PARP
Grupa PFR

Branżowy Bilans
Kapitału Ludzkiego II

Raport z II edycji badań

Branża telekomunikacji i cyberbezpieczeństwa

Branżowy
Bilans Kapitału Ludzkiego

Branżowy Bilans Kapitału Ludzkiego II

Branża telekomunikacji i cyberbezpieczeństwa

Raport z II edycji badań

Branżowy Bilans Kapitału Ludzkiego II – branża telekomunikacji i cyberbezpieczeństwa.
Raport podsumowujący II edycję badań realizowanych w latach 2022 i 2023.

Autorzy raportu:
Adrian Kargul
Karolina Drozdowicz
Konrad Kuźma

Wykonawca badań:
Konsorcjum firm IBC Advisory S.A. i Centrum Badań Marketingowych INDICATOR Sp. z o.o.

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

ISBN: 978-83-7633-540-7

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

Warszawa 2023

Spis treści

Szanowni Państwo,

oddajemy w Państwa ręce raport z wynikami drugiej edycji Branżowego Bilansu Kapitału Ludzkiego II dla branży telekomunikacji i cyberbezpieczeństwa. Badania te, prowadzone we współpracy z Sektorową Radą ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo, mają na celu zwiększenie wiedzy na temat stanu i kierunków rozwoju kadr w branży i związanego z nim zapotrzebowania na kompetencje, a także określenie determinujących go wyzwań, mających swe źródło w zmianach społecznych, gospodarczych i technologicznych.

Raport obejmuje wyniki badań ilościowych prowadzonych wśród pracodawców branży telekomunikacji i cyberbezpieczeństwa oraz pracowników zatrudnionych na kluczowych stanowiskach w firmach z tej branży. Jednym z głównych celów badania było opracowanie bilansu kompetencji, czyli ocena kluczowych kompetencji na poszczególnych stanowiskach z perspektywy pracodawców i pracowników. Zestawienie tych ocen powinno pomóc w określeniu podaży pracowników o odpowiednich kompetencjach, zapotrzebowania na nich ze strony pracodawców oraz sformułować rekomendacje, których adresatem są instytucje kształcenia, podmioty rynku pracy oraz sami pracodawcy.

Wyniki badań jakościowych oraz badanie foresightowe przeprowadzone wśród ekspertów branżowych umożliwiły ponadto rozpoznanie trendów i wyzwań oraz pozwoliły na przygotowanie scenariuszy rozwoju sektora.

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

Jednocześnie serdecznie dziękujemy przedstawicielom Sektorowej Rady ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo za wsparcie podczas całego procesu badawczego, a także wszystkim przedstawicielom firm z branży oraz ekspertom, którzy zgodzili się wziąć udział w Branżowym Bilansie Kapitału Ludzkiego II.

Zespół badawczy

1. Główne wnioski z badania

Projekt badawczy Branżowy Bilans Kapitału Ludzkiego II w branży telekomunikacji i cyberbezpieczeństwa dostarcza wiedzy nt. obecnego i przyszłego zapotrzebowania na kompetencje i kwalifikacje w branży. Prezentowane w niniejszym raporcie wyniki opracowano na podstawie opinii pozyskanych od zróżnicowanego grona respondentów – pracodawców, pracowników, przedstawicieli instytucji edukacyjnych oraz ekspertów branżowych – w ramach realizacji II edycji tego projektu. Analizy zgromadzonych danych pozwalają na sformułowanie następujących wniosków:

Aktualna sytuacja w branży

- Spośród najważniejszych czynników, które wpływają na branżę, wyróżniamy: inflację, kryzys energetyczny, następstwa pandemii, takie jak zmiany w formule pracy (czynniki zewnętrzne), a także odpływ wysoce wykwalifikowanych specjalistów do zagranicznych firm (czynnik wewnętrzny). Aktualna pozostaje również potrzeba zapewnienia odpowiedniego stopnia zabezpieczeń przed cyberatakami oraz zwiększenia nakładów na zabezpieczenia cyfrowe w przedsiębiorstwach i jednostkach administracji państwowej.

Przyszłość branży

- Najważniejszymi wyzwaniami, z jakimi branża będzie mierzyć się w przyszłości, będą pogłębiający się deficyt kadrowy spowodowany odpływem specjalistów do zagranicznych firm oraz trudności w rekrutacji nowych pracowników (50% wskazań na znaczenie tego wyzwania dla sektora telekomunikacji i 62% dla cyberbezpieczeństwa). Równie ważnym wyzwaniem będzie pozyskanie pracowników o kompetencjach z zakresu IT do pracy w branży (kolejno: 46% i 55% wskazań).
- W perspektywie najbliższych 5 lat w branży nie pojawią się zupełnie nowe stanowiska. Zmianie ulegnie natomiast zakres zadań zawodowych i kompetencji wymaganych od osób zatrudnionych na kluczowych stanowiskach. Na znaczeniu zyskają kompetencje związane z wykorzystaniem AI oraz innych nowych technologii cyfrowych, a także kompetencje społeczne (miękkie).

- Przedsiębiorcy z branży w przyszłości mogą potencjalnie obierać jedną z trzech strategii działania: aktywny rozwój wewnętrzny przedsiębiorstwa, realizację działań za pośrednictwem zewnętrznych kontraktorów lub podejmowanie czynnej współpracy z jednostkami naukowymi.

Zatrudnienie

- Głównymi czynnikami kształtującymi strukturę zatrudnienia w branży są: rozwój nowych technologii cyfrowych oraz przeniesienie działalności przedsiębiorstw oraz szkół i uczelni do sieci.
- W ciągu 12 miesięcy poprzedzających badanie, 17% firm poszukiwało nowych pracowników. Blisko co czwarty pracodawca poszukujący nowych pracowników odnotował problemy ze znalezieniem odpowiednich osób, przy czym nieco częściej taka sytuacja miała miejsce w sektorze cyberbezpieczeństwa niż w sektorze telekomunikacji (33% vs. 22%). W sektorze telekomunikacji najczęściej poszukiwanymi specjalistami byli developerzy (programiści), inżynierowie oraz architekci systemów. W sektorze cyberbezpieczeństwa byli to architekci ds. bezpieczeństwa, audytorzy bezpieczeństwa oraz eksperci ds. bezpieczeństwa.
- Niezależnie od sektora, w zdecydowanej większości firm (86%) pracodawcy z branży telekomunikacji i cyberbezpieczeństwa deklarują, że w ciągu najbliższych 12 miesięcy po realizacji badania wielkość zatrudnienia pozostanie bez zmian. Stanowiska, na które przedsiębiorcy rozważają zatrudnienie nowych osób, to dla sektora telekomunikacji: programista (14%), inżynier (12%), architekt systemów i kierownik projektu (po 11%). Natomiast dla sektora cyberbezpieczeństwa: CISO (12%), audytor bezpieczeństwa (12%) i ekspert ds. bezpieczeństwa (10%).
- Zdecydowana większość (92%) firm z branży nie zatrudnia pracowników zagranicznych. Są oni obecni w zaledwie co dwudziestej firmie (5%). Niemal 9 na 10 pracodawców z firm zatrudniających pracowników zagranicznych zatrudnia obywateli Ukrainy.

Ocena, rozwój i motywowanie pracowników

- Ocena potrzeb kompetencyjnych pracowników w 28% spośród wszystkich przedsiębiorstw z branży odbywa się regularnie – przynajmniej raz w roku, a w 23% firm

odbywa się sporadycznie – rzadziej niż raz w roku. W niemal połowie firm (49%) w ogóle nie jest prowadzona.

- Zarówno w opinii pracodawców z branży, jak i badanych pracowników zatrudnionych na kluczowych stanowiskach, najczęściej wykorzystywaną metodą oceny zapotrzebowania na kompetencje wśród pracowników jest rozmowa z przełożonym (69% wskazań w przypadku pracodawców i 65% w przypadku pracowników).
- Pracodawcy na ogół pozytywnie oceniają poziom umiejętności zatrudnionych pracowników – 59% uważa, że umiejętności są na tyle dobre, że nie ma potrzeby dodatkowych szkoleń, przy czym znacznie częściej (71%) jest to opinia przedsiębiorców ze średnich i dużych firm.
- Zdaniem przedsiębiorców dostrzegających braki kompetencyjne u pracowników, zatrudnionym najczęściej brakuje umiejętności ogólnych takich jak samoorganizacja, pomysłowość, terminowość (56%), a także kompetencji społecznych takich jak praca w grupie, komunikacja z zespołem (44%).
- Blisko dwie trzecie firm (63%) – w przypadku braku konkretnych umiejętności u swoich pracowników – decyduje się na szkolenie tych osób. Przedsiębiorcy dający pracownikom możliwości rozwoju kompetencji, najczęściej korzystali z kursów e-learningowych (34%), kursów i szkoleń wewnętrznych (33%) oraz kursów i szkoleń realizowanych przez firmy zewnętrzne (32%). Formy rozwoju kompetencji w miejscu pracy, które firma proponowała, to najczęściej szkolenia (instruktaż) z obsługi sprzętu oraz oprogramowania dostępnego w miejscu pracy (56%), mentoring (40%) oraz bezpośrednia obserwacja pracy innego pracownika (39%).
- Ogólna ocena przygotowania nowo przyjmowanych osób do firm jest pozytywna. Zdaniem 41% pracodawców nowi pracownicy posiadają pełne przygotowanie do pracy, a 38% jest zdania, że potrzebne jest tylko niewielkie szkolenie przed rozpoczęciem pracy.

Zadowolenie z pracy i motywacja pracowników

- Niemal wszyscy (98%) badani pracownicy zatrudnieni na kluczowych dla branży stanowiskach są zadowoleni z wykonywanej pracy, głównie ze względu na możliwości rozwoju, jakie ona daje. W rezultacie aż 97% pracowników z branży deklaruje, że planuje kontynuować pracę w obecnej firmie.
- Pracownicy oceniający rozmaite aspekty dotyczące obecnej pracy oceniali pozytywnie większości z nich (16 z 22). Najwyższe oceny dotyczą pozytywnych odczuć co do pracy

– sensowności jej wykonywania (96%), realizowania zadań, które się lubi (95%), dawania przez pracę poczucia bezpieczeństwa (również finansowego) (95%) czy przebywania w miejscu, w którym panuje dobra atmosfera (94%).

- Mimo tak wysokiego odsetka badanych pracowników, którzy są ogólnie zadowoleni z pracy, odnotowano spory udział pracowników odczuwających wzrastający poziom przeciążenia zadaniami zawodowymi (53%), co może być skutkiem zwiększonego popytu na usługi z branży w połączeniu z deficytem pracowników posiadających specjalistyczne kompetencje niezbędne do pracy w określonym zawodzie.
- Najczęstszym stosowanym przez pracodawców sposobem motywacji pracowników są premie roczne (73%) oraz możliwość pracy stacjonarnej (63%) lub hybrydowej (51%) (możliwość dopasowania miejsca pracy do indywidualnych potrzeb pracownika). Relatywnie często stosowane są również rozwiązania kładące nacisk na zachowanie równowagi między pracą a życiem prywatnym (*well-being*) (58%) oraz próby zapewnienia pracownikom przyjaznych warunków pracy (57%).

Bilans kompetencji

- Patrząc na profile poszczególnych stanowisk z sektora telekomunikacji i sektora cyberbezpieczeństwa można stwierdzić, że procentowo największy udział kompetencji trudno dostępnych odnotowano na stanowisku: architekta systemów i QA w sektorze telekomunikacji oraz pen-testera i eksperta ds. bezpieczeństwa w sektorze cyberbezpieczeństwa.
- Na stanowiskach z sektora cyberbezpieczeństwa odnotowano kompetencje, które w opiniach pracodawców zatrudniających osoby na tych stanowiskach będą zyskiwały na znaczeniu w ciągu 3 lat od realizacji badania, jednak pracodawcy byli powściągliwi w kwestii wskazywania kompetencji, których znaczenie już teraz szybko rośnie albo wkrótce szybko wzrośnie[1].

[1] W kontekście stanowisk z sektora cyberbezpieczeństwa, ze względu na niskie liczebności próby, wyniki należy traktować jako poglądowe.

2. Metodologia badania

2.1. Cele badania

W badaniach zrealizowanych w II edycji projektu dążono do zwiększenia wiedzy o potrzebach kompetencyjnych w branży telekomunikacji i cyberbezpieczeństwa, również poprzez weryfikację i aktualizację danych pozyskanych w I edycji. Głównymi celami działań badawczych były:

1. weryfikacja i aktualizacja profili kompetencyjnych dla kluczowych stanowisk,
2. ocena kompetencji pracowników na kluczowych stanowiskach – analiza ważności kompetencji w opinii pracodawców (strona popytowa) i pracowników (strona podażowa),
3. identyfikacja nowych kompetencji (kompetencje przyszłości) i kompetencji, których znaczenie już teraz szybko rośnie lub wzrośnie w perspektywie najbliższych 3 lat (*hot skills*) w odniesieniu do kluczowych stanowisk,
4. identyfikacja nowych stanowisk w branży, które mogą pojawić się w perspektywie kolejnych 3 lat,
5. weryfikacja i aktualizacja wyzwań, z którymi mierzą się i będą mierzyć się w przyszłości przedsiębiorcy z branży.

2.2. Techniki badawcze

Na potrzeby projektu 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).

Badania jakościowe realizowano od lipca do listopada 2022 roku. W ramach tych badań przeprowadzono:

- pogłębione wywiady indywidualne – 20 wywiadów indywidualnych z przedsiębiorcami,
- 4 panele eksperckie – w tym 2 dla sektora telekomunikacji (panel prospektywny: 8 ekspertów, panel kompetencyjny: 6 ekspertów) i 2 dla sektora cyberbezpieczeństwa (panel prospektywny: 7 ekspertów, panel kompetencyjny: 7 ekspertów),
- badanie delfickie (dwie iteracje) z łącznym udziałem 43 ekspertów,
- panel podsumowujący z dziesięcioma członkami Sektorowej Rady ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo.

Badania ilościowe realizowano w lutym i marcu 2023 r.[2] Przeprowadzono wywiady kwestionariuszowe z pracodawcami działającymi w branży i pracownikami zatrudnionymi na stanowiskach kluczowych dla branży. Wywiady zrealizowano wyłącznie metodą CAPI (standaryzowane wywiady bezpośrednie z użyciem laptopa).

Do realizacji badania posłużyła baza firm pobrana z operatu losowania BISNODE w dniu 31 stycznia 2023 r. Badania miały charakter wyczerpujący – objęto nimi wszystkie podmioty wpisujące się w definicję branży. Stopa zwrotu z badania wyniosła ok. 72%. Oprócz branży brano również pod uwagę podział próby pod względem: wielkości firm oraz makroregionów.

Wywiady ilościowe zostały przeprowadzone z 803 przedstawicielami firm oraz 1011 pracownikami[3]. Zgodnie z założoną próbą, w rozkładzie prezentującym zrealizowane wywiady dominują reprezentanci firm z sektora telekomunikacji (Tabela 1).

[2] Badanie właściwe poprzedzono pilotażem przeprowadzonym w styczniu 2023 r.

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

Tabela 1. Liczba zrealizowanych wywiadów w podziale na podsektory (wg klasyfikacji PKD)

Grupa wg kodu	Opis grupy	Badanie pracodawców		Badanie pracowników	
		n	%	n	%
sekcja J: 61.1	Działalność w zakresie telekomunikacji przewodowej	423	53	536	53
sekcja J: 61.2	Działalność w zakresie telekomunikacji bezprzewodowej, z wyłączeniem telekomunikacji satelitarnej	142	18	175	17
sekcja J: 61.3	Działalność w zakresie telekomunikacji satelitarnej	36	4	44	4
sekcja J: 61.9	Działalność w zakresie pozostałej telekomunikacji	84	10	103	10
sekcja J: 62.03.Z	Działalność związana z zarządzaniem urządzeniami informatycznymi (cyberbezpieczeństwo)	118	15	153	15
	Ogółem	**803**	**100%**	**1011**	**100%**

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, II edycja.

Ze względu na relatywnie niewielką liczbę wywiadów z reprezentantami firm zatrudniających 250 i więcej pracowników oraz 50–249 pracowników, obie grupy analizowane są łącznie jako grupa 50 i więcej pracowników (Tabela 2). Niezależnie od sektora, w branży dominują firmy mikro – zatrudniające od 2 do 9 osób (w zrealizowanej próbie w sektorze telekomunikacji 449 na 685 firm, w sektorze cyberbezpieczeństwa 85 na 118 firm).

Tabela 2. Liczba zrealizowanych wywiadów w podziale na wielkość zatrudnienia

Wielkość zatrudnienia	Badanie pracodawców		Badanie pracowników	
	n	%	n	%
2–9 pracowników	534	67	544	54
10–49 pracowników	217	27	374	37
50 i więcej pracowników	52	6	93	9
Ogółem	**803**	**100%**	**1011**	**100%**

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, II edycja.

W badaniu pracodawców respondentami były osoby dysponujące najbardziej obszerną wiedzą na temat polityki personalnej firmy, w tym w szczególności działań rekrutacyjnych oraz oceny kompetencji pracowników. W badanym przedsiębiorstwie musiał być zatrudniony przynajmniej jeden pracownik na kluczowym stanowisku, natomiast podczas rozmowy pracodawca określał

wymagania kompetencyjne maksymalnie dla dwóch stanowisk, które występowały w jego firmie (łącznie oceniono 1606 stanowisk). Respondentami w przypadku badania pracowników były osoby zajmujące kluczowe dla branży stanowiska w firmie. Przekłada się to na różną liczbę ocen stanowisk dokonaną przez pracodawców i pracowników (Tabela 3).

Tabela 3. Liczba i udział ocenianych stanowisk kluczowych dla sektora w zrealizowanej próbie pracodawców i pracowników

Zatrudnienie osób na kluczowych stanowiskach (sektor*)	Pracodawca			Pracownik	
	Liczba firm zatrudniających pracowników na danym stanowisku	Odsetek firm zatrudniających pracowników na danym stanowisku	Liczba oceniających stanowisko	Liczba zrealizowanych wywiadów	Odsetek wywiadów z pracownikami na kluczowym stanowisku
Architekt systemów (T)	430	54%	254	153	15%
Inżynier (każdej specjalizacji) (T)	558	69%	343	162	16%
Developer (programista) (T)	493	61%	247	159	16%
Project manager (kierownik projektu) (T)	419	52%	200	136	13%
Quality assurance (tester) (T)	353	44%	164	134	13%
CISO (chief information security officer) (C)	72	9%	41	22	2%
Audytor bezpieczeństwa (C)	67	8%	35	19	2%
Architekt ds. bezpieczeństwa (C)	70	9%	39	19	2%
Penetration tester (C)	59	7%	33	19	2%
Koordynator SOC (security operation center) (C)	51	6%	22	18	2%
Ekspert ds. bezpieczeństwa systemów/ sieci/aplikacji (C)	82	10%	48	40	4%
Dyrektor handlowy (U)	455	57%	189	130	13%
Ogółem	**803**	**100%**	**1606**	**1011**	**100%**

* Oznaczenie stanowisk: T – sektor telekomunikacji, C – sektor cyberbezpieczeństwa, U – stanowisko uniwersalne.
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

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 zaokrągleń lub możliwości wskazania wielu odpowiedzi.

W niniejszym raporcie znajdują się odniesienia do raportu z I edycji badania Branżowy Bilans Kapitału Ludzkiego II w branży telekomunikacji i cyberbezpieczeństwa realizowanego w latach 2020–2021. Terminy: „poprzednia edycja badania” i „I edycja badania” odnoszą się bezpośrednio do wyników wspomnianego raportu i będą używane zamiennie.

3. Aktualna sytuacja w branży

W tym rozdziale opisano aktualną sytuację w branży oraz wskazano i omówiono czynniki, które na nią oddziałują.

Najważniejsze wnioski z rozdziału:

- Spośród czynników zewnętrznych, największy wpływ na funkcjonowanie branży mają obecnie inflacja, kryzys energetyczny oraz następstwa pandemii COVID-19 (w szczególności zmiany w formule pracy).
- Spośród czynników wewnętrznych, największy wpływ na funkcjonowanie branży ma odpływ wysoce wykwalifikowanych specjalistów do zagranicznych firm.
- Następstwa pandemii COVID-19 nadal są widoczne w branży, przede wszystkim z uwagi na potrzebę zapewnienia odpowiedniego stopnia zabezpieczeń, powszechność pracy zdalnej oraz intensyfikację działań podejmowanych za pomocą kanałów zdalnych.

3.1. Sytuacja w branży w świetle danych statystycznych

Dla lepszego zobrazowania wniosków zaprezentowanych w niniejszym raporcie, zdecydowano się przedstawić kilka najważniejszych statystyk prezentujących aktualną sytuację w branży. Warto zaznaczyć, że wiele podstawowych statystyk dotyczących sektora cyberbezpieczeństwa nie jest dostępnych, ponieważ przedsiębiorstwa te są klasyfikowane w ramach tych samych kategorii co firmy zajmujące się innymi obszarami, np. branża IT.

Wartość przychodów z działalności telekomunikacyjnej w 2021 roku wyniosła około 40,8 mld zł[4]. Liczba podmiotów z sektora telekomunikacji w 2022 roku wyniosła 9902, to jest o 0,4% mniej niż w 2021 roku (9945)[5]. Przedstawienie dokładnych wartości przychodów i liczby podmiotów dla sektora cyberbezpieczeństwa nie jest możliwe, ale szacuje się,

[4] GUS, 2022, Telekomunikacja 2021, Szczecin.

[5] GUS, 2023, Zmiany strukturalne grup podmiotów gospodarki narodowej w rejestrze REGON 2022 r., Warszawa.

że w sektorze funkcjonuje około 300 przedsiębiorstw, w których nadal brakuje kilku tysięcy specjalistów, co stanowi o potencjale rozwoju sektora[6]. Potencjał ten jest widoczny również z uwagi na zwiększający się zakres incydentów bezpieczeństwa cyfrowego. 69% firm w Polsce przyznaje, że odnotowało w 2021 roku przynajmniej jeden incydent cyberbezpieczeństwa – to o 5 punktów procentowych (dalej: p.p.) więcej niż w 2020 roku[7]. Do najczęściej występujących cyberzagrożeń zaliczano: wyłudzanie danych uwierzytelniających (*phishing*), wycieki danych za pośrednictwem złośliwego oprogramowania (*malware*), zaawansowane ukierunkowane ataki (*Advanced Persistent Threat*, APT). Liczni przedsiębiorcy przyznają tym samym, że w kolejnych latach planować będą zwiększenie inwestycji w zabezpieczenia, mające na celu wyeliminowanie wymienionych zagrożeń[8].

3.2. Czynniki wpływające na branżę

Poniżej zaprezentowano kluczowe – zewnętrzne i wewnętrzne – czynniki, które w momencie prowadzenia badań wpływały na branżę. Zostały one uporządkowane, zaczynając od czynnika mającego największy wpływ na branżę, a kończąc na mającym najmniejszy wpływ. Prezentowane czynniki zostały zidentyfikowane, a następnie uporządkowane na podstawie materiału badawczego pochodzącego z badań ilościowych oraz przy uwzględnieniu opinii ekspertów biorących udział w badaniach jakościowych w ramach II edycji projektu.

Czynniki **zewnętrzne**:

- inflacja,
- kryzys energetyczny,
- pandemia COVID-19,
- wojna w Ukrainie,
- przerwane lub ograniczone łańcuchy dostaw.

6 KRK S.A. i HackerU, 2023, *Raport Cybersecurity. Rynek pracy w Polsce 2023.*

7 KPMG, 2022, *Barometr cyberbezpieczeństwa.*

8 Ibidem.

Czynniki **wewnętrzne**:

- odpływ wysoce wykwalifikowanych specjalistów do zagranicznych firm [T][C],
- rozwój łączności bezprzewodowej (sieci 5G) oraz infrastruktury światłowodowej [T],
- zapewnienie pracownikom możliwość rozwoju osobistego [C],
- rosnący popyt na usługi cyberbezpieczeństwa [C].

[T] – czynnik dotyczy sektora telekomunikacji

[C] – czynnik dotyczy sektora cyberbezpieczeństwa

Czynniki zewnętrzne

Główny czynnik zewnętrzny jakim jest **inflacja** w opinii 6 na 7 przedsiębiorców z branży telekomunikacji i cyberbezpieczeństwa wpłynął w średnim lub dużym stopniu na działalność ich firm w 2022 r.[9] (Tabela 5). Eksperci biorący udział w badaniach jakościowych zauważali, że inflacja widoczna jest przede wszystkim w kontekście kosztów prowadzenia działalności gospodarczej, w co należy wliczyć szybko rosnące wynagrodzenia dla specjalistów, podwyżki cen energii oraz koszty związane z zakupem odpowiedniego sprzętu. Wymienione wyżej aspekty wymuszają na przedsiębiorcach poszukiwanie obszarów, w których możliwa byłaby redukcja kosztów, co niejednokrotnie wiązać się będzie ze zmianami strategii firmy, np. przemodelowaniem strategii rozwoju firmy, zmniejszeniem nakładów na działy badań i rozwoju itp.

Drugim czynnikiem wpływającym na branżę jest **kryzys energetyczny**, który został określony przez więcej niż 3 na 4 przedsiębiorców z branży jako mający średni lub duży wpływ na działanie reprezentowanych firm w minionym roku. Na co najmniej średni wpływ tego czynnika wskazywali nieznacznie częściej przedsiębiorcy reprezentujący sektor telekomunikacji niż sektor cyberbepieczeństwa (77% vs. 73%) i nieco częściej obserwowano go w przypadku firm średnich i dużych (ponad 80% wskazań) niż firm mikro i małych (po ok. 75% wskazań). Kryzys energetyczny w dużej mierze wynika z inwazji Rosji na Ukrainę, a tym samym ze zmiany polityki energetycznej krajów Unii Europejskiej, w tym Polski. Efektem jest znaczne zwiększenie kosztów energii, co jest odczuwalne dla branży telekomunikacji i cyberbezpieczeństwa, w której znaczącą kategorią kosztów są również

[9] Postrzeganie to nie jest zależne ani od sektora, w którym działa przedsiębiorca, ani od wielkości reprezentowanej firmy.

koszty związane z energią potrzebną do zasilania infrastruktury telekomunikacyjnej, ale także np. komputerów, serwerów, maszyn i innych sprzętów elektronicznych.

Trzeci czynnik zewnętrzny – następstwa **pandemii COVID-19** – został wskazany przez 7 na 10 przedsiębiorców z branży jako mający średni lub duży wpływ na działanie ich przedsiębiorstw w 2022 r., przy czym udział reprezentantów sektora cyberbezpieczeństwa odczuwających taki wpływ był nieznacznie wyższy niż sektora telekomunikacji (72% vs. 69%). Przede wszystkim chodzi o takie aspekty, jak dynamiczny wzrost cyfryzacji społeczeństwa i przeniesienie działalności firm do sieci oraz ogólna popularyzacja pracy i nauki w formie zdalnej lub hybrydowej. Następstwem pandemii wpływającym aktualnie na branżę jest również konieczność dostosowania obecnych w firmach procesów biznesowych, aby możliwe było realizowanie zadań zawodowych bez fizycznej obecności pracowników w biurze. Pozytywnym aspektem wpływu tego czynnika na branżę jest potrzeba zapewnienia coraz sprawniejszych i szybszych rozwiązań z zakresu transmisji danych dla użytkowników, którzy wykonują swoją pracę bądź uczą się w formie zdalnej, co napędza popyt na wysokiej jakości usługi telekomunikacyjne. Negatywem aspektem z perspektywy przedsiębiorców z branży jest natomiast – wynikający z upowszechnienia pracy zdalnej – fakt podejmowania przez specjalistów pracy w zagranicznych przedsiębiorstwach ulokowanych fizycznie za granicą. Pracodawcy zagraniczni otworzyli się na rekrutację osób spoza ich regionu, ponieważ przekonali się, że brak fizycznej obecności w biurze nie musi być jednoznaczny z gorszym wykonywaniem obowiązków służbowych. To przyczyniło się natomiast do pogłębienia problemu związanego z deficytem pracowników w obu sektorach. Zmiany wprowadzone podczas pandemii COVID-19 w części firm zostały utrwalone. Największy procent przedsiębiorców z branży jako za trwałą zmianę wywołaną pandemią COVID-19 uznał zwiększenie wymogów bezpieczeństwa, które częściej dotyczyło firm z sektora telekomunikacji niż sektora cyberbezpieczeństwa (przewaga 5 p.p.). Na drugim miejscu znalazła się możliwość pracy zdalnej – sektor w tym przypadku nie różnicuje odpowiedzi. Inaczej jest natomiast w przypadku intensyfikacji działań podejmowanych za pomocą kanałów zdalnych. Istotnie częściej (różnica 11 p.p.) taką zmianę obserwuje się w firmach z sektora cyberbezpieczeństwa niż sektora telekomunikacji.

