Minister Edukacji i Nauki

Ministerstwo Edukacji i Nauki

Łukasiewicz
Instytut Technologii Eksploatacji

Projekt pn. „**Kompetencje przyszłości kluczem do rozwoju technologicznego Polski**”
finansowany ze środków Ministerstwa Edukacji i Nauki

OPIS
PROFILU KOMPETENCJI PRZYSZŁOŚCI

CYBERBEZPIECZEŃSTWO

Źródło: Kreator obrazów Microsoft Bing

Wprowadzenie

Opisy profili kompetencji przyszłości zostały opracowane przez Łukasiewicz – Instytut Technologii Eksploatacji w projekcie pn. *„Kompetencje przyszłości kluczem do rozwoju technologicznego Polski”* finansowanym ze środków Ministerstwa Edukacji i Nauki.

Opracowano TOP10 najbardziej pożądanych (spośród 30 kompetencji zidentyfikowanych w badaniu diagnostycznym) kompetencji przyszłości wspólnych dla trzech poziomów edukacji formalnej (szkolnictwo podstawowe, ponadpodstawowe i wyższe) o najwyższej liczbie wskazań respondentów.

Lp.	TOP 10 kompetencji przyszłości dla trzech poziomów edukacji formalnej: szkoły podstawowe, ponadpodstawowe, wyższe	Liczba wskazań respondentów
1.	**Komunikatywność**	1394
2.	**Kreatywność**	1231
3.	**Krytyczne myślenie**	992
4.	**Znajomość języków**	975
5.	**Korzystanie z informacji i danych**	958
6.	**Umiejętność radzenia sobie ze stresem**	956
7.	**Biegłość w obsłudze nowych mediów**	942
8.	**Inteligencja emocjonalna**	900
9.	**Umiejętność uczenia się przez całe życie**	855
10.	**Cyberbezpieczeństwo**	823

Źródło: Raport z realizacji Działania 1 – Diagnoza stanu faktycznego poziomu kompetencji przyszłości

Każda z ww. **kompetencji przyszłości** staje się coraz bardziej potrzebna w dynamicznie zmieniającym się świecie pracy i społeczeństwie. Są one kluczowe dla skutecznego funkcjonowania w przyszłości, umożliwiają podejmowanie decyzji, wykonywanie zadań w środowisku pracy i wspomagają osiąganie sukcesów zawodowych i osobistych.

Cel opracowania opisów profili kompetencji przyszłości:

- udostępnienie opisu profilu kompetencji jako narzędzia wsparcia w procesie kształtowania i walidacji kompetencji w edukacji formalnej na trzech poziomach: szkolnictwo podstawowe, szkolnictwo ponadpodstawowe i szkolnictwo wyższe,
- wspomaganie autodiagnozy posiadanych i oczekiwanych kompetencji od absolwentów poszczególnych poziomów edukacji formalnej w aspekcie podstawowych cech właściwych dla danej kompetencji przyszłości oraz punkt odniesienia do identyfikacji luk kompetencyjnych,
- zwrócenie uwagi na potrzebę drożności pionowej (między trzema poziomami edukacji formalnej) oraz korelacji efektów kształcenia w programach nauczania odnoszących się do kompetencji przyszłości,

- wsparcie dla doradców zawodowych (szkoły podstawowe i ponadpodstawowe), biur karier (szkoły wyższe) oraz doradców klienta (system publicznych służb zatrudnienia) przy udzielaniu porad oraz informacji indywidulanych i grupowych w wyborze kierunku kształcenia, ścieżki rozwoju czy zawodu,
- wskazanie obszarów doskonalenia zawodowego kadry (m.in. dyrektorzy szkół, nauczyciele, doradcy zawodowi, kadra B+R i inni przedstawiciele otoczenia społeczno-gospodarczego) uczestniczącej w procesie rozwoju kompetencji przyszłości dzieci, młodzieży i studentów w aspekcie rozwoju rekomendowanych metod kształtowania kompetencji oraz metod walidacji kompetencji przyszłości.

