PARP
Grupa PFR

Branżowy Bilans
Kapitału Ludzkiego II

Raport z I edycji badań

Branża telekomunikacji i cyberbezpieczeństwa

Branżowy
Bilans Kapitału Ludzkiego

Branżowy Bilans Kapitału Ludzkiego II

Branża telekomunikacji i cyberbezpieczeństwa

Raport z I edycji badań

Branżowy Bilans Kapitału Ludzkiego II – branża telekomunikacji i cyberbezpieczeństwa.
Raport podsumowujący I edycję badań realizowanych w roku 2021.

Autorzy raportu:
dr hab. Daniel Mider
Adrian Kargul
Jakub Wróblewski
Wojciech Terlikowski
Konrad Kuźma

Współpraca merytoryczna:
dr Magdalena Jelonek (Centrum Ewaluacji i Analiz Polityk Publicznych, UJ)

Koordynacja i współpraca merytoryczna (PARP):
Iwona Krysińska
Agata Kosińska
Anna Tarnawa

Wykonawca badań:
Konsorcjum firm IBC GROUP Central Europe Holding S.A. i Centrum Badań Marketingowych INDICATOR sp. z o.o.

Raport przygotowany we współpracy z Sektorową Radą ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo.

ISBN: 978-83-7633-470-7.

Skład, łamanie, korekta i druk: Pracownia C&C Sp. z o.o.

Warszawa 2022

Spis treści

Szanowni Państwo,

oddajemy w Państwa ręce raport z wynikami pierwszej edycji projektu pn. „Branżowy Bilans Kapitału Ludzkiego II – branża telekomunikacji i cyberbezpieczeństwa”. Badania realizowane w ramach projektu mają na celu zwiększenie wiedzy na temat stanu i kierunków rozwoju kadr w branży i związanego z nimi zapotrzebowania na kompetencje, a także określenie wyzwań stojących przed branżą, mających swe źródło w zmianach społecznych, gospodarczych, technologicznych i prawnych.

Raport obejmuje wyniki badań ilościowych prowadzonych wśród pracodawców sektorów: telekomunikacja oraz cyberbezpieczeństwo, a także pracowników zatrudnionych na kluczowych stanowiskach w firmach działających w branży. Zestawienie ze sobą potrzeb i oczekiwań pracodawców oraz kompetencji, jakimi dysponują pracownicy, pozwoliło określić obszary niedopasowań oraz sformułować rekomendacje zmian, adresatem których mogą być instytucje kształcenia, instytucje rynku pracy oraz sami pracodawcy.

Wywiady oraz panele eksperckie, stanowiące uzupełnienie badań ankietowych, umożliwiły ponadto rozpoznanie trendów oddziałujących na branżę oraz zmian czekających ją w najbliższych latach, na które silnie wpłynęła pandemia COVID-19. Badanie realizowano od II do IV kwartału 2021 r., a więc w czasie, w którym zjawiska pandemii doświadczano już od ponad roku.

Wierzymy, że prezentowane wyniki okażą się interesujące oraz użyteczne dla osób zarządzających firmami, obecnych oraz przyszłych pracowników branży telekomunikacji i cyberbezpieczeństwa, a także wszystkich osób zainteresowanych tematyką kompetencji w branży.

Jednocześnie serdecznie dziękujemy za współpracę wszystkim przedstawicielom firm oraz ekspertom, którzy zgodzili się wziąć udział w Branżowym Bilansie Kapitału Ludzkiego, a także Sektorowej Radzie ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo.

Zespół badawczy

Słownik pojęć

Bilans kompetencji: zestawienie popytu i podaży na poziomie konkretnych kompetencji związanych ze stanowiskami pracy (z uwzględnieniem wiedzy, umiejętności i kompetencji społecznych).

Kompetencja: szeroko rozumiana zdolność podejmowania określonych działań i wykonywania zadań z wykorzystaniem efektów uczenia się i własnych doświadczeń. Termin ten może oznaczać m.in. działania, zakres uprawnień do podejmowania decyzji, merytoryczne przygotowanie do wykonania określonego zadania[1].

Wiedza: zbiór opisów obiektów i faktów, zasad, teorii oraz praktyk, przyswojonych w procesie uczenia się, odnoszących się do dziedziny uczenia się lub działalności zawodowej[2].

Umiejętność: przyswojona w procesie uczenia się zdolność wykonywania zadań i rozwiązywania problemów właściwych dla dziedziny uczenia się lub działalności zawodowej[3].

Kompetencja społeczna: rozwinięta w toku uczenia się zdolność kształtowania własnego rozwoju oraz autonomicznego i odpowiedzialnego uczestniczenia w życiu zawodowym i społecznym, z uwzględnieniem etycznego kontekstu własnego postępowania[4].

Proces biznesowy: sekwencje działań prowadzących do uzyskania określonego celu biznesowego. Cel biznesowy procesu stanowi efekt, który może zostać osiągnięty i wykorzystany przez klienta danego procesu. W skład procesów biznesowych wchodzą procesy zarządcze (odpowiedzialne za kierowanie działaniem całego systemu, tj. przedsiębiorstwa) oraz procesy pomocnicze (wspierające pozostałe procesy główne)[5].

---

1 https://www.parp.gov.pl/storage/publications/pdf/poz-27-Raport---WCAG.pdf (dostęp: 6.01.2022).

2 https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/zintegrowany-system-kwalifikacji-18267966 (art. 2 pkt. 23) (dostęp: 6.01.2022).

3 Tamże, art. 2 pkt. 21.

4 Tamże, art. 2 pkt. 7.

5 https://www.parp.gov.pl/storage/publications/pdf/poz-27-Raport---WCAG.pdf (dostęp: 6.01.2022).

Profil kompetencyjny: tworzony na podstawie analizy stanowiska pracy zestaw zadań realizowanych na danym stanowisku oraz wymagań kompetencyjnych wobec kandydatów, które niezbędne są do poprawnej realizacji zadań związanych z danym stanowiskiem lub rolą zawodową.

Rola zawodowa: określone oczekiwania normatywne, które dotyczą zarówno obowiązków, jak też uprawnień nosiciela roli. Treścią roli zawodowej są normy, wzory postaw i zachowań dotyczące czynności, które wykonuje dana osoba w ramach swoich obowiązków służbowych.

Najważniejsze wnioski

Opis sytuacji w branży

- Branża telekomunikacji i cyberbezpieczeństwa, na potrzeby projektu badawczego Branżowy Bilans Kapitału Ludzkiego II, została określona poprzez następujące sekcje z klasyfikacji PKD: Działalność w zakresie telekomunikacji przewodowej (sekcja J.61.1), Działalność w zakresie telekomunikacji innej niż przewodowa (sekcje J.61.2, 61.3 oraz 61.9), Działalność związana z zarządzaniem urządzeniami informatycznymi (sekcja J.62.03.Z).
- Według danych prezentowanych przez GUS, na koniec września 2021 r. w branży telekomunikacji i cyberbezpieczeństwa (definiowanej w oparciu o wyżej wymienione sekcje PKD) działało 15 438 firm.
- W roku 2019, liczba pracowników sektora telekomunikacji wynosiła ponad 41,5 tysiąca. Według prognoz na najbliższe lata, w 2023 r. liczba ta będzie wynosić około 43 tysiące osób[6]. Wielkość zatrudnienia w sektorze telekomunikacji utrzymuje się na raczej stałym poziomie z niewielkim, długookresowym, trendem wzrostowym.
- Wielkość sprzedaży zarówno sprzętu, jak i usług w sektorze telekomunikacji w roku 2019 wyniosła ponad 41,5 mln zł[7].
- Niemal połowa przedsiębiorców z sektora telekomunikacji oraz ponad 40% z sektora cyberbezpieczeństwa wskazało, że pandemia nie wpłynęła znacząco na sytuację w branży. Nieznaczna większość dostrzegła jednak – pozytywny bądź negatywny – wpływ pandemii.
- W przypadku obu analizowanych sektorów, najistotniejszymi problemami przedsiębiorstw wynikającymi z trwającej pandemii COVID-19 były: wzrost kosztów funkcjonowania firm oraz dostosowanie procedur firm do wymogów bezpieczeństwa i higieny w związku z zagrożeniem epidemiologicznym (kolejno: 75% i 67% wskazań w przypadku sektora telekomunikacji oraz kolejno: 80% i 81% wskazań w przypadku sektora cyberbezpieczeństwa).

[6] Społeczeństwo informacyjne w Polsce w 2020 r., GUS, s.31.

[7] Tamże.

Pozytywnie ocenianym aspektem przez ponad połowę pracodawców (56%) z sektora telekomunikacji oraz blisko trzech na czterech (71%) z sektora cyberbezpieczeństwa był wzrost liczby usług świadczonych przez firmy. W połowie przedsiębiorstw z sektora telekomunikacji oraz trzech na pięciu (61%) z sektora cyberbezpieczeństwa w czasie pandemii nawiązano także współpracę z nowymi partnerami biznesowymi.

Ocena pracowników[8] dotycząca warunków pracy w branży

- Zdecydowana większość badanych pracowników jest zadowolona z wykonywanej pracy. Takiej odpowiedzi udzieliło 95% rozmówców.
- Ogólny poziom zadowolenia z pracy jest wynikiem pozytywnej oceny różnych czynników związanych z ogólnymi warunkami pracy. Spośród wielu ocenionych bardzo wysoko (ponad 80% odpowiedzi co najmniej „raczej się zgadzam") aspektów pracy w branży, najistotniejsze okazały się: dobra atmosfera panująca w miejscu pracy, wysoki poziom umiejętności współpracowników, a także dostęp do odpowiednich narzędzi/sprzętu do wykonywania pracy.
- Ponad 70% kobiet[9] deklaruje, że otrzymuje zbyt dużo zadań, by możliwa była ich należyta realizacja w określonym czasie, podczas gdy wśród mężczyzn takie odczucie podziela 59% badanych.
- Niezależnie od sektora, większość osób biorących udział w badaniu pracowników obejmujących kluczowe stanowiska jest ogólnie zadowolona ze współpracy ze swoimi przełożonymi, jednak prawie 40% z nich dostrzega u swoich przełożonych braki w postaci skłonności do unikania podejmowania decyzji.

[8] W badaniu wzięli udział pracownicy zajmujący kluczowe, z punktu widzenia branży telekomunikacji i cyberbezpieczeństwa, stanowiska, które zostały wymienione w kolejnych wnioskach.

[9] Przedstawiona zależność może wynikać ze zróżnicowania stanowisk i wynikających z nich zadań zawodowych.

Kluczowe stanowiska oraz najważniejsze procesy biznesowe

- W toku prowadzonych badań jakościowych zidentyfikowano główne procesy biznesowe oraz powiązane z nimi kluczowe stanowiska. Do wyodrębnionych stanowisk stworzono – w oparciu o role zawodowe – profile kompetencyjne, które następnie zostały wykorzystane w badaniu ilościowym.
- Procesy unikatowe dla obszaru telekomunikacji ze wskazaniem na powiązane z nimi kluczowe stanowiska:
  - Proces tworzenia oprogramowania i systemów:
    - Architekt systemów
    - Developer (programista)
    - Quality Assurance (tester)
  - Proces projektowania infrastruktury telekomunikacyjnej oraz urządzeń:
    - Inżynier (każdej specjalizacji: sieciowej, bezprzewodowej, satelitarnej)
  - Proces koordynacji usług i utrzymania infrastruktury telekomunikacyjnej:
    - Project Manager (kierownik projektu)
- Procesy unikatowe dla obszaru cyberbezpieczeństwa ze wskazaniem na powiązane z nimi kluczowe stanowiska:
  - Proces prowadzenia audytów bezpieczeństwa:
    - Audytor bezpieczeństwa
    - Penetration Tester (tester penetracyjny, pentester)
  - Proces ochrony aktywów/identyfikacji zagrożeń/analizy:
    - CISO (ang. Chief Information Security Officer, pol. dyrektor ds. bezpieczeństwa informacji)
  - Proces prewencji w celu zapewnienia bezpieczeństwa oraz obsługa incydentów:
    - Architekt ds. bezpieczeństwa
    - Ekspert ds. bezpieczeństwa systemów/sieci/aplikacji
    - Koordynator SOC (ang. Security Operation Center, pol. Centrum operacji bezpieczeństwa)
- Proces uniwersalny ze wskazaniem na powiązane z nim kluczowe stanowisko:
  - Proces sprzedaży (pozyskanie klienta):
    - Dyrektor handlowy/sprzedaży

Zapotrzebowanie na pracowników w branży

- W niemal co piątej spośród wszystkich badanych firm poszukiwano nowych pracowników w ciągu 12 miesięcy poprzedzających badanie (październik 2020 r. – październik 2021 r.). W sektorze telekomunikacji w niemal połowie firm poszukiwano pracowników na stanowisko inżyniera (każdej specjalizacji) (48% z badanych firm poszukujących pracowników), a w sektorze cyberbezpieczeństwa na stanowisko audytora bezpieczeństwa (49%).
- W większości przedsiębiorstw, w ciągu 12 miesięcy poprzedzających badanie, pojawiły się problemy związane ze znalezieniem odpowiednich pracowników. W sektorze telekomunikacji problem ten wynikał głównie z braku odpowiednich kompetencji, których oczekiwano w przedsiębiorstwach od kandydatów, natomiast w sektorze cyberbezpieczeństwa – z niewielkiego zainteresowania ofertą pracy.
- W opinii zdecydowanej większości badanych, liczba pracowników zatrudnianych w przedsiębiorstwach z analizowanej branży w ciągu kolejnych 12 miesięcy pozostanie na tym samym poziomie. Nieliczni wskazują na wzrost w tym zakresie (odpowiednio: 10% w sektorze telekomunikacji oraz 5% w sektorze cyberbezpieczeństwa). Więcej przedsiębiorstw oczekuje natomiast wzrostu zatrudnienia w perspektywie najbliższych 3 lat. W sektorze cyberbezpieczeństwa 36% przedsiębiorców deklaruje wzrost zatrudnienia i jest to o 24 p.p. więcej w stosunku do sektora telekomunikacji.
- Ogólnie w branży telekomunikacji i cyberbezpieczeństwa nie przewiduje się większych zmian w zapotrzebowaniu na pracowników, jednakże zróżnicowanie w prognozach pojawia się przy analizach uwzględniających stanowiska kluczowe dla branży. Niezależnie od perspektywy czasowej, najwięcej pracodawców deklarujących wzrost zatrudnienia prognozuje, że wystąpi on w przypadku stanowiska programisty, natomiast w perspektywie 3 lat wzrost wielkości zatrudnienia dotyczyć będzie zapotrzebowania na stanowisko eksperta ds. bezpieczeństwa (31%; to więcej o 18 p.p. w zestawieniu z perspektywą 12 miesięcy).
- Niezależnie od sektora, badani pracodawcy deklarują, że na wyróżnione dla branży kluczowe stanowiska najchętniej zatrudniliby osoby posiadające wykształcenie wyższe. Wynika to z dwóch powodów: (1) na stanowiska specjalistyczne ogólnie chętniej zatrudniane są osoby z wykształceniem wyższym, (2) wybrane stanowiska (ze względu na swoją specyfikę) są bardzo mocno wyspecjalizowane.

- Zarówno w sektorze telekomunikacji, jak i cyberbezpieczeństwa pracodawcy oczekują od potencjalnych kandydatów na każdym z wyróżnionych stanowisk doświadczenia zawodowego, natomiast na ogół nie wymagają posiadania przez pracowników zawodowych uprawnień, certyfikatów bądź licencji do realizacji zadań na poszczególnych stanowiskach.

Ocena umiejętności pracowników

- W dwóch trzecich spośród wszystkich badanych przedsiębiorstw weryfikuje się (sporadycznie lub systematycznie), jakich umiejętności potrzebują zatrudnieni pracownicy.
- Najczęściej wskazywaną przez pracodawców metodą identyfikującą zapotrzebowanie na konkretne kompetencje u zatrudnionych pracowników jest rozmowa pracownika z przełożonym.
- Połowa pracodawców zgadza się ze stwierdzeniem, że umiejętności ich pracowników są w pełni zadowalające i zatrudnione osoby nie wymagają dodatkowych szkoleń.
- W przypadku zidentyfikowania u pracowników braku konkretnych umiejętności, najczęstszym działaniem podejmowanym przez pracodawców jest próba doszkalania pracowników.
- Niezależnie od sektora, ponad połowa pracodawców z branży deklaruje, że absolwenci szkół i uczelni są odpowiednio przygotowani do podjęcia pracy zawodowej.

Rozwój kompetencji pracowników

- Pracodawcy najchętniej decydują się na rozwijanie kompetencji u swoich pracowników w miejscu pracy. Najczęściej stosowaną metodą jest przeprowadzanie instruktaży dotyczących obsługi nowego sprzętu (ponad 60% wszystkich wskazań respondentów).
- Korzystanie z przynajmniej jednej formy rozwoju kompetencji u swoich pracowników zadeklarowało łącznie 86% wszystkich badanych przedsiębiorców.
- Pracodawcy starają się być atrakcyjni dla pracowników. Najczęściej stawiają na benefit w postaci umożliwienia pracownikom pracy zdalnej. Inne często stosowane elementy motywacyjne to premie roczne oraz elastyczny czas pracy.

Wyzwania stojące przed branżą w perspektywie kolejnych 3 lat

- Trzy najważniejsze wyzwania stojące przed branżą w perspektywie najbliższych lat to:
  - dbanie o rozwój pracowników w celu utrzymania przez nich zatrudnienia – 51% wskazań ogółem (sektor telekomunikacji: 51%, sektor cyberbezpieczeństwa: 53%);
  - spełnienie norm i wymogów dla pojawiających się nowych technologii, ponieważ obecne przepisy prawne nie do końca przystają do rzeczywistości technologicznej[10] – 50% wskazań ogółem (sektor telekomunikacji: 50%, sektor cyberbezpieczeństwa: 49%);
  - informowanie klientów o zagrożeniach przy korzystaniu z technologii i usług telekomunikacyjnych/internetowych oferowanych przez firmę – 46% wskazań ogółem (sektor telekomunikacji: 45%, sektor cyberbezpieczeństwa: 49%).
- W przypadku niektórych wyzwań zaobserwowano (inaczej niż w przypadku wyzwań najważniejszych) dużą różnicę bezwzględną pomiędzy sektorami. Trzy wyzwania z największą różnicą (wszystkie na korzyść sektora cyberbezpieczeństwa):
  - znalezienie nowych pracowników (specjalistów) z zakresu IT, którzy zajmują się projektowaniem systemów, programów, aplikacji itp. (różnica 10 p.p.);
  - weryfikacja nowych pracowników w zakresie ich kompetencji i historii o ochronie danych osobowych (różnica: 9 p.p.);
  - zwiększenie poziomu dbałości o doświadczenia użytkownika podczas korzystania z technologii i usług oferowanych przez firmę (różnica: 6 p.p.).

[10] Przykładem w polskim prawodawstwie są ataki SQL injection, które w teorii miały być karane z paragrafów o atakach hakerskich, oraz łamanie algorytmów systemowych. Więcej na ten temat w niepublikowanym materiale będącym w posiadaniu autora: „Na najniższym poziomie porządku gradacyjnego będą czyny, które nie są ścigane w żaden sposób na gruncie normatywnym, ale naruszają normy przyjęte wśród internautów. Innymi słowy, czyny o niskim stopniu natężenia skupiają się przede wszystkim na normach społecznych, a nie normach prawnych. Będą to więc czyny, które wywodzą się z grupy przestępstw komputerowych, które mogą zaistnieć wyłącznie w cyberprzestrzeni. Przykładem tego typu czynu może być wspomniany już SQL injection. Do innych ataków o niskim stopniu natężenia należy zaliczyć także czyny związane z łamaniem algorytmów systemowych. W tej kategorii należy sytuować wszystkie działania, w których cyberprzestępca używał będzie do swoich działań kryptografii. Główną motywację dla czynów o niskim stopniu natężenia w wymiarze społecznym stanowi partykularny interes hakera. Nie uzyskuje on z tego benefitów finansowych (lub są one bardzo małe). Sam czyn nie niesie za sobą istotnych fizycznych zmian i związany jest bardziej z błędami (złe zabezpieczenia systemu). Wynika on z małych umiejętności osoby odpowiedzialnej za bezpieczeństwo systemu.” [za:] Mincewicz W. (2019). *Cyberdewiacja w Internecie, czyli o dewiacjach społecznych na przykładzie Ransomware i Distributed Denial of Service attack*. *Studium socjologiczne.*

Bilans kompetencji

- Ocena ważności kompetencji z perspektywy pracodawców jest, niezależnie od sektora, stosunkowo wysoka (w sektorze telekomunikacji średnia wartość ważności kompetencji waha się w przedziale: 4,26–4,80, a w sektorze cyberbezpieczeństwa: 3,87–4,84), choć w sektorze cyberbezpieczeństwa znacznie bardziej rozproszona.
- Samoocena kompetencji posiadanych przez pracowników jest nieco niższa niż relatywna ocena pracodawców – w sektorze telekomunikacji średnia samoocena waha się w przedziale: 4,07–4,55, a w sektorze cyberbezpieczeństwa: 3,67–4,61.
- Kompetencje relatywnie ważniejsze dla pracodawców, trudne do pozyskania i zyskujące na znaczeniu w przyszłości są w sektorze telekomunikacji, inaczej niż w przypadku sektora cyberbezpieczeństwa, nieliczne i dotyczą tylko jednego stanowiska. W sektorze cyberbezpieczeństwa jest ich zdecydowanie więcej i dotyczą większej liczby stanowisk.
- Na znaczeniu zyskiwać będą kompetencje związane z wiedzą o najnowszych rozwiązaniach technologicznych oraz umiejętności związane z optymalizacją działań (w sektorze telekomunikacji), a także wiedza o tym, w jaki sposób identyfikować i weryfikować informacje oraz przeciwdziałać zagrożeniom (w sektorze cyberbezpieczeństwa).

1. Metodologia badania

Celem działań badawczych realizowanych w ramach projektu Branżowy Bilans Kapitału Ludzkiego II w branży telekomunikacji i cyberbezpieczeństwa jest określenie stanu i kierunków rozwoju kadr i związanego z nim zapotrzebowania na kompetencje, a także określenie krótkookresowych wyzwań (perspektywa najbliższych 3 lat), przed którymi stoi branża. Działania badawcze obejmują:

1. Określenie głównych procesów biznesowych dla branży telekomunikacji i cyberbezpieczeństwa, określenie zadań służących realizacji tych procesów oraz oznaczenie, czy w głównych procesach biznesowych istnieją elementy/części, które mogą funkcjonować także w innych branżach;
2. Określenie profili kompetencyjnych dla kluczowych stanowisk, w tym ocena ważności poszczególnych kompetencji;
3. Określenie, czy pojawią się nowe stanowiska wraz z informacją czy zostaną one utworzone, czy też przenikną z innych branż;
4. Analizę popytu i podaży dla określonych kluczowych stanowisk;
5. Ocenę kompetencji pracowników na kluczowych stanowiskach;
6. Analizę działań/praktyk skierowanych na podnoszenie kompetencji kadr;
7. Określenie wyzwań, przed jakimi stoi branża i ocenę ich wpływu na rozwój kadr w branży;
8. Określenie potencjalnych zmian w strukturze zatrudnienia w perspektywie kolejnych 3 lat;
9. Określenie kompetencji, których znaczenie będzie rosło/malało w ramach wskazanych kluczowych stanowisk.

By osiągnąć wskazane cele, zostały zrealizowane badania jakościowe, w ramach których przeprowadzono wywiady indywidualne oraz grupowe z ekspertami z branży, a następnie badania ilościowe, w których respondentami byli uczestnicy rynku pracy działający w branży – pracodawcy i pracownicy zatrudnieni na 12 kluczowych stanowiskach (będących wynikiem badań jakościowych). Podsumowywana edycja (pierwsza z dwóch zakładanych) projektu badawczego trwała od połowy grudnia 2020 r. do połowy stycznia 2022 r.

Na potrzeby zrealizowanych badań, branża telekomunikacji i cyberbezpieczeństwa określona została poprzez następujące kategorie wyszczególnione w ramach Polskiej Klasyfikacji Działalności (PKD):

- działalność w zakresie telekomunikacji przewodowej (J.61.1),
- działalność w zakresie telekomunikacji bezprzewodowej, z wyłączeniem telekomunikacji satelitarnej (J.61.2),
- działalność w zakresie telekomunikacji satelitarnej (J.61.3),
- działalność w zakresie pozostałej telekomunikacji (J.61.9),
- działalność związana z zarządzaniem urządzeniami informatycznymi (J.62.03.Z) (wyłącznie dla firm z sektora cyberbezpieczeństwa).

1.1. Badania jakościowe

Pierwszy, jakościowy etap procesu badawczego polegał na przeprowadzeniu indywidualnych i grupowych wywiadów z ekspertami, a także realizacji badania metodą delficką[11]. Przeprowadzono:

- 40 wywiadów indywidualnych (w okresie od 20 kwietnia 2021 r. do 10 maja 2021 r.),
- 4 panele eksperckie (w okresie od 28 do 30 czerwca 2021 r.),
- badanie delfickie z łącznym udziałem 53 ekspertów (tych samych w obu falach badania; przeprowadzono dwie iteracje badania w formie on-line w okresie od 28 czerwca 2021 r. do 14 lipca 2021 r.),
- panel podsumowujący z Sektorową Radą ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo (w dniu 23 lipca 2021 r.).

Respondentami w badaniach jakościowych byli:

- eksperci specjalizujący się w analizie branży, w tym osoby działające w instytucjach zrzeszających przedstawicieli branży,
- przedsiębiorcy (pracodawcy) z branży telekomunikacja i cyberbezpieczeństwo,

[11] Metoda delficka należy do metod heurystycznych, w których do podejmowania decyzji wykorzystuje się wiedzę specjalistów z danej dziedziny. Biorący udział w badaniu eksperci mają za zadanie odpowiadanie na pytania dotyczące analizowanej tematyki. Po podsumowaniu wyników uzyskanych w I turze badani są o nich informowani i ponownie proszeni o zajęcie stanowiska. Jest to zatem metoda wypracowywania konsensusu w grupie ekspertów poprzez kolejne iteracje ocen odnoszących się do danego zjawiska.

- przedstawiciele środowisk edukacyjnych, firm rekrutacyjnych, analitycy trendów w obszarze rynku pracy.

Wnioski z paneli, wywiadów oraz badania delfickiego zostały poddane walidacji w czasie panelu podsumowującego z Sektorową Radą ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo.

1.2. Badania ilościowe

Drugi, ilościowy etap procesu badawczego polegał na przeprowadzeniu wywiadów kwestionariuszowych z respondentami reprezentującymi grupy: pracodawców i pracowników. Wywiady zrealizowano głównie metodą CAPI (standaryzowane wywiady bezpośrednie z użyciem laptopa), ale także metodami dodatkowymi wykorzystującymi zdalne kanały kontaktu (wywiady telefoniczne lub wywiady z wykorzystaniem komunikatora internetowego)[12].

Badaniem objęto podmioty zdefiniowane przez wskazane wyżej kody PKD. Do realizacji badania posłużyła baza firm pobrana z operatu badawczego BISNODE w dniu 30 września 2021 r. Cała próba była traktowana jako baza podstawowa ze względu na zastosowanie próby wyczerpującej oraz liczbę podmiotów w rzeczywistości działających na rynku. Starano się jednocześnie uwzględnić podział próby pod względem: wielkości firm oraz makroregionów. Z każdą firmą w próbie skontaktowano się minimum jeden raz.

Badania ilościowe zrealizowano w terminie od 7 do 27 października 2021 r.

Badanie pracodawców:
Wywiady były realizowane z osobami dysponującymi najbardziej obszerną wiedzą na temat polityki personalnej firmy, w tym w szczególności działań rekrutacyjnych oraz oceny kompetencji pracowników. Łącznie przeprowadzono 800 wywiadów.

[12] Zarówno w badaniu pracodawców, jak i w badaniu pracowników ok. 74% wywiadów zrealizowano metodą CAPI, a ok. 26% wywiadów metodą CATI.

Tabela 1. Rozkład liczebności zrealizowanej próby w badaniu pracodawców w podziale na sekcje/działy PKD i wielkość firmy

Sekcja/dział PKD	Mikro (2–9 pracowników)	Mała (10–49 pracowników)	Średnia (50–249 pracowników)	Duża (250+ pracowników)	Ogółem
Sekcja J: 61.1[13]	281	118	20	4	423
Sekcja J: 61.2, 61.3, 61.9[14]	169	75	14	4	262
Sekcja J: 62.03.Z[15]	77	27	11	0	115
Razem	527	220	45	8	800

Źródło: opracowanie własne.

Badanie pracowników:

Wywiady były przeprowadzane z pracownikami zatrudnionymi na jednym z 12 kluczowych stanowisk w następującym podziale: 5 stanowisk w sektorze telekomunikacji, 6 stanowisk w sektorze cyberbezpieczeństwa oraz 1 stanowisko uniwersalne. Stanowiska zostały zdefiniowane na podstawie wyników przeprowadzonego wcześniej badania jakościowego oraz ustaleń z Zamawiającym. Łącznie przeprowadzono 965 wywiadów[16].