Tabela 4. Trwałe zmiany wywołane przez pandemię COVID-19 w firmach z sektora telekomunikacji (n = 570) i cyberbezpieczeństwa (n = 100)

Zmiany	Telekomunikacja	Cyberbezpieczeństwo	Ogółem
Zwiększenie wymogów bezpieczeństwa	58%	53%	57%
Praca zdalna	46%	47%	46%
Intensyfikacja obsługi/działań online	42%	53%	44%
Żadna zmiana	15%	13%	14%
Nie wiem/trudno powiedzieć	2%	2%	2%

Wyniki nie sumują się do 100%, ponieważ respondent mógł wskazać więcej niż jedną odpowiedź.
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

Czwartym czynnikiem zewnętrznym jest **wojna w Ukrainie**, wskazywana przez 4 na 7 przedsiębiorców z branży jako czynnik mający w 2022 r. średni lub duży wpływ na działanie reprezentowanych przedsiębiorstw. Częściej ten wpływ odczuwali przedsiębiorcy z sektora cyberbezpieczeństwa niż sektora telekomunikacji (63% vs. 56%). Rosnące napięcia na arenie globalnej skutkują coraz większą aktywnością hakerów, których celem są ataki na strony, usługi oraz bazy danych kluczowych przedsiębiorstw krajowych oraz organów administracji centralnej. Eksperci podczas badań jakościowych mówili o wielu nadużyciach i oszustwach finansowych, a także wskazywali na wzmożony poziom dezinformacji w postaci pojawiających się tzw. *fake newsów*. Wojna w Ukrainie zwiększyła także poziom świadomości na temat zagrożeń branż strategicznych cyberatakami. Poruszane problemy ilustrują poniższe cytaty:

> *Wojna ma różne oblicza. Wojna informacyjna i wojna cyfrowa stała się de facto rzeczywistością szybciej niż pisarze science fiction byli w stanie to napisać. Więc tak, pojawiło się zdecydowanie więcej pracy, pojawiły się tematy, które dotychczas były uznane za jakieś drugorzędne, bo były ważniejsze problemy, natomiast w związku z rozwojem sytuacji w Ukrainie i w Rosji pojawiły się pewne problemy, wyszły, że tak powiem, przed szereg. Także zwiększona ilość pracy – zdecydowanie tak.*
> [Cytat z wywiadu pogłębionego – przedstawiciel sektora telekomunikacji]

> *Myślę, że w ostatnim czasie, pewnie na większość branż, ale na telekomunikację szczególnie jednak miała i ma wpływ wojna w Ukrainie. W ciągu dosłownie kilku tygodni musieliśmy się mocno przygotować na różne zagrożenia. My jako spółka telekomunikacyjna dość mocno byliśmy narażeni i chyba ciągle jesteśmy na wszelkie ataki. Ale trzeba przyznać, że działania w zakresie ochrony cyfrowej przed wojną bardzo mocno zastopowały. W sensie takim, że właściwie w pewnych tematach nastąpiła, powiedzmy taka inercja działań.*
> [Cytat z wywiadu pogłębionego – przedstawiciel sektora cyberbezpieczeństwa]

Ostatnim czynnikiem zewnętrznym są **przerwane lub ograniczone łańcuchy dostaw** powiązane z ograniczeniem dostępności produktów – takich jak np. komputery, podzespoły, czujniki, przekaźniki, modemy – co często skutkuje podniesieniem cen deficytowych komponentów. Dla co drugiego przedsiębiorcy z branży był to czynnik mający średni lub duży wpływ na działanie jego przedsiębiorstwa w 2022 r. Problemy dotyczące dostaw były bardziej znaczące z punktu widzenia dużych firm (ponad 60% wskazań), natomiast w mniejszym stopniu – firm mikro (49% wskazań) i małych (43% wskazań). Wpływ przerwanych łańcuchów dostaw w nieco większym stopniu dotyczy firm z sektora cyberbezpieczeństwa niż telekomunikacji (przewaga 4 p.p.).

W jednej na trzy firmy z branży widoczny jest wpływ na działalność przedsiębiorstwa w ramach wszystkich pięciu czynników. Co piąty przedsiębiorca deklarował, że w jego przedsiębiorstwie odczuwalne są następstwa czterech z pięciu czynników.

Tabela 5. Czynniki wpływające na sytuację w branży – ogółem oraz w podziale na sektory

Czynniki	Telekomunikacja (n = 685)	Cyberbezpieczeństwo (n = 118)	Ogółem (n = 803)
Inflacja	86%	84%	85%
Kryzys energetyczny	77%	73%	77%
Pandemia COVID-19	69%	72%	70%
Wojna w Ukrainie	56%	63%	57%
Przerwane lub ograniczone łańcuchy dostaw	49%	53%	50%

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

Czynniki wewnętrzne

Głównym czynnikiem wewnętrznym mającym wpływ na funkcjonowanie obu sektorów jest obserwowany przez ekspertów branżowych **odpływ wysoce wykwalifikowanych specjalistów do zagranicznych spółek** (głównie ze względu na konkurencyjne stawki i lepsze warunki pracy przy jednoczesnej możliwości pracy zdalnej z Polski), który – w najbliższych latach – spowoduje trudności w rekrutacji nowych pracowników.

Dla sektora telekomunikacji istotny jest przede wszystkim **rozwój łączności bezprzewodowej (sieci 5G), jak również rozwój infrastruktury światłowodowej**. Stale powiększająca się w kraju dostępność sieci 5G oraz sieci światłowodowych z jednej strony umożliwia oferowanie przez firmy usług o coraz wyższej jakości, a z drugiej strony wymusza na przedsiębiorcach chcących nadążyć za zmianami w architekturze wykorzystywanej do obsługi tych technologii zatrudnianie pracowników, którzy posiadają kompetencje z pogranicza branży IT. Jest to utrudnione ze względu na deficyt takich pracowników na rynku pracy oraz z uwagi na wysokie wynagrodzenia, które należy zapewnić tego typu specjalistom.

Czynnikiem wpływającym na aktualną sytuację w sektorze cyberbezpieczeństwa jest konieczność **zapewnienia pracownikom możliwości rozwoju osobistego** (tj. możliwości awansu zawodowego, udziału w międzynarodowych projektach, uczestnictwa w atrakcyjnych kursach/szkoleniach podnoszących kompetencje), co ma związek z szybką dezaktualizacją wiedzy w tym sektorze. Ten czynnik jest ważny zarówno dla przedsiębiorców, którzy potrzebują pracowników posiadających kompetencje pozwalające realizować codzienne zadania zawodowe, jak i dla samych pracowników, którzy aktualizując swoją wiedzę zwiększają szanse na utrzymanie się na rynku pracy. Jeżeli firma nie oferuje możliwości rozwoju osobistego, pracownicy będą poszukiwali nowego miejsca pracy, które zapewni im tę możliwość. Ten typ działania dotyczy przede wszystkim pracowników młodszych i nieposiadających zobowiązań życia prywatnego (np. rodziny, kredytu, przywiązania do konkretnego miejsca zamieszkania), którzy są ukierunkowani na szybki rozwój. Pracownicy starsi ze względu na zobowiązania życia prywatnego będą w mniejszym stopniu skłonni do podejmowania ryzyka związanego ze zmianą pracy, a tym samym mogą zgodzić się na pozostanie w firmie w zamian za np. zwiększanie wynagrodzenia.

Kolejnym istotnym czynnikiem w tym sektorze jest **rosnący popyt na usługi cyberbezpieczeństwa**. Wynika on z coraz większej cyfryzacji przedsiębiorstw, przez co zwiększają się zasoby, które wymagają zapewnienia odpowiednich zabezpieczeń cyfrowych. Z drugiej strony obserwowana jest także wzmożona aktywność hakerów, którzy stale poszukują nowych sposobów na łamanie zabezpieczeń. Nieobojętnym – w kwestii popytu na usługi z obszaru cyberbezpieczeństwa – pozostaje także wspomniany wyżej fakt wojny w Ukrainie.

4. Przyszłość branży

W poniższym rozdziale zidentyfikowano najważniejsze wyzwania, z którymi będą mierzyć się przedsiębiorcy z branży. Opisano także zmiany w zakresie kompetencji, które nastąpią w perspektywie najbliższych 3 lat w ramach poszczególnych profili kompetencyjnych 12 kluczowych stanowisk w branży. Ostatnim elementem rozdziału jest przedstawienie scenariuszy przyszłości branży, w których opisane zostały strategie działania, które potencjalnie mogą być realizowane przez przedsiębiorców w przyszłości.

Najważniejsze wnioski z rozdziału:

- Najważniejszymi wyzwaniami, z jakimi branża będzie mierzyć się w przyszłości, będą pogłębiający się deficyt kadrowy spowodowany odpływem specjalistów do zagranicznych firm oraz trudności w rekrutacji nowych pracowników (50% wskazań dla sektora telekomunikacji i 62% dla cyberbezpieczeństwa). Na drugim miejscu znalazła się potrzeba pozyskania pracowników o kompetencjach z zakresu IT (kolejno: 46% i 55% wskazań).
- W perspektywie najbliższych 5 lat w branży nie pojawią się zupełnie nowe stanowiska. Zmianie ulegnie natomiast zakres zadań zawodowych na wielu aktualnie występujących stanowiskach (w tym kluczowych dla branży), a co za tym idzie – zakres kompetencji, które będą musieli posiadać pracownicy. Kompetencje, które pojawią się w branży, najczęściej będą związane z wykorzystaniem nowych technologii tj. AI, IoT, technologie chmurowe itp.
- Przedsiębiorcy z branży w przyszłości potencjalnie będą obierali jedną z trzech strategii działania: aktywny rozwój wewnętrzny przedsiębiorstwa, realizację działań za pośrednictwem zewnętrznych kontraktorów lub podejmowanie czynnej współpracy z jednostkami naukowymi.

4.1. Wyzwania stojące przed firmami oraz zmiany planowane w perspektywie 3 lat

Jednym z kluczowych zadań projektu była weryfikacja wyzwań, które będą wpływać na branżę w perspektywie kolejnych 3 lat. Wyzwania omawiane były w trakcie badań jakościowych (przede wszystkim podczas wywiadów pogłębionych z ekspertami branżowymi), a następnie poddane ocenie w trakcie badań ilościowych. W Tabeli 6 przedstawiono podsumowanie otrzymanych wyników.

Tabela 6. Wyzwania dla branży – ogółem oraz w podziale na sektory

Wyzwania	Telekomunikacja (n = 685)	Cyberbezpieczeństwo (n = 118)	Ogółem (n = 803)*
Potrzeba opracowania zabezpieczeń i zidentyfikowanie podatności dla nowych rozwiązań/technologii	n/d	53%	53%
Zatrzymanie w firmie specjalistów telekomunikacji i cyberbezpieczeństwa, którzy przechodzą do firm zagranicznych	50%	62%	52%
Znalezienie nowych pracowników (specjalistów) z zakresu IT	46%	55%	47%
Znalezienie nowych pracowników posiadających specjalistyczną wiedzę z zakresu cyberbezpieczeństwa	45%	52%	46%
Nawiązanie współpracy z kontrahentami zagranicznymi i wzrost konkurencyjności na arenie międzynarodowej	40%	36%	39%
Zwiększenie poziomu dbałości o doświadczenia użytkownika podczas korzystania z technologii i usług oferowanych przez firmę	37%	n/d	37%

* Sortowanie wg wyników dla ogółu.
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

Wśród wyzwań, które oddziałują i będą oddziaływać w przyszłości na przedsiębiorstwa z obu sektorów, najczęściej wskazywano na **zatrzymanie pracowników, którzy chcieliby przejść do firm zagranicznych** (50% wskazań dla sektora telekomunikacji i 62% dla sektora cyberbezpieczeństwa). Jak zostało wskazane w niniejszym raporcie, wyzwanie to wynika głównie z upowszechnienia pracy zdalnej, co jest następstwem pandemii COVID-19. Otwarcie

się firm z branży na pracę świadczoną zdalnie skłoniło i w dalszym ciągu będzie skłaniać specjalistów do podejmowania pracy w zagranicznych przedsiębiorstwach ulokowanych fizycznie za granicą. Decyzje polskich pracowników o przejściu do firm zagranicznych są i będą motywowane atrakcyjnymi warunkami zatrudnienia oferowanymi w zagranicznych firmach (tj. wyższe wynagrodzenie, przyjazna kultura organizacyjna, możliwość udziału w międzynarodowych projektach). Wyzwaniem dla branży będzie więc znalezienie sposobów na zatrzymanie pracowników w firmach krajowych. Wskazane problemy ilustruje poniższy cytat:

> *Tak, to jest wyzwanie, bo jednak ten pocovidowy rynek pracy otworzył się na pracę zdalną, więc faktycznie ciężko jest firmom z polskim kapitałem zaoferować warunki finansowe takie jak są oferowane w firmach nie wiem… w Berlinie, w Londynie. Więc odejścia pracowników z polskich firm to jest i będzie duże wyzwanie.*
> [Cytat z wywiadu pogłębionego – przedstawiciel sektora cyberbezpieczeństwa]

Drugim wyzwaniem, istotnym dla obu sektorów jest **znalezienie nowych pracowników (specjalistów) posiadających kompetencje z zakresu IT** (kolejno wg sektorów: 46% i 55% wskazań). Zapotrzebowanie na tego typu specjalistów w sektorze telekomunikacji jest związane ze zmianami w wykorzystywanej architekturze, co jest spowodowane wdrażaniem technologii takich jak 5G, a także dużo większym naciskiem na obsługę istniejącej infrastruktury telekomunikacyjnej z wykorzystaniem systemów komputerowych. W sektorze cyberbezpieczeństwa poszukiwanie specjalistów z zakresu IT dotyczy raczej poszukiwania osób, które są w stanie uzupełnić luki kadrowe. Aby sprostać temu wyzwaniu przedsiębiorcy będą musieli wprowadzić działania mające na celu zmniejszenie luki kadrowej (np. tworzenie klas patronackich, przyjmowanie pracowników mniej doświadczonych, a następnie ich doszkalanie). Argumenty, które przemawiają za pojawieniem się tego wyzwania w sektorze telekomunikacji, obrazuje następujący cytat:

> *A tę zmianę dramatyczną spowoduje wejście 5G. Nie dlatego, że będą większe transmisje i będzie można szybciej ściągać różne rzeczy. Tylko dlatego, że 5G z punktu widzenia właśnie kompetencji, które są potrzebne do rozwijania tej technologii, kompletnie wywraca do góry nogami to takie zasiedziałe trochę towarzystwo telekomunikacyjne. Bo 5G wymusza tak naprawdę to, że te tradycyjne sieci telekomunikacyjne, czy to komórkowe, czy zwykłe, o tak naprawdę bardzo starej architekturze, nagle muszą się kompletnie zmieniać i przechodzić do świata IT.*
> [Cytat z wywiadu pogłębionego – przedstawiciel sektora telekomunikacji]

Trzecim wyzwaniem wspólnym dla obu sektorów jest **znalezienie nowych pracowników posiadających specjalistyczną wiedzę z zakresu cyberbezpieczeństwa** (45% i 52% wskazań). To wyzwanie będzie obecne w sektorze cyberbezpieczeństwa ze względu na małą liczbę takich osób na rynku pracy. W sektorze telekomunikacji będzie mieć natomiast związek z potrzebą projektowania zabezpieczeń dla nowej infrastruktury oraz nowych systemów telekomunikacyjnych. Z uwagi na prognozowane trudności ze znalezieniem specjalistów, przedsiębiorcy będą zobligowani do zwiększenia wysiłków związanych z rekrutacją pracowników do pracy w obu sektorach. Pogłębiający się deficyt specjalistów zwiększy bowiem oczekiwania kandydatów względem warunków pracy, co wymusi na przedstawicielach firm wprowadzanie ciągłych zmian w kwestii oferowanych warunków zatrudnienia (np. wyższe wynagrodzenia, elastyczne godziny pracy, różne formy zatrudnienia, świadczenia pozapłacowe czy finansowanie rozwoju pracownika).

Czwartym wyzwaniem w obu sektorach jest **nawiązanie współpracy z kontrahentami zagranicznymi i wzrost konkurencyjności na arenie międzynarodowej** (40% i 36% wskazań). Chęć zagwarantowania stałego rozwoju technologii oraz oferowanych usług wymusi na przedsiębiorstwach z branży angażowanie się we współpracę międzynarodową z firmami, które przodują w rozwoju technologicznym – głównie z uwagi na wymianę doświadczeń, czyli tzw. *know-how*. Równie ważnym elementem potrzebnym dla rozwoju polskich firm będzie wzrost konkurencyjności na arenie międzynarodowej, który pozwoli trafić z oferowanymi usługami do większej grupy potencjalnych klientów. Wyzwaniem dla przedsiębiorców z branży będzie więc opracowanie strategii działania pozwalających inicjować współpracę międzynarodową oraz budować silną markę na arenie międzynarodowej. W związku z tym wyzwaniem, obserwowalny będzie także wzrost zapotrzebowania na kompetencje międzykulturowe wśród pracowników, w szczególności z zakresu komunikacji zespołowej i znajomości języków obcych.

Dodatkowo, zidentyfikowano dwa wyzwania, które są unikalne dla poszczególnych sektorów. W sektorze cyberbezpieczeństwa jest to **potrzeba opracowania zabezpieczeń i zidentyfikowania podatności dla nowych rozwiązań/technologii cyfrowych** (53% wskazań). Wraz z rozwojem technologicznym przedsiębiorstwa zaczną powszechnie korzystać z nowych technologii takich jak np. 5G, IoT, technologie chmurowe, sztuczna inteligencja, AR/VR. Wyzwaniem dla przedsiębiorców z sektora cyberbezpieczeństwa będzie więc potrzeba opracowania zabezpieczeń i zidentyfikowania podatności dla wspomnianych nowych technologii. Te działania będą niezbędne dla zapewnienia bezpiecznego użytkowania

wskazanych technologii przez użytkowników indywidualnych, przedsiębiorstwa, jak również podmioty państwowe.

W sektorze telekomunikacji wyróżniamy natomiast wyzwanie dotyczące zwiększenia poziomu dbałości o doświadczenia użytkowników podczas korzystania z oferowanych przez firmy technologii i usług (37% wskazań). W celu zapewnienia możliwie najlepszej jakości usług, przedsiębiorstwa z sektora telekomunikacji będą musiały zacząć w większym stopniu uwzględniać w oferowanych usługach aspekt dbałości o doświadczenia użytkowników. Mowa tutaj o poprawie intuicyjności, użyteczności i ergonomii oferowanych usług. Wyzwaniem dla przedsiębiorstw z sektora będzie więc modyfikacja procesów biznesowych, aby w większym stopniu uwzględniały doświadczenia użytkowników, co będzie wymagało ponownego przemyślenia procesów projektowych i strategii przedsiębiorstwa, zatrudnienia nowych specjalistów, a nawet utworzenia osobnych działów projektowych. W związku z tym wyzwaniem wzrośnie znaczenie pracowników zajmujących się procesem projektowym (Product/UX Researcher, Product/UX Designer, UX/UI Designer, UX Writer).

W perspektywie 3 lat firmy planują wiele zmian. Najczęściej wskazywaną zmianą jest – w przypadku obu sektorów – podwyższenie cen produktów/usług. W nieco większym stopniu dotyczy to telekomunikacji (+5 p.p.) (Tabela 7). Na drugim miejscu – nieco częściej w cyberbezpieczeństwie (+5 p.p.) znalazło się zwiększenie nakładów na innowacyjność. Na trzecim zaś – zwiększenie nakładów na nowe technologie (częściej w cyberbezpieczeństwie; +8 p.p.). W przypadku pozostałych zmian nie ma różnic pomiędzy sektorami. Najrzadziej planowaną zmianą jest zaangażowanie firmy we współpracę ze szkołami/uczelniami.

Tabela 7. Zmiany planowane w perspektywie 3 lat – ogółem oraz w podziale na sektory

Zmiana	Telekomunikacja (n = 685)	Cyberbezpieczeństwo (n = 118)	Ogółem (n = 803*)
Podwyższyć cenę usług	64%	59%	64%
Zwiększyć nakłady na innowacyjność w firmie	46%	51%	47%
Zainwestować lub zwiększyć nakłady inwestycyjne w nowe technologie (uczenie maszynowe, sztuczna inteligencja) i nowe oprogramowanie	41%	49%	42%
Stworzyć nowe usługi/produkty	39%	41%	39%
Zainwestować lub zwiększyć inwestowanie w rozwój umiejętności pracowników (szkolenia, kursy)	38%	40%	38%
Zautomatyzować wybrane procesy w firmie	36%	37%	36%
Rozpocząć lub zintensyfikować prace B+R w firmie samodzielnie lub we współpracy z jednostkami naukowymi	32%	31%	32%
Zaangażować firmę lub zwiększyć zaangażowanie firmy we współpracę ze szkołami bądź uczelniami w celu wykształcenia i zdobycia przyszłych pracowników	28%	34%	29%

* Sortowanie wg wyników dla ogółu.
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

Do przyczyn związanych z koniecznością wprowadzenia podwyżek cen produktów/usług zalicza się zmiany gospodarcze obserwowane w ostatnich okresach w kraju, mianowicie wzrastający poziom inflacji oraz kosztów prowadzenia działalności gospodarczej. Powodem takich decyzji jest również deficyt pracowników oraz wzmożone zapotrzebowania na usługi z zakresu telekomunikacji i cyberbezpieczeństwa. Opisywane zmiany obrazuje następujący cytat:

> *Płaca minimalna jest podnoszona, media się podnoszą, w sensie mówimy o prądzie, co za tym idzie czynszach i całej reszcie. Mówimy o kosztach zakupu infrastruktury, ale mamy nad sobą presje UKE, UOKIK i jeszcze paru innych instytucji, żeby nie podnosić cen Internetu. Ta sytuacja jest bardzo zła, kiedy bazowy przychód liczony jest w złotówkach, a nie w euro. Czyli mamy bardzo duże problemy regulacyjne i niezrozumienie tego rynku.*
>
> [Cytat z wywiadu pogłębionego – przedstawiciel sektora telekomunikacji]

4.2. Stanowiska i kompetencje przyszłości w perspektywie kolejnych 5 lat

Analiza jakościowych i ilościowych wyników badania pozwala przypuszczać, że w perspektywie najbliższych 5 lat w branży telekomunikacji i cyberbepieczeństwa nie pojawią się zupełnie nowe stanowiska[10]. Zmianie ulegnie natomiast zakres zadań zawodowych na wielu aktualnie występujących stanowiskach (w tym kluczowych dla branży), a co za tym idzie – zakres kompetencji, które będą musieli posiadać pracownicy. Wywiady z ekspertami pozwoliły na sformułowanie przewidywanych zmian, które dotyczyć będą osób zatrudnionych na kluczowych stanowiskach w branży[11].

W zestawieniu (Tabela 8) wskazano także **kompetencje przyszłości**, a więc kompetencje, które pojawią się w branży w najbliższych latach i będą ważne dla odpowiedniego wykonywania zadań zawodowych na poszczególnych stanowiskach.

Tabela 8. Zmiany w zadaniach zawodowych oraz kompetencje przyszłości w odniesieniu do 12 kluczowych stanowisk w branży

Nazwa stanowiska	Zmiany w zadaniach zawodowych oraz kompetencje przyszłości
Architekt systemów	Architekci systemów w przyszłości będą wykonywać projekty, które coraz częściej będą realizowane z wykorzystaniem architektury mikroserwisów lub systemów chmurowych. Coraz większe znaczenie będzie miała także wiedza z zakresu sztucznej inteligencji, przede wszystkim *machine learningu*. Coraz ważniejsza będzie także umiejętność projektowania spersonalizowanych produktów w oparciu o zidentyfikowane potrzeby klienta – architekci coraz częściej będą uczestniczyć w rozmowach z klientami. Kompetencje przyszłości, które pojawią się w profilu zawodowym dla tego stanowiska: – wiedza z zakresu sztucznej inteligencji (AI), szczególnie *machine learningu*, – tworzenie systemów w oparciu o nowe metody realizacji (mikroserwisy, technologie chmurowe).

[10] Takie przekonanie, wypowiadając się podczas wywiadów w badaniach ilościowych, podzieliło 99% przedsiębiorców z branży.

[11] Ekspertów pytano o to: Czy pojawią się nowe stanowiska? Jakie kompetencje w przypadku danego stanowiska będą zyskiwać na znaczeniu w najbliższej przyszłości (perspektywa najbliższych 3 lat) i dlaczego? Czy w najbliższej przyszłości (perspektywa najbliższych 3 lat) osoby zatrudnione na danym stanowisku będą musiały posiadać jakieś nowe kompetencje, aktualnie niewymienione w profilu kompetencyjnym i dlaczego one staną się ważne?

Nazwa stanowiska	Zmiany w zadaniach zawodowych oraz kompetencje przyszłości
Developer (programista)	Ze względu na dynamiczny rozwój usług wykorzystujących generatywną sztuczną inteligencję, w perspektywie kolejnych 3 lat zyskiwać będzie umiejętność projektowania rozwiązań w oparciu o potrzeby klienta oraz umiejętność rozwiązywania problemów w działaniu systemów. Kompetencje te będą ważniejsze niż umiejętność technicznego pisania kodu programistycznego. Ważne będzie również wykorzystywanie w codziennej pracy wiedzy na temat technologii sztucznej inteligencji – przede wszystkim *machine learningu*. Kompetencje przyszłości, które pojawią się w profilu zawodowym dla tego stanowiska: – wiedza z zakresu sztucznej inteligencji (AI), szczególnie *machine learningu*, – umiejętność wykorzystania narzędzi generatywnej AI do pisania kodu.
Quality assurance (tester)	Część zadań zawodowych osób zatrudnionych na stanowisku quality assurance (szczególnie tych dotyczących testowania manualnego) w kolejnych latach może zostać zautomatyzowana, przez co ważniejsze staną się kompetencje związane z tworzeniem standardów pisania kodu dla programistów, pisanie testów automatycznych, a nawet testowanie oprogramowania pod kątem ergonomii i użyteczności (kompetencje z pogranicza dziedziny User Experience). Kompetencja przyszłości, która pojawi się w profilu zawodowym dla tego stanowiska: – umiejętność pisania testów automatycznych dla oprogramowania napisanego w systemach chmurowych lub w architekturze mikroserwisów.
Inżynier (każdej specjalizacji)	Główną zmianą w zadaniach zawodowych inżynierów będzie potrzeba montowania i projektowania urządzeń wykorzystywanych do technologii IoT takich jak np. czujniki, kamery, przekaźniki. Kompetencje potrzebne do realizacji zadań zawodowych nie ulegną zmianie, zmienią się jednak produkty i technologie wytwarzane przez inżynierów. Kompetencja przyszłości, która pojawi się w profilu zawodowym dla tego stanowiska: – wiedza z zakresu projektowania urządzeń, czujników wykorzystywanych przy technologii Internetu Rzeczy (IoT).
Project manager	Ze względu na rosnący stopień skomplikowania realizowanych projektów, od project managerów coraz częściej będzie się wymagać posiadania specjalistycznej wiedzy technicznej. Do zadań zawodowych project managerów coraz częściej będzie należeć budowanie interdyscyplinarnych zespołów podzielonych ze względu na preferowany typ pracy (np. praca zdalna, praca stacjonarna). Kompetencja przyszłości, która pojawi się w profilu zawodowym dla tego stanowiska: – umiejętność budowania zespołów w odniesieniu do preferowanego modelu pracy (zespoły zdalne, stacjonarne, mieszane) oraz zespołów interdyscyplinarnych.

Nazwa stanowiska	Zmiany w zadaniach zawodowych oraz kompetencje przyszłości
Audytor bezpieczeństwa	Audytorzy w przyszłości będą musieli poświęcać więcej czasu na samą aktualizację swojej wiedzy, tak aby móc realizować audyty w oparciu o najnowsze standardy certyfikacji, które będą coraz bardziej złożone i będą uwzględniać wykorzystanie nowych technologii cyfrowych takich jak AI czy też IoT. Zadania zawodowe na tym stanowisku nie ulegną wiec zmianie, ważne będzie jednak realizowanie audytów w oparciu o nowe standardy, wymogi prawne oraz potrzeby, które pojawią się w związku z rozwojem technologicznym (np. nowe wymogi w kwestii dostępności fizycznej oraz cyfrowej). Kompetencja przyszłości, która pojawi się w profilu zawodowym dla tego stanowiska: – wiedza z zakresu najnowszych standardów certyfikacji (m.in. spełnianie odpowiednich standardów bezpieczeństwa przy wykorzystaniu nowych technologii cyfrowych takich jak AI, IoT).
Penetration tester	Zadania zawodowe realizowane przez osoby zatrudnione na tym stanowisku nie ulegną zmianie. Pen-testerzy będą musieli wciąż aktualizować swoją wiedzę o nowe techniki i nowe sposoby łamania zabezpieczeń zarówno cyfrowych, jak i niecyfrowych. Ważnym elementem będzie poszerzanie wiedzy o nowych technologiach cyfrowych takich jak AI oraz IoT, w szczególności na potrzeby testowania zabezpieczeń projektowanych dla tych technologii. Kompetencje przyszłości, które pojawią się w profilu zawodowym dla tego stanowiska: – wiedza z zakresu sztucznej inteligencji (AI), szczególnie *machine learningu*, – wiedza z zakresu Internetu Rzeczy (IoT).
CISO (chief information security officer)	W najbliższej przyszłości dla osób obejmujących stanowisko CISO istotne będzie poszerzanie wiedzy o nowych technologiach cyfrowych takich jak AI oraz IoT, aby możliwe było projektowanie strategii bezpieczeństwa dla firm wykorzystujących te technologie. Kompetencja przyszłości, która pojawi się w profilu zawodowym dla tego stanowiska: – zabezpieczenie danych fizycznych i cyfrowych przed cyberatakami wykorzystującymi nowe technologie (np. AI).
Architekt ds. bezpieczeństwa	W najbliższej przyszłości dla osób obejmujących stanowisko architekta ds. bezpieczeństwa istotne będzie poszerzanie wiedzy o nowych technologiach cyfrowych takich jak AI oraz IoT, aby możliwe było projektowanie zabezpieczeń dla firm wykorzystujących te technologie. Kompetencja przyszłości, która pojawi się w profilu zawodowym dla tego stanowiska: – zabezpieczenie danych analogowych i cyfrowych przez cyberatakami wykorzystującymi nowe technologie (np. AI)
Ekspert ds. bezpieczeństwa sieci/systemów	Kompetencje potrzebne dla wykonywania zadań zawodowych na tym stanowisku nie ulegną zmianie. Ważne będzie natomiast ciągłe poszerzanie swojej wiedzy o nowe standardy bezpieczeństwa oraz nowe sposoby zabezpieczania systemów i sieci.

Nazwa stanowiska	Zmiany w zadaniach zawodowych oraz kompetencje przyszłości
Koordynator SOC (security operations center)	W zakresie zadań zawodowych oraz w zakresie kompetencji wymaganych od osób obejmujących to stanowisko nie nastąpią znaczące zmiany.
Dyrektor handlowy/sprzedaży	W zakresie zadań zawodowych oraz w zakresie kompetencji wymaganych od osób obejmujących to stanowisko nie nastąpią znaczące zmiany.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badania jakościowe, II edycja.

Ważnym czynnikiem wpływającym na kształt kompetencji przyszłości dla wszystkich stanowisk w branży będzie również rozwój systemów generatywnej sztucznej inteligencji (AI). Wykorzystanie tych systemów w ostatnich miesiącach stało się w branży coraz bardziej powszechne, mimo że nie oferują one jeszcze odpowiedniego (a w wielu przypadkach nawet akceptowalnego) poziomu precyzji. Systemy te są wykorzystywane w branży np. do automatycznej zmiany części programu napisanego w konkretnym języku na inny język programowania lub do tworzenia części programu w oparciu o wprowadzone wytyczne. W przyszłości, systemy te staną się coraz bardziej precyzyjne, a ich wykorzystanie pozbawione licznych błędów, co w konsekwencji zmieni wagę poszczególnych kompetencji. Na znaczeniu zyskają kompetencje związane ze zrozumieniem klienta i projektowaniem rozwiązań, stracą natomiast kompetencje związane z samym pisaniem kodu programistycznego.

