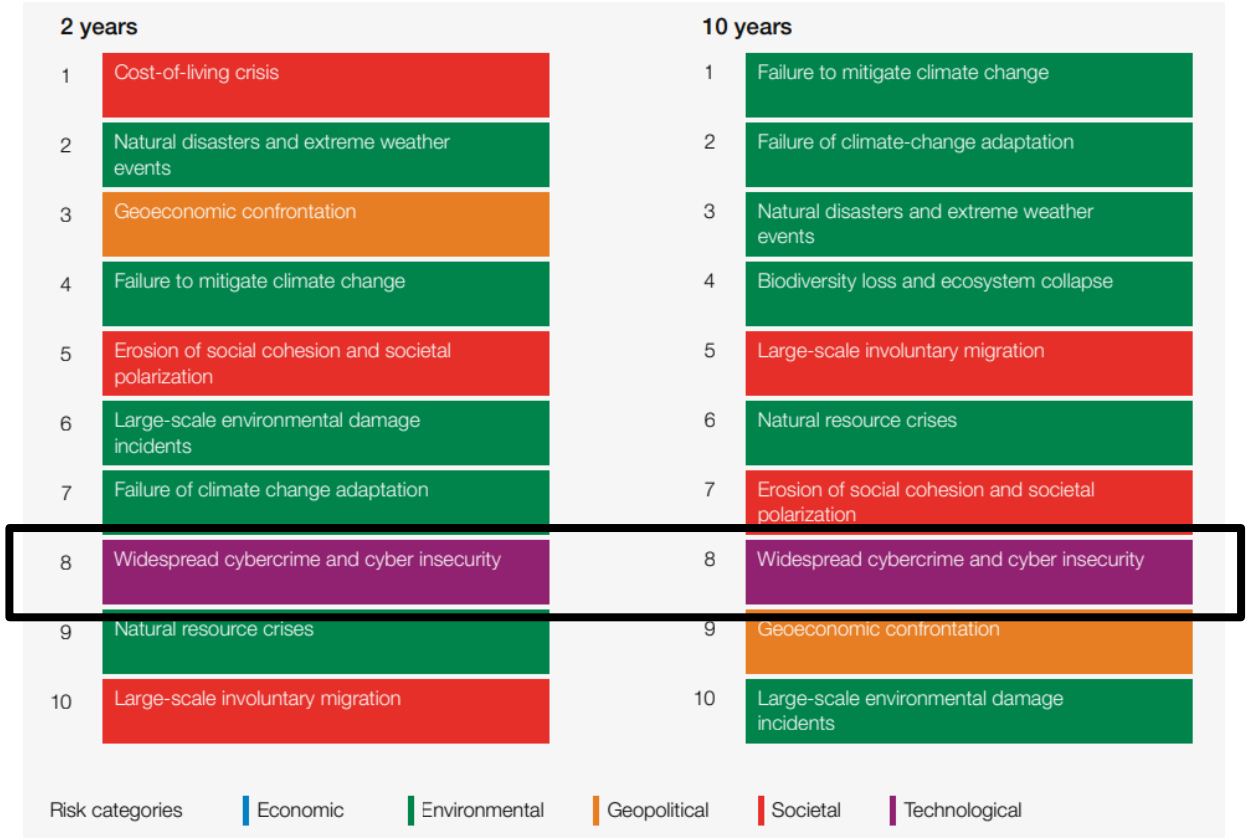
Cyberbezpieczeństwo – perspektywa dla Zarządzających

Tomasz Klekowski
Sektorowa Rada ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo
30 października 2023 r.

Sektorowa Rada ds. Kompetencji Informatyka
Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo
Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
PARP
Unia Europejska Europejski Fundusz Społeczny

Percepcja zagrożeń cybernetycznych



The Global Risks Report 2023, weforum.org

https://www.bbc.com/news/world-europe-57184977 maj 2021

Percepcja zagrożeń cybernetycznych

Ryzyka się materializują

[Cyber-attack on Irish health service 'catastrophic' - BBC News]

- Dr Vida Hamilton said it was "affecting every aspect of patient care". She described the incident as a "major disaster" and said there were difficulties around accessing patient records.
- The number of appointments in some areas of the system has dropped by 80%.
- (Irish PM) Micheál Martin said cyber-security is under continuous review across all state agencies in the Republic of Ireland.
- HSE cyber-attack: Irish health service still recovering months after hack (wrzesień)

The Global Risks Report 2023, weforum.org

https://www.bbc.com/news/world-europe-57184977 maj 2021

Organizacyjny kontekst cybersecurity

- Poziom świadomości zależności od technologii cyfrowych w poszczególnych obszarach działalności przedsiębiorstwa
- Cybersecurity jest głównie widziane jako domena techniczna
  - Raport Trend Micro: głównie jako domena techniczna (41%),
  - Całkowicie jako domena techniczna (21%)
- Nie ma wystarczającego powiązania głównych inicjatyw biznesowych z wymaganiami cybersecurity
  - Tylko 23% firm deklaruje, że wymagania cybersecurity należą do głównych czynników podczas projektowania nowych inicjatyw biznesowych

