PARP
Grupa PFR

Branżowy Bilans
Kapitału Ludzkiego II

Branżowy Bilans Kapitału Ludzkiego II

Branża telekomunikacja i cyberbezpieczeństwo

Wybrane wyniki
z I edycji badań

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Społeczny

PARP
Grupa PFR

Branżowy Bilans
Kapitału Ludzkiego II

Informacje o projekcie

Nazwa projektu:

Branżowy Bilans Kapitału Ludzkiego II
Branża telekomunikacja i cyberbezpieczeństwo

Główne cele projektu:

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

Czas realizacji I edycji:

18 grudnia 2020 r. - 14 stycznia 2022 r.

Metodologia

Zastosowany schemat w procesie badawczym:

40 wywiadów indywidualnych z pracodawcami, ekspertami branżowymi oraz ds. HR w branży

4 panele eksperckie

Badanie delphi z 53 ekspertami z branży

Panel podsumowujący z Sektorową Radą ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

Wywiady indywidualne z pracodawcami (N=800) i pracownikami (N=965) z branży

Badania jakościowe (czas realizacji: 20. 04. 2021 r. – 14. 07. 2021 r.)

Badania ilościowe (czas realizacji: 7 – 27. 10. 2021 r.)

Informacje o branży

Definicja branży (w oparciu o sekcje PKD):

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

Kluczowe dane dotyczące zatrudnienia:

15 438
przedsiębiorstw*

42 687
pracowników
w sektorze
telekomunikacji**

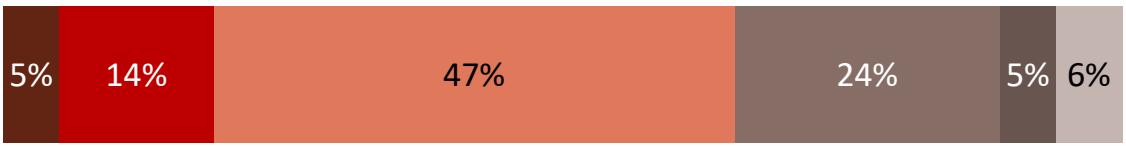
wielkość sprzedaży
produktów
i usług w sektorze
telekomunikacji:

41,5 mld zł**

* Dane kwartalne REGON, GUS, stan na 30.09.2021;
wyłącznie kody PKD wskazane powyżej

** Społeczeństwo informacyjne w Polsce, GUS

Wpływ pandemii na branżę



Pozytywny wpływ: **19%**

W sektorze:

Telekomunikacji (T): **18%**
Cyberbezpieczeństwa (C): **27%**

Negatywny wpływ: **29%**

W sektorze:

Telekomunikacji (T): **29%**
Cyberbezpieczeństwa (C): **23%**

Najczęstsze zmiany:

POZYTYWNE:

- wzrost liczby świadczonych usług (T: 56%, C: 78%)
- wprowadzenie pracy zdalnej (T: 54%, C: 58%)
- pozyskanie nowych partnerów do współpracy (T: 50%, C: 61%)

NEGATYWNE:

- wzrost kosztów funkcjonowania firmy (T: 75%, C: 80%)
- dostosowanie procedur firmy do wymogów bezpieczeństwa i higieny w związku z COVID-19 (T: 67%, C: 81%)
- braki kadrowe wynikające z przebywania pracowników na kwarantannie (T: 65%, C: 55%)

Źródło: BBKLII w branży telekomunikacji i cyberbezpieczeństwa, edycja I, ilościowe badanie pracodawców, n = 800.