[13] Działalność w zakresie telekomunikacji przewodowej.

[14] 61.2 – Działalność w zakresie telekomunikacji bezprzewodowej, z wyłączeniem telekomunikacji satelitarnej; 61.3 – Działalność w zakresie telekomunikacji satelitarnej oraz 61.9 – Działalność w zakresie pozostałej telekomunikacji.

[15] Działalność związana z zarządzaniem urządzeniami informatycznymi.

[16] W badaniu zastosowano tzw. reprezentatywność typologiczną oznaczającą, że każdy typ pracownika/kluczowe stanowisko (zgodne/y z profilem kompetencyjnym) jest w próbie reprezentowany.

Tabela 2. Rozkład liczebności próby w badaniu pracowników pod względem zajmowanego stanowiska i płci

Stanowisko (sektor)	Mężczyzna	Kobieta	Ogółem
Architekt systemów (Telekomunikacja)	72	17	89
Inżynier (każdej specjalizacji) (Telekomunikacja)	165	22	187
Developer (programista) (Telekomunikacja)	190	28	218
Project Manager (kierownik projektu) (Telekomunikacja)	54	25	79
Quality Assurance (tester) (Telekomunikacja)	66	24	90
CISO (Chief Information Security Officer) (Cyberbezpieczeństwo)	21	7	28
Audytor bezpieczeństwa (Cyberbezpieczeństwo)	22	7	29
Architekt ds. bezpieczeństwa (Cyberbezpieczeństwo)	20	4	24
Penetration tester (tester penetracyjny) (Cyberbezpieczeństwo)	6	4	10
Koordynator SOC (Security Operation Center) (Cyberbezpieczeństwo)	12	8	20
Ekspert ds. bezpieczeństwa systemów/sieci/aplikacji (Cyberbezpieczeństwo)	34	3	37
Dyrektor handlowy (Stanowisko uniwersalne)	106	48	154
Razem	768	197	965

Źródło: opracowanie własne.

W tabelach i na wykresach opracowanych na podstawie badań ilościowych wyniki procentowe nie zawsze sumują się do 100%, co – o ile nie zaznaczono inaczej – jest konsekwencją ważenia danych, zaokrągleń lub możliwości wskazania wielu odpowiedzi.

2. Opis sytuacji w branży telekomunikacji i cyberbezpieczeństwa

Sektor telekomunikacji i sektor cyberbezpieczeństwa to dwa uzupełniające się sektory będące jednak na różnym stopniu rozwoju – zarówno jeżeli chodzi o liczbę firm działających na rynku, jak i oferowane usługi. Podczas gdy rynek telekomunikacji wydaje się rynkiem dojrzałym (z tego względu w obliczu wyczerpujących się możliwości wzrostu, poszukuje się na nim stale nowych modeli generowania zysków[17]), to cyberbezpieczeństwo jest wciąż w fazie wzrostu.

Firmy działające w obszarze telekomunikacji operują w ramach pięciu głównych segmentów rynku: telefonii komórkowej[18], telefonii stacjonarnej, stacjonarnego dostępu do Internetu[19], transmisji danych oraz płatnej telewizji[20], a zakres ich działań obejmuje szereg zadań – od projektowania infrastruktury fizycznej, przez jej obsługę (przy wykorzystaniu odpowiednio przygotowanych do tego celu programów i systemów) do koordynacji i utrzymania (w celu zachowania ciągłości działania systemów czy sieci). Aby zadania w obszarze telekomunikacyjnym realizowane były sprawnie, ważne jest zapewnienie ochrony zarówno samych sieci informatycznych, jak i urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem, czym zajmuje się cyberbezpieczeństwo[21]. Firmy działające w obszarze cyberbezpieczeństwa realizują zadania w zakresie: projektowania, tworzenia, wdrażania rozwiązań związanych z zapewnieniem bezpieczeństwa

17 https://www.ict2020.pl/uploads/1/2/1/5/121555005/raport_piit_stan_rynku_it_i_telekomunikacyjnego.pdf, s.19-20; (dostęp: 18.01.2020).

18 W tym mobilny dostęp do internetu (nie tylko w formie pakietów danych w telefonach komórkowych, ale też dostarczany za pomocą urządzeń mobilnych służących jako punkty tetheringowe).

19 W tym m.in. połączenia światłowodowe, internet kablowy, telefoniczne łącze przewodowe.

20 Analiza rynku telekomunikacyjnego w obszarze inwestycji MŚP w sieci szerokopasmowe. Raport dla Ministerstwa Cyfryzacji. Audytel, 2016, s. 32; (dostęp: 30.11.2021).

21 https://web.archive.org/web/20200408234425/ https://safebit.pl/czym-jest-cyberbezpieczenstwo/; (dostęp: 11.01.2022).

przesyłanym danym i użytkownikom w telekomunikacji przewodowej, bezprzewodowej i telekomunikacji satelitarnej[22].

Zgodnie z danymi GUS, na koniec września 2021 r. w branży telekomunikacji i cyberbezpieczeństwa[23] działało 15 438 firm, z czego zdecydowaną większość stanowiły firmy zatrudniające od 2 do 9 pracowników (nazywane dalej mikrofirmami) (tabela 3).

Tabela 3. Liczba firm w populacji pod względem typu (sekcja/dział PKD) i wielkości podmiotu

Sekcja/dział PKD	Mikro (2–9 pracowników)	Mały (10–49 pracowników)	Średni (50–249 pracowników)	Duży (250+ pracowników)	Ogółem
Telekomunikacja przewodowa (J: 61.1)	4 120	179	22	5	4 326
Telekomunikacja inna niż przewodowa (J: 61.2, 61.3, 61.9)	4 099	101	15	5	4 220
Zarządzanie urządzeniami informatycznymi[24] (J: 62.03.Z)	6 836	46	10	0	6 892
RAZEM	15 055	326	47	10	15 438

Źródło: opracowanie własne na podstawie danych GUS, stan na 30.09.2021.

Liczba osób zatrudnionych w sektorze telekomunikacji oscyluje w okolicach 42–43 tysięcy (tabela 4). Brak jest natomiast podobnych, jednoznacznie określonych danych dla sektora cyberbezpieczeństwa. Trudno ocenić skalę zatrudnienia w tym sektorze, ale przypuszcza się, że część wakatów (według szacunków ekspertów, w sektorze cyberbezpieczeństwa jest

[22] Cyberbezpieczeństwo (zarówno globalnie, jak i w Unii Europejskiej) stało się w ciągu ostatniej dekady (lata 2010–2020) priorytetem (i znaczącym obszarem inwestycyjnym) dla rządów, przedsiębiorstw i obywateli: zmniejsza się liczba wycieków danych (o 27% w ciągu roku) oraz bezpośrednich ataków (o 11%). [za:] Bissell K., Lasalle R.M., Dal Cin P., *Innovate for Cyber Resilience. Lessons from Leaders to master cybersecurity execution*, *Accenture Security*, [w:] https://www.accenture.com/us-en/insights/security/invest-cyber-resilience; (dostęp: 11.01.2022).

[23] Definiowanej przez następujące kody z klasyfikacji PKD: Działalność w zakresie telekomunikacji przewodowej (sekcja J.61.1), Działalność w zakresie telekomunikacji innej niż przewodowa (w tym bezprzewodowa i satelitarna) (sekcje J.61.2, 61.3 oraz 61.9), Działalność związana z zarządzaniem urządzeniami informatycznymi (sekcja J.62.03.Z).

[24] Wyłącznie firmy z sektora cyberbezpieczeństwa.

ok. 17,5 tysiąca wolnych stanowisk[25]) zostanie obsadzonych niekoniecznie na drodze nowych rekrutacji, ale dzięki inwestycji w podnoszenie kompetencji już zatrudnionych pracowników z działów IT.

Tabela 4. Liczba pracujących w sektorze telekomunikacji

Rok	2015	2016	2017	2018	2019	2020	2021	2022	2023
Liczba pracujących	39 785	42 336	42 061	43 235	41 685	43 603	42 687	44 266	43 004
Zmiana w stosunku do poprzedniego roku		106,4%	99,4%	102,8%	96,4%	104,6%	97,9%	103,7%	97,1%

Źródło: Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2015–2019, GUS, s. 30; Społeczeństwo informacyjne w Polsce w 2020 r., GUS, s. 30. W ramce zamieszczono średnioterminową prognozę czystą na kolejne lata[26].

Analiza wielkości sprzedaży w sektorze telekomunikacji wskazuje, że w 2019 r. wartość ta osiągała poziom ok. 41,5 mld złotych. Wielkość sprzedaży stale wzrastająca do 2018 r., w 2019 r. odnotowała niewielki spadek wartości (tabela 5).

Tabela 5. Przychody netto ze sprzedaży produktów i usług w sektorze ICT (telekomunikacja)

Rok	2015	2016	2017	2018	2019
Sprzedaż (w mln zł)	40 425,0	40 822,3	41 417,9	41 586,3	41 560,1

Źródło: Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2015–2019, GUS, s. 31; Społeczeństwo informacyjne w Polsce w 2020 r., GUS, s. 31.

Obserwowana w czasie pandemii COVID-19 zmiana sposobu prowadzenia działalności wynikająca z wprowadzonych przepisów, dała firmom m.in. szersze możliwości pracy zdalnej. W rezultacie, w 2021 r. ponad trzykrotnie (w stosunku do 2020 r.) zwiększyła się liczba pracowników zdalnych w skali globalnej, a dwukrotnie w Polsce[27]. Zdania przedsiębiorców odnośnie zmian związanych z trwającą pandemią są podzielone.

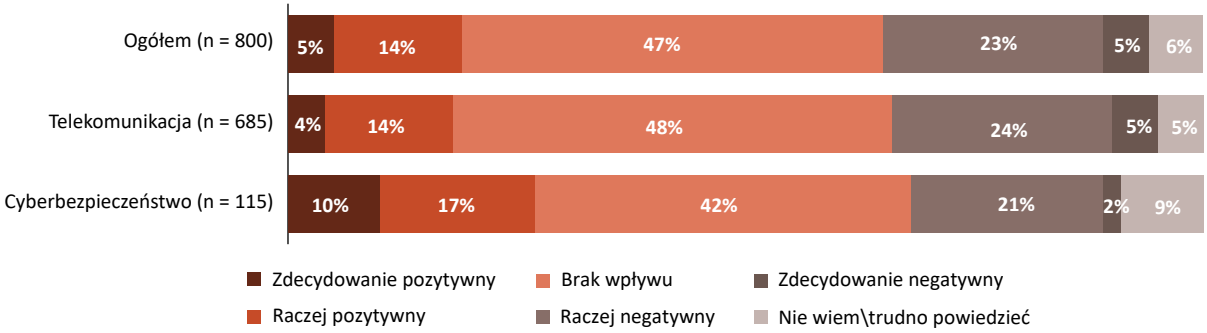
[25] Cybersecurity. Raport o rynku pracy w Polsce [za:] https://biznes.newseria.pl/news/na-rynku-brakuje,p1514763928; (dostęp: 12.01.2022).

[26] Prognoza została wygenerowana w oparciu o analizę zjawiska poprzez ekstrapolację danych na kolejne lata, do 2023 roku z zachowaniem cykliczności analiz.

[27] http://www.it-professional.pl/bezpieczenstwo/artykul,9283,cyberbezpieczenstwo-w-dobie-pandemii.html; (dostęp: 12.01.2022).

Niemal połowa przedsiębiorców z sektora telekomunikacji oraz ponad 40% przedsiębiorców reprezentujących sektor cyberbezpieczeństwa uważa, że pandemia nie miała znaczącego wpływu na sytuację w branży. Większość jednak dostrzegła pewne zmiany[28]. Spośród przedsiębiorców, którzy zauważyli wpływ pandemii COVID-19 na działanie firm, dominowali tacy, dla których był on negatywny (to zdanie 23% przedsiębiorców z sektora cyberbezpieczeństwa oraz 29% badanych z sektora telekomunikacji). Jednak wśród respondentów byli też tacy, którzy mimo pandemii zauważyli poprawę sytuacji firmy – taką opinię wyraziło 27% pracodawców z sektora cyberbezpieczeństwa i 18% badanych pracodawców z sektora telekomunikacji (wykres 1).

Wykres 1. Wpływ pandemii COVID-19 na działalność przedsiębiorstw (ogółem oraz w podziale na sektory)

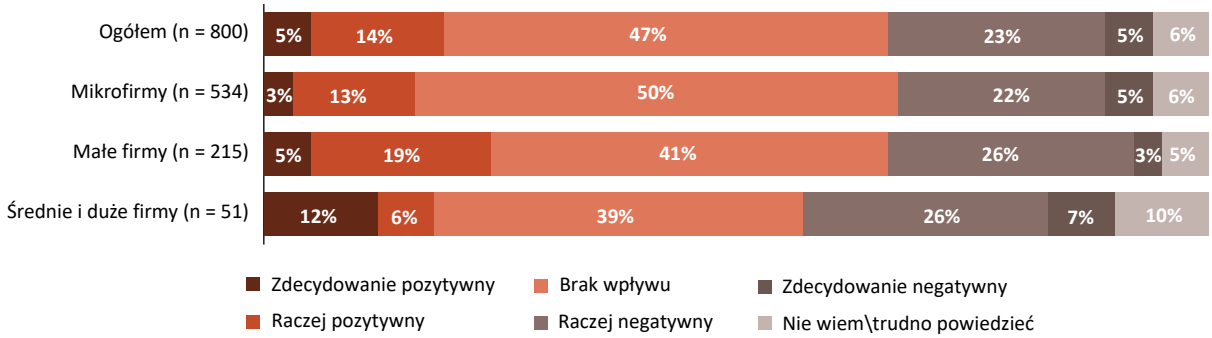


Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Zróżnicowanie wpływu pandemii jest widoczne przy uwzględnieniu rozkładu odpowiedzi ze względu na wielkość firm reprezentowanych przez badanych respondentów (wykres 2). Największy udział firm, w których dostrzeżono pozytywny wpływ pandemii na działanie przedsiębiorstw zaobserwowano wśród małych firm (24% wskazań), a negatywny – w przypadku średnich i dużych firm (33% wskazań). Branża telekomunikacji i cyberbezpieczeństwa jest branżą, w przypadku której częściej dostrzegano pozytywny wpływ pandemii niż w innych branżach badanych w ramach projektu BBKL.

[28] Określenie pozytywnego bądź negatywnego wpływu oparte jest o sumy odpowiedzi „zdecydowanie pozytywny”/„zdecydowanie negatywny” oraz „raczej pozytywny”/„raczej negatywny”.

Wykres 2. Wpływ pandemii COVID-19 na działalność przedsiębiorstw (ogółem oraz w podziale ze względu na wielkość firmy)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Do najistotniejszych problemów przedsiębiorców prowadzących swoją działalność w branży telekomunikacji i cyberbezpieczeństwa (niezależnie od sektora) należy zaliczyć kwestie związane ze wzrostem kosztów funkcjonowania firm (75% wskazań w sektorze telekomunikacji i 80% w sektorze cyberbezpieczeństwa) oraz z koniecznością dostosowania procedur firm do wymogów bezpieczeństwa i higieny w związku z zagrożeniem epidemiologicznym (kolejno wg sektorów: 67% i 81%). Biorąc pod uwagę sektor telekomunikacji, trzecią w kolejności barierą – wskazywaną przez 65% badanych pracodawców – były braki kadrowe wynikające z przebywania pracowników na kwarantannie, natomiast w sektorze cyberbezpieczeństwa – zagrożenie zdrowotne pracowników z uwagi na potencjalną możliwość zachorowania na COVID-19 (66% odpowiedzi) (tabela 6).

Przeciążenie pracą wśród pracowników – negatywna zmiana najrzadziej wskazywana przez pracodawców z sektora telekomunikacji – relatywnie często było zauważane przez pracodawców z sektora cyberbezpieczeństwa (co drugi przedsiębiorca wskazywał na ten aspekt). Jednocześnie niewielu (co czwarty pracodawca z tego sektora) deklarowało narażenie pracowników na długotrwały, silny stres.

Tabela 6. Negatywne zmiany wywołane przez pandemię COVID-19 w firmach z sektorów: telekomunikacja (N = 685) i cyberbezpieczeństwo (N = 115)

Negatywne zmiany	Telekomunikacja	Cyberbezpieczeństwo	Ogółem*
Wzrost kosztów funkcjonowania firmy	75%	80%	77%
Dostosowanie procedur firmy do wymogów bezpieczeństwa i higieny w związku z COVID-19	67%	81%	74%
Zagrożenie zdrowotne dla pracowników (narażenia na zachorowanie na COVID-19)	62%	66%	64%
Braki kadrowe wynikające z przebywania pracowników na kwarantannie	65%	55%	60%
Problemy z dostawcami/problemy z dostawą sprzętu i materiałów	47%	63%	55%
Zachwianie płynności finansowej	55%	42%	49%
Braki kadrowe spowodowane przez absencję, niezwiązane z opieką nad dzieckiem i kwarantanną	52%	44%	48%
Braki kadrowe spowodowane przez absencję pracowników w związku z koniecznością opieki nad dzieckiem	48%	42%	45%
Ograniczenie inwestycji	39%	49%	44%
Przeciążenie pracą wśród pracowników	36%	52%	44%
Trudniejszy dostęp do specjalistów i wykwalifikowanych pracowników	36%	45%	40%
Problemy z dostawcami usług zewnętrznych (np. catering, transport)	38%	40%	39%
Narażenie pracowników na długotrwały, silny stres	48%	27%	37%
Konieczność wprowadzenia zmianowego czasu pracy	40%	33%	36%

*Sortowanie po ogóle odpowiedzi.

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Niezależnie od sektora, najbardziej znaczącymi pozytywnie ocenianym aspektami wynikającymi z sytuacji pandemii były: wzrost liczby świadczonych usług (56% odpowiedzi w sektorze telekomunikacji i 78% w sektorze cyberbezpieczeństwa) oraz nawiązanie współpracy z nowymi partnerami biznesowymi (kolejno wg sektorów: 50% i 61%). Należy podkreślić, że wielu pracowników z branży telekomunikacji i cyberbezpieczeństwa ma możliwość wykonywania swoich obowiązków służbowych w sposób zdalny, dlatego też powszechne wprowadzenie pracy zdalnej zostało wysoko ocenione przez respondentów reprezentujących oba sektory (kolejno: 54% i 58% wskazań) (tabela 7).

Pozytywnymi zmianami relatywnie rzadziej wskazywanymi przez przedsiębiorców były: nabycie umiejętności działania w sytuacji kryzysowej oraz łatwiejszy dostęp do wykwalifikowanych pracowników (kolejno: 32% i 29% w sektorze telekomunikacji i kolejno: 40% i 39% w sektorze cyberbezpieczeństwa).

Tabela 7. Pozytywne zmiany wywołane przez pandemię COVID-19 w firmach z sektorów: telekomunikacja (N = 685) i cyberbezpieczeństwo (N = 115)[29]

Pozytywne zmiany	Telekomunikacja	Cyberbezpieczeństwo	Ogółem*
Wzrost liczby świadczonych usług	56%	78%	67%
Wprowadzenie pracy zdalnej	54%	58%	56%
Pozyskanie nowych partnerów do współpracy	50%	61%	56%
Zmniejszenie kosztów utrzymania firmy	43%	56%	50%
Poszerzenie oferty (wprowadzenie nowych usług)	42%	51%	47%
Wzrost inwestycji	41%	49%	45%
Wzrost efektywności pracowników	44%	45%	44%
Uzyskanie przez pracowników nowych umiejętności	36%	47%	42%
Uruchomienie/intensyfikacja pracy zdalnej[30]	23%	52%	38%
Nabycie/przetestowanie umiejętności działania w sytuacji kryzysowej	32%	40%	36%
Łatwiejszy dostęp do wykwalifikowanych pracowników	29%	39%	31%

*Sortowanie po ogóle odpowiedzi.

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Ten pozytywny wpływ komunikowali już w trakcie wywiadów jakościowych oraz paneli eksperckich respondenci, mówiąc o tym, że dla niektórych firm pandemia stanowiła nawet czynnik zwiększający popyt na oferowane produkty czy usługi. Dla sektora telekomunikacji można mówić o zwiększonym zapotrzebowaniu na sprzęt elektroniczny (np. mikrofony,

[29] Odpowiedzi „uruchomienie pracy zdalnej" oraz „wprowadzenie pracy zdalnej" należy traktować z dużą ostrożnością. W założeniu, „wprowadzenie pracy zdalnej" rozumiane było jako umożliwienie w firmie takiego typu pracy, ale jeszcze bez jej rzeczywistego wykonywania czy narzucania. Natomiast odpowiedź „uruchomienie pracy zdalnej" to już jej rzeczywiste wykonywanie. W toku badania ustalono, że w niektórych przypadkach respondenci mieli problem z udzieleniem odpowiedzi zgodnie z założeniem.

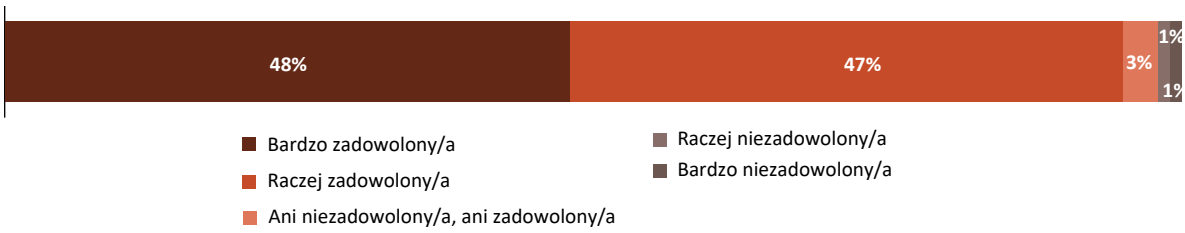
[30] Duża rozbieżność w przypadku tej kategorii wynika z faktu wykonywania w telekomunikacji pewnych zadań poza biurem firmy, zatem – w przeciwieństwie do cyberbezpieczeństwa – zwiększenie udziału pracy zdalnej w tej branży nie było tak duże.

kamery), jak również na usługi (np. dostęp do Internetu lub zwiększenie aktualnej przepustowości łącza ze względu na zwiększenie się liczby użytkowników przypadających na jedno gospodarstwo domowe, zawieranie przez klientów nowych umów zapewniających otrzymanie sprzętu elektronicznego takiego jak smartfony, laptopy). Te ruchy konsumentów miały przełożenie na sektor cyberbezpieczeństwa. Wzmożony ruch sieciowy oraz przeniesienie niektórych sfer życia (jak nauka czy praca) do świata online to czynniki, które wymusiły – ze względu na wzrost liczby incydentów związanych z cyfrową przestępczością – intensyfikację działań firm z sektora cyberbezpieczeństwa.

3. Ocena pracowników dotycząca warunków pracy w branży

Zdecydowana większość pracowników zatrudnionych na kluczowych stanowiskach jest zadowolona[31] **z wykonywanej pracy. Takiej odpowiedzi udzieliło 95% badanych pracowników.** Jedynie 2% respondentów zadeklarowało brak zadowolenia ze swojej pracy (wykres 3).

Wykres 3. Zadowolenie pracowników zatrudnionych na kluczowych stanowiskach z wykonywanej pracy (N = 965)

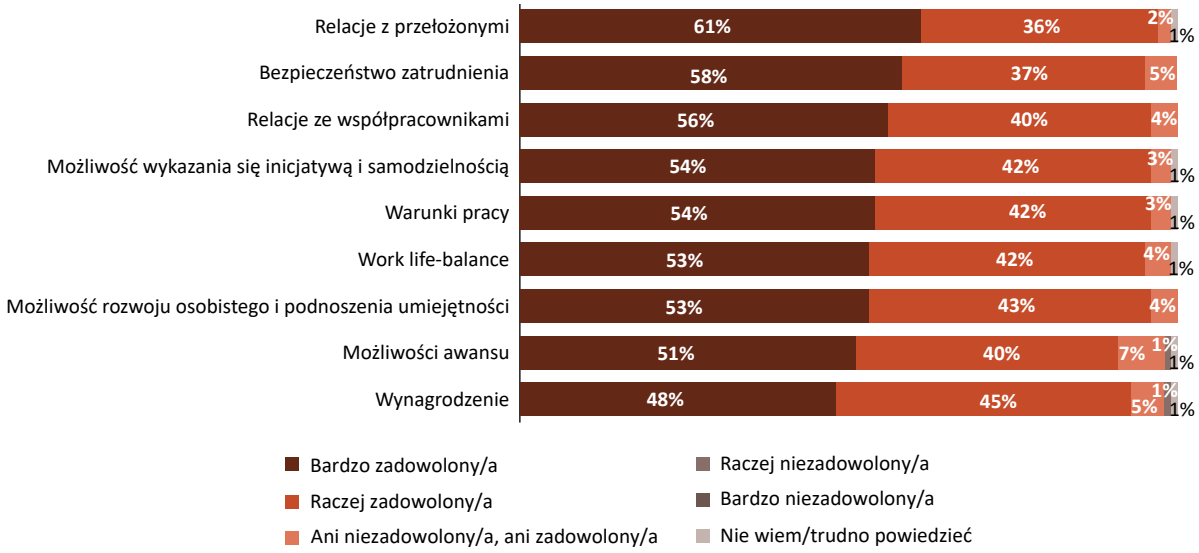


Źródło: opracowanie własne na podstawie wyników badania ilościowego pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Każdy wyszczególniony aspekt zadowolenia z pracy jest wysoko oceniany przez uczestników badania (wykres 4). Zróżnicowanie w odpowiedziach pomiędzy poszczególnymi wymiarami jest niewielkie (maksymalna różnica to 6 p.p.). Badani pracownicy najwyżej oceniali relacje z przełożonymi (97%), relacje ze współpracownikami, możliwość wykazania się inicjatywą i samodzielnością oraz warunki pracy (po 96%).

[31] Określenie zadowolenia bądź braku zadowolenia oparte jest na sumach odpowiedzi „bardzo zadowolony”/„bardzo niezadowolony” oraz „raczej zadowolony”/„raczej niezadowolony”.

Wykres 4. Zadowolenie pracowników z wykonywanej pracy w oparciu o wybrane aspekty (N = 965)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Ogólny poziom zadowolenia pracowników zatrudnionych na kluczowych stanowiskach z wykonywanej pracy jest wynikiem pozytywnej oceny różnych czynników związanych z ogólnymi warunkami pracy w branży. Badani pracownicy branży telekomunikacja i cyberbezpieczeństwo ocenili bardzo wysoko[32] aż 13 na 21 poszczególnych aspektów pracy w branży (tabela 8). Najwyżej oceniono: dobrą atmosferę panującą w miejscu pracy, wysoki poziom umiejętności współpracowników (odpowiedzi otrzymały po 97% wskazań) oraz dostęp do odpowiednich narzędzi/sprzętu do wykonywania pracy (96% wskazań).
Warto podkreślić, że problem związany ze zbyt dużą liczbą obowiązków zawodowych zadeklarowało ponad 60% badanych pracowników, a blisko 60% rozmówców, że w ramach obowiązków służbowych, często wykonują oni zadania, które są zbyt trudne albo zbyt proste w stosunku do posiadanych przez nich umiejętności. Niewiele ponad 50% respondentów wskazało również, że często brakuje im odpowiedniej wiedzy lub umiejętności, które umożliwiłyby poprawną realizację zadań zawodowych przypisanych do ich stanowiska.

[32] W analizie wzięto pod uwagę aspekty, w przypadku których suma odpowiedzi „zdecydowanie się zgadzam" oraz „raczej się zgadzam" wynosiła ponad 80%.

Najrzadziej zgadzano się ze stwierdzeniami o negatywnym wpływie pracy na zdrowie pracowników (39%) oraz o braku czasu na życie rodzinne (43%). Można zaryzykować stwierdzenie, że według większości badanych wykonywana praca nie wpływa niekorzystnie na powyższe sfery.

