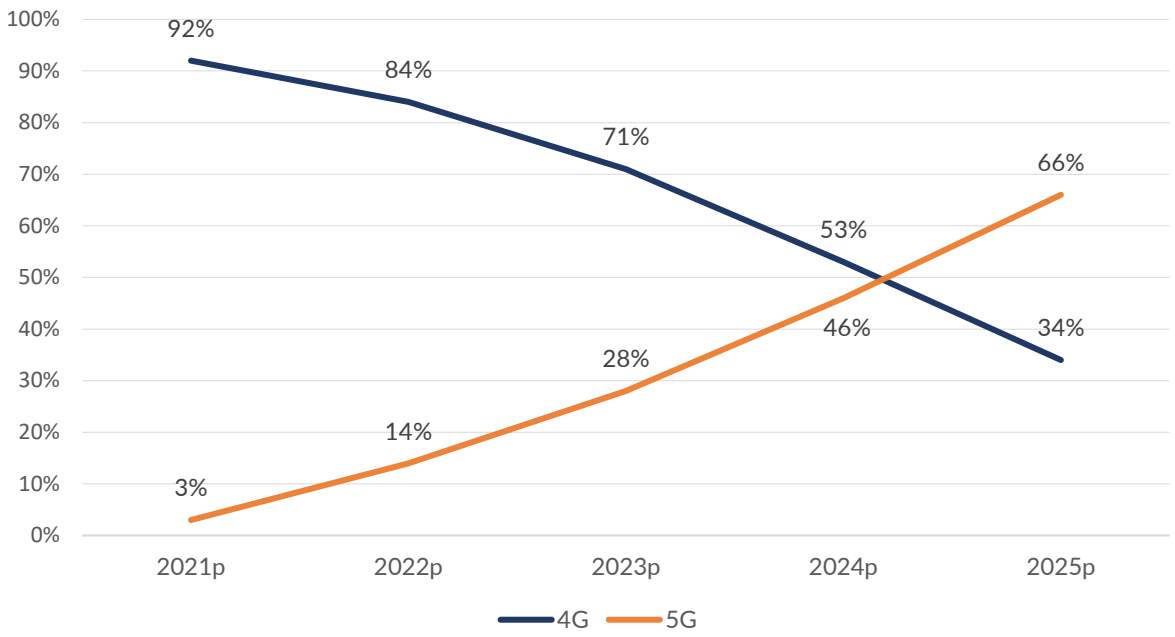
22 Penetracja pow. 100% oznacza w tym przypadku dostęp do internetu mobilnego u danego użytkownika za pomocą więcej niż jednego rodzaju dostępu.

dla województwa pomorskiego wynosi 94,9%, co jest wartością najniższą w skali kraju (średnia dla Polski to 97%)[23]

Wyzwaniem na najbliższe lata dla Polski i województwa pomorskiego w zakresie sieci mobilnych usług będzie bezpieczne i sprawne wdrożenie technologii 5G. W porównaniu do poprzednich generacji sieci mobilnych zapewni nawet 20 razy szybszą transfer danych (do 10 Gb/s przy wysyłaniu oraz do 20 GB/s przy pobieraniu), znacznie ograniczy opóźnienia w komunikacji (do jednej milisekundy), a także pozwoli na zwiększenie liczby urządzeń podłączonych do sieci (nawet do 1 miliona urządzeń na kilometr kwadratowy). Dzięki tym cechom należy spodziewać się dynamicznego rozwoju Internetu Rzeczy, a tym samym nowych rozwiązań dla inteligentnego transportu, inteligentnego miasta (smart city) oraz Przemysłu 4.0. Sieć 5G może przyczynić się nie tylko do wzrostu gospodarczego i pobudzenia przedsiębiorczości, lecz także wpłynąć bezpośrednio na życie codzienne obywateli. Jak dotąd nie został jeszcze w pełni formalnie zakończony proces standaryzacji sieci 5G. Obecnie wdrażane komercyjne sieci 5G buduje się głównie na bazie istniejących już sieci 4G\LTE. O ile w zakresie usług sieci 5G na koniec 2019 roku dominowały rozwiązania z zakresu eMBB (enhanced Mobile Broadband), czyli tzw. rozszerzonego dostępu do Internetu, to do końca 2022 roku powinny zostać zamknięte standardy z kategorii usługowych URLLC (Ultra Reliable Low Latency Communications) oraz mMTC (massive Machine Type Communications), pozwalające na rozwój usług m.in. Przemysłu 4.0, autonomicznych samochodów, czy inteligentnego miasta[24]. Dopiero wdrożenie tych standardów przełoży się na pełne spektrum możliwości sieci 5G. Pierwszą sieć 5G uruchomiła w maju 2020 roku spółka Polkomtel Sp. Z o.o., świadcząca usługi pod marką Plus. Obecnie dostęp do sieci 5G jest już oferowany przez wszystkich największych operatorów, głównie na obszarach znajdujących się w pobliżu miast wojewódzkich, ale zasięg dostępu do tej technologii jest systematycznie powiększany.

