PARP
Grupa PFR

Branżowy Bilans
Kapitału Ludzkiego II

# Branżowy Bilans Kapitału Ludzkiego II

# Branża telekomunikacji i cyberbezpieczeństwa

## Wybrane wyniki II edycji badań

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Społeczny

# Informacje o projekcie

## Nazwa projektu

Branżowy Bilans Kapitału Ludzkiego II
Branża telekomunikacji
i cyberbezpieczeństwa (II edycja)

## Główne cele projektu

- zwiększenie wiedzy na temat obecnego i przyszłego zapotrzebowania na kompetencje w branży telekomunikacji i cyberbezpieczeństwa
- określenie wyzwań dla branży (perspektywa 3 lat)

## Czas realizacji II edycji projektu

czerwiec 2022 r. – czerwiec 2023 r.

## Definicja branży
(w oparciu o sekcje PKD)

Telekomunikacja przewodowa (PKD J.61.1)
Telekomunikacja bezprzewodowa (PKD J.61.2)
Telekomunikacja satelitarna (PKD J.61.3)
Pozostała telekomunikacja (PKD J.61.9)
Cyberbezpieczeństwo (PKD J.62.03.Z)

# Metodologia

## Badania jakościowe
(czas realizacji: lipiec 2022 – listopad 2022)

20 wywiadów indywidualnych z pracodawcami

4 panele eksperckie (2 prospektywne i 2 kompetencyjne)

Badanie delphi z 43 ekspertami z branży

Panel podsumowujący z Sektorową Radą ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

## Badania ilościowe
(czas realizacji: luty 2023 - marzec 2023)

Badania sondażowe z pracodawcami z branży (n = 803) i pracownikami zatrudnionymi na kluczowych dla branży stanowiskach (n = 1011)

# Czynniki wpływające na branżę

## Czynniki zewnętrzne:

inflacja

kryzys energetyczny

pandemia COVID-19

wojna w Ukrainie

przerwane lub ograniczone łańcuchy dostaw

## Czynniki wewnętrzne*:

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

*oznaczenie sektorów, których dotyczy czynnik:
C - Cyberbezpieczeństwo, T- Telekomunikacja

Źródło: opracowanie własne na podstawie wyników badań: ilościowego pracodawców (n = 803) oraz jakościowego realizowanego w ramach projektu BBKLII w branży telekomunikacji i cyberbezpieczeństwa, edycja II.

# Wyzwania* w branży telekomunikacji i cyberbezpieczeństwa

## Zapewnienie bezpieczeństwa

- **53%** dostrzega potrzebę opracowywania zabezpieczeń i zidentyfikowanie podatności dla nowych rozwiązań/ technologii [C]

## Trudności kadrowe

- **52%** dostrzega trudność w zatrzymaniu specjalistów przed przejściem do firm zagranicznych [C: 62%, T: 50%]
- **47%** zwraca uwagę na problem znalezienia nowych pracowników z branży IT [C: 55% ,T: 46%]
- **46%** pracodawców widzi problem ze znalezieniem specjalistów z zakresu cyberbezpieczeństwa [C: 52%, T: 45%]

## Globalizacja

- **39%** pracodawców dostrzega potrzebę wzrostu konkurencyjności międzynarodowej [C: 36%, T: 40%].

## Dbałość o użytkownika

- **37%** pracodawców dostrzega potrzebę zwiększania dbałości o doświadczenie użytkownika [T]

---

* oznaczenie sektorów, których dotyczy wyzwanie: C - Cyberbezpieczeństwo, T- Telekomunikacja

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców (n = 803) realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Scenariusze przyszłości

W wyniku procesu badawczego, opracowano trzy scenariusze przyszłości przedstawiające strategie działania, które potencjalnie będą realizowane w przyszłości przez przedsiębiorstwa z branży w zależności od intensyfikacji lub osłabienia poszczególnych czynników oddziałujących na branżę.

## Scenariusz 1

### Aktywny rozwój wewnętrzny przedsiębiorstwa

Możliwa realizacja przez przedsiębiorstwa oferujące autorskie usługi lub produkty, które chcą rozwijać.