Struktura opisu profilu kompetencji przyszłości

Każdy z 10 profili kompetencji przyszłości posiada identyczną strukturę opisu, na którą składają się następujące elementy:

1) Wprowadzenie – informacja wspólna dla wszystkich 10 profili kompetencji przyszłości kierowana do różnych grup odbiorców korzystających z opisów profili kompetencji.
2) Nazwa danej kompetencji przyszłości wraz z ilustracją w formie graficznej (obraz i ikona kompetencji).
3) Definicje danej kompetencji przyszłości przyjętej w badaniu oraz dobranych dodatkowo w kontekście „edukacji", „psychologii" lub „społecznym" wraz z podaniem źródła definicji.
4) Podstawowy katalog cech osoby posiadającej daną kompetencję przyszłości, który pozwala budować kryteria weryfikacji, w jakim zakresie dana kompetencja została osiągnięta.
5) Rekomendowane metody stosowane w kształtowaniu danej kompetencji przyszłości zidentyfikowane w ramach badania diagnostycznego.
6) Dodatkowe metody wspomagające kształtowanie danej kompetencji przyszłości.
7) Rekomendowane metody stosowane w walidacji (ocenianiu) danej kompetencji przyszłości zidentyfikowane w ramach badania diagnostycznego.
8) Dodatkowe metody wspomagające walidację (ocenianie) danej kompetencji przyszłości.
9) Informacje do kontaktu.

CYBERBEZPIECZEŃSTWO

DEFINICJA KOMPETENCJI

Przyjęta w projekcie

Cyberbezpieczeństwo to kompetencja cyfrowa polegająca na umiejętności dostrzegania zagrożeń cyfrowych oraz ochrony i zabezpieczania danych

Źródło: Prognoza zapotrzebowania na kompetencje i kwalifikacje w wybranych branżach w związku ze zmianami w gospodarce, Warszawa 2023, Autorzy wiodący: dr Olena Shelest-Szumilas, dr hab. Piotr Trąpczyński.

W kontekście edukacji

Cyberbezpieczeństwo w kontekście edukacyjnym to proces kształcenia i podnoszenia świadomości w zakresie ochrony danych osobowych, bezpiecznego korzystania z internetu oraz identyfikacji i przeciwdziałania zagrożeniom w cyberprzestrzeni.

Źródło: European Commission. (2018). „Digital Education Action Plan".

W kontekście społecznym

Cyberbezpieczeństwo w kontekście społecznym obejmuje inicjatywy mające na celu ochronę jednostek, społeczności i instytucji przed zagrożeniami związanymi z cyberprzestrzenią, a także promowanie etycznego i bezpiecznego korzystania z technologii cyfrowej.

Źródło: European Union Agency for Cybersecurity (ENISA). (2019). „Cybersecurity Culture in Organizations".

CECHY OSOBY POSIADAJĄCEJ KOMPETENCJĘ

- **Skrupulatność.** Dokładność wykonywania działań zgodnie z zaleceniami i przepisami.
- **Zapobiegliwość**. Przewidywanie możliwych zagrożeń ze strony cyberprzestępców i staranie się zapobieganiu ich wystąpienia poprzez podejmowanie odpowiednich działań i decyzji.
- **Odpowiedzialność**. Świadomość konsekwencji dla otoczenia wynikających z własnych działań, które mogą mieć negatywny wpływ na cyberbezpieczeństwo, przestrzeganie zasad związanych z cyberbezpieczeństwem.