4.3. Scenariusze przyszłości

Ważnym elementem prac badawczych w ramach II edycji projektu było stworzenie scenariuszy rozwoju branży w przyszłości. Scenariusze przedstawiają strategie działania, które potencjalnie będą realizowane w przyszłości przez przedsiębiorstwa z branży, w zależności od intensyfikacji lub osłabienia poszczególnych czynników oddziałujących na branżę. Czynniki (zewnętrzne i wewnętrzne), które będą wpływać na branżę, włączone do poszczególnych wariantów scenariuszy to[12]:

[12] Czynniki – w ramach obu typów – uporządkowano, zaczynając do czynnika mającego największy wpływ na branżę, a kończąc na czynniku mającym najmniejszy wpływ. Czynniki opracowano na podstawie wyników badań ilościowych i jakościowych zrealizowanych w ramach II edycji badawczej.

w ramach **czynników zewnętrznych**:

- inflacja,
- rozwój systemów generatywnej sztucznej inteligencji (AI),
- długofalowe skutki pandemii COVID-19,
- intensyfikacja konfliktów międzynarodowych (w tym aktualna wojna w Ukrainie).

w ramach **czynników wewnętrznych**:

- deficyt specjalistów z branży telekomunikacji i cyberbezpieczeństwa na rynku pracy,
- poziom kompetencji posiadanych przez pracowników,
- współpraca na linii edukacja–biznes,
- poziom świadomości społeczeństwa na temat cyberbezpieczeństwa.

Scenariusze zostały opracowane przy wykorzystaniu zmodyfikowanej metody scenariuszy możliwych zdarzeń. W swoich pierwotnych założeniach metoda ta opiera się przede wszystkim na logice intuicyjnej, której istotą jest tworzenie opisu potencjalnych wydarzeń, z uwzględnieniem ich przyczyn oraz spodziewanej siły i kierunku zjawisk, które wystąpią z uwagi na te wydarzenia. Scenariusze przedstawione w niniejszym raporcie zostały opracowane z wykorzystaniem wniosków pochodzących z analizy materiału empirycznego zgromadzonego podczas badań jakościowych i ilościowych.

Elementy wspólne dla wszystkich scenariuszy

Wśród czynników, które oddziałują na branżę, wyróżnić należy te, które wpłyną w jednakowy sposób na wszystkie przedsiębiorstwa, niezależnie od obieranych przez nie strategii działań. Do takich czynników należą inflacja oraz intensyfikacja konfliktów międzynarodowych (w tym obecnie trwającej wojny w Ukrainie).

Następstwem szybko postępującej inflacji będzie wzrost oczekiwań pracowników dotyczących wysokości ich wynagrodzenia. Specjaliści będą dążyli do osiągnięcia odpowiednio wyższego wynagrodzenia, tak aby w jak najmniejszym stopniu odczuwać wzrost cen produktów i usług. Sytuacja ta będzie najtrudniejsza w przypadku firm, które realizują wieloletnie projekty, w których nie przewiduje się waloryzacji wartości umowy względem sytuacji na rynku. Firmy te będą musiały zwiększyć wynagrodzenia dla pracowników (mimo braku możliwości zwiększenia wpływów z realizacji prowadzonych projektów), aby nie dopuścić do ich odejścia ze stanowisk pracy.

Kolejnym czynnikiem wspólnym dla wszystkich firm w branży będzie intensyfikacja konfliktów na arenie międzynarodowej (a przede wszystkim aktualna sytuacja wojny w Ukrainie). Do następstw napiętej sytuacji międzynarodowej zaliczyć należy stały wzrost liczby incydentów bezpieczeństwa cyfrowego, co jest związane m.in. z coraz większą aktywnością cyberterrorystów i grup hakerów wspieranych przez obce państwa. W związku z wpływem tego czynnika, wszystkie przedsiębiorstwa w branży (a szczególnie te z sektora cyberbezpieczeństwa) odnotują coraz większe zapotrzebowanie na oferowane przez siebie usługi z zakresu zapewnienia bezpieczeństwa cyfrowego. Ta sytuacja pogłębi z kolei zapotrzebowanie na specjalistów posiadających kompetencje związane z cyberbezpieczeństwem, a pośrednio przyczyni się również do jeszcze większego wzrostu ich oczekiwań finansowych.

Scenariusz 1 – Aktywny rozwój wewnętrzny przedsiębiorstwa

Które firmy będą realizowały tę strategię?

- Przedsiębiorstwa oferujące autorskie usługi lub produkty, które chcą rozwijać.
- Przedsiębiorstwa każdej wielkości (zdecydowaną większość grupy stanowić będą jednak firmy średnie i duże), które charakteryzują się stabilnością finansową oraz posiadają odpowiednie środki na rozwój wewnętrznych zespołów.

Głównym czynnikiem wewnętrznym wpływającym w przyszłości na przedsiębiorstwa w branży będzie deficyt specjalistów na rynku pracy. Strategia pierwsza zakłada, że firmy będą próbowały poradzić sobie z niedoborem specjalistów poprzez tworzenie autorskich programów stażowych lub *bootcampów* (obozów treningowych). Realizacja takich programów pozwoli na samodzielne wykształcenie pracowników, którzy po ukończeniu stażu będą mogli objąć stanowiska młodszych specjalistów. Rekrutacja do programów stażowych będzie odbywała się za pośrednictwem specjalnie przygotowanego procesu, który – w odróżnieniu od rekrutacji realizowanej dla innych pracowników – będzie ukierunkowany na rozpoznanie kompetencji społecznych (miękkich) takich jak: chęć do ciągłego rozwoju, umiejętność przyswajania wiedzy, ukierunkowanie na realizację celów, kreatywność, wysoki poziom komunikacji interpersonalnej, umiejętność formułowania wypowiedzi, umiejętność pracy w zespole. Programy stażowe będą dedykowane głównie studentom ostatnich lat, podejmującym naukę na kierunkach związanych z branżą telekomunikacji

i cyberbezpieczeństwa. Na podstawie specyfiki podejmowanych działań można stwierdzić, że firmy realizujące programy stażowe będą poszerzać swoje zasoby kadrowe głównie w oparciu o polskich studentów. Powyższe wnioski obrazuje cytat:

> *Szkoła wykształci specjalistę bezpieczeństwa, cyberbezpieczeństwa ogólnego. To będzie osoba, która akurat tym się zajmuje, cyberbezpieczeństwem, więc to jest osoba, która ma ogólne pojęcie, wie, jakie są zagrożenia, wie teoretycznie jak im przeciwdziałać, niemniej jednak dla mnie brakuje tego trzonu takiego praktycznego: wziąć, zrób, dotknij, niech ci ktoś pokaże, także tutaj jestem raczej za połączeniem edukacji i biznesu […] dla mnie tutaj najlepszym rozwiązaniem byłoby takie połączenie z jednej strony edukacja, szkolnictwo, które wyrobi podstawy i domknięciem, taką klamrą spinającą byłby właśnie staż w firmie ze specjalistami, którzy się tym konkretnie problemem zajmują.*
> [Cytat z wywiadu pogłębionego – przedstawiciel sektora cyberbezpieczeństwa]

Drugim czynnikiem wpływającym na działania, które będą podejmowane przez firmy, jest ogólny poziom kompetencji posiadanych przez pracowników firmy. W przedsiębiorstwach nastawionych na autorskie rozwiązania bardzo ważne jest utrzymywanie niskiej rotacji pracowników ze szczególną dbałością o pracowników z wieloletnim stażem. Są to bowiem osoby, które zazwyczaj były w firmie już na początkowych etapach tworzenia produktu i posiadają o nim szeroką wiedzę, którą mogą przekazywać innym.

Biorąc pod uwagę powyższe informacje, firmy realizujące strategię pierwszą będą inwestowały w podniesienie poziomu kompetencji pracowników głównie poprzez organizowanie wewnątrz i na zewnątrz firmowych szkoleń i kursów, a także zapewniając im dostęp do najważniejszych wydarzeń branżowych. Dzięki tym działaniom, pracownicy firmy będą w stanie stale realizować swoje zadania zawodowe pomimo dynamicznych zmian w branży (tj. nowych standardów, nowych technologii, języków programowania, metod zarządzania projektem itd.). Firmy te będą mogły pozwolić sobie także na zatrudnianie osób mniej doświadczonych, ponieważ wraz z upływem czasu – dzięki uczestnictwu w szkoleniach oraz codziennemu wsparciu pracowników z dłuższym stażem (np. na zasadach *buddy*[13]) – będą oni stawali się coraz lepszymi specjalistami.

[13] Termin *buddy* (tłum. z ang. kolega/kumpel) odnosi się do osoby, która pełni rolę opiekuna i mentora dla nowo zatrudnionego pracownika. Zadaniami tej osoby jest wdrożenie nowego pracownika w obowiązujące w firmie standardy oraz pomoc w codziennych zadaniach. *Buddy* najczęściej pojawia się w procesach związanych z *onboardingiem* (wdrażaniem nowych pracowników w specyfikę i kulturę organizacyjną firmy).

Czynnik jakim jest rozwój systemów generatywnej sztucznej inteligencji (AI) wśród firm realizujących strategię pierwszą będzie widoczny poprzez przemodelowanie kompetencji, których będą nauczani pracownicy firmy. W trakcie szkoleń, kursów oraz podczas nauki od innych członków zespołu, większy nacisk kładziony będzie na rozwój kompetencji społecznych (tj. umiejętność pracy zespołowej, umiejętność pracy w zespołach interdyscyplinarnych i międzynarodowych, kreatywność, analityczny umysł) oraz rozwój kompetencji związanych z umiejętnościami: projektowania rozwiązań w oparciu o potrzeby klientów, tworzenia strategii, a także samego wykorzystania AI do realizacji codziennych zadań zawodowych. Będą to bowiem kompetencje, które zyskają na znaczeniu w porównaniu do umiejętności samego pisania kodu programistycznego bądź analizy incydentów bezpieczeństwa – te działania zostaną raczej zautomatyzowane.

Strategia pierwsza, w kontekście czynnika dotyczącego współpracy na linii edukacja–biznes zakłada, że firmy będą podejmowały i współtworzyły inicjatywy takie jak organizacja przestrzeni do podejmowania dyskusji, wymiany wniosków oraz przekazywania informacji o aktualnym zapotrzebowaniu na pracowników oraz na poszczególne kompetencje wśród pracodawców (np. konferencje, fora, debaty). Współpraca z sektorem edukacji będzie widoczna także poprzez zatrudnianie do szkół i uczelni wykładowców wizytujących, będących pracownikami prosperujących firm z branży, którzy będą prowadzić warsztaty lub kursy obejmujące praktyczne zagadnienia związane z pracą w zawodach związanych z telekomunikacją oraz cyberbezpieczeństwem. Powyższą koncepcję obrazuje cytat:

> *To są też współprace moim zdaniem z uczelniami, z uczelniami technicznymi. Uczelnie też mają swoje dość mocne zaplecze takie badawczo-rozwojowe, wymiany studenckie też i nieraz światowe. I tutaj jest duży potencjał. Uważam, że tu jest wręcz największy potencjał, bo ciężko jest wymagać od osoby, która... w tej branży nie da się spędzić 10–15 lat nie będąc ciągle na bieżąco ze wszystkimi specyfikacjami, aktualizacjami, wprowadzonymi nowościami. A wydaje mi się jednak, że mimo wszystko tym takim młodym osobom z taką umiejętnością analitycznego myślenia i też takiego koncepcyjnego myślenia przychodzi to po prostu łatwiej i szybciej, więc moim zdaniem warto jednak zainwestować w ten taki młody potencjał.*
> [Cytat z wywiadu pogłębionego – przedstawiciel sektora telekomunikacji]

Dla wielu firm realizujących strategię pierwszą ważne będą kwestie społecznej odpowiedzialności biznesu oraz edukacji społeczeństwa. Firmy te będą członkami zespołów, klastrów oraz innych zrzeszeń, w ramach których zaangażują się w realizację kampanii informacyjnych dla ogółu społeczeństwa (np. w związku z cyberprzestępczością lub bezpieczeństwem podczas korzystania z nowych technologii cyfrowych). Firmy te będą również realizowały darmowe, ogólnodostępne webinaria skierowane do ogółu społeczeństwa bądź do pracowników branżowych. Opisane powyżej działania, można zaliczyć do działań na rzecz poprawy sytuacji społecznej w wymiarze dotyczącym ogólnego poziomu świadomości społeczeństwa na temat cyberbezpieczeństwa. Firmy w ramach powyższej strategii obiorą więc kierunek aktywnych działań na rzecz poprawy świadomości społecznej na temat cyberbezpieczeństwa. Realizowane działania wpłyną także na podniesienie widoczności oraz budowanie reputacji firm na rynku.

Warto dodać, że firmy będą musiały podjąć działania w celu standaryzacji procesów w odniesieniu do aspektów, które pojawiły się wraz z nadejściem pandemii COVID-19. Mowa tu przede wszystkim o powszechnej obecności zjawiska świadczenia pracy w sposób zdalny. W ramach pierwszej strategii firmy zdecydują się na podział zespołów na stacjonarne lub hybrydowe oraz na w pełni zdalne. Rozdzielenie tych zespołów niesie za sobą podział także w obowiązujących zasadach pracy, procedurach, procesach oraz w systemach oceny i systemach płacowych – z tego względu podział zespołów pozwoli na efektywniejsze zarządzanie firmą. W firmach realizujących strategię pierwszą występować będzie większa dominacja zespołów stacjonarnych (z ewentualnymi elementami hybrydowymi np. możliwość pracy zdalnej 1–2 razy w tygodniu) ponieważ przedsiębiorcom, oprócz realizacji zadań, będzie zależeć na tworzeniu kultury organizacyjnej opartej na wsparciu, współpracy i reprezentowaniu wspólnych wartości. Powyższe wątki pojawiły się również w wypowiedziach respondentów:

> *Ja myślę, że w ogóle w perspektywie każdego stanowiska, ważnym elementem pracy jest odnajdywanie się po prostu w zmiennym środowisku. Pokazała to pandemia, pokazuje to wojna. I te osoby, które będą potrafiły się łatwiej przekwalifikować, zmienić swój system pracy ze stacjonarnego na zdalny bądź odwrotnie zmienić, będą mogły się szybko przystosować do zmiany project managera czy firmy.*
> [Wywiad indywidualny pogłębiony z przedsiębiorcą – sektor cyberbezpieczeństwa]

Scenariusz 2 – Realizacja działań za pośrednictwem zewnętrznych kontraktorów

Które firmy będą realizowały tę strategię?

- Przedsiębiorstwa realizujące usługi lub prowadzące projekty w konkretnej branży lub w kilku branżach dla wielu klientów.
- Przede wszystkim firmy mikro i małe, które nie mają (lub nie chcą poświęcać) środków na budowę stałych, wewnątrzfirmowych zespołów.

Strategia druga zakłada, że firmy, w związku z niedoborem specjalistów na rynku pracy, będą rezygnowały z zatrudniania pracowników na stałe (szczególnie na umowę o pracę), na rzecz pracowników kontraktowych. Taki rodzaj działania będzie motywowany dwoma głównymi argumentami. Po pierwsze, pracownicy kontraktowi będą zatrudniani jedynie na okres realizacji konkretnego projektu, co zniweluje niektóre koszty pracownicze, w szczególności te związane z utrzymaniem pracowników, dla których firma chwilowo nie ma żadnych zadań np. z uwagi na ich niedopasowanie kompetencyjne. Po drugie, zatrudnianie pracowników na zasadach B2B będzie w wielu sytuacjach niwelować koszty związane z podnoszeniem kompetencji pracowników – do każdego projektu poszukiwane będą jedynie takie osoby, które w momencie dołączenia do projektu będą posiadać odpowiedni, wymagany zestaw kompetencji, przez co nie wystąpi potrzeba finansowania szkoleń i kursów. Na podstawie specyfiki podejmowanych działań można stwierdzić, że firmy pozyskujące pracowników kontraktowych będą zatrudniać pracowników pochodzących z Polski, jak również pracowników zagranicznych (pochodzących np. z Indii, Ukrainy, Białorusi). Powyższe wnioski były poruszane również przez respondentów:

> *Przypływ pracowników z Ukrainy i z Białorusi, bo część osób na Białorusi… raczej studenci, są nastawieni opozycyjnie, w związku z tym raczej też starali się wyjeżdżać z kraju. I rzeczywiście w dużej mierze zaczęliśmy też współpracować dużo szerzej z takimi organizacjami, które zajmują się po prostu relokacją, osiedlaniem i pomocą pracownikom ze Wschodu, żeby mogli rozkręcać własne usługi w branży IT. Ja patrzę na branżę IT, pewnie w innych też… natomiast rzeczywiście liczba tych osób, które zaczęły dla nas pracować ze Wschodu także wzrosła.*
> [Wywiad pogłębiony z przedsiębiorcą – sektor telekomunikacji]

Odnosząc się do ogólnego poziomu kompetencji posiadanych przez pracowników, firmy, które będą realizować strategię drugą, nie będą szczególnie zainteresowane dbałością o rozwój kompetencji pracowników ze względu na specyfikę ich zatrudniania – krótko- lub średnioterminowe kontrakty. Przedsiębiorcy będą oczekiwać od pracowników podejmujących kontrakt posiadania wszystkich niezbędnych kompetencji, które pozwolą na należytą realizację danego projektu. Przedsiębiorcy nie będą więc uczestniczyć w rozwoju kompetencji kontraktorów lub będą ją ograniczać jedynie do zagwarantowania pracownikom wstępu na poszczególne konferencje branżowe. Specyfika podejmowanych działań będzie wymagała od przedsiębiorców realizujących tę strategię poświecenia większych środków na wynagrodzenia dla kontraktorów, ponieważ będą oni wliczali w koszt swoich usług całokształt zasobów poświęconych na to, aby sprostać danym wymaganiom rekrutacyjnym.

Wpływ czynnika związanego z rozwojem systemów generatywnej sztucznej inteligencji (AI) na przedsiębiorstwa realizujące strategię drugą będzie zauważalny głównie poprzez wzmożone zainteresowanie tych firm możliwością jak najszerszego wykorzystania tych systemów w codziennej pracy, a co za tym idzie – automatyzacji działań w realizowanych przedsięwzięciach.

Firmy realizujące strategię drugą, w ramach współpracy na linii edukacja–biznes będą angażować się w uczestnictwo w różnych inicjatywach (np. konferencje, fora, debaty) głównie w celu przekazania informacji na temat aktualnego zapotrzebowania na pracowników oraz kompetencje w branży. Firmy te nie będą na ogół zainteresowane szerszym aspektem, np. współtworzenia takich inicjatyw, ze względu na to, że głównym celem prowadzenia działalności firm realizujących strategię drugą będzie utrzymywanie rentowności biznesu oraz uzyskiwanie jak największych zysków.

Realizacja strategii drugiej w ramach wymiaru dotyczącego świadomości społeczeństwa na temat cyberbezpieczeństwa zakłada, że przedsiębiorstwa będą inwestowały w tworzenie własnych, prywatnych projektów mających na celu podniesienie ogólnej świadomości społecznej na temat cyberbezpieczeństwa lub zagrożeń związanych z nowymi technologiami cyfrowymi. Realizacja takich projektów może obejmować np. tworzenie spotów reklamowych, broszur lub krótkich filmików zamieszczanych w social mediach. Główną funkcją takich działań jest dbałość o dobry wizerunek firmy, jej widoczność oraz rozpoznawalność na rynku, a także stawianie firmy w roli lidera opinii.

Firmy podejmujące strategię drugą, w celu standaryzacji zachowań, które wystąpiły z uwagi na długofalowe konsekwencje pandemii COVID-19 (m.in. przyzwyczajenie do pracy zdalnej), będą musiały rozdzielać tworzone zespoły na stacjonarne, hybrydowe lub zdalne. Element ten będzie ważny głównie z uwagi na potrzebę rozwijania zasad, procedur oraz systemów ocen i płac, które będą odrębne dla poszczególnych zespołów i pozwolą na lepsze zarządzanie firmą. W przypadku strategii drugiej, firmy będą preferowały tworzenie zespołów w pełni zdalnych i asynchronicznych, ponieważ dzięki temu będą mogły rekrutować do nich osoby z różnych części Polski, a także pracowników zagranicznych. We wspomnianych firmach znacznie częściej będą powstawać zespoły międzynarodowe. Powyższe informacje obrazuje cytat:

> *Branża jest tak wygłodniała i tak chłonna, że epidemia COVID-19 de facto potwierdziła to, że praca zdalna jest możliwa do wykonania. I jedyne co się zmieniło na rynku to fakt, że firmy, które uparcie tkwiły przy postanowieniu, że z momentem końca pandemii pracownicy wrócą, straciły tych pracowników. Bardzo dużo ogarniętych i dobrze zarządzanych firm popełniło błąd nakazując pracownikom powrót do biur w momencie końca pandemii.*
> [Wywiad pogłębiony z przedsiębiorcą – sektor cyberbezpieczeństwa]

Scenariusz 3 – Czynna współpraca z jednostkami naukowymi

Które firmy będą realizowały tę strategię?

- Zarówno przedsiębiorstwa oferujące własne usługi i/lub produkty, jak i te realizujące usługi lub projekty dla różnych firm.
- Głównie przedsiębiorstwa średnie i duże posiadające odpowiednie środki finansowe przeznaczone na rozwój, które są w stanie „zamrozić" na rzecz nowych pracowników, pomimo oddalonego w czasie zwrotu z tej inwestycji.

Strategia trzecia zakłada, że przedsiębiorstwa w celu uniknięcia głównego problemu, jakim jest deficyt specjalistów z branży na rynku pracy, podejmą działania ukierunkowane na nawiązanie współpracy na linii edukacja–biznes ze szkołami i uniwersytetami kształcącymi na kierunkach związanych z branżą telekomunikacji i cyberbezpieczeństwa. Przedsiębiorstwa będą finansowały klasy patronackie, dzięki czemu nauka zawodu będzie odbywała się przy wykorzystaniu najnowszych technologii, nowoczesnych sprzętów, a także z udziałem

specjalistów pracujących na co dzień w branży. Z drugiej strony firmy będą tworzyć także programy stypendialne, które będą przeznaczane dla wybranych uczniów. Stypendia będą pomocne dla ich beneficjentów w trakcie nauki do konkretnego zawodu w ramach kształcenia ustawowego. W zamian przedsiębiorstwa będą oczekiwały podjęcia pracy (przez określony czas) w ich firmie po zakończeniu edukacji. Firmy będą mogły „wyłapywać" utalentowane osoby na etapie np. kształcenia w szkołach średnich. Oferowanie wsparcia finansowego na podjęcie dalszej nauki w zamian za deklarację pracy w firmie zapewni przedsiębiorcom stały dopływ odpowiednio wykształconych specjalistów.

Należy dodać, że powodzenie prezentowanych działań będzie wymagało od firm podejmowania zintegrowanej współpracy na linii edukacja–biznes. Potencjalną barierą w realizacji tego podejścia będzie natomiast potrzeba modyfikacji bądź stworzenia nowych regulacji prawnych. Przedsiębiorcy będą musieli współpracować z organizacjami branżowymi w celu ustanowienia odpowiednich regulacji, tak aby projekt stypendiów mógł być realizowany w zgodzie z obowiązującym prawem.

Dalsze losy osób uczęszczających do klas patronackich lub korzystających z programów stypendialnych będą różnić się w zależności od profilu przedsiębiorstwa. Firmy, które tworzą swoje produkty i usługi, będą dalej rozwijać kompetencje osób, które zaczną pracę w firmie np. po udziale w programie stypendialnym, licząc, że pracownicy w sposób naturalny uzupełnią luki po osobach, które zrezygnowały z pracy. Firmy, które realizują różne projekty dla różnych klientów, będą natomiast wprowadzać osoby np. z programów stypendialnych do projektów, w których potrzebne jest dodatkowe wsparcie, np. z uwagi na utratę kontraktorów czy eskalację zakresu realizowanego projektu, licząc, że osoby te rozwiną swoje umiejętności w praktyce zawodowej, oraz z uwagi na współpracę z wysoko wykwalifikowanymi kontraktorami, co sprawi, że firma zyska doświadczonych w realnie realizowanych projektach pracowników, niejako bez dodatkowej ingerencji. Odwołanie do tego wątku znajduje się także w następującym cytacie:

> *My musimy zadbać o edukację, poziom edukacji. Szkoły zawodowe są bardzo zaniedbane, nawet w takim aspekcie promocyjnym, ponieważ są wśród młodzieży odbierane negatywnie. Tam jest naprawdę bardzo niewielki procent dzieciaków, które idą tam z wyboru. I to też jest rzecz, za którą odpowiada psychologia, odkręcenie tego, że wybrana szkoła zawodowa nie jest taka super, uświadomienie, że można uzyskać umiejętności i faktycznie znaleźć się na rynku pracy w łatwiejszy sposób.*
> [Cytat z kompetencyjnego panelu eksperckiego – przedstawiciel sektora telekomunikacji]

Firmy, które podejmą strategię trzecią, z uwagi na fakt realizacji programów stypendialnych oraz klas patronackich, będą realizować również działania mające na celu zapewnienie sobie stałego dopływu pracowników o wysokim poziomie kompetencji. W zależności od profilu działalności, firmy te będą dbały dodatkowo o stały rozwój pracowników poprzez wewnątrz i zewnątrz firmowe szkolenia pracowników, a także udział w najważniejszych wydarzeniach branżowych (firmy tworzące swoje produkty i usługi) lub nie będą realizowały dodatkowych działań, licząc, że osoby po programach stypendialnych zdobędą doświadczenie w trakcie realizacji realnych projektów, przyczyniając się tym samym do stworzenia stabilnego rdzenia zasobów kadrowych w razie problemów z pracownikami kontraktowymi.

W tematyce wykorzystania systemów generatywnej sztucznej inteligencji widoczna będzie zmiana dotycząca rodzaju kompetencji rozwijanych wśród pracowników. Większy nacisk kładziony będzie na rozwój kompetencji społecznych (np. umiejętność pracy zespołowej, umiejętność pracy w zespołach interdyscyplinarnych i międzynarodowych, kreatywność) oraz umiejętności takich jak tworzenie strategii, projektowanie rozwiązań w oparciu o potrzeby klientów, a także samego wykorzystania AI do realizacji codziennych zadań zawodowych.

Realizacja strategii trzeciej, w wymiarze edukacji społeczeństwa na temat cyberbezpieczeństwa, będzie dotyczyć zaangażowanych działań w ramach zespołów, klastrów lub innych zrzeszeń, które będą polegać na realizacji kampanii informacyjnych dla ogółu społeczeństwa. Firmy te będą organizowały także webinaria lub innego rodzaju działania mające na celu edukację społeczną, ale także wzmacnianie wizerunku samej firmy. W przypadku firm realizujących różne projekty, działania mogą przybrać wymiar prywatnych projektów, których efekty będą bardziej widoczne np. w firmowych social mediach.

W przypadku firm realizujących strategie trzecią również widoczny będzie podział zespołów na stacjonarne (częściej występujące w firmach tworzących własne produkty i usługi) oraz na zdalne (w firmach realizujących różne projekty dla wielu klientów). Firmy w większości będą jednak ukierunkowane na tworzenie zespołów stacjonarnych bądź hybrydowych ze względu na chęć integracji pracowników rekrutowanych w ramach programów stażowych i klas patronackich oraz w celu tworzenia środowiska przyjaznego przekazywaniu wiedzy nowym pracownikom przez obecnych już specjalistów.

5. Zatrudnienie

Rozmowy z ekspertami oraz przedsiębiorcami z branży umożliwiły określenie, na które spośród 12 kluczowych dla branży stanowisk występuje obecnie największe zapotrzebowanie, a także jakie problemy występują w trakcie procesów rekrutacyjnych. Dodatkowo, w trakcie badania przyjrzano się sytuacji zatrudniania cudzoziemców w polskich przedsiębiorstwach z branży.

Najważniejsze wnioski z rozdziału:

- Głównymi czynnikami kształtującymi strukturę zatrudnienia są: rozwój nowych technologii cyfrowych oraz przeniesienie działalności przedsiębiorstw oraz szkół i uczelni do sieci. Wpływają one na wzrost zainteresowania usługami świadczonymi przez firmy działające w branży.
- W ciągu 12 miesięcy poprzedzających badanie, 17% firm poszukiwało nowych pracowników. Wynik ten jest porównywalny z pierwszą edycją badania. Blisko co czwarty pracodawca poszukujący nowych pracowników odnotował problemy ze znalezieniem odpowiednich osób, przy czym częściej taka sytuacja miała miejsce w sektorze cyberbezpieczeństwa niż w sektorze telekomunikacji (33% vs. 22%).
- W przypadku sektora telekomunikacji, najczęściej poszukiwanymi specjalistami byli developerzy (programiści) (22%), inżynierowie (22%) oraz architekci systemów (13%), a w sektorze cyberbezpieczeństwa najczęściej poszukiwani byli architekci ds. bezpieczeństwa, audytorzy bezpieczeństwa oraz eksperci ds. bezpieczeństwa (po 3% wskazań).
- Niezależnie od sektora, w zdecydowanej większości firm pracodawcy z branży telekomunikacji i cyberbezpieczeństwa deklarują, że w ciągu najbliższych 12 miesięcy po realizacji badania wielkość zatrudnienia pozostanie bez zmian (86% wskazań dla ogółu). Stanowiska, na które przedsiębiorcy rozważają zatrudnienie nowych osób, to dla sektora telekomunikacji: programista (14%), inżynier (12%), architekt systemów i kierownik projektów (po 11%). Natomiast dla sektora cyberbezpieczeństwa: CISO (12%), audytor bezpieczeństwa (12%) i ekspert ds. bezpieczeństwa (10%).
- Ponad 2/3 przedsiębiorców jest zdania, że w ciągu najbliższych 5 lat w ich firmie nie pojawi się żadne nowe, obecnie niewystępujące stanowisko, a niemal 1/3 nie wie lub nie jest w stanie określić czy w przyszłości pojawią się jakieś nowe stanowiska.