Źródło: https://www.helpnetsecurity.com/2021/02/01/board-members-cybersecurity/

W 60% przypadków funkcje cyberbezpieczeństwa są ulokowane w technicznych działach IT, co jest złą praktyką i jednym z najczęściej występujących problemów strukturalnych w zakresie cyberbezpieczeństwa. Podobnie jak transformacja cyfrowa, cyberbezpieczeństwo widziane jest jako funkcja techniczna. Może pojawiać się konflikt wynikający z tego, że cyberbezpieczeństwo podlega pod tych, których ma w pierwszej kolejności kontrolować. - "Ocena dojrzałości cyfrowej przedsiębiorstw rynku energii elektrycznej w Polsce„ www.gov.pl

https://www.gov.pl/web/ai/ocena-dojrzalosci-cyfrowej-przedsiebiorstw-rynku-energii-elektrycznej-w-polsce

Cybersecurity z perspektywy zarządczej

- 73% organizacji było obiektem cyberataku
- Tylko 41% organizacji angażuje w tworzenie planów oceny ryzyka cybernetycznego działy prawne, finansowe, operacyjne i zarządzania łańcuchem dostaw
- Tylko 26% respondentów stwierdziło, że ich organizacja stosuje mierniki finansowe w zakresie oceny ryzyka cybernetycznego
- 53% organizacji uważa, że największą barierą w ocenie ryzyka cybernetycznego jest brak odpowiednich pracowników/umiejętności, aby to zrobić

The state of cyber resilience 2022. https://www.marsh.com/dk/en/services/cyber-risk/insights/the-state-of-cyber-resilience.html

Odpowiedzialność prawna członków zarządów

- Odpowiedzialność członków zarządu za zobowiązania i działania spółki ma charakter bezwzględny
- „Odpowiedzialności członka zarządu nie uchyla umowa łącząca członków zarządu co do sposobu kierowania sprawami spółki, w szczególności ustalony w umowie podział czynności”
- Obszary odpowiedzialności zarządów
  - Zarządzanie
  - Zarządzanie ryzykiem i zgodnością
  - Audyt wewnętrzny

Wyrok Sądu Najwyższego z dnia 14 kwietnia 2016 r. IV CSK 485/15.

Wszyscy ponoszą odpowiedzialność

Wymagania Aktu o Cyberodporności

– dla produktów i usług z elementami cyfrowymi

Obowiązki

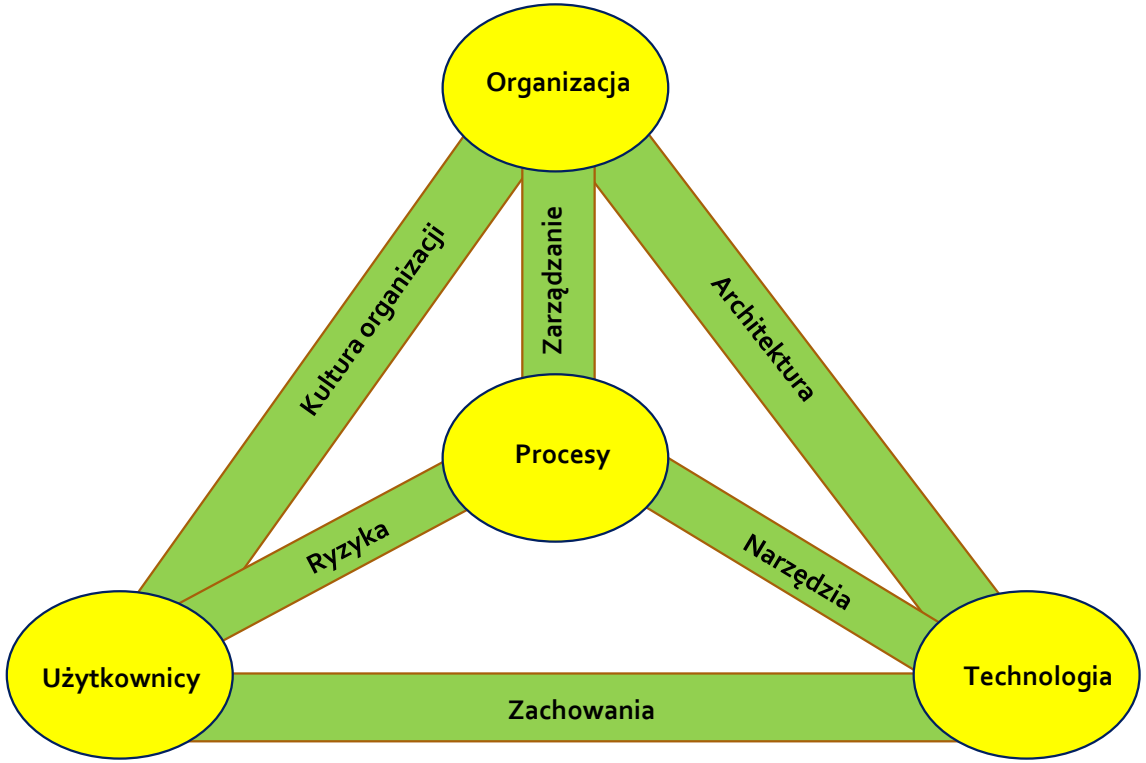
- Przeprowadzić ocenę ryzyka związanego z używaniem przez klientów produktów i usług, aby zidentyfikować wynikające z nich zagrożenia dla cyberbezpieczeństwa.
- Wdrożyć odpowiednie środki bezpieczeństwa w celu zminimalizowania tych zagrożeń, ich przyczyn i konsekwencji.
- Testować produkty i usługi o nie oparte pod kątem podatności na zagrożenia bezpieczeństwa.
- Opracować plan reagowania na incydenty związane z bezpieczeństwem dotyczące całego cyklu życia produktów.
- Edukować pracowników na temat najlepszych praktyk z zakresu cyberbezpieczeństwa w odniesieniu do całego cyklu życia produktów z komponentem cyfrowym.