Tabela 8. Ocena pracowników dotycząca warunków pracy w branży (N = 965)

Warunki pracy	Zdecydowanie się zgadzam	Raczej się zgadzam	Raczej się nie zgadzam	Zdecydowanie się nie zgadzam	Nie wiem/trudno powiedzieć
W moim miejscu pracy panuje dobra atmosfera	59%	38%	3%	0%	0%
Mam zapewnione odpowiednie narzędzia/sprzęt do wykonywania mojej pracy	57%	39%	3%	1%	0%
W mojej pracy czuję się bezpiecznie	57%	36%	5%	2%	0%
Osoby, z którymi współpracuję, są dobre w tym, co robią	56%	41%	3%	0%	0%
Mam możliwość realizacji swoich własnych pomysłów	56%	38%	5%	1%	0%
Czuję, że w pracy wykorzystuję swoją wiedzę i umiejętności	56%	38%	4%	1%	1%
W pracy robię to, co lubię	55%	33%	8%	4%	0%
Czuję, że praca, którą wykonuję, ma sens	55%	33%	9%	3%	0%
W razie potrzeby mam możliwość zrobienia krótkiej przerwy w pracy	52%	43%	4%	1%	0%
Dzięki pracy ciągle uczę się nowych rzeczy	47%	47%	5%	1%	0%
Mogę sam decydować o organizacji mojego dnia pracy	45%	46%	8%	1%	0%
Każdego dnia w mojej pracy wykonuję podobne zadania	41%	42%	15%	2%	0%
Moja praca wymaga ciągłego dokształcania się	38%	51%	9%	2%	0%
Często muszę wykonywać zadania, które są zbyt trudne w stosunku do moich umiejętności	31%	27%	23%	19%	0%
Mam zbyt dużo zadań, by dobrze wykonać je na czas	31%	31%	28%	9%	0%
Często muszę wykonywać zadania, które są zbyt proste w stosunku do moich umiejętności	27%	31%	23%	18%	1%

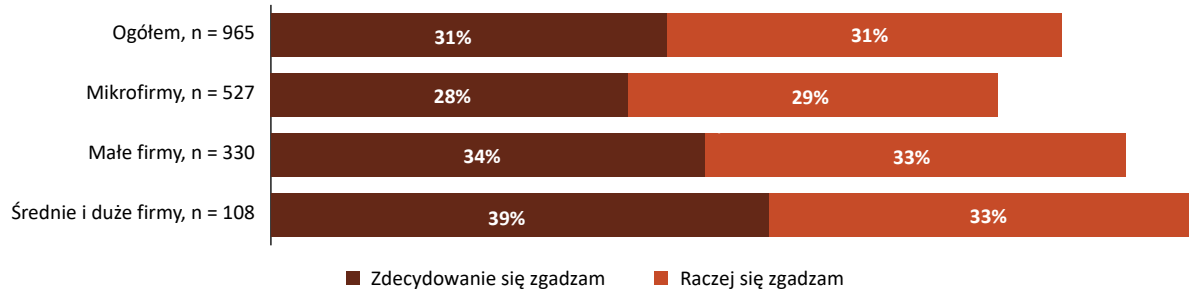
Warunki pracy	Zdecydowanie się zgadzam	Raczej się zgadzam	Raczej się nie zgadzam	Zdecydowanie się nie zgadzam	Nie wiem/trudno powiedzieć
Czasem zauważam, że brakuje mi wiedzy lub umiejętności, by dobrze wykonać zadania, które mam zrealizować w pracy	25%	26%	30%	18%	1%
Często czuję się zbyt zmęczony/a po pracy, żeby zająć się pracami domowymi	25%	22%	28%	24%	1%
Wskutek nadmiaru pracy nie mam zbyt wiele czasu na rozrywkę i kontakty ze znajomymi	22%	24%	28%	26%	0%
Moja praca uniemożliwia mi poświęcanie rodzinie tyle czasu, ile bym chciał(a)	21%	22%	31%	26%	0%
Czuję, że praca ma negatywny wpływ na moje zdrowie	20%	19%	30%	31%	0%

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Analiza na poziomie sektorów pokazała, że pracownicy zatrudnieni na kluczowych stanowiskach w sektorze cyberbezpieczeństwa mają mniejszą możliwość podejmowania decyzji o organizacji swojego dnia pracy w porównaniu do badanych pracujących w sektorze telekomunikacji (81% vs. 93% wskazań odpowiedzi co najmniej „raczej się zgadzam").

Wskazana wyżej **ocena zjawiska związanego z otrzymywaniem zbyt dużej liczby zadań jest zróżnicowana w podziale ze względu na wielkość firmy, w której pracują badani. Z danych wynika, że wraz ze wzrostem wielkości firmy, pracownicy częściej wskazują na występowanie problemu związanego z nadmiarem obowiązków (wykres 5).** Odsetek dostrzegających ten problem rośnie od 57% w przypadku mikrofirm do 72% w przypadku średnich i dużych przedsiębiorstw.

Wykres 5. Ocena pracowników dotycząca przeciążenia zadaniami, które wpływa na możliwość wykonania ich odpowiednio dobrze w określonym czasie (ogółem i w podziale ze względu na wielkość firmy)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Niemal wszyscy respondenci przyznają, że przełożeni odnoszą się do nich z szacunkiem (wykres 6). Dodatkowo, również niemal wszyscy pracownicy są angażowani w podejmowanie decyzji, które mają wpływ na ich pracę. Zdecydowana większość pracowników (97%) deklaruje także, że ich praca jest sprawiedliwie oceniana.

Wykres 6. Ocena wybranych aspektów dotyczących relacji pracowników z przełożonymi (N = 965)

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

4. Główne procesy biznesowe w branży i zatrudnienie osób na kluczowych stanowiskach

Na podstawie badań jakościowych (wywiadów indywidualnych i paneli eksperckich) zidentyfikowane zostały główne procesy biznesowe w branży telekomunikacji i cyberbezpieczeństwa. Jako proces biznesowy rozumieć należy zestaw powiązanych ze sobą zadań, które prowadzą do osiągnięcia zaplanowanego efektu.

4.1. Sektor telekomunikacji

Wymienione poniżej główne procesy biznesowe odnoszą się do wszystkich podobszarów telekomunikacji, tj. specjalizacji przewodowej, bezprzewodowej i satelitarnej. W każdym z tych podobszarów występują tożsame procesy związane z samym projektowaniem infrastruktury fizycznej, którą następnie należy obsłużyć, wykorzystując odpowiednio przygotowane do tego celu programy i systemy. W każdej podkategorii występuje również proces koordynacji i utrzymania, dzięki któremu zapewniana jest ciągłość działania systemów czy sieci.

4.1.1. Proces tworzenia oprogramowania, systemów, programów i aplikacji

Proces ten dotyczy tworzenia oprogramowania i systemów umożliwiających obsługę pasywnej infrastruktury oraz urządzeń elektronicznych takich jak telefony, modemy, dekodery itp. Każde wymienione urządzenie, czy też konkretny element infrastruktury telekomunikacyjnej do prawidłowej obsługi potrzebuje specjalnego systemu (software), dzięki któremu możliwe staje się sterowanie i użytkowanie urządzenia. Wytwarzane oprogramowanie można podzielić na takie, które będzie obsługiwane przez specjalistów (np. osoby odpowiedzialne za sterowanie systemem integracji infrastruktury

telekomunikacyjnej takiej jak anteny, stacje bazowe) oraz takie, które będzie przeznaczone dla użytkowników prywatnych (np. programy do konfiguracji sprzętu elektronicznego, aplikacje mobilne, interfejsy urządzeń).

Zadania zawodowe, które są realizowane w tym procesie, to: (a) tworzenie spójnej i logicznej architektury informacyjnej w systemach/programach, (b) ustalanie najlepszej możliwej drogi (wykorzystywanych narzędzi, technologii, sposobów osiągnięcia ustalonych w projekcie założeń) dopasowanej do konkretnego zadania w celu osiągnięcia założonych efektów, (c) programowanie (pisanie kodu) systemów, programów i aplikacji najczęściej związanych z obsługą konkretnych sprzętów elektronicznych, (d) przeprowadzanie testów manualnych i automatycznych, (e) wyszukiwanie błędów w działaniu systemu, programu, usługi oraz (f) poprawa projektowanych systemów i usług pod względem ich użyteczności.

Kluczowe stanowiska odpowiedzialne za realizację zadań w tym procesie biznesowym to: architekt systemów, developer (programista) oraz quality assurance (tester).

4.1.2. Proces projektowania infrastruktury telekomunikacyjnej oraz urządzeń

Proces ten polega na tworzeniu projektów pasywnej infrastruktury, np. stacji bazowych, anten, przekaźników, ale także wszelkiego rodzaju urządzeń elektronicznych jak telefony, modemy. Wewnątrz projektu powinny znaleźć się informacje dotyczące ilości oraz rodzaju potrzebnych do wykonania produktu materiałów. W infrastrukturze pasywnej kluczowe jest również uwzględnienie jakie narzędzia, maszyny oraz jak liczna kadra i o jakich specyficznych umiejętnościach będzie potrzebna do realizacji prac montażowych. Jednym z efektów procesu projektowego jest stworzenie szczegółowej dokumentacji technicznej opisującej każdy aspekt projektu.

Zadania zawodowe, które są realizowane w tym procesie, to: (a) projektowanie sieci przewodowych i bezprzewodowych, (b) tworzenie dokumentacji, (c) praca przy modernizowaniu infrastruktury telekomunikacyjnej oraz (d) konfiguracja urządzeń.

Kluczowe stanowisko odpowiedzialne za realizację zadań w tym procesie biznesowym to inżynier (każdej specjalizacji).

4.1.3. Proces koordynacji usług i utrzymania infrastruktury telekomunikacyjnej

W tym procesie wyróżnia się działania związane z naprawą, modernizacją oraz zapewnieniem nieprzerwanego działania stacji bazowych, anten i innych urządzeń (a także programów oraz usług wykupionych przez klientów) umożliwiających dostęp do sieci telefonicznej, Internetu, sygnału telewizyjnego itd.

Infrastruktura telekomunikacyjna opiera się na poprawnym działaniu anten, przekaźników i innych urządzeń, które zapewniają tzw. ciągłość emisji. Wraz z upływem czasu i rozwojem nowych technologii, które charakteryzują się szybszym działaniem, lepszą jakością sygnału oraz zwiększoną przepustowością, pojawia się potrzeba modernizowania aktualnej infrastruktury bądź budowanie nowej, np. przy wykorzystaniu technologii 5G. Ważnym zadaniem wewnątrz procesu jest także zapewnienie kompatybilności starych elementów infrastruktury z nowymi.

Zadania zawodowe, które są realizowane w tym procesie, to: (a) dbanie o wyniki projektu (operacyjne, finansowe), (b) wdrażanie odpowiedniego sposobu realizacji do konkretnych projektów (z uwzględnieniem zasobów ludzkich, technologicznych), (c) tworzenie kosztorysów projektów we współpracy z działami pozyskania klienta, (d) utrzymywanie kontaktu z interesariuszami ze strony zamawiającego oraz (e) pomoc w przeprowadzaniu procesów rekrutacyjnych.

Kluczowe stanowisko odpowiedzialne za realizację zadań w tym procesie biznesowym to project manager (kierownik projektu).

4.2. Sektor cyberbezpieczeństwa

Główne procesy biznesowe w sektorze cyberbezpieczeństwa nie są linearne. To znaczy, że występowanie konkretnego procesu nie jest wymuszone występowaniem innego, poprzedzającego go procesu. Wymienione poniżej procesy są realizowane w konkretnych przedsiębiorstwach zgodnie z aktualnym zapotrzebowaniem bądź pojawieniem się niespodziewanego incydentu (jak np. atak hakerski, wykrycie podatności).

Etap badań jakościowych potwierdził, że działania związane z zapewnieniem bezpieczeństwa można podzielić na fizyczne i cyfrowe, a także na ofensywne i defensywne. Bezpieczeństwo fizyczne dotyczy dostępu do urządzeń, budynków, dokumentów oraz innych rzeczy, które mają charakter niecyfrowy, podczas gdy bezpieczeństwo cyfrowe dotyczy tworzenia cyfrowych zabezpieczeń systemów, programów, aplikacji. Działania ofensywne dotyczą prób przeprowadzania pozorowanych ataków na aktywa cyfrowe i niecyfrowe, w celu sprawdzenia podatności i niedokładności w zaprojektowanych zabezpieczeniach, natomiast działania defensywne dotyczą zadań związanych z zaprojektowaniem, modernizacją zabezpieczeń oraz utrzymaniem systemów. Prezentowany opis procesów uwzględnia te podziały.

4.2.1. Proces prowadzenia audytów bezpieczeństwa

W ramach tego procesu wyróżnia się działania związane z oceną infrastruktury, systemów czy też aplikacji pod względem spełnienia konkretnych założeń oraz norm bezpieczeństwa. Weryfikowanie założeń i norm może dotyczyć zarówno kwestii bezpieczeństwa cyfrowego, jak i bezpieczeństwa fizycznego. W Polsce najczęściej wykonywane są audyty na potrzeby wewnętrzne, które są związane z weryfikacją wcześniej ustalonych założeń danego systemu, programu lub aplikacji, a także audyty weryfikacyjne, sprawdzające spełnienie konkretnych norm i skutkujące uzyskaniem konkretnego certyfikatu np. ISO 9001, ISO/IEC 20000-1.

Zadania zawodowe, które są realizowane w tym procesie, to: (a) prowadzenie audytów w oparciu o standardy i normy bezpieczeństwa, (b) przeprowadzanie oceny zgodności firmy/systemu/produktu/usługi z konkretnymi standardami i normami bezpieczeństwa, (c) sporządzanie dokumentacji poaudytowej, (d) formułowanie rekomendacji dotyczących poprawy bezpieczeństwa oraz (e) pozorowanie faktycznych ataków cyfrowych, mających na celu kradzież informacji, sprawdzanie podatności systemów, testowanie dostępu do programów, usług, danych.

Kluczowe stanowiska odpowiedzialne za realizację zadań w tym procesie biznesowym to: audytor bezpieczeństwa oraz penetration tester (tester penetracyjny).

4.2.2. Proces ochrony aktywów/identyfikacji zagrożeń/analizy

Złożoność nazwy procesu wynika z różnorodności stosowanej nomenklatury w poszczególnych firmach, jednak najważniejszymi zadaniami wewnątrz tego procesu (znajdującymi odbicie w różnych sposobach nazewnictwa) są: potrzeba identyfikacji wszelkich dóbr, które znajdują się w firmie (urządzenia, dokumenty, aktywa cyfrowe itp.) oraz przemyślenie, czy konkretne zasoby są chronione w sposób wystarczający. Końcowym etapem jest opracowanie ewentualnych rekomendacji co do wprowadzenia usprawnień w stosowanych zabezpieczeniach. Zidentyfikowane zasoby mogą mieć charakter zarówno fizyczny, jak i cyfrowy, a sam proces zapewnienia ich ochrony należy do działań typowo defensywnych.

Zadania zawodowe, które są realizowane w tym procesie, to: (a) zarządzanie bezpieczeństwem aktywów firmowych, (b) tworzenie strategii bezpieczeństwa fizycznego, bezpieczeństwa informacji i bezpieczeństwa produktów cyfrowych (systemów, programów usług), (c) przyporządkowywanie i rozdzielanie zadań dla działów czy konkretnych zespołów, (d) ciągła współpraca z zespołem w celu weryfikacji bieżących problemów oraz (e) wspieranie realizacji celów biznesowych przedsiębiorstwa.

Kluczowe stanowisko odpowiedzialne za realizację zadań w tym procesie biznesowym to dyrektor ds. bezpieczeństwa informacji (CISO; Chief Information Security Officer).

4.2.3. Proces prewencji w celu zapewnienia bezpieczeństwa oraz obsługa incydentów

Proces prewencji dzieli się na dwie części. Po pierwsze, ważne jest monitorowanie systemów i sieci w celu wykrywania potencjalnych zagrożeń. Coraz częściej spotykane jest występowanie w przedsiębiorstwach specjalnych zespołów SOC (Security Operations Center), które zajmują się tymi czynnościami. Oczywiście rozpoznanie potencjalnych zagrożeń wymaga wiedzy dziedzinowej. Drugą częścią tego procesu jest obsługa incydentów, w której skład wchodzą czynności związane z zablokowaniem danego incydentu (jeżeli taki wystąpi), przywróceniem ładu oraz ewentualnymi działaniami mającymi na celu naprawę i wyciągnięcie wniosków na przyszłość.

Zadania zawodowe, które są realizowane w tym procesie, to: (a) tworzenie architektury systemów bezpieczeństwa, (b) zarządzanie systemami bezpieczeństwa, (c) tworzenie zabezpieczeń dla systemów, programów, usług, (d) monitorowanie systemów w celu wyszukiwania potencjalnych incydentów, (e) koordynacja zespołu SOC, w tym monitorowanie w trybie ciągłym poziomu cyberbezpieczeństwa, (f) obsługiwanie incydentów cyberataków, (g) uruchamianie procesów odtwarzania awaryjnego (lub innych zapewniających ciągłość działania systemu), (h) tworzenie dokumentacji z incydentów, (i) wdrażanie, rozwijanie i udoskonalanie standardów cyberbezpieczeństwa.

Kluczowe stanowiska odpowiedzialne za realizację zadań w tym procesie biznesowym to: architekt ds. bezpieczeństwa, koordynator SOC (Security Operations Center) oraz ekspert ds. bezpieczeństwa systemów/sieci/aplikacji.

4.3. Proces uniwersalny dla obu sektorów

Proces biznesowy, który jest uniwersalny dla wielu branż, w tym również dla branży telekomunikacji i cyberbezpieczeństwa, to proces związany ze sprzedażą oraz pozyskaniem klientów/kontraktów.

4.3.1 Proces sprzedaży/pozyskania klienta

W ramach tego procesu realizowane są zadania polegające na prowadzeniu rozmów z kontrahentami, prowadzeniu negocjacji oraz podpisywaniu umów na prowadzenie usług z branży telekomunikacji i cyberbezpieczeństwa. Celem procesu jest przede wszystkim znalezienie interesariuszy, którzy będą zainteresowani produktami niezależnie od tego, czy firma zajmuje się projektowaniem systemów, instalacjami infrastruktury pasywnej, czy też zapewnia bezpieczeństwo cyfrowe poprzez outsourcing zespołu SOC.

Zgodnie z wypowiedziami ekspertów, proces ten jest potrzebny w każdej organizacji z branży, ponieważ co prawda bez niego możliwe jest tworzenie rozwiązań i urządzeń, ale nie będzie możliwości ich sprzedaży, przez co działania projektowe staną się niepotrzebne. Wewnątrz procesu sprzedaży wyróżnia się także tworzenie strategii marketingowych.

Zadania zawodowe, które są realizowane w tym procesie, to: (a) pozyskiwanie nowych kontraktów i projektów dla firmy, (b) zarządzanie projektami, (c) analizowanie wymagań projektów, (d) prowadzenie negocjacji i rozmów z kontrahentami, (e) tworzenie kosztorysów oraz (f) ocena ofert konkurencji.

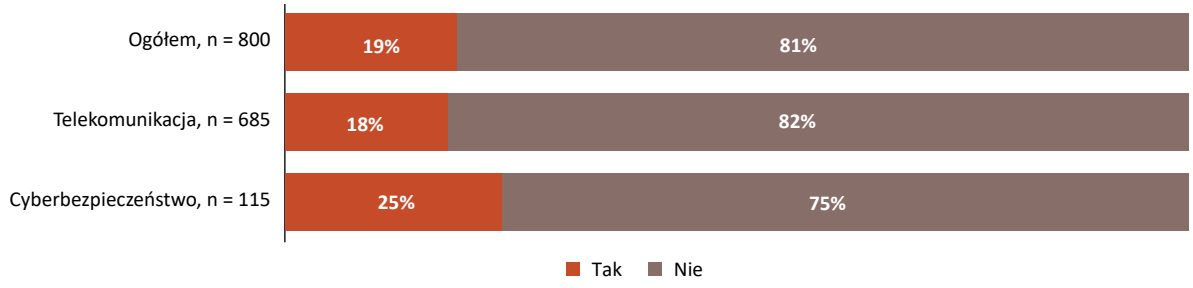
Kluczowe stanowisko odpowiedzialne za realizację zadań w tym procesie biznesowym to dyrektor handlowy/sprzedaży.

5. Zapotrzebowanie na pracowników w branży telekomunikacji i cyberbezpieczeństwa

W niemal co piątej firmie z branży poszukiwano nowych pracowników w ciągu 12 miesięcy poprzedzających badanie[33]. W sektorze cyberbezpieczeństwa odsetek ten wyniósł 25% i był wyższy o 7 p.p. w porównaniu z sektorem telekomunikacji (wykres 7).

Odsetek ten jest relatywnie wysoki w porównaniu do innych branż objętych badaniami BBKL. Nadal jednak przedsiębiorcy są znacznie bardziej zachowawczy w swoich opiniach niż eksperci branżowi, którzy wyrażali zdanie, że zapotrzebowanie na nowych pracowników w firmach z branży telekomunikacji i cyberbezpieczeństwa nieustannie rośnie.

Wykres 7. Poszukiwanie nowych pracowników w ciągu 12 miesięcy poprzedzających badanie przez pracodawców (ogółem i w podziale na sektory)

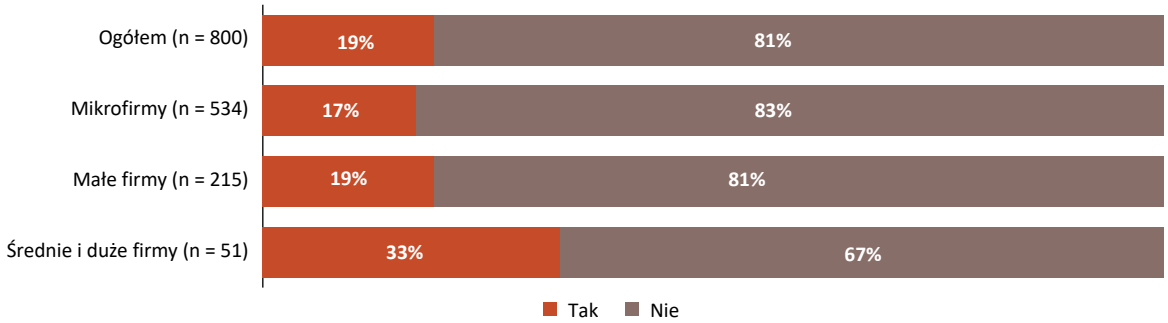


Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Zapotrzebowanie na nowych pracowników różni się w zależności od wielkości przedsiębiorstwa, które reprezentował pracodawca (wykres 8). W przypadku mikro i małych firm odsetek przedsiębiorców, którzy poszukiwali nowych pracowników, wahał się między 17% a 19%, natomiast w przypadku średnich i dużych firm osiągnął wartość 33%.

[33] Badanie przeprowadzono w październiku 2021 r.

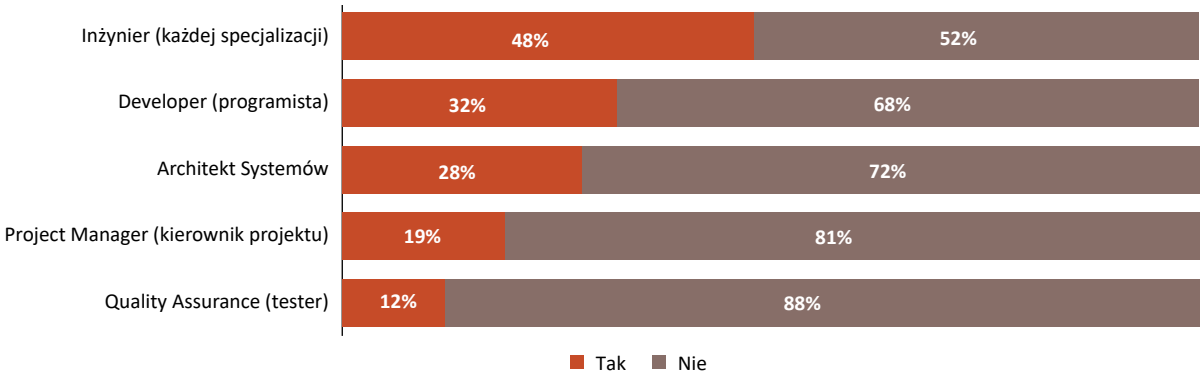
Wykres 8. Poszukiwanie nowych pracowników w ciągu 12 miesięcy poprzedzających badanie przez pracodawców (ogółem i w podziale ze względu na wielkość firmy)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Bardziej szczegółowa analiza pokazuje, że **w sektorze telekomunikacji pracodawcy najczęściej (48%) poszukiwali pracowników na stanowisko inżyniera (każdej specjalizacji) (wykres 9).** Duża liczba wskazań świadczy też o zapotrzebowaniu na stanowisko programisty (32% wskazań). Najrzadziej poszukiwanymi specjalistami w obrębie tego sektora są testerzy (12% wskazań).

Wykres 9. Zapotrzebowanie na nowych pracowników z sektora telekomunikacji – deklaracje pracodawców (N = 685)

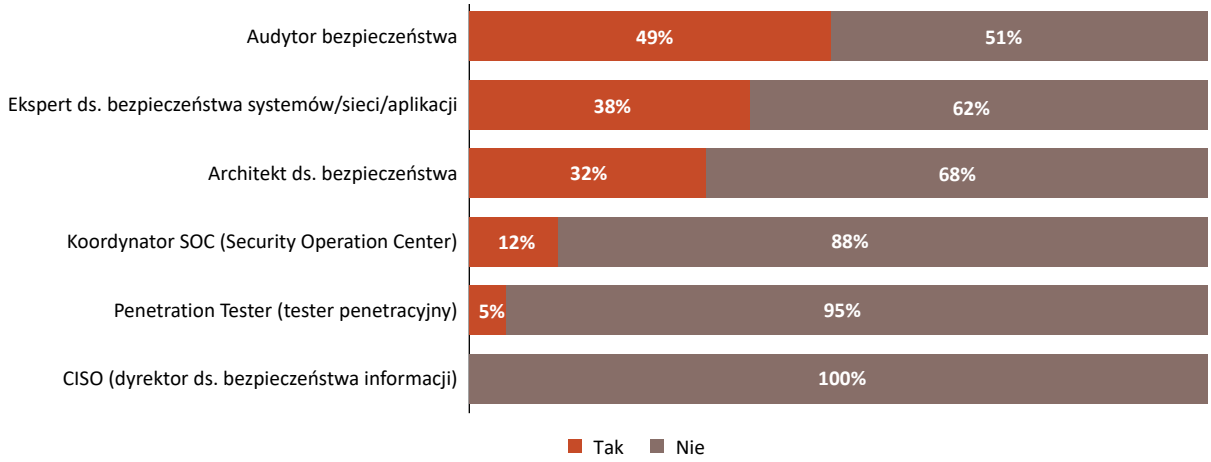


Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Z kolei w sektorze cyberbezpieczeństwa pracodawcy najczęściej poszukują pracowników na stanowisko audytora bezpieczeństwa (49% odpowiedzi) (wykres 10). Duże zapotrzebowanie jest także na ekspertów ds. bezpieczeństwa systemów/sieci/aplikacji

(38%). Rzadziej pracodawcy poszukiwali pracowników na stanowisko testera penetracyjnego (5% wskazań). Żaden z badanych pracodawców w omawianym sektorze nie poszukiwał specjalistów na stanowisko dyrektora ds. bezpieczeństwa informacji (Chief Information Security Officer; CISO). Warto jednak dodać, że jest to stanowisko rangi zarządczej i zazwyczaj w firmach obejmuje je jedna osoba, najczęściej będąca już w strukturze firmy.