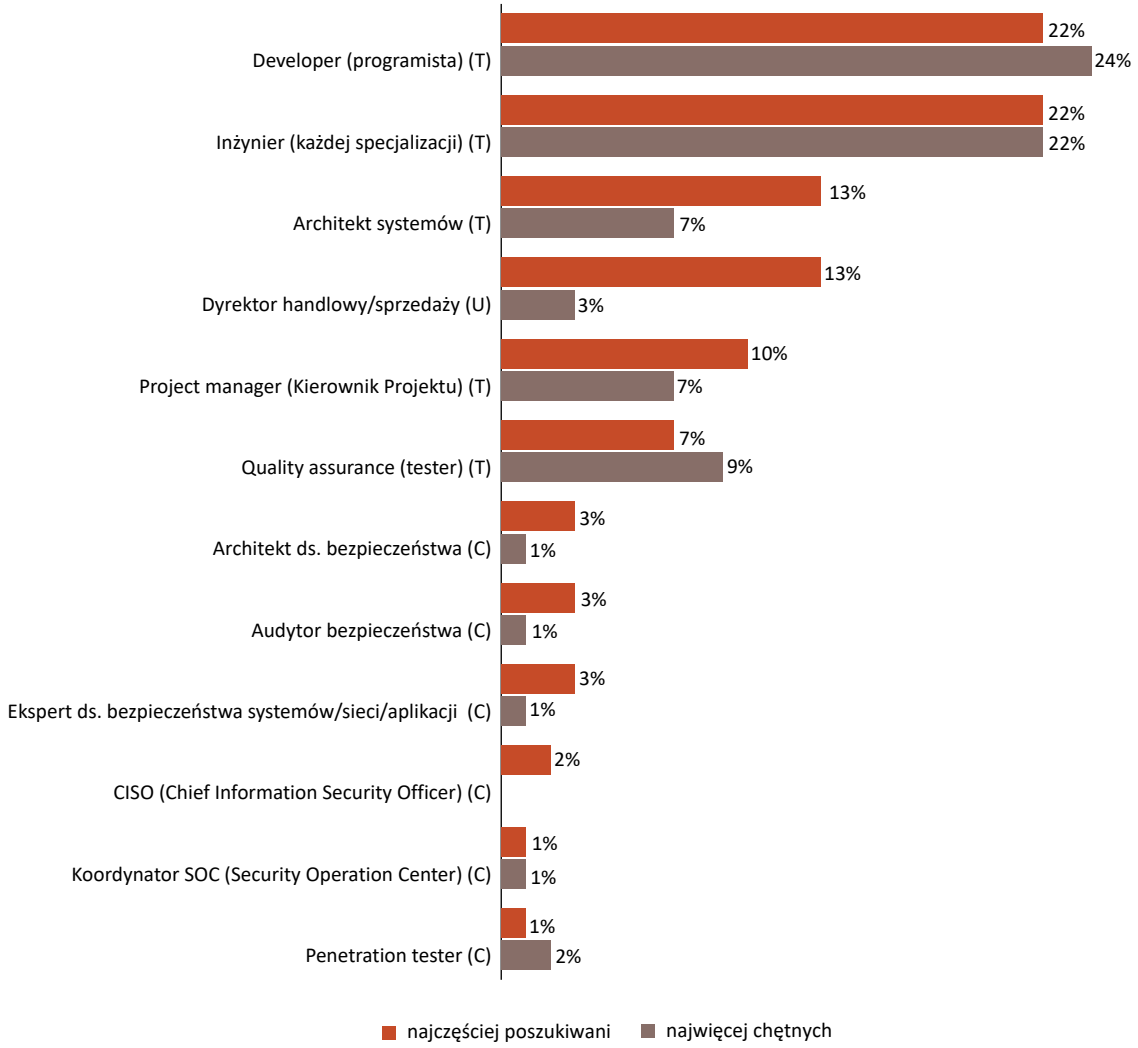
- Zdecydowana większość firm z branży (92%) nie zatrudnia pracowników zagranicznych. Są oni obecni w zaledwie w co dwudziestej firmie (5%). Firmy zatrudniające pracowników zagranicznych najczęściej zatrudniają pracowników z Ukrainy (88% wskazań) lub z innych państw europejskich (33% wskazań).

5.1. Poszukiwanie pracowników

Obecnie 17% firm poszukuje nowych pracowników. To wynik porównywalny z poprzednią edycją badania. Stanowiskami, na które pracodawcy najczęściej poszukują pracowników, są jednocześnie stanowiskami, w ramach których jest największe zatrudnienie, tj. programista (22%) i inżynier (22%). Na kolejnych miejscach, relatywnie rzadziej wskazywane, znalazły się takie stanowiska jak architekt systemów i dyrektor handlowy (po 13%) oraz kierownik projektu (10%).

Spośród stanowisk, na które zgłasza się najwięcej chętnych, na pierwszych dwóch miejscach znalazły się programista (24%) oraz inżynier (22%). Na trzech kolejnych miejscach znalazły się takie stanowiska jak: quality assurance (9%) oraz architekt systemów i kierownik projektu (po 7%).

Wykres 1. Stanowiska*, na które są najczęściej poszukiwani oraz najchętniej zgłaszający się pracownicy

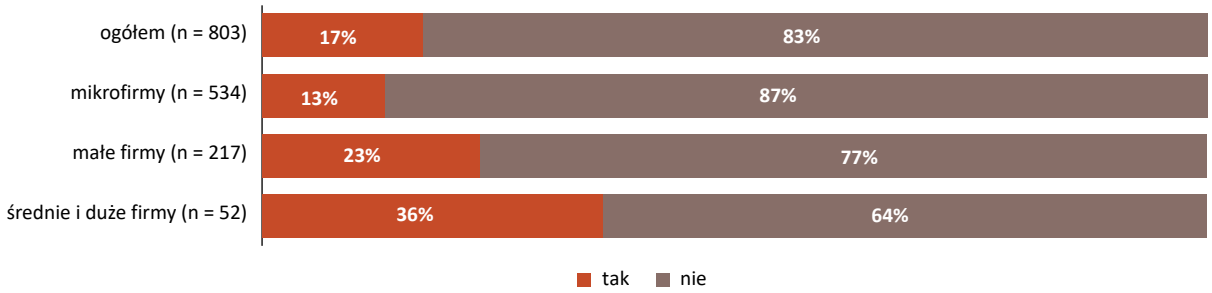


* Oznaczenie stanowisk: T – sektor telekomunikacji, C – sektor cyberbezpieczeństwa, U – stanowisko uniwersalne.
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

17% badanych przedsiębiorców z branży w ciągu 12 miesięcy poprzedzających badanie poszukiwało nowych pracowników. Fakt ten jest mocno skorelowany z wielkością firmy. W przypadku firm mikro (13%), a w przypadku małych, średnich i dużych jest to wyższy odsetek (tj. 23% w przypadku firm małych oraz 36% dla firm średnich i dużych).

W poprzedniej edycji odsetki te były zbliżone do siebie (np. dla ogółu różnica wynosi nieco ponad 1 p.p. mniej, a dla firm mikro jest to spadek o niecałe 4 p.p.).

Wykres 2. Poszukiwanie nowych pracowników w ciągu 12 miesięcy poprzedzających badanie (ogółem i w podziale na wielkość firmy)



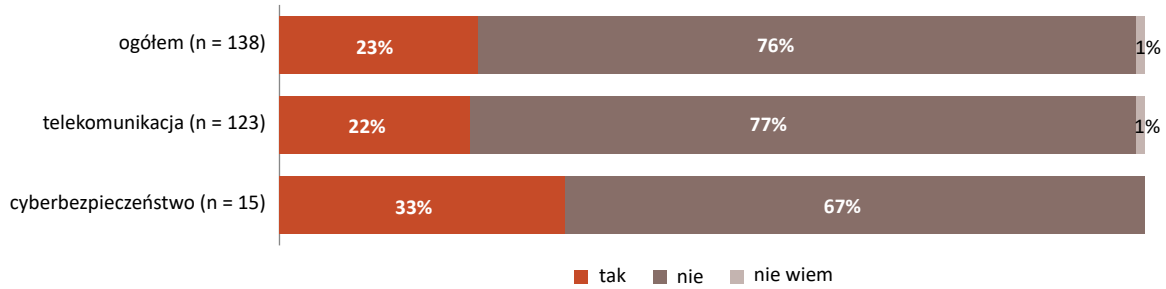
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

Blisko co czwarty pracodawca poszukujący nowych pracowników odnotował problemy ze znalezieniem odpowiednich osób, przy czym nieco częściej taka sytuacja miała miejsce w sektorze cyberbezpieczeństwa niż w sektorze telekomunikacji (33%[14] vs. 22%) (Wykres 3). Największymi problemami[15], z jakimi musieli zmierzyć się pracodawcy chcący zatrudnić nowych pracowników, były brak odpowiednich kwalifikacji (70%; 16 osób), brak odpowiedniego doświadczenia (57%; 13 osób) oraz – w nieco mniejszym stopniu – brak niezbędnego wykształcenia (26%; 6 osób).

[14] Ze względu na niską podstawę odsetek ten należy traktować poglądowo.

[15] Ze względu na niską podstawę (n = 23) wskazane problemy należy traktować w ujęciu komparatystycznym, które ukazuje stopień danego problemu wśród ogółu problemów.

Wykres 3. Problemy pracodawców ze znalezieniem odpowiednich pracowników (ogółem i w podziale na sektory)



Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

Pracodawcy z sektora cyberbezpieczeństwa, jeśli już mają problem ze znalezieniem pracowników, to zwykle na wszystkie stanowiska, na które zatrudniają. Nieco inaczej jest w przypadku sektora telekomunikacji, gdzie stanowiska, na które pracodawcy mają największy problem ze znalezieniem pracowników, są jednocześnie stanowiskami najpopularniejszymi w tym sektorze.

Tabela 9. Stanowiska, na które pracodawcy mają największe problemy z rekrutacją pracowników

	Architekt systemów	**Inżynier (każdej specjalizacji)**	**Developer (programista)**	**Project manager (Kierownik projektu)**	**Quality assurance (tester)**	**CISO (*chief information security officer*)**	**Audytor bezpieczeństwa**	**Architekt ds. bezpieczeństwa**	**Penetration tester**	**Koordynator SOC (security operation center)**	**Ekspert ds. bezpieczeństwa systemów/sieci**	**Dyrektor handlowy/sprzedaży**
Sektor*	T	T	T	T	T	C	C	C	C	C	C	U
N	28	28	28	28	28	5	5	5	5	5	5	33
Procent	29	29	43	7	11	100	100	100	100	100	80	20

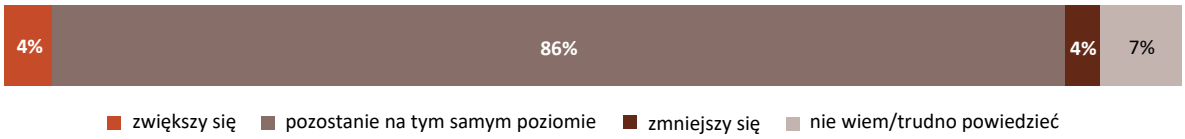
* Oznaczenie stanowisk: T – sektor telekomunikacji, C – sektor cyberbezpieczeństwa, U – stanowisko uniwersalne.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

5.2. Zapotrzebowanie na pracowników i prognozowane zmiany

Niezależnie od sektora, w zdecydowanej większości firm pracodawcy z branży telekomunikacji i cyberbezpieczeństwa deklarują, że w ciągu 12 miesięcy po realizacji badania wielkość zatrudnienia pozostanie bez zmian (86% wskazań dla ogółu). Taki sam odsetek pracodawców planuje zwiększenie zatrudnienia, co jego zmniejszenie (po 4%). W poprzedniej edycji liczba podmiotów, w których planowano utrzymanie zatrudnienia na tym samym poziomie, była nieznacznie wyższe (o nieco ponad 2 p.p.). Podobną zmianę zaobserwowano w przypadku zwiększenia zatrudnienia (również 2 p.p.).

Wykres 4. Prognozowana zmiana zatrudnienia w ciągu 12 miesięcy po badaniu (ogółem)



Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

Stanowiska, na które przedsiębiorcy z sektora telekomunikacyjnego rozważają zatrudnienie nowych osób, to najczęściej programista (14%), inżynier (12%) oraz – w równym stopniu – architekt systemów i kierownik projektów (po 11%). W sektorze cyberbezpieczeństwa są to natomiast CISO i audytor bezpieczeństwa (po 12%) oraz ekspert ds. bezpieczeństwa (10%). W poprzedniej edycji badania – w sektorze telekomunikacyjnym – wszystkie stanowiska (z wyjątkiem architekta systemów) rozważane były w równym stopniu, nieco niższym niż w obecnym pomiarze (8–9%). W sektorze cyberbezpieczeństwa były to natomiast stanowiska penetration tester (29%, o 21 p.p. więcej) oraz koordynator SOC (25%, o 14 p.p. więcej).

Tabela 10. Rozważane zatrudnienie nowych osób na kluczowych stanowiskach

Stanowisko	Architekt systemów	Inżynier (każdej specjalizacji)	Developer (programista)	Project manager (Kierownik projektu)	Quality assurance (tester)	CISO (chief information security officer)	Audytor bezpieczeństwa	Architekt ds. bezpieczeństwa	Penetration tester	Koordynator SOC (security operation center)	Ekspert ds. bezpieczeństwa systemów/sieci	Dyrektor handlowy/sprzedaży
Sektor*	T	T	T	T	T	C	C	C	C	C	C	U
N	685	685	685	685	685	118	118	118	118	118	118	803
Odsetek wskazań	11%	12%	14%	11%	7%	12%	12%	5%	8%	9%	10%	5%

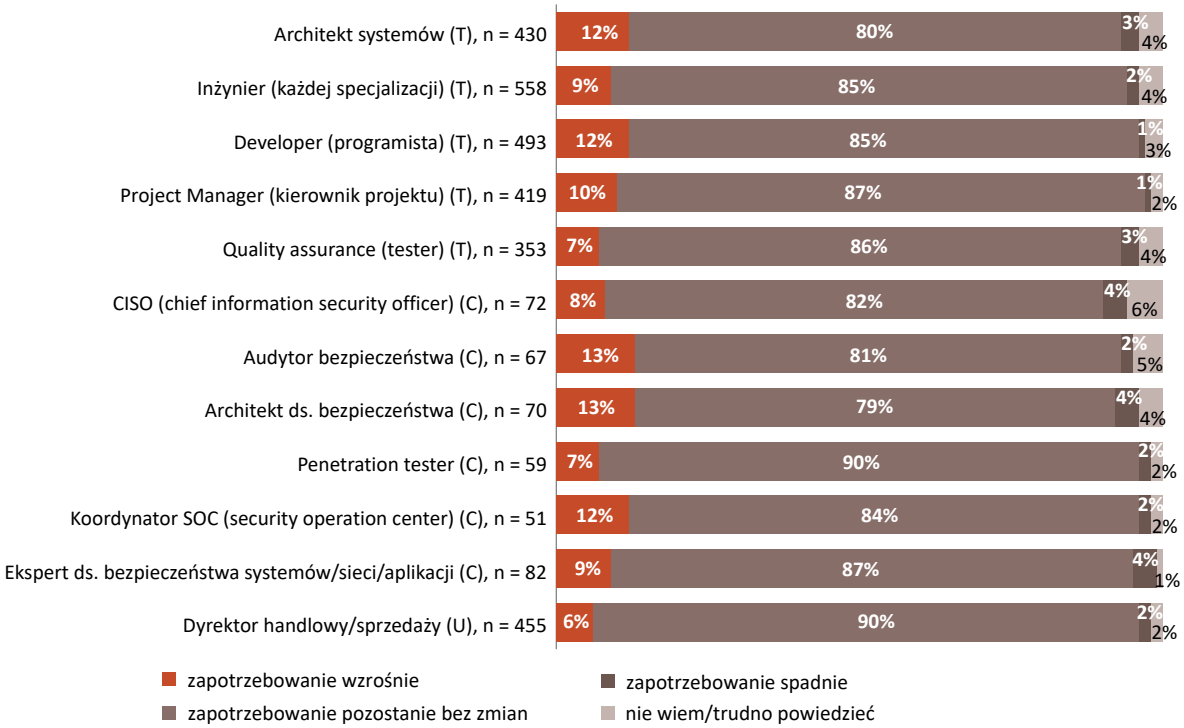
* Oznaczenie stanowisk: T – sektor telekomunikacji, C – sektor cyberbezpieczeństwa, U – stanowisko uniwersalne.
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

Przewidywany poziom zatrudnienia pracowników w ciągu najbliższego roku w większości przedsiębiorstw nie ulegnie zmianie, pozostając na obecnym poziomie. Jeśli planowana jest zmiana, to relatywnie częściej prognozowany jest wzrost, a nie spadek zatrudnienia. W II edycji największy przewidywany wzrost w sektorze telekomunikacji dotyczy stanowisk architekta systemów oraz programisty (po 12%)[16]. W poprzedniej edycji stanowiskiem wiodącym w tym względzie był inżynier (13%). W sektorze cyberbezpieczeństwa – w obecnej edycji – przewiduje się wzrost na następujących stanowiskach: audytor bezpieczeństwa i architekt ds. bezpieczeństwa (po 13%) oraz koordynator SOC (12%)[17]. W poprzedniej edycji najczęściej wskazywano stanowiska: penetration testera (16%, o 9 p.p. więcej niż obecnie), audytora bezpieczeństwa (15%, o 2 p.p. więcej niż obecnie) oraz eksperta ds. bezpieczeństwa (13%, o 4 p.p. więcej niż obecnie).

[16] W I edycji architekta systemów wskazało o ponad 8 p.p. mniej przedsiębiorców, a programistę blisko o 5 p.p. mniej.

[17] W I edycji architekta ds. bezpieczeństwa wskazało o 3 p.p. mniej przedsiębiorców, a koordynatora SOC o 8 p.p. mniej.

Wykres 5. Zmiana przewidywanego poziomu zatrudnienia pracowników w ciągu najbliższego roku*



* Oznaczenie stanowisk: T – sektor telekomunikacji, C – sektor cyberbezpieczeństwa, U – stanowisko uniwersalne.
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

Podobnie jak w ubiegłej edycji, ponad 2/3 przedsiębiorców jest zdania, że w ciągu najbliższych 5 lat w ich firmie nie pojawi się żadne nowe, obecnie niewystępujące stanowisko, a niemal 1/3 nie jest w stanie określić, czy takie stanowiska się pojawią. Jedynie 1% przedsiębiorców jest zdania, że w branży pojawią się jakieś nowe stanowiska. Przedsiębiorcy, którzy przewidują pojawienie się nowego stanowiska w branży, stawiają na programistę AI[18]. Wciąż duży odsetek osób niezdecydowanych uważa, że przedsiębiorcy nie są w stanie ocenić rozwoju i zapotrzebowania w swojej firmie w ciągu najbliższych 5 lat.

[18] Odwołując się do informacji przedstawionych w rozdziale 8, w przyszłości należy raczej spodziewać się zmiany zadań zawodowych i zakresu kompetencji, które będą musiały posiadać osoby obecnie zatrudnione na stanowiskach programistów. Nie przewiduje się bowiem, aby stanowiska programistów i programistów AI funkcjonowały jako osobne. W poprzedniej edycji jako nowe stanowisko w branży wskazywano na influencera.

Wykres 6. Przewidywanie pojawienia się nowych ról zawodowych

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

5.3. Pracownicy zagraniczni

Zważając na pogłębiający się deficyt kadrowy spowodowany m.in. wspominanym w raporcie odejściem pracowników do zagranicznych firm, szansą na uzupełnienie luk kadrowych może być otwartość na zatrudnienie w polskich przedsiębiorstwach nowych, wysoce wykwalifikowanych specjalistów z zagranicy.

Jednak w momencie prowadzenia badania, zdecydowana większość (92%) firm z branży nie zatrudnia pracowników zagranicznych. Są oni obecni w zaledwie co dwudziestej firmie (5%). Firmy zatrudniające pracowników zagranicznych najczęściej zatrudniają obywateli Ukrainy (88% wskazań) lub pracowników z innych państw europejskich (33% wskazań). Pracownicy pochodzący z pozostałych części świata pojawiają się w polskich przedsiębiorstwach zdecydowanie rzadziej (np. z państw azjatyckich – 15% czy z Białorusi – 10%) lub są w ogóle nieobecni (państwa afrykańskie). W grudniu 2022 r. pracodawcy deklarowali, że cudzoziemcy najczęściej są zatrudniani w firmach już od 1–2 lat (33%) lub powyżej 3 lat (30%), co pokazuje, że branża na ogół nie musiała mierzyć się z migracjami ze względu na aktualne napięcia na arenie międzynarodowej (w tym szczególnie ze względu na wojnę w Ukrainie). Firmy deklarowały, że w porównaniu do 2021 r. liczba zatrudnianych cudzoziemców nie uległa zmianie (62%) lub nieznacznie wzrosła (36%). W sektorze cyberbezpieczeństwa pracowników spoza Polski praktycznie nie ma, a pracownicy zagraniczni zatrudnieni w sektorze telekomunikacji najczęściej obejmują stanowiska inżynierów (41%) oraz programistów (30%).

6. Ocena i rozwój kompetencji pracowników

Rozdział przedstawia wnioski nt. częstotliwości i sposobów oceny kompetencji pracowników w branży, działań rozwojowych, a także porusza temat kształcenia formalnego.

Najważniejsze wnioski z rozdziału:

- Proces oceny potrzeb kompetencyjnych pracowników w 28% przedsiębiorstw odbywa się regularnie – przynajmniej raz w roku, w 21% firm odbywa się sporadycznie – rzadziej niż raz w roku. W blisko połowie firm (49%) nie jest prowadzona ocena potrzeb kompetencyjnych. Najczęściej stosowaną, ale rzadziej niż w I edycji, metodą oceny zapotrzebowania na kompetencje u pracowników jest rozmowa z przełożonym (69% wskazań; spadek o 10 p.p.). Ocena opisowa przygotowywana np. przez przełożonego jest stosowana już w nieco ponad jednej trzeciej (36%) firm – to o 14 p.p. więcej niż w poprzedniej edycji.
- Podobnie jak w opinii przedsiębiorców, również według pracowników najpopularniejszą (65% wskazań) metodą oceny zapotrzebowania na kompetencje jest rozmowa z przełożonym, a na drugim miejscu – ocena opisowa (37%).
- Pracodawcy pozytywnie oceniają poziom umiejętności zatrudnionych pracowników (59%, wzrost o 9 p.p. w stosunku do poprzedniej edycji), przy czym warto zaznaczyć, że ocena ta jest lepsza w średnich i dużych firmach (w 71% tych firm uważa się, że pracownicy nie potrzebują dodatkowego szkolenia, ponieważ ich wiedza i umiejętności są wystarczające).
- Zdaniem przedsiębiorców, którzy dostrzegają braki kompetencyjne u pracowników, najczęściej brakuje pracownikom umiejętności ogólnych (56% wskazań), a także kompetencji społecznych (44%).
- Blisko dwie trzecie (63%) firm – w przypadku braku konkretnych umiejętności u swoich pracowników – decyduje się na szkolenie tych osób. Obecnie jest to rozwiązanie obserwowane rzadziej (spadek o 18 p.p.) niż w I edycji.
- Przedsiębiorstwa prowadzące szkolenie pracowników w równym stopniu korzystały z kursów e-learningowych (34%, spadek w stosunku do poprzedniej edycji o 3 p.p.), kursów i szkoleń wewnętrznych (33%, spadek o 4 p.p.) oraz kursów i szkoleń realizowanych przez firmy zewnętrzne (32%, spadek o 4 p.p.).

- Najczęściej proponowanymi formami rozwoju kompetencji w miejscu pracy były: szkolenia/instruktaże z obsługi sprzętu oraz oprogramowania dostępnego w miejscu pracy (56%), mentoring (40%) oraz bezpośrednia obserwacja pracy innego pracownika (39%).
- Generalnie ocena przygotowania osób nowo przyjmowanych do firm jest pozytywna. Zdaniem 41% pracodawców nowi pracownicy posiadają pełne przygotowanie do pracy (o 18 p.p. więcej niż w poprzedniej edycji), a 38% (o 2 p.p. mniej niż w poprzedniej edycji) jest zdania, że potrzebne jest tylko niewielkie szkolenie przed rozpoczęciem pracy. Jednocześnie niemal 9 na 10 badanych pracowników (niezależnie od sektora) ma poczucie, że szkoła czy uczelnia, którą ukończyli, przygotowała ich do pracy na obecnym stanowisku.

6.1. Weryfikacja i ocena umiejętności

Ocena potrzeb kompetencyjnych pracowników jest niezwykle istotnym elementem zarządzania przedsiębiorstwem. W 28% przedsiębiorstw proces ten odbywa się regularnie, przynajmniej raz w roku, a w 21% firm – sporadycznie, rzadziej niż raz w roku. W blisko połowie firm (49%) nie dokonuje się oceny potrzeb kompetencyjnych. W stosunku do poprzedniej edycji widać relatywnie duży spadek liczby firm, w których dokonuje się oceny – o 8 p.p. mniej w przypadku oceny regularnej oraz o 8 p.p. w przypadku oceny sporadycznej. Tym samym odsetek firm nieprowadzących oceny potrzeb kompetencyjnych znacznie wzrósł w porównaniu do I edycji (o 16 p.p.).

Ocena potrzeb kompetencyjnych częściej jest prowadzona w sposób regularny w sektorze telekomunikacyjnym niż w sektorze cyberbezpieczeństwa (kolejno: 29% i 23%). Natomiast w przypadku prowadzenia oceny w sposób sporadyczny sytuacja jest odwrócona – w sektorze telekomunikacyjnym prowadzona jest ona rzadziej niż w sektorze cyberbezpieczeństwa (kolejno: 20% i 24%). Odsetek firm, w których ocena nie jest prowadzona, jest zbliżony (sektor telekomunikacji: 48%; sektor cyberbezpieczeństwa: 53%).

Wykres 7. Ocena potrzeb kompetencyjnych pracowników w opinii pracodawców (ogółem)

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

Najczęściej stosowaną metodą oceny zapotrzebowania na kompetencje u pracowników jest rozmowa z przełożonym (69%). Jest to relatywnie rzadziej wskazywana metoda (o 10 p.p.) niż w poprzedniej edycji. Ocena opisowa przygotowywana np. przez przełożonego jest stosowana w nieco ponad jednej trzeciej (36%; wzrost o 14 p.p.) firm. Wykorzystanie pozostałych technik jest relatywnie mniejsze, ale każda z nich – w stosunku do poprzedniej edycji – jest stosowana częściej[19].

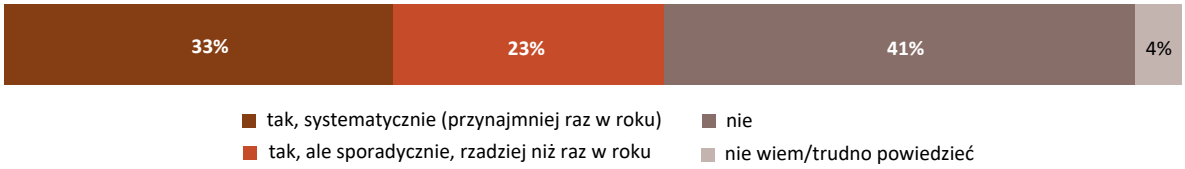
Wykres 8. Metody oceny zapotrzebowania na kompetencje u pracowników w opinii pracodawców (ogółem)

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

[19] W stosunku do I edycji przede wszystkim istotnie częściej stosowano kwestionariusz oceny, którego wykorzystanie wzrosło czterokrotnie w stosunku do poprzedniego pomiaru (z 5% do 20%).

Ocena potrzeb kompetencyjnych w opinii badanych pracowników jest spójna z informacjami uzyskanymi od pracodawców, choć nieco wyższy odsetek badanych (+5 p.p.) niż w przypadku pracodawców deklarował, że taka ocena odbywa się systematycznie. Porównując dane uzyskane od pracowników i pracodawców pracujących w tej samej firmie, można zauważyć, że różnice te w dużym stopniu[20] wynikają z odmiennego postrzegania interwałów czasowych, w jakich odbywa się ocena, np. pracodawca mówił, że w jego firmie ocena odbywa się sporadycznie, a pracownik, że jest to zjawisko regularne. Analogicznie, pracodawca mówił ankieterowi, że nie prowadzi oceny potrzeb kompetencyjnych swoich pracowników, a pracownik deklarował, że ocena się odbywa, ale nieregularnie.

Wykres 9. Ocena potrzeb kompetencyjnych w opinii pracowników (ogółem)



Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 1011), II edycja.

Podobnie jak wśród przedsiębiorców, również wśród pracowników najpopularniejszą (65%, spadek o 12 p.p. w stosunku do poprzedniej edycji) metodą oceny zapotrzebowania na kompetencje jest rozmowa z przełożonym, a na drugim miejscu – ocena opisowa (37%, wzrost o 16 p.p. w stosunku do poprzedniej edycji). Istotną różnicą pomiędzy grupą pracodawców (23%) a pracowników (31%) jest korzystanie z testów pracowniczych, które dodatkowo są wykorzystywane znacznie częściej niż deklarowano w poprzedniej edycji (+15 p.p.). Pozostałe metody są wykorzystywane w podobnym stopniu w opiniach pracodawców i pracowników.

[20] Analiza wykazała, że opisana w dalszej części tekstu zależność jest prawdziwa dla 96% przypadków.

Wykres 10. Metody oceny zapotrzebowania na kompetencje w opinii pracowników

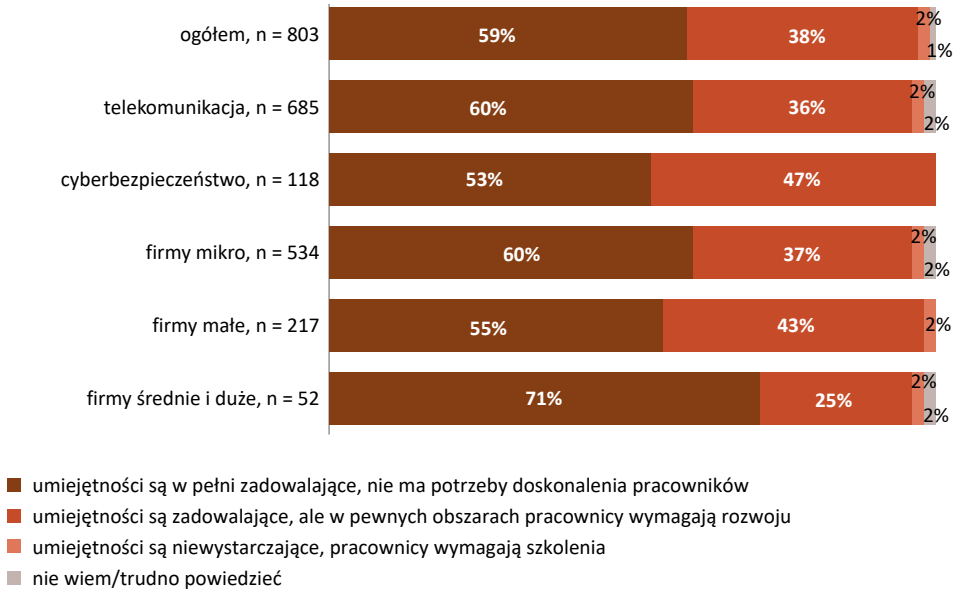
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracowników (n = 561), II edycja.