Sektorowa Rada ds. Kompetencji Informatyka
Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo
Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
PARP
Unia Europejska Europejski Fundusz Społeczny

Istotne wymagania i kierunki

- Zwiększenie wiedzy na temat specyfiki branży wśród specjalistów cyberbezpieczeństwa i wymagań cyberbezpieczeństwa wśród specjalistów danej branży
- Stworzenie zaleceń i rozwiązań specyficznych dla danej branży.
- Zwiększenie współpracy pomiędzy managerami zarządzającymi procesami i organizacjami zajmującymi się cyberbezpieczeństwem a managerami innych obszarów przedsiębiorstwa
- Umocowanie i rozpoznanie wagi cyberbezpieczeństwa na poziomie zarządów
- Zapewnienie edukacji z zakresu cyberbezpieczeństwa dla kluczowych grup specjalistów z innych niż cyberbezpieczeństwo obszarów
- Rozszerzenie świadomości, wiedzy i umiejętności budowy bezpiecznych procesów, usług i produktów przez firmy i stworzenie w firmach powszechnej kultury cyberbezpieczeństwa opartej o zasady cybersecurity-by-design i umożliwienie cybersecurity-by-default.

Model organizacji cyberbezpieczeństwa



Zorientowane na organizację procesów

- Matryca NIST
- Norma ISO EIC 27001

Zorientowane na rozwój kompetencji

- Rama Kwalifikacji European Cybersecurity Skills Framework
- Sektorowa Rama Kwalifikacji dla sektora Cyberbezpieczeństwa (SRK Cyber)

Matryca NIST

- Spójny, powszechnie używany język opisu
- Obejmuje szeroki zakres technologii, sektorów, etapów rozwoju
- Oparty o ocenę ryzyka
- Oparta o międzynarodowe standardy
- Regularnie aktualizowana
- Wynik współpracy sektora publicznego, prywatnego i naukowego

Europen Cybersecurity Skills Framework

1. CHIEF INFORMATION SECURITY OFFICER (CISO)
2. CYBER INCIDENT RESPONDER
3. CYBER LEGAL, POLICY & COMPLIANCE OFFICER
4. CYBER THREAT INTELLIGENCE SPECIALIST
5. CYBERSECURITY ARCHITECT
6. CYBERSECURITY AUDITOR
7. CYBERSECURITY EDUCATOR
8. CYBERSECURITY IMPLEMENTER
9. CYBERSECURITY RESEARCHER
10. CYBERSECURITY RISK MANAGER
11. DIGITAL FORENSICS INVESTIGATOR
12. PENETRATION TESTER