## Scenariusz 2

### Realizacja działań za pośrednictwem zewnętrznych kontraktorów

Możliwa realizacja przez przedsiębiorstwa oferujące usługi lub prowadzące projekty w konkretnej branży lub w kilku branżach dla wielu klientów.

## Scenariusz 3

### Czynna współpraca z jednostkami naukowymi

Możliwa realizacja zarówno przez przedsiębiorstwa oferujące własne usługi i/lub produkty, jak i te realizujące usługi lub projekty dla różnych firm.

Źródło: opracowanie własne na podstawie wyników badania jakościowego realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Scenariusze przyszłości

## Scenariusz 1
## Aktywny rozwój wewnętrzny przedsiębiorstwa

**Które firmy będą realizowały tę strategię?**

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

**W założeniu firmy realizujące tę strategię:**

- będą próbowały poradzić sobie z niedoborem specjalistów poprzez tworzenie autorskich programów stażowych lub bootcampów (obozów treningowych),
- aby obniżyć rotacje pracowników, 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,
- w kontekście współpracy z sektorem edukacji, będą podejmowały i współtworzyły inicjatywy tj. organizacja przestrzeni do podejmowania dyskusji, wymiany wniosków oraz przekazywania informacji o aktualnym zapotrzebowaniu na pracowników oraz na poszczególne kompetencje wśród pracodawców,
- będą dbać o kwestie społecznej odpowiedzialności biznesu oraz edukacji społeczeństwa.

Źródło: opracowanie własne na podstawie wyników badania jakościowego realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Scenariusze przyszłości

## 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.

**W założeniu firmy realizujące tę strategię:**

- będą rezygnowały z zatrudniania pracowników na stałe (szczególnie w oparciu o umowę o pracę), na rzecz pracowników kontraktowych,
- nie będą szczególnie zainteresowane dbałością o rozwój kompetencji pracowników ze względu na specyfikę zatrudniania pracowników; przedsiębiorcy będą oczekiwać od pracowników posiadania wszystkich niezbędnych kompetencji, które pozwolą na należytą realizację danego projektu,
- w kontekście współpracy z sektorem edukacji, będą uczestniczyć w różnych inicjatywach głównie w celu przekazania informacji na temat aktualnego zapotrzebowania na pracowników oraz kompetencje w branży, ale nie będą się mocno angażować,
- będą inwestowały w tworzenie własnych projektów mających na celu podniesienie ogólnej świadomości społecznej na temat cyberbezpieczeństwa lub zagrożeń związanych z nowymi technologiami cyfrowymi.

Źródło: opracowanie własne na podstawie wyników badania jakościowego realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Scenariusze przyszłości

## 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.

**W założeniu firmy realizujące tę strategię:**

- 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 (klasy patronackie, programy stypendialne),
- będą ukierunkowane na tworzenie zespołów stacjonarnych bądź hybrydowych ze względu na chęć integracji pracowników rekrutowanych w ramach programów stażowych i klas patronackich oraz potrzebę tworzenia środowiska przyjaznego przekazywaniu wiedzy nowym pracownikom przez obecnych już specjalistów.

Źródło: opracowanie własne na podstawie wyników badania jakościowego realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Branża wobec przyszłości

## Planowane przez przedsiębiorstwa zmiany w ciągu 3 lat następujących po badaniu:

**64%** podwyższy cenę usług

**47%** zwiększy nakłady na innowacyjność w firmie

**42%** zainwestuje lub zwiększy nakłady inwestycyjne w nowe technologie (uczenie maszynowe, sztuczna inteligencja) i nowe oprogramowanie

**39%** stworzy nowe usługi/produkty

**38%** zainwestuje lub zwiększy inwestowanie w rozwój umiejętności pracowników (szkolenia, kursy)

**36%** zautomatyzuje wybrane procesy w firmie

**32%** rozpocznie lub zintensyfikuje prace B+R w firmie samodzielnie lub we współpracy z jednostkami naukowymi

**29%** zaangażuje firmę lub zwiększy zaangażowanie firmy we współpracę ze szkołami bądź uczelniami w celu wykształcenia i zdobycia przyszłych pracowników