Duża część pracodawców jest zdania, że umiejętności pracowników są w pełni zadowalające i nie ma potrzeby ich doskonalenia (59%, wzrost o 9 p.p. w stosunku do poprzedniej edycji), a niemal 2 na 5 (38%, spadek o 5 p.p. w stosunku do poprzedniego pomiaru) pracodawców jest zdania, że sytuacja jest zadowalająca, ale nadal jest miejsce na poprawę. Odpowiedzi skrajnie negatywne są nieliczne (2%, spadek o 2 p.p. w stosunku do poprzedniej edycji). Warto dodać, że w I edycji projektu przedsiębiorcy najczęściej wskazywali konieczność pozyskania pracowników, którzy potrafią samodzielnie rozwijać swoje umiejętności, natomiast w II edycji badani wskazują, że kwestia samodzielnego rozwijania kompetencji przez pracowników jest niezbędnym elementem pracy w branży z uwagi na szybką dezaktualizację wiedzy (tj. zmieniające się technologie, dynamiczny rozwój branży, zmieniające się regulacje prawne, trendy rynkowe).

W przypadku firm mikro i małych odsetek respondentów uważających, że ich pracownicy nie muszą być doszkalani, jest na zbliżonym poziomie (różnica 5 p.p. jest w tym przypadku[21] w zasadzie pomijalna). Firmy średnie i duże w większym stopniu są zadowolone z zatrudnianych pracowników – 71% firm jest zdania, że nie potrzebują oni dodatkowego szkolenia, ponieważ ich wiedza i umiejętności są wystarczające.

[21] Wielkość błędu szacowania dla próby n = 217 jest większa niż różnica pomiędzy odpowiedziami.

Wykres 11. Ocena pracodawców dotycząca umiejętności ich pracowników (ogółem, w podziale na sektory oraz wielkość firm)



Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

Zdaniem przedsiębiorców działających w branży, dostrzegających braki kompetencyjne u pracowników, pracownikom najczęściej brakuje umiejętności ogólnych, tj. samoorganizacji, pomysłowości czy terminowości (56%) oraz społecznych, tj. umiejętności pracy w grupie czy komunikatywności (44%). Natomiast umiejętności zawodowych, specyficznych na zajmowanym stanowisku, zdaniem pracodawców pracownikom nie brakuje (jedynie 3% przedsiębiorców wskazało, że pracownikom brakuje takich umiejętności).

Większość firm wymaga wcześniejszego doświadczenia na stanowisku, które ma zajmować pracownik. Stanowiskiem, którego dotyczy to w największym stopniu, jest CISO (83%). Jest to jednocześnie stanowisko, w przypadku którego nastąpiła największa zmiana w stosunku do poprzedniej edycji (+28 p.p.). Kolejne stanowiska, na które wymaga się doświadczenia, to przede wszystkim: programista (72%, +6 p.p. w stosunku do poprzedniej edycji) oraz kierownik projektu (70%, –7 p.p. w stosunku do poprzedniej edycji).

Posiadanie certyfikatu potwierdzającego doświadczenie na danym stanowisku jest wymagane w największym stopniu na stanowiskach architekta ds. bezpieczeństwa (64%) oraz audytora bezpieczeństwa (60%). Pomimo że na pierwszych miejscach znalazły się stanowiska związane

z cyberbezpieczeństwem, nie jest to wymóg jednakowy dla wszystkich stanowisk z tego sektora – dla przykładu certyfikat dla stanowiska penetration tester jest wymagany w jednej trzeciej firm (35%).

Średnia liczba lat wymaganego doświadczenia jest większa w sektorze telekomunikacji niż w sektorze cyberbezpieczeństwa, np. dla stanowiska quality assurance (sektor telekomunikacji) wynosi ona prawie 7 lat, podczas gdy na stanowiskach CISO czy koordynatora SOC (sektor cyberbezpieczeństwa) najwyższe średnie doświadczenie to 3 lata. Jest to czas krótszy niż najkrótszy wymagany w sektorze telekomunikacji (średnio 3,5 roku dla inżyniera).

Tabela 11. Kwestie związane z posiadaniem doświadczenia oraz certyfikatów (w podziale ze względu na stanowiska)

Stanowisko (sektor*)	Wymóg doświadczenia[22]	Posiadanie certyfikatu[23]	Średnia wymagana długość doświadczenia (w latach)
Architekt systemów (T)	69% (–6 p.p.)	45%	3,8
Inżynier (każdej specjalizacji) (T)	58% (–4 p.p.)	42%	3,6
Developer (programista) (T)	72% (+6 p.p.)	51%	4
Project manager (Kierownik projektu) (T)	70% (–7 p.p.)	48%	3,8
Quality assurance (tester) (T)	59% (+4 p.p.)	31%	6,7
CISO (chief information security officer) (C)	83% (+28 p.p.)	46%	3,1
Audytor bezpieczeństwa (C)	60% (–5 p.p.)	60%	2,4
Architekt ds. bezpieczeństwa (C)	69% (+12 p.p.)	64%	2,5
Penetration tester (C)	67% (+14 p.p.)	24%	2,1
Koordynator SOC (security operation center) (C)	68% (+2 p.p.)	36%	3,1
Ekspert ds. bezpieczeństwa systemów/sieci/aplikacji (C)	63% (–1 p.p.)	42%	2,6
Dyrektor handlowy/sprzedaży (U)	62% (–4 p.p.)	35%	3,6

* Oznaczenie stanowisk: T – sektor telekomunikacji, C – sektor cyberbezpieczeństwa, U – stanowisko uniwersalne.
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

22 W nawiasach podano różnicę w stosunku do poprzedniej edycji.

23 Brak porównania do poprzedniej edycji ze względu na zmianę konstrukcji pytania.

6.2. Sposoby rozwijania umiejętności

Blisko dwie trzecie firm – w przypadku odnotowania braku konkretnych umiejętności u swoich pracowników – decyduje się na szkolenie tych osób (63% wskazań; spadek o 18 p.p. w stosunku do I edycji). Jedna trzecia firm decyduje się w takiej sytuacji zatrudnić pracowników o odpowiednich umiejętnościach (35%; wzrost o 14 p.p.). Również zatrudnianie nowych pracowników, aby ich wyszkolić, jest popularniejsze niż wcześniej (26%; wzrost o 18 p.p.). Podobnie często zaobserwować można przesunięcia w ramach firmy, aby na konkretnych stanowiskach znalazły się osoby o wymaganych umiejętnościach (25%; wzrost o 15 p.p.).

Odnotowano relatywnie duży wzrost udziału firm, które nie podejmują żadnych działań. W poprzednim pomiarze takich firm było nieco ponad 6%, obecnie jest ich ponad dwukrotnie więcej.

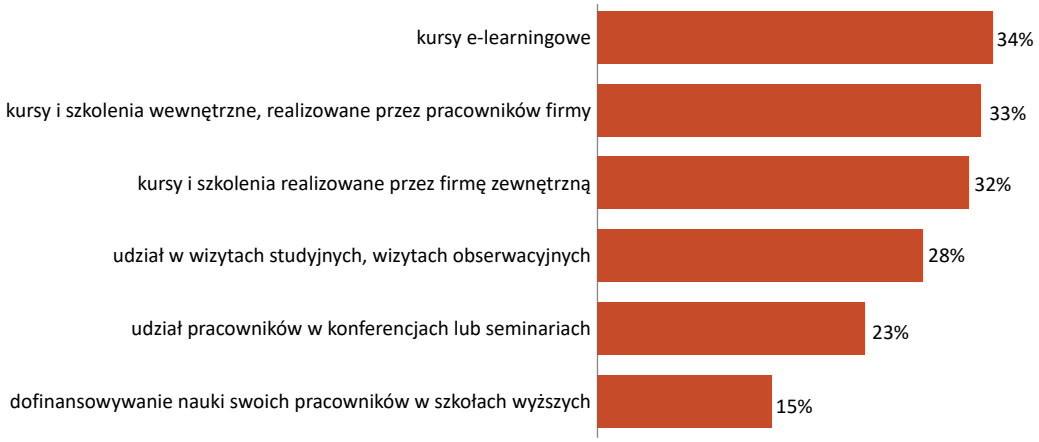
Wykres 12. Działania podejmowane przez pracodawców w przypadku zidentyfikowania braku konkretnych umiejętności u pracowników (ogółem)

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

Przedsiębiorstwa w równym stopniu korzystały z kursów e-learningowych (34%, spadek w stosunku do poprzedniej edycji o 3 p.p.), kursów i szkoleń wewnętrznych (33%, spadek o 4 p.p.) oraz kursów i szkoleń realizowanych przez firmę zewnętrzną (32%, spadek o 4 p.p.).

Kursy e-learningowe są wykorzystywane relatywnie częściej w sektorze cyberbezpieczeństwa niż w sektorze telekomunikacji (47% vs. 32%). W przypadku pozostałych form brak jest istotnych różnic pomiędzy sektorami.

Wykres 13. Formy rozwoju kompetencji, z których korzystała firma w ciągu ostatnich 12 miesięcy* (ogółem)



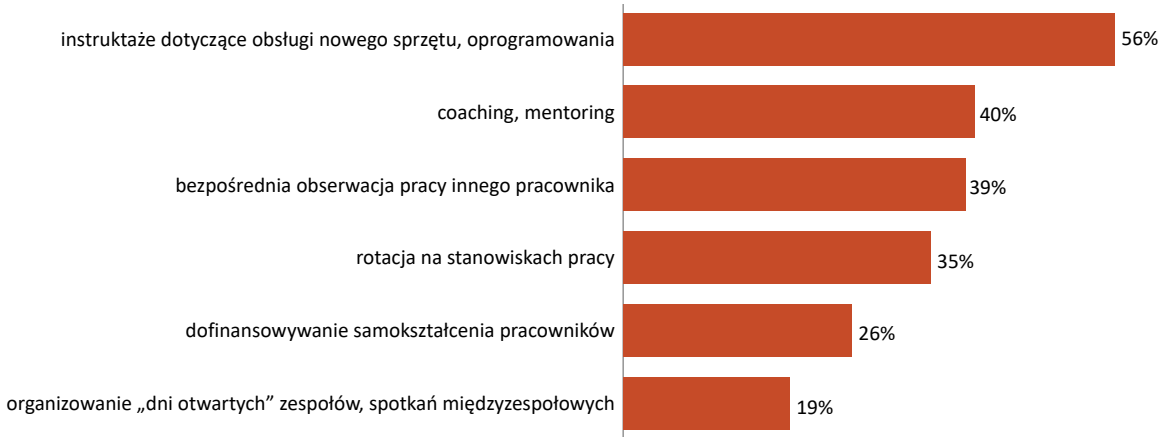
*Wartości nie sumują się do 100%, ponieważ respondent mógł wybrać więcej niż jedną odpowiedź.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

Formy rozwoju kompetencji w miejscu pracy, które firma proponowała, to najczęściej szkolenia (instruktaż) z obsługi sprzętu oraz oprogramowania dostępnego w miejscu pracy (56%, spadek o 1 p.p. w stosunku do I edycji badania). Na drugim miejscu firmy postawiły na mentoring (40%[24]) oraz bezpośrednią obserwację pracy innego pracownika (39%, spadek o 2 p.p.). Trochę częściej, co już pojawiło się w przypadku braku odpowiednich kompetencji pracownika, stosowano rotację pracowników w ramach firmy (35%, wzrost o 5 p.p.). Dofinansowanie samokształcenia pracowników (26%, brak różnicy w stosunku do poprzedniej edycji) oraz organizowanie spotkań międzyzespołowych (19%, wzrost o 1 p.p.) było stosowane rzadziej.

[24] W poprzedniej edycji odpowiedź „coaching/mentoring" była rozdzielona na „mentoring" oraz „uczenie się pod kierunkiem innej osoby, trenera lub przełożonego" czyli coaching, które uzyskały odpowiednio 16% i 41%. Ze względu na zmianę konstrukcji pytania nie podano bezpośredniego porównania.

Wykres 14. Formy rozwoju kompetencji w miejscu pracy, z których korzystała firma w ciągu ostatnich 12 miesięcy (ogółem)



Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

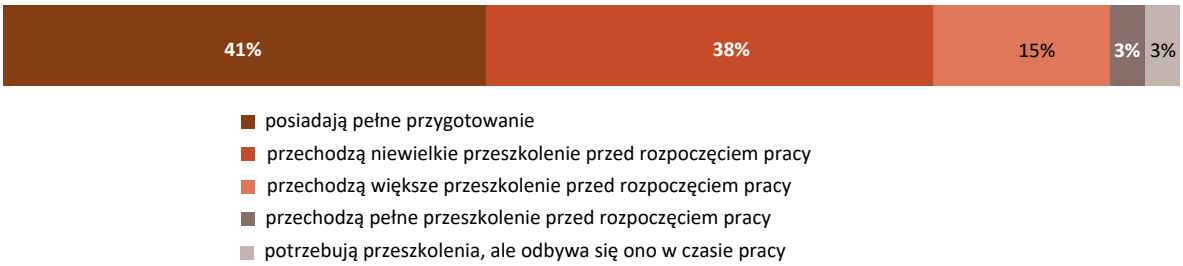
6.3. Kształcenie formalne

Niemal 85% pracodawców jest zdania, że absolwenci opuszczający szkoły/uczelnie posiadają umiejętności potrzebne obecnie na rynku[25]. Ocena przygotowania osób nowo przyjmowanych do firm jest również pozytywna. Co piąty nowy pracownik wymaga większego lub pełnego przeszkolenia przed rozpoczęciem pracy lub zaraz po jej rozpoczęciu (21% obecnie vs. 37% w I edycji[26]). Zdaniem 41% pracodawców absolwenci posiadają pełne przygotowanie do pracy (o 18 p.p. więcej niż w poprzedniej edycji), a dalsze 38% (o 2 p.p. mniej niż w poprzedniej edycji) jest zdania, że potrzebne jest tylko niewielkie szkolenie przed rozpoczęciem pracy. Sektory nie różnicują znacząco tej oceny.

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

[26] Spadek obserwowany głównie ze względu na zmniejszanie się (o 9 p.p.) udziału nowych pracowników, którzy wymagają większego przeszkolenia przed rozpoczęciem pracy.

Wykres 15. Ocena pracodawców dotycząca poziomu przygotowania nowych pracowników do podjęcia pracy zawodowej (ogółem)



Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

Jednocześnie 9 na 10 badanych pracowników (niezależnie od sektora) ma poczucie, że szkoła czy uczelnia, którą ukończyli, przygotowała ich do pracy na obecnym stanowisku.

Zdaniem większości (86%) pracodawców programy kształcenia są dopasowane do potrzeb rynku pracy. W celu podniesienia poziomu nauczania w szkołach branżowych oraz na uczelniach przedsiębiorcy proponują włączenie przedstawicieli firm do tworzenia podstaw programowych w ramach edukacji, zarówno na poziomie szkół podstawowych, jak i ponadpodstawowych. Konsultacje z sektorem biznesu powinny dotyczyć też programów oferowanych na studiach. Takie rozwiązanie pozwoli potencjalnym nowym pracownikom na nabycie kompetencji potrzebnych w branży.

> *Z pewnością zachęcanie szkolnictwa, żeby wyciągało też chętniej rękę do przedsiębiorcy i pytało się, jakie ma przedsiębiorca zapotrzebowanie, czy ewentualnie jakieś wdrożenie programów stażowych, czy dotowanie nawet tych staży. Moja firma ma patronat nad jednym z techników nad klasą telekomunikacyjną i mam świetny kontakt z panią dyrektor, ale wiem, że to jest wyjątek. Zawsze co roku zapraszamy uczniów, żeby przyjrzeli się tej pracy tej branży u nas, natomiast też ze względu na rozmiar biura i możliwości niestety nie możemy przyjąć tyle, ile byśmy chcieli i tylu, ilu jest chętnych. Więc myślę, że ściślejsza współpraca branży ze szkolnictwem też by coś wniosła*.
>
> [Cytat z prospektywnego panelu eksperckiego – przedstawiciel sektora telekomunikacji]

Wykres 16. Dopasowanie programów nauczania do rynku pracy (ogółem)

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

W opinii pracodawców z branży, szkoły i uczelnie powinny przede wszystkim uczyć umiejętności specjalistycznych (46%)[27] oraz podstawowych umiejętności związanych z wykonywaniem zawodu (41%). Odsetki wskazań pozostałych odpowiedzi są zbliżone do siebie (od 27% do 32%). Wiedza interdyscyplinarna jest najrzadziej pożądana (27%)[28].

Wykres 17. Wiedza i umiejętności, jakie powinny być przekazywane w szkołach/na uczelniach w kontekście pracy w branży (ogółem)

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

[27] Na ten typ umiejętności zwraca uwagę 60% pracodawców reprezentujących średnie i duże przedsiębiorstwa.

[28] Aczkolwiek nieco częściej w przypadku reprezentantów średnich i dużych firm. Ta grupa pracodawców zdecydowanie rzadziej (12% w stosunku do 33% w przypadku małych firm) wskazywała na umiejętności miękkie i społeczne jako te, które powinny być przekazywane w toku edukacji formalnej.

Jak wynika z wypowiedzi badanych ekspertów, z uwagi na ciągłe zmiany, m.in. technologiczne, prawne czy rynkowe, warto byłoby położyć większy nacisk w branży na współpracę na linii edukacja–biznes. Partycypacja przedsiębiorców w zakresie opracowywania programów kształcenia i wyznaczania aktualnego zapotrzebowania na kompetencje pozwoliłaby na lepsze przygotowanie potencjalnych nowych pracowników skutkujące podjęciem z nimi dalszej współpracy.

> *(…) ja bym zaczął od samego źródła jeżeli chodzi o poszukiwanie specjalistów. Uczelnie wyższe czy nawet szkoły na poziomie techników powinny skłaniać tych młodych ludzi, żeby jednak wybierali ten kierunek, żeby właśnie szli w stronę cyberbezpieczeństwa…* [Cytat z prospektywnego panelu eksperckiego – przedstawiciel sektora cyberbezpieczeństwa]

Zdecydowana większość firm (95%) nie współpracuje ze szkołami i/lub uczelniami wyższymi. Bardziej widoczna jest natomiast ich współpraca z firmami szkoleniowymi (18%).

Ewentualna współpraca ze szkołami i/lub uczelniami najczęściej przyjmuje formę praktyk i staży dla uczniów/studentów (43%) oraz prowadzenia zajęć przez przedstawicieli przedsiębiorstwa (34%). Natomiast najrzadziej wykorzystywane formy współpracy to zamawiane prace dyplomowe (6%) czy realizacja kierunku na zlecenie przedsiębiorstwa (8%).

7. Zadowolenie z pracy i motywacja pracowników

W rozdziale zawarto ocenę ogólną zadowolenia z pracy pracowników objętych badaniem, a także zadowolenia z wybranych aspektów ich pracy. Przyjrzano się również sposobom motywacji stosowanym przez pracodawców oraz atrakcyjnym dla pracowników.

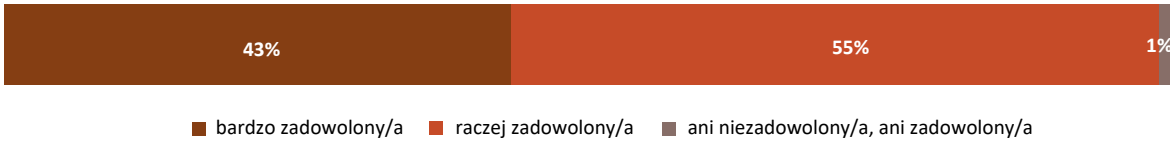
Najważniejsze wnioski z rozdziału:

- Badani pracownicy zatrudnieni w branży na kluczowych stanowiskach w większości (98%) są zadowoleni z wykonywanej pracy, ze względu na możliwości rozwoju, jakie ona daje. Warto podkreślić, że zadowolenie było wysokie również w I edycji projektu (95% wskazań). Mimo tak wysokiego odsetka badanych pracowników, którzy są ogólnie zadowoleni z pracy, odnotowano spory udział pracowników odczuwających wzrastający poziom przeciążenia zadaniami zawodowymi (59%), co może być skutkiem zwiększonego popytu na usługi z branży w połączeniu z deficytem pracowników posiadających specjalistyczne kompetencje niezbędne do pracy w określonym zawodzie.
- Aż 97% pracowników z branży deklaruje, że planuje kontynuować pracę w obecnej firmie.
- Pracownicy poproszeni o ocenę poszczególnych stwierdzeń dotyczących obecnej pracy w branży wypowiadali się pozytywnie o większości z nich (16 z 22). Najlepsze oceny obejmują najważniejsze, pozytywne odczucia co do pracy – sensowność jej wykonywania (96%), realizowanie zadań, które się lubi (95%), dawanie przez pracę poczucia bezpieczeństwa (również finansowego) (95%) czy przebywanie w miejscu, w którym panuje dobra atmosfera (94%).
- Najczęstszym stosowanym przez pracodawców sposobem motywacji pracowników są premie roczne (73%) oraz możliwość pracy stacjonarnej (63%) lub hybrydowej (51%) (możliwość dopasowania miejsca pracy do indywidualnych potrzeb pracownika). Wskazywano również wysokie znaczenie harmonii między pracą a życiem prywatnym (58%) oraz zapewnienie przyjaznych warunków pracy (57%).

7.1. Zadowolenie z wykonywanej pracy

Pracownicy są ogólnie zadowoleni z wykonywanej pracy – suma odpowiedzi „bardzo zadowolony" i „raczej zadowolony" wynosi 98% (w I edycji: 95%)[29].

Wykres 18. Zadowolenie z wykonywanej pracy pracowników zatrudnionych na kluczowych stanowiskach



Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracowników (n = 1011), II edycja.

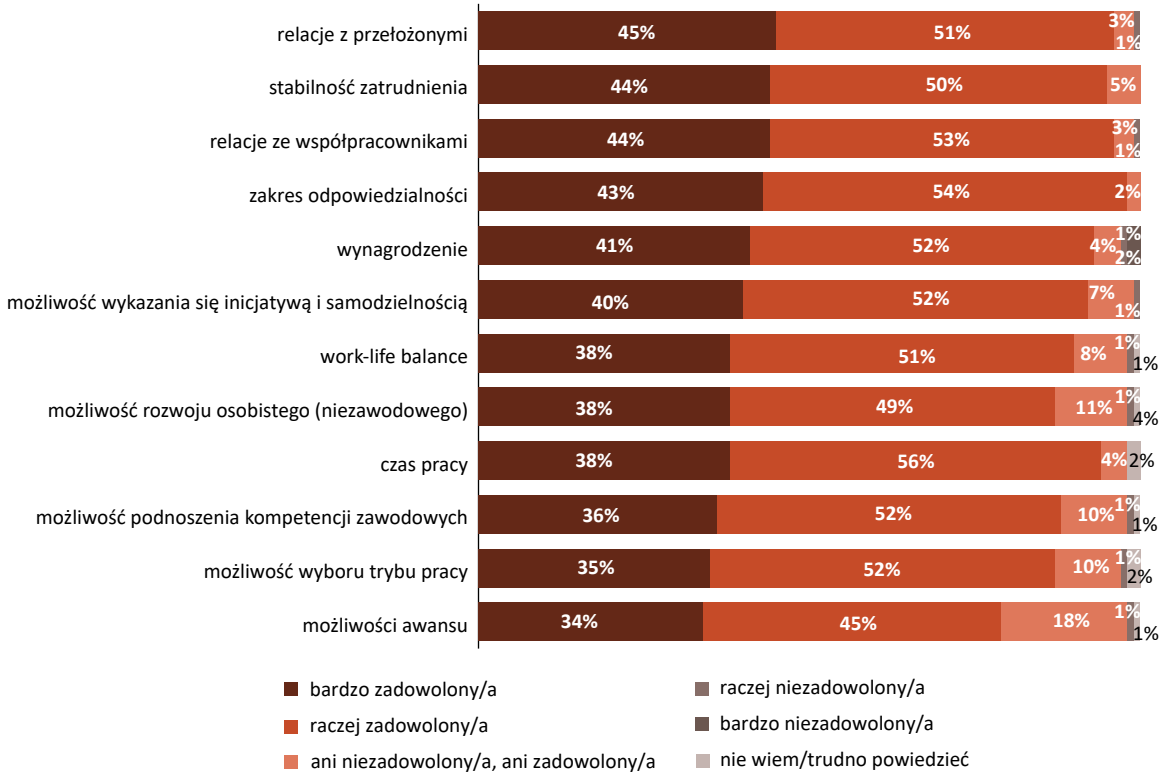
Również rozmaite aspekty związane z pracą i wykonywaniem zadań zawodowych zostały ocenione przez pracowników stosunkowo dobrze. Największy udział bardzo zadowolonych pracowników zatrudnionych na stanowiskach kluczowych dla branży obserwuje się w przypadku relacji z przełożonymi (45% bardzo zadowolonych i 96% odpowiedzi ogólnie pozytywnych – co najmniej „raczej zadowolonych" vs. 97% w I edycji) oraz ze współpracownikami (44% bardzo zadowolonych i 97% ogólnie pozytywnie nastawionych vs. 96% w I edycji). Wśród elementów, które budzą najbardziej pozytywne odczucia, są także: poczucie stabilności zatrudnienia (44% bardzo zadowolonych i 94% ogólnie pozytywnie nastawionych vs. 95% w I edycji) oraz zakres odpowiedzialności, jaki posiadają pracownicy (43% bardzo zadowolonych i 97% ogólnie pozytywnie nastawionych[30]). Warto zwrócić uwagę również na zadowolenie z wynagrodzenia – 2 na 5 pracowników zatrudnionych na stanowiskach kluczowych dla branży jest bardzo zadowolonych z wynagrodzenia, a ponad połowa – raczej zadowolona.

Najrzadziej pozytywnie oceniana jest możliwość awansu, ale nawet w tym przypadku blisko czterech na pięciu badanych (79%) jest raczej zadowolonych z możliwości, jakie daje firma. Aczkolwiek w stosunku do I edycji obserwuje się relatywnie duży spadek (o 12 p.p.) udziału raczej zadowolonych.

[29] Na wykresie nie zaprezentowano odpowiedzi negatywnych: „raczej niezadowolony/a" i „bardzo niezadowolony/a", ponieważ właściwie odpowiedzi te nie wystąpiły. Tylko jedna osoba określiła się jako „bardzo niezadowolona" co stanowi 0,1% całej próby.

[30] Aspekt nieoceniany w I edycji.

Wykres 19. Zadowolenie pracowników z wykonywanej pracy w oparciu o wybrane aspekty*



*Sortowanie po odsetku odpowiedzi „bardzo zadowolony/a".
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracowników (n = 1011), II edycja.

Pracownicy poproszeni o ocenę poszczególnych stwierdzeń dotyczących m.in. komfortu pracy, zadań zawodowych czy nastawienia do obecnie wykonywanej pracy wypowiadali się pozytywnie[31] o większości z nich (16 z 22).

Patrząc na wysoko ocenione stwierdzenia, można wskazać, że najlepsze oceny obejmują najważniejsze, pozytywne odczucia co do pracy – sensowność jej wykonywania (96%), realizowanie zadań, które się lubi (95%), dawanie przez pracę poczucia bezpieczeństwa (również finansowego) (95%) czy przebywanie w miejscu, w którym panuje dobra atmosfera (94%).

[31] Suma odpowiedzi „raczej tak" oraz „zdecydowanie tak" powyżej 66%.

Wszystkie analizowane stwierdzenia wraz z odsetkami wskazań zamieszono w Tabeli 12. Na zielono zaznaczono stwierdzenia, w przypadku których suma odpowiedzi „zdecydowanie tak" oraz „raczej tak" (dalej: top2boxes) wynosi min. 70%. Dodatkowo **pogrubiono** stwierdzenia, dla których top2boxes wynosi ponad 90%. Kolorem czerwonym oznaczono te aspekty, w przypadku których suma odpowiedzi: „zdecydowanie nie" oraz „raczej nie" (bottom2boxes) wynosi min. 50%. Wyjątkiem w drugim przypadku są stwierdzenia z tzw. odwróconą skalą, czyli stwierdzenia z zastosowaną negacją. W tym przypadku bottom2boxes jest również zaznaczony na zielono.