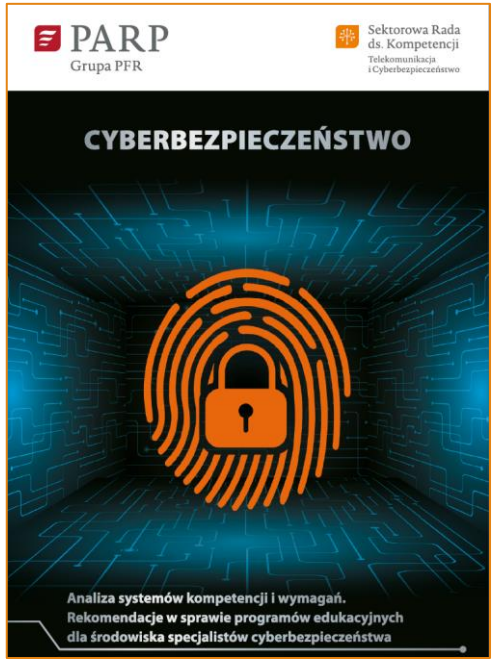
Nazwa profilu	**Manager Zarządzania Ryzykiem Cybernetycznym**
Inne nazwy profilu	•Analityk Ryzyka Bezpieczeństwa Informacyjnego •Konsultant ds. Zapewniania Bezpieczeństwa Cybernetycznego •Konsultant ds Ryzyk Cyberbezpieczeństwa •Analityk Wpływu Zagrożeń Cybernetycznych •Manger Ryzyk Cyberbezpieczeństwa
Podsumowanie roli	Zarządza ryzykiem związanym z cyberbezpieczeństwem organizacji w odniesieniu do realizacji jej strategii. Opracowuje, utrzymuje i wdraża procesy zarządzania ryzykiem pochodzącym z zagrożeń cybernetycznych i informacyjnych
Opis misji	Zarządza (identyfikuje, analizuje, ocenia, szacuje, odpowiada na) ryzyka związane z cyberbezpieczeństwem w zakresie infrastruktury, systemów i usług ICT poprzez planowanie, stosowanie, raportowanie i komunikowanie analizy, oceny i przetwarzania ryzyka. Ustanawia strategię zarządzania ryzykiem dla organizacji i zapewnia, że ryzyko pozostaje na akceptowalnym dla organizacji poziomie poprzez wybór i wdrażanie działań zapobiegawczych i kontrolnych.
Przykładowe rezultaty	•Raport oceny ryzyka dla cyberbezpieczeństwa •Plan działania na rzecz usuwania ryzyka cybernetycznego
Główne zadania	•Opracowanie strategii zarządzania ryzykiem cyberbezpieczeństwa w organizacji • Zarządzanie inwentaryzacją zasobów organizacji •Identyfikacja i ocena zagrożeń i podatności systemów teleinformatycznych związanych z cyberbezpieczeństwem •Identyfikacja krajobrazu zagrożeń, w tym profili atakujących i oszacowanie potencjału ataków •Ocena zagrożeń dla cyberbezpieczeństwa i zaproponowanie najodpowiedniejszych opcji zarządzania ryzykiem, •W tym środków kontroli oraz ograniczania i unikania ryzyka, w odniesieniu do realizacji strategii organizacji •Monitorowanie skuteczności kontroli cyberbezpieczeństwa i poziomów ryzyka •Zapewnienie, że wszystkie zagrożenia dla cyberbezpieczeństwa pozostaną na akceptowalnym poziomie dla organizacji •Opracowanie, utrzymanie, raportowanie i komunikowanie działań pełnego cyklu zarządzania ryzykiem
Główne umiejętności	•Umiejętności wdrożenia ram, metodologii i wytycznych dotyczących zarządzania ryzykiem w cyberbezpieczeństwie oraz zapewnienie zgodności z przepisami i standardami •Umiejętności analizy i wykorzystania praktyk zarządzania jakością i ryzykiem w organizacji •Umożliwienie właścicielom procesów i obszarów biznesowych, kadrze kierowniczej i innym interesariuszom podejmowania decyzji ze świadomością ryzyka i możliwością zarządzania nim •Umiejętności budowy środowiska rozumienia ryzyka w zakresie cyberbezpieczeństwie •Umiejętności komunikacji, prezentowania i raportowania do odpowiednich interesariuszy w organizacji •Umiejętności definiowania opcji zarządzania ryzyka
Najważniejsze obszary wiedzy	•Zna i rozumie standardy, metodologie i ramy zarządzania ryzykiem • Zna i rozumie narzędzia zarządzania ryzykiem •Zna i rozumie zalecenia i najlepsze praktyki w zakresie zarządzania ryzykiem •Zna i rozumie zagrożenia cybernetyczne •Zna i rozumie luki w zabezpieczeniach systemów komputerowych Zna zasady kontroli procesów i stosowania rozwiązań w zakresie cyberbezpieczeństwa •Zna i rozumie zagrożenia dla cyberbezpieczeństwa •Zna i rozumie zasady monitorowania, testowania i oceny skuteczności kontroli bezpieczeństwa cybernetycznego •Zna u rozumie zakres korzyści i wykorzystania certyfikatów związanych z cyberbezpieczeństwem •Zna i rozumie technologie związane z cyberbezpieczeństwem
Wymagane kompetencje z ramy kompetencji e-CF	•E.3. Risk Management – poziom 4 •E.5. Process Improvement – poziom 3 •E.7. Business Change Management – poziom 4 •E.9. IS-Governance – poziom 4

Przewodnik po bezpieczeństwie cybernetycznym dla MŚP - 12 kroków do bezpieczeństwa twojej firmy