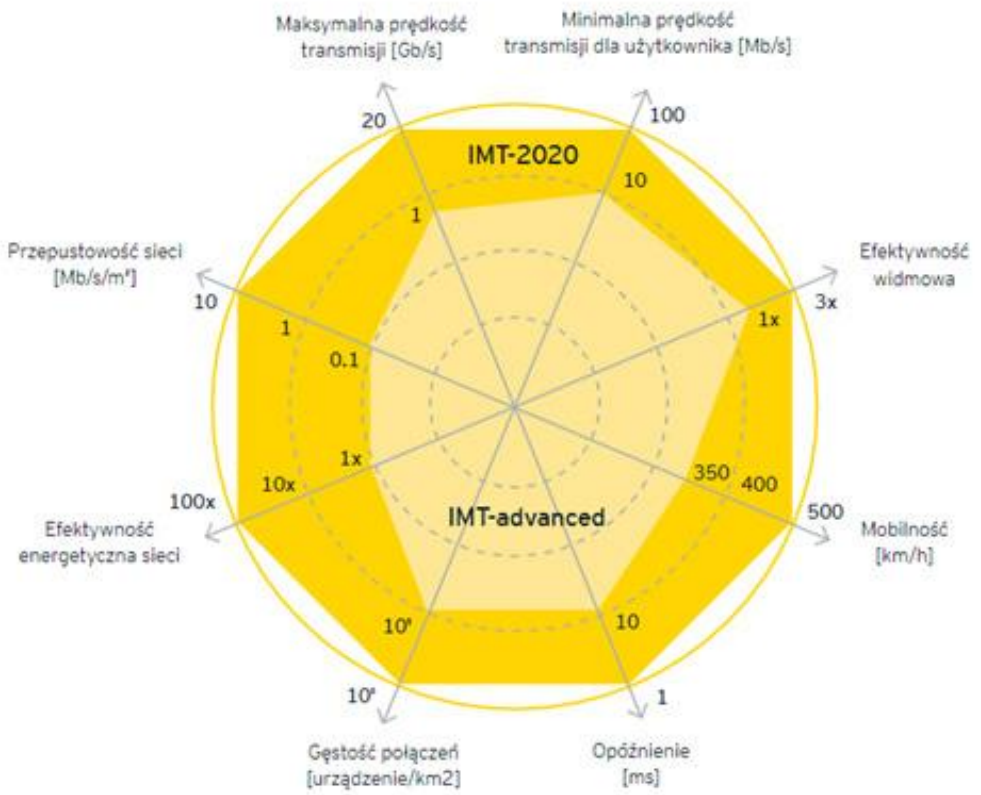
Ze względu na dezinformację rozwój sieci 5G ma niestety negatywny wpływ na poczucie bezpieczeństwa zdrowotnego mieszkańców. Istotne jest zapobieganie przekazowi fałszywych informacji, który może opóźniać wdrażanie tej technologii. Od kilku lat trwają testowe wdrożenia na terenie Europy, a jak już wspomniano, w Polsce pierwsze działające instalacje komercyjne pojawiły się w 2020 roku. Równocześnie do użytkowników poprzez media społecznościowe niesprawdzone informacje ukierunkowane na wzbudzenie obaw i strachu przed nowymi technologiami. Podejmowanie działań uświadamiających, jak również monitorujących ewentualne zagrożenia stanowić powinno jeden z obszarów towarzyszących zmianom technologicznym.

23 Na podstawie danych z „Raportu o stanie rynku telekomunikacyjnego w Polsce w 2020 r.". UKE, czerwiec 2021 r.
24 „5G SZANSE ZAGROŻENIA WYZWANIA". FAUSTINE FELICI, ANDREA GARCÍA RODRÍGUEZ, PIOTR MIECZKOWSKI, KAMIL MIKULSKI, TOMASZ PIEKARZ, BARBARA SZTOKFISZ, REDAKCJA: ROBERT SIUDAK. Instytut Kościuszki. Kraków 2020.



Rys. 5 Prognozowany udział technologii 4G i 5G w łącznej liczbie dedykowanych urządzeń do mobilnego dostępu do Internetu w latach 2021-2025.

Źródło: Analysys Mason, DataHub



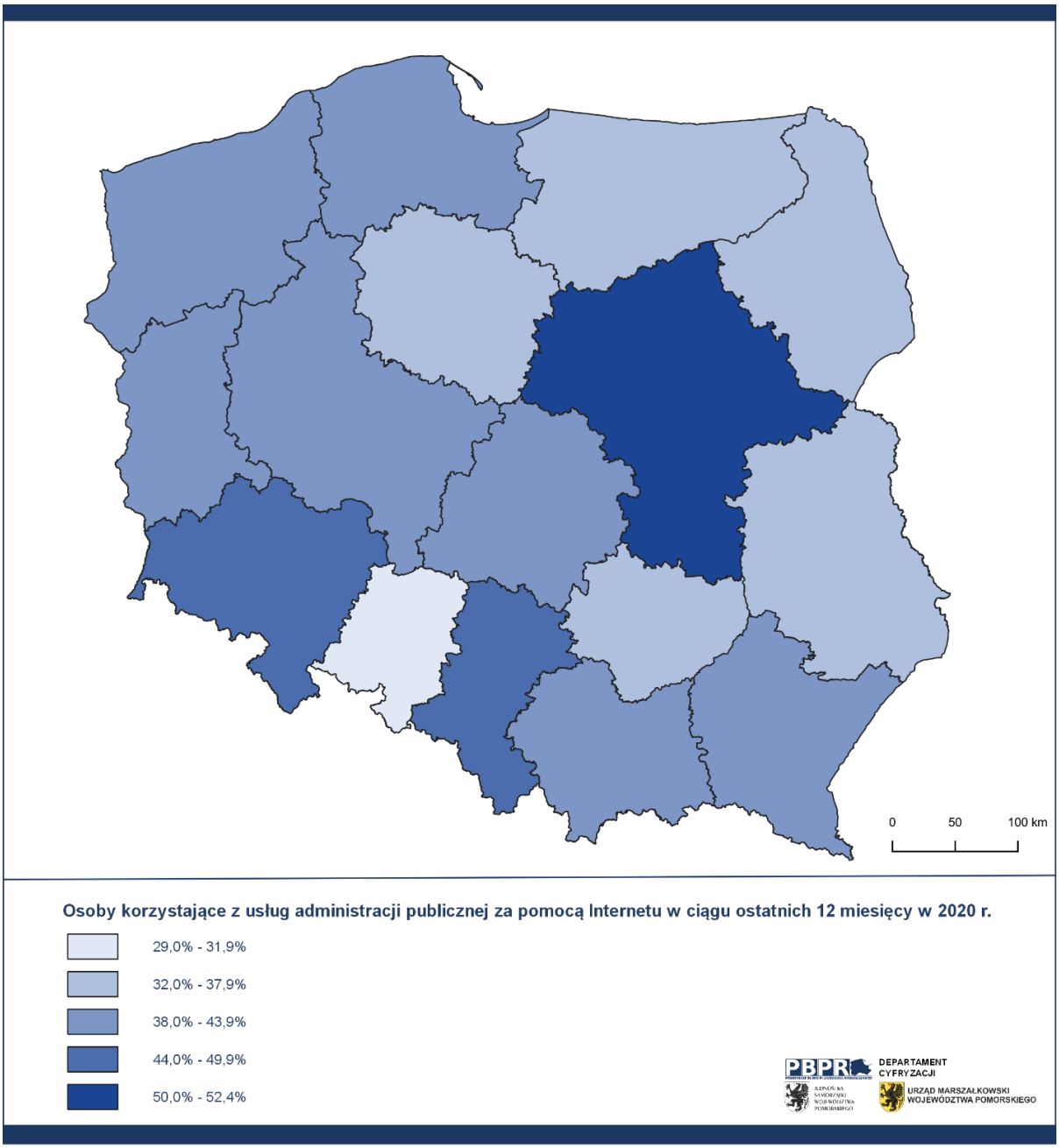
Rys. 6 Różnice pomiędzy standardem sieci 4G\LTE (IMT-Advanced), a 5G (IMT-2020).