Tabela 12. Ocena pracowników dotycząca poszczególnych stwierdzeń odnoszących się do obecnej pracy*

Stwierdzenia dotyczące obecnej pracy	Zdecydowanie nie	Raczej nie	Raczej tak	Zdecydowanie tak
W pracy robię to, co lubię.	1%	5%	38%	57%
Czuję, że praca, którą wykonuję, ma sens.	1%	3%	41%	55%
Czuję, że w pracy wykorzystuję swoją wiedzę i umiejętności.	2%	5%	40%	52%
W mojej pracy czuję się bezpiecznie.	1%	4%	43%	51%
Mam zapewnione odpowiednie narzędzia/sprzęt do wykonywania mojej pracy.	3%	8%	39%	50%
Moja praca daje mi poczucie bezpieczeństwa finansowego.	1%	4%	46%	49%
W moim miejscu pracy panuje dobra atmosfera.	1%	5%	45%	49%
Mam możliwość realizacji swoich własnych pomysłów.	5%	11%	35%	49%
Osoby, z którymi współpracuję, są dobre w tym, co robią.	1%	4%	46%	48%
Dzięki pracy ciągle uczę się nowych rzeczy.	2%	10%	44%	43%
W razie potrzeby mam możliwość zrobienia krótkiej przerwy w pracy.	3%	10%	47%	41%
Każdego dnia w mojej pracy wykonuję podobne zadania.	3%	23%	40%	32%
Mogę sam decydować o organizacji mojego dnia pracy.	3%	25%	41%	31%
Moja praca wymaga ciągłego dokształcania się.	2%	21%	45%	30%
Mam zbyt dużo zadań, by dobrze wykonać je na czas.	10%	37%	30%	23%
Często muszę wykonywać zadania, które są zbyt proste w stosunku do moich umiejętności.	14%	41%	23%	22%
Czasem zauważam, że brakuje mi wiedzy lub umiejętności, by dobrze wykonać zadania, które mam zrealizować w pracy.	15%	43%	23%	18%
Często muszę wykonywać zadania, które są zbyt trudne w stosunku do moich umiejętności.	16%	43%	23%	18%

Stwierdzenia dotyczące obecnej pracy	Zdecydowanie nie	Raczej nie	Raczej tak	Zdecydowanie tak
Często czuję się zbyt zmęczony(a) po pracy, żeby zająć się pracami domowymi.	15%	42%	26%	17%
Moja praca uniemożliwia mi poświęcanie rodzinie tyle czasu, ile bym chciał(a).	16%	41%	26%	16%
Wskutek nadmiaru pracy, nie mam zbyt wiele czasu na rozrywkę i kontakty ze znajomymi.	17%	42%	25%	16%

*Sortowanie według odsetka wskazań odpowiedzi „zdecydowanie tak".
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracowników (n = 1011), II edycja.

Zdecydowana większość pracowników (suma odpowiedzi: „zdecydowanie tak" oraz „raczej tak" wynosi 96–97%), niezależnie od branży, zamierza kontynuować pracę w obecnym miejscu zatrudnienia. Przeciwnego zdania jest 3% badanych, spośród których nikt obecnie nie poszukuje aktywnie pracy. Podobne wyniki uzyskano w I edycji.

Wykres 20. Plany pracowników dotyczące kontynuacji zatrudnienia w obecnym miejscu pracy

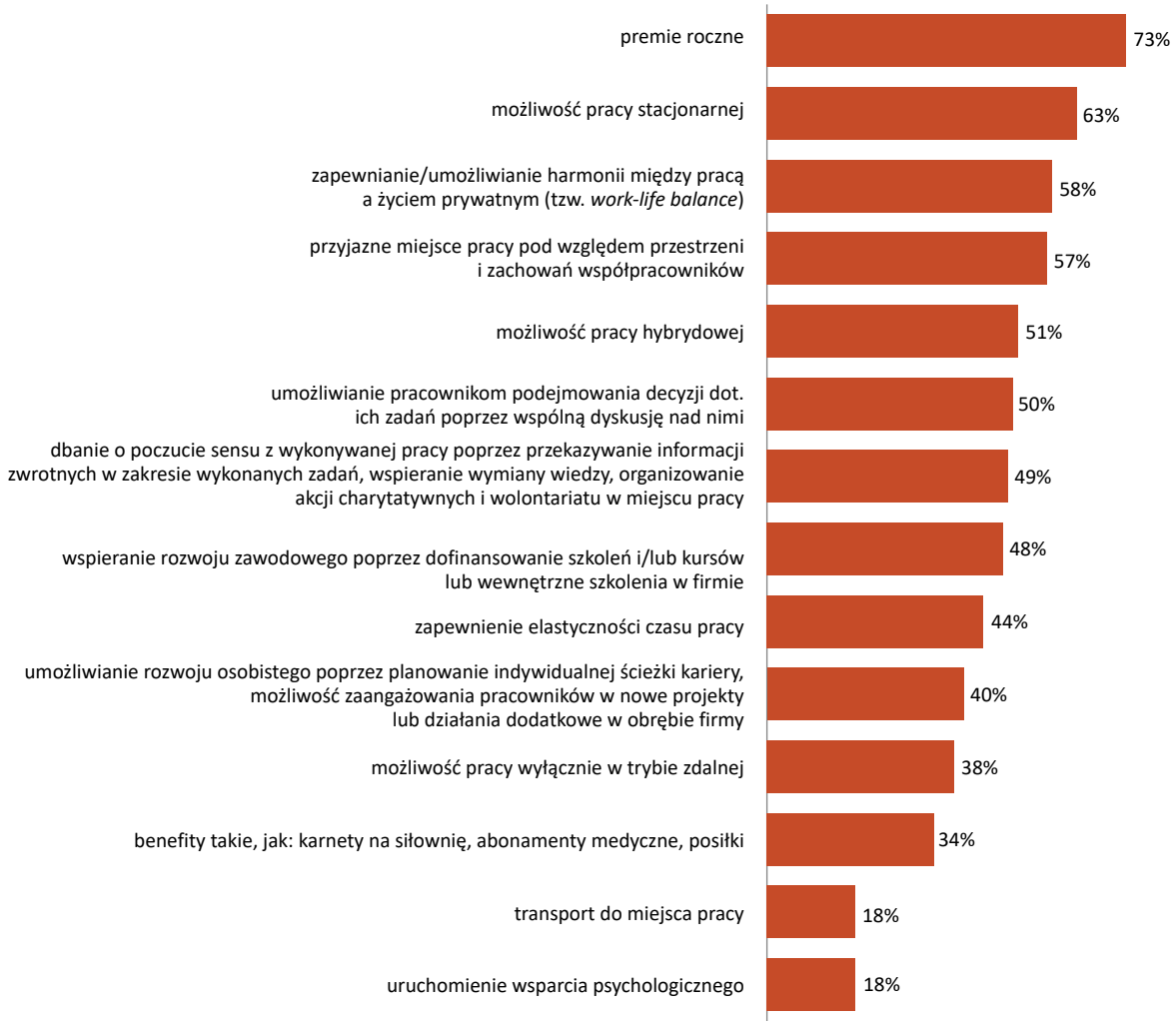
Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracowników (n = 1011), II edycja.

7.2. Motywacje pracowników

Zarówno najczęściej stosowanym przez pracodawców, jak i najatrakcyjniejszym z punktu widzenia pracowników zatrudnionych w branży na kluczowych stanowiskach motywatorem są premie (73% wskazań w przypadku pracodawców i 81% w przypadku pracowników). Na kolejnych miejscach pod kątem stosowania w firmach przez pracodawców są takie motywatory, jak: oferowanie możliwości pracy stacjonarnej (63%), rozwiązania zapewniające *work-life balance* (58%), przyjazne miejsce pracy (57%) czy możliwość pracy hybrydowej (51%). Dla pracowników istotne (poza podstawowym wynagrodzeniem) jest: dbanie o dobrą atmosferę między pracownikami (66%), dobrze zorganizowane stanowisko pracy (64%), abonament medyczny (59%) oraz *work-life balance* (58%).

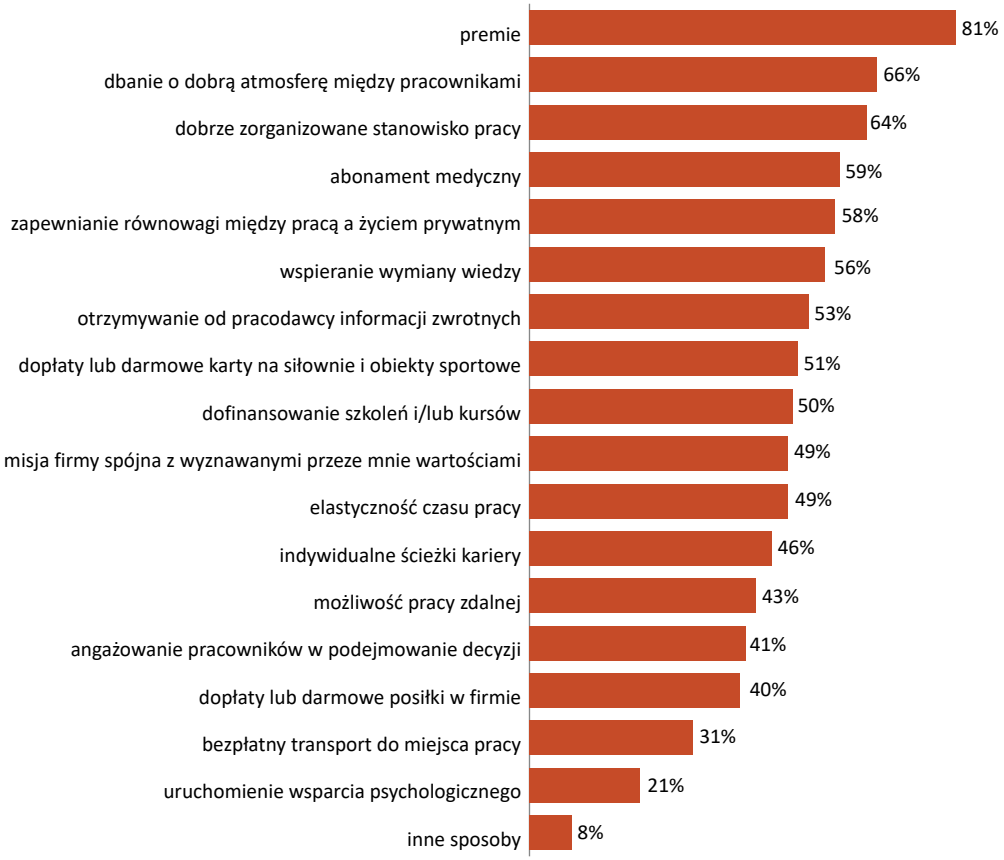
Warto zwrócić uwagę również na inne aspekty wskazywane przez więcej niż połowę pracowników jako atrakcyjne: wspieranie wymiany wiedzy, otrzymywanie informacji zwrotnych od pracowników czy dofinansowanie szkoleń i/lub kursów. Są to elementy stosowane przez część pracodawców, ale warte wzmocnienia.

Wykres 21. Sposoby motywacji pracowników stosowane w firmach z branży telekomunikacji i cyberbezpieczeństwa – perspektywa pracodawcy (ogółem)



Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 803), II edycja.

Wykres 22. Najbardziej atrakcyjne sposoby motywacji stosowane w firmach z branży telekomunikacji i cyberbezpieczeństwa – perspektywa pracownika (ogółem)



Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracowników (n = 1011), II edycja.

8. Bilans kompetencji

8.1. Wprowadzenie do bilansu

Jednym z głównych celów badań ilościowych było opracowanie bilansu kompetencji, czyli swoistego spojrzenia na kluczowe kompetencje na poszczególnych stanowiskach z perspektyw pracodawców i pracowników. Zestawienie tych ocen może pomóc w zbilansowaniu rynku pracy w analizowanych sektorach w zakresie podaży pracowników o odpowiednich kompetencjach oraz zapotrzebowania na nich ze strony pracodawców.

Pracodawcy w badaniu ilościowym odnieśli się do kompetencji pod kątem:

- ważności kompetencji[32],
- trudności znalezienia osoby, która posiada określoną kompetencję potrzebną do pracy na danym stanowisku[33],
- prognozy zmiany znaczenia tej kompetencji w ciągu najbliższych trzech lat[34].

Dodatkowo, wśród kompetencji, których – w opinii pracodawców – znaczenie w ciągu następnych trzech lat wzrośnie, wyznaczono te, których znaczenie już teraz szybko rośnie lub będzie rosło najszybciej w perspektywie najbliższych trzech lat roku tzw. *hot skills*.

[32] Treść pytania: Myśląc o Pana/Pani branży, proszę ocenić, jak ważna jest dana umiejętność w kontekście pracy na ocenianym stanowisku z punktu widzenia Państwa firmy? Proszę ocenić ważność na pięciopunktowej skali, na której 1 oznacza marginalnie ważna, a 5 – kluczowa. Inne możliwe odpowiedzi: nie wiem/trudno powiedzieć oraz: odmowa odpowiedzi.

[33] Treść pytania: Proszę ocenić, czy trudno, czy łatwo jest znaleźć do pracy na ocenianym stanowisku osobę, która posiada tę umiejętność? Odpowiedzi: trudno, łatwo. Inne możliwe odpowiedzi: nie wiem/trudno powiedzieć oraz: odmowa odpowiedzi.

[34] Treść pytania: Proszę wskazać, czy w Pana/Pani opinii znaczenie tej umiejętności zmieni się w ciągu najbliższych 3 lat? Odpowiedzi: znaczenie wzrośnie, pozostanie bez zmian, znaczenie zmniejszy się. Inne możliwe odpowiedzi: nie wiem/trudno powiedzieć oraz: odmowa odpowiedzi.

Pracownicy w badaniu ilościowym oceniali natomiast własny poziom kompetencji przypisanych do zajmowanego przez nich stanowiska[35] oraz chęć ich rozwoju[36].

Uwzględnione w bilansie profile – zgodnie z założeniami projektu – tworzone są przez kompetencje kluczowe do realizacji zadań zawodowych na danym stanowisku. W prezentowanych analizach przyjęto, że:

- o kompetencjach trudno dostępnych mówimy, gdy minimum 51% pracodawców oceniających dany profil kompetencyjny wskazuje, że trudno jest znaleźć na rynku pracy osoby posiadające dane kompetencje,
- o kompetencjach o wzrostowym znaczeniu mówimy wówczas, gdy przynajmniej 33% pracodawców wskaże je jako te, których znaczenie wzrośnie w perspektywie 3 lat,
- kompetencjami *hot skills* są te, które zostały wskazane przez minimum 20% pracodawców jako takie, których znaczenie rośnie bardzo szybko lub będzie rosło najszybciej w perspektywie 3 lat,
- oznaczanych jest jedynie pięć kompetencji[37], które pracownicy wskazywali najczęściej jako te, które chcieliby rozwinąć w najbliższym czasie.

Na prezentowanych w ramach stanowisk wykresach kompetencje sortowane są wg średniej ważności określonej przez pracodawcę (od kompetencji najważniejszej z punktu widzenia wykonywania obowiązków na danym stanowisku do najmniej ważnej; oznaczenie graficzne: brązowe koło). Na ten sam wykres naniesiono także średnie wartości samooceny kompetencji pracowników (oznaczenie graficzne: jasnobrązowy kwadrat).

[35] Treść pytania: Praca na konkretnym stanowisku wymaga określonego poziomu umiejętności. Często jest tak, że w jednej lub dwóch dziedzinach nasze umiejętności są w miarę wysokie, podczas gdy w innych są one znacznie niższe. Przeczytam teraz listę umiejętności wymaganych na Pana/Pani stanowisku. Przy każdej z nich poproszę Pana/Panią o ocenę poziomu własnych umiejętności pod tym względem na 5-punktowej skali, gdzie 1 oznacza poziom niski, a 5 – bardzo wysoki. Inne możliwe odpowiedzi: nie wiem/trudno powiedzieć oraz: odmowa odpowiedzi.

[36] Treść pytania: Biorąc pod uwagę specyfikę pracy na Pana/Pani stanowisku, proszę pomyśleć i powiedzieć, jakie umiejętności chciałby/chciałaby Pan/Pani rozwinąć? Proszę wskazać co najwyżej trzy takie umiejętności.

[37] Liczba kompetencji może być mniejsza lub większa w zależności od odpowiedzi udzielonych przez respondentów. Jeśli taki sam odsetek badanych wskaże np. 7 kompetencji, to w wykazie zostanie ujęte wszystkie siedem. W drugą stronę – mniejszej liczby kompetencji – mamy do czynienia z sytuacją, w której respondent wskazał np. 4 kompetencje wskazywane często, a piąta jest wskazywana np. dwukrotnie rzadziej. Aby nie zaburzać odbioru, że coś jest ważne w sytuacji, kiedy nie jest, taka kompetencja zostanie pominięta.

Dodatkowe symbole (poza bazowymi dla wykresu: oceną ważności i samooceną posiadanych kompetencji) uwzględnione w Tabeli 13 zostały umieszczone przy opisie danej kompetencji, a nie na samym wykresie. Celem jest zwiększenie czytelności wykresu.

Tabela 13. Legenda do bilansu kompetencji

Symbol	Znaczenie
●	ocena ważności poszczególnych kompetencji dokonana przez pracodawcę
■	samoocena posiadanej kompetencji dokonana przez pracownika
●	kompetencja wskazana jako trudna do pozyskania przez pracodawców[38]
⬆	kompetencja, której znaczenie będzie rosło w ciągu najbliższych 3 lat
🔥	*hot skills*
Kompetencja	kompetencja, którą pracownicy chcieliby najbardziej rozwijać

[38] Zastąpienie brązowego koloru punktu pomarańczowym wskazuje na trudną dostępność kompetencji.

8.2. Szczegółowy bilans kompetencji dla kluczowych stanowisk

Architekt systemów

Głównymi zadaniami specjalisty na tym stanowisku są: tworzenie spójnej i logicznej architektury w systemach, programach; ustalanie najlepszej możliwej drogi (wykorzystywanych narzędzi, technologii, sposobów na osiągnięcie ustalonych w projekcie założeń) dopasowanej do konkretnego zadania w celu osiągniecia założonych celów; komunikowanie się z zespołem programistów w celu omówienia zadań i problemów; edukowanie programistów i innych członków zespołu na temat opracowanej architektury systemu, programu.

W przypadku tego stanowiska kompetencje trudno dostępne dotyczą zarówno obszaru wiedzy (np. wiedza dziedzinowa z zakresu telekomunikacji czy wiedza z zakresu architektury systemów), jak również umiejętności (np. znajomość języków programowania czy wykorzystania metodyk zwinnych).

Obecnie w profilu kompetencyjnym architekta systemów nie występują kompetencje, które można by uznać za *hot skills*, natomiast kompetencje zyskujące na znaczeniu to wiedza z obszaru architektury systemów, technologii komputerowych, umiejętność pełnego wykorzystania rozwiązań dostępnych wewnątrz firmy czy analityczne myślenie.

Warto dodać, że przedsiębiorcy z branży poproszeni o odniesienie się do konkretnych kompetencji zdefiniowanych przez ekspertów branżowych biorących udział w badaniach jakościowych jako obecnie niewystępujące w profilu, ale z perspektywą wzrostu znaczenia w ciągu nadchodzących 3 lat podzielili odczucia ekspertów – 2 na 3 przedsiębiorców widzi szansę na wzrost znaczenia, w kontekście analizowanego profilu, wiedzy z zakresu sztucznej inteligencji (AI), a 7 na 10 – wiedzy z zakresu technologii *machine learning*.

Badani architekci systemów najlepiej oceniają swoje: umiejętności zarządzania cyklem życia systemów (średnia samoocena: 4,52) oraz skuteczne komunikowanie się i kreatywność (średnia samoocena: 4,45). Kompetencje, które badani architekci systemów chcieliby rozwinąć w najbliższym czasie, dotyczą przede wszystkim wiedzy z obszaru telekomunikacji.

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

52% firm z sektora telekomunikacji zatrudnia przynajmniej jedną osobę na stanowisku architekta systemów.

13% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku architekta systemów.

12% pracodawców zatrudniających architekta systemów prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

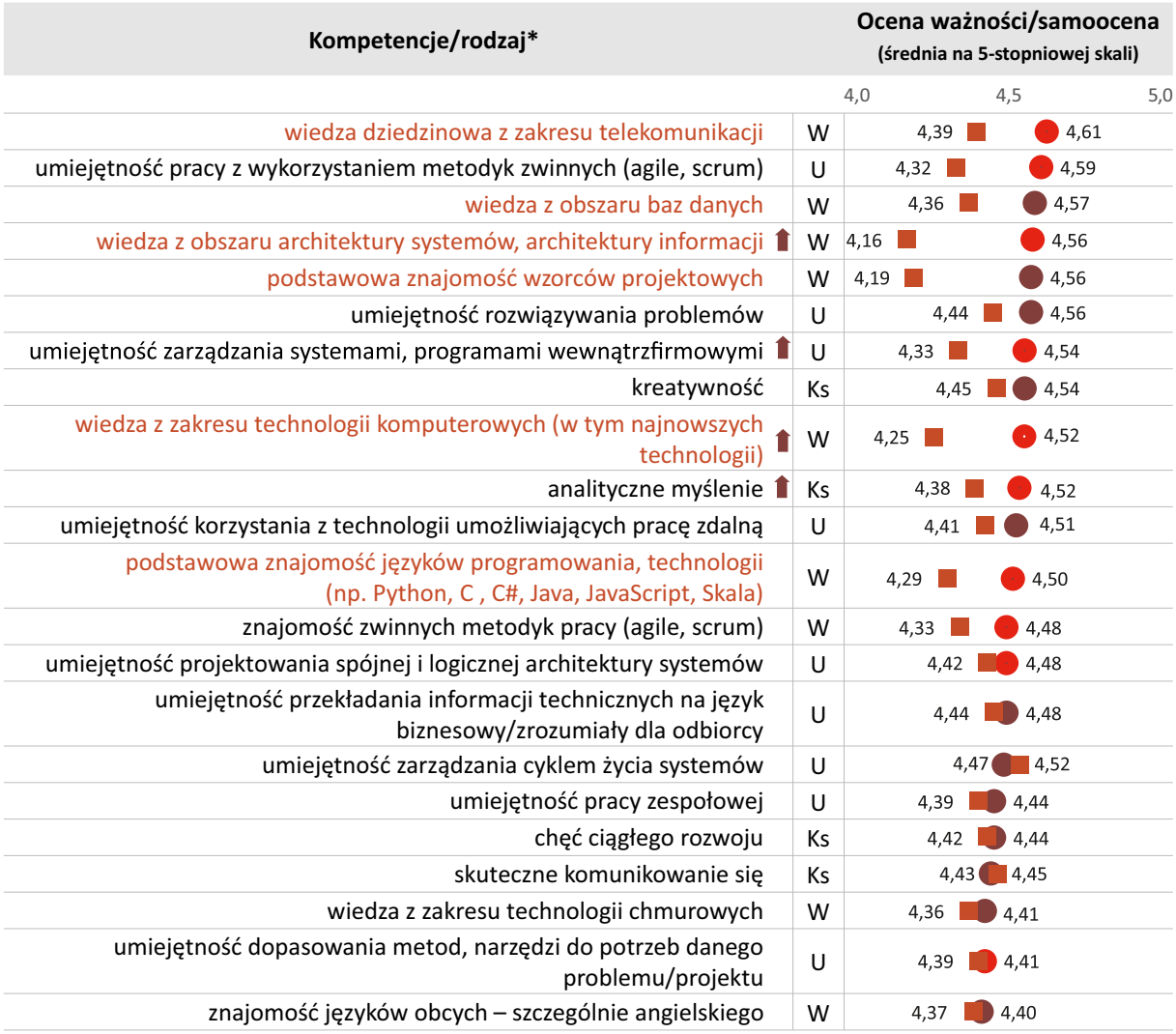
99% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

98% pracowników pozytywnie ocenia swoje warunki pracy.

43% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **24%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

89% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 23. Bilans kompetencji dla stanowiska: architekt systemów



* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 254) i badanie ilościowe pracowników (n = 153), II edycja.

Inżynier

Głównymi zadaniami specjalisty na tym stanowisku są: projektowanie sieci przewodowych oraz bezprzewodowych, tworzenie dokumentacji, praca przy modernizowaniu infrastruktury telekomunikacyjnej, konfiguracja urządzeń oraz pomoc w przeprowadzaniu procesów rekrutacyjnych.

Kompetencje trudne do pozyskania w większym stopniu dotyczą umiejętności niż wiedzy. Wynika to wprost z zadań realizowanych na stanowisku inżyniera. Są to przede wszystkim: umiejętność projektowania sieci czy tworzenia zrozumiałych dokumentacji technicznych. W przypadku tego stanowiska nie odnotowano, w oparciu o przyjęte kryteria procentowe, ani kompetencji przewidywanych jako wzrostowe w perspektywie nadchodzących 3 lat, ani kompetencji, które można by określić jako *hot skills*.

Badani inżynierowie pracujący w sektorze telekomunikacji najlepiej oceniają swoje możliwości w zakresie: samodzielnego rozwiązywania problemów czy zadań (średnia samoocena: 4,49) oraz konfiguracji urządzeń (średnia samoocena: 4,45). Chcieliby w najbliższym czasie zdobyć przede wszystkim wiedzę związaną z wiodącymi w branży technologiami, łącznością czy systemami i oprogramowaniem.

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

68% firm z sektora telekomunikacji zatrudnia przynajmniej jedną osobę na stanowisku inżyniera.

22% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku inżyniera.

9% pracodawców zatrudniających inżynierów prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

98% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

99% pracowników pozytywnie ocenia swoje warunki pracy.

41% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **24%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

86% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 24. Bilans kompetencji dla stanowiska: inżynier

Kompetencje/rodzaj*		Ocena ważności/samoocena (średnia na 5-stopniowej skali)
		4,0 4,5 5,0
zapewnianie zabezpieczeń dostępu do urządzeń, narzędzi	U	4,33 4,84
umiejętność projektowania sieci przewodowych, bezprzewodowych	U	4,41 4,83
konfiguracja urządzeń	U	4,45 4,83
umiejętność analizy wydajności systemów	U	4,40 4,79
konserwacja urządzeń	U	4,38 4,75
umiejętność wyszukiwania informacji oraz weryfikacji ich rzetelności	U	4,44 4,75
wiedza z zakresu łączności przewodowej, bezprzewodowej, radiowej, satelitarnej	W	4,23 4,66
wiedza z zakresu wiodących technologii w branży	W	4,44 4,64
umiejętność związana z rozumieniem dokumentacji technicznych	U	4,39 4,64
umiejętność samodzielnego rozwiązywania problemów, zadań	U	4,49 4,59
wiedza z zakresu systemów i oprogramowania	W	4,37 4,57
chęć ciągłego rozwoju	Ks	4,38 4,57
skuteczne komunikowanie się	Ks	4,44 4,55
umiejętność wdrażania nowych technologii do użytku	U	4,31 4,53
umiejętność pracy w zespole	U	4,44 4,53
umiejętność tworzenia zrozumiałych dokumentacji technicznych	U	4,37 4,49
znajomość języków obcych – szczególnie angielskiego	W	4,23 4,46

Pracodawca:

- trudno pozyskać na rynku pracy
- *hot skills* znaczenie wzrośnie

Pracownik:

- samoocena
- kompetencja – kompetencja, którą chce rozwijać

* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 343) i badanie ilościowe pracowników (n = 162), II edycja.

Developer (programista)

Głównymi zadaniami specjalisty na tym stanowisku są: programowanie (pisanie kodu) systemów, programów i aplikacji najczęściej związanych z obsługą konkretnych sprzętów elektronicznych; kooperacja z zespołem programistów w celu stworzenia spójnego produktu.

W przypadku tego stanowiska kompetencji trudnych do pozyskania jest relatywnie niewiele. Są one skupione w obszarze wiedzy i dotyczą takich kwestii, jak znajomość metodyk zwinnych, znajomość języków programowania czy wiedza dziedzinowa z zakresu telekomunikacji.

Obecnie w profilu kompetencyjnym Developera/programisty występuje jedna kompetencja, którą można określić jako *hot skill*, a mianowicie: znajomość języków programowania. Jest to najważniejsza – z punktu widzenia pracodawców – kompetencja do wykonywania zadań zawodowych na tym stanowisku. W profilu wyróżnić również można kompetencje, które przewiduje się, że będą zyskiwać na znaczeniu w ciągu nadchodzących 3 lat: umiejętność przeprowadzania testów jednostkowych, wiedza dziedzinowa z zakresu telekomunikacji oraz znajomość języków obcych. Aczkolwiek ta ostatnia kompetencja ma relatywnie małe znaczenie z punktu widzenia pracodawców (relatywnie niska średnia ważność).

Programiści najlepiej oceniają własne umiejętności w zakresie: poprawy jakości i czytelności kodu (średnia samoocena: 4,4), rozwiązywania problemów oraz pracy zespołowej (średnia samoocena: 4,39 w obu przypadkach). Największa grupa spośród badanych programistów najchętniej poszerzyłaby wiedzę w zakresie cyberbezpieczeństwa, znajomości oprogramowania do kontroli wersji, wzorców projektowych, zaktualizowała wiadomości w zakresie optymalizacji pisania kodów, a także nabyła lub poszerzyła umiejętności w zakresie zwinnych metodyk pracy.

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

60% firm z sektora telekomunikacji zatrudnia przynajmniej jedną osobę na stanowisku developera/programisty.

22% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisko developera/programisty.

12% pracodawców zatrudniających developerów/programistów prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

93% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

98% pracowników pozytywnie ocenia swoje warunki pracy.

52% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **26%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

95% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 25. Bilans kompetencji dla stanowiska: developer (programista)

Kompetencje/rodzaj*		Ocena ważności/samoocena (średnia na 5-stopniowej skali)
		4,0 4,5 5,0
znajomość języków programowania (np. Python, C , C#, Java, JavaScript, Skala)	W	4,31 4,50
umiejętność kodowania w oparciu o *user story*	U	4,33 4,48
umiejętność przeprowadzania testów jednostkowych	U	4,31 4,43
umiejętność rozwiązywania problemów	U	4,39 4,43
umiejętność pisania kodu (programowania)	U	4,28 4,42
wiedza z zakresu cyberbezpieczeństwa (ochrona informacji)	W	4,30 4,41
wiedza dziedzinowa z zakresu telekomunikacji	W	4,26 4,40
znajomość architektury programowanego systemu lub usługi	W	4,35 4,40
umiejętność poprawy jakości i czytelności kodu	U	4,38 4,40
umiejętność korzystania z technologii umożliwiających pracę zdalną	U	4,30 4,37
wiedza z zakresu technologii chmurowych	W	4,35 4,36
znajomość Github lub podobnego oprogramowania do kontroli wersji	W	4,23 4,35
umiejętność pracy z wykorzystaniem metodyk zwinnych (agile, scrum)	U	4,26 4,35
analityczne myślenie	Ks	4,33 4,35
znajomość wzorców projektowych	W	4,29 4,34
chęć ciągłego rozwoju	Ks	4,33 4,38
kreatywność	Ks	4,32 4,33
wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)	W	4,14 4,32
łatwość adaptacji do szeroko pojętych zmian	Ks	4,28 4,30
umiejętność pracy w oparciu o dokumentację, wymagania i wytyczne projektu	U	4,29 4,32
skuteczne komunikowanie się	Ks	4,29 4,32
znajomość zwinnych metodyk pracy (agile, scrum)	W	4,19 4,27
umiejętność pracy zespołowej	U	4,27 4,39
znajomość języków obcych – szczególnie angielskiego	W	4,24 4,25
znajomość najbardziej aktualnych i optymalnych sposobów pisania kodu	**W**	4,16 4,27

Pracodawca:

- trudno pozyskać na rynku pracy
- *hot skills* znaczenie wzrośnie

Pracownik:

- samoocena
- kompetencja – kompetencja, którą chce rozwijać

* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 247) i badanie ilościowe pracowników (n = 159), II edycja.