- Rozwój kultury cyberbezpieczeństwa
- Przypisanie na poziomie zarządu odpowiedzialności za cyberbezpieczeństwo
- Potrzeby uświadomienia pracowników i uzyskania zrozumienia dla konieczności stosowania się do wymagań cyberbezpieczeństwa
- Przeprowadzanie audytów cyberbezpieczeństwa
- Ochrona danych
- Organizacja szkoleń
- Organizacja współpracy z innymi podmiotami ekosystemu cyberbezpieczeństwa (dostawcami systemów, CERTami)
- Opracowanie planów reagowania na incydenty
- Zabezpieczenie systemów, urządzeń i sieci

https://www.enisa.europa.eu/publications/report-files/smes-leaflet-translations/enisa-cybersecurity-guide-for-smes_pl.pdf

Materiały Sektorowej Rady ds. Kompetencji Telekomunikacji i Cyberbezpieczeństwa



Raporty analityczne z rekomendacjami oraz udział w przygotowaniu ramy kwalifikacji

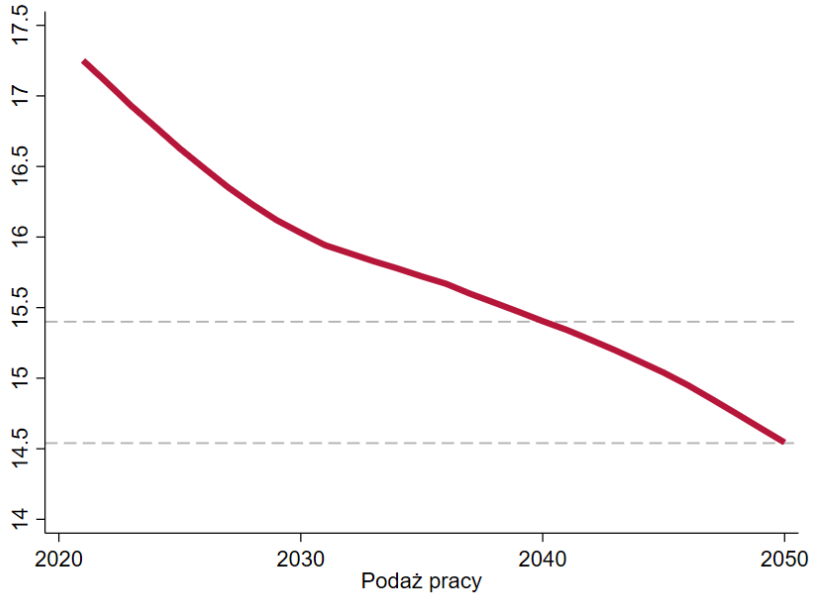
- Analiza systemów kompetencji i wymagań w zakresie kompetencji cyberbezpieczeństwa
- Rekomendacje w sprawie programów edukacyjnych dla środowiska specjalistów cyberbezpieczeństwa
- Przygotowanie Sektorowej Ramy Kwalifikacji dla sektora Cyberbezpieczeństwa (SRK Cyber)

Bardzo dziękuję

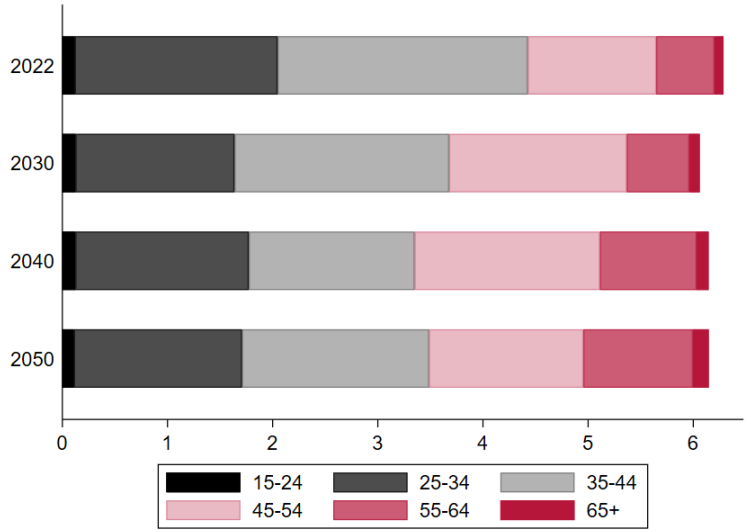
tomasz.klekowski@insead.edu

Demografia polskiego rynku pracy

Do 2040 roku łączna podaż pracy spadnie o 10%, a podaż pracy osób w sile wieku o 17%.