Źródło: EY.

2.2. E-usługi publiczne i praca zdalna

Poprzez ciągły rozwój komputeryzacji oraz przenoszenie życia do świata wirtualnego zmienia się podejście do korzystania z komputera i Internetu. Elektroniczne usługi administracji publicznej stają się coraz bardziej popularne. W 2020 roku w województwie pomorskim aż 99,3% jednostek administracji publicznej udostępniało obywatelom usługi poprzez Internet.

Z drugiej strony w 2020 roku jedynie 40,1% osób w województwie pomorskim korzystało z usług administracji publicznej za pomocą Internetu w ciągu ostatnich 12 miesięcy. Daje to 6 miejsce wśród województw (średnia w skali kraju to 41,9%)[25].



Rys. 7 Osoby korzystające z usług administracji publicznej za pomocą Internetu w ciągu ostatnich 12 miesięcy w 2020 r.

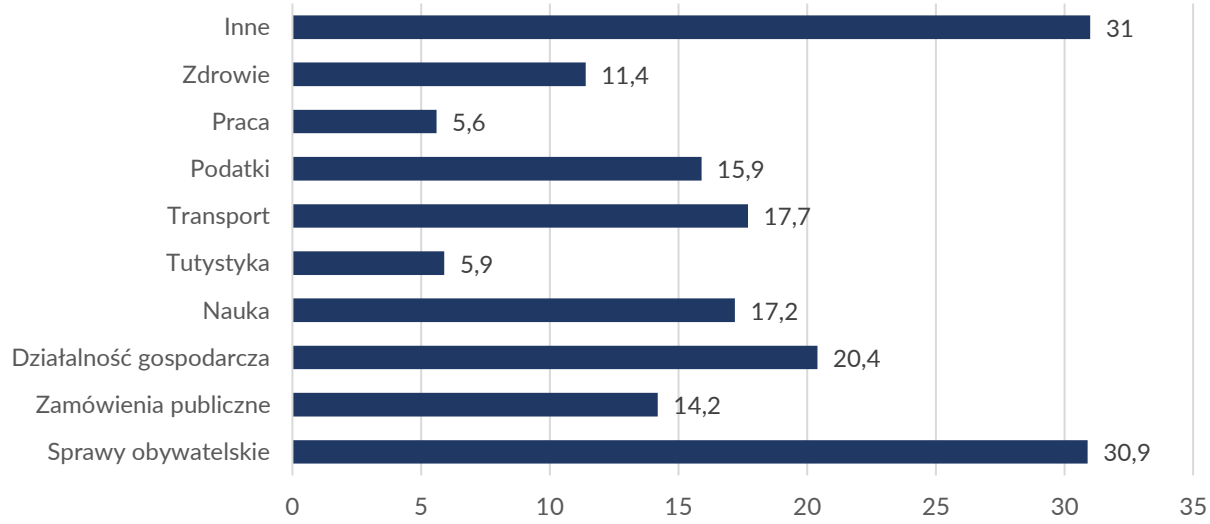
Źródło: GUS.

25 Na podstawie danych z raportu „Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej, przedsiębiorstwach i gospodarstwach domowych w 2020 roku". GUS.

E-usługi świadczone przez jednostki administracji publicznej na poziomie interakcji dwukierunkowej według badań GUS z 2018 roku w największym stopniu dotyczyły obszaru: spraw obywatelskich, działalności gospodarczej, transportu, nauki i podatków.

Dzięki rozwojowi Internetu i coraz większej jego dostępności rosną również możliwości jego wykorzystania do zdalnej pracy i telepracy. Pozwala to na uzyskanie oszczędności przez pracodawcę, który nie musi ponosić kosztów wynajmu pomieszczeń biurowych i ich wyposażenia, ale może także wpłynąć na zmniejszenie ruchu w aglomeracjach miejskich, a w konsekwencji spowodować obniżenie poziomu zanieczyszczeń środowiska. Dodatkowe korzyści stosowania pracy zdalnej i telepracy ujawniały się w latach 2020-2021 ze względu na wystąpienie pandemii COVID-19. Ten rodzaj pracy okazał się często jedynym, który pozwalał na utrzymanie działalności przedsiębiorstw i jednostek sektora publicznego.

Podstawowym warunkiem do wykonywania pracy zdalnej jest zapewnienie pracownikom bezpiecznego i wydajnego dostępu do infrastruktury i systemów teleinformatycznych przedsiębiorstwa lub jednostki sektora publicznego poprzez sieć Internet.



Rys. 8 Jednostki administracji publicznej świadczące usługi elektroniczne na poziomie interakcji dwukierunkowej według obszarów usług (w % jednostek świadczących usługi elektroniczne) w 2018 r.

Źródło: GUS.

W 2020 r. w województwie pomorskim większość jednostek administracji publicznej umożliwiała pracę zdalną. W przypadku 71,6% jednostek (w skali Polski 62,8%) była to możliwość zdalnego dostępu do dokumentów służbowych i ich modyfikacji. Taki sam odsetek pomorskich JST zadeklarował możliwość zdalnego wykorzystania aplikacji dedykowanych (w skali Polski 62,8%). To ogromny wzrost w porównaniu z 2019 rokiem, kiedy to w województwie pomorskim możliwość zdalnego dostępu do dokumentów służbowych i ich modyfikacji deklarowało zaledwie 19,1% jednostek (w skali kraju 28,3%), a możliwość zdalnego wykorzystania aplikacji dedykowanych zapewniało 31,2% pomorskich jednostek (w skali kraju 34,0%). Bez wątpienia przyczyną tego wzrostu była pandemia COVID-19 i wprowadzone w jej skutku możliwości pracy zdalnej[26].