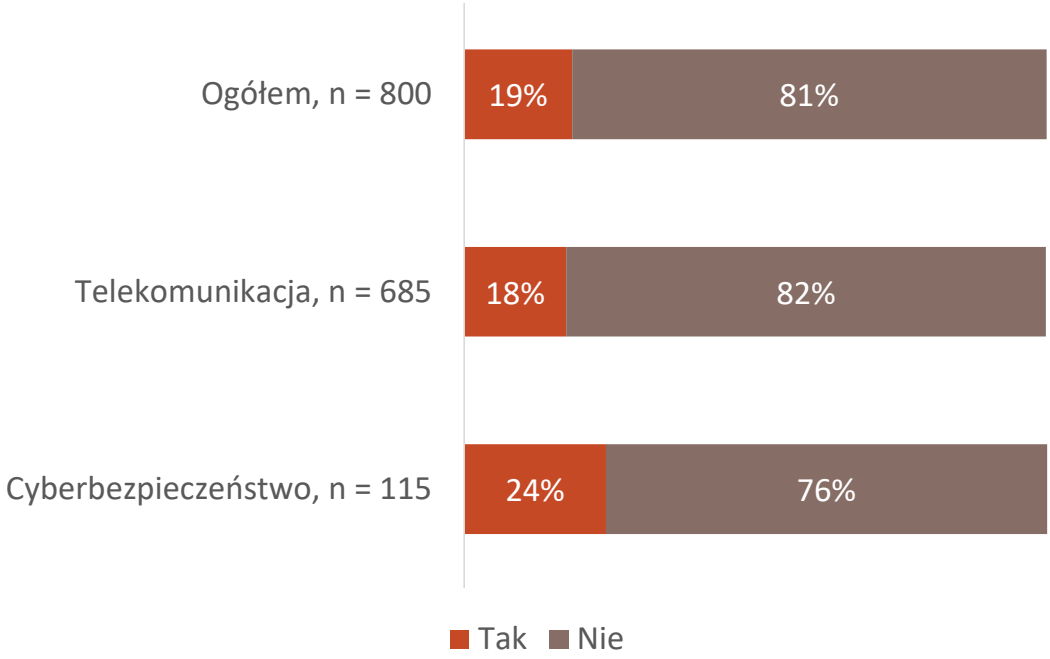
Główne procesy biznesowe w sektorze **telekomunikacji** i przypisane do nich stanowiska

Procesy biznesowe	Kluczowe stanowiska sektorowe
Proces tworzenia oprogramowania, systemów, programów i aplikacji Proces dotyczy tworzenia oprogramowania i systemów umożliwiających obsługę pasywnej infrastruktury oraz urządzeń elektronicznych takich jak telefony, modemy, dekodery itp. Każde wymienione urządzenie, czy też konkretny element infrastruktury telekomunikacyjnej do prawidłowej obsługi potrzebuje specjalnego systemu (software), dzięki któremu możliwe staje się sterowanie i użytkowanie urządzenia.	• **Architekt systemów** • **Developer (programista)** • **Quality Assurance**
Proces projektowania infrastruktury telekomunikacyjnej oraz urządzeń Proces polega na tworzeniu projektów pasywnej infrastruktury np. stacji bazowych, anten, przekaźników, ale także wszelkiego rodzaju urządzeń elektronicznych jak telefony, modemy.	• **Inżynier**
Proces koordynacji usług i utrzymania infrastruktury telekomunikacyjnej W procesie wyróżnia się działania związane z naprawą, modernizacją oraz zapewnieniem nieprzerwanego działania (ciągłości emisji) stacji bazowych, anten i innych urządzeń (a także programów oraz wykupionych przez klientów usług) umożliwiających dostęp do sieci telefonicznej, Internetu, sygnału telewizyjnego itd.	• **Project Manager**
Proces sprzedaży	• **Dyrektor handlowy**

Główne procesy biznesowe w sektorze **cyberbezpieczeństwa** i przypisane do nich stanowiska

Procesy biznesowe	Kluczowe stanowiska sektorowe
Proces prowadzenia audytów bezpieczeństwa Proces oparty o ocenę infrastruktury, systemów czy też aplikacji pod względem spełnienia konkretnych założeń oraz norm bezpieczeństwa.	• **Audytor bezpieczeństwa** • **Penetration Tester**
Proces ochrony aktywów/ identyfikacji zagrożeń/ analizy Proces obejmujący identyfikację wszelkich dóbr, które znajdują się w firmie (urządzenia, dokumenty, aktywa cyfrowe itp.) oraz przemyślenie, czy konkretne zasoby są chronione w sposób wystarczający.	• **CISO (ang. Chief Information Security Officer, pol. Dyrektor ds. bezpieczeństwa informacji)**
Proces prewencji w celu zapewnienia bezpieczeństwa Proces zakładający monitorowanie systemów i sieci w celu wykrywania potencjalnych zagrożeń, obsługę incydentów, w której skład wchodzą czynności związane z zablokowaniem danego incydentu, przywrócenie ładu oraz ewentualne działania mające na celu naprawę i wyciągnięcie wniosków na przyszłość.	• **Architekt ds. bezpieczeństwa** • **Koordynator SOC (ang. Security Operation Center, pol. Centrum operacji bezpieczeństwa)** • **Ekspert ds. bezpieczeństwa systemów/sieci/aplikacji**
Proces sprzedaży	• **Dyrektor handlowy**

Zapotrzebowanie na pracowników w branży



- **Co piąta firma** w ciągu 12 miesięcy poprzedzających badanie poszukiwała nowych osób do pracy
- **Kluczowe stanowiska,** na które jest największe zapotrzebowanie:

w sektorze telekomunikacji:

» Inżynier (48%)

» Developer (32%)

» Architekt systemów (28%)

w sektorze cyberbezpieczeństwa:

» Audytor bezpieczeństwa (49%)

» Ekspert ds. bezpieczeństwa (38%)

» Architekt ds. bezpieczeństwa (32%)

Źródło: BBKLII w branży telekomunikacji i cyberbezpieczeństwa, edycja I, ilościowe badanie pracodawców, n = 800.