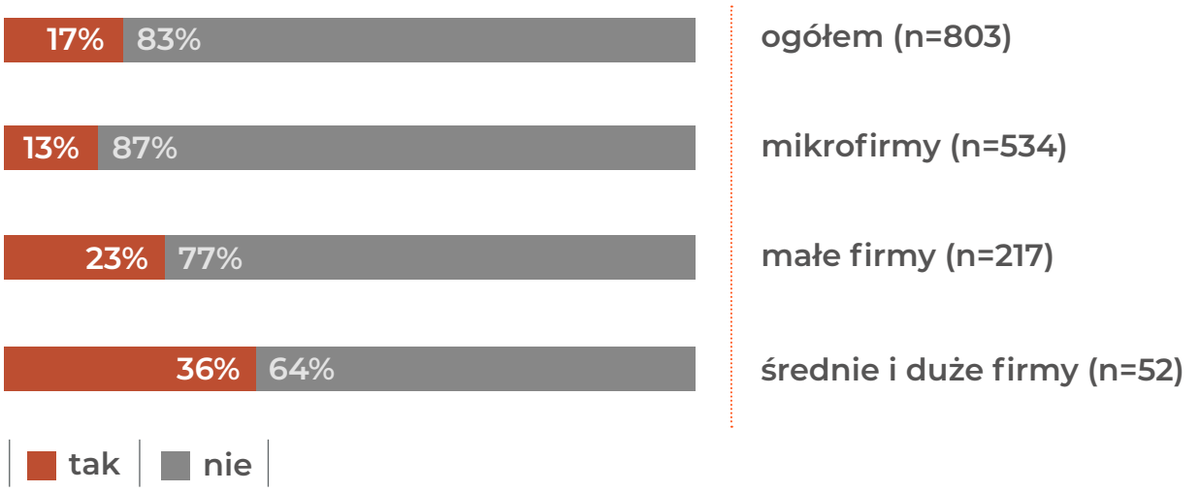
Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców (n = 803) realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Zapotrzebowanie na pracowników w branży