Podaż pracy osób z wykształceniem wyższym

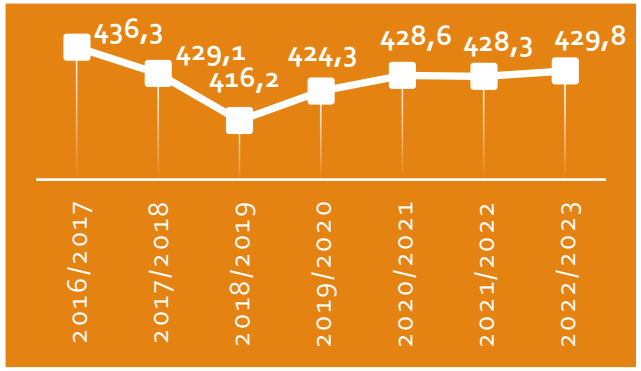


Źródło: System Prognozowania Polskiego Rynku Pracy

Edukacja ICT nie zapełna luki kadrowej

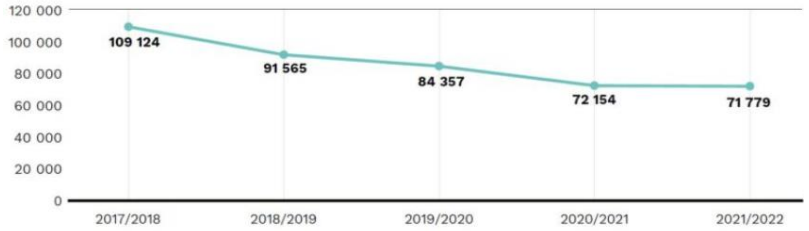
(MEiN 2023)

Wśród 429,8 tys. przyjętych na studia w roku 2022/2023 …informatyka nadal numerem 1.



	Kierunek studiów	*Liczba zgłoszeń 2022/2023 (tys.)*
1	**Informatyka**	**44,2**
2	Psychologia	40,6
3	Zarządzanie	36,5,2
4	Prawo	22,0
5	Medycyna *)	20,0

Zmiana liczby studentów kierunków STEM

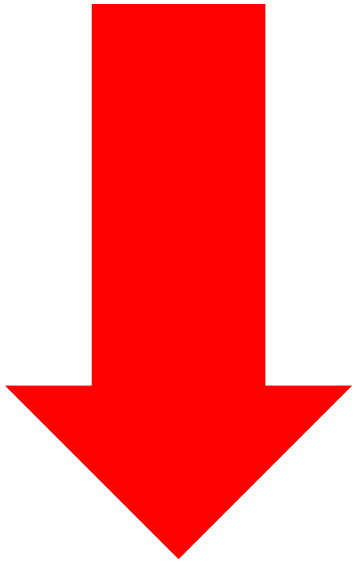


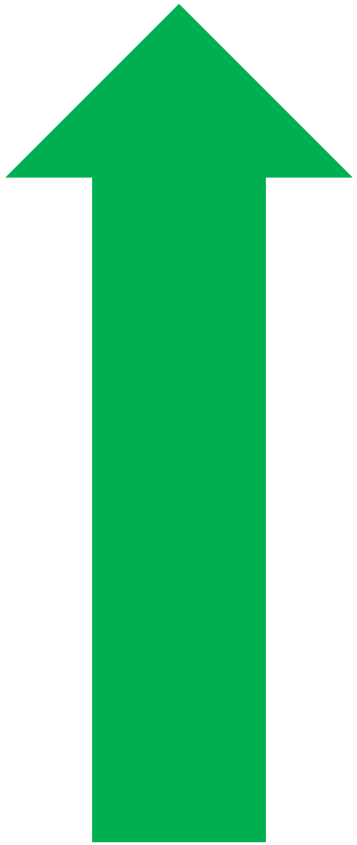
Źródło: opracowanie własne PIE na podstawie danych GUS.

- 147 tys. specjalistów IT brakuje, aby ich udział wśród wszystkich pracowników w Polsce był taki sam, jak w UE
- 42 proc. wakatów na stanowisko specjalisty IT zostało zidentyfikowanych jako trudne do obsadzenia.
- 64 proc. ankietowanych firm zatrudniło mniej specjalistów IT niż planowało,
- 20 proc. często musiało odmawiać realizacji projektu z powodu braku wystarczającej liczby specjalistów.
- **Aby wypełnić lukę IT, 3,5 razy więcej osób w Polsce powinno kończyć studia na kierunkach STEM, a więc związanych z technologią, inżynierią i matematyką**

Czy sztuczne inteligencja i automatyzacja zabierze nam pracę?

W ciągu najbliższych pięciu lat prognozuje się utratę 83 milionów miejsc pracy i utworzenie 69 milionów nowych, **co stanowi strukturalne przetasowanie rynku pracy o 152 miliony miejsc pracy, czyli 23% spośród 673 milionów pracowników** w badanym zbiorze danych. Oznacza to zmniejszenie zatrudnienia o 14 milionów miejsc pracy, czyli 2%. Future of Jobs Report 2023