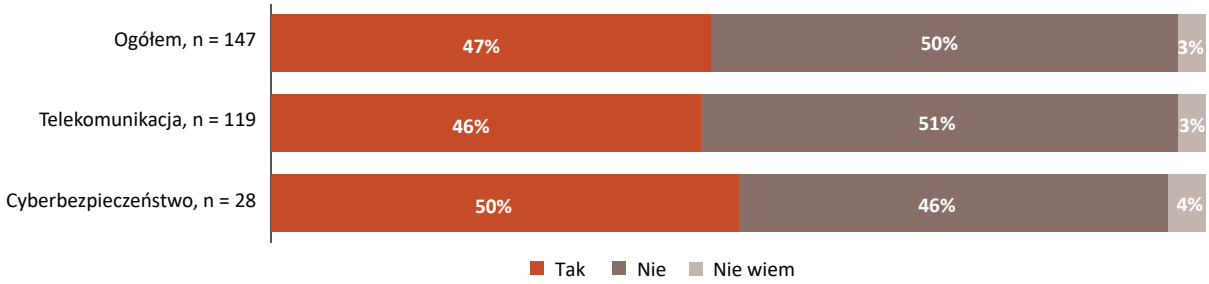
Wykres 10. Zapotrzebowanie na nowych pracowników z sektora cyberbezpieczeństwa – deklaracje pracodawców (N = 115)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Odsetek pracodawców poszukujących pracownika na uniwersalne w analizowanej branży stanowisko dyrektora handlowego jest niewielki. Jedynie 9% badanych zadeklarowało potrzebę zatrudnienia tego typu specjalisty. **Prawie połowa (47%) pracodawców z branży telekomunikacji i cyberbezpieczeństwa miała problem ze znalezieniem odpowiednich pracowników w ciągu 12 miesięcy poprzedzających badanie (wykres 11).**

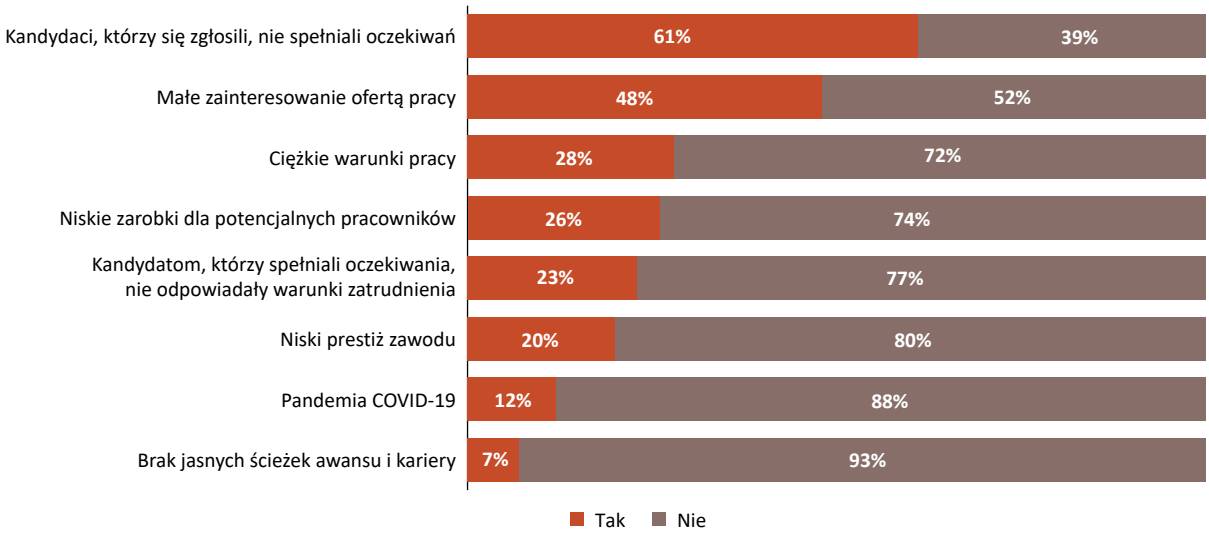
Wykres 11. Problemy pracodawców ze znalezieniem odpowiednich pracowników (ogółem i w podziale na sektory)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Dla 3 na 5 pracodawców z sektora telekomunikacji głównym powodem wystąpienia problemu ze znalezieniem odpowiedniej osoby do pracy była kwestia braku odpowiednich kompetencji kandydatów (wykres 12). Rzadziej pojawiającymi się problemami były: małe zainteresowanie ofertą pracy (wskazywane przez niemal 50% pracodawców), ciężkie warunki pracy oraz zbyt niskie – dla potencjalnych pracowników – zarobki. Najrzadziej (jedynie 7% odpowiedzi) wskazano problem związany z brakiem jasnych ścieżek awansu i kariery.

Wykres 12. Powody wystąpienia problemów ze znalezieniem odpowiednich pracowników – sektor telekomunikacji (N = 55)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

W sektorze cyberbezpieczeństwa najczęściej wskazywanym problemem z zatrudnieniem nowych osób było małe zainteresowanie ofertą pracy wśród potencjalnych kandydatów. Dodatkowo, przedsiębiorcy zwracali uwagę na trudność związaną z brakiem odpowiednich kompetencji posiadanych przez kandydatów. Innymi, rzadziej wskazywanymi problemami były: nieodpowiednie warunki zatrudnienia w opinii potencjalnych pracowników oraz ciężkie warunki pracy. Warto nadmienić, że pandemia COVID-19 oraz brak jasnych ścieżek awansu i kariery nie zostały zakwalifikowane jako powód wystąpienia problemów ze znalezieniem odpowiednich pracowników przez żadnego uczestnika badania[34].

W opinii pracodawców, stanowiskami w sektorze telekomunikacji budzącymi największe zainteresowanie wśród potencjalnych kandydatów są: inżynier – niezależnie od specjalizacji (18% wskazań) oraz tester (14% wskazań). Najpopularniejszymi stanowiskami, które budzą zainteresowanie potencjalnych kandydatów w sektorze cyberbezpieczeństwa, są CISO (Chief Information Security Officer) oraz Penetration Tester (po 17% wskazań). Brakuje natomiast chętnych osób do pracy na stanowiskach: audytor bezpieczeństwa, koordynator SOC (Security Operation Center) oraz ekspert ds. bezpieczeństwa systemów/sieci/aplikacji. Stanowiska te nie zostały wskazane przez żadnego uczestnika badania (tabela 9).

Tabela 9. Kluczowe stanowiska w branży telekomunikacja i cyberbezpieczeństwo, na które aplikuje najwięcej chętnych do pracy

	Inżynier (każdej specjalizacji)	Quality Assurance (tester)	Project Manager (kierownik projektu)	Architekt systemów	Developer (programista)	CISO (dyrektor ds. bezpieczeństwa informacji)	Penetration Tester (tester penetracyjny)	Architekt ds. bezpieczeństwa	Audytor bezpieczeństwa	Koordynator SOC (Security Operation Center)	Ekspert ds. bezpieczeństwa systemów/ sieci/aplikacji	Dyrektor handlowy/sprzedaży
Sektor*	T	T	T	T	T	C	C	C	C	C	C	U
N =	55	55	55	55	55	9	9	9	9	9	9	64
Tak	18%	14%	12%	9%	9%	17%	17%	7%	0%	0%	0%	12%
Nie	82%	86%	88%	91%	91%	83%	83%	93%	100%	100%	100%	88%

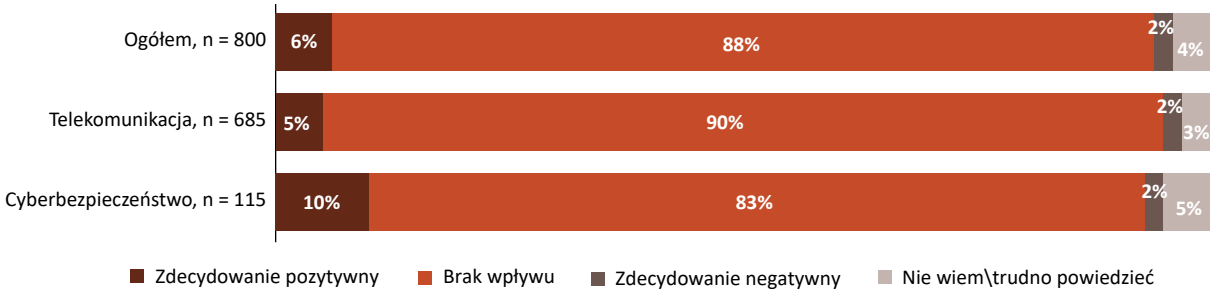
* Sektor: T – Telekomunikacja, C – Cyberbezpieczeństwo, U – stanowisko uniwersalne.

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

[34] Ze względu na niską liczebność grupy pracodawców ustosunkowujących się do pytania o problemy związane z zatrudnianiem nowych osób podane odpowiedzi należy traktować jako poglądowe.

W opinii 90% przedsiębiorców reprezentujących sektor telekomunikacji oraz niemal 85% sektor cyberbezpieczeństwa, liczba pracowników zatrudnianych w przedsiębiorstwach w ciągu 12 miesięcy następujących po badaniu pozostanie na tym samym poziomie (wykres 13).

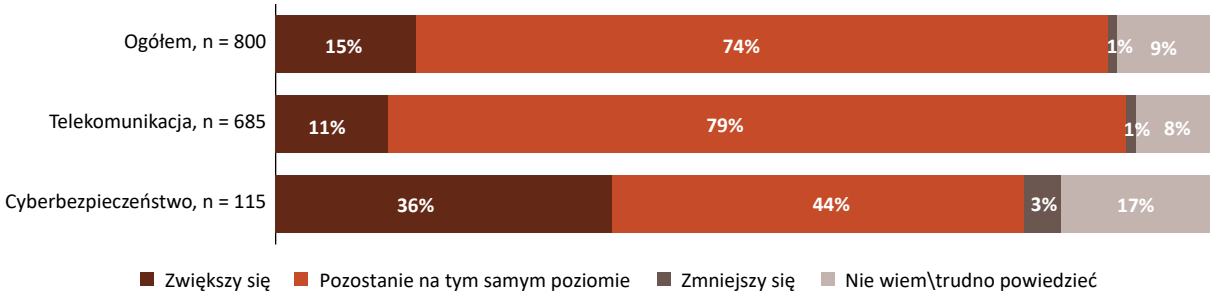
Wykres 13. Prognozowane zmiany w zatrudnieniu pracowników w ciągu 12 miesięcy następujących po badaniu (ogółem i w podziale na sektory)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Bardziej optymistyczne prognozy dotyczą zatrudnienia w perspektywie najbliższych 3 lat. Około 35% przedsiębiorców z sektora cyberbezpieczeństwa przewiduje wzrost zatrudnienia w branży (to o niemal 25 p.p. więcej w stosunku do sektora telekomunikacji) (wykres 14). W sektorze telekomunikacji zdecydowanie dominuje pogląd, że liczba zatrudnionych pracowników w firmie pozostanie na tym samym poziomie (zdanie 4 na 5 przedstawicieli sektora). Pracodawcy z obu sektorów nie przewidują zmniejszenia liczby zatrudnionych pracowników (1% odpowiedzi w sektorze telekomunikacji oraz 3% w sektorze cyberbezpieczeństwa).

Wykres 14. Prognozowane w ciągu najbliższych 3 lat zmiany w zatrudnieniu pracowników (ogółem i w podziale na sektory)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Zarówno w sektorze telekomunikacji, jak i cyberbezpieczeństwa nie przewiduje się raczej większych zmian w zapotrzebowaniu na pracowników, jednakże zróżnicowanie w prognozach pojawia się przy podziale na wyróżnione kluczowe stanowiska (tabela 10). Najwyższy prognozowany wzrost zatrudnienia dotyczy stanowiska programisty – 44% przedsiębiorców spodziewa się wzrostu zapotrzebowania w ciągu najbliższych 3 lat (+37 p.p. w porównaniu do perspektywy 12 miesięcy). Istotny wzrost zapotrzebowania w dłuższej perspektywie czasowej widać również w przypadku eksperta ds. bezpieczeństwa systemów/sieci/aplikacji (13% wskazuje na wzrost zapotrzebowania w ciągu 12 miesięcy od badania, a 31% w ciągu 3 lat).

Tabela 10. Zmiany w zatrudnieniu pracowników w branży telekomunikacja i cyberbezpieczeństwo – perspektywa 12 miesięcy i 3 lat

Nazwa stanowiska (Sektor*)	Perspektywa czasowa	Zatrudnienie wzrośnie	Zatrudnienie pozostanie bez zmian	Zatrudnienie spadnie	Nie wiem/trudno powiedzieć
Developer (programista) (T)	Kolejne 12 miesięcy	7%	88%	2%	3%
	Kolejne 3 lata	44%	52%	1%	3%
Inżynier (każdej specjalizacji) (T)	Kolejne 12 miesięcy	12%	84%	1%	3%
	Kolejne 3 lata	11%	79%	4%	6%
Project Manager (kierownik projektu) (T)	Kolejne 12 miesięcy	8%	87%	2%	4%
	Kolejne 3 lata	9%	88%	2%	2%
Quality Assurance (tester) (T)	Kolejne 12 miesięcy	7%	88%	1%	4%
	Kolejne 3 lata	4%	91%	4%	1%
Architekt systemów (T)	Kolejne 12 miesięcy	4%	94%	0%	2%
	Kolejne 3 lata	9%	87%	1%	2%
Ekspert ds. bezpieczeństwa systemów/sieci/aplikacji (C)	Kolejne 12 miesięcy	13%	82%	2%	3%
	Kolejne 3 lata	31%	54%	1%	14%
Audytor bezpieczeństwa (C)	Kolejne 12 miesięcy	14%	67%	2%	17%
	Kolejne 3 lata	19%	79%	2%	0%
Architekt ds. bezpieczeństwa (C)	Kolejne 12 miesięcy	10%	89%	1%	0%
	Kolejne 3 lata	16%	76%	5%	3%
Penetration Tester (C)	Kolejne 12 miesięcy	16%	82%	2%	0%
	Kolejne 3 lata	14%	80%	6%	0%
CISO (Chief Information Security Officer) (C)	Kolejne 12 miesięcy	12%	75%	3%	10%
	Kolejne 3 lata	8%	87%	0%	5%
Koordynator SOC (Security Operation Center) (C)	Kolejne 12 miesięcy	4%	96%	0%	0%
	Kolejne 3 lata	11%	80%	5%	4%
Dyrektor handlowy/sprzedaży (U)	Kolejne 12 miesięcy	2%	96%	0%	2%
	Kolejne 3 lata	6%	89%	1%	4%

*Sektor: T – Telekomunikacja, C – Cyberbezpieczeństwo, U – stanowisko uniwersalne.

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

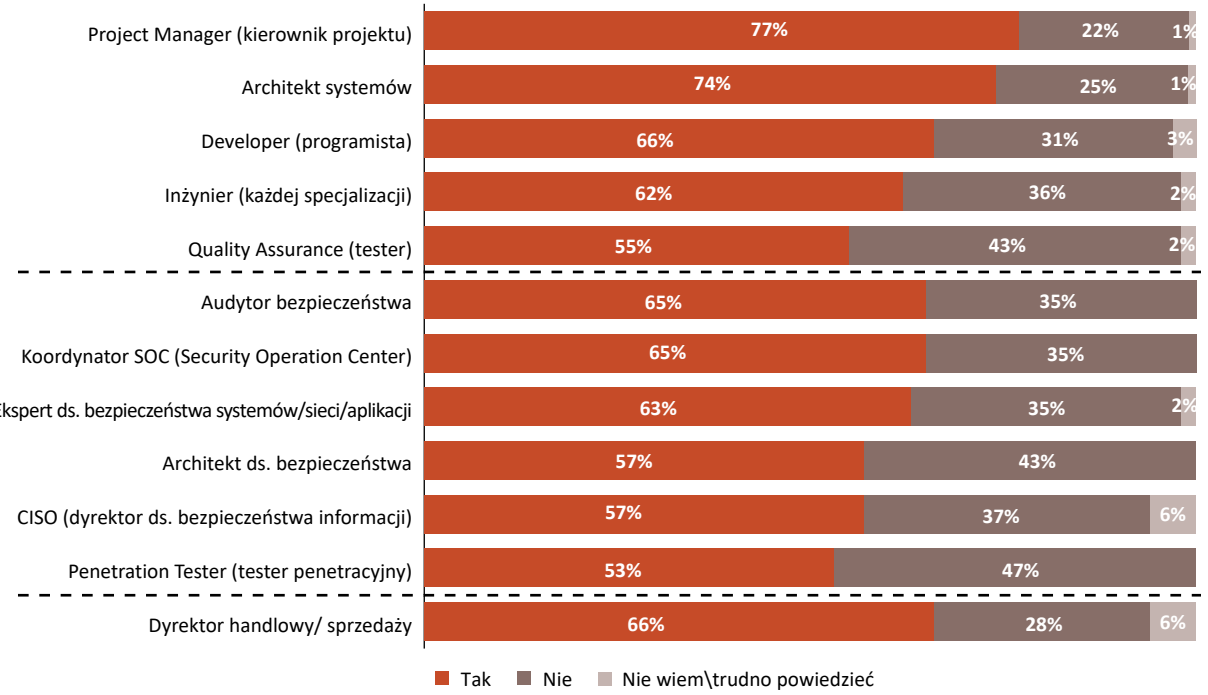
Warto zauważyć, że choć przy kilku stanowiskach pojawia się dosyć wysoki odsetek odpowiedzi „nie wiem/trudno powiedzieć", to z uwagi na relatywnie niewielką liczebność respondentów w przypadku tych kluczowych stanowisk jest to raczej informacja jakościowa. Badani nie potrafią jednoznacznie określić potencjalnej zmiany lub jej braku w zatrudnieniu osób na stanowisko eksperta ds. bezpieczeństwa systemów/sieci/aplikacji w perspektywie 3 lat (14% wszystkich wskazań) oraz audytora bezpieczeństwa w perspektywie 12 miesięcy (17% wszystkich wskazań). W badaniu delfickim eksperci wskazywali, że zapotrzebowanie na wszystkich specjalistów rośnie i będzie rosło w przyszłości. W przypadku eksperta ds. bezpieczeństwa systemów/sieci/aplikacji w perspektywie 3 lat uczestnicy badania delfickiego przyznali średnio 8,38 punktów (w pierwszym etapie badania) oraz średnio 8,49 punktów (w drugim etapie badania) na 10 możliwych[35], a w przypadku audytora bezpieczeństwa było to odpowiednio średnio 7,55 oraz 7,7 punktów.

Przedsiębiorcy, w zdecydowanej większości, nie prognozują, aby w przyszłości powstały lub też zostały zaadaptowane z innych branż, nowe zawody. Jedynymi, w dodatku jednostkowymi, wskazaniami są zawód influencera oraz, bliżej niesprecyzowane w nazwie, stanowisko związane z bezpieczeństwem przetwarzania danych.

Pracodawcy wymagają od potencjalnych kandydatów do pracy doświadczania. W przypadku kluczowych stanowisk w sektorze telekomunikacji, najczęściej wymagane jest doświadczenie na stanowisku kierownika projektu (77% wskazań). Najniższy odsetek wskazań odnotowano w przypadku stanowiska testera (55%). W sektorze cyberbezpieczeństwa, najczęściej doświadczenie zawodowe jest wymagane na stanowiskach: audytora bezpieczeństwa oraz koordynatora SOC (po 65%). Spośród analizowanych kluczowych stanowisk, najrzadziej wymaga się go na stanowisku testera penetracyjnego (53% wskazań) (wykres 15).

[35] W badaniu stosowana jest 10-stopniowa skala (od 0 do 10), na której 0 oznaczało brak zgody, że dane zjawisko wystąpi, natomiast 10 pełną zgodę na wystąpienie zjawiska.

Wykres 15. Wymagania dotyczące doświadczenia zawodowego w odniesieniu do kluczowych stanowisk* – sektor telekomunikacji (N = 685) oraz cyberbezpieczeństwa (N = 115)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

*Stanowiska od 1 do 5 – sektor telekomunikacji, od 6 do 11 – sektor cyberbezpieczeństwa, 12 – stanowisko uniwersalne. Sortowanie w obrębie wyodrębnionych grup.

Większość pracodawców (66%) w branży telekomunikacji i cyberbezpieczeństwa oczekuje doświadczenia zawodowego przy zatrudnianiu nowej osoby na stanowisko dyrektora handlowego/sprzedaży. W większości przypadków wskazuje się na doświadczenie nieprzekraczające 3 lat (83%), natomiast częściej niż co dziesiąty pracodawca mówi o dłuższym okresie, ale nieprzekraczającym 10 lat.

Pracodawcy z branży na ogół nie wymagają posiadania zawodowych uprawnień, certyfikatów bądź licencji do realizacji zadań od pracowników na poszczególnych stanowiskach (tabela 11). W sektorze telekomunikacji najczęściej jednak tego typu uprawnień oczekuje się od kandydatów na stanowisku inżyniera niezależnie od specjalizacji (26% wskazań), a najniższy odsetek wskazań odnotowany został przy stanowisku architekta systemów (13%). W sektorze cyberbezpieczeństwa specjalnych uprawnień bądź certyfikacji oczekuje się najczęściej od osób na stanowiskach penetration testerów i architektów ds. bezpieczeństwa

(jest to jednak jedynie 29% i 26% wskazań). Zdecydowana większość pracodawców z obu sektorów (92%) nie wymaga uprawnień zawodowych, certyfikatów oraz licencji na stanowisku dyrektora handlowego/sprzedaży.

Tabela 11. Wymóg dotyczący uprawnień zawodowych, certyfikatów lub licencji na poszczególnych stanowiskach w obydwu sektorach

	Inżynier (każdej specjalizacji)	Developer (programista)	Project Manager (kierownik projektu)	Quality Assurance (tester)	Architekt systemów	Penetration Tester (tester penetracyjny)	Architekt ds. bezpieczeństwa	Audytor bezpieczeństwa	Ekspert ds. bezpieczeństwa systemów/sieci/aplikacji	Koordynator SOC (Security Operation Center)	CISO (dyrektor ds. bezpieczeństwa informacji)	Dyrektor handlowy/sprzedaży
Sektor*	T	T	T	T	T	C	C	C	C	C	C	U
N =	527	364	179	163	351	52	18	51	35	25	36	166
Tak	26%	18%	18%	15%	13%	29%	26%	20%	19%	15%	9%	5%
Nie	68%	76%	82%	81%	85%	65%	67%	68%	72%	85%	89%	92%
Nie wiem/trudno powiedzieć	6%	6%	0%	4%	2%	6%	7%	12%	9%	0%	2%	3%

*Sektor: T – Telekomunikacja, C – Cyberbezpieczeństwo, U – stanowisko uniwersalne.

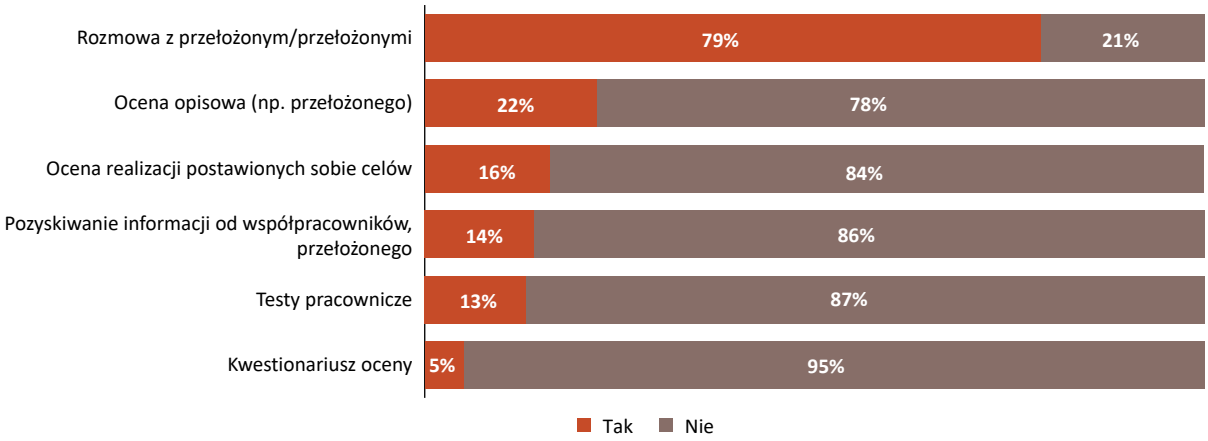
Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Niemal dwie trzecie przedsiębiorców z branży (65%) weryfikuje (systematycznie bądź sporadycznie), jakich umiejętności potrzebują zatrudnieni pracownicy. Jak wynika z badań, systematyczną kontrolę umiejętności pracowników (przynajmniej raz w roku) deklaruje 36% pracodawców, z kolei 29% badanych taką ocenę przeprowadza sporadycznie (rzadziej niż raz w roku). Warto zauważyć, że dosyć duży odsetek pracodawców (33%) w ogóle nie diagnozuje umiejętności potrzebnych pracownikom.

Najczęściej wskazywaną przez pracodawców metodą identyfikującą zapotrzebowanie na konkretne kompetencje pracowników jest rozmowa z przełożonym(i) (79% wskazań). W firmach stosowane są również: oceny opisowe (22%) oraz oceny realizacji postawionych

celów (16%). Najrzadziej wykorzystywaną formą oceny jest kwestionariusz oceny (jedynie 5% wskazań) (wykres 16).

Wykres 16. Metody oceny zapotrzebowania na kompetencje u pracowników (N = 800)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

O najbardziej popularnych rozmowach z przełożonym(i) częściej mówią przedsiębiorcy z sektora telekomunikacji niż z sektora cyberbezpieczeństwa (81% vs. 69%).

Pracodawcy ogólnie pozytywnie oceniają posiadane przez pracowników umiejętności (wykres 17). **Połowa pracodawców z branży uważa, że są one w pełni zadowalające i nie widzi potrzeby dodatkowych szkoleń**, natomiast niemal 45% – mimo ogólnego zadowolenia w kontekście analizowanego aspektu – widzi potrzebę doszkolenia pracowników w pewnych obszarach.

Mimo że ogólnie pracodawcy reprezentujący sektor cyberbezpieczeństwa nieco częściej są zadowoleni lub w pełni zadowoleni niż reprezentanci sektora telekomunikacji z umiejętności posiadanych przez pracowników (96% vs. 92%), to jednak większość z nich widzi obszary, w których pracownicy potrzebowaliby się rozwinąć (niemal 63% tej grupy w ramach sektora cyberbezpieczeństwa). Jednocześnie ponad połowa pracodawców sektora telekomunikacji zadowolonych z umiejętności pracowników nie widzi potrzeby rozwoju zawodowego, myśląc o zatrudnionych pracownikach.

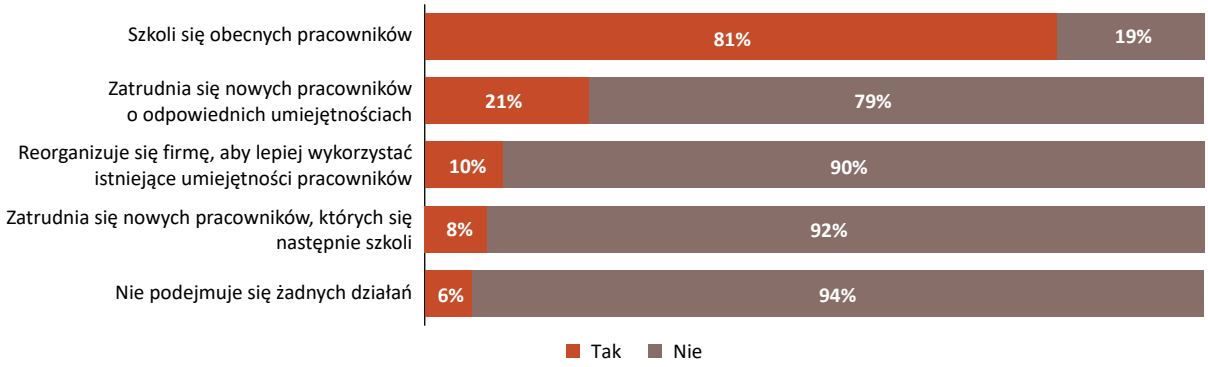
Wykres 17. Ocena pracodawców dotycząca umiejętności swoich pracowników (ogółem, w podziale na sektory oraz w podziale na wielkość firmy)

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Przedsiębiorcy ze średnich i dużych firm w branży telekomunikacji i cyberbezpieczeństwa najczęściej uważają, że umiejętności pracowników są zadowalające, ale w pewnych obszarach wymagają doszkolenia, natomiast reprezentanci mikro i małych przedsiębiorstw są mniej krytyczni – większość uważa, że są one w pełni zadowalające, więc pracownicy nie potrzebują się szkolić.

W przypadku braku konkretnych umiejętności u pracowników, najczęstszym działaniem (81% wskazań) podejmowanym przez pracodawców jest doszkalanie pracowników (wykres 18). Co piąty przedsiębiorca z branży, będący w takiej sytuacji, zatrudnia nowych pracowników o odpowiednich umiejętnościach. Jedynie 6% badanych przyznało, że nie podejmuje żadnych działań w momencie zidentyfikowania potencjalnych braków umiejętności. Branża oraz wielkość firmy nie różnicują istotnie podejścia do tej kwestii.

Wykres 18. Działania podejmowane przez pracodawców w przypadku zidentyfikowania braku konkretnych umiejętności u pracowników (N = 800)



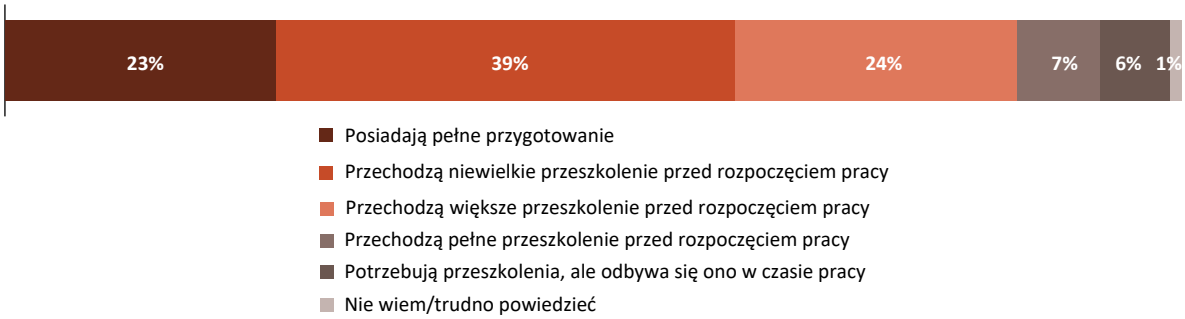
Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Warto zwrócić uwagę, że na zatrudnienie nowych pracowników o odpowiednich umiejętnościach częściej decydują się pracodawcy reprezentujący sektor cyberbezpieczeństwa (35% deklaracji) niż telekomunikacji (19% deklaracji).