Zbliżone wyniki płyną z badana przeprowadzonego przez UMWP, W przypadku pomorskich JST, w 2020 roku 69,7% spośród podmiotów które wzięły udział w badaniu zapewniło pracownikom dostęp do urzędowego systemu informatycznego i jego zasobów poprzez Internet, w tym do dokumentów służbowych. Kolejne 18,3% zapewniło dostęp jedynie do służbowej poczty internetowej. W przypadku

26 Na podstawie danych z raportu „Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej, przedsiębiorstwach i gospodarstwach domowych w 2020 roku". GUS.

jednostek organizacyjnych i spółek Województwa Pomorskiego dostęp do dokumentów służbowych poprzez Internet zapewniło 60,4% podmiotów, a do służbowej poczty internetowej kolejne 29,2%[27].

Aby możliwe było sprawne świadczenie e-usług i pracy zdalnej, zazwyczaj konieczne jest posiadanie systemów typu back office, takich jak system elektronicznego zarządzania dokumentami (EZD). W 2020 roku z takiego systemu w województwie pomorskim korzystało 84,4% jednostek administracji publicznej, natomiast 42,9% jednostek EZD stosowało jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw. Powyższe wskaźniki posiadały wartości powyżej średniej krajowej, wynoszącej odpowiednio 81,2% i 31,2%. Mimo stosowania systemów EZD i e-usług, w 2020 roku nadal zaledwie 8,2% dokumentów wysłanych przez pomorskie jednostki administracji publicznej było w formie elektronicznej, przy średniej krajowej na poziomie 15,4%.

Rosnące potrzeby w zakresie dostępu do informacji przestrzennej i ich wykorzystania w procesach decyzyjnych połączone z lawinowym przyrostem różnego rodzaju danych odniesionych do zjawisk nad, na i pod powierzchnią ziemi oraz postęp technologiczny sprawiły, że od kilku lat w Polsce jest szeroko dyskutowana problematyka budowy infrastruktury i rozwoju e-usług informacji przestrzennej. Podstawowym celem tworzenia infrastruktury informacji przestrzennej jest optymalizacja kosztów pozyskiwania danych oraz ułatwienie dostępu do informacji przestrzennej, gromadzonej przez administrację na różnych szczeblach w tym również za pomocą zestandaryzowanych usług sieciowych umożliwiających automatyczny dostęp do danych.

Niezbędnymi czynniki warunkującymi dostęp do informacji przestrzennej są:

- technologia,
- infrastruktura telekomunikacyjna,
- infrastruktura podpisu elektronicznego,
- organizacja,
- system prawny,
- postać danych umożliwiająca użycie przez użytkowników o rożnym stopniu zaawansowania.

Administracja publiczna oparta na wiedzy, to powszechna dostępność technologii informatycznych, umożliwiających tworzenie nowych jakościowo form dostępu mieszkańców do informacji, z jednoczesnym wykorzystaniem przestrzennych zasobów informacyjnych (geoinformacji), technik ich przetwarzania i integrowania z innymi zasobami, co prowadzi do nowego sposobu zarządzania, organizacji i porozumiewania się między ludźmi, usprawniając jednocześnie działania organów administracji publicznej. W celu zapewnienia możliwości reagowania na stale zmieniające się potrzeby rynku, wpływu na zrównoważony rozwój oraz na wzrost dochodów w szczególności w sferze oferty turystycznej i czasu wolnego, zachodzi potrzeba stworzenia interaktywnej platformy (docelowo transakcyjnej) dającej możliwość zwiększenia dostępności w sieci usług świadczonych przez przedsiębiorców.

Zastosowanie systemów informacji przestrzennej (SIP), w których technologia informatyczna jest wykorzystywana do budowy i integracji baz danych w jednostkach samorządu terytorialnego i instytucjach publicznych, w ostatnich latach znacząco wzrosło, wspomagając w coraz szerszym zakresie wykonywanie zadań własnych. Jednak dostępność i powszechność wykorzystania informacji przestrzennej ogranicza się najczęściej do zakupu informacji na nośnikach, a bardzo rzadko do wzajemnej wymiany wytworzonej informacji przestrzennej poprzez infrastrukturę ICT.

Polskie regiony, w tym województwo pomorskie rozpoczęły działania związane z wdrażaniem systemów informacji przestrzennej, ale stopień tych działań jest zróżnicowany. Zasadniczym problemem jest brak

27 Badanie przeprowadzone w 2021 roku w którym wzięło udział 78% urzędów powiatowych i gminnych z obszaru województwa pomorskiego.

szerokiego zastosowania zintegrowanych systemów informatycznych umożliwiających dostęp do informacji przestrzennej, a tym samym poprawę sposobów zarządzania regionem. Wynika to przede wszystkim z dużego stopnia rozproszenia informacji przestrzennej o terenie, braku efektywnych narzędzi zarządzania przestrzenią w skali ponadlokalnej, w szczególności w wymagających takiego współdziałania procesach: planowania przestrzennego, ochrony środowiska, inwestycji liniowych i infrastrukturalnych, zarządzania kryzysowego i ochrony ludności, turystyki i transportu oraz z braku optymalnych warunków organizacyjnych i technicznych umożliwiających dostęp do wiarygodnych i aktualnych informacji niezbędnych do zarządzania każdą jednostką samorządu terytorialnego, prowadzenia racjonalnej gospodarki przestrzennej, planowania i realizacji inwestycji oraz zrównoważonego rozwoju i ochrony środowiska.