- **Dyskrecja**. Świadomość konieczności zachowania poufności w zakresie informacji mogących wpływać negatywnie na cyberbezpieczeństwo
- **Zapobiegliwość**. Możliwość działania nieszablonowego w nagłych sytuacjach zagrożenia w zakresie cyberbezpieczeństwa.
- **Logiczne myślenie.** Zdolność do analizowania, syntetyzowania i przetwarzania informacji nabywających z różnych kierunków i źródeł.
- **Komunikacja i współpraca.** Umiejętność wymiany informacji z zakresu cyberbezpieczeństwa i zrozumienia potrzeb innych w tym zakresie

METODY KSZTAŁTOWANIA KOMPETENCJI

Metody rekomendowane:

- **Burza mózgów** – angażująca wszystkich słuchaczy forma dyskusji pozwalająca doskonalić podejmowanie decyzji np. z zakresu cyberbezpieczeństwa.
- **Gry dydaktyczne (symulacyjne, decyzyjne, psychologiczne)** – stosowanie gier edukacyjnych jako metody symulacji angażuje słuchaczy w interaktywne scenariusze pozwalające na odtwarzanie rzeczywistych, zaistniałych sytuacji w zakresie cyberbezpieczeństwa i odniesienie rezultatów do rozwiązań rzeczywistych.
- **Prezentacja, film** – multimedialny przekaz pozwalający oddziaływać na odbiorcę różnymi bodźcami co wpływa korzystnie na utrwalenie poruszanych zagadnień z zakresu cyberbezpieczeństwa przez słuchaczy.
- **Metoda projektów** (np. puzzle tematyczne, kolaże, tablice informacyjne, filmiki, blogi i vlogi uczniowskie) – pozwala zaangażować słuchaczy bezpośrednio w pracę nad tematem cyberbezpieczeństwa co pozwala doskonalić ich działania w zakresie tej kompetencji.
- **Interaktywne quizy** – pozwalają na wprowadzenie w grupie słuchaczy elementu rywalizacji, a zastosowanie elementów multimedialnych podnosi atrakcyjność zajęć z zakresu cyberbezpieczeństwa. Istnieje możliwość szybkiego wyświetlenia statystyk przeprowadzonego quizu

Metody dodatkowe:

- **Zajęcia praktyczne w grupach** – kreowanie sytuacji, w których uczniowie mogą rozwiązywać problemy z zakresu cyberbezpieczeństwa w bezpiecznym otoczeniu grupy.

METODY WALIDACJI KOMPETENCJI

Metody rekomendowane:

- **Test praktyczny / próba pracy** – pozwala na przeprowadzenie kompleksowego działania słuchacza w zakresie zaplanowanych zadań z cyberbezpieczeństwa.
- **Obserwacja w warunkach rzeczywistych** – pozwala na analizowanie działań słuchacza w rzeczywistych warunkach w zakresie postawionych problemów z cyberbezpieczeństwa
- **Test kompetencyjny** – pozwala na sprawdzenie kompetencji słuchacza w zakresie cyberbezpieczeństwa
- **Obserwacja w warunkach symulowanych** – pozwala na analizę działań słuchacza w zakresie cyberbezpieczeństwa w warunkach imitujących rzeczywistą sytuację, stworzonych do przeprowadzenia walidacji
- **Wywiad swobodny** – swobodna rozmowa ze słuchaczem na temat cyberbezpieczeństwa pozwalająca na obszerne wypowiedzi osoby przystępującej do walidacji.

Dodatkowe metody zalecane przez ekspertów

- **Ankiety i kwestionariusze** – zbieranie subiektywnych opinii na temat kompetencji cyfrowych w tym cyberbezpieczeństwa.
- **Autoocena i refleksja** – samopoznanie, świadomość własnych mocnych stron i obszarów do poprawy w zakresie cyberbezpieczeństwa.

INFORMACJE DO KONTAKTU

Sieć Badawcza Łukasiewicz – Instytut Technologii Eksploatacji
https://www.itee.lukasiewicz.gov.pl/

Centrum Badań Edukacji Zawodowej i Zarzadzania Innowacjami
https://www.itee.lukasiewicz.gov.pl/obszary/centrum-badan-edukacji-zawodowej-i-zarzadzania-innowacjami