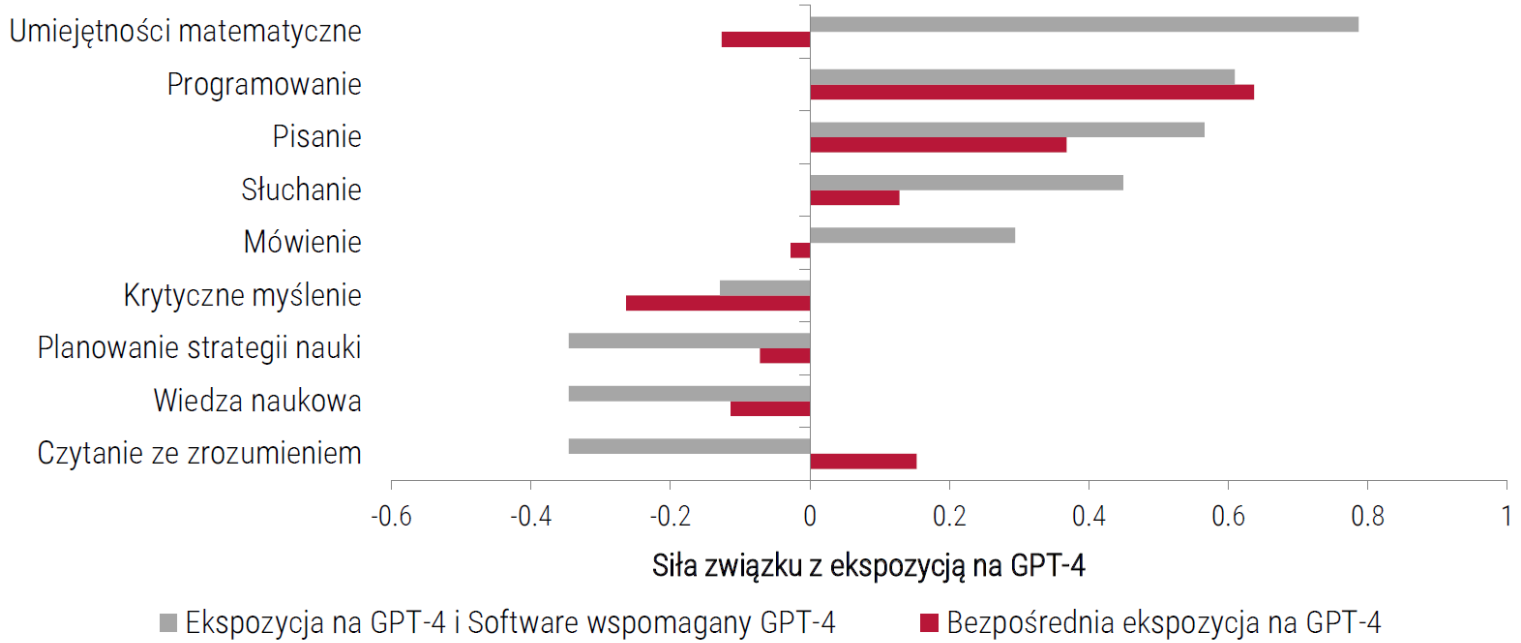




- Różnica w liczbie tworzonych miejsc pracy i eliminowanych miejsc pracy
- Różnica w lokalizacji miejsc pracy
- Czas na znalezienie nowego miejsca pracy
- Czas na zdobycie nowych kwalifikacji lub nowego zawodu
- Kompetencje i nakłady potrzebne do tranzycji

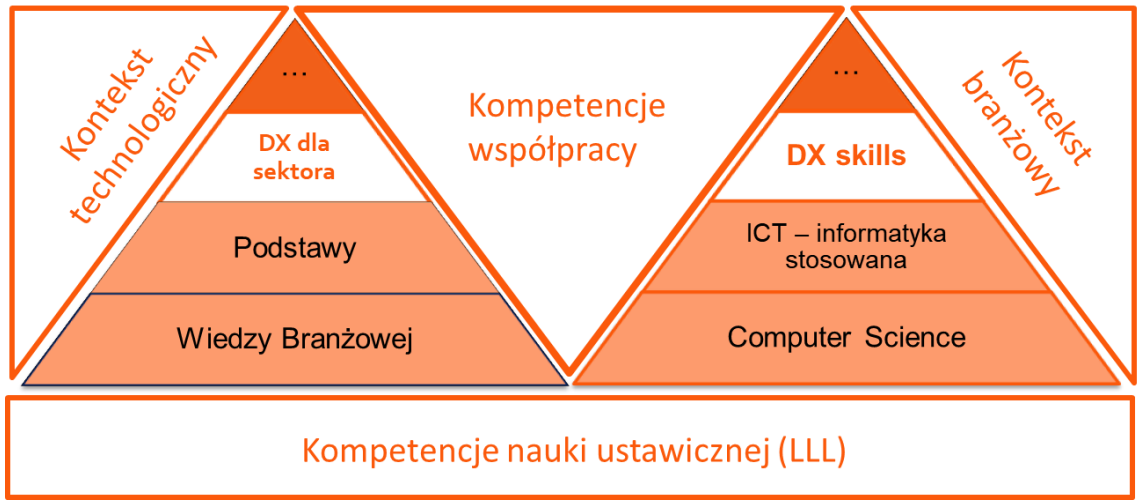
Wpływ AI

Umiejętności związane z czytaniem ze zrozumieniem, wykorzystywaniem wiedzy naukowej do rozwiązywania problemów i planowaniem najmniej narażone na GPT-4