W 2020 roku 88,7% pomorskich jednostek administracji publicznej (w skali kraju 85,4%) korzystało z map numerycznych (cyfrowych i dostępnych danych przestrzennych). W przeważającej mierze wykorzystywano je w celach: ewidencji gruntów i budynków (95,2%), planowania przestrzennego (92,0%), gospodarki nieruchomościami (86,4%), planowania inwestycji (73,6%) oraz ochrony środowiska (74,4%). Posiadane dane przestrzenne udostępniało obywatelom w 2020 roku w skali kraju 78,3% jednostek administracji publicznej. W województwie pomorskim ten wskaźnik był wyższy i wynosił 87,2%. Udostępniane dane dotyczyły przede wszystkim informacji o ewidencji gruntów i budynków oraz danych przestrzennych w formie ortofotomap [28].

Istotny wpływ na bezpieczeństwo cyfrowe instytucji publicznych mają niewątpliwie pracownicy komórek informatycznych lub firmy którym powierzono wsparcie teleinformatyczne tych jednostek. Choć w 2020 roku nadal 78,0% pomorskich jednostek administracji publicznej zatrudniało specjalistów ICT, to aż 17% podmiotów całkowicie powierzyło obsługę informatyczną firmom zewnętrznym, a w przypadku kolejnych 26,2% podmiotów część zadań informatycznych realizowali wydzieleni pracownicy lub komórka organizacyjna, a część podmiot zewnętrzny. Udział firm zewnętrznych biorących udział w obsłudze informatycznej instytucji publicznej z roku na rok wzrasta, jednak ten wzrost jest stosunkowo wolny. Odsetek pomorskich jednostek administracji publicznej, w których obsługą informatyczną powierzono w całości firmom zewnętrznym wynosił w latach 2017-2020 odpowiednio: 13,3% (w 2017 roku), 12,9%, 15,6% i 17% (w 2020 roku). Wiąże się to m.in. z coraz większymi problemami z zatrudnieniem wysoko wykwalifikowanej kadry informatyków.

2.3. Cyberbezpieczeństwo

Znaczenie cyberbezpieczeństwa rośnie wraz ze wzrostem liczby urządzeń i użytkowników systemów komputerowych. W Polsce wzrost ten jest konsekwencją między innymi prowadzonej szeroko edukacji w zakresie możliwości korzystania z funkcjonalności e-Usług, upowszechnienia bankowości elektronicznej, mediów społecznościowych, handlu w sieci Internet, a także odstępności mobilnego i szerokopasmowego Internetu.

Obserwacje i porównania z poprzednimi latami wskazują, że utrzymuje się tendencja wzrostowa w liczbie zgłoszeń incydentów. Liczba zarejestrowanych incydentów w 2020 roku była wyższa o 60,7% niż rok wcześniej i wyniosła 10 42029. W porównaniu do 2016 roku jest to już wzrost aż o 541%.

Z raportu CERT Polska za rok 2020 wynika wprost, że w 2020 roku trzy najczęściej występujące typy incydentów to phishing (73,15%), dystrybucja złośliwego oprogramowania (7,16%) i spam (3,22%)[30]. Phishing jest przebiegłą metodą oszustwa internetowego, za którego pośrednictwem przestępca podszywa się pod jakąś instytucję lub osobę. Działanie to ma na celu wyłudzenie osobistych danych,

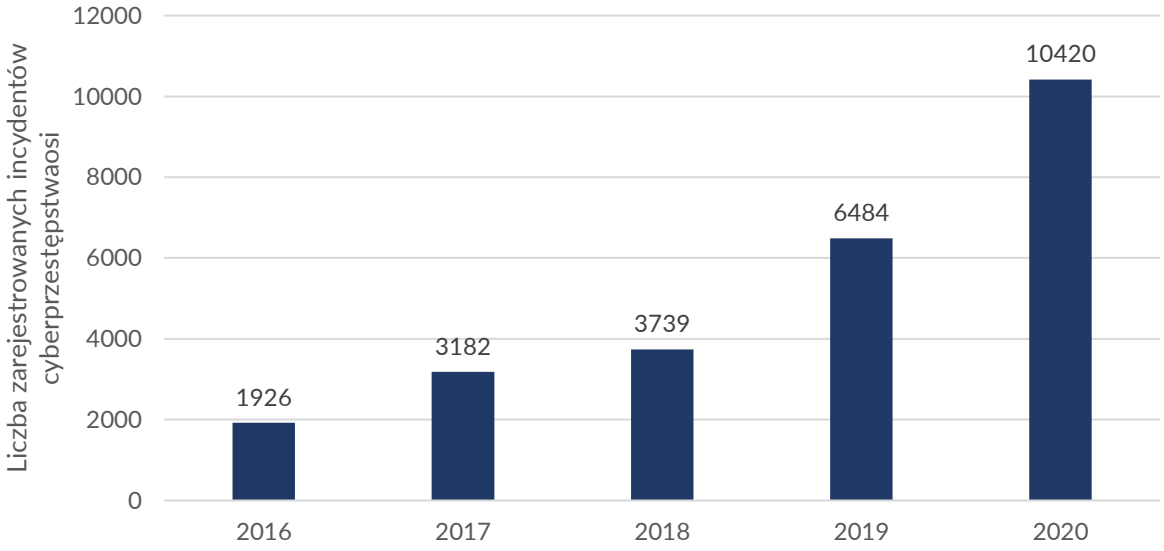
28 Na podstawie danych z raportu „Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej, przedsiębiorstwach i gospodarstwach domowych w 2020 roku". GUS.

29 Na podstawie „Raportu rocznego z działalności CERT Polska 2020 – Krajobraz bezpieczeństwa polskiego internetu". CERT Polska.

30 Na podstawie „Raportu rocznego z działalności CERT Polska 2020 – Krajobraz bezpieczeństwa polskiego internetu". CERT Polska.

takich jak: numery kont bankowych i kart kredytowych, hasła do logowania oraz innych poufnych informacji. Phishing to kategoria najbardziej wyróżniająca się na tle pozostałych ataków.