Niemal 80% pracodawców twierdzi, że absolwenci opuszczający szkoły/uczelnie posiadają umiejętności potrzebne obecnie na rynku[36]. Takiego odczucia nie ma 15% przedsiębiorców z branży. Jednak ocena przygotowania nowo przyjmowanych osób do firm jest już mniej pozytywna. Ponad 35% pracowników przechodzi większe lub pełne przeszkolenie przed rozpoczęciem pracy lub już po jej rozpoczęciu. Według 23% pracodawców absolwenci są w pełni przygotowani do pracy, natomiast w opinii prawie 40% przedsiębiorców absolwenci powinni przejść niewielkie przeszkolenie przed przyjęciem obowiązków zawodowych (wykres 19). Wielkość firmy nie jest w tym przypadku czynnikiem różnicującym odpowiedzi.

[36] Aby łatwiej było ocenić respondentom tą kwestię, byli oni pytani o umiejętności, na które jest obecnie zapotrzebowanie w ich firmach.

Wykres 19. Ocena pracodawców dotycząca poziomu przygotowania absolwentów do podjęcia pracy zawodowej (N = 800)

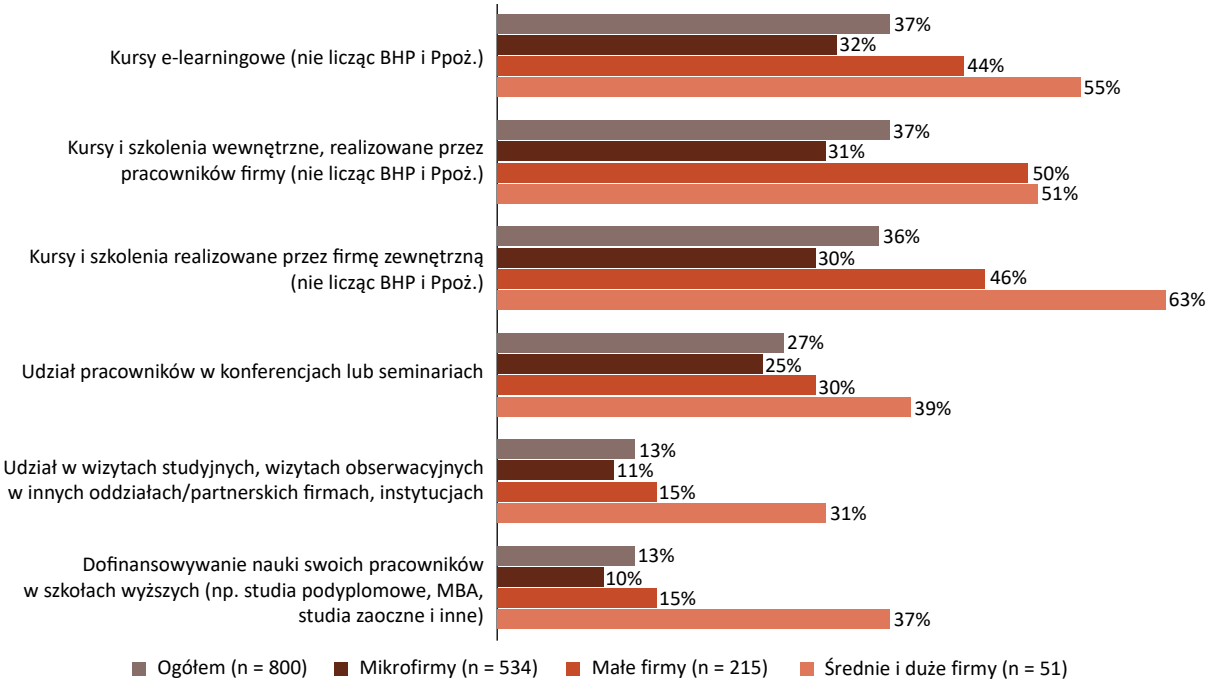


Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

6. Rozwój kompetencji pracowników

Korzystanie przez firmy działające w branży z ujętych w badaniu form rozwoju kompetencji pracowników w ciągu 12 miesięcy poprzedzających badanie było stosunkowo mało popularne – najczęściej wskazywane kursy e-learningowe, kursy organizowane dla pracowników przez pracowników oraz kursy zewnętrzne zostały wskazane przez niewiele ponad 35% przedsiębiorców (wykres 20). Korzystanie z poszczególnych form rozwoju kompetencji różnicowane jest przez wielkość firmy – im większe przedsiębiorstwo, tym częściej pracodawcy decydują się na skorzystanie z danej formy rozwoju kompetencji. W średnich i dużych firmach dominującą formą proponowaną pracownikom jest organizacja kursów i szkoleń realizowanych przez firmy zewnętrzne (63% wskazań), natomiast w małych przedsiębiorstwach najczęściej skorzystać można z oferty kursów i szkoleń realizowanych wewnętrznie – przez pracowników firmy (50% wskazań).

Wykres 20. Formy rozwijania kompetencji pracowników (ogółem oraz w podziale ze względu na wielkość firmy)



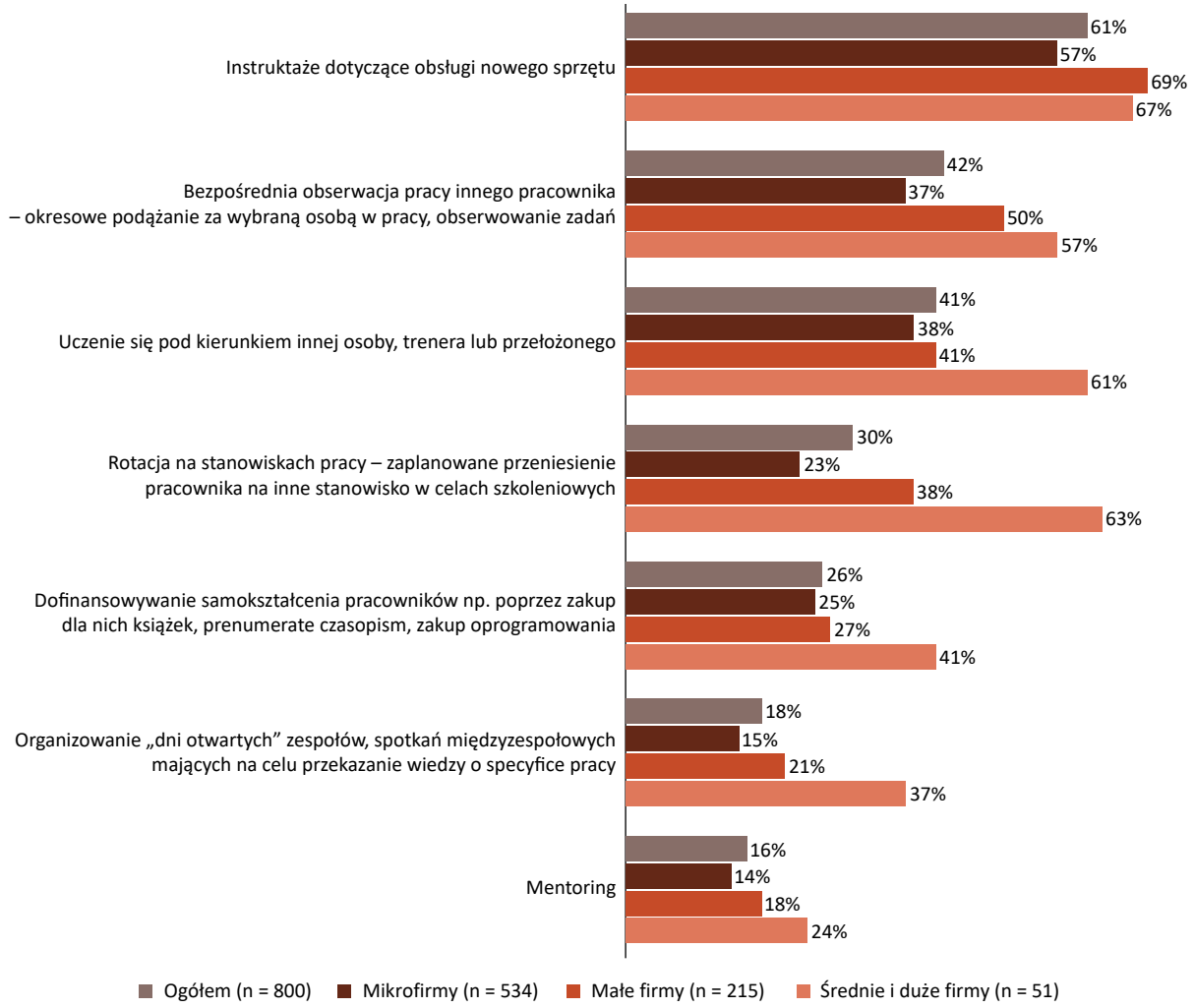
Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Organizowanie kursów i szkoleń wewnętrznych realizowanych przez pracowników średnich i dużych firm znacząco różni się pomiędzy badanymi sektorami. Ta forma rozwoju jest zdecydowanie bardziej popularna w średnich i dużych przedsiębiorstwach z sektora cyberbezpieczeństwa niż z sektora telekomunikacji (71% vs. 48%). W kontekście zróżnicowania między sektorami zwraca również uwagę kwestia udziału pracowników małych firm w konferencjach lub seminariach. Według deklaracji pracodawców, pracownicy z małych firm w sektorze cyberbezpieczeństwa mają zdecydowanie większą możliwość udziału w konferencjach lub seminariach niż osoby zatrudnione w małych firmach w sektorze telekomunikacji (odpowiednio: 52% oraz 26%)[37].

Pracodawcy chętnie decydują się na rozwijanie kompetencji u swoich pracowników w miejscu pracy. Najczęściej w ramach szkoleń firmowych przeprowadzane są instruktaże dotyczące obsługi nowego sprzętu (61% wskazań) (wykres 21). Dosyć powszechną formą, z której korzystają przedsiębiorstwa, jest także bezpośrednia obserwacja pracy i wykonywanych zadań przez innego pracownika (42% odpowiedzi). Najmniej popularnymi formami są natomiast: organizacja „dni otwartych" zespołów/spotkań międzyzespołowych mających na celu przekazanie wiedzy o specyfice pracy oraz mentoring (kolejno: 18% i 16% wskazań). Popularność form rozwoju kompetencji pracowników realizowanych w miejscu pracy jest zróżnicowana ze względu na wielkość przedsiębiorstwa. Podobnie jak przy wcześniejszej analizie, wraz z wielkością firmy rośnie udział przedsiębiorstw decydujących się na korzystanie z każdej z metod rozwijającej kompetencje zatrudnionych pracowników.

[37] Analiza ilościowa najpopularniejszych newsletterów skierowanych do specjalistów telekomunikacji i cyberbezpieczeństwa pokazuje, że oferta konferencji i seminariów dla cyberbezpieczeństwa jest liczniejsza niż w przypadku telekomunikacji.

Wykres 21. Formy rozwoju kompetencji pracowników w miejscu pracy (ogółem i w podziale ze względu na wielkość firmy)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Korzystanie z formy rozwoju kompetencji, jaką jest szkolenie pracowników pod kierunkiem trenera, przełożonego lub innej osoby w obrębie realizacji bieżących zadań, jest różnicowane przez omawiane sektory – takie działanie zadeklarowano w 54% przypadków w sektorze cyberbezpieczeństwa i 38% w sektorze telekomunikacji.

Ciekawym wskaźnikiem aktywności rozwojowej firm może być określenie odsetka przedsiębiorstw, które korzystały z co najmniej jednej formy rozwoju kompetencji pracowników. W branży telekomunikacji i cyberbezpieczeństwa wartość tego wskaźnika

osiągnęła poziom 86%. W sektorze cyberbezpieczeństwa odsetek ten był wyższy i wyniósł 96%, natomiast w telekomunikacji – 84%. Im większa pod względem zatrudnienia pracowników firma, tym omawiany wskaźnik wyższy – od 83% w przypadku mikrofirm, przez 90% w przypadku małych firm po 96% w przypadku średnich i dużych przedsiębiorstw (wykres 22).

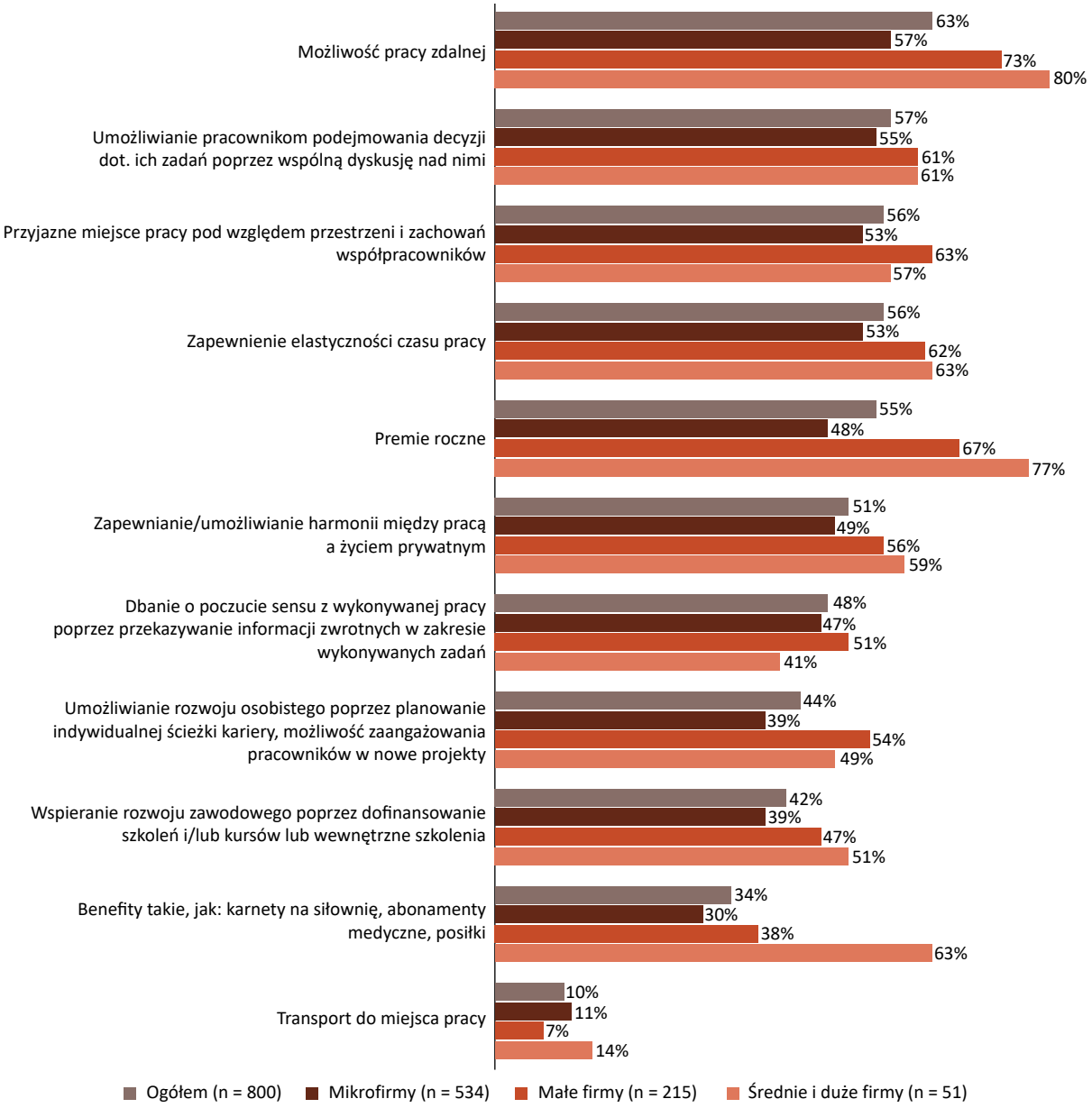
Wykres 22. Korzystanie z form rozwoju kompetencji pracowników przez firmy (ogółem i w podziale ze względu na wielkość firmy)

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Pracodawcy na ogół chętnie stosują różnorodne sposoby motywacji swoich pracowników. Najczęściej oferowaną przez przedsiębiorców z branży telekomunikacji i cyberbezpieczeństwa zachętą jest umożliwienie pracownikom pracy zdalnej (wykres 23). Warto zauważyć, że powszechność stosowania różnorodnych sposobów motywacji zatrudnionych pracowników jest uzależniona od wielkości przedsiębiorstwa, nie ma natomiast różnic w przypadku sektorów tworzących branżę. Odsetek wskazań dotyczących motywacji pracodawców reprezentujących firmy o średniej i dużej wielkości jest zazwyczaj zdecydowanie wyższy niż odsetek obserwowany w przypadku pracodawców z firm małych oraz mikro. Z badań ilościowych wynika, że przedsiębiorstwa te zdecydowanie częściej oferują udogodnienia takie jak premie roczne (77% wskazań) oraz benefity w postaci karnetów na siłownię, abonamentów medycznych i posiłków (63% wskazań). Z kolei przedstawiciele mikrofirm stosunkowo często deklarują umożliwianie pracownikom podejmowania decyzji dotyczącej ich zadań poprzez wspólną dyskusję nad nimi (55% wskazań). W małych firmach natomiast, powszechnymi sposobami motywacji kadry

pracowniczej są udzielane premie roczne (67% wskazań) oraz zapewnianie przyjaznego (pod względem przestrzeni i zachowania współpracowników) miejsca pracy (63% wskazań).

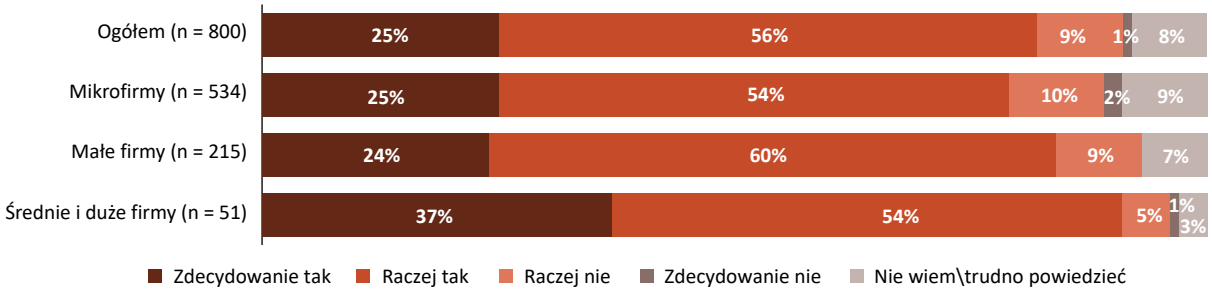
Wykres 23. Sposoby motywacji pracowników stosowane w firmach z branży telekomunikacji i cyberbezpieczeństwa (ogółem i w podziale ze względu na wielkość firmy)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

W opinii pracodawców aktualne programy w szkołach i na uczelniach odpowiadają zapotrzebowaniu na umiejętności pracowników (wykres 24). Według 81% przedsiębiorców, absolwenci szkół/uczelni posiadają odpowiednie kompetencje potrzebne w pracy zawodowej. Wygląda na to, że wielkość badanego przedsiębiorstwa nie wpływa istotnie na ocenę programu nauczania w szkołach i na uczelniach – różnice są niewielkie.

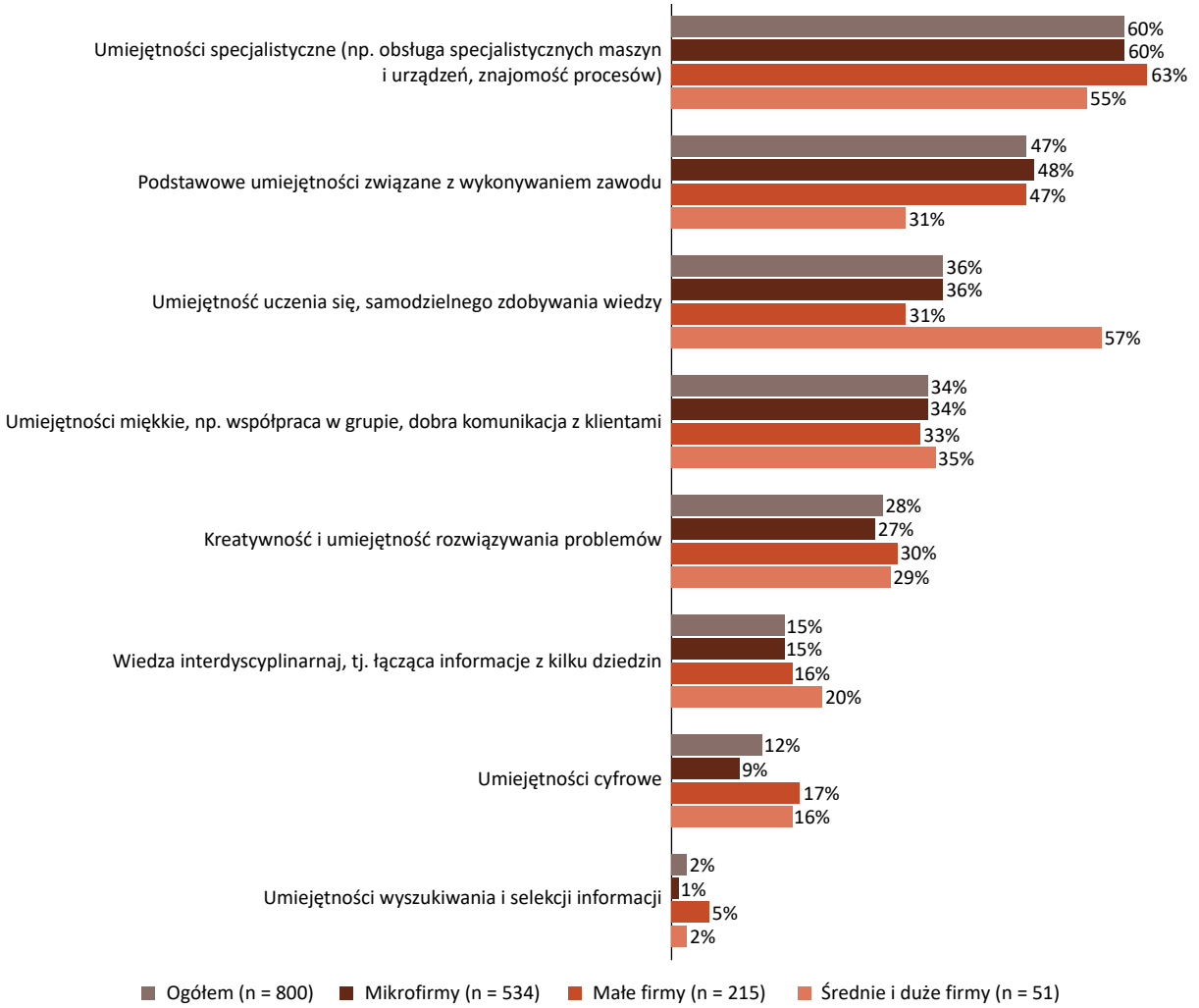
Wykres 24. Programy nauczania a kompetencje potrzebne w pracy zawodowej (ogółem i w podziale ze względu na wielkość firmy)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

Według zdecydowanej większości pracodawców, szkoły i uczelnie przygotowujące do pracy w branży telekomunikacji i cyberbezpieczeństwa przede wszystkim powinny uczyć umiejętności specjalistycznych (60% wskazań) oraz podstawowych umiejętności związanych z wykonywaniem zawodu (47% odpowiedzi). Relatywnie duże znaczenie dla pracodawców ma również umiejętność samodzielnego uczenia się (36%) oraz umiejętności miękkie (34%). Najrzadziej wskazywano natomiast kompetencje związane z wyszukiwaniem i selekcją informacji (2%).

Wykres 25. Wiedza i umiejętności jakie powinny być przekazywane w szkołach/na uczelniach w kontekście pracy w branży (ogółem i w podziale ze względu na wielkość firmy)



Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

7. Bilans kompetencji

Charakterystyka Bilansu

Zgodnie z przyjętymi w badaniu BBKL II założeniami, bilans kompetencji w branży powstał poprzez przygotowanie zestawienia opinii pracodawców i pracowników na temat wiedzy, umiejętności i kompetencji społecznych[38] dla każdego kluczowego stanowiska zdefiniowanego w jakościowej części procesu badawczego. Bilans tworzą: ocena niedopasowania kompetencyjnego, identyfikacja luki kompetencyjnej oraz ocena ważności kompetencji w przyszłości.

Składowe profili kompetencyjnych zdefiniowane dla każdego z 12 kluczowych stanowisk wyróżnionych w branży telekomunikacji i cyberbezpieczeństwa poddano w badaniu ilościowym ocenie dwóch stron: pracodawców i pracowników. Pracodawcy odnieśli się do kompetencji pod kątem: ważności kompetencji oraz trudności znalezienia osoby, która posiada określoną kompetencję potrzebną do pracy na danym stanowisku, a także prognozy zmiany znaczenia tej kompetencji w perspektywie 3 lat. Pracownicy z kolei oceniali własny poziom kompetencji zdefiniowanych dla profilu odpowiadającemu zajmowanemu kluczowemu stanowisku.

Do tworzenia poszczególnych wymiarów bilansu wykorzystano następujące pytania z badania pracodawców:

- Myśląc o stanowisku [nazwa analizowanego stanowiska], proszę ocenić, jak ważna jest wymieniona kompetencja z punktu widzenia Państwa firmy? Proszę posłużyć się pięciopunktową skalą, gdzie 1 oznacza „marginalnie ważna", a 5 – „kluczowa". Proszę ocenić, czy trudno czy łatwo jest znaleźć do pracy osobę, która posiada tę umiejętność potrzebną do pracy na stanowisku [nazwa analizowanego stanowiska]?[39]
- Proszę wskazać, czy w Pana/Pani opinii znaczenie tej umiejętności zmieni się w perspektywie najbliższych 3 lat?[40]

[38] Składających się na profile kompetencyjne będące efektem badania jakościowego.

[39] Możliwe odpowiedzi: Trudno, Łatwo, Nie wiem/trudno powiedzieć, Odmowa odpowiedzi.

[40] Możliwe odpowiedzi: Znaczenie wzrośnie, Pozostanie takie samo, Znaczenie zmniejszy się, Nie wiem/trudno powiedzieć, Odmowa odpowiedzi.

oraz z badania pracowników:

– Przeczytam teraz listę umiejętności wymaganych na zajmowanym przez Pana/Panią stanowisku. Przy każdej z nich poproszę o ocenę poziomu własnych umiejętności na 5-punktowej skali, gdzie 1 oznacza „poziom niski", a 5 – „bardzo wysoki"[41].

Ocena niedopasowania kompetencyjnego

Niedopasowanie kompetencyjne (ang. *skills mismatch*) to wynik zestawienia oceny ważności danej kompetencji, dokonywanej przez pracodawców z punktu widzenia pracy na danym stanowisku z samooceną poziomu kompetencji posiadanych przez pracowników zatrudnionych na tym stanowisku. Przy ocenie dokonywanej przez pracodawców, aby zdefiniować, które kompetencje są relatywnie ważniejsze od innych zamiast bezpośredniego porównania średnich ocen dla danej kompetencji zastosowano zabieg centrowania. Polega on na tym, że najpierw obliczana jest średnia ocena dla każdej kompetencji na danym stanowisku, a następnie – w oparciu o te średnie – obliczana jest średnia ocena dla wszystkich kompetencji dla tego stanowiska. Wynik centrowania dla danej kompetencji to odchylenie wartości jej średniej od wartości ogólnej średniej dla wszystkich kompetencji. Kompetencje, które w wyniku centrowania uzyskały wynik dodatni, określone zostały jako relatywnie ważniejsze, natomiast kompetencje, które uzyskały wynik ujemny, określone zostały jako relatywnie mniej ważne[42]. Analogiczną operację centrowania wykonano również w przypadku samooceny kompetencji dokonanej przez pracowników.

W rezultacie otrzymujemy 4 wymiary oceny niedopasowania kompetencyjnego:

- **kompetencje nadwyżkowe** – kompetencje relatywnie mniej ważne dla pracodawców przy relatywnie wyższej samoocenie pracowników[43],
- **kompetencje zrównoważone** – kompetencje relatywnie ważniejsze dla pracodawców i jednocześnie relatywnie wyżej oceniane przez pracowników,

[41] Możliwe odpowiedzi: Poziom niski, Poziom podstawowy, Poziom średni, Poziom wysoki, Poziom bardzo wysoki, Nie wiem/trudno powiedzieć, Odmowa odpowiedzi.

[42] Zob. więcej: S. Czarnik, J. Górniak, M. Jelonek, K. Kasparek, M. Kocór, K. Lisek, P. Prokopowicz, A. Strzebońska, A. Szczucka, B. Worek, *Aktywność zawodowa i edukacyjna dorosłych Polaków wobec wyzwań współczesnej gospodarki. Raport podsumowujący VI edycję badania BKL w latach 2017–2018; PARP, Warszawa 2019, s. 158–168).*

[43] Pomimo mniejszej ważności dla pracodawców nie oznacza to, że są to kompetencje, których pracodawcy nie potrzebują. Są one ważne, ale w mniejszym stopniu niż inne, które pracodawca wskazał.