Ocena przygotowania absolwentów do podjęcia pracy zawodowej

80%

pracodawców twierdzi, że **absolwenci** opuszczający szkoły/ uczelnie **posiadają umiejętności potrzebne** obecnie **na rynku**

Jednak...

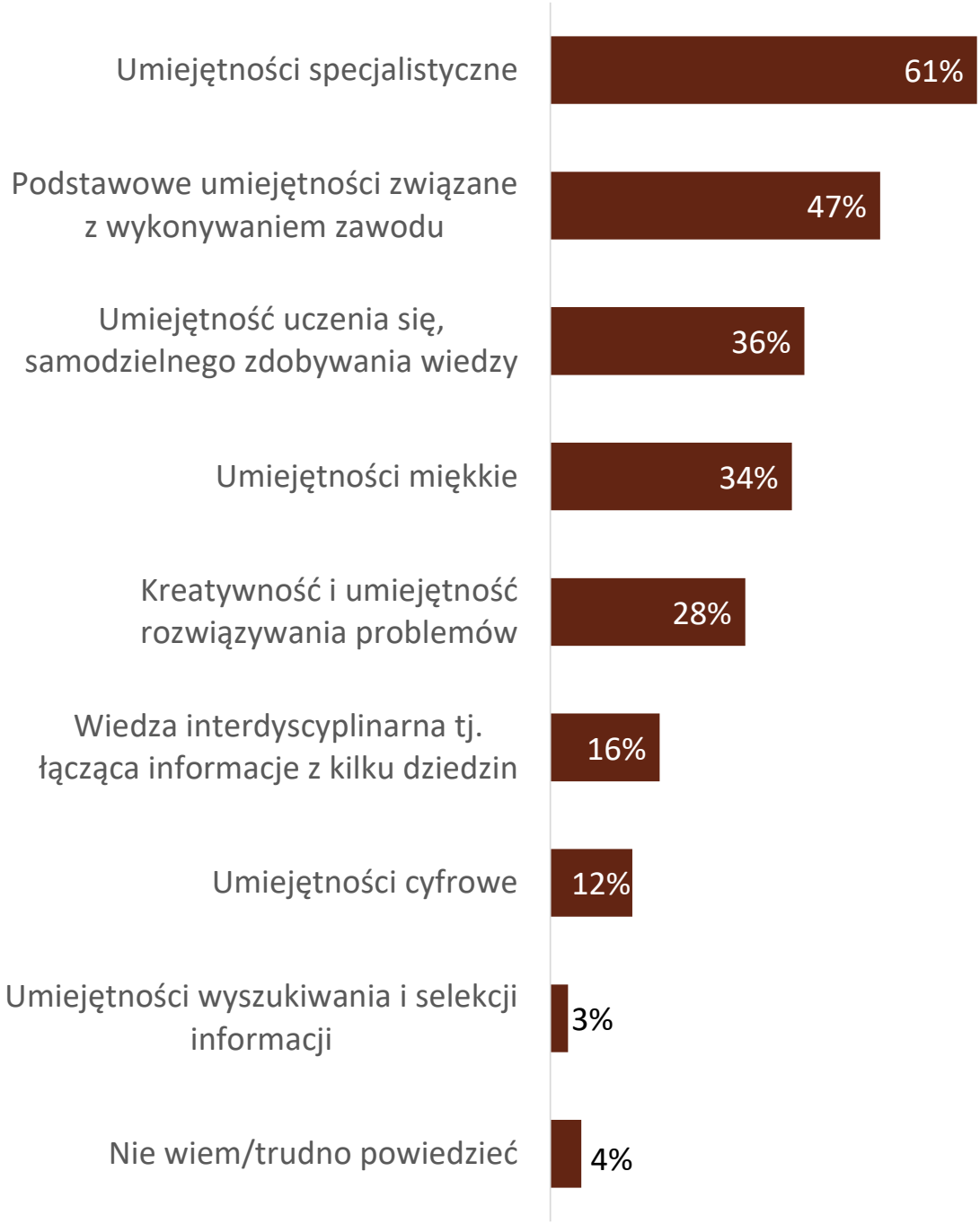
Ocena przygotowania nowo przyjmowanych osób do firm jest już mniej pozytywna:

- **już tylko co czwarty pracodawca** uważa, że absolwenci są w pełni przygotowani do pracy;
- **2 na 5 przedsiębiorców,** że powinni przejść przez niewielkie przeszkolenie przed rozpoczęciem pracy;
- **ponad 35% pracowników** przechodzi większe lub pełne przeszkolenie przed rozpoczęciem pracy lub już po jej rozpoczęciu;

Źródło: : BBKLII w branży telekomunikacji i cyberbezpieczeństwa, edycja I, ilościowe badanie pracodawców, n = 800.

Wiedza i umiejętności jakie powinny być przekazywane w szkołach/na uczelniach

Kluczowymi umiejętnościami są umiejętności specjalistyczne.



Bilans kompetencji

Ocena niedopasowania kompetencyjnego: zestawienie oceny ważności danej kompetencji (w kontekście pracy na danym stanowisku) dokonywanej przez pracodawców z samooceną poziomu kompetencji posiadanych przez pracowników zatrudnionych na tym stanowisku.

Samoocena kompetencji pracowników

Wyższa

Ważność dla pracodawców

Mniej ważne

Kompetencje mniej ważne, przy wyższej samoocenie kompetencje relatywnie mniej ważne dla pracodawców, przy relatywnie wyższej samoocenie pracowników **Kompetencje nadwyżkowe (T: 21%; C: 28%)**	**Kompetencje ważniejsze, przy wyższej samoocenie** kompetencje relatywnie ważniejsze dla pracodawców i jednocześnie relatywnie wysoko oceniane przez pracowników **Kompetencje zrównoważone (T: 36%; C: 23%)**
Kompetencje mniej ważne, przy niższej samoocenie kompetencje relatywnie mniej ważne dla pracodawców i jednocześnie relatywnie niżej oceniane przez pracowników **Kompetencje wystarczające (T: 28%; C: 24%)**	**Kompetencje ważniejsze, przy niższej samoocenie** kompetencje relatywnie ważniejsze dla pracodawców przy relatywnie niższej samoocenie pracowników **Kompetencje niedoboru (T: 15%; C: 25%)**

Ważniejsze

Niższa

Luka kompetencyjna: występuje, kiedy mamy do czynienia z kompetencjami relatywnie ważniejszymi dla pracodawców i jednocześnie trudnymi do pozyskania w opinii 51% lub więcej pracodawców oceniających dany profil kompetencyjny.

Kompetencje przyszłości: oceniane są na podstawie rozkładu odpowiedzi pracodawców na pytanie o przewidywaną zmianę znaczenia danej umiejętności w przyszłości. Perspektywa czasowa, do której odnosili się pracodawcy to 3 lata.

W nawiasach podano odsetki danego typu kompetencji w każdym z sektorów: T – Telekomunikacja, C – Cyberbezpieczeństwo.

Bilans kompetencji

Kompetencje relatywnie ważniejsze dla pracodawców z niższą samooceną pracowników (**kompetencje niedoboru**), które są obecnie trudno dostępne (**luka kompetencyjna**) i których znaczenie będzie rosło (**kompetencje przyszłości**) dotyczą stanowisk*:

Quality Assurance (telekomunikacja)

- Umiejętność poprawy jakości i czytelności kodu;
- Umiejętność identyfikacji błędów w działaniu systemu, programu, usługi;

Ekspert ds. bezpieczeństwa (cyberbezpieczeństwo)

- Umiejętność obsługi platform bezpieczeństwa (np. firewalle aplikacyjne, sieciowe);
- Umiejętność zablokowania zagrożeń (w tym potencjalnych sytuacji zagrożenia);
- Wiedza z zakresu systemów plików i zasad ich działania;
- Umiejętność obsługi systemów i sieci pod względem zabezpieczeń;
- Umiejętność odzyskiwania utraconych (np. w wyniku incydentu) danych;
- Wiedza z zakresu systemów operacyjnych;
- Umiejętność rozpoznawania cyberataków bądź niepokojących incydentów;

Architekt ds. bezpieczeństwa (cyberbezpieczeństwo)

- Wiedza z zakresu bezpieczeństwa cyfrowego (systemy zabezpieczeń, programy zabezpieczające);
- Odpowiedzialność;
- Umiejętność zarządzania systemami bezpieczeństwa;
- Umiejętność przewidywania w jaki sposób może dojść do ataku na dany system, program, usługę;
- Znajomość języków obcych - szczególnie angielskiego;

* Wskazano stanowiska z największą liczbą kompetencji, a pominięto te, w których są jednostkowe kompetencje.