Można zauważyć, że w obliczu rozwoju technologii działania przestępców niezmiennie (również w okresie przed rewolucją komputerową) polegają na poszukiwaniu ofiar wyłudzeń poprzez dopasowanie metod do technologii przy niezmieniających się „słabych punktach leżących w naturze człowieka. Nawet jeśli inne są cele pośrednie atakujących, niezmienny jest cel główny – pieniądze. Ofiarami wyłudzeń mogą być osoby fizyczne, firmy, jednostki samorządu, podmioty lecznicze, energetyczne, administracja rządowa. Budzenie u potencjalnych ofiar ataków świadomości istnienia słabych punktów technologii jest ważnym zadaniem dla lokalnych samorządów, a także dla edukatorów i podmiotów wdrażających nowe rozwiązania na bazie sprzętu komputerowego. Metody w obszarze narzędzi komputerowych to np. fałszywe witryny www, listy elektroniczne przesyłane zarówno pocztą elektroniczną jak i sms-ami, podrzucane urządzenia elektroniczne z elementami szpiegującymi, podsłuch urządzeń elektronicznych jak i połączeń między nimi (łączy w sieciach lokalnych zarówno kablowych jak i radiowych).



Rys. 9 Liczba zarejestrowanych incydentów cyberbezpieczeństwa przez CERT Polska w latach 2016-2020.

Źródło: Opracowanie własne na podstawie danych CERT Polska i NASK.

Cele pośrednie - szantaż, kradzież tożsamości, kradzież danych osobowych, w tym danych wrażliwych, ukierunkowane są na niezmienne słabe punkty – czynnik ludzki wiedziony ciekawością, współczuciem (metoda „na wnuczka"), pośpiechem (oferty rabatowe typu „kup teraz", maile z powiadomieniami o przesyłkach awizowanych)), chciwością (maile z powiadomieniami o wygranych, spreparowane „zguby" - np. urządzenia typu Pendrive (pamięci USB) podrzucane wybranym osobom – potencjalnym ofiarom. Cel końcowy (główny) atakujących – niezmiennie stanowi korzyść materialna lub wartość mogąca przełożyć się na pieniądz.

W 2018 roku zaszły istotne zmiany w systemie prawnym dotyczące cyberbezpieczeństwa – weszły w życie: ogólne rozporządzenie o ochronie danych osobowych (RODO), a 28 sierpnia 2018 r. weszła w życie ustawa o krajowym systemie cyberbezpieczeństwa, której skutkiem było desygnowanie trzech CSIRT-ów (Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego, ang. Computer Security Incident Response Team) poziomu krajowego, prowadzonych przez NASK – Państwowy Instytut Badawczy z działającym w nim zespołem CERT Polska (ang. Computer Emergency Response Team) - CSIRT NASK, szefa Agencji Bezpieczeństwa Wewnętrznego - CSIRT GOV oraz Ministra Obrony

Narodowej - CSIRT MON. Jedną z największych zmian jest wprowadzenie obowiązku zgłaszania niektórych incydentów komputerowych.

Koordynacją incydentów dotyczących wszystkich pozostałych podmiotów takich jak większość operatorów usług kluczowych, dostawcy usług cyfrowych czy administracja samorządowa, zajmuje się CSIRT NASK. Do CSIRT NASK incydenty mogą także zgłaszać osoby fizyczne – zwykli obywatele. Można więc powiedzieć, że CSIRT NASK stanowi tzw. „CERT ostatniej szansy" (CERT of last resort).

Zanotowano wiele incydentów z próbami włamań do systemów, urządzeń i aplikacji – zakończonych sukcesem bądź tylko podjętych. Identyfikuje się nowe obiekty tych ataków - poprzez słabo zabezpieczone IoT (ang. IoT – Internetof Things - tzw. urządzenia Internetu Rzeczy), które często posiadają niezmienioną, standardową konfigurację producenta z domyślnym hasłem dostępowym. Liczb takich urządzeń w naszym otoczeniu rośnie lawinowo (zdalnie sterowane centrale domowe obsługujące czujniki otwarcia drzwi, telewizory z opcją smart, lodówki, drukarki sieciowe, samochody itp.). Liczbę incydentów obsłużonych przez CERT w podziale na sektory gospodarki przedstawiono na rysunku 10.

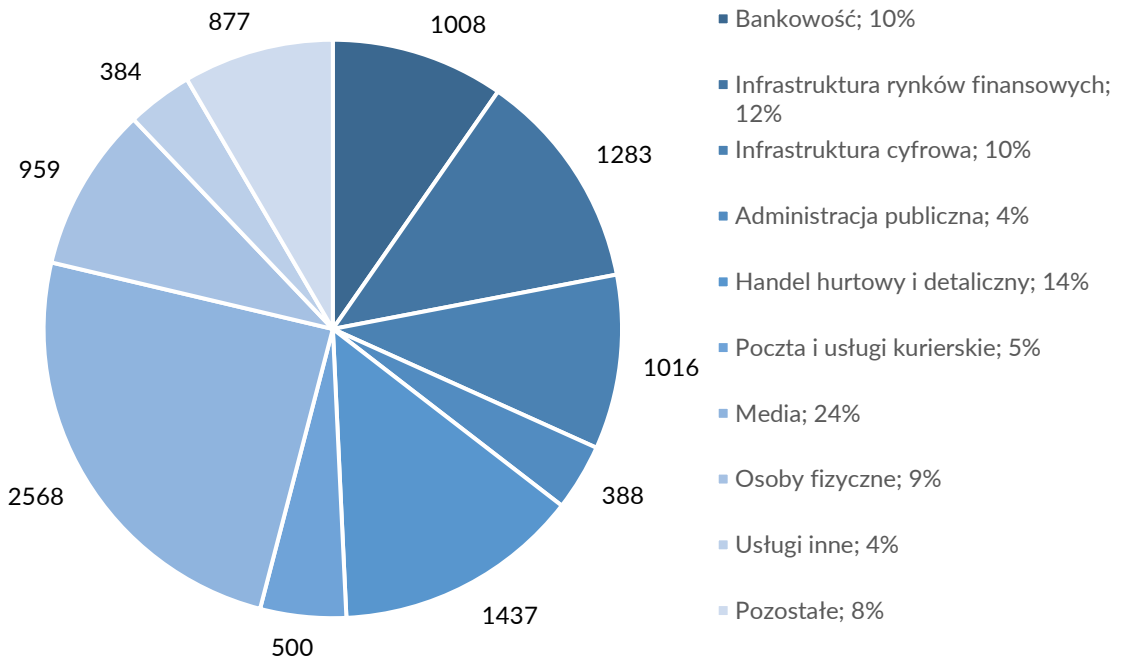
Liczba incydentów zarówno w służbie zdrowia (112 w roku, 1,07% wszystkich zgłoszeń) jak i w sektorze administracji publicznej (388 w roku, 3,72%) w porównaniu z: mediami (24,64%), infrastrukturą rynków finansowych i bankowością (łącznie 22,06%), czy handlem (13,79%)[31] jest nieproporcjonalnie mała i pozwala przypuszczać, że przy oczekiwanym w najbliższych latach wzroście dostępnych funkcjonalności e-Usług medycznych, upowszechnieniu EDM (Elektronicznej Dokumentacji Medycznej) jak również e-Usług administracji publicznej , spodziewać się można zwielokrotnienia liczby incydentów. Dlatego podjęcie ukierunkowanych na pracowników instytucji samorządowych i ochrony zdrowia skoordynowanych działań, podnoszących świadomość zagrożenia, a towarzyszących wprowadzaniu nowych technologii, staje się niezbędnym wymogiem, który należy uwzględnić w planowanych wdrożeniach systemów. Dodatkowo działania informacyjne lub treningowe (w postaci testów odpornościowych lub treningów praktycznych) mogą stanowić wsparcie dla już działających systemów, a także wspierać działania edukacyjne na poziomie szkoły podstawowej i ponadpodstawowej. Należy także przewidywać, że w Polsce jesteśmy przed skokowym wzrostem korzystania przez obywateli z e-Usług, biorąc pod uwagę statystyki europejskie. Na przykład osoby korzystające z elektronicznej administracji publicznej w zakresie wysyłania wypełnionych formularzy w 2019 r. stanowiły 31% ogółu mieszkańców przy wartości średniej 36% i maksymalnej powyżej 70% w Danii, Estonii, Szwecji i Finlandii[32]. Pokazuje to skalę potencjalnego zagrożenia zwielokrotnieniem incydentów, a tym samym skutecznych ataków.