- **kompetencje wystarczające** – kompetencje relatywnie mniej ważne dla pracodawców i jednocześnie relatywnie niżej oceniane przez pracowników,
- **kompetencje niedoboru** – kompetencje relatywnie ważniejsze dla pracodawców przy relatywnie niższej samoocenie pracowników.

Rysunek 1. Wymiary obrazujące niedopasowanie kompetencyjne na danym stanowisku

Źródło: opracowanie własne.

Luka kompetencyjna

Luka kompetencyjna (ang. *skills gap*) występuje w sytuacji identyfikacji kompetencji relatywnie ważniejszych dla pracodawców i jednocześnie trudnych do pozyskania w opinii co najmniej 51% pracodawców oceniających dany profil kompetencyjny.

Kompetencje przyszłości

Kompetencje przyszłości to kompetencje, które – w ocenie co najmniej 30% pracodawców – będą zyskiwać na znaczeniu w perspektywie najbliższych 3 lat.

Wyniki bilansu uwzględniające wszystkie opisane wyżej wymiary, zostały przedstawione w zbiorczych tabelach, w których wykorzystano następujące oznaczenia:

- dla kompetencji zrównoważonych – pogrubienie oraz **kolor brązowy**,
- dla kompetencji niedoboru – pogrubienie oraz **kolor ciemny brązowy**,

- dla kompetencji wystarczających i nadwyżkowych – brak dodatkowego oznaczenia,
- w przypadku zidentyfikowania luki kompetencyjnej – pogrubienie oraz **kolor brązowy**,
- w przypadku braku luki kompetencyjnej – brak dodatkowego oznaczenia,
- przy odnotowaniu wzrostu znaczenia w przyszłości – pogrubienie oraz **kolor brązowy** w przypadku trzech kompetencji najczęściej wskazywanych przez przedsiębiorców.

Główne wnioski dotyczące bilansu kompetencji

Na podstawie analizy ważności kompetencji w branży telekomunikacji i cyberbezpieczeństwa można zaryzykować stwierdzenie, że ogólnie badane kompetencje są ważne z punktu widzenia pracodawców. W przypadku sektora telekomunikacji, średnia wartość ważności zawiera się w przedziale od 4,26 (znajomość języków obcych – szczególnie angielskiego w przypadku stanowisk inżynierskich) do 4,8 (umiejętność przeprowadzania testów jednostkowych w przypadku stanowiska Quality Assurance). W sektorze cyberbezpieczeństwa średnia ta oscyluje między 3,87 (kreatywność w przypadku stanowiska Penetration Tester) a 4,84 (niezależność w przypadku stanowiska audytor bezpieczeństwa).

Analiza średnich samoocen kompetencji posiadanych przez pracowników pozwala określić, że w sektorze telekomunikacji średnio najniżej (ale relatywnie wciąż wysoko) oceniana jest znajomość języków obcych (szczególnie angielskiego) w przypadku stanowisk inżynierskich (średnia na poziomie: 4,07), a najwyżej umiejętność korzystania z technologii umożliwiającej pracę zdalną w przypadku stanowiska Developer (programista) (średnia na poziomie: 4,55). W sektorze cyberbezpieczeństwa, samoocena umiejętności jest średnio najniższa w przypadku wiedzy z zakresu prawa i aktualnych regulacji prawnych dla stanowiska architekt ds. bezpieczeństwa (średnia wartość: 3,67), a najwyższa w przypadku wiedzy z zakresu bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych) dla stanowiska CISO (średnia wartość: 4,61).

Odrębnym, uniwersalnym stanowiskiem jest natomiast stanowisko dyrektora handlowego, w przypadku którego średnia ważność kompetencji (z perspektywy pracodawców) zawiera się w przedziale od 4,25 (w przypadku umiejętności współpracy w zespole międzynarodowym) do 4,55 (w przypadku umiejętności prowadzenia rozmów z kontrahentami), a pracownicza samoocena w przedziale od 4,05 (wiedza z zakresu prawa) do 4,45 (odpowiedzialność).

W sektorze telekomunikacji, kompetencje relatywnie ważniejsze dla pracodawców z niższą samooceną pracowników (kompetencje niedoboru), które są obecnie trudno dostępne (luka kompetencyjna) i których znaczenie będzie rosło[44] (kompetencje przyszłości), dotyczą wyłącznie stanowiska Quality Assurance. Są to: umiejętność poprawy jakości i czytelności kodu oraz umiejętność identyfikacji błędów w działaniu systemu, programu, usług.
W sektorze cyberbezpieczeństwa stanowisk, których dotyczy omawiana kwestia, jest zdecydowanie więcej. Ekspert ds. bezpieczeństwa jest stanowiskiem z najwyższą ich liczbą[45], a na drugim miejscu plasuje się architekt ds. bezpieczeństwa[46]. W przypadku pozostałych stanowisk kompetencje spełniające założenie występują raczej pojedynczo.

Analizując kompetencje, które będą zyskiwać na znaczeniu w sektorze telekomunikacji, wskazać należy: umiejętność przeprowadzania/pisania testów automatycznych, podstawową znajomość języków programowania i technologii (np. Python, C , C#, Java, JavaScript, Angular, React, Skala itp.), wiedzę z zakresu wykorzystywania technologii chmurowych, wiedzę z zakresu technologii komputerowych (z naciskiem na najnowsze) oraz umiejętność poprawy jakości i czytelności kodu. W sektorze cyberbezpieczeństwa są to natomiast: umiejętność planowania strategii ataków cyfrowych, znajomość norm prawnych w zakresie pen-testów i odpowiedzialności pen-testera, umiejętność blokowania zagrożeń (również potencjalnych), wysoki poziom komunikacji interpersonalnej oraz umiejętność zbierania informacji oraz weryfikacji ich rzetelności.

[44] W ocenie co najmniej 30% pracodawców.

[45] Kompetencje spełniające założenie: umiejętność obsługi platform bezpieczeństwa (np. firewalle aplikacyjne, sieciowe); umiejętność blokowania zagrożeń (w tym potencjalnych sytuacji zagrożenia); wiedza z zakresu systemów plików i zasad ich działania; umiejętność obsługi systemów i sieci pod względem zabezpieczeń; umiejętność odzyskiwania utraconych (np. w wyniku incydentu) danych; wiedza z zakresu systemów operacyjnych; umiejętność rozpoznawania cyberataków bądź niepokojących incydentów.

[46] Kompetencje spełniające założenie: wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające); odpowiedzialność; umiejętność zarządzania systemami bezpieczeństwa; umiejętność przewidywania, w jaki sposób może dojść do ataku na dany system, program, usługę; znajomość języków obcych – szczególnie angielskiego.

7.1. Bilans dla stanowisk kluczowych w sektorze telekomunikacji

7.1.1. Architekt systemów

W grupie **kompetencji niedoboru** dla tego stanowiska znalazły się kompetencje: wiedza z obszaru baz danych, chęć ciągłego rozwoju oraz umiejętność pracy z wykorzystaniem metodyk zwinnych (agile, scrum). Żadna z tych kompetencji nie znalazła się w luce kompetencyjnej.

Grupa **kompetencji zrównoważonych** jest liczniejsza, a w jej skład wchodzą: wiedza dziedzinowa z zakresu telekomunikacji, umiejętność zarządzania systemami, programami wewnątrzfirmowymi, umiejętność rozwiązywania problemów, analityczne myślenie, kreatywność, wiedza z zakresu technologii komputerowych (z naciskiem na najnowsze), znajomość zwinnych metodyk pracy (agile, scrum), umiejętność korzystania z technologii umożliwiających pracę zdalną oraz podstawowa znajomość wzorców projektowych. Dwie z tych kompetencji (i jedyne dla tego profilu) znalazły się w luce kompetencyjnej. Są to: umiejętność zarządzania systemami, programami wewnątrzfirmowymi oraz znajomość zwinnych metodyk pracy (agile, scrum).

Grupę **kompetencji nadwyżkowych** tworzą: znajomość języków obcych (głównie angielskiego) oraz skuteczne komunikowanie się.

Ostatnią grupą są **kompetencje wystarczające**, do których zaliczono: wiedzę z obszaru architektury systemów/informacji, umiejętność pracy zespołowej, umiejętność dopasowania metod, narzędzi do potrzeb danego problemu/projektu, umiejętność projektowania spójnej i logicznej architektury systemów, wiedzę z zakresu wykorzystywania technologii chmurowych oraz podstawową znajomość języków programowania, technologii (np. Python, C, C#, Java, JavaScript, Angular, React, Skala itp.).

Kompetencje zyskujące na znaczeniu w przyszłości wskazywane najczęściej to: podstawowa znajomość języków programowania, technologii (wzrost znaczenia przewidywany przez: 37% przedsiębiorców; samoocena pracowników: 4,25), wiedza z zakresu technologii komputerowych (37%; 4,34) oraz wiedza dziedzinowa z zakresu telekomunikacji (36%; 4,37). Pierwsza z nich jest obecnie kompetencją wystarczającą, dwie pozostałe to kompetencje zrównoważone.

Tabela 12. Architekt systemów – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Wiedza dziedzinowa z zakresu telekomunikacji	4,63	4,37	zrównoważone	nie	36
Umiejętność zarządzania systemami, programami wewnątrzfirmowymi	4,61	4,4	zrównoważone	tak	31
Umiejętność rozwiązywania problemów	4,59	4,36	zrównoważone	nie	21
Wiedza z obszaru baz danych	4,56	4,26	niedoboru	nie	31
Analityczne myślenie	4,56	4,31	zrównoważone	nie	23
Kreatywność	4,56	4,31	zrównoważone	nie	16
Wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)	4,56	4,34	zrównoważone	nie	37
Chęć ciągłego rozwoju	4,56	4,2	niedoboru	nie	22
Umiejętność pracy z wykorzystaniem metodyk zwinnych (agile, scrum)	4,55	4,21	niedoboru	nie	33
Znajomość zwinnych metodyk pracy (agile, scrum)	4,55	4,4	zrównoważone	tak	36
Umiejętność korzystania z technologii umożliwiających pracę zdalną	4,55	4,31	zrównoważone	nie	21
Podstawowa znajomość wzorców projektowych	4,53	4,42	zrównoważone	nie	30
Wiedza z obszaru architektury systemów, architektury informacji	4,5	4,28	wystarczające	n/d	23
Umiejętność pracy zespołowej	4,48	4,18	wystarczające	n/d	21
Umiejętność dopasowania metod, narzędzi do potrzeb danego problemu/projektu	4,47	4,24	wystarczające	n/d	28
Umiejętność projektowania spójnej i logicznej architektury systemów	4,47	4,12	wystarczające	n/d	25
Znajomość języków obcych – szczególnie angielskiego	4,47	4,4	nadwyżkowe	n/d	24
Wiedza z zakresu wykorzystywania technologii chmurowych	4,46	4,19	wystarczające	n/d	34
Podstawowa znajomość języków programowania, technologii (np. Python, C , C#, Java, JavaScript, Angular, React, Skala itp.)	4,42	4,25	wystarczające	n/d	37
Skuteczne komunikowanie się	4,42	4,3	nadwyżkowe	n/d	12

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 179, n = 89.

7.1.2. Inżynier (każdej specjalizacji: sieciowej, bezprzewodowej, satelitarnej)

W przypadku kluczowego stanowiska, jakim jest inżynier (niezależnie od specjalizacji), ważną informacją jest to, że żadna kompetencja nie została zaklasyfikowana do luki kompetencyjnej, co oznacza, że kompetencje relatywnie ważniejsze dla pracodawców nie są trudno dostępne.

Na grupę **kompetencji niedoboru** dla tego profilu składają się dwie kompetencje: wiedza z zakresu łączności przewodowej, bezprzewodowej, radiowej, satelitarnej oraz zapewnianie zabezpieczeń dostępu do urządzeń, narzędzi. O przewidywanym wzroście ich znaczenia w przyszłości mówiło natomiast odpowiednio: 20% oraz 23%[47] przedsiębiorców.

W grupie **kompetencji zrównoważonych** znalazło się 9 następujących kompetencji: wiedza z zakresu wiodących technologii w branży, umiejętność projektowania sieci przewodowych i bezprzewodowych, umiejętność tworzenia zrozumiałych dokumentacji technicznych, umiejętność związana z rozumieniem dokumentacji technicznych, umiejętność samodzielnego rozwiązywania problemów, zadań, konfiguracja urządzeń, umiejętność wyszukiwania informacji oraz weryfikacji ich rzetelności, skuteczne komunikowanie się oraz wiedza z zakresu systemów i oprogramowania.

Trzecia grupa to – niezbyt liczne dla tego profilu – **kompetencje nadwyżkowe**: konserwacja urządzeń, umiejętność wdrażania nowych technologii do użytku oraz umiejętność pracy w zespole.

Grupę **kompetencji wystarczających** tworzą: chęć ciągłego rozwoju oraz znajomość języków obcych – szczególnie angielskiego.

Kompetencje, których znaczenie ma szansę wzrosnąć w przyszłości, to: wiedza z zakresu wiodących technologii w branży (wzrost znaczenia przewidywany przez: 27% przedsiębiorców; samoocena pracowników: 4,26), umiejętność wdrażania nowych technologii do użytku (25%; 4,26) oraz zapewnianie zabezpieczeń dostępu do urządzeń i narzędzi (23%; 4,21). Są to odpowiednio kompetencje: zrównoważona, nadwyżkowa i niedoboru.

[47] Trzeci, pod względem odsetka odpowiedzi pracodawców, wynik wskazujący na wzrost znaczenia analizowanej w ramach tego stanowiska kompetencji w przyszłości.

Tabela 13. Inżynier (każdej specjalizacji: sieciowej, bezprzewodowej, satelitarnej) – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Wiedza z zakresu wiodących technologii w branży	4,51	4,26	zrównoważone	nie	27
Umiejętność projektowania sieci przewodowych, bezprzewodowych	4,51	4,26	zrównoważone	nie	21
Umiejętność tworzenia zrozumiałych dokumentacji technicznych	4,49	4,31	zrównoważone	nie	22
Umiejętność związana z rozumieniem dokumentacji technicznych	4,47	4,26	zrównoważone	nie	22
Umiejętność samodzielnego rozwiązywania problemów, zadań	4,46	4,35	zrównoważone	nie	16
Wiedza z zakresu łączności przewodowej, bezprzewodowej, radiowej, satelitarnej	4,45	4,2	niedoboru	nie	20
Konfiguracja urządzeń	4,45	4,3	zrównoważone	nie	22
Umiejętność wyszukiwania informacji oraz weryfikacji ich rzetelności	4,45	4,33	zrównoważone	nie	17
Skuteczne komunikowanie się	4,43	4,32	zrównoważone	nie	15
Wiedza z zakresu systemów i oprogramowania	4,41	4,25	zrównoważone	nie	22
Zapewnianie zabezpieczeń dostępu do urządzeń, narzędzi	4,41	4,21	niedoboru	nie	23
Konserwacja urządzeń	4,4	4,27	nadwyżkowe	n/d	21
Umiejętność wdrażania nowych technologii do użytku	4,39	4,26	nadwyżkowe	n/d	25
Chęć ciągłego rozwoju	4,39	4,2	wystarczające	n/d	16
Umiejętność pracy w zespole	4,34	4,26	nadwyżkowe	n/d	12
Znajomość języków obcych – szczególnie angielskiego	4,26	4,07	wystarczające	n/d	20

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 349; n = 187.

7.1.3. Developer (programista)

W grupie **kompetencji niedoboru** dla tego profilu znalazły się: wiedza dziedzinowa z zakresu telekomunikacji, umiejętność pracy w oparciu o dokumentację, wymagania i wytyczne projektu oraz umiejętność przeprowadzania testów jednostkowych.

Grupę **kompetencji zrównoważonych** tworzą: chęć ciągłego rozwoju, umiejętność kodowania w oparciu o user story, umiejętność korzystania z technologii umożliwiających pracę zdalną, znajomość języków programowania (np. Python, C, C#, Java, JavaScript, Angular, React, Skala itp.), umiejętność poprawy jakości i czytelności kodu, umiejętność pracy z wykorzystaniem metodyk zwinnych (agile, scrum), kreatywność, znajomość wzorców projektowych, umiejętność rozwiązywania problemów oraz skuteczne komunikowanie się. Wymienione wyżej: umiejętność kodowania w oparciu o user story oraz znajomość języków programowania znalazły się w luce kompetencyjnej. Są to jedyne kompetencje w ramach tego profilu, które zidentyfikowano w ramach luki.

Kompetencje nadwyżkowe są nieliczne – są to jedynie: analityczne myślenie oraz umiejętność pracy zespołowej.

Kompetencje wystarczające są niemal tak liczne jak kompetencje zrównoważone. W grupie tej znalazły się: wiedza z zakresu technologii komputerowych (w tym najnowszych technologii), umiejętność pisania kodu (programowania), znajomość architektury programowanego systemu lub usługi, znajomość zwinnych metodyk pracy (agile, scrum), wiedza z zakresu wykorzystywania technologii chmurowych, znajomość języków obcych (szczególnie angielskiego), znajomość najbardziej aktualnych i optymalnych sposobów pisania kodu oraz znajomość Github lub podobnego oprogramowania do kontroli wersji.

Kompetencje najczęściej wskazywane jako te, które zyskają na znaczeniu w ciągu trzech najbliższych lat: znajomość wzorców projektowych (wzrost znaczenia przewidywany przez: 31% przedsiębiorców; samoocena pracowników: 4,49), znajomość architektury programowanego systemu lub usługi (30%; 4,32) oraz umiejętność przeprowadzania testów jednostkowych (30%; 4,32). Są to odpowiednio kompetencje: zrównoważona, wystarczająca i niedoboru.

Tabela 14. Developer (programista) – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Chęć ciągłego rozwoju	4,68	4,49	zrównoważone	nie	24
Umiejętność kodowania w oparciu o user story	4,66	4,45	zrównoważone	tak	28
Umiejętność korzystania z technologii umożliwiających pracę zdalną	4,64	4,55	zrównoważone	nie	27
Wiedza dziedzinowa z zakresu telekomunikacji	4,64	4,33	niedoboru	nie	28
Znajomość języków programowania (np. Python, C, C#, Java, JavaScript, Angular, React, Skala itp.)	4,63	4,43	zrównoważone	tak	29
Umiejętność poprawy jakości i czytelności kodu	4,63	4,41	zrównoważone	nie	27
Umiejętność pracy z wykorzystaniem metodyk zwinnych (agile, scrum)	4,60	4,44	zrównoważone	nie	28
Umiejętność pracy w oparciu o dokumentację, wymagania i wytyczne projektu	4,60	4,39	niedoboru	nie	27
Kreatywność	4,59	4,48	zrównoważone	nie	22
Znajomość wzorców projektowych	4,59	4,49	zrównoważone	nie	31
Umiejętność rozwiązywania problemów	4,59	4,46	zrównoważone	nie	20
Skuteczne komunikowanie się	4,59	4,52	zrównoważone	nie	22
Umiejętność przeprowadzania testów jednostkowych	4,58	4,32	niedoboru	nie	30
Wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)	4,57	4,3	wystarczające	n/d	26
Umiejętność pisania kodu (programowania)	4,57	4,31	wystarczające	n/d	24
Znajomość architektury programowanego systemu lub usługi	4,56	4,32	wystarczające	n/d	30
Znajomość zwinnych metodyk pracy (agile, scrum)	4,56	4,36	wystarczające	n/d	27
Wiedza z zakresu wykorzystywania technologii chmurowych	4,55	4,39	wystarczające	n/d	23
Analityczne myślenie	4,55	4,49	nadwyżkowe	n/d	19
Umiejętność pracy zespołowej	4,54	4,44	nadwyżkowe	n/d	21
Znajomość języków obcych – szczególnie angielskiego	4,54	4,33	wystarczające	n/d	23
Znajomość najbardziej aktualnych i optymalnych sposobów pisania kodu	4,51	4,31	wystarczające	n/d	28
Znajomość Github lub podobnego oprogramowania do kontroli wersji	4,48	4,39	wystarczające	n/d	29

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 363; n = 218.

7.1.4. Project Manager (kierownik projektu)

Grupę **kompetencji niedoboru** w analizowanym profilu tworzą: umiejętność zarządzania budżetem zespołu, umiejętność rozdzielania zadań zgodnie z umiejętnościami konkretnego działu, zespołu, pracownika, umiejętność samodzielnego rozwiązywania problemów oraz umiejętność motywowania pracowników. Żadna z tych kompetencji nie znalazła się w luce kompetencyjnej.

Z kolei **kompetencje zrównoważone** to grupa, do której kwalifikują się: znajomość wiodących technologii w branży, wiedza dziedzinowa z zakresu telekomunikacji, analityczne myślenie, odpowiedzialność, umiejętność pracy pod wpływem stresu oraz umiejętność tworzenia kosztorysów projektów. Dwie z nich – znajomość wiodących technologii w branży oraz umiejętność tworzenia kosztorysów projektów – znalazły się w luce kompetencyjnej.

Kompetencje nadwyżkowe w tym profilu to: chęć ciągłego rozwoju, znajomość języków obcych (szczególnie angielskiego), znajomość zwinnych metodyk pracy (agile, scrum) oraz umiejętność pracy zespołowej.

Najliczniejszą w tym profilu grupę **kompetencji wystarczających** tworzą: wiedza z zakresu zarządzania (projektem, pracownikami), znajomość procesów biznesowych, umiejętność pracy pod presją czasu, umiejętność efektywnego zarządzania zespołem, umiejętność prowadzenia negocjacji, wysoki poziom komunikacji interpersonalnej oraz umiejętność tworzenia strategii realizacji projektów.

Kompetencje wskazywane najczęściej przez przedsiębiorców **w kontekście wzrostu znaczenia w przyszłości**: wiedza dziedzinowa z zakresu telekomunikacji (wzrost znaczenia przewidywany przez: 35% przedsiębiorców; samoocena pracowników: 4,37), znajomość zwinnych metodyk pracy (agile, scrum) (34%; 4,32) oraz umiejętność tworzenia kosztorysów projektów (32%; 4,35). Znajomość zwinnych metodyk pracy to kompetencja nadwyżkowa, a dwie pozostałe to kompetencje zrównoważone.

Tabela 15. Project Manager (kierownik projektu) – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Umiejętność zarządzania budżetem zespołu	4,66	4,3	**niedoboru**	nie	17
Znajomość wiodących technologii w branży	4,63	4,5	**zrównoważone**	**tak**	30
Wiedza dziedzinowa z zakresu telekomunikacji	4,63	4,37	**zrównoważone**	nie	**35**
Umiejętność rozdzielania zadań zgodnie z umiejętnościami konkretnego działu, zespołu, pracownika	4,59	4,29	**niedoboru**	nie	23
Umiejętność samodzielnego rozwiązywania problemów	4,56	4,32	**niedoboru**	nie	23
Analityczne myślenie	4,56	4,41	**zrównoważone**	nie	22
Odpowiedzialność	4,54	4,35	**zrównoważone**	nie	19
Umiejętność pracy pod wpływem stresu	4,54	4,35	**zrównoważone**	nie	29
Umiejętność tworzenia kosztorysów projektów	4,52	4,35	**zrównoważone**	**tak**	**32**
Umiejętność motywowania pracowników	4,52	4,27	**niedoboru**	nie	18
Chęć ciągłego rozwoju	4,51	4,35	nadwyżkowe	n/d	26
Wiedza z zakresu zarządzania (projektem, pracownikami)	4,5	4,23	wystarczające	n/d	27
Znajomość języków obcych – szczególnie angielskiego	4,5	4,41	nadwyżkowe	n/d	16
Znajomość zwinnych metodyk pracy (agile, scrum)	4,49	4,32	nadwyżkowe	n/d	**34**
Znajomość procesów biznesowych	4,46	4,28	wystarczające	n/d	22
Umiejętność pracy zespołowej	4,44	4,34	nadwyżkowe	n/d	24
Umiejętność pracy pod presją czasu	4,44	4,2	wystarczające	n/d	30
Umiejętność efektywnego zarządzania zespołem	4,42	4,23	wystarczające	n/d	19
Umiejętność prowadzenia negocjacji	4,41	4,24	wystarczające	n/d	18
Wysoki poziom komunikacji interpersonalnej	4,40	4,27	wystarczające	n/d	16
Umiejętność tworzenia strategii realizacji projektów	4,39	4,24	wystarczające	n/d	20

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 158; n = 78.

7.1.5. Quality Assurance (tester)

Kompetencje niedoboru zidentyfikowane dla tego stanowiska, które dodatkowo spełniają kryterium luki kompetencyjnej to: umiejętność poprawy jakości i czytelności kodu, umiejętność przeprowadzania testów manualnych oraz umiejętność identyfikacji błędów w działaniu systemu, programu, usługi. Ważność tych kompetencji będzie wzrastać w opinii odpowiednio: 36%[48], 28% oraz 32% pracodawców. Również kompetencją niedoboru niebędącą jednak w luce jest wysoki poziom komunikacji interpersonalnej, którego wzrost znaczenia przewiduje 31% przedsiębiorców.

Kompetencje zrównoważone dla tego profilu to: umiejętność przeprowadzania testów jednostkowych, umiejętność przeprowadzania/pisania testów automatycznych, znajomość języków programowania (np. Python, Selenium itp.), dokładność, umiejętność pracy zespołowej oraz znajomość języków obcych (głównie angielskiego). Pierwsze trzy znalazły się w luce kompetencyjnej. Każda kompetencja zrównoważona, czyli relatywnie ważniejsza dla pracodawców i wyżej oceniana przez pracowników zyska na znaczeniu. Kompetencją testera z najwyższym odsetkiem wskazań pracodawców (38%[49]), jeśli chodzi o spodziewany wzrost znaczenia w przyszłości, jest umiejętność przeprowadzania/pisania testów automatycznych.

Kompetencje nadwyżkowe w przypadku Quality Assurance to: znajomość architektury programowanego systemu lub usługi, rzetelność, wiedza dziedzinowa z zakresu telekomunikacji, cierpliwość, chęć ciągłego rozwoju, umiejętność korzystania z technologii umożliwiających pracę zdalną oraz analityczne myślenie.

Ostatnia grupa – **kompetencje wystarczające** – tworzona jest przez następujące kompetencje: znajomość zwinnych metodyk pracy (agile, scrum), wiedza z zakresu wykorzystywania technologii chmurowych, umiejętność tworzenia rekomendacji w celu naprawy błędów systemu, programu, usługi, umiejętność pracy z wykorzystaniem metodyk zwinnych (agile, scrum) oraz wiedza z zakresu User Experience (UX).

[48] Trzecia, pod względem wskazań pracodawców, kompetencja analizowana w ramach tego stanowiska, która zyska na znaczeniu w przyszłości.

[49] Jest to kompetencja w ramach analizowanego stanowiska, którą wskazał największy odsetek przedsiębiorców w kontekście przewidywanego wzrostu znaczenia w ciągu najbliższych 3 lat.

Najczęściej wskazywanymi **kompetencjami, które będą zyskiwać na znaczeniu,** są: umiejętność przeprowadzania/pisania testów automatycznych (wzrost znaczenia przewidywany przez: 37% przedsiębiorców; samoocena pracowników: 4,46), wiedza z zakresu wykorzystywania technologii chmurowych (37%; 4,36) oraz umiejętność poprawy jakości i czytelności kodu (36%; 4,36). Są to odpowiednio kompetencje: zrównoważona, wystarczająca i niedoboru.

Tabela 16. Quality Assurance (tester) – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Umiejętność przeprowadzania testów jednostkowych	4,8	4,48	zrównoważone	tak	28
Umiejętność przeprowadzania/pisania testów automatycznych	4,76	4,46	zrównoważone	tak	37
Dokładność	4,71	4,43	zrównoważone	nie	28
Umiejętność poprawy jakości i czytelności kodu	4,69	4,36	niedoboru	tak	36
Umiejętność pracy zespołowej	4,68	4,4	zrównoważone	nie	29
Wysoki poziom komunikacji interpersonalnej	4,67	4,39	niedoboru	nie	31
Umiejętność przeprowadzania testów manualnych	4,65	4,38	niedoboru	tak	28
Umiejętność identyfikacji błędów w działaniu systemu, programu, usługi	4,61	4,34	niedoboru	tak	32
Znajomość języków obcych – szczególnie angielskiego	4,6	4,47	zrównoważone	nie	28
Znajomość języków programowania (np. Python, Selenium itp.)	4,59	4,43	zrównoważone	tak	22
Znajomość architektury programowanego systemu lub usługi	4,55	4,43	nadwyżkowe	n/d	36
Rzetelność	4,54	4,43	nadwyżkowe	n/d	20
Wiedza dziedzinowa z zakresu telekomunikacji	4,52	4,44	nadwyżkowe	n/d	30
Chęć ciągłego rozwoju	4,5	4,43	nadwyżkowe	n/d	26
Umiejętność korzystania z technologii umożliwiających pracę zdalną	4,5	4,44	nadwyżkowe	n/d	29
Znajomość zwinnych metodyk pracy (agile, scrum)	4,5	4,2	wystarczające	n/d	35
Wiedza z zakresu wykorzystywania technologii chmurowych	4,48	4,36	wystarczające	n/d	37

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Umiejętność tworzenia rekomendacji w celu naprawy błędów systemu, programu, usługi	4,46	4,39	wystarczające	n/d	32
Umiejętność pracy z wykorzystaniem metodyk zwinnych (agile, scrum)	4,46	4,37	wystarczające	n/d	33
Analityczne myślenie	4,45	4,44	nadwyżkowe	n/d	31
Wiedza z zakresu User Experience (UX)	4,45	4,23	wystarczające	n/d	35
Cierpliwość	4,42	4,43	nadwyżkowe	n/d	23

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 163; n = 90.