Bilans kompetencji

Średnia ważność kompetencji*:

- Telekomunikacja – od 4,26 do 4,8
- Cyberbezpieczeństwo – od 3,87 do 4,84

Średnia samoocena kompetencji*:

- Telekomunikacja – od 4,07 do 4,55
- Cyberbezpieczeństwo – od 3,67 do 4,61

* Do oceny użyto skali pięciopunktowej

Kompetencje przyszłości to kompetencje, które zdaniem przedsiębiorców będą zyskiwać na znaczeniu w przyszłości. Poniżej przedstawiono po pięć kompetencji przyszłości wskazywanych najczęściej przez przedsiębiorców w analizowanych sektorach.

Telekomunikacja

Umiejętność przeprowadzania/ pisania testów automatycznych

Podstawowa znajomość języków programowania, technologii (np. Python, C, C#, Java, JavaScript, Angular, React, Skala itp.)

Wiedza z zakresu wykorzystywania technologii chmurowych

Wiedza z zakresu technologii komputerowych (w tym najnowszych technologii)

Umiejętność poprawy jakości i czytelności kodu

Cyberbezpieczeństwo

Umiejętność planowania strategii ataków cyfrowych

Znajomość norm prawnych w zakresie pen-testów i odpowiedzialności pen-testera

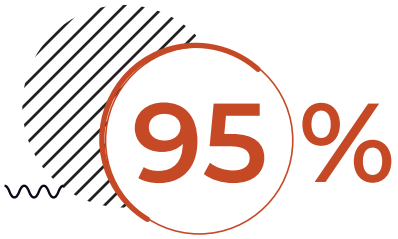
Umiejętność zablokowania zagrożeń (w tym potencjalnych sytuacji zagrożenia)

Wysoki poziom komunikacji interpersonalnej

Umiejętność zbierania informacji oraz weryfikacji ich rzetelności

Ocena zadowolenia z wykonywanej pracy

- bardzo zadowolony/a
- raczej zadowolony/a
- ani niezadowolony/a, ani zadowolony/a
- raczej niezadowolony/a
- bardzo niezadowolony/a



pracowników zatrudnionych na kluczowych stanowiskach **jest zadowolona z wykonywanej pracy**

Najwyżej oceniane aspekty pracy

» relacje z przełożonymi (97%)

» relacje ze współpracownikami (96%)

» możliwość wykazania się inicjatywą i samodzielnością (96%)

» warunki pracy (96%)

Wyzwania w branży

Trzy najważniejsze wyzwania

- Dbanie o rozwój pracowników w celu utrzymania przez nich zatrudnienia – ogółem: 51%, T: 51%, C: 53%
- Spełnienie norm i wymogów dla pojawiających się nowych technologii – ogółem: 50%, T: 50%, C: 49%
- Informowanie klientów o zagrożeniach przy korzystaniu z technologii i usług telekomunikacyjnych/internetowych, oferowanych przez firmę – ogółem: 46%, T: 45%, C: 49%

Wyzwania o największej różnicy bezwzględnej między branżami

- Znalezienie nowych pracowników (specjalistów) z zakresu IT, którzy zajmują się projektowaniem systemów, programów, aplikacji itp. – 9 p.p. (dla C)
- Weryfikacja nowych pracowników w zakresie ich kompetencji i historii o ochronie danych osobowych – 9 p.p. (dla C)
- Zwiększenie poziomu dbałości o doświadczenia użytkownika podczas korzystania z technologii i usług oferowanych przez firmę – 6 p.p. (dla C)

Oznaczenie sektorów: T – Telekomunikacja, C – Cyberbezpieczeństwo.

Źródło: BBKLII w branży telekomunikacji i cyberbezpieczeństwa, edycja I, ilościowe badanie pracodawców i pracowników;

Prezentowane odsetki to udział przedsiębiorców z branży udzielających danej odpowiedzi.

PARP
Grupa PFR

Branżowy Bilans
Kapitału Ludzkiego II

Pełne omówienie wyników badań
znajduje się w Raporcie:

Branżowy Bilans Kapitału Ludzkiego II
branża telekomunikacja i cyberbezpieczeństwo

Raport z I edycji badań:

https://www.parp.gov.pl/component/site/site/bilans-kapitalu-ludzkiego#wynikibadanbranzowych

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Społeczny