W przypadku jednostek administracji publicznej w województwie pomorskim w 2020 roku 9,2% z tych które wzięły udział w badaniu GUS doświadczyło incydentów związanych z bezpieczeństwem ICT (w skali Polski było to 9,7%), w tym aż 53,8% jednostek zadeklarowało, że incydenty miały na celu spowodowanie niemożności korzystania z zasobów ICT jednostki (np. z powodu ataków DDos, ransomware, awarii sprzętu lub oprogramowania). W przypadku 30,8% pomorskich jednostek wskazano na incydenty których celem było zniszczenie lub uszkodzenie danych (np. z powodu zainfekowania złośliwym oprogramowaniem, włamania lub awarii oprogramowania lub sprzętu). Jednostki administracji publicznej zazwyczaj mają świadomość rosnących cyberzagrożeń o czym mogą świadczyć przeprowadzone audyty bezpieczeństwa. Według danych z 2020 roku, w województwie pomorskim przeprowadziło je 83,7% jednostek (spośród biorących udział w badaniu GUS), a w skali Polski 70,4%), z czego 89,0% z pomorskich jednostek dokonało audytu wewnętrznego, a 36,4% audytu zewnętrznego

Z drugiej strony aż, 30,5% jednostek administracji publicznej w województwie pomorskim zadeklarowało w 2020 roku, że nie zapewniło szkoleń dla pracowników w zakresie ICT, a wśród jednostek które takie szkolenia zagwarantowały, tylko 67,3% poinformowało, że były to szkolenia dla specjalistów ICT [33].

31 Na podstawie „Raportu rocznego z działalności CERT Polska 2020 – Krajobraz bezpieczeństwa polskiego internetu". CERT Polska.
32 Na podstawie raportu „Społeczeństwo informacyjne w Polsce w 2020 r.". GUS.
33 Na podstawie raportu „Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej, przedsiębiorstwach i gospodarstwach domowych w 2020 roku". GUS.

Jednocześnie, w badaniu przeprowadzonym przez Województwo Pomorskie 19 JST (17.4%) które w nim uczestniczyło zadeklarowało, że nie prowadzi szkoleń z zakresu cyberbezpieczeństwa i ochrony danych dla własnych informatyków, a aż 38 JST (34,9%) nie prowadzi takich szkoleń dla własnych pracowników nie będących informatykami. Co gorsze, pomorskie JST w 35,8% nie planują przeprowadzenia szkoleń tego rodzaju w ciągu najbliższych 12 miesięcy dla informatyków i w 40,4% dla pracowników nie będących informatykami[34].



Rys. 10 Liczba incydentów cyberbezpieczeństwa i ich procent w łącznej liczbie obsłużonych przez CERT Polska w 2020 roku w podziale na sektor gospodarki.

Źródło: Opracowanie własne na podstawie danych CERT Polska.

W 2020 roku w przypadku aż 55 pomorskich JST (50,5% biorących udział w badaniu[34]) do realizacji wszystkich zadań teleinformatycznych zatrudniono jedynie jedną osobę Oznacza to, że nie posiada ona zastępstwa w przypadku nieobecności i takie jednostki mogą być narażone na problemy w zakresie bezpieczeństwa informatycznego w okresie zatrudniania nowego pracownika na tym stanowisku. Co równie niepokojące, aż 39,4% pomorskich JST nie posiadało ani jednego etatu którego zadaniem jest wyłącznie obsługa zabezpieczeń systemów teleinformatycznych. Zatrudnieni informatycy muszą zatem kwestiami związanymi z cyberbezpieczeństwem zajmować się wyłącznie doraźnie, w przerwach pomiędzy realizacją innych zadań.

Jednocześnie 5,7% jednostek administracji publicznej w województwie pomorskim wg. danych z 2020 roku miało problemy podczas rekrutacji specjalistów ICT, głównie z powodu braku kandydatów z wykształceniem i doświadczeniem zawodowym w zakresie ICT, w ogóle braku kandydatów lub ich zbyt wygórowanych oczekiwań finansowych[35].