**17% firm z branży** w ciągu 12 miesięcy poprzedzających badanie **poszukiwało nowych osób do pracy**

Odsetek przedsiębiorców poszukujących pracowników rośnie wraz z wielkością firmy

## Fakt poszukiwania pracowników do firmy




**Najczęściej** poszukiwani byli:

Developer/ programista **22%**

Inżynier (niezależnie od specjalizacji) **22%**

Architekt systemów **13%**

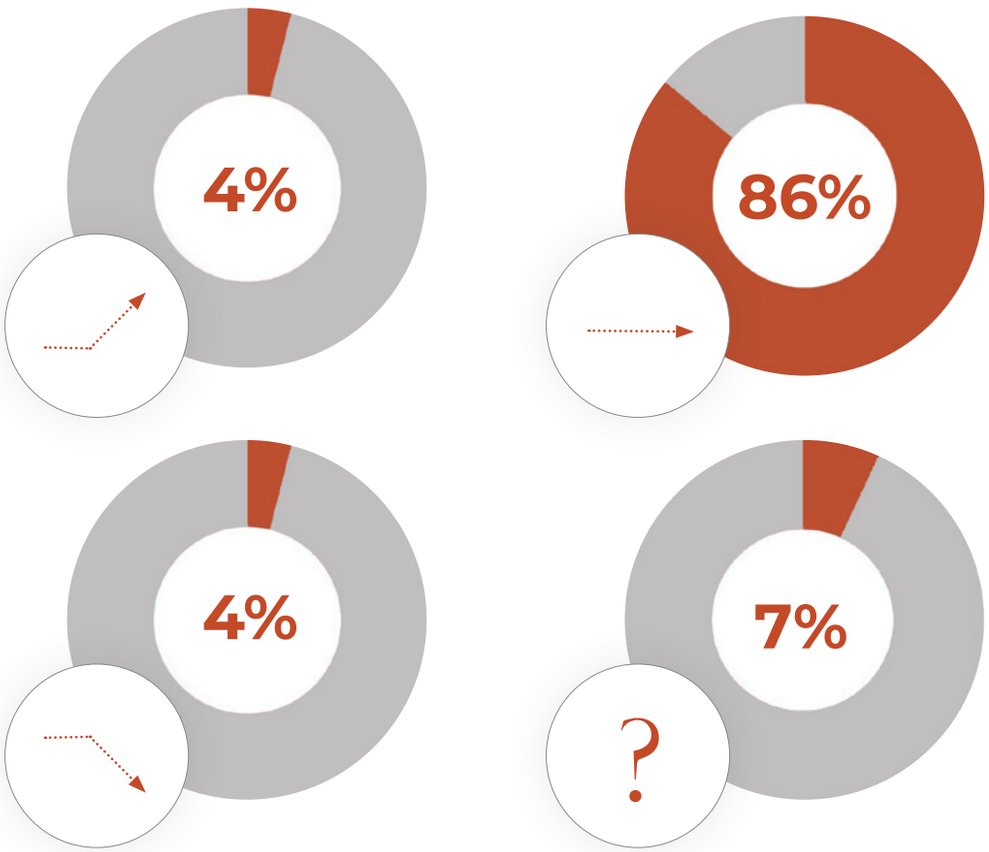
Dyrektor handlowy **13%**

Kierownik projektu **10%**

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców (n = 803) realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Przewidywane zmiany w zatrudnieniu

Niezależnie od sektora, **ponad 85% firm** z branży uważa, że w ciągu 12 miesięcy po badaniu **poziom zatrudnienia** w branży pozostanie **bez zmian**



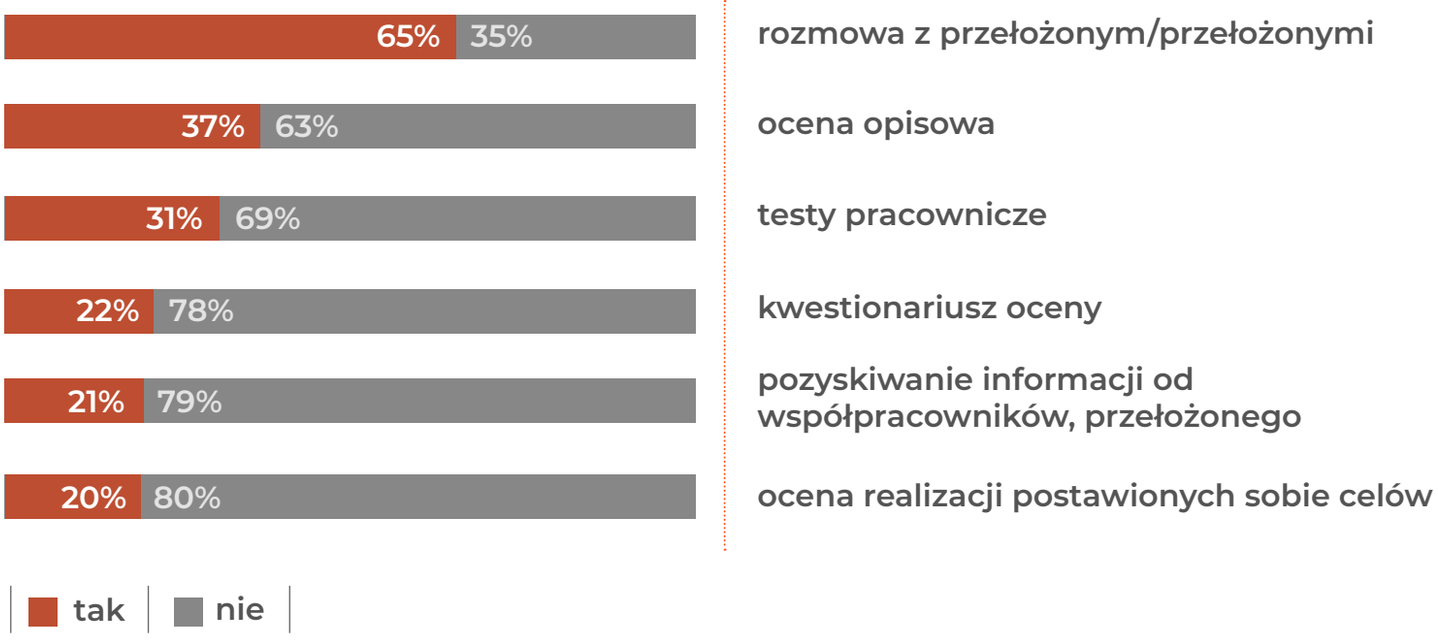

- **4%** zwiększy się
- **86%** pozostanie na tym samym poziomie
- **4%** zmniejszy się
- **7%** nie wiem/trudno powiedzieć