Project manager

Głównymi zadaniami specjalisty na tym stanowisku są: dbanie o wyniki projektu (operacyjnego, finansowego), wdrażanie odpowiedniego sposobu realizacji do konkretnych projektów (z uwzględnieniem zasobów ludzkich, technologicznych), tworzenie kosztorysów projektów we współpracy z działami pozyskania klienta, utrzymywanie kontaktu z interesariuszami ze strony zamawiającego, pomoc w przeprowadzaniu procesów rekrutacyjnych.

Kompetencje trudne do pozyskania dla stanowiska project manager skupiają się głównie na zarządzaniu projektami oraz zespołami, a także są to kwestie związane z kosztorysowaniem czy pracą pod wpływem stresu.

Obecnie w profilu kompetencyjnym project managera nie występują kompetencje, które można by uznać za *hot skills*, natomiast kompetencje zyskujące na znaczeniu to wiedza dziedzinowa z zakresu telekomunikacji i znajomość wiodących technologii w branży. Warto dodać, że przedsiębiorcy z branży poproszeni o odniesienie się do kompetencji jaką jest umiejętność budowania zespołu – zdefiniowaną przez ekspertów branżowych biorących udział w badaniach jakościowych jako jeszcze niezbyt istotną, ale z perspektywą wzrostu znaczenia w ciągu nadchodzących 3 lat – podzielili odczucia ekspertów. Niemal 63% przedsiębiorców widzi szansę na wzrost jej znaczenia w kontekście analizowanego profilu.

Project managerowie najlepiej oceniają własną: znajomość wiodących technologii w branży (średnia samoocena: 4,46), wiedzę dziedzinową z zakresu telekomunikacji (średnia samoocena: 4,43) oraz umiejętność prowadzenia negocjacji (średnia samoocena: 4,39).

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

68% firm z sektora telekomunikacji zatrudnia przynajmniej jedną osobę na stanowisku project managera.

10% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku project managera.

9% pracodawców zatrudniających project managerów prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

98% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

99% pracowników pozytywnie ocenia swoje warunki pracy.

63% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **30%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

74% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 26. Bilans kompetencji dla stanowiska: project manager

Kompetencje/rodzaj*		Ocena ważności/samoocena (średnia na 5-stopniowej skali)
		4,0 4,5 5,0
umiejętność pracy pod wpływem stresu	W	4,30 4,50
umiejętność tworzenia kosztorysów projektów	U	4,27 4,46
znajomość wiodących technologii w branży ⬆	U	4,44 4,46
umiejętność zarządzania budżetem zespołu	U	4,37 4,44
umiejętność pracy zespołowej	U	4,34 4,44
wiedza z zakresu zarządzania	W	4,21 4,43
wiedza dziedzinowa z zakresu telekomunikacji ⬆	W	4,43 4,43
umiejętność pracy pod presją czasu	W	4,34 4,43
znajomość procesów biznesowych	U	4,24 4,42
umiejętność prowadzenia negocjacji	U	4,39 4,42
umiejętność motywowania pracowników	U	4,24 4,42
analityczne myślenie	W	4,38 4,42
umiejętność samodzielnego rozwiązywania problemów	W	4,26 4,40
chęć ciągłego rozwoju	U	4,29 4,40
umiejętność tworzenia strategii realizacji projektów	Ks	4,34 4,39
umiejętność efektywnego zarządzania zespołem (w szczególności w sposób zdalny)	Ks	4,36 4,37
znajomość zwinnych metodyk pracy (agile, scrum)	Ks	4,26 4,35
umiejętność rozdzielania zadań zgodnie z umiejętnościami konkretnego działu, zespołu, pracownika	W	4,29 4,35
odpowiedzialność	Ks	4,35 4,37
wysoki poziom komunikacji interpersonalnej	Ks	4,30 4,35
znajomość języków obcych – szczególnie angielskiego	U	4,21 4,33

Pracodawca:

● trudno pozyskać na rynku pracy

hot skills ⬆ znaczenie wzrośnie

Pracownik:

■ samoocena

kompetencja – kompetencja, którą chce rozwijać

* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 200) i badanie ilościowe pracowników (n = 136), II edycja.

Quality assurance

Głównymi zadaniami specjalisty na tym stanowisku są: przeprowadzanie testów manualnych i automatycznych, wyszukiwanie błędów w działaniu systemu, programu, usługi, poprawa projektowanych systemów i usług pod względem użyteczności, raportowanie błędów do przełożonych.

Quality assurance to stanowisko, dla którego jest relatywnie dużo kompetencji trudno dostępnych. Z jednej strony, jest to wiedza odnosząca się do architektury programowanego systemu, znajomość metodyk zwinnych czy języków programowania. Z drugiej, są to umiejętności odnoszące się do przeprowadzania testów jednostkowych czy tworzenia rekomendacji, które będą pomocne w naprawianiu błędów systemu czy usługi. Wśród trudno dostępnych są kompetencje, które – w opinii pracodawców – są najważniejsze dla wykonywania zadań na stanowisku QA.

O ile w profilu nie ma kompetencji, które przy przyjętych założeniach mogłyby zostać uznane za wzrostowe w perspektywie 3 lat, to można wyróżnić jedną kompetencję, której znaczenie już teraz szybko rośnie – wiedzę z zakresu UX.

Badani pracownicy na stanowiskach quality assurance najlepiej oceniają własną cierpliwość (średnia samoocena: 4,56), chęci ciągłego rozwoju (średnia samoocena: 4,41), umiejętność korzystania z technologii umożliwiających pracę zdalną oraz rzetelność (średnia samoocena: 4,39 w obu przypadkach).

Kompetencje, które pracownicy chcieliby rozwijać, to głównie te, które pojawiły się w ostatnim czasie, np. znajomość metodyki scrum, agile czy wiedza z zakresu UX.

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

43% firm z sektora telekomunikacji zatrudnia przynajmniej jedną osobę na stanowisku quality assurance.

7% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku quality assurance.

7% pracodawców zatrudniających quality assurance prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

95% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

99% pracowników pozytywnie ocenia swoje warunki pracy.

65% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **27%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

90% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 27. Bilans kompetencji dla stanowiska: quality assurance

Kompetencje/rodzaj*		Ocena ważności/samoocena (średnia na 5-stopniowej skali)
		4,0 4,5 5,0
umiejętność przeprowadzania testów jednostkowych	U	4,26 4,55
znajomość architektury programowanego systemu lub usługi	W	4,29 4,52
umiejętność identyfikacji błędów w działaniu systemu, programu, usługi	U	4,24 4,50
umiejętność korzystania z technologii pracy zdalnej	U	4,39 4,50
chęć ciągłego rozwoju	Ks	4,41 4,50
znajomość zwinnych metodyk pracy (agile, scrum)	W	4,09 4,49
znajomość języków programowania (np. Python, Selenium)	W	4,03 4,48
umiejętność tworzenia rekomendacji w celu naprawy błędów systemu, programu, usługi	U	4,20 4,46
umiejętność pracy zespołowej	U	4,34 4,44
umiejętność przeprowadzania/pisania testów automatycznych	U	4,22 4,43
dokładność	Ks	4,32 4,43
umiejętność pracy z wykorzystaniem metodyk zwinnych (agile, scrum)	U	4,30 4,42
wiedza dziedzinowa z zakresu telekomunikacji	W	4,22 4,41
rzetelność	Ks	4,39 4,41
wiedza z zakresu User Experience (UX)	W	4,11 4,40
analityczne myślenie	Ks	4,31 4,40
wiedza z zakresu technologii chmurowych	W	4,37 4,38
znajomość języków obcych – szczególnie angielskiego	W	4,21 4,38
wysoki poziom komunikacji interpersonalnej	Ks	4,32 4,38
umiejętność przeprowadzania testów manualnych	U	4,34 4,37
umiejętność poprawy jakości i czytelności kodu	U	4,33 4,37
cierpliwość	Ks	4,37 4,56

Pracodawca:
- trudno pozyskać na rynku pracy
- *hot skills* znaczenie wzrośnie

Pracownik:
- samoocena
- kompetencja – kompetencja, którą chce rozwijać

* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 164) i badanie ilościowe pracowników (n = 134), II edycja.

CISO (chief information security officer)

Głównymi zadaniami specjalisty na tym stanowisku są: zarządzanie bezpieczeństwem aktywów firmowych, tworzenie strategii bezpieczeństwa fizycznego, bezpieczeństwa informacji i bezpieczeństwa produktów cyfrowych (systemów, programów usług), przyporządkowywanie i rozdzielanie zadań dla działów, konkretnych zespołów, ciągła współpraca z zespołem w celu weryfikacji bieżących problemów, wspieranie realizacji celów biznesowych.

Umiejętność projektowania strategii bezpieczeństwa fizycznego (np. dostęp do budynków, dokumentów, BHP) to kompetencja najważniejsza z punktu widzenia pracodawców, jeżeli chodzi o wykonywanie zadań zawodowych CISO, która jest równocześnie trudna do pozyskania na rynku. Pozostałe dwie trudno dostępne są relatywnie mniej ważne.

Kompetencjami, które uznać można za *hot skills*, są: wiedza z zakresu technologii komputerowych oraz wiedza z zakresu bezpieczeństwa informacji. Ostatnia wymieniona należy także do kompetencji określonych jako wzrostowe w perspektywie najbliższych 3 lat.

W przypadku samooceny pracowników najlepiej postrzeganymi aspektami były: wiedza z zakresu bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych) i wiedza z zakresu bezpieczeństwa fizycznego (np. dostęp do budynków, dokumentów, BHP) (średnia: 4,82 w obu przypadkach) oraz umiejętność zarządzania zespołem (w szczególności w sposób zdalny) i charyzma (średnia: 4,73 w obu przypadkach). Mimo wysokiej samooceny w kontekście wiedzy z zakresu bezpieczeństwa informacji, badani pracownicy chcieliby rozwijać się w tym zakresie.

Relatywnie niewielka grupa oceniających każe traktować te dane z dużą dozą ostrożności.

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

8% firm z sektora cyberbezpieczeństwa zatrudnia przynajmniej jedną osobę na stanowisku CISO.

2% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku CISO.

8% pracodawców zatrudniających CISO prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

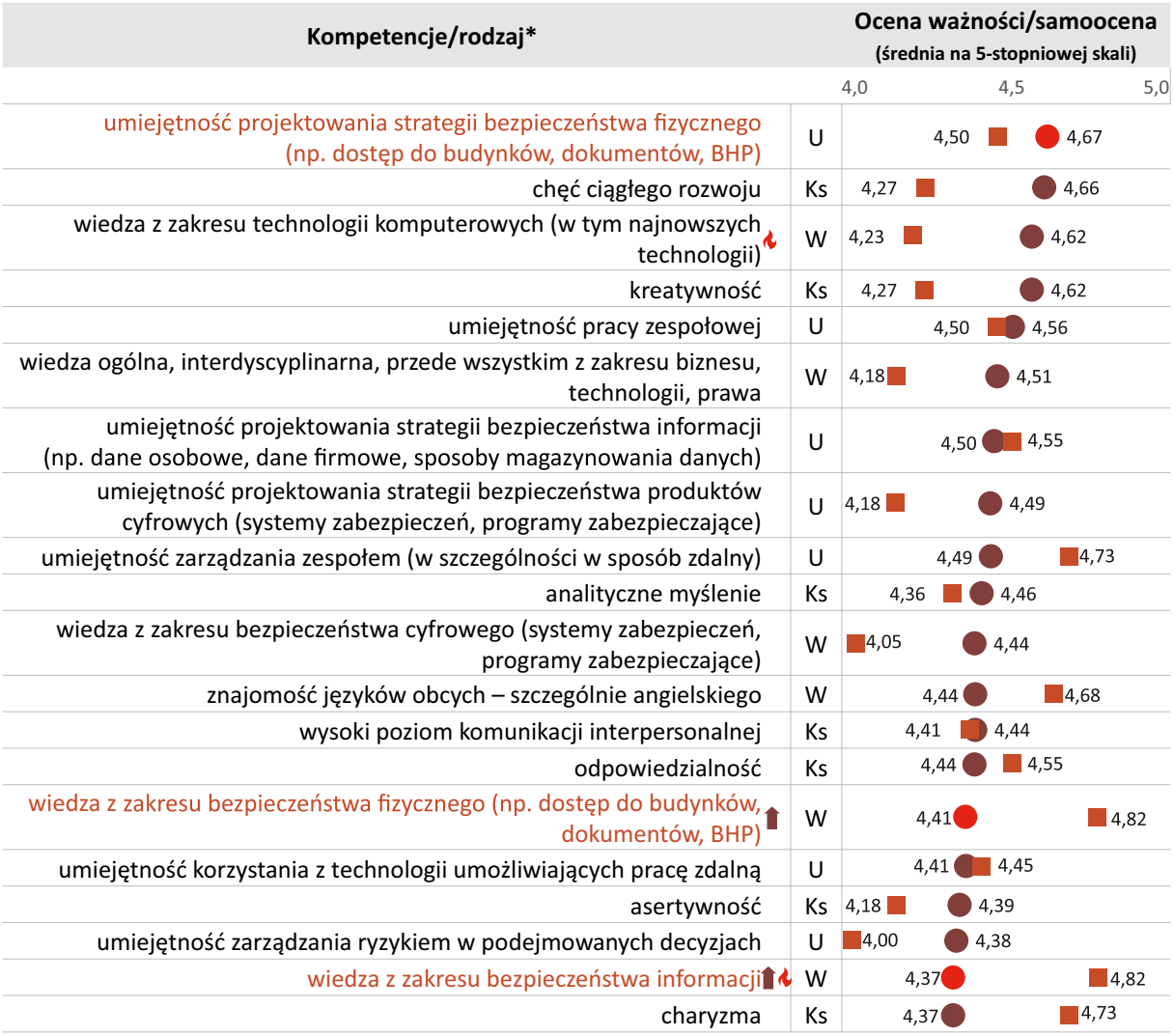
100% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

91% pracowników pozytywnie ocenia swoje warunki pracy.

73% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **41%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

77% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 28. Bilans kompetencji dla stanowiska: CISO



* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 41) i badanie ilościowe pracowników (n = 22), II edycja.

Audytor bezpieczeństwa

Głównymi zadaniami specjalisty na tym stanowisku są: prowadzenie audytów wewnątrz- i zewnątrzfirmowych w oparciu o standardy i normy bezpieczeństwa, przeprowadzanie oceny zgodności firmy/systemu/produktu/usługi z konkretnymi standardami i normami bezpieczeństwa, sporządzanie dokumentacji poaudytowej, formułowanie rekomendacji dotyczących poprawy bezpieczeństwa.

Obecnie w profilu kompetencyjnym audytora bezpieczeństwa nie występują kompetencje, które można by uznać za *hot skills*, natomiast kompetencje zyskujące na znaczeniu to wiedza z zakresu: prawa i aktualnych regulacji prawnych, bezpieczeństwa fizycznego i cyfrowego czy technologii komputerowych, ale także chęć rozwoju i niezależność. Część z tych kompetencji jest obecnie trudna – w opinii pracodawców – do pozyskania na rynku pracy.

Badani audytorzy bezpieczeństwa najlepiej oceniają własną niezależność (średnia samoocena: 4,58) oraz wysoki poziom komunikacji interpersonalnej (średnia samoocena: 4,53).

Relatywnie niewielka grupa oceniających każe traktować te dane z dużą dozą ostrożności.

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

8% firm z sektora cyberbezpieczeństwa zatrudnia przynajmniej jedną osobę na stanowisku audytora bezpieczeństwa.

3% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku audytora bezpieczeństwa.

13% pracodawców zatrudniających audytora bezpieczeństwa prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

100% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

100% pracowników pozytywnie ocenia swoje warunki pracy.

58% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **26%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

95% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 29. Bilans kompetencji dla stanowiska: audytor bezpieczeństwa

Kompetencje/rodzaj*		Ocena ważności/samoocena (średnia na 5-stopniowej skali)
		4,0 4,5 5,0
umiejętność identyfikacji i analizy ryzyka w konkretnych sposobach zabezpieczenia systemów, produktów, usług	U	4,21 4,66
wiedza z zakresu bezpieczeństwa fizycznego (np. dostęp do budynków, dokumentów, BHP) ⬆	W	4,44 4,51
niezależność ⬆	Ks	4,26 4,49
profesjonalizm	Ks	4,49 4,58
wiedza z zakresu bezpieczeństwa informacji	W	4,42 4,46
wiedza z zakresu technologii komputerowych (w tym najnowszych technologii) ⬆	W	4,21 4,46
umiejętność sporządzania zrozumiałych rekomendacji dla podmiotów, w których prowadzony jest audyt	U	4,21 4,46
wiedza z zakresu prawa i aktualnych regulacji prawnych ⬆	W	4,16 4,43
umiejętność oceny firm, systemów, produktów, usług w oparciu o konkretne normy i standardy	U	4,32 4,43
umiejętność weryfikacji podatności systemów, produktów, usług	U	4,17 4,43
wiedza z zakresu technologii chmurowych	W	4,32 4,40
znajomość języków obcych – szczególnie angielskiego	W	4,28 4,40
rzetelność	Ks	4,35 4,37
wiedza ogólna, interdyscyplinarna, przede wszystkim z zakresu biznesu, technologii, psychologii	W	4,00 4,34
wysoki poziom komunikacji interpersonalnej	Ks	4,34 4,53
chęć ciągłego rozwoju ⬆	Ks	4,32 4,34
wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające) ⬆	W	4,31 4,33
obiektywizm	Ks	4,21 4,31
asertywność	Ks	4,17 4,37

Pracodawca:
- ● trudno pozyskać na rynku pracy
- *hot skills* ⬆ znaczenie wzrośnie

Pracownik:
- ■ samoocena
- kompetencja – kompetencja, którą chce rozwijać

* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 35) i badanie ilościowe pracowników (n = 19), II edycja.

Architekt ds. bezpieczeństwa

Głównymi zadaniami specjalisty na tym stanowisku są: tworzenie architektury systemów bezpieczeństwa, zarządzanie systemami bezpieczeństwa, tworzenie zabezpieczeń dla systemów, programów, usług, zarządzanie mniejszymi etapami w projektowaniu zabezpieczeń, wybór najbardziej efektywnej drogi do uzyskania rozwiązania problemu, zbieranie sugestii i wniosków od członków zespołu.

Wśród kompetencji z profilu architekta ds. bezpieczeństwa należy wyróżnić takie, które są relatywnie ważniejsze, jednocześnie trudne do pozyskania i przewiduje się, że ich znaczenie wzrośnie w perspektywie 3 lat. Są to: wiedza z zakresu technologii komputerowych, umiejętność projektowania architektury systemów bezpieczeństwa i wiedza z zakresu systemów operacyjnych. Umiejętność przewidywania, w jaki sposób może dojść do ataku, a także wiedza z zakresu technologii komputerowych to kompetencje postrzegane jako *hot*.

Architekci ds. bezpieczeństwa najlepiej oceniają poziom własnej wiedzy z zakresu technologii chmurowych (średnia samoocena: 4,49), odpowiedzialność (średnia samoocena: 4,46) oraz wiedzę z zakresu działania sieci komputerowych i urządzeń sieciowych (średnia samoocena: 4,41).

Relatywnie niewielka grupa oceniających każe traktować te dane z dużą dozą ostrożności.

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

8% firm z sektora cyberbezpieczeństwa zatrudnia przynajmniej jedną osobę na stanowisku architekta ds. bezpieczeństwa.

3% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku architekt ds. bezpieczeństwa.

13% pracodawców zatrudniających architekta ds. bezpieczeństwa prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

95% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

100% pracowników pozytywnie ocenia swoje warunki pracy.

80% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **37%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

90% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 30. Bilans kompetencji dla stanowiska: architekt ds. bezpieczeństwa

Kompetencje/rodzaj*		Ocena ważności/samoocena (średnia na 5-stopniowej skali)
		4,0 4,5 5,0
chęć ciągłego rozwoju ⬆	Ks	4,26 4,69
umiejętność zarządzania systemami bezpieczeństwa	U	4,42 4,64
umiejętność korzystania z technologii umożliwiających pracę zdalną	U	4,42 4,62
wiedza z zakresu technologii komputerowych (w tym najnowszych technologii) ⬆🔥	W	4,37 4,51
znajomość języków obcych – szczególnie angielskiego	W	4,26 4,51
umiejętność projektowania architektury systemów bezpieczeństwa ⬆	U	4,37 4,51
wiedza z zakresu systemów operacyjnych (w tym systemów plików i zasad ich działania) ⬆	W	4,44 4,49
wiedza z zakresu technologii chmurowych	W	4,49 4,61
umiejętność wyszukiwania podatności systemów, programów, usług	U	4,26 4,49
kreatywność ⬆	Ks	4,42 4,49
umiejętność przewidywania, w jaki sposób może dojść do ataku na dany system, program, usługę ⬆🔥	U	4,26 4,46
umiejętność tworzenia zabezpieczeń dla systemów, programów, usług	U	4,32 4,46
odpowiedzialność	Ks	4,46 4,58
wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające) ⬆	W	4,21 4,44
znajomość systemów opartych o architekturę klient–serwer	W	4,32 4,44
wiedza z zakresu działania sieci komputerowych i urządzeń sieciowych	W	4,41 4,53
wysoki poziom komunikacji interpersonalnej	Ks	4,26 4,41
wiedza (przynajmniej podstawowa) z zakresu psychologii	W	4,32 4,36
wiedza (przynajmniej podstawowa) z zakresu prawa i aktualnych regulacji prawnych	W	4,33 4,37
umiejętność pracy zespołowej	U	4,33 4,47
umiejętność zarządzania zespołem (w szczególności w sposób zdalny)	U	4,31 4,42

Pracodawca:

● trudno pozyskać na rynku pracy

🔥 *hot skills* ⬆ znaczenie wzrośnie

Pracownik:

■ samoocena

kompetencja – kompetencja, którą chce rozwijać

* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 39) i badanie ilościowe pracowników (n = 19), II edycja.

Penetration tester

Głównymi zadaniami specjalisty na tym stanowisku są: pozorowanie faktycznych ataków cyfrowych mających na celu kradzież informacji, sprawdzenie podatności systemu, testowanie dostępu do programów, usług, danych.

W przypadku tego stanowiska, ze względu na jego specyfikę, prawie wszystkie kompetencje określone w profilu są trudne do pozyskania. Spośród TOP10 kompetencji najważniejszych dla wykonywania zadań zawodowych na stanowisku pen-testera aż siedem kompetencji ma potencjał wzrostowy – pracodawcy wskazali je jako te, których znaczenie będzie rosnąć w najbliższym czasie. Są to kompetencje związane z posiadaniem wiedzy nt. bezpieczeństwa cyfrowego bądź fizycznego, umiejętności – planowania strategii i prowadzenia ataków cyfrowych, ale także umiejętności: posługiwania się socjotechnikami, wywierania wpływu na ludzi czy odwaga. W profilu odnotowano jedną kompetencję, którą określić można jako *hot skill*: wiedzę z zakresu bezpieczeństwa informacji.

W przypadku samooceny pracowników najlepiej ocenianymi aspektami były: znajomość norm prawnych w zakresie pen-testów i odpowiedzialności pen-testera (średnia samoocena: 4,74), umiejętność zbierania informacji oraz weryfikacji ich rzetelności (średnia samoocena: 4,68) oraz wiedza z zakresu systemów operacyjnych (w tym systemów plików i zasad ich działania) (średnia samoocena: 4,68).

Relatywnie niewielka grupa oceniających każe traktować te dane z dużą dozą ostrożności.

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

7% firm z sektora cyberbezpieczeństwa zatrudnia przynajmniej jedną osobę na stanowisku penetration tester.

1% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku penetration tester.

7% pracodawców zatrudniających penetration testerów prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

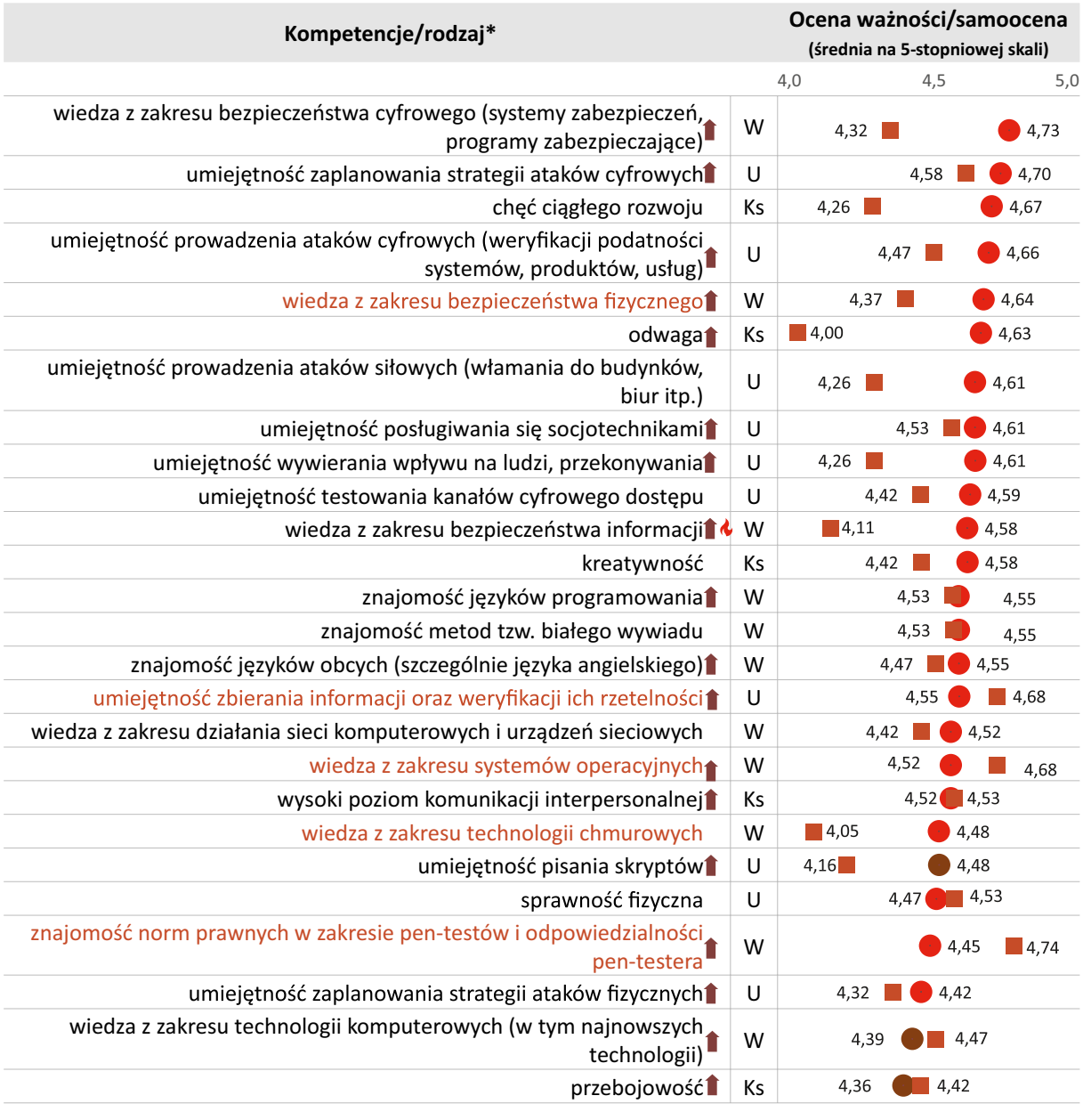
84% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

95% pracowników pozytywnie ocenia swoje warunki pracy.

74% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **42%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

95% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 31. Bilans kompetencji dla stanowiska: penetration tester



* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 33) i badanie ilościowe pracowników (n = 19), II edycja.

Koordynator SOC (security operation center)

Głównymi zadaniami specjalisty na tym stanowisku są: monitorowanie systemów w celu wyszukiwania potencjalnych incydentów, koordynacja zespołu SOC, w tym monitorowanie w trybie ciągłym poziomu cyberbezpieczeństwa, obsługiwanie incydentów cyberataków, uruchamianie procesów odtwarzania awaryjnego (lub innych zapewniających ciągłość działania systemu), tworzenie dokumentacji z incydentów, wdrażanie, rozwijanie i udoskonalanie standardów cyberbezpieczeństwa.

W przypadku tego stanowiska relatywnie niewiele kompetencji zostało uznanych za trudno dostępne. Kompetencje zyskujące na znaczeniu to przede wszystkim umiejętności takie jak blokowanie cyberataków i zagrożeń, przywracania sprawności zaatakowanych systemów czy programów, monitorowania systemów i tworzenia raportów dot. stanu cyberbezpieczeństwa, podstawowej analizy kodów czy adaptacji do zmian. Spośród nich jedna – wiedza z zakresu blokowania zagrożeń – to równocześnie kompetencja *hot*.

W przypadku samooceny pracowników najlepiej ocenianymi aspektami były: umiejętność podstawowej analizy kodu pod względem potencjalnych zagrożeń (średnia samoocena: 5,0), chęć ciągłego rozwoju (średnia samoocena: 4,83), ale także umiejętność pracy w systemie zmianowym, umiejętność pracy zespołowej oraz dokładność (średnie samooceny: 4,78 każda z umiejętności).

Relatywnie niewielka grupa oceniających każe traktować te dane z dużą dozą ostrożności.

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

68% firm z sektora cyberbezpieczeństwa zatrudnia przynajmniej jedną osobę na stanowisku koordynator SOC.

24% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku koordynator SOC.