Kierunki działań

- Wzrost liczby absolwentów kierunków STEM
- Upskilling - uaktualnianie i rozwój kompetencji obecnych specjalistów
- Reskilling na rzecz kompetencji IT i cyberbezpieczeństwa
- Umieszczanie kompetencji związanych z IT i zapewnianiem cyberbezpieczeństwa w programach edukacyjnych innych specjalności
- Umieszczanie kompetencji związanych z IT i zapewnianiem cyberbezpieczeństwa w programach edukacyjnych Life Long Learning



Projekt i realizatorzy

POLSKIE TOWARZYSTWO INFORMATYCZNE

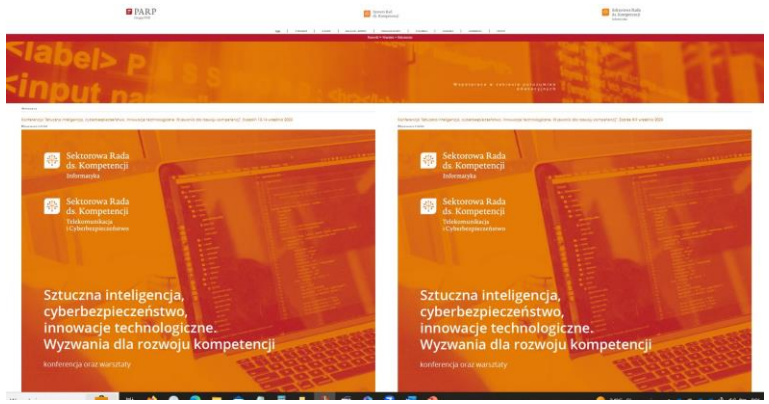
PIIT

- **Sektorowa Rada ds. Kompetencji – Informatyka**
- **Sektorowa Rada ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo**
  - dofinansowane za pośrednictwem PARP z Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza, Edukacja, Rozwój
- **Realizatorzy – partnerzy**
  - **Polskie Towarzystwo Informatyczne** (lider)
    - stowarzyszenie zawodowe teoretyków, dydaktyków oraz praktyków-specjalistów informatyki (istniejące od 1981 r.)
  - **Polska Izba Informatyki i Telekomunikacji**
    - izba gospodarcza firm działających w sektorze teleinformatyki i komunikacji elektronicznej (istniejąca od 1993 r.)
- **Cel działania**
  - dopasowanie systemu edukacji (formalnej i pozaformalnej) specjalistów ICT do dzisiejszych i przyszłych potrzeb

Obszary działalności – badania i analizy

- **Obserwacja i analizy trendów cyfrowej transformacji**
  - m. in. na potrzeby rekomendacji dla PARP dotyczącej potrzeb kompetencyjnych
- **Badania potrzeb kompetencyjnych**
  - „covidowe" i „zwykłe"
- **Inne analizy i ankiety**
  - analizy bieżące rynku pracy IT
- **Analizy Sektorowych Ram Kwalifikacji**
- **Udział w Branżowych Badaniach Kapitału Ludzkiego:**
  - w sektorze IT *(Centrum Ewaluacji i Analiz Polityk Publicznych UJ , edycje 2020 i 2021)*
  - w branży telekomunikacja i cyberbezpieczeństwo *(IBC GROUP Central Europe Holding/CBM INDICATOR, edycja 2021)*
- **Powołanie Komitetu Technicznego 337 ds. Kompetencji IT w Polskim Komitecie Normalizacyjnym**

Obszary działalności – opinie i stanowiska



- **Opiniowanie**
  - kolejnych edycji Programu Rozwoju Kompetencji Cyfrowych - dla Ministerstwa Cyfryzacji, Rady ds. Cyfryzacji oraz KPRM Cyfryzacja)
  - wniosków do Zintegrowanego Systemu Kwalifikacji
  - programów studiów informatycznych przy wnioskach uczelni o uruchamianie studiów informatycznych
  - podstaw programowych w szkołach branżowych
- **Opinie i stanowiska Rad**
  - Opinie wspólnych zespołów ekspertów SRIT i SRTCB w sprawie wpływu na rynek pracy ICT:
    - wydarzeń na Białorusi dla programu Polish Business Harbour
    - imigracji z Ukrainy po agresji Rosji
  - Udział przedstawicieli i ekspertów Rad
    - w grupach roboczych i zespołach Ministerstwa Cyfryzacji/KPRM Cyfryzacja
    - w analizach Polskiego Instytutu Ekonomicznego dotyczących luki kadrowej ICT
    - w innych przedsięwzięciach związanych z edukacją ICT