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców (n = 803) realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Ocena umiejętności pracowników

**56% pracowników** zatrudnionych na kluczowych stanowiskach jest **ocenianych** przez pracodawców **pod kątem umiejętności** jakich potrzebują, przy czym **co trzeci** oceniany jest **systematycznie** (co najmniej raz na rok)

## Metody oceny umiejętności pracowników



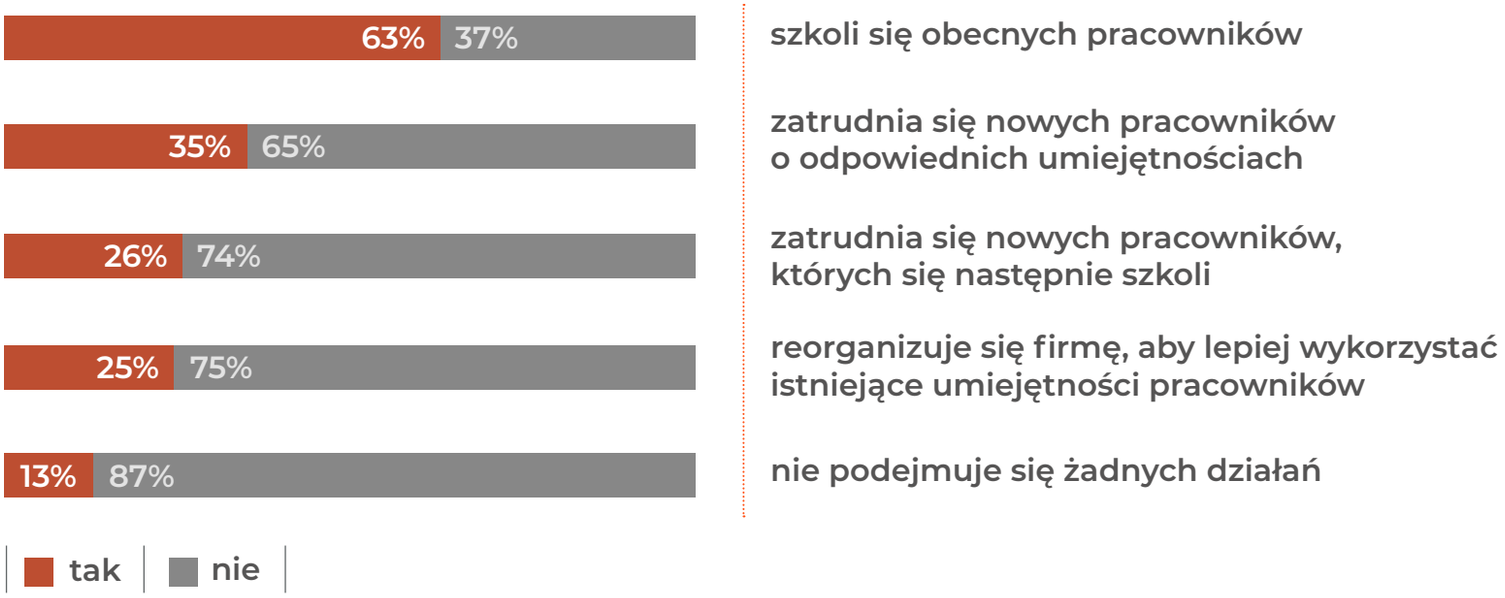

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracowników (n = 1011) realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Strategie działania pracodawców wobec deficytów kompetencyjnych

**59%** pracodawców ocenia, że kompetencje ich pracowników są w pełni zadawalające

**38%** pracodawców dostrzega potrzebę rozwoju kompetencji pracowników

## Działania podejmowane przez pracodawców w przypadku zidentyfikownia braku konkretnych umiejętności u pracowników




Źródło: opracowanie własne na podstawie wyników badania ilościowego pracodawców (n = 803) realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Bilans kompetencji

**Bilans kompetencji** to zestawienie ocen kluczowych kompetencji na poszczególnych stanowiskach w branży telekomunikacji i cyberbezpieczeństwa z perspektywy pracodawców i pracowników służące lepszemu zbilansowaniu rynku pracy 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 dla wykonywania obowiązków zawodowych,
- trudności znalezienia osoby, która posiada określoną kompetencję potrzebną do pracy na danym stanowisku,
- prognozy zmiany znaczenia tej kompetencji w ciągu najbliższych trzech lat.