W 2020 roku 90,8% pomorskich JST biorących w badaniu zadeklarowało, że posiada urządzenia typu firewall na styku sieci LAN z siecią Internet. W przypadku 10 JST (10%) są to już jednak urządzenia starsze niż 5 lat. Aż 41,3% pomorskich JST planuje wymiany urządzenia typu firewall w okresie najbliższych 24

34 Badanie przeprowadzone przez Województwo Pomorskie w 2021 roku w którym wzięło udział 78% urzędów powiatowych i gminnych z obszaru województwa pomorskiego.
35 Na podstawie raportu „Społeczeństwo informacyjne w Polsce w 2020 r.". GUS.

miesięcy, ale 21% nie ma na ten cel środków finansowych, a 16,5% ma środki na realizację tylko częściowych potrzeb[18].

Na poziom bezpieczeństwa systemów teleinformatycznych wykorzystywanych w jednostkach publicznych ma wpływ m.in. wdrożony system zarządzania dostępem do zasobów danych i użytkownikami tego systemu (system zarządzania domenowego, usługa katalogowa itp.). Niestety 33,0% pomorskich JST nie posiada takiego systemu, z czego połowa z nich widzi potrzebę wdrożenia takiego systemu[18].

O ile większość pomorskich JST (98,2%) stosuje zabezpieczenia przed zanikiem zasilania (urządzenia UPS), to tylko w przypadku 28,4% jednostek takie zabezpieczenie stanowi sieć zasilania gwarantowanego (dominują natomiast indywidualne urządzenia UPS), a w przypadku 22% jednostek zasilanie awaryjne systemów informatycznych może zapewnić agregat prądotwórczy.

Na jeszcze większe zagrożenia związane z cyberbezpieczeństwem narażone są przedsiębiorstwa. W 2018 roku 13,6% przedsiębiorstw z terenu województwa pomorskiego doświadczyło incydentów związanych z bezpieczeństwem ICT. O wadze tego rodzaju zagrożeń może świadczyć fakt, że w 2019 roku już 9,1% przedsiębiorstw z terenu województwa pomorskiego posiadało ubezpieczenie od ryzyka zaistnienia incydentów związanych z bezpieczeństwem ICT[36].

Biorąc pod uwagę wcześniej przytoczone dane dotyczące systematycznego wzrostu dostępu do sieci Internet wśród mieszkańców i przedsiębiorców województwa pomorskiego oraz uwzględniając coraz szerszy zakres świadczonych e-usług (w tym publicznych) należy wnioskować, że również ryzyka związane z zagrożeniami cyberbezpieczeństwa będą dynamicznie rosnąć i należy podjąć działania, które będą im zapobiegały.

W badaniu przeprowadzonym w 2021 roku przez Województwo Pomorskie ponad 90% JST i ponad 80% jednostek organizacyjnych i spółek Województwa Pomorskiego wyraziło zainteresowanie udziału w regionalnym projekcie podnoszącym poziom bezpieczeństwa systemów ICT (w zakresie sprzętu i oprogramowania) oraz przewidującym szkolenia z zakresu cyberbezpieczeństwa[37].

2.4. Technologie interaktywne w środowisku nasyconym informacyjnie

W 2015 roku określono cztery Inteligentne Specjalizacje Pomorza (ISP) mające przyczynić się do poprawy poziomu innowacyjności w województwie pomorskim. Jedna z tych specjalizacji dotyczy nadania priorytetowego znaczenia inwestycjom w badania, rozwój i innowacje w obszarze „Technologii interaktywnych w środowisku nasyconym informacyjnie" (tzw. ISP 2). Specjalizacja ta opiera się na znacznej aktywności uczestników podążających za rozwojem technologii w zakresie megatrendów branżowych, szczególnie powiązanych ze sztuczną inteligencją czy systemami autonomicznymi. Przeciętne zatrudnienie w sektorze informacji i komunikacji ulega corocznemu zwiększeniu. W ciągu ostatnich sześciu lat wzrosło o ok. 65% (w 2013 r. zatrudnionych było 11,2 tys. osób, a w 2019 r. – 18,5 tys.), co dało 5. miejsce pod względem liczby zatrudnionych osób w branży ICT wśród województw w Polsce (2019 r.). Obecne zatrudnienie w 2020 r. w sektorze IT wyniosło 25,5 tys. osób. Obrazuje to wzrost znaczenia branży dla regionu i określa jej potencjał rozwojowy i konkurencyjność na tle innych regionów. Szansą do dalszego rozwoju tej branży może być między innymi intensyfikacja projektów związanych z gromadzeniem, analizą i wizualizacją danych oraz tworzeniem innowacyjnych systemów. Szybki wzrost potencjału ISP 2 możliwy jest dzięki dostępowi do zaplecza badawczego, m. in. interdyscyplinarnego laboratorium FutureLab, Innowacyjnych Zastosowań Informatyki, Zanurzonej Wizualizacji Przestrzennej, Akustyki Fonicznej czy Laboratorium Badawczego Hydroakustyki – a także dostęp do wiedzy i międzynarodowych sieci powiązań tworzonych w ramach

36 Na podstawie raportu „Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej, przedsiębiorstwach i gospodarstwach domowych w 2019 roku". GUS.

37 Badanie przeprowadzone przez Województwo Pomorskie w 2021 roku w którym wzięło udział m.in. 78% urzędów powiatowych i gminnych z obszaru województwa pomorskiego oraz jednostki organizacyjne i spółki Województwa Pomorskiego.

dużych wysokobudżetowych inicjatyw europejskich: InSecTT (sztuczna inteligencja, IoT), BEYOND5 (systemy komunikacyjne przyszłości), SECREDAS (cybersecurity) i innych[38]. Działania zaplanowane w ramach niniejszego RPS będą miały na celu zapewnienie warunków do dalszego rozwoju ISP 2.

38 „Regionalny Program Strategiczny w zakresie gospodarki, rynku pracy, oferty turystycznej i czasu wolnego". Załącznik nr 1 do uchwały nr 755/271/21 Zarządu Województwa Pomorskiego z dnia 29 lipca 2021 r.

Spis ilustracji