7.2. Bilans dla stanowisk kluczowych w sektorze cyberbezpieczeństwa

7.2.1. CISO (ang. Chief Information Security Officer, pol. dyrektor ds. bezpieczeństwa informacji)

Kompetencje niedoboru w ramach profilu CISO są stosunkowo liczne. Do grupy tych kompetencji należą: umiejętność zarządzania ryzykiem przy podejmowaniu decyzji, umiejętność projektowania strategii bezpieczeństwa fizycznego (np. dostępu do budynków, dokumentów, BHP), wiedza z zakresu technologii komputerowych (w tym najnowszych technologii), wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające), umiejętność identyfikacji aktywów firmowych (np. dokumenty, sprzęty, systemy, programy) oraz umiejętność projektowania strategii bezpieczeństwa produktów cyfrowych (systemy zabezpieczeń, programy zabezpieczające). Dwie z nich (umiejętność projektowania strategii bezpieczeństwa fizycznego oraz wiedza z zakresu bezpieczeństwa cyfrowego) znalazły się w luce kompetencyjnej.

Kompetencje zrównoważone są równoliczne z kompetencjami niedoboru. Należą do nich: umiejętność weryfikacji podatności aktywów firmowych (np. dokumentów, sprzętów, systemów, programów), znajomość języków obcych (głównie angielskiego), wiedza z zakresu

bezpieczeństwa fizycznego (np. dostęp do budynków, dokumentów, BHP), wiedza z zakresu bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych), wysoki poziom komunikacji interpersonalnej, charyzma. Większość z tych kompetencji znalazła się w luce kompetencyjnej.

W ramach **kompetencji nadwyżkowych** możemy znaleźć: umiejętność pracy zespołowej, kreatywność, umiejętność projektowania strategii bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych), umiejętność korzystania z technologii umożliwiających pracę zdalną oraz odpowiedzialność.

Grupa **kompetencji wystarczających** jest najmniej liczną w ramach profilu CISO. Cztery kompetencje w tej grupie to: wiedza ogólna, interdyscyplinarna (przede wszystkim z zakresu biznesu, technologii, prawa), analityczne myślenie, chęć ciągłego rozwoju oraz umiejętność zarządzania zespołem.

Najczęściej wymieniane **kompetencje, które będą zyskiwać na znaczeniu w przyszłości,** dla stanowiska CISO to: wiedza z zakresu bezpieczeństwa cyfrowego (wzrost znaczenia przewidywany przez: 37% przedsiębiorców; samoocena pracowników: 4,18), charyzma (35%; 4,61) oraz umiejętność projektowania strategii bezpieczeństwa produktów cyfrowych (33%; 4,32). Pierwsza i trzecia z nich to kompetencje niedoboru, zaś druga wymieniona to kompetencja zrównoważona.

Tabela 17. CISO (Chief Information Security Officer, pol. dyrektor ds. bezpieczeństwa informacji) – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Umiejętność zarządzania ryzykiem w podejmowanych decyzjach	4,55	4,25	**niedoboru**	nie	30
Umiejętność projektowania strategii bezpieczeństwa fizycznego (np. dostęp do budynków, dokumentów, BHP)	4,43	4,14	**niedoboru**	**tak**	32
Umiejętność weryfikacji podatności aktywów firmowych (np. dokumenty, sprzęty, systemy, programy)	4,41	4,43	**zrównoważone**	**tak**	10

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Znajomość języków obcych – szczególnie angielskiego	4,40	4,39	zrównoważone	nie	23
Wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)	4,37	4,04	niedoboru	nie	29
Wiedza z zakresu bezpieczeństwa fizycznego (np. dostęp do budynków, dokumentów, BHP)	4,33	4,46	zrównoważone	tak	23
Wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające)	4,33	4,18	niedoboru	tak	37
Wiedza z zakresu bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych)	4,31	4,61	zrównoważone	nie	32
Umiejętność identyfikacji aktywów firmowych (np. dokumenty, sprzęty, systemy, programy)	4,29	4,25	niedoboru	nie	10
Wysoki poziom komunikacji interpersonalnej	4,28	4,54	zrównoważone	tak	17
Umiejętność projektowania strategii bezpieczeństwa produktów cyfrowych (systemy zabezpieczeń, programy zabezpieczające)	4,25	4,32	niedoboru	nie	33
Charyzma	4,24	4,61	zrównoważone	tak	35
Umiejętność pracy zespołowej	4,12	4,43	nadwyżkowe	n/d	14
Wiedza ogólna, interdyscyplinarna, przede wszystkim z zakresu biznesu, technologii, prawa	4,10	4,11	wystarczające	n/d	15
Kreatywność	4,07	4,39	nadwyżkowe	n/d	29
Umiejętność projektowania strategii bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych)	4,07	4,43	nadwyżkowe	n/d	32
Analityczne myślenie	4,03	4,11	wystarczające	n/d	23
Umiejętność korzystania z technologii umożliwiających pracę zdalną	3,97	4,39	nadwyżkowe	n/d	20
Odpowiedzialność	3,94	4,50	nadwyżkowe	n/d	21
Chęć ciągłego rozwoju	3,93	4,11	wystarczające	n/d	27
Umiejętność zarządzania zespołem	3,91	4,32	wystarczające	n/d	19

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 52; n = 28.

7.2.2. Audytor bezpieczeństwa

Analizując bilans kompetencji w ramach niniejszego kluczowego stanowiska należy mieć świadomość relatywnie niskiej liczby obserwacji (n = 25 w badaniu pracodawców oraz n = 29[50] w badaniu pracowników)[51]. Podane liczebności zasadnicze, gdyby ściśle trzymać się reguł wnioskowania statystycznego, uniemożliwiają wnioskowanie w tym zakresie. Nadal jednak omówione niżej wyniki można traktować jako pewien zarys zjawiska.

Kompetencje niedoboru w ramach tego profilu to: umiejętność identyfikacji i analizy ryzyka w konkretnych sposobach zabezpieczenia systemów, produktów, usług, rzetelność, wiedza z zakresu technologii komputerowych (w tym najnowszych technologii), znajomość języków obcych (głównie angielskiego) oraz obiektywizm. Pierwsze trzy znalazły się w luce kompetencyjnej.

Kompetencje zrównoważone w profilu audytor bezpieczeństwa są relatywnie nieliczne. Z grupy trzech kompetencji: niezależność, wiedza ogólna, interdyscyplinarna (przede wszystkim z zakresu biznesu, technologii, psychologii) oraz wysoki poziom komunikacji interpersonalnej, w luce kompetencyjnej znalazła się tylko niezależność.

Grupa **kompetencji nadwyżkowych** jest równie mało liczna. Liczy dwie kompetencje: umiejętność oceny firm, systemów, produktów, usług w oparciu o konkretne normy i standardy oraz wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające).

Ostatnią, najliczniejszą w tym profilu, grupę stanowią **kompetencje wystarczające**. Tworzą ją: wiedza z zakresu bezpieczeństwa fizycznego (np. dostęp do budynków, dokumentów, BHP), chęć ciągłego rozwoju, umiejętność weryfikacji podatności systemów, produktów, usług, wiedza z zakresu bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych), profesjonalizm, wiedza z zakresu prawa i aktualnych regulacji

[50] Liczba pracowników zatrudnionych na danym stanowisku i biorących udział w badaniu może być wyższa niż liczba pracodawców je oceniających co wynika z założenia pozyskiwania do badania respondentów. Nawet jeżeli w firmie występowało więcej kluczowych stanowisk niż dwa, pracodawca oceniał tylko dwa profile, natomiast do badania pracowników pracodawca mógł wyznaczyć osobę zajmującą inne kluczowe stanowisko niż oceniane.

[51] Liczebność próby jest w tym przypadku pochodną całkowitej próby dla sektora cyberbezpieczeństwa, w ramach której wyodrębniono profil kompetencyjny audytor bezpieczeństwa.

prawnych oraz umiejętność sporządzania zrozumiałych rekomendacji dla podmiotów, w których prowadzony jest audyt.

Kompetencjami wskazywanymi najczęściej jako te, **których znaczenie będzie rosło w przyszłości,** są: niezależność (wzrost znaczenia przewidywany przez: 49% przedsiębiorców; samoocena pracowników: 4,52), umiejętność weryfikacji podatności systemów, produktów, usług (37%; 4,41) oraz wiedza z zakresu bezpieczeństwa fizycznego (33%, 4,34).

Tabela 18. Audytor bezpieczeństwa – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Niezależność	4,84	4,52	zrównoważone	tak	49
Umiejętność identyfikacji i analizy ryzyka w konkretnych sposobach zabezpieczenia systemów, produktów, usług	4,62	4,24	niedoboru	tak	28
Rzetelność	4,53	4,34	niedoboru	tak	25
Wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)	4,51	4,38	niedoboru	tak	21
Znajomość języków obcych – szczególnie angielskiego	4,46	4,41	niedoboru	nie	12
Wiedza ogólna, interdyscyplinarna, przede wszystkim z zakresu biznesu, technologii, psychologii	4,44	4,45	zrównoważone	nie	31
Obiektywizm	4,43	4,34	niedoboru	nie	20
Wysoki poziom komunikacji interpersonalnej	4,39	4,48	zrównoważone	nie	29
Wiedza z zakresu bezpieczeństwa fizycznego (np. dostęp do budynków, dokumentów, BHP)	4,33	4,34	wystarczające	n/d	33
Umiejętność oceny firm, systemów, produktów, usług w oparciu o konkretne normy i standardy	4,32	4,48	nadwyżkowe	n/d	20
Chęć ciągłego rozwoju	4,32	4,41	wystarczające	n/d	29
Umiejętność weryfikacji podatności systemów, produktów, usług	4,29	4,41	wystarczające	n/d	37
Wiedza z zakresu bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych)	4,26	4,38	wystarczające	n/d	24
Profesjonalizm	4,24	4,41	wystarczające	n/d	24

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Wiedza z zakresu prawa i aktualnych regulacji prawnych	4,19	4,41	wystarczające	n/d	29
Umiejętność sporządzania zrozumiałych rekomendacji dla podmiotów, w których prowadzony jest audyt	4,12	4,34	wystarczające	n/d	12
Wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające)	4,05	4,59	nadwyżkowe	n/d	29

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 25; n = 29.

7.2.3. Architekt ds. bezpieczeństwa

Analizując bilans kompetencji w ramach niniejszego kluczowego stanowiska należy mieć świadomość relatywnie niskiej liczby obserwacji (n = 35 w badaniu pracodawców oraz n = 24 w badaniu pracowników)[52]. Z tego względu omówione niżej wyniki traktować należy jako pewien zarys zjawiska, który powinien być traktowany z dużą dozą ostrożności, aby uniknąć błędnego wnioskowania.

Kompetencje niedoboru w ramach tego profilu to: wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające), umiejętność przewidywania, w jaki sposób może dojść do ataku na dany system, program czy usługę, umiejętność zarządzania systemami bezpieczeństwa, znajomość języków obcych (głównie angielskiego) oraz odpowiedzialność. Każda z tych kompetencji znalazła się w luce kompetencyjnej.

W grupie **kompetencji zrównoważonych** znajdziemy następujące cztery kompetencje: wiedza z zakresu systemów operacyjnych (w tym systemów plików i zasad ich działania), wiedza z zakresu technologii komputerowych (w tym najnowszych technologii), umiejętność tworzenia zabezpieczeń dla systemów, programów czy usług oraz wiedza z zakresu działania

[52] Liczebność próby jest w tym przypadku pochodną całkowitej próby dla sektora cyberbezpieczeństwa, w ramach której wyodrębniono profil kompetencyjny architekt ds. bezpieczeństwa.

sieci komputerowych i urządzeń sieciowych. Również w przypadku tej grupy wszystkie kompetencje znalazły się w luce kompetencyjnej określonej dla tego profilu.

Kompetencje nadwyżkowe to: umiejętność wyszukiwania podatności systemów, programów czy usług, umiejętność projektowania architektury systemów bezpieczeństwa, umiejętność korzystania z technologii umożliwiających pracę zdalną, kreatywność, chęć ciągłego rozwoju, wysoki poziom komunikacji interpersonalnej.

Grupa **kompetencji wystarczających** to: umiejętność pracy zespołowej, umiejętność zarządzania zespołem, wiedza (przynajmniej podstawowa) z zakresu prawa i aktualnych regulacji prawnych.

Kompetencje najczęściej wymieniane przez pracodawców jako te, **których znaczenie będzie rosło** w przyszłości: wiedza z zakresu bezpieczeństwa cyfrowego (wzrost znaczenia przewidywany przez: 52% przedsiębiorców; samoocena pracowników: 4,08), wiedza z zakresu technologii komputerowych (49%; 4,13) oraz umiejętność tworzenia zabezpieczeń dla systemów, programów czy usług (48%; 4,29). Pierwsza z nich to kompetencja niedoboru, dwie pozostałe – kompetencje zrównoważone.

Tabela 19. Architekt ds. bezpieczeństwa – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające)	4,77	4,08	**niedoboru**	**tak**	**52**
Wiedza z zakresu działania sieci komputerowych i urządzeń sieciowych	4,6	4,17	**zrównoważone**	**tak**	37
Umiejętność tworzenia zabezpieczeń dla systemów, programów, usług	4,6	4,29	**zrównoważone**	**tak**	**48**
Odpowiedzialność	4,59	4,04	**niedoboru**	**tak**	38
Znajomość języków obcych – szczególnie angielskiego	4,5	3,88	**niedoboru**	**tak**	30
Umiejętność zarządzania systemami bezpieczeństwa	4,44	4,04	**niedoboru**	**tak**	42
Umiejętność przewidywania, w jaki sposób może dojść do ataku na dany system, program, usługę	4,41	3,96	**niedoboru**	**tak**	47
Wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)	4,39	4,13	**zrównoważone**	**tak**	**49**
Wiedza z zakresu systemów operacyjnych (w tym systemów plików i zasad ich działania)	4,37	4,17	**zrównoważone**	**tak**	38
Umiejętność pracy zespołowej	4,33	4,08	wystarczające	n/d	38
Kreatywność	4,29	4,13	nadwyżkowe	n/d	23
Umiejętność wyszukiwania podatności systemów, programów, usług	4,27	4,17	nadwyżkowe	n/d	41
Umiejętność projektowania architektury systemów bezpieczeństwa	4,25	4,13	nadwyżkowe	n/d	43
Umiejętność zarządzania zespołem	4,22	4	wystarczające	n/d	32
Umiejętność korzystania z technologii umożliwiających pracę zdalną	4,22	4,38	nadwyżkowe	n/d	37
Wysoki poziom komunikacji interpersonalnej	4,17	4,25	nadwyżkowe	n/d	33
Wiedza (przynajmniej podstawowa) z zakresu prawa i aktualnych regulacji prawnych	4,16	3,67	wystarczające	n/d	47
Chęć ciągłego rozwoju	4,13	4,21	nadwyżkowe	n/d	33

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 35; n = 24.

7.2.4. Penetration tester (tester penetracyjny)

Analizując bilans kompetencji w ramach niniejszego kluczowego stanowiska, należy mieć świadomość relatywnie niskiej liczby obserwacji (n = 18 w badaniu pracodawców oraz n = 10 w badaniu pracowników)[53]. Podane liczebności zasadnicze, gdyby ściśle trzymać się reguł wnioskowania statystycznego, uniemożliwiają wnioskowanie w tym zakresie. Nadal jednak omówione niżej wyniki można traktować jako pewien zarys zjawiska.

Trzy **kompetencje niedoboru** to: znajomość norm prawnych w zakresie pen-testów i odpowiedzialności pen-testera, umiejętność prowadzenia ataków cyfrowych (weryfikacji podatności systemów, produktów, usług) oraz umiejętność pisania skryptów (na potrzeby przeprowadzenia ataku). Tylko pierwsza z nich znalazła się w luce kompetencyjnej dla tego profilu.

Kompetencje zrównoważone to: wiedza z zakresu systemów operacyjnych (w tym systemów plików i zasad ich działania), wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające), umiejętność planowania strategii ataków cyfrowych oraz znajomość języków programowania (na potrzeby rozumienia jak działa dany program). Dwie z nich znalazły się w luce kompetencyjnej profilu.

Kompetencje nadwyżkowe to: chęć ciągłego rozwoju, znajomość języków obcych (szczególnie języka angielskiego), wiedza z zakresu bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych), kreatywność.

W grupie **kompetencji wystarczających** znalazły się: wysoki poziom komunikacji interpersonalnej, umiejętność zbierania informacji oraz weryfikacji ich rzetelności, wiedza z zakresu technologii komputerowych (w tym najnowszych technologii), wiedza z zakresu działania sieci komputerowych i urządzeń sieciowych oraz umiejętność testowania kanałów cyfrowego dostępu.

W przypadku analizowanego stanowiska **kompetencje, które będą zyskiwać na znaczeniu,** w opinii największej liczby przedsiębiorców to: umiejętność planowania strategii ataków cyfrowych (wzrost znaczenia przewidywany przez: 62% przedsiębiorców; samoocena pracowników: 4,5),

[53] Liczebność próby jest w tym przypadku pochodną całkowitej próby dla sektora cyberbezpieczeństwo, w ramach której wyodrębniono profil kompetencyjny testera penetracyjnego.

znajomość norm prawnych w zakresie pen-testów i odpowiedzialności pen-testera (60%; 4,3) oraz wysoki poziom komunikacji interpersonalnej i umiejętność zbierania informacji oraz weryfikacji ich rzetelności (po 53% każdy; 4,3 każdy). Pierwsza z nich to kompetencja niedoboru, druga – zrównoważona, a ostatnie dwie to kompetencje wystarczające.

Tabela 20. Penetration tester (tester penetracyjny) – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Wiedza z zakresu systemów operacyjnych (w tym systemów plików i zasad ich działania)	4,67	4,4	zrównoważone	nie	41
Wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające)	4,55	4,6	zrównoważone	tak	51
Umiejętność zaplanowania strategii ataków cyfrowych	4,55	4,5	zrównoważone	nie	62
Znajomość norm prawnych w zakresie pen-testów i odpowiedzialności pen-testera	4,48	4,3	niedoboru	tak	60
Umiejętność prowadzenia ataków cyfrowych (weryfikacji podatności systemów, produktów, usług)	4,44	4,1	niedoboru	nie	27
Znajomość języków programowania (na potrzeby rozumienia jak działa dany program)	4,32	4,4	zrównoważone	tak	50
Umiejętność pisania skryptów (na potrzeby przeprowadzenia ataku)	4,30	4,1	niedoboru	nie	43
Wysoki poziom komunikacji interpersonalnej	4,23	4,3	wystarczające	n/d	53
Umiejętność zbierania informacji oraz weryfikacji ich rzetelności	4,17	4,3	wystarczające	n/d	53
Chęć ciągłego rozwoju	4,16	4,5	nadwyżkowe	n/d	19
Znajomość języków obcych (szczególnie języka angielskiego)	4,15	4,6	nadwyżkowe	n/d	35
Wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)	4,13	4,3	wystarczające	n/d	30
Wiedza z zakresu działania sieci komputerowych i urządzeń sieciowych	4,03	4	wystarczające	n/d	19
Wiedza z zakresu bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych)	4,01	4,6	nadwyżkowe	n/d	52

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Umiejętność testowania kanałów cyfrowego dostępu	4	4,2	wystarczające	n/d	36
Kreatywność	3,87	4,5	nadwyżkowe	n/d	46

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 18; n = 10.

7.2.5. Koordynator SOC (ang. Security Operation Center, pol. Centrum operacji bezpieczeństwa)

Analizując bilans kompetencji w ramach niniejszego kluczowego stanowiska należy mieć świadomość relatywnie niskiej liczby obserwacji (n = 36 w badaniu pracodawców oraz n = 20 w badaniu pracowników)[54]. Z tego względu omówione niżej wyniki traktować należy jako pewien zarys zjawiska, który powinien być traktowany z dużą dozą ostrożności, aby uniknąć błędnego wnioskowania.

Grupę **kompetencji niedoboru** tworzą: wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające), znajomość języków obcych (szczególnie języka angielskiego), umiejętność blokowania zagrożeń (w tym potencjalnych sytuacji zagrożenia – prewencja), umiejętność poznawania cyberataków bądź niepokojących monitów, logów. Niemal wszystkie te kompetencje (z wyjątkiem kompetencji jaką jest znajomość języków obcych) znalazły się w luce kompetencyjnej.

Grupa **kompetencji zrównoważonych** jest równoliczna z grupą kompetencji niedoboru. Cztery kompetencje, które ją tworzą, to: wiedza z zakresu systemów plików i zasad ich działania, skuteczne komunikowanie się, umiejętność pracy w systemie zmianowym oraz dokładność. Dwie pierwsze znalazły się w luce kompetencyjnej.

[54] Liczebność próby jest w tym przypadku pochodną całkowitej próby dla sektora cyberbezpieczeństwa, w ramach której wyodrębniono profil kompetencyjny SOC.

Kompetencje nadwyżkowe są grupą najliczniejszą w tym profilu, stanowiąc blisko połowę kompetencji, które podlegały ocenie w tym profilu. Grupę kompetencji tworzą: cierpliwość, umiejętność zarządzania zespołem, umiejętność pracy zespołowej, chęć ciągłego rozwoju, umiejętność korzystania z technologii umożliwiających pracę zdalną, umiejętność podstawowej analizy kodu pod względem potencjalnych zagrożeń, umiejętność monitorowania systemów, sieci w celu identyfikacji zagrożeń, wiedza z zakresu technologii komputerowych (w tym najnowszych technologii) oraz umiejętność odzyskiwania utraconych (np. w wyniku incydentu) danych.

Najczęściej wskazywane **kompetencje, które** przewiduje się, że **będą zyskiwać na znaczeniu,** to przede wszystkim: umiejętność blokowania zagrożeń (wzrost znaczenia przewidywany przez: 49% przedsiębiorców; samoocena pracowników: 4,2), umiejętność odzyskiwania utraconych, np. w wyniku incydentu, danych (48%; 4,5) oraz umiejętność podstawowej analizy kodu pod względem potencjalnych zagrożeń i umiejętność monitorowania systemów, sieci w celu identyfikacji zagrożeń (po 39% każda; 4,4 każda). Pierwsza z nich to kompetencja niedoboru, pozostałe natomiast to kompetencje nadwyżkowe.

Tabela 21. Koordynator SOC – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Wiedza z zakresu systemów plików i zasad ich działania	4,73	4,5	zrównoważone	tak	23
Skuteczne komunikowanie się	4,71	4,4	zrównoważone	tak	24
Wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające)	4,6	4,35	niedoboru	tak	27
Znajomość języków obcych (szczególnie języka angielskiego)	4,54	4,25	niedoboru	nie	21
Umiejętność pracy w systemie zmianowym	4,51	4,4	zrównoważone	nie	12
Umiejętność zablokowania zagrożeń (w tym potencjalnych sytuacji zagrożenia – prewencja)	4,51	4,2	niedoboru	tak	49
Umiejętność rozpoznawania cyberataków bądź niepokojących monitów, logów	4,48	4,2	niedoboru	tak	37
Dokładność	4,45	4,4	zrównoważone	nie	12
Cierpliwość	4,41	4,6	nadwyżkowe	n/d	12

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Umiejętność zarządzania zespołem	4,4	4,42	nadwyżkowe	n/d	12
Umiejętność tworzenia raportów ze stanu cyberbezpieczeństwa	4,39	4,3	wystarczające	n/d	12
Umiejętność pracy zespołowej	4,38	4,58	nadwyżkowe	n/d	12
Chęć ciągłego rozwoju	4,37	4,5	nadwyżkowe	n/d	18
Umiejętność korzystania z technologii umożliwiających pracę zdalną	4,37	4,55	nadwyżkowe	n/d	12
Umiejętność podstawowej analizy kodu pod względem potencjalnych zagrożeń	4,32	4,4	nadwyżkowe	n/d	**39**
Umiejętność monitorowania systemów, sieci w celu identyfikacji zagrożeń	4,29	4,4	nadwyżkowe	n/d	**39**
Wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)	4,28	4,45	nadwyżkowe	n/d	19
Umiejętność odzyskiwania utraconych (np. w wyniku incydentu) danych	4,26	4,5	nadwyżkowe	n/d	**48**
Umiejętność użytkowania platform i narzędzi obsługujących logi i korelacje między nimi	4,26	4,2	wystarczające	n/d	18
Umiejętność przywracania sprawności dla zaatakowanego systemu, programu, usługi	4,14	4,25	wystarczające	n/d	38

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 36; n = 20.

7.2.6. Ekspert ds. bezpieczeństwa systemów/sieci/aplikacji

Analizując bilans kompetencji w ramach niniejszego kluczowego stanowiska należy mieć świadomość relatywnie niskiej liczby obserwacji (n = 52 w badaniu pracodawców oraz n = 37 w badaniu pracowników)[55]. Z tego względu omówione niżej wyniki traktować należy jako pewien zarys zjawiska, który powinien być traktowany z dużą dozą ostrożności, aby uniknąć błędnego wnioskowania.

[55] Liczebność próby jest w tym przypadku pochodną całkowitej próby dla sektora cyberbezpieczeństwo, w ramach której wyodrębniono profil kompetencyjny Ekspert ds. bezpieczeństwa systemów/sieci/aplikacji.

Najliczniejszą grupę w ramach tego profilu, grupę **kompetencji niedoboru**, tworzą: umiejętność obsługi platform bezpieczeństwa (np. firewalle aplikacyjne, sieciowe), wiedza z zakresu systemów plików i zasad ich działania, wiedza z zakresu systemów operacyjnych, umiejętność blokowania zagrożeń (w tym potencjalnych sytuacji zagrożenia), umiejętność obsługi systemów i sieci pod względem zabezpieczeń, umiejętność rozpoznawania cyberataków bądź niepokojących incydentów, umiejętność odzyskiwania utraconych (np. w wyniku incydentu) danych. Wszystkie z nich znalazły się w luce kompetencyjnej dla profilu.

Kompetencje zrównoważone to: wiedza z zakresu działania sieci komputerowych i urządzeń sieciowych, umiejętność nadawania uprawnień/dostępu do konkretnych narzędzi, programów, budynków itp., wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające), umiejętność przywracania sprawności dla zaatakowanego systemu, programu czy usługi oraz wiedza z zakresu technologii komputerowych (w tym najnowszych technologii). Również w tym przypadku wszystkie kompetencje znalazły się w luce kompetencyjnej[56].

Najmniej liczna grupa kompetencji w tym profilu to **kompetencje nadwyżkowe**, w skład których wchodzą: umiejętność zarządzania bazami danych (zarządzanie, przenoszenie, łączenie), umiejętność korzystania z technologii umożliwiających pracę zdalną, znajomość języków obcych (szczególnie języka angielskiego) oraz umiejętność pracy zespołowej.

Ostatnia, ale nie najmniej znacząca, grupa to **kompetencje wystarczające** tj.: dokładność, wiedza z zakresu baz danych, skuteczne komunikowanie się, chęć ciągłego rozwoju.

W przypadku analizowanego stanowiska **kompetencjami, które będą zyskiwać na znaczeniu** w opinii największej liczby pracodawców, są: umiejętność blokowania zagrożeń (wzrost znaczenia przewidywany przez: 55% przedsiębiorców; samoocena pracowników: 4,16), wiedza z zakresu technologii komputerowych (54%; 4,24) oraz umiejętność obsługi platform bezpieczeństwa (50%; 4,16). Umiejętność blokowania zagrożeń to kompetencja zrównoważona, pozostałe dwie to kompetencje niedoboru.

[56] Profil eksperta ds. bezpieczeństwa jest drugim – po architekcie ds. bezpieczeństwa – profilem, w którym taka sytuacja ma miejsce. Należy jednak wciąż mieć na uwadze informację dotycząca liczebności, na których opierają się analizy.