9% pracodawców zatrudniających koordynatorów SOC prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

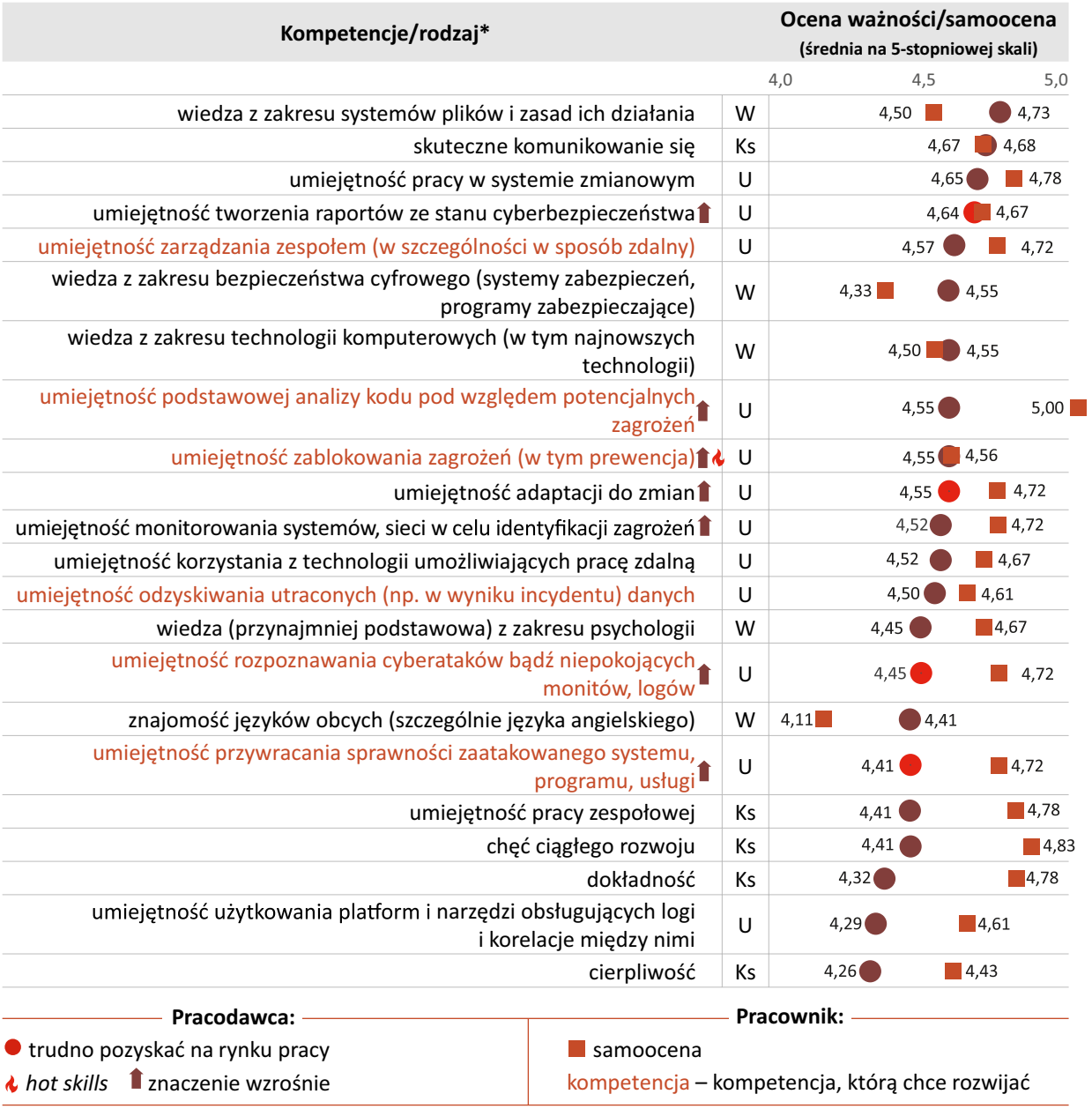
100% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

100% pracowników pozytywnie ocenia swoje warunki pracy.

50% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **33%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

72% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 32. Bilans kompetencji dla stanowiska: koordynator SOC



* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 22) i badanie ilościowe pracowników (n = 18), II edycja.

Ekspert ds. bezpieczeństwa

Głównymi zadaniami specjalisty na tym stanowisku są: projektowanie zabezpieczeń dla systemów, sieci i urządzeń, wyszukiwanie elementów, które wymagają poprawy, obsługa systemów, sieci i urządzeń. Przydzielanie dostępu do konkretnych narzędzi, budynków, miejsc w budynku, dbanie o bezpieczne przekazywanie informacji wewnątrz- i zewnątrzfirmowych za pomocą e-maili, dysków sieciowych, programów i usług wykorzystywanych w firmie.

Większość z TOP10 kompetencji relatywnie ważniejszych dla wykonywania zadań zawodowych na tym stanowisku jest – w opinii pracodawców – obecnie trudna do pozyskania na rynku. Wśród nich są wiedza z zakresu technologii komputerowych, umiejętność obsługi platform bezpieczeństwa czy umiejętność rozpoznawania cyberataków bądź innych niepokojących incydentów, które równocześnie – wg przewidywań pracodawców – będą zyskiwać na znaczeniu w najbliższym czasie.

Badani eksperci ds. zabezpieczeń najlepiej oceniają własną: wiedzę z zakresu systemów operacyjnych (średnia samoocena: 4,59), umiejętność przekazywania informacji wewnątrz i na zewnątrz organizacji w bezpieczny sposób (średnia samoocena: 4,58) oraz wiedzę z zakresu działania sieci komputerowych i urządzeń sieciowych (średnia samoocena: 4,58). Wśród kompetencji trudno dostępnych są też takie, które pracownicy chcą przede wszystkim rozwijać. Są to: wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające), umiejętność rozpoznawania cyberataków bądź niepokojących incydentów oraz wiedza z zakresu systemów operacyjnych.

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

10% firm z sektora cyberbezpieczeństwa zatrudnia przynajmniej jedną osobę na stanowisku eksperta ds. bezpieczeństwa.

3% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku eksperta ds. bezpieczeństwa.

9% pracodawców zatrudniających eksperta ds. bezpieczeństwa prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

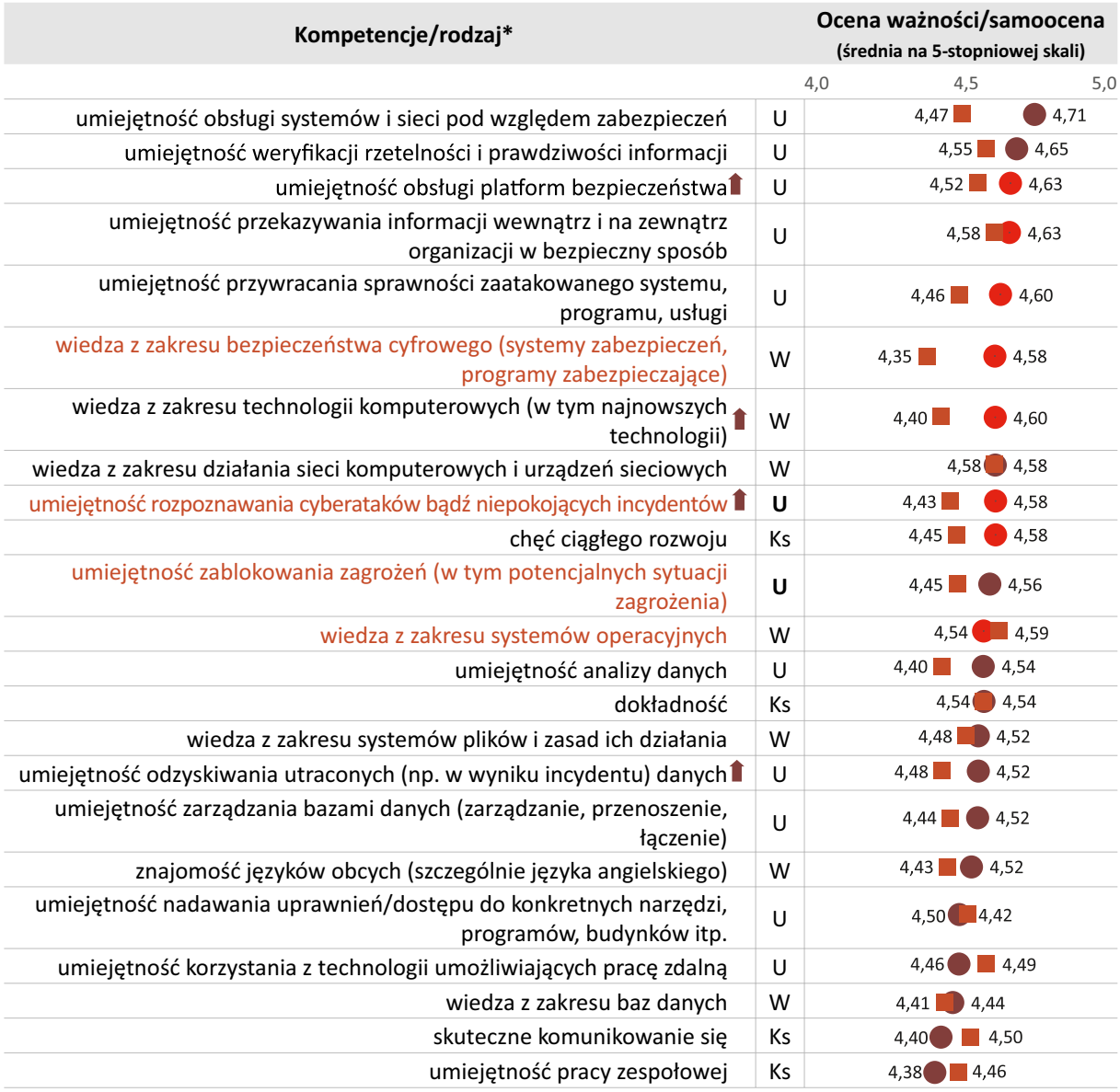
98% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

98% pracowników pozytywnie ocenia swoje warunki pracy.

46% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **38%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

90% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 33. Bilans kompetencji dla stanowiska: ekspert ds. bezpieczeństwa



* Rodzaj kompetencji: W – Wiedza – zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 48) i badanie ilościowe pracowników (n = 40), II edycja.

Dyrektor handlowy

Głównymi zadaniami specjalisty na tym stanowisku są: pozyskiwanie nowych kontraktów i projektów dla firmy, zarządzanie projektami, analizowanie wymagań projektów, prowadzenie negocjacji i rozmów z kontrahentami, tworzenie kosztorysów, ocena ofert konkurencji.

Odpowiedzialność i umiejętność prowadzenia rozmów z kontrahentami to kompetencje relatywnie najważniejsze z punktu widzenia pracodawców zatrudniających dyrektorów handlowych, które jednocześnie trudno pozyskać na rynku. Innymi trudnymi do pozyskania umiejętnościami są: analiza wymagań klienta oraz pozyskiwanie nowych zleceń dla firmy. Ostatnia z wymienionych umiejętności to umiejętność wskazywana przez pracowników wśród tych, które chcieliby rozwijać w najbliższym czasie.

W profilu nie zostały wyróżnione żadne kompetencje, które – wg przyjętych założeń – można by było określić jako wzrostowe, ani żadne o szybko rosnącym znaczeniu.

Dyrektorzy handlowi najlepiej oceniają własny poziom: odpowiedzialności (średnia samoocena: 4,42) oraz zorientowanie na cel (średnia samoocena: 4,41).

Kilka faktów wypływających od pracodawców zatrudniających na tym stanowisku:

57% firm z branży zatrudnia przynajmniej jedną osobę na stanowisku dyrektora handlowego.

13% pracodawców poszukujących pracowników w ciągu 12 miesięcy poprzedzających badanie najczęściej szukało osób do pracy na stanowisku dyrektora handlowego.

6% pracodawców zatrudniających dyrektora handlowego prognozuje wzrost zatrudnienia na tym stanowisku w ciągu 12 miesięcy po zakończeniu badania.

Kilka faktów wypływających od badanych pracowników zatrudnionych na tym stanowisku:

98% pracowników zamierza kontynuować pracę u obecnego pracodawcy w perspektywie najbliższych 12 miesięcy.

99% pracowników pozytywnie ocenia swoje warunki pracy.

53% pracowników rozwijało swoje kompetencje w ciągu 12 miesięcy poprzedzających badanie, a **34%** pracowników chciałoby rozwijać je w ciągu 12 miesięcy po zakończeniu badania.

60% pracowników ma wykształcenie zgodne z obecnym zatrudnieniem.

Wykres 34. Bilans kompetencji dla stanowiska: dyrektor handlowy

Kompetencje/rodzaj*		Ocena ważności/samoocena (średnia na 5-stopniowej skali)
		4,0 4,5 5,0
odpowiedzialność	Ks	4,42 4,55
wiedza produktowa	W	4,35 4,52
umiejętność prowadzenia rozmów z kontrahentami	U	4,30 4,52
orientacja na cel	Ks	4,41 4,51
umiejętność tworzenia kosztorysów	U	4,30 4,48
umiejętność oceny jakości ofert konkurencyjnych	U	4,30 4,45
wiedza z zakresu zarządzania (projektem, pracownikami)	W	4,22 4,41
umiejętność pozyskiwania nowych zleceń dla firmy	U	4,25 4,41
umiejętność analizy wymagań klienta	U	4,29 4,41
umiejętność motywowania zespołu	U	4,30 4,41
umiejętność przekazywania wytycznych do realizacji projektów	U	4,31 4,41
wysoki poziom komunikacji interpersonalnej	Ks	4,30 4,41
umiejętność prowadzenia negocjacji	U	4,28 4,39
umiejętność przygotowania strategii i planów sprzedaży	U	4,20 4,39
chęć ciągłego rozwoju	Ks	4,25 4,38
umiejętność zarządzania projektami	U	4,30 4,37
znajomość języków obcych	W	4,18 4,25
wiedza z zakresu prawa	W	4,20 4,25
umiejętność współpracy w zespole międzynarodowym	U	4,20 4,30

Pracodawca:

● trudno pozyskać na rynku pracy

hot skills ⬆ znaczenie wzrośnie

Pracownik:

■ samoocena

kompetencja – kompetencja, którą chce rozwijać

* Rodzaj kompetencji: W – Wiedza –zna i rozumie; U – Umiejętności – potrafi; Ks – Kompetencje społeczne – jest gotów do .

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców (n = 189) i badanie ilościowe pracowników (n = 130), II edycja.

8.3. Podsumowanie bilansu

Patrząc na profile poszczególnych stanowisk z sektora telekomunikacji i sektora cyberbezpieczeństwa, można stwierdzić, że procentowo największy udział kompetencji trudno dostępnych odnotowano na stanowisku: architekta systemów i QA w sektorze telekomunikacji oraz pen-testera i eksperta ds. bezpieczeństwa w sektorze cyberbezpieczeństwa[39]. W przypadku:

- architekta systemu dotyczyły one przede wszystkim elementów wiedzy (tj. wiedzy dziedzinowej z zakresu telekomunikacji, architektury systemów/informacji, technologii komputerowych, znajomości języków programowania i teorii metodyk zwinnych) i umiejętności (praca z metodykami zwinnymi, zarządzanie systemami wewnątrzfirmowymi, projektowanie spójnej i logicznej architektury systemu i dopasowanie metod/narzędzi do problemu), ale także kompetencji społecznej, jak analityczne myślenie;
- quality assurance to głównie elementy wiedzy (tj. znajomość architektury programowanego systemu, teorii zwinnych metodyk pracy, wiedza z zakresu UX, technologii chmurowych czy języków programowania), ale też umiejętności (tj. umiejętność przeprowadzenia testów jednostkowych, pisania/przeprowadzania testów automatycznych czy tworzenia rekomendacji w celu naprawy błędów systemu, programu i usługi);
- pen-testera to niemal wszystkie kompetencje z profilu (23 na 26 tworzących profil);
- eksperta ds. bezpieczeństwa to głównie elementy umiejętności (tj. obsługa platform bezpieczeństwa, przywracanie sprawności zaatakowanego systemu/programu/usługi, przekazywania informacji wewnątrz i na zewnątrz organizacji w bezpieczny sposób, rozpoznawania cyberataków lub niebezpiecznych incydentów), ale też wiedzy (tj. z zakresu bezpieczeństwa cyfrowego, technologii komputerowej czy systemów operacyjnych), a także kompetencji społecznej, jaką jest chęć ciągłego rozwoju.

Warto także zauważyć, że na stanowiskach z sektora cyberbezpieczeństwa odnotowano kompetencje, które w opiniach pracodawców zatrudniających osoby na tych stanowiskach będą zyskiwały na znaczeniu w ciągu 3 lat od realizacji badania, jednak pracodawcy byli powściągliwi w kwestii wskazywania kompetencji, których znaczenie już teraz szybko rośnie

[39] W kontekście stanowisk z sektora cyberbezpieczeństwa, ze względu na niskie liczebności próby wyniki należy traktować jako poglądowe.

albo wkrótce szybko wzrośnie (*hot skills*). Częściej niż co piąty pracodawca mający w swoim zespole pracownika na danym stanowisku wskazał jedynie kilka kompetencji – zostały one wypisane w Tabeli 14.

Tabela 14. Kompetencje *hot skills* i trudne do pozyskania (spośród pięciu najważniejszych dla wykonywania zadań na stanowisku)

Stanowisko (sektor*)	Hot skills	Kompetencje trudno dostępne spośród top5 najważniejszych w profilu
Architekt systemów (T)	brak	– wiedza dziedzinowa z zakresu telekomunikacji – umiejętność pracy z wykorzystaniem metodyk zwinnych (agile, scrum) – wiedza z obszaru architektury systemów, architektury informacji
Inżynier (T)	brak	– zapewnianie zabezpieczeń dostępu do urządzeń, narzędzi – umiejętność projektowania sieci przewodowych, bezprzewodowych
Developer (programista) (T)	– znajomość języków programowych	– znajomość języków programowych
Project manager (T)	brak	– umiejętność pracy pod wpływem stresu – umiejętność tworzenia kosztorysów projektów – znajomość wiodących technologii w branży – umiejętność pracy zespołowej
Quality assurance/tester (T)	– wiedza z zakresu UX	– umiejętność przeprowadzania testów jednostkowych – znajomość architektury programowanego systemu lub usługi
CISO (C)	– wiedza z zakresu bezpieczeństwa informacji – wiedza z zakresu technologii komputerowych	– umiejętność projektowania strategii bezpieczeństwa fizycznego
Audytor bezpieczeństwa (C)	brak	– wiedza z zakresu bezpieczeństwa fizycznego – wiedza z zakresu bezpieczeństwa informacji
Architekt ds. bezpieczeństwa (C)	– wiedza z zakresu technologii komputerowych (w tym najnowszych technologii) – umiejętność przewidywania, w jaki sposób może dojść do ataku na dany system, program, usługę	– wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)

Stanowisko (sektor*)	Hot skills	Kompetencje trudno dostępne spośród top5 najważniejszych w profilu
Penetration tester (C)	– wiedza z zakresu bezpieczeństwa informacji (np. dane osobowe, dane firmowe, sposoby magazynowania danych)	– wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające) – umiejętność zaplanowania strategii ataków cyfrowych – chęć ciągłego rozwoju – umiejętność prowadzenia ataków cyfrowych (weryfikacji podatności systemów, produktów, usług) – wiedza z zakresu bezpieczeństwa fizycznego
Koordynator SOC (C)	– umiejętność blokowania zagrożeń	– umiejętność tworzenia raportów ze stanu cyberbezpieczeństwa
Ekspert ds. bezpieczeństwa (C)	brak	– umiejętność obsługi platform bezpieczeństwa – umiejętność przekazywania informacji wewnątrz i na zewnątrz organizacji w bezpieczny sposób – umiejętność przywracania sprawności zaatakowanego systemu, programu, usługi
Dyrektor handlowy (U)	brak	– odpowiedzialność – umiejętność prowadzenia rozmów z kontrahentami

* Oznaczenie stanowisk: T – sektor telekomunikacji, C – sektor cyberbezpieczeństwa, U – stanowisko uniwersalne.

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, badanie ilościowe pracodawców, II edycja.

9. Rekomendacje

Poniższy rozdział przedstawia rekomendacje dla przedsiębiorców z branży telekomunikacyjnej i cyberbezpieczeństwa przygotowane na podstawie najważniejszych wniosków z badania. Przedstawiono w nim sposoby wdrażania podanych propozycji zmian, jak również podmioty odpowiedzialne za ich realizację.

Tabela 15. Rekomendacje

L.p.	Wniosek z badania	Rekomendacja opracowana na podstawie wniosku	Wdrożenie rekomendacji	Adresat rekomendacji
1	W najbliższych latach kluczowym zadaniem dla sektora cyberbezpieczeństwa będzie opracowanie zabezpieczeń i zidentyfikowanie podatności dla nowych technologii cyfrowych (np. AI, IoT).	Koniecznym będzie udzielenie wsparcia dla przedsiębiorstw w zakresie opracowania lub nabycia rozwiązań chroniących infrastrukturę. Należy podnieść jakość kształcenia specjalistów ds. cyberbezpieczeństwa, tak aby byli odpowiednio przygotowani do opracowywania i wdrażania zabezpieczeń. Poza rekomendacjami wprost kierowanymi do sektora cyberbezpieczeństwa, warto również zintensyfikować działania edukacyjne zorientowane na podniesienie świadomości społecznej o atakach w sieci poprzez organizację szkoleń i kampanii społecznych. Działania edukacyjne powinny być w szczególności kierowane do uczniów i uczennic szkół średnich, czyli osób młodych wchodzących na rynek pracy.	Za wdrożenie rekomendacji powinny być odpowiedzialne poniższe podmioty: – instytucje publiczne np. PARP – podmioty administracji rządowej, tj. Ministerstwo Edukacji i Nauki Podmioty, które powinny być włączone w proces wdrażania: – szkoły podstawowe i średnie, uniwersytety – organizacje pozarządowe	– przedsiębiorstwa – instytucje publiczne

L.p.	Wniosek z badania	Rekomendacja opracowana na podstawie wniosku	Wdrożenie rekomendacji	Adresat rekomendacji
2	Na rynku pracy obserwowalny jest deficyt specjalistów branżowych (w szczególności dotyczy to zawodów: developer (programista), inżynier, architekt systemów, architekt ds. bezpieczeństwa, audytor bezpieczeństwa, ekspert ds. bezpieczeństwa). Deficyt ten będzie pogłębiał się w przyszłości.	W celu zmniejszenia deficytu pracowników w kolejnych latach należy zintensyfikować działania zmierzające do promocji pracy w branży telekomunikacji i cyberbezpieczeństwa wśród uczniów i rodziców. Działania przede wszystkim powinny skupiać się na organizacji dni otwartych, stworzeniu lokalnych katalogów z listą przedsiębiorstw reprezentujących branżę telekomunikacji i cyberbezpieczeństwa gotowych do zaoferowania staży/praktyk, które zapewniają możliwość zatrudnienia po odbytym stażu. Ponadto, konieczne będzie podjęcie współpracy przedsiębiorstw z branży telekomunikacji i cyberbezpieczeństwa z instytucjami edukacyjnymi w celu wymiany informacji na temat aktualnego zapotrzebowania na konkretne kompetencje. Powinny zostać wprowadzone zmiany w systemie edukacji, tak aby klasy profilowane zbliżone do tematyki branży zapewniały specjalistyczną i aktualną edukację, dostosowaną do potrzeb rynkowych. Warto również zidentyfikować kierunki kształcenia, które są częściowo zbieżne tematycznie z zagadnieniami potrzebnymi w branży i kształtować w tej grupie kompetencje typowe dla branży telekomunikacji i cyberbezpieczeństwa.	Za wdrożenie rekomendacji powinny być odpowiedzialne poniższe podmioty: – instytucje publiczne np. PARP, – podmioty administracji rządowej, tj. Ministerstwo Edukacji i Nauki – szkoły podstawowe i średnie, uniwersytety Podmioty, które powinny być włączone w proces wdrażania: – organizacje pozarządowe – przedsiębiorstwa	– przedsiębiorstwa – instytucje publiczne

L.p.	Wniosek z badania	Rekomendacja opracowana na podstawie wniosku	Wdrożenie rekomendacji	Adresat rekomendacji
3	Problemem w branży jest widoczny odpływ specjalistów do zagranicznych firm (w tym praca świadczona zdalnie z Polski na rzecz firm zagranicznych).	Konieczne będzie wsparcie przedsiębiorstw poprzez udzielenie dofinansowania w ramach certyfikowanych szkoleń/kursów dla pracowników, tak aby podnieść atrakcyjność pracodawców dla obecnych i potencjalnych pracowników. Należy również wprowadzić zintegrowane działania promocyjne w zakresie pracy w branży. Kampanie promocyjne powinny być kierowane zarówno do uczniów, jak i rodziców. W przypadku łatwiejszego zatrudnienia pracowników pochodzących z innych krajów powinno się wdrożyć systemowe mechanizmy regulacyjne (tj. kwestia pozwolenia na pracę, spełnienie formalności wizowych).	Za wdrożenie rekomendacji powinny być odpowiedzialne poniższe podmioty: – podmioty administracji rządowej, tj. Ministerstwo Edukacji i Nauki, Ministerstwo Rodziny, Pracy i Polityki Społecznej – instytucje publiczne odpowiedzialne za wdrażanie programów wsparcia o zasięgu wojewódzkim, regionalnym Podmioty, które powinny być włączone w proces wdrażania: – instytucje publiczne, np. PARP – szkoły podstawowe i średnie, uniwersytety – organizacje pozarządowe	– przedsiębiorstwa z branży telekomunikacji i cyberbezpieczeństwa
4	Dynamiczny rozwój branży przyczynia się do szybkiej dezaktualizacji wiedzy. W związku z tym, pojawia się konieczność regularnych szkoleń pracowników.	Konieczne będzie ciągłe aktualizowanie programów nauczania oraz oczekiwanych efektów kształcenia na uczelniach tak, aby kompetencje, które są przekazywane w procesie edukacji, odpowiadały aktualnym zagadnieniom potrzebnym na rynku pracy. W związku z tym, należy wesprzeć współpracę przedsiębiorstw z sektora telekomunikacji z instytucjami edukacyjnymi w celu wymiany informacji na temat aktualnego zapotrzebowania na konkretne kompetencje.	Za wdrożenie rekomendacji powinny być odpowiedzialne poniższe podmioty: – przedsiębiorstwa Podmioty, które powinny być włączone w proces wdrażania: – firmy szkoleniowe – sektor edukacji (np. uniwersytety w ramach studiów podyplomowych)	– przedsiębiorstwa z branży telekomunikacji i cyberbezpieczeństwa – firmy szkoleniowe

L.p.	Wniosek z badania	Rekomendacja opracowana na podstawie wniosku	Wdrożenie rekomendacji	Adresat rekomendacji
5	Ważnym czynnikiem wpływającym na kształt kompetencji przyszłości dla wszystkich stanowisk w branży będzie również rozwój systemów generatywnej sztucznej inteligencji (AI).	Potrzebne będzie podjęcie działań ukierunkowanych na zmianę kompetencji, które będą zdobywać obecni i przyszli pracownicy z branży zarówno w trakcie edukacji (dla przyszłych pracowników), jak i na poziomie szkoleń i kursów firmowych (dla aktualnych pracowników). Należy położyć większy nacisk na rozwój kompetencji społecznych takich jak: umiejętność pracy zespołowej, pracy w zespołach interdyscyplinarnych i międzynarodowych, kreatywność, analityczny umysł, oraz na rozwój umiejętności tworzenia strategii, projektowania rozwiązań w oparciu o potrzeby klientów itp. Będą to bowiem kompetencje, które zyskają na znaczeniu i nie ulegną automatyzacji.	Za wdrożenie rekomendacji powinny być odpowiedzialne poniższe podmioty: – podmioty administracji rządowej, tj. Ministerstwo Edukacji i Nauki – sektor edukacji – przedsiębiorstwa Podmioty, które powinny być włączone w proces wdrażania: – firmy szkoleniowe	– instytucje publiczne – sektor edukacji – przedsiębiorstwa z branży telekomunikacji i cyberbezpieczeństwa
6	W perspektywie najbliższych 5 lat w branży nie pojawią się zupełnie nowe stanowiska. Zmianie ulegnie natomiast zakres zadań zawodowych wielu aktualnie występujących stanowisk (w tym kluczowych dla branży), a co za tym idzie zakres kompetencji, które będą musieli posiadać pracownicy.	Konieczne będzie podjęcie zmian w systemie edukacji, w oczekiwanych efektach kształcenia na uczelniach oraz na rynku szkoleniowym. Aby odpowiednio przygotować pracowników do zmieniającego się rynku pracy, należy skupić się na rozwijaniu kompetencji społecznych (tj. umiejętności pracy zespołowej, umiejętności pracy w zespołach interdyscyplinarnych i międzynarodowych, kreatywności, analitycznego umysłu) oraz rozwój kompetencji związanych z umiejętnościami: projektowania rozwiązań w oparciu o potrzeby klientów, tworzenia strategii, a także samego wykorzystania AI do realizacji codziennych zadań zawodowych. Będą to kompetencje, które zyskają na znaczeniu w porównaniu do umiejętności takich jak pisanie kodu programistycznego, bądź analiza incydentów bezpieczeństwa, które mogą zostać zautomatyzowane.	Za wdrożenie rekomendacji powinny być odpowiedzialne poniższe podmioty: – podmioty administracji rządowej, tj. Ministerstwo Edukacji i Nauki – sektor edukacji – firmy szkoleniowe – przedsiębiorstwa	– podmioty administracji rządowej, tj. Ministerstwo Edukacji i Nauki – sektor edukacji – firmy szkoleniowe – przedsiębiorstwa z branży

L.p.	Wniosek z badania	Rekomendacja opracowana na podstawie wniosku	Wdrożenie rekomendacji	Adresat rekomendacji
7	Następstwem pandemii COVID-19, które jest ciągle obserwowalne w branży, jest upowszechnienie się pracy w formie zdalnej lub hybrydowej.	Firmy będą musiały podjąć działania w celu standaryzacji procesów w ramach powszechnej obecności zjawiska świadczenia pracy w sposób zdalny lub hybrydowy. Potrzebne będzie wprowadzenie podziału zespołów na zespoły stacjonarne lub hybrydowe i w pełni zdalne. Rozdzielenie tych zespołów będzie konieczne z uwagi na potrzebę podziału obowiązujących zasad pracy, procedur, procesów oraz systemów oceny i systemów płacowych (podział zespołów pozwoli na efektywniejsze zarządzanie firmą).	Za wdrożenie rekomendacji powinny być odpowiedzialne poniższe podmioty: – przedsiębiorstwa	– przedsiębiorstwa z branży

Źródło: opracowanie własne na podstawie BBKL II dla branży telekomunikacji i cyberbezpieczeństwa, II edycja.

Spis wykresów i tabel

Wykresy

Tabele