W oparciu o opinie pracodawców wyróżniono tzw. hot skills, czyli umiejętności, których znaczenie rośnie, lub będzie szybko rosło w perspektywie najbliższych 3 lat.

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

# Bilans kompetencji

- Procentowo największy udział kompetencji trudno dostępnych odnotowano na stanowisku: architekta systemów i quality assurance w sektorze telekomunikacji oraz pen-testera i eksperta ds. bezpieczeństwa w sektorze cyberbezpieczeństwa*.

- Kompetencje hot skills – określone wg przyjętego założenia – występują przede wszystkim w sektorze cyberbezpieczeństwa*. W przypadku np.:

  - CISO to wiedza z zakresu bezpieczeństwa informacji oraz z zakresu technologii komputerowych,
  - architekta ds. bezpieczeństwa to wiedza z zakresu technologii komputerowych i umiejętności przewidywania, w jaki sposób mogło dojść do ataku na system, program czy usługę,
  - pen-testera to widza z zakresu bezpieczeństwa informacji (np. danych osobowych, danych firmowych, sposobów magazynowania danych),
  - koordynatora SOC to umiejętność blokowania zagrożeń.

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

Źródło: opracowanie własne na podstawie wyników badania ilościowego pracowników (n = 803) realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

# Kompetencje przyszłości

Kompetencje przyszłości, które – w opinii ekspertów branżowych wyrażonych w badaniach jakościowych – pojawią się w profilu kompetencyjnym danego stanowiska.

| Zawód | Kompetencje przyszłości |
|---|---|
| Architekt systemów | • wiedza z zakresu sztucznej inteligencji (AI), szczególnie machine learningu<br>• tworzenie systemów w oparciu o nowe metody realizacji (mikroserwisy, technologie chmurowe) |
| Developer/Programista | • wiedza z zakresu sztucznej inteligencji (AI), szczególnie machine learningu<br>• umiejętność wykorzystania narzędzi generatywnej AI do pisania kodu |
| Quality assurance/tester | • umiejętność pisania testów automatycznych dla oprogramowania napisanego w systemach chmurowych lub w architekturze mikroserwisów |
| Inżynier każdej specjalizacji | • wiedza z zakresu projektowania urządzeń, czujników wykorzystywanych przy technologii Internetu rzeczy (IoT) |
| Project manager | • umiejętność budowania zespołów w odniesieniu do preferowanego modelu pracy (zespoły zdalne, stacjonarne, mieszane) oraz zespołów interdyscyplinarnych |
| Audytor bezpieczeństwa | • wiedza z zakresu najnowszych standardów certyfikacji (m.in. spełnianie odpowiednich standardów bezpieczeństwa przy wykorzystaniu nowych technologii cyfrowych takich jak AI, IoT) |
| Penetration tester | • wiedza z zakresu sztucznej inteligencji (AI), szczególnie machine learningu<br>• wiedza z zakresu Internetu Rzeczy (IoT) |
| CISO | • zabezpieczenie danych fizycznych i cyfrowych przez cyberatakami wykorzystującymi nowe technologie (np. AI) |
| Architekt ds. bezpieczeństwa | • zabezpieczenie danych analogowych i cyfrowych przez cyberatakami wykorzystującymi nowe technologie (np. AI) |
| Ekspert ds. bezpieczeństwa sieci/ systemów | • brak wskazanych kompetencji |
| Koordynator SOC | • brak wskazanych kompetencji |
| Dyrektor handlowy/ sprzedaży | • brak wskazanych kompetencji |

Źródło: opracowanie własne na podstawie wyników badania jakościowego realizowanego w ramach projektu BBKLII w branży telekomunikacja i cyberbezpieczeństwo, edycja II.

Pełne omówienie wyników badań znajduje się w publikacji:

## Branżowy Bilans Kapitału Ludzkiego II - branża telekomunikacji i cyberbezpieczeństwa. Raport z II edycji