Tabela 22. Ekspert ds. bezpieczeństwa systemów/sieci/aplikacji – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Wiedza z zakresu działania sieci komputerowych i urządzeń sieciowych	4,61	4,24	zrównoważone	tak	43
Umiejętność nadawania uprawnień/dostępu do konkretnych narzędzi, programów, budynków itp.	4,57	4,3	zrównoważone	tak	30
Umiejętność obsługi platform bezpieczeństwa (np. firewalle aplikacyjne, sieciowe)	4,56	4,16	niedoboru	tak	50
Wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające)	4,54	4,22	zrównoważone	tak	43
Wiedza z zakresu systemów plików i zasad ich działania	4,52	4,11	niedoboru	tak	41
Umiejętność przywracania sprawności dla zaatakowanego systemu, programu, usługi	4,5	4,35	zrównoważone	tak	48
Wiedza z zakresu systemów operacyjnych	4,49	4,08	niedoboru	tak	42
Umiejętność zablokowania zagrożeń (w tym potencjalnych sytuacji zagrożenia)	4,48	4,16	niedoboru	tak	55
Umiejętność obsługi systemów i sieci pod względem zabezpieczeń	4,45	4,11	niedoboru	tak	48
Wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)	4,4	4,24	zrównoważone	tak	54
Umiejętność rozpoznawania cyberataków bądź niepokojących incydentów	4,39	4	niedoboru	tak	50
Umiejętność odzyskiwania utraconych (np. w wyniku incydentu) danych	4,36	4,08	niedoboru	tak	49
Dokładność	4,33	4,03	wystarczające	n/d	21
Wiedza z zakresu baz danych	4,29	4,05	wystarczające	n/d	45
Umiejętność zarządzania bazami danych (zarządzanie, przenoszenie, łączenie)	4,27	4,41	nadwyżkowe	n/d	34
Skuteczne komunikowanie się	4,19	4,08	wystarczające	n/d	12
Umiejętność korzystania z technologii umożliwiających pracę zdalną	4,18	4,54	nadwyżkowe	n/d	40
Chęć ciągłego rozwoju	4,10	4,03	wystarczające	n/d	15
Znajomość języków obcych (szczególnie języka angielskiego)	4,09	4,27	nadwyżkowe	n/d	15
Umiejętność pracy zespołowej	4,01	4,19	nadwyżkowe	n/d	8

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 52; n = 37.

7.3. Bilans dla stanowiska uniwersalnego w obu sektorach

7.3.1. Dyrektor handlowy/sprzedaży

Profil dyrektora handlowego jest analizowany wspólnie dla sektorów telekomunikacji oraz cyberbezpieczeństwa z uwagi na fakt, że na etapie operacjonalizacji (a więc przed rozpoczęciem badania) stanowisko to zostało określone stanowiskiem uniwersalnym.

Kompetencje niedoboru w ramach tego profilu to: umiejętność zarządzania projektami, chęć ciągłego rozwoju, wiedza z zakresu prawa, umiejętność motywowania zespołu, umiejętność prowadzenia negocjacji. W luce kompetencyjnej znalazła się wyłącznie wiedza z zakresu prawa.

Kompetencje zrównoważone to w przypadku analizowanego stanowiska: umiejętność prowadzenia rozmów z kontrahentami, wiedza produktowa (wiedza dotycząca właściwości technicznych i użytkowych sprzedawanych produktów), odpowiedzialność, umiejętność tworzenia kosztorysów, umiejętność przygotowania strategii i planów sprzedaży oraz orientacja na cel. Trzy z nich znalazły się w luce kompetencyjnej.

Kompetencje nadwyżkowe to: umiejętność analizy wymagań klienta, umiejętność oceny jakości ofert konkurencyjnych, umiejętność przekazywania wytycznych realizacji projektów oraz znajomość języków obcych (szczególnie języka angielskiego).

W grupie **kompetencji wystarczających** znalazły się: umiejętność pozyskiwania nowych zleceń dla firmy, wysoki poziom komunikacji interpersonalnej, wiedza z zakresu zarządzania (projektem, pracownikami) oraz umiejętność współpracy w zespole międzynarodowym.

Kompetencje, które zgodnie z przewidywaniami pracodawców **zyskają na znaczeniu w przyszłości,** to: wiedza z zakresu prawa (wzrost ważności przewidywany przez: 33% przedsiębiorców; samoocena pracowników: 4,05), umiejętność analizy wymagań klienta (27%; 4,29) oraz umiejętność współpracy w zespole międzynarodowym (26%; 4,21).
Są to odpowiednio kompetencje: niedoboru, nadwyżkowa i wystarczająca.

Tabela 23. Dyrektor handlowy/sprzedaży – tabela podsumowująca bilans kompetencji

Kompetencja	Średnia ocena ważności – pracodawcy	Średnia samoocena – pracownicy	Typ kompetencji	Luka kompetencyjna	Wzrost znaczenia w przyszłości (% wskazań pracodawców)
Umiejętność prowadzenia rozmów z kontrahentami	4,55	4,39	zrównoważone	tak	25
Wiedza produktowa (wiedza dotycząca właściwości technicznych i użytkowych sprzedawanych produktów)	4,54	4,44	zrównoważone	nie	24
Odpowiedzialność	4,53	4,45	zrównoważone	tak	20
Umiejętność tworzenia kosztorysów	4,45	4,38	zrównoważone	nie	17
Umiejętność zarządzania projektami	4,42	4,2	niedoboru	nie	22
Chęć ciągłego rozwoju	4,41	4,14	niedoboru	nie	21
Umiejętność przygotowania strategii i planów sprzedaży	4,4	4,33	zrównoważone	tak	21
Wiedza z zakresu prawa	4,4	4,05	niedoboru	tak	33
Umiejętność motywowania zespołu	4,4	4,23	niedoboru	nie	24
Orientacja na cel	4,4	4,32	zrównoważone	nie	20
Umiejętność prowadzenia negocjacji	4,39	4,19	niedoboru	nie	24
Umiejętność analizy wymagań klienta	4,39	4,29	nadwyżkowe	n/d	27
Umiejętność oceny jakości ofert konkurencyjnych	4,38	4,35	nadwyżkowe	n/d	19
Umiejętność pozyskiwania nowych zleceń dla firmy	4,35	4,18	wystarczające	n/d	22
Umiejętność przekazywania wytycznych realizacji projektów	4,35	4,28	nadwyżkowe	n/d	20
Wysoki poziom komunikacji interpersonalnej	4,34	4,09	wystarczające	n/d	20
Wiedza z zakresu zarządzania (projektem, pracownikami)	4,34	4,17	wystarczające	n/d	20
Znajomość języków obcych (szczególnie języka angielskiego)	4,26	4,28	nadwyżkowe	n/d	20
Umiejętność współpracy w zespole międzynarodowym	4,25	4,21	wystarczające	n/d	26

Źródło opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I; n = 164; n = 154.

8. Wyzwania stojące przed branżą telekomunikacji i cyberbezpieczeństwa w perspektywie kolejnych 3 lat

Analizy będące efektem prowadzonego projektu badawczego pozwoliły na określenie szeregu wyzwań: społecznych, gospodarczych, technologicznych oraz prawnych, przed którymi stoi branża telekomunikacji i cyberbezpieczeństwa. Ze względu na złożoność procesu badawczego wyzwania bazują na opiniach ekspertów wypowiadających się podczas jakościowych wywiadów indywidualnych, paneli eksperckich oraz badania delfickiego, a także na opiniach przedsiębiorców biorących udział w badaniu ilościowym[57]. Eksperci oraz przedsiębiorcy zdecydowanie różnią się w ocenie wyzwań, z jakimi mierzyć się będzie branża w najbliższych trzech latach. Rozdźwięk ten może być spowodowany odmienną perspektywą obu grup – eksperci wypowiadają się o rynku jako całości, natomiast przedsiębiorcy raczej patrzą na niego przez pryzmat własnych firm, w których dane wyzwanie ma lub nie ma szansy zaistnieć. Prawdopodobnie stąd też mało jednoznacznych opinii wśród przedsiębiorców.

Najważniejszym wyzwaniem dla firm z branży telekomunikacji i cyberbezpieczeństwa jest dbanie o rozwój pracowników w celu utrzymania przez nich zatrudnienia (51% odpowiedzi). Wyzwanie to nieznacznie częściej wskazują przedsiębiorcy z sektora cyberbezpieczeństwa (53%) niż telekomunikacji (51%). Eksperci branżowi zwracali uwagę, że w branży telekomunikacji i cyberbezpieczeństwa na kluczowych stanowiskach pracują specjaliści wysoko wykwalifikowani, którzy mają świadomość szybkości rozwoju branży. Dlatego właśnie tak ważne jest dla nich ciągłe podnoszenie swoich kompetencji, które zapewnia stabilność zatrudnienia. Istotna jest również możliwość awansu w wewnętrznych strukturach firmowych, co wiąże się ze zwiększeniem zakresu obowiązków, odpowiedzialności, ale także zwiększeniem poziomu kompetencji pracownika. Według

[57] Różnice w ocenie ekspertów oraz przedsiębiorców wynikają m.in. z zastosowanej metody badawczej (przedsiębiorcy uczestniczyli w ustrukturyzowanym wywiadzie ilościowym, który uniemożliwia zbytnie odejście od scenariusza) oraz różnego sposobu zadawania pytań.

ekspertów pracownicy oczekują, że to firma, w której pracują, będzie odpowiedzialna za zapewnienie odpowiednich możliwości rozwoju (inwestowanie w rozwój kompetencji i rozwój zawodowy pracownika, umożliwienie awansu wewnątrzfirmowego).

Niemal tak samo ważnym w obu sektorach i ogólnie drugim, pod względem istotności, wyzwaniem jest spełnienie norm i wymogów dla pojawiających się nowych technologii (50% odpowiedzi). Zgodnie z opiniami uzyskanymi od ekspertów w trakcie badania delfickiego, w perspektywie najbliższych trzech lat ujednolicone zostaną systemy certyfikacji w zakresie cyberbezpieczeństwa[58] (średnia dla wyzwania: 7,49 na 10 punktów). Według ekspertów, spełnienie właściwych dla dużych firm norm cyfrowego bezpieczeństwa będzie trudne do osiągnięcia dla mikro i małych przedsiębiorstw. Skutkiem tego zjawiska będzie coraz częściej występujący problem na linii współpracy pomiędzy mikro, małymi a dużymi firmami (ocena tego wyzwania otrzymała średnią 6,54 na 10 punktów).

Listę trzech kluczowych wyzwań zamyka informowanie klientów o zagrożeniach przy korzystaniu z technologii i usług telekomunikacyjnych/internetowych oferowanych przez firmy (46% odpowiedzi). Pomiędzy sektorami występuje różnica 4 p.p. na korzyść sektora cyberbezpieczeństwa. Pomimo że testowano wyłącznie kwestię informowania klientów, warto nadmienić, że konieczne jest również ich edukowanie (także przez firmy) w tym zakresie oraz wprowadzanie nowych rozwiązań technologicznych, które będą zmniejszać ryzyko tych zagrożeń. Opracowane rozwiązania mogłyby zostać oparte m.in. na teoriach psychologii kognitywnej. Również w tym przypadku możemy mówić o zachowaniu spójności z opiniami ekspertów, którzy wskazywali, że wraz z postępującą cyfryzacją i przenoszeniem kolejnych sfer życia do świata on-line, pojawia się coraz więcej zagrożeń wynikających z cyfrowej przestępczości[59]. Eksperci zwracali uwagę na oszustwa w świecie cyfrowym polegające np. na próbach wyłudzania pieniędzy lub kradzieży danych osobowych.

[58] „Mówi się o szkoleniach nie zwracając uwagi na efekty. Jeśli mówimy o szkoleniach uświadamiających management, ale też szkoleniach dla specjalistów, to szkolenia są, natomiast mierzenie efektów tego szkolenia już niekoniecznie, prawda? Lista obecności jest jedynym miernikiem i kryterium, to jest słabe.” (wypowiedź eksperta; panel podsumowujący).

[59] „To pokolenie zarazem bardzo samo narusza wszelkie zasady bezpieczeństwa, publikując na Facebookach niemal wszystkie kluczowe informacje prywatne, tak bardzo się odsłaniając. Więc tu przede wszystkim trzeba bardzo ich zacząć uświadamiać, że to bezpieczeństwo jest ważne, że mogą narobić sobie kłopotu. To jest właśnie też dylemat, nad którym właśnie stoją firmy, jak te osoby w ogóle zachęcić do przestrzegania tych procedur”. (wypowiedź analityka branży; wywiad ekspercki).

Kwestia **zatrzymania w firmie specjalistów od telekomunikacji i cyberbezpieczeństwa, którzy przechodzą do firm zagranicznych,** jest niemal tak samo istotna jak trzecie kluczowe wyzwanie (45% wskazań), a różnica pomiędzy sektorami jest znikoma (1 p.p.). Wyniki te znajdują odzwierciedlenie w opiniach ekspertów branżowych, którzy zauważyli, że ważnym wyzwaniem dla branży będzie odpływ specjalistów do zagranicznych firm (w tym, aby świadczyć pracę w sposób zdalny)[60]. Do zwiększenia się skali tego zjawiska przyczyniła się przede wszystkim sytuacja pandemii, która zwiększyła popularność zdalnego modelu wykonywania pracy. Specjaliści posługujący się biegle językiem obcym obowiązującym w firmie, mogą więc bez przeszkód pracować w zagranicznym przedsiębiorstwie. Eksperci w trakcie rozmów panelowych wskazywali na czynniki zachęcające pracowników do zmiany pracy, tj. przede wszystkim: większe wynagrodzenie oferowane w przedsiębiorstwach zagranicznych, wyższa kultura organizacyjna (np. metodyki pracy zwinnej, płaska struktura zarządu firmy), a także możliwość pracy w ciekawych projektach w międzynarodowym środowisku.

Wśród pozostałych wyzwań jest wiele takich, które są wyraźnie różnicowane przez sektor. Są to np. znalezienie nowych pracowników (specjalistów) z zakresu IT, którzy zajmują się projektowaniem systemów, programów, aplikacji itp. (wynik ogólny: 42%, różnica: 10 p.p. na korzyść cyberbezpieczeństwa), weryfikacja nowych pracowników w zakresie ich kompetencji i historii o ochronie danych osobowych (wynik ogólny: 40%, różnica: 9 p.p.) czy zwiększenie poziomu dbałości o doświadczenia użytkownika podczas korzystania z technologii i usług oferowanych przez firmę (wynik ogólny: 42%, różnica: 6 p.p.).

[60] „Tak, bo już to obserwujemy, tak, że przede wszystkim wynagrodzenia bardzo wysoko poszybowały w górę, gdzieś na przełomie roku i ewidentnie jest to spowodowane takim odpływem wysokiej klasy specjalistów na projekty zagraniczne, bez konieczności przemieszczania się, tak i próbą minimalizacji tego problemu poprzez ściąganie innych specjalistów, tak, a co automatycznie podnosi, podnosi stawki". (wypowiedź przedsiębiorcy z branży; wywiad ekspercki).

Tabela 24. Wyzwania dla branży – ogółem oraz w podziale na sektory

Wyzwania	Telekomunikacja, n = 685	Cyberbezpieczeństwo, n = 115	Ogółem, n = 800
Dbanie o rozwój pracowników w celu utrzymania przez nich zatrudnienia	51%	53%	51%
Spełnienie norm i wymogów dla pojawiających się nowych technologii	50%	49%	50%
Informowanie klientów o zagrożeniach przy korzystaniu z technologii i usług telekomunikacyjnych/internetowych oferowanych przez firmę	45%	49%	46%
Zatrzymanie w firmie specjalistów w zakresie telekomunikacji i cyberbezpieczeństwa, którzy przechodzą do firm zagranicznych	45%	46%	45%
Pozyskanie pracowników, którzy nie uczą się konkretnych rozwiązań, ale potrafią samodzielnie rozwijać swoje umiejętności	44%	41%	44%
Potrzeba opracowania zabezpieczeń i zidentyfikowania podatności dla nowych rozwiązań/technologii, tak aby możliwe było bezpieczne korzystanie z tych technologii w ramach firmy	43%	44%	43%
Zwiększenie poziomu dbałości o doświadczenia użytkownika podczas korzystania z technologii i usług oferowanych przez firmę	41%	47%	42%
Znalezienie nowych pracowników (specjalistów) z zakresu IT, którzy zajmują się projektowaniem systemów, programów, aplikacji itp.	40%	50%	42%
Weryfikacja nowych pracowników w zakresie ich kompetencji i historii o ochronie danych osobowych	39%	48%	40%
Wytworzenie kultury pracy łączącej pracę zdalną i pracę w biurze – integracja pracowników, dopracowanie narzędzi	39%	43%	40%
Znalezienie nowych pracowników posiadających specjalistyczną wiedzę z zakresu cyberbezpieczeństwa ze względu na małą liczbę takich specjalistów na rynku pracy	39%	43%	39%
Nawiązanie współpracy z kontrahentami zagranicznymi i wzrost konkurencyjności na arenie międzynarodowej	35%	35%	35%

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców i pracowników realizowanego w ramach projektu BBKL II w branży telekomunikacja i cyberbezpieczeństwo, edycja I.

9. Scenariusze rozwoju branży

Sytuację polskiej branży telekomunikacji i cyberbezpieczeństwa należy rozpatrywać w kontekście globalnych zmian technologicznych oraz z uwzględnieniem lokalnego kontekstu społecznego i gospodarczego. Kontekst ogólnoświatowy wyznacza trendy rozwoju technologii, ale to specyfika polskiej branży w dużej mierze będzie określać kierunek rozwoju sektora i zdecyduje o jego progresie lub recesji czy stopniowej marginalizacji.

Przedstawione wcześniej wyzwania będą mieć niewątpliwie wpływ na funkcjonowanie branży. Stanowią one zbiór czynników, które zależnie od zakresu wystąpienia będą w znacznej mierze moderować zmiany w branży i w zależności od jej reakcji tworzyć warunki sprzyjające wzrostowi lub recesji. Dwa możliwe scenariusze – pozytywny (wariant wzrostu) oraz negatywny (wariant recesji) – opracowano na podstawie analizy procesów obserwowanych w branży i jej otoczeniu. Kluczowymi czynnikami moderującymi sytuację branży są: oczekiwania klientów (strona popytowa) i możliwości udzielenia pozytywnej odpowiedzi na oczekiwania rynku (strona podażowa).

9.1. Scenariusz pozytywny

Scenariusz pozytywny zakłada zaistnienie czynników sprzyjających rozwojowi branży. Czynnikami determinującymi rozwój branży telekomunikacji i cyberbezpieczeństwa jest wzrost zapotrzebowania na jej usługi, a także potencjał kadrowy[61] i technologiczny umożliwiający zaspokojenia popytu. W korzystnym dla branży scenariuszu będzie rosła świadomość instytucjonalnych i prywatnych klientów dotycząca konieczności dbania o cyberbezpieczeństwo, jak też zakres wykorzystania rozwiązań telekomunikacyjnych. Chodzi tutaj zarówno o samą świadomość, że mechanizmy takie istnieją, ale również o idące za nimi rozwiązania prawne. Jest to tym istotniejsze, że obecnie obowiązujące akty wykonawcze do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa są nieliczne. W korzystnym dla branży scenariuszu, wzrost popytu będzie mógł być zaspokojony

[61] Chodzi tutaj wyłącznie o polski potencjał kadrowy, z pominięciem pracowników zagranicznych zatrudnianych w polskich firmach.

dzięki rozwojowi zasobów kadrowych i kompetencyjnych polskiej branży telekomunikacji i cyberbezpieczeństwa. Branża może pozyskiwać zasoby kadrowe na kilka różnych sposobów. Po pierwsze, poprzez dokształcanie pracowników już zatrudnionych w firmie. Po drugie, poprzez przekwalifikowywanie pracowników pracujących już w firmie. Po trzecie wreszcie, poprzez zatrudnianie pracowników nie do końca spełniających wymagania na danym stanowisku i ich dalsze dokształcanie, już po zatrudnieniu. Na podstawie przeprowadzonych badań można stwierdzić, że istotnym ryzykiem dla branży telekomunikacji i cyberbezpieczeństwa będzie zatrzymanie w firmie specjalistów i hamowanie procesu ich migracji do podmiotów zagranicznych. Scenariusz pozytywny zakłada wdrożenie przez firmy rozwiązań, które będę wspierać rozwój pracowników, a jednocześnie stanowić dla nich bodziec motywujący do długoterminowego związania się z danym pracodawcom.

9.2. Scenariusz negatywny

Scenariusz negatywny opiera się na potencjalnym braku możliwości zaspokojenia oczekiwań rynku przez polskie firmy działające w branży. Zapotrzebowanie zarówno na usługi telekomunikacyjne, jak też z obszaru cyberbezpieczeństwa będzie rosło, ale należy liczyć się z zagrożeniem ze strony dostawców usług OTT lub IPTV. Choć progres popytu może przybierać różną dynamikę, to należy przyjąć, że w dającej się przewidzieć perspektywie nie będzie on spadał. Za bardzo mało prawdopodobne należy uznać zahamowanie popytu na usługi technologiczne dostarczane przez analizowaną branże. Przeprowadzone badania pokazują, że pandemia COVID-19 i towarzyszący jej czasowy lockdown nie wpłynął negatywnie na analizowaną branżę.

Warto jednak mieć świadomość, że paradoksalnie korzystne warunki rozwoju i wzrost popytu mogą stanowić zagrożenie dla polskiej branży telekomunikacji i cyberbezpieczeństwa. Brak możliwości pozyskania odpowiedniej liczby specjalistów o wymaganych kompetencjach[62] będzie prowadził do marginalizacji polskich firm działających w analizowanym obszarze.

W scenariuszu negatywnym, niekorzystnym rozwiązaniem z punktu widzenia całej branży w Polsce jest pozyskiwanie pracowników zagranicznych, co z jednej strony może wiązać się

[62] Może to dotyczyć chociażby osób posiadających wiedzę z zakresu kryptologii, sposobu funkcjonowania technologii blockchain czy rozwiązań stosowanych w IoT.

z zaniżaniem wynagrodzeń na danym stanowisku, a z drugiej może powodować stopniowe zmniejszanie się (względem rynkowego standardu) zasobu wiedzy i doświadczenia. Zjawisko to może potęgować proces marginalizacji, prowadząc do całkowitej utraty przewag konkurencyjnych.

Dodatkowo, kwestie kadrowe pogorszyć może migracja pracowników do firm zagranicznych, która obecnie jest znacznie łatwiejsza i nie musi wiązać się ze zmianą miejsca zamieszkania. Czynnik ten potęgować będzie tempo utraty zasobów kadrowych i kompletnych firm, które nie będą w stanie zapewnić atrakcyjnych i prorozwojowych warunków zatrudnienia rodzimym pracownikom.

10. Rekomendacje[63]

Rekomendacje dla pracodawców

- Rekomenduje się **inwestowanie w działania mające na celu budowanie pozytywnego wizerunku** tzw. „pracodawcy z wyboru" (*employer branding*). Prowadzenie tych działań przekładać będzie się na zwiększenie efektywności w kwestii pozyskania nowych pracowników do firmy oraz pozwoli zatrzymać w firmie aktualnych pracowników. Przykładowymi działaniami w tym zakresie mogą być np.: budowanie wizerunku firmy „na zewnątrz" (dzięki śledzeniu i reagowaniu na komentarze dotyczące firmy), budowanie tegoż wizerunku w oczach pracowników (poprzez tworzenie miłej atmosfery w firmie czy wygodnego miejsca do pracy) czy oferowanie wraz z zatrudnieniem atrakcyjnych benefitów pozafinansowych.
- Rekomenduje się **zaangażowanie** w ograniczonym zakresie czasowym aktywności zawodowej **pracowników kończących karierę** w sektorze telekomunikacji (głównie inżynierów) **w proces przygotowania młodszych kadr** poprzez wchodzenie w role mentorów, coach-ów. Takie działanie pozwala w krótkim czasie wprowadzić nowych pracowników w struktury firmy oraz metodykę pracy wykorzystywaną w firmie (*onboarding*), a także pozwala na doszkolenie nowych pracowników w zakresie brakujących kompetencji.
- Rekomenduje się **wsparcie pracowników w procesie rozwoju kompetencji** (np. poprzez finansowanie bądź współfinansowanie studiów podyplomowych lub kursów specjalistycznych) w zakresie wymaganym przez zmieniające się potrzeby rynku. Kluczowe wydają się wiedza na temat nowych technologii (np. 5G, IoT, AI, AR/VR) i znajomość narzędzi niezbędnych do realizacji zadań zawodowych z nimi związanymi.
- Rekomenduje się **współpracę ze szkołami/uczelniami i „zamawianie" kierunków** na uczelniach poprzez kierowanie własnych pracowników do pracy w charakterze wykładowców oraz współpracę przy układaniu programu nauczania. W działaniu tym niemal pewne jest pozyskanie do pracy osób w pełni przygotowanych do objęcia

[63] Zaproponowane rekomendacje dotyczą czynności, które powinny być realizowane stale, bez określonej perspektywy czasowej zakończenia działań. Rozpoczęcie wdrażania rekomendowanych działania warto rozpocząć tak szybko, jak to jest możliwe.

konkretnych funkcji, natomiast konieczne jest odpowiednie, strategiczne planowanie ze względu na długość procesu kształcenia (min. 2–3 lata).

- Rekomenduje się również **rozwój współpracy między przedsiębiorstwami a szkołami/uczelniami** w zakresie uczestnictwa w prowadzonych przez firmy projektach. Uczniowie/studenci mieliby możliwość sprawdzenia się i wykorzystania nabytych umiejętności w rzeczywistych warunkach, natomiast pracodawcy mogliby zyskać nowych pracowników do swoich firm, bądź oddelegować do szkół/uczelni część zadań rozpisanych w ramach prowadzonych projektów.

Rekomendacje dla administracji publicznej, organizacji branżowych, instytucji edukacyjnych i innych organizacji

- Rekomenduje się **dalszą promocję kształcenia przygotowującego do podjęcia pracy w branży** telekomunikacji i cyberbezpieczeństwa. Działania promocyjne powinny być skierowane szczególnie do uczniów szkół zawodowych i szkół średnich. Działania promocyjne, w zależności od dostępnego budżetu, mogą przybierać wąską lub szeroką formę obejmującą zarówno tradycyjne działania (np. akcja plakatowa), jak też kanały nowoczesnego marketingu (np. kampanie w mediach społecznościowych, zaangażowanie technologicznych influencerów). W przekazach promocyjnych warto promować aspekty takie jak: potencjalne wysokie stawki wynagrodzenia w branży, stabilność zatrudnienia, uczestnictwo w ciekawych technologicznie projektach, praca przy tworzeniu rozwiązań i urządzeń odpowiadających na potrzeby społeczeństwa.
- Rekomenduje się **tworzenie kolejnych programów/projektów mających na celu zwiększenie ogólnej liczby osób kształcących się na kierunkach związanych z branżą** telekomunikacji i cyberbezpieczeństwa, co przyczyni się do zwiększenia ogólnej liczby specjalistów z tej branży dostępnych na rynku pracy. Rekomendacja uargumentowana jest prognozowanym w kolejnych latach wzrostem zapotrzebowania na specjalistów mogących podjąć pracę w analizowanej branży.
- Rekomenduje się **zidentyfikowanie kierunków studiów, które w prosty sposób mogą zostać uzupełnione o przedmioty z zakresu cyberbezpieczeństwa** (przykładowym kierunkiem może być np. elektronika). Może się to odbywać poprzez stworzenie specjalizacji finansowanej z funduszy zewnętrznych, np. środków własnych firmy, funduszy unijnych czy funduszy celowych oferowanych przez instytucje państwowe.

Rekomendacje dla pracowników

Rekomenduje się podjęcie przez pracowników działań rozwojowych mających na celu przede wszystkim zwiększenie własnej atrakcyjności na rynku pracy oraz zwiększenie elastyczności, jeżeli chodzi o wybór pracodawców czy rotację między stanowiskami. Zaleca się inwestowanie w rozwój kompetencji, które są relatywnie ważniejsze dla pracodawców i jednocześnie postrzegane przez nich jako trudno dostępne, a także których znaczenie – w ocenie pracodawców – będzie rosło w przyszłości. Do grupy tych kompetencji należą:

- w sektorze telekomunikacji:
  - umiejętność poprawy jakości i czytelności kodu,
  - umiejętność identyfikacji błędów w działaniu systemu, programu i usługi,

- w sektorze cyberbezpieczeństwa:
  - wiedza z zakresu systemów plików i zasad ich działania,
  - wiedza z zakresu systemów operacyjnych,
  - wiedza z zakresu bezpieczeństwa cyfrowego,
  - umiejętność obsługi platform bezpieczeństwa,
  - umiejętność blokowania zagrożeń,
  - umiejętność obsługi systemów i sieci pod względem zabezpieczeń,
  - umiejętność odzyskiwania utraconych danych,
  - umiejętność rozpoznawania cyberataków bądź niepokojących incydentów,
  - umiejętność zarządzania systemami bezpieczeństwa,
  - umiejętność przewidywania, w jaki sposób może dojść do ataku na dany system, program, usługę,
  - znajomość języków obcych (szczególnie angielskiego),
  - odpowiedzialność.

Spis tabel i wykresów

Spis tabel:

Spis wykresów: