Co-funded by the European Union

# STRUKTURA ŚCIEŻKI NAUKI AGENTÓW ZMIAN W ZAKRESIE CYBERBEZPIECZEŃSTWA W MŚP

CYBER AGENT 06.2024

**Call: ERASMUS-EDU-2022-PI-ALL-INNO**
**Type of Action: ERASMUS-LS**
**Project No. 101111732**

Pakiet roboczy 2: Podejście i projekt struktury CyberAgent

Element dostarczany 2.3: Struktura ścieżki nauki agentów zmian w zakresie cyberbezpieczeństwa w MŚP.

Lider of WP2 – Olemisen Balanssia ry
Lider produktu 2.3 – Vilnius University

# SPIS TREŚCI

## SKRÓTY

CBL – Model uczenia się oparty na wyzwaniach

CL – Model uczenia się opartego na współpracy

EC – Komisja Europejska

ECTS – Europejski System Transferu I Akumulacji Punktów

ERK – Europejskie Ramy Kwalifikacji

GICL – Model uczenia się opartego na współpracy z dociekaniem kierowanym

HEI – Uczelnie

PBL – Model nauczania opartego na projektach

POGIL – Zorientowany na proces model uczenia się z kierowanym dociekaniem

MŚP – Małe i średnie przedsiębiorstwa

VET – Placówki Kształcenia Zawodowego

## SPIS FIGUR



## SPIS TABEL

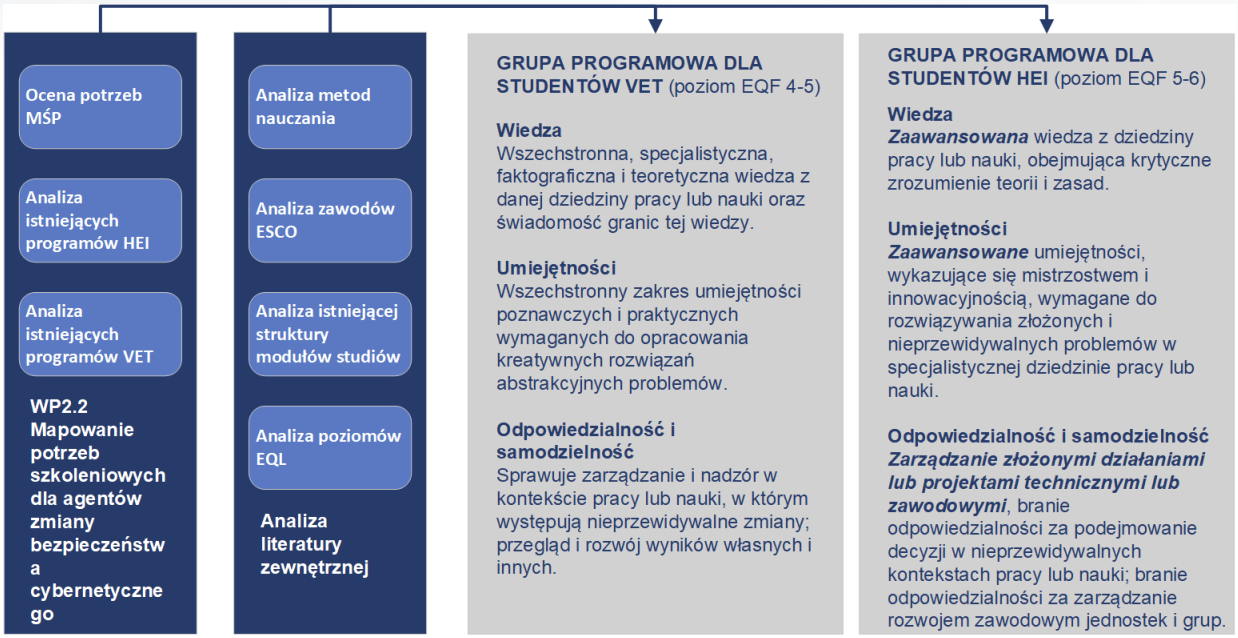
# WPROWADZENIE

Ogólnym celem niniejszego sprawozdania jest opracowanie i opisanie nowych ścieżek kształcenia zawodowego służących podnoszeniu umiejętności w zakresie cyberbezpieczeństwa wśród pracowników europejskich MŚP (małych i średnich przedsiębiorstw).

Na podstawie ustaleń z mapowania potrzeb szkoleniowych dla agentów zmian w zakresie cyberbezpieczeństwa MŚP zidentyfikowano analizę efektów uczenia się pod kątem wiedzy, umiejętności i kompetencji pod kątem zasobów zewnętrznych. Po przeanalizowaniu zidentyfikowanych efektów uczenia się, niniejszy raport zawiera wytyczne dotyczące dwóch rodzajów programów szkoleniowych od poziomu 4 do 6 ERK (Europejskich Ram Kwalifikacji), aby objąć zakres umiejętności i wiedzy wymaganych od grup docelowych projektu, pracowników MŚP i studentów oraz dostosować wyniki szkolenia do różnych środowisk i profili uczestników.

- Poziom 4-5 ERK zostanie wdrożony dla pracowników MŚP nieposiadających wykształcenia w szkolnictwie wyższym, a także studiów VET (kształcenia i szkolenia zawodowego). Poziom ten zapewni podstawowe umiejętności i wiedzę z zakresu cyberbezpieczeństwa z podstawową specjalizacją w niektórych modułach.
- Poziom 5-6 ERK, który będzie ofertą dla pracowników MŚP, którzy mają również odpowiednie przygotowanie, aby go realizować, oraz studentów uczelni wyższych. Na tym poziomie prowadzone będą bardziej zaawansowane i złożone działania szkoleniowe.

Zdecydowano się na aktualizację poziomów ERK do 4-6 nie tylko w celu uwzględnienia szerokiego zakresu efektów uczenia się, jak wspomniano wcześniej, ale także w celu umożliwienia przejścia między programami szkoleniowymi jako ścieżki podnoszenia umiejętności dla studentów i pracowników kształcenia i szkolenia zawodowego na poziomie 4 w celu osiągnięcia poziomu 6.




***Rysunek 1. Diagram ilustracyjny, zgodny z wytycznymi EC, przedstawia osiem poziomów ERK, zapewniając wizualną reprezentację ram kształcenia.[1]***

Program nauczania odnosi się do efektów uczenia się i potrzeby szkolenia pracowników MŚP w celu podnoszenia kwalifikacji w celu pełnienia roli agentów ds. zmian w zakresie cyberbezpieczeństwa MŚP oraz kształcenia studentów uczelni i kształcenia i szkolenia zawodowego w celu pełnienia tej roli po zakończeniu studiów. Każdy program nauczania składa się z ośmiu modułów obejmujących cztery podtematy:

- Umiejętności techniczne - Aktualna wiedza na temat zagrożeń cyberbezpieczeństwa i związanych z nimi zagadnień prawnych - Praktyczna wiedza na temat radzenia sobie z zagrożeniami cyberbezpieczeństwa.
- Umiejętności analityczne - Nastawienie na krytyczne myślenie - Umiejętność analizowania i rozumienia lokalnych zagrożeń, sposobu ich powstawania, osób zagrożonych itp.
- Zarządzanie ryzykiem - Dowiedz się, jak zapewnić i opisać miejsca pracy dla MŚP za pomocą procedur cyberbezpieczeństwa - Stwórz własny podręcznik dla MŚP w zakresie cyberbezpieczeństwa w miejscu pracy i dowiedz się, jak go śledzić.
- Umiejętności organizacyjne – jak wdrażać nowe procedury i sposoby pracy w cyberbezpieczeństwie w miejscach pracy MŚP; Prowadzenie wsparcia lidera w zakresie cyberbezpieczeństwa.

Ponadto centralnym elementem tworzenia ścieżek edukacyjnych służących podnoszeniu umiejętności w zakresie cyberbezpieczeństwa wśród europejskich MŚP jest sposób wdrażania mikropoświadczeń. Muszą one odnosić się do efektów uczenia się (wiedzy, umiejętności i kompetencji), treści kursu, szkolenia (wiedzy, umiejętności i kompetencji), elementów grywalizacji, czasu trwania i liczby ECTS (Europejskiego Systemu Transferu i Akumulacji

[1] https://europa.eu/europass/en/description-eight-eqf-levels

Punktów). Aby osiągnąć ten cel, należy je realizować poprzez ustanowienie partnerstw między instytucjami szkolnictwa wyższego a organizatorami kształcenia i szkolenia zawodowego oraz prywatnymi przedsiębiorstwami z sektora cyberbezpieczeństwa.

Mikrosekcje zapewniają uczącym się większą swobodę w wyborze modułów lub części modułów oraz w decydowaniu, jakiego poziomu certyfikatu potrzebują: certyfikatów uczestnictwa lub certyfikatu ukończenia kursu z testem certyfikacyjnym, czyli dowodu, że kurs został ukończony wraz z nabyciem określonej kompetencji. Certyfikaty ukończenia kursu są wydawane za zdanie testu końcowego z wynikiem co najmniej 75%, a certyfikaty uczestnictwa są wydawane za udział w szkoleniu bezpośrednim, mieszanym lub online w określonych tematach/modułach. Praktyka ta nie tylko zwiększa przydatność i skuteczność szkolenia, ale także stymuluje motywację do nauki, zapewniając jasną perspektywę wartości dla kariery i dalszego rozwoju uczestników.

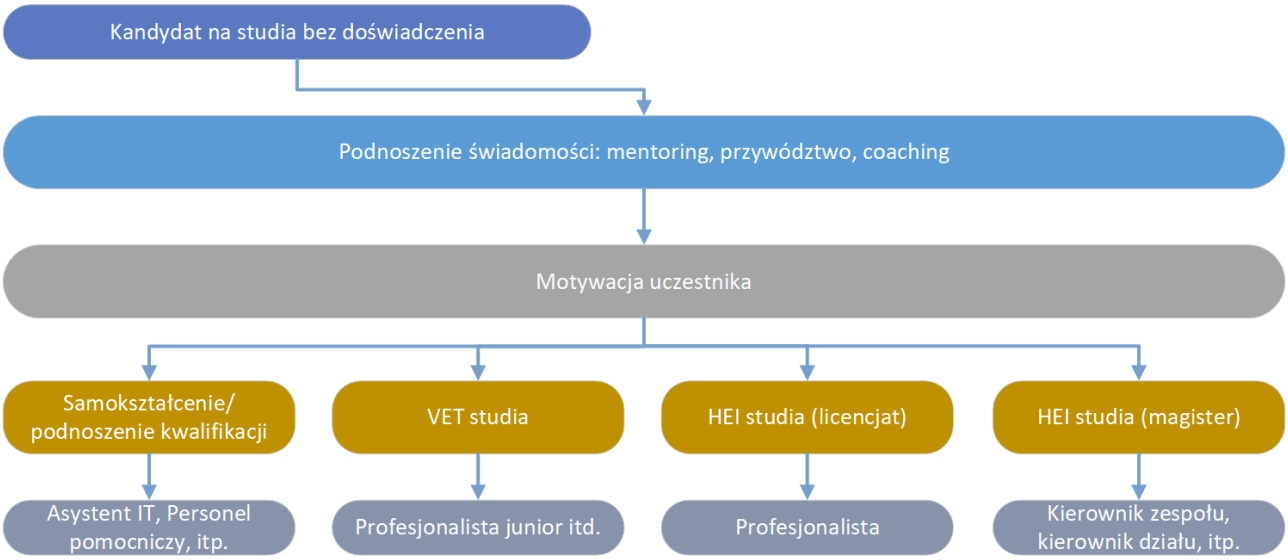
Ogólnie rzecz biorąc, niniejszy raport przedstawia szczegółowe wytyczne dotyczące rozwoju modułów CyberAgent, w tym zarys treści ścieżek studiów i kariery, metodologie szkolenia i oceny oraz plan budowy programu nauczania.

# 1. ŚCIEŻKA NAUKI

Ścieżka uczenia się to cała podróż, którą uczestnik odbywa od momentu, w którym zdaje sobie sprawę, że musi poprawić umiejętności, rozpocząć i ukończyć szkolenie, do momentu, w którym zakończy naukę i zacznie stosować otrzymaną wiedzę. Ścieżka edukacyjna składa się z 3 etapów:

- Wstępne nauczanie,
- Uczenie się
- Nauka końcowa.

Etap wstępnego uczenia się zilustrowano na poniższym rysunku.




***Rysunek 2. Ścieżka nauki przed rozpoczęciem studiów***

W kontekście MŚP ta ścieżka uczenia się/studiowania może być kontynuowana. Na rysunku uczestnik albo decyduje się na samodzielne szkolenie, albo jest pod wpływem kampanii uświadamiającej i zyskuje wiedzę na temat korzyści płynących ze szkolenia, możliwości i kariery, które można zdobyć po szkoleniu.

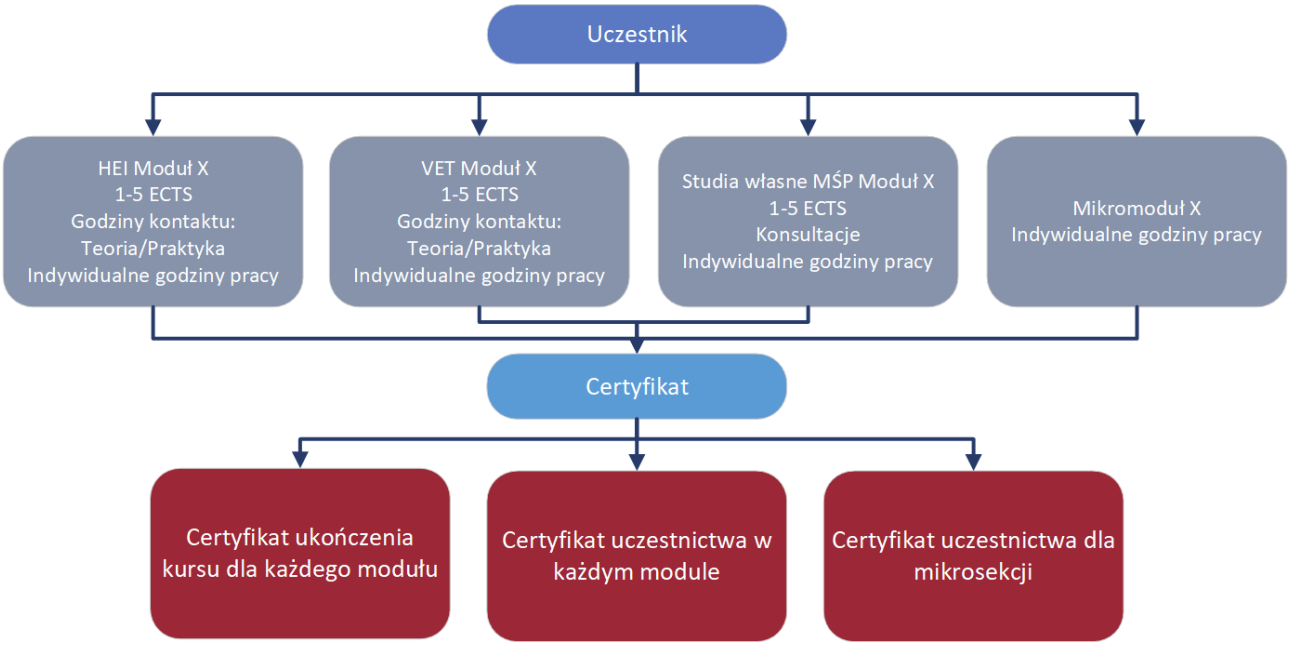
Zaproponowano również ścieżkę edukacyjną jako typowy moduł poprzez strukturę OLE (Online Learning Environment). Po analizie literatury i kilku projektach wykorzystujących zasadę mikropoświadczeń[2,3],[4] każdy moduł CyberAgent ma mieć 1-5 punktów ECTS (każdy ECTS to 25-30 godzin pracy) i rozpoczyna się wprowadzeniem, a następnie jest podzielony na tematy, które są podtematami.

[2] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Idąc naprzód i dalej w edukacji: koncepcja ELASTYCZNYCH ŚCIEŻEK UCZENIA SIĘ. W KTU leidykla "Technologija" eBooki. https://doi.org/10.5755/e01.9786090218204

[3] https://argus-alliance.eu/call/argus-microcredential-development-f2f-workshop/

[4] https://www.youtube.com/watch?v=ECH0VvHIyRI, https://ndma.lt/alta2023/

Na końcu tematów podany jest test samooceny składający się z kilku pytań. Materiały szkoleniowe modułu powinny wspierać naukę 6-8 tematów, z których każdy składa się z 4-6 podtematów. Kurs może zakończyć się testem wiedzy, który nie jest obowiązkowy. Daje to pracownikom MŚP i studentom instytucji szkoleniowych możliwość nabycia i wykazania się kompetencjami zdobytymi w konkretnym module lub części szkolenia.




Rysunek 3. Struktura studiów

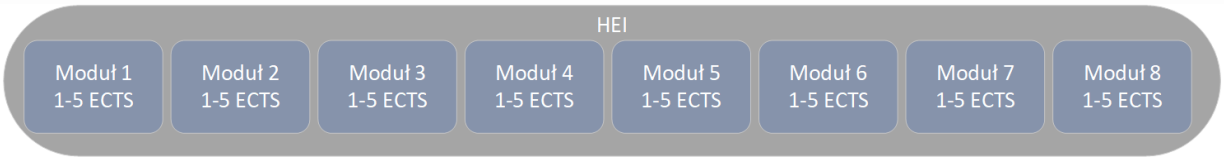
Mikropoświadczenia są włączane do procesu uczenia się poprzez następujące kluczowe działania:

- Opracowanie modułów szkoleniowych: każdy moduł musi być starannie sformułowany, biorąc pod uwagę specyficzną wiedzę i umiejętności wymagane w sektorze MŚP, z jasnymi celami, efektami uczenia się, metodami nauczania i uczenia się, czasem trwania kursu.
- Praktyczne zadania i projekty: osoby uczące się wykonują zadania praktyczne i opracowują projekty, które są oceniane i stanowią wyraźny dowód nabytych umiejętności.
- Jasno opisana strategia oceny wiedzy i kryteria oceny: na koniec każdego modułu organizowana jest ocena wiedzy w celu ustalenia, czy uczestnik osiągnął wymagane efekty uczenia się i czy kwalifikuje się do uzyskania certyfikatu potwierdzającego to.

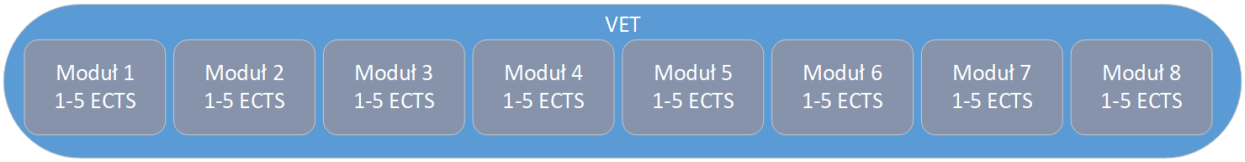
Ponieważ grupą docelową projektu są pracownicy MŚP, studenci uczelni wyższych i kształcenia i szkolenia zawodowego, dostępne są cztery rodzaje studiów, w zależności od możliwości i potrzeb osób uczących się:

- studia na uczelniach: 8 modułów, każdy 1-5 ECTS, w których są godziny kontaktowe (teoria i praktyka) oraz indywidualne godziny pracy;
- Studia VET: 8 modułów, każdy 1-5 ECTS, w których są godziny kontaktowe (teoria i praktyka) oraz indywidualne godziny pracy;
- Samodzielna nauka (dla MŚP): 8 modułów, każdy 1-5 ECTS, w których odbywają się konsultacje (w razie potrzeby) i indywidualne godziny pracy;

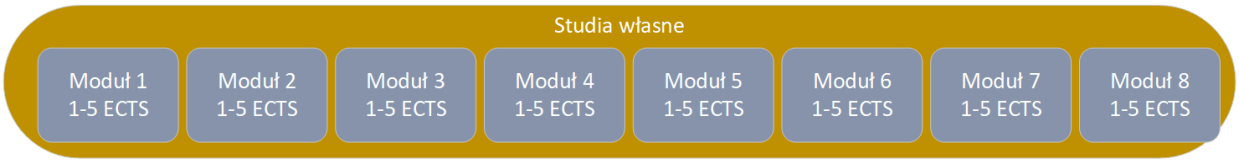
- Mikromoduły: indywidualna godzina pracy zależna od ilości wybranych tematów.



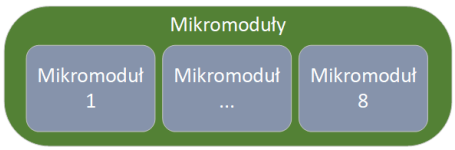

***Rysunek 4. Struktura studiów w uczelni***




***Rysunek 5. Struktura studiów dla kształcenia i szkolenia zawodowego***

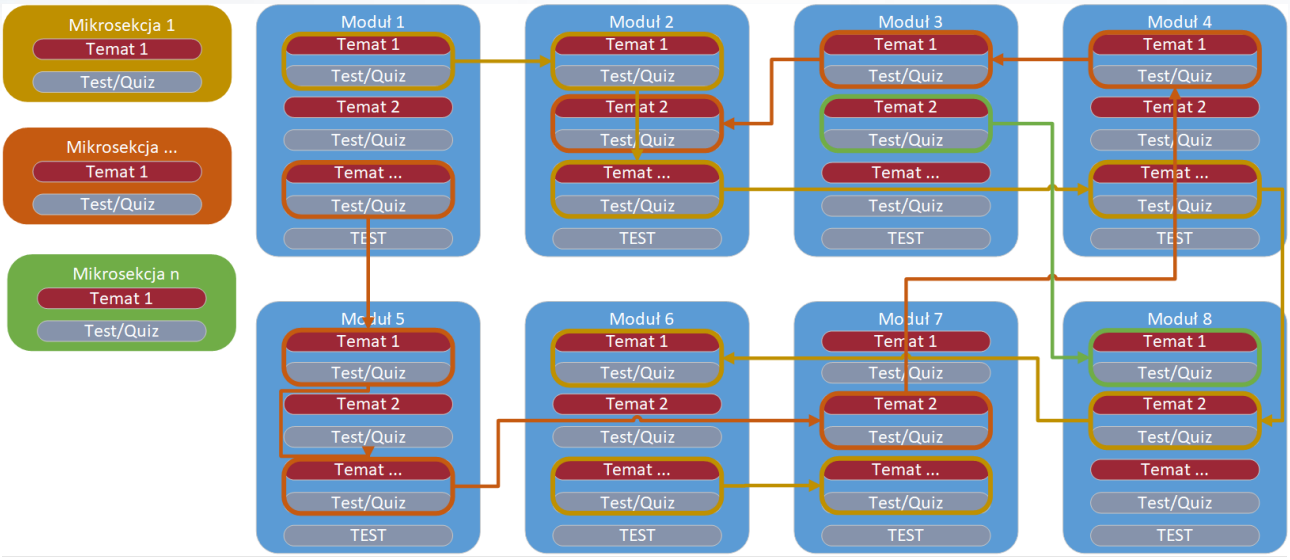



***Rysunek 6. Struktura studiów dla samodzielnej nauki***




***Rysunek 7. Struktura studiów dla mikromodułu***

Studenci uczelni wyższych i kształcenia i szkolenia zawodowego będą mogli studiować jeden moduł po 1-5 punktów każdy. MŚP będą mogły wziąć udział w jednym module na raz lub możemy zaoferować mikrosekcje w ramach kursu.




***Rysunek 8. Powiązania ścieżek szkoleniowych***

We wszystkich trzech typach kształcenia (uczelnie, kształcenie i szkolenie zawodowe, MŚP) student studiuje 8 modułów. W przypadku mikromodułów, uczeń wybiera moduły według własnego wyboru.

Mikromoduły to krótkie lub długie, przejrzyście oceniane doświadczenia edukacyjne. Uczestnik podejmuje je razem z wyzwaniem lub osobno. Każdy mikromoduł jest wyceniany za pomocą innej miary obciążenia nauką (np. ECTS) i kończy się oceną. Pomyślne ukończenie oceny mikromodułowej nagradza uczniów mikropoświadczeniami.

Propozycja jest taka, że każdy moduł z programu szkolnictwa wyższego może być podzielony na moduły w jeden mikromoduł, z których każdy zawiera specjalistyczne zadania i szczegółowy plan wdrożenia. Wyniki testów można oceniać za pomocą identyfikatorów, które są oparte na obrazach i powszechnie czytelne dla komputerów. Obrazy te zawierają metadane wyszczególniające kompetencje związane z każdą odznaką oraz informacje o uczestniku, który ją posiada.

Mikropoświadczenie oznacza zapis efektów uczenia się, które uczestnik uzyskał po przeprowadzeniu niewielkiej liczby badań. Te efekty uczenia się będą oceniane według przejrzystych i jasno określonych kryteriów. Doświadczenia edukacyjne prowadzące do uzyskania mikropoświadczeń mają na celu dostarczenie uczestnikowi konkretnej wiedzy, umiejętności i kompetencji, które odpowiadają potrzebom społecznym, osobistym, kulturowym lub na rynku pracy.[5,6].

[5] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Idąc naprzód i dalej w edukacji: koncepcja ELASTYCZNYCH ŚCIEŻEK UCZENIA SIĘ. W KTU leidykla "Technologija" eBooki. https://doi.org/10.5755/e01.9786090218204

[6] Zalecenie Rady z dnia 16 czerwca 2022 r. w sprawie europejskiego podejścia do mikropoświadczeń do celów uczenia się przez całe życie i zwiększania szans na zatrudnienie. Dziennik Urzędowy Unii Europejskiej, tom 2022/C, 16 czerwca 2022 r., https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(02)&from=PL

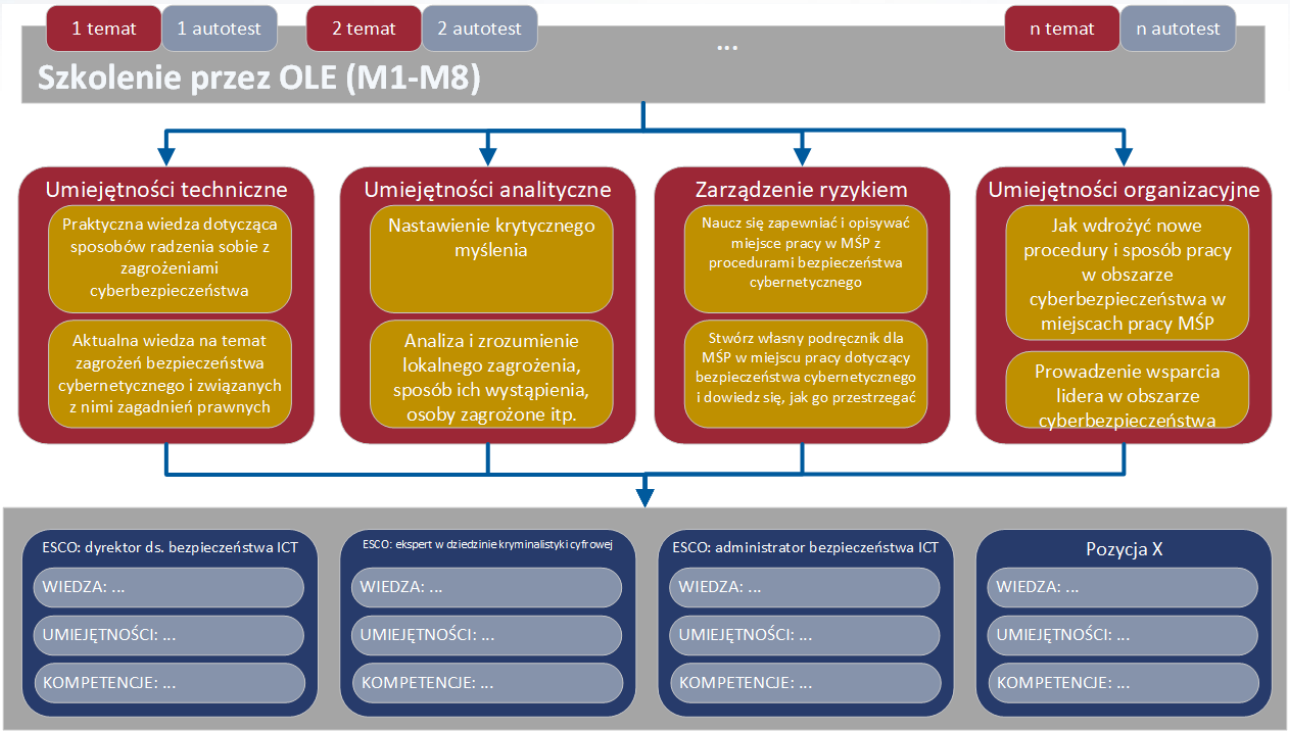
## 2. ŚCIEŻKA KARIERY

Ścieżkę po nauczaniu można nazwać ścieżką kariery. Na początku projektu przeprowadzono analizę badawczą zawodów ESCO (opisanych w raporcie: D2.2 - Raport mapowania potrzeb szkoleniowych agentów zmian w zakresie cyberbez-pieczeństwa w MŚP.). Analiza przeprowadzona w trzech fazach miała na celu zbadanie różnych zawodów związanych z cyberbezpieczeństwem wymienionych w ramach ESCO. W pierwszej fazie zawody związane z cyberbezpieczeństwem zostały zidentyfikowane i udokumentowane na **portalu ESCO**, podkreślając ich umiejętności, kompetencje i wiedzę. Zawody te obejmowały takie stanowiska, jak dyrektor ds. bezpieczeństwa ICT, ekspert ds. kryminalistyki cyfrowej, inżynier ds. bezpieczeństwa systemów wbudowanych, etyczny haker, menedżer ds. odporności ICT, administrator bezpieczeństwa ICT, inżynier bezpieczeństwa ICT, kierownik ds. bezpieczeństwa ICT i inżynier wiedzy. Każdy zawód został zdefiniowany przez jego konkretne obowiązki i obszary zainteresowania w dziedzinie cyberbezpieczeństwa, począwszy od funkcji bezpieczeństwa korporacyjnego, a skończywszy na kryminalistyce cyfrowej, etycznym hakowaniu i planowaniu odporności.

W drugiej fazie dla każdego analizowanego zawodu ESCO wypełniono tabelę, wyszczególniając jego nazwę i podstawowe obowiązki. Obejmowały one takie zadania, jak planowanie i wdrażanie środków bezpieczeństwa, przeprowadzanie ocen podatności na zagrożenia, opracowywanie modeli odporności i odzyskiwania danych po awarii oraz integrowanie wiedzy z systemami komputerowymi.

Ponadto trzecia faza obejmowała mapowanie zawodów ESCO wraz z powiązanymi efektami uczenia się, kategoryzując je na wiedzę, umiejętności i kompetencje. Proces ten ułatwił kompleksowe zrozumienie wymagań edukacyjnych i oczekiwanych biegłości dla każdej roli w zakresie cyberbezpieczeństwa, zapewniając zgodność ze standardami branżowymi i najlepszymi praktykami. Na tych etapach analiza dostarczyła cennych informacji na potrzeby dalszych badań.


***Rysunek 9. Zawody ESCO zdefiniowane w poprzednim raporcie***




***Rysunek 10. Możliwe ścieżki po zakończeniu nauki***

Na rys. 10 przedstawiono potencjalne ścieżki kariery, które można realizować po ukończeniu studiów za pośrednictwem OLE (Online Learning Environment) (HEI, VET, MŚP) i nabyciu umiejętności, zgodnie z zawodami ESCO.

Dzięki lepszemu zrozumieniu możliwości kariery studenci uczelni i kształcenia i szkolenia zawodowego studiujący cyberbezpieczeństwo zyskają lepsze zrozumienie możliwości kariery i będą mogli wybrać dalszy kierunek studiów lub pracować w firmach na określonych stanowiskach, podczas gdy studenci IT i inni będą mogli wybrać moduły CyberAgent jako indywidualne moduły studiów, podnosząc w ten sposób swoje kompetencje w zakresie studiów. takie jak umiejętności organizacyjne i umiejętności zarządzania ryzykiem itp.

Pracownicy MŚP będą mieli możliwość podnoszenia kwalifikacji i rozwijania swoich kompetencji w miejscu pracy. W oparciu o opracowaną ścieżkę kariery i jasne możliwości rozwoju kariery inni pracownicy MŚP będą mogli przekwalifikować się w dziedzinie cyberbezpieczeństwa.

Planowane jest zwiększenie zaangażowania zarówno studentów, jak i kadry MŚP poprzez integrację programów mentoringowych, organizację wydarzeń upowszechniających, warsztatów (projekt obejmuje 6 wspólnych warsztatów organizowanych przez wszystkich partnerów, a także kampanie upowszechniające organizowane przez każdego z partnerów), zapraszanie przedstawicieli biznesu i cyberbezpieczeństwa, współpracę z partnerami społecznymi i siecią CyberAgent, oferowanie staży studentom, itd. Ponadto nasze inicjatywy na rzecz różnorodności, w tym ukierunkowane programy informacyjne i wsparcia, mają na celu zwiększenie udziału kobiet, wspierając inkluzywną siłę roboczą zajmującą się cyberbezpieczeństwem.

Dzięki kompleksowemu mapowaniu zawodów ESCO do naszych modułów szkoleniowych CyberAgent, uczestnicy mogą płynnie przechodzić ze środowisk edukacyjnych do wpływowych ról w cyberbezpieczeństwie. Aby śledzić rozwój kariery stażystów CyberAgent, planowane jest zorganizowanie ankiet przedszkoleniowych, poszkoleniowych i 3-miesięcznych ankiet poszkoleniowych, aby dowiedzieć się, w jaki sposób ich umiejętności przyczyniają się do cyberbezpieczeństwa organizacji, w których pracują. Ankiety zostaną zintegrowane z platformą szkoleniową i będą automatycznie oferowane uczestnikom przed rozpoczęciem kursu, po jego zakończeniu, w celu zmierzenia postępów oraz oceny kursu i jakości szkolenia. Trzecia ankieta zostanie wykorzystana, aby dowiedzieć się, czy nastąpiły jakieś zmiany w karierze uczestników.

## 3. METODY NAUCZANIA

Analiza metod pedagogicznych programu studiów Systemy Informacyjne i Cyberbezpieczeństwo Uniwersytetu Wileńskiego (VU), programów studiów Timtal i Moisil Buzau oraz literatury zewnętrznej pozwala nam zarekomendować kilka innowacyjnych kombinacji metod nauczania. Kombinacje te można zawrzeć w modułach studiów, biorąc pod uwagę strukturę każdego modułu.[7]

***Tabela 1. Rekomendowane metody nauczania***

| Kategoria | Szczegółowe informacje |
|---|---|
| **Wykład i bezpośrednie instrukcje** | - **Wykłady teoretyczne:** podstawowe pojęcia i teorie.<br>- **Zaproszeni prelegenci** ((certyfikowani specjaliści w zakresie: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), CompTIA Security+, Certified Ethical Hacker (CEH), GIAC Security Essentials Certification (GSEC), Systems Security Certified Practitioner (SSCP), CompTIA Advanced Security Practitioner (CASP+), GIAC Certified Incident Handler (GCIH), Offensive Security Certified Professional (OSCP))). |
| **Praktyka i praktyczna nauka** | - **Zadania praktyczne/laboratoria:** praktyczne eksperymenty i ćwiczenia praktyczne.<br>- **Zajęcia praktyczne**: rzeczywiste aplikacje i interaktywne zadania.<br>- **Techniczna analiza wideo:** analiza treści wideo w celu nauki umiejętności technicznych.<br>- **Symulowane środowiska**:<br>  o Hostowane maszyny dla środowiska chmury.<br>  o Przeprowadzanie ataków na maszynę docelową.<br>  o Maszyna do planowania i wykonywania ataków – skrzynka ataku. |

[7] Nauczanie cyberbezpieczeństwa: podejście do uczenia się opartego na projektach i kierowanego dociekania https://scholar.utc.edu/cgi/viewcontent.cgi?article=1945&context=theses https://scholar.utc.edu/cgi/viewcontent.cgi?article=1945&context=theses

| Kategoria | Szczegółowe informacje |
|---|---|
| **Ocena i ewaluacja** | - **Quizy, gry, nakazy i zakazy**: angażujące i interaktywne oceny.<br>- **Testy samooceny**: Do samooceny ucznia na końcu tematów. |
| **Samodzielna nauka** | - **Samodzielna nauka:** ta metoda obsługuje spersonalizowane ścieżki edukacyjne i może być wzbogacona o zasoby cyfrowe i treści modułowe, do których uczniowie mają dostęp w razie potrzeby. |
| **Uczenie się oparte na współpracy i partnerstwie** | - **Uczenie się oparte na współpracy, praca zespołowa**: projekty grupowe i zadania zespołowe.<br>- **Nauczanie i uczenie się jak równy z równym**: uczniowie uczą się i uczą się od siebie nawzajem.<br>- **Mentoring grupowy i/lub mentoring indywidualny**: wskazówki udzielane przez bardziej doświadczone osoby. |
| **Nauka wspomagana technologią** | - **Wykorzystanie gamifikowanej platformy edukacyjnej w zakresie cyberbezpieczeństwa**: angażowanie uczniów poprzez elementy podobne do gier na platformach edukacyjnych.<br>- **Konkursy Capture the Flag**: konkurencyjne wydarzenia mające na celu zwiększenie umiejętności w zakresie cyberbezpieczeństwa.<br>- **Konkursy**: konkursy sprawdzają umiejętności i wiedzę uczniów w praktycznym, praktycznym otoczeniu i stanowią miarę ich kompetencji w formie konkursu. |
| **Wspólnota i zaangażowanie społeczne** | - **Wydarzenia edukacyjne:** wydarzenia specjalne podczas inicjatyw takich jak Miesiąc Cyberbezpieczeństwa.<br>- **Prezentacje publiczne**: seminaria, konferencje i webinaria.<br>- **Sieci społecznościowe**: wykorzystanie mediów społecznościowych i sieci do uczenia się i angażowania. |

| Kategoria | Szczegółowe informacje |
|---|---|
| | - **Kampus dzienny**: zazwyczaj obejmuje wciągające wydarzenia na terenie kampusu, które mogą obejmować warsztaty, wykłady i możliwości networkingu |
| **Innowacyjne modele uczenia się** | - **Model instruktażowy BSCS 5E (5E)** – 5E koncentruje się na następujących fazach, na które składają się: Zaangażowanie, Eksploracja, Wyjaśnienie, Opracowanie, Ocena.<br>- **Model uczenia się oparty na wyzwaniach (CBL)** – wczesne wdrożenie CBL zapewnia ramy, które składają się z sześciu faz: Opisz wyzwanie, Generowanie i burza mózgów pomysłów, Przegląd wielu perspektyw, które kwestionują i wspierają, Badaj i poprawiaj w poszukiwaniu najlepszych rozwiązań, Testuj hipotezę, Podziel się ustaleniami i wnioskami.<br>- **Model uczenia się opartego na współpracy (CL)** – podobnie jak modele 5E i CBL, uczenie się oparte na współpracy promuje aktywne uczenie się w małych grupach, a uczniowie otrzymują nagrodę na podstawie swoich wyników, która może obejmować ocenę, namacalną nagrodę, taką jak certyfikat lub stypendium, lub aprobatę nauczyciela.<br>- **Model uczenia się oparty na projektach (PBL)** – uczenie się oparte na projektach i uczenie się oparte na problemach używają tego samego skrótu PBL i oba koncentrują się na poprawie rozwiązywania problemów, krytycznego myślenia, pracy zespołowej, komunikacji i umiejętności twórczych; jednak składają się z różnych faz., Badania niezależne i grupowe, Rozwijaj i prezentuj, Analizuj i oceniaj proces.<br>- **Zorientowany na proces model uczenia się z kierowanym dociekaniem (POGIL)** – podejście to prowadzi uczniów przez eksplorację koncepcji, po której następuje wymyślanie koncepcji, w której uczniowie syntetyzują i wyjaśniają koncepcję, a także zamyka cykl uczenia się z zastosowaniem koncepcji teoretycznej. |

| Kategoria | Szczegółowe informacje |
|---|---|
| | - **Model uczenia się opartego na współpracy z dociekaniem kierowanym (GICL)** – to nowe podejście w dużej mierze oparte na modelu POGIL. |

Aby zapewnić jak najlepszy wpływ różnych oferowanych strategii szkoleniowych, każde podejście zostanie wybrane i dostosowane do konkretnych celów edukacyjnych modułów cyberbezpieczeństwa przy opracowywaniu kompleksowego programu nauczania modułów i materiałów szkoleniowych. Dodatkowe metody mogą być również wybrane przez wykładowców/mentorów, którzy będą prowadzić szkolenie z obsługi CyberAgenta. W fazie opracowywania materiałów szkoleniowych instruktorzy szkoleń pilotażowych zostaną przeszkoleni w celu poinformowania ich o celach, procesie i odpowiedzialności szkolenia oraz przygotowania ich do skutecznego nauczania programu nauczania CyberAgent. Pilotażowy proces szkoleniowy obejmuje również gromadzenie informacji zwrotnych od osób uczących się i trenerów w celu monitorowania skuteczności stosowanych metod szkoleniowych i wprowadzania korekt w razie potrzeby.

Moduły będą prowadzone w różnych formach nauczania:

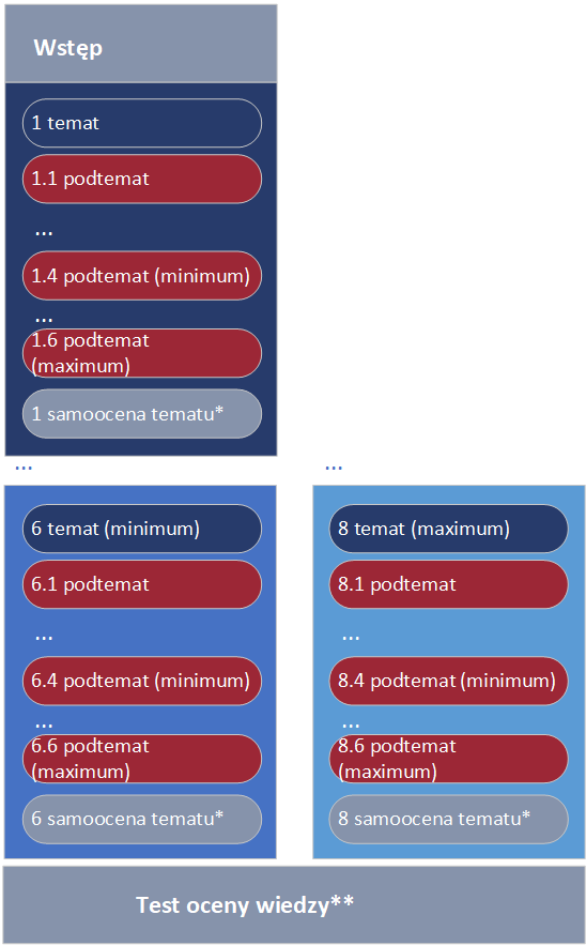
- w **formacie zdalnym**,
- w **nauczaniu synchronicznym** (pełne wsparcie nauczyciela),
- oraz w **nauczaniu asynchronicznym** (wsparcie nauczyciela w razie potrzeby), nauczaniu mieszanym i samokształceniu.

Ponieważ przewiduje się różne sposoby prowadzenia szkolenia, metody szkoleniowe są przedstawiane na tym etapie jako wytyczne.

## 4. STRUKTURA MODUŁU

Analiza struktury modułowej programu studiów VU Cyber security, analiza struktury modułowej projektów międzynarodowych (**CyberPhish**, **FuseIT, dComFra**) oraz analiza struktury modułowej platform komercyjnych, takich jak **Udemy** i **Coursera**, doprowadziła do stworzenia typowej struktury modułowej, która może być zastosowana zarówno do modułów szkolnictwa wyższego, jak i kształcenia i szkolenia zawodowego.

Głównym celem jest opracowanie 8 modułów, z których 8 byłoby przeznaczonych dla studentów uczelni wyższych (poziom 5-6 ERK), dla studentów kształcenia i szkolenia zawodowego oraz MŚP (poziom 4-5 ERK) oraz mikromodułów dla wszystkich typów studentów.




***Rysunek 11. Struktura modułu***

* Zaleca się, aby po każdym podtemacie następowały pytania do autotestu (autorefleksji). Jednak na etapie opracowywania modułu można wybrać inną metodę lub opcję oceniania w zależności od wybranego rodzaju studiów, np. studenci mogą otrzymać ćwiczenia praktyczne, symulacje itp., podczas gdy pytania do samodzielnego testu są oferowane samodzielnym uczniom.

** Test sprawdzający wiedzę jest opcjonalny. Jeśli osoba ucząca się chce uzyskać certyfikat ukończenia kursu w celu weryfikacji zdobytej wiedzy, test ten jest obowiązkowy. Uczeń ma jednak

możliwość uzyskania certyfikatu ukończenia kursu, aby udowodnić, że uczestniczył w szkoleniu, w którym to przypadku test ten jest opcjonalny.

Aby zapewnić, że każdy moduł szkoleniowy jest bezpośrednio powiązany z praktycznym zastosowaniem, opis każdego modułu będzie zawierał jasne przykłady zastosowania teorii w praktyce. Obejmuje to nie tylko szczegółowe scenariusze zastosowania modułów, ale także konkretne zadania, które studenci podejmą, aby utrwalić wiedzę teoretyczną w rzeczywistych sytuacjach cyberbezpieczeństwa.

Każdy moduł powinien zapewniać umiejętności techniczne, umiejętności analityczne, umiejętności zarządzania ryzykiem, umiejętności organizacyjne o różnych proporcjach. Test samooceny służy do sprawdzenia wiedzy uczniów na końcu dowolnej części modułu (tematu). Pozwala to nie tylko na ocenę czy ewaluację zdobytej wiedzy, ale także rejestrowane są postępy ucznia, a uczestnik zbiera punkty i odznaki, co pozwala uczestnikowi na większe zaangażowanie w proces uczenia się.

Spełnienie formalności ECTS, gdzie każdy ECTS to 25-30 godzin pracy. Zgodnie z tym każdy moduł może być równy 5 ECTS. Godziny pracy można rozłożyć w następujący sposób:

***Tabela 2. Godziny pracy***

| | Ilość modułów | Suma punktów ECTS | Godziny zdalne dla umiejętności teoretycznych | Zdalne godziny zdobywania umiejętności praktycznych | Indywidualny czas pracy | Łączna liczba godzin pracy |
|---|---|---|---|---|---|---|
| Moduły dla studentów uczelni (ERK na poziomie 5-6) | 8 | 8-40 | 20% | 20% | 60% | 200-1200 |
| Moduły dla studentów kształcenia i szkolenia zawodowego (poziom 4-5 ERK) | 8 | 8-40 | 15% | 25% | 60% | 200-1200 |
| Samodzielna nauka (nauczanie mieszane) | 8 | 8-40 | 10% | | 90% | 200-1080 |
| Samodzielna nauka (online) | 8 | 8-40 | | | | 200-1200 |
| Mikromoduły | 1-8 | 1-40 | | | | 25-1200 |

*Tabela 3. Rekomendowane obciążenie modułów*

| Moduł | ECTS | Łączna liczba godzin | Godziny kontaktowe | Godziny kontaktowe (teoria) | Godziny kontaktowe (praktyka) | Indywidualny czas pracy |
|---|---|---|---|---|---|---|
| Tytuł modułu szkolnictwa wyższego | 1-5 | 25-150 | 40% | 20% | 20% | 60% |
| Tytuł modułu dla studentów kształcenia i szkolenia zawodowego | 1-5 | 25-150 | 40% | 15% | 25% | 60% |
| Samodzielna nauka (nauczanie mieszane) | 1-5 | 25-150 | 10% | | | 90% |
| Samodzielna nauka (online) | 1-5 | 25-150 | | | | 100% |
| Mikrosekcje | | | | | | 10%-100% |

Każdy moduł powinien mieć swój własny opis. Po przeanalizowaniu VU, Timtal i innych programów wykorzystujących mikropoświadczenia zaproponowano typową strukturę modułową dla każdego modułu CyberAgent (przykład typowej struktury modułowej podano w załączniku 1).

***Tabela 4. Typowa struktura modułów CyberAgenta***

| Kategoria | Szczegółowe informacje |
|---|---|
| **Identyfikacja modułu** (podstawowe informacje o module) | - Tytuł modułu<br>- Kod modułu<br>- Wykładowca<br>- Instytucja lub dział, w którym dostarczany jest moduł<br>- Sposób dostawy<br>- Język<br>- Warunki wstępne |
| **Czas trwania modułu i obciążenie pracą** (wyraźne zaangażowanie czasowe i zarys struktury) | - Łączny czas trwania (liczba punktów ECTS)<br>- Nakład pracy studenta w godzinach<br>- Godziny kontaktowe pracy<br>- Indywidualny czas pracy |
| **Cele edukacyjne i efekty uczenia się** (szczegóły dotyczące tego, co moduł ma na celu osiągnąć i czego nauczą się uczniowie) | - Cel i rezultaty modułu<br>- Wyniki nauki<br>  o Umiejętności techniczne<br>  o Umiejętności analityczne<br>  o Umiejętności związane z ryzykiem<br>  o Umiejętności organizacyjne |
| **Metody nauczania i uczenia się** | - Metody nauczania i uczenia się |
| **Ocenianie i ewaluacja** (wyjaśnienie, w jaki sposób uczniowie będą oceniani) | - Metody oceniania<br>- Zadania (laboratoria, projekty, prezentacje, raporty itp.)<br>- Strategia oceniania, kryteria oceniania |
| **Ułatwianie korzystania z zasobów** | - Sprzęt, oprogramowanie i technologia |
| **Treść kursu** | - Tematy i podtematy modułu |
| **Zasoby** | - Lista źródeł<br>- Dodatkowe źródła |

Za każdy ECTS uważa się 25-30 godzin (godziny kontaktowe lub online + nauka indywidualna).

Moduł powinien mieć co najmniej dwupoziomową hierarchię:

- **Pierwszy poziom hierarchii** – tematy. Na tym poziomie głównymi elementami modułu mogą być wprowadzenie, test wstępny, test końcowy oraz element bazowy – temat.
- **Drugi poziom hierarchii** – podtematy, główne elementy edukacyjne modułu.

Każdy moduł na pierwszym poziomie hierarchii powinien zawierać:

- **WPROWADZENIE** do modułu (opis tekstowy, wprowadzenie wideo): znaczenie i korzyści płynące z modułu, podstawowe cele i wyniki modułu, wymagane oprogramowanie i sprzęt, wymagania dla uczestników.
- **TEMATYKA** – główne tematy kursu, materiał teoretyczny oraz teoretyczne metody nauczania.
- **PODTEMAT** – podtemat każdego tematu, praktyczna, analityczna analiza i zadania, praktyczne i analityczne metody nauczania. Tematy i podtematy mogą obejmować informacje tekstowe, filmy, klipy audio, prezentacje, linki do dalszej lektury.
- **MODUŁ Test wprowadzający** (w razie potrzeby). Test wprowadzający na poziomie średniozaawansowanym i zaawansowanym powinien potwierdzić, że kandydat opanował wystarczającą wiedzę i umiejętności na poprzednich poziomach.
- **Testy potwierdzające MODUŁ**. Test potwierdzający powinien zapewnić obiektywną weryfikację umiejętności studenta i wykazać jego kompetencje zgodnie z wymaganiami modułu.
- **WYTYCZNE dla mentorów/nauczycieli**. Dokument ten powinien zawierać zalecenia metodyczne dla mentorów/nauczycieli dotyczące wykorzystania modułowych elementów edukacyjnych.

Każdy TEMAT na drugim poziomie hierarchii powinien zawierać:

- **WPROWADZENIE** do tematu cele i rezultaty, krótka treść.
- **PODTEMATY:** wszystkie niezbędne elementy edukacyjne wspierające ucznia w opanowaniu odpowiednich umiejętności.
- **Test TEMATYCZNY**: krótkie rekomendacje dla mentorów/nauczycieli dotyczące wdrożenia i zastosowania modułu. Każdy PODTEMAT powinien składać się z elementów edukacyjnych, których treść odpowiada zadaniom opisu modułu. Każdy podtemat może (powinien) zawierać TEST podtematyczny, potwierdzający, że uczeń opanował odpowiednie umiejętności na wystarczająco wysokim poziomie.

Materiały szkoleniowe modułu powinny wspierać naukę 6-8 tematów, z których każdy składa się z 4-6 podtematów i co najmniej jednego testu tematycznego. Tak więc moduł powinien zawierać (w przybliżeniu) 30-40 elementów edukacyjnych (metody opisane w sekcji metody nauczania) oraz 6-8 testów i jeden moduł końcowy test potwierdzający.

# 5. PROGRAM NAUCZANIA I SZKOLENIA CYBERAGENT

**Mapa tworzenia programu nauczania**

Program nauczania i program szkoleniowy CyberAgent jest zgodny z wytycznymi programowymi dla programów studiów policealnych w zakresie cyberbezpieczeństwa, opracowanymi przez wspólną grupę zadaniową ACM, IEEE, AIS, SIGSEC i IFIP (2017)[8] (dalej – **Wytyczne**). Dokładniej rzecz ujmując, ponieważ głównym celem projektu CyberAgent jest zwiększenie wewnętrznych kompetencji w zakresie cyberbezpieczeństwa europejskich MŚP, program nauczania jest zgodny z ramami obszaru wiedzy o bezpieczeństwie organizacji, zgodnie z zaleceniami zawartymi w niniejszych wytycznych.

To powiedziawszy, pierwszym krokiem w budowaniu programu nauczania jest mapowanie predefiniowanych podtematów i modułów w projekcie CyberAgent z jednostkami wiedzy i kluczowymi tematami, zalecanymi i opisanymi w Wytycznych (str. 59-70). Mapowanie opiera się na logicznej korelacji między tymi dwoma filarami, omówionej i uzgodnionej przez partnerów projektu.

Drugim krokiem jest przypisanie konkretnych efektów uczenia się, zidentyfikowanych i opisanych w T2.2 "Mapowanie potrzeb szkoleniowych dla agentów zmian w zakresie cyberbezpieczeństwa MŚP" z jednostką wiedzy i kluczowymi tematami, zmapowanymi powyżej. Należy w tym miejscu zauważyć, że różne zawody związane z cyberbezpieczeństwem mogą charakteryzować się różnorodną wiedzą, umiejętnościami i kompetencjami, co zostało elokwentnie przedstawione w wyżej wymienionym dokumencie T2.2. Poniższa propozycja odzwierciedla jednak oczekiwany przez CyberAgenta zestaw wiedzy, umiejętności i kompetencji, który może być dostosowany do specyficznych potrzeb konkretnych zawodów lub grup stażystów.

Mając to na uwadze, wyniki tego ćwiczenia w zakresie budowania programu nauczania przedstawiono w tabeli 5 poniżej.

[8] Wspólna grupa zadaniowa ds. edukacji w zakresie cyberbezpieczeństwa. (2017). Wytyczne programowe dla programów studiów policealnych w zakresie cyberbezpieczeństwa: raport z serii programów nauczania informatyki. Stowarzyszenie Maszyn Obliczeniowych, 31 grudnia 2017 r. Dostępne pod adresem: **https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf** [Dostęp 3 marca 2024 r.]

*Table 5. Plan tworzenia programu nauczania*

| Podtematy i moduły | Jednostka wiedzy i kluczowe tematy | Wyniki nauki HEI | Wyniki nauki VET |
|---|---|---|---|
| **Umiejętności techniczne** | | | |
| - **Aktualna wiedza na temat zagrożeń cyberbezpieczeństwa i związanych z nimi zagadnień prawnych** | **Zarządzanie programami bezpieczeństwa**<br>- Zarządzanie projektem<br>- Zarządzanie zasobami<br>- Metryki zabezpieczeń<br>- Zapewnienie jakości i kontrola jakości | **Wiedza**: Uczniowie zdobędą zaawansowaną wiedzę na temat zaawansowanych zasad cyberbezpieczeństwa, w tym wyrafinowanych zagrożeń cybernetycznych i wektorów ataków, krajowych i międzynarodowych przepisów, standardów i wymagań dotyczących zgodności z przepisami dotyczącymi cyberbezpieczeństwa istotnych dla ich branży.<br>**Umiejętności**: Uczniowie będą posiadać umiejętności projektowania i wdrażania zaawansowanych strategii oceny ryzyka i zarządzania w celu ograniczenia zidentyfikowanych zagrożeń, przy użyciu zaawansowanych metodologii i narzędzi.<br>**Kompetencje**: Uczniowie będą kompetentni do kierowania i zarządzania projektami i zespołami z zakresu cyberbezpieczeństwa wdrażającymi strategiczne polityki i | **Wiedza**: Uczniowie zdobędą praktyczną wiedzę na temat najnowszych zagrożeń cyberbezpieczeństwa, w tym phishingu, ransomware i ataków DDoS, oraz sposobów zarządzania nimi poprzez efektywne zarządzanie projektami i zasobami oraz wdrażanie środków zapewnienia i kontroli jakości.<br>**Umiejętności**: Uczniowie będą umieć korzystać z narzędzi i oprogramowania do ochrony przed ewoluującymi zagrożeniami cybernetycznymi oraz stosować solidne praktyki bezpieczeństwa w zarządzaniu projektami i zasobami w celu poprawy ogólnych wskaźników bezpieczeństwa i kontroli jakości w swoich organizacjach.<br>**Kompetencje**: Uczniowie będą kompetentni w zakresie oceny i łagodzenia potencjalnych zagrożeń bezpieczeństwa, skutecznego komunikowania problemów związanych z cyberbezpieczeństwem oraz dokładnego |

| | | | |
|---|---|---|---|
| | | ramy cyberbezpieczeństwa dostosowane do celów organizacji i zobowiązań w zakresie zgodności. | zgłaszania zagrożeń i naruszeń za pośrednictwem odpowiednich kanałów w organizacji. |
| - **Praktyczna wiedza na temat radzenia sobie z zagrożeniami cyberbezpieczeństwa** | **Administracja systemami**<br>- Administrowanie systemem operacyjnym<br>- Administracja systemem bazy danych<br>- Administrowanie siecią<br>- Administracja chmurą<br>- Administrowanie systemami cyberfizycznymi<br>- Hartowanie systemu<br>- Dostępność | **Wiedza**: Uczniowie zdobędą zaawansowaną wiedzę z zakresu obsługi operacyjnej, baz danych, sieci, chmury i administrowania systemami cyberfizycznymi oraz innych obszarów, co pozwoli im skutecznie wzmocnić systemy i zapewnić dostępność przy jednoczesnym zastosowaniu najnowszych mechanizmów obrony cyberbezpieczeństwa.<br>**Umiejętności**: Uczniowie będą umieć korzystać z zaawansowanych metodologii i narzędzi do projektowania i wdrażania bezpiecznych architektur systemowych — w tym systemów operacyjnych, baz danych, sieci i infrastruktur chmurowych<br>**Kompetencje**: Uczniowie będą kompetentni do opracowywania i wdrażania strategicznych ram cyberbezpieczeństwa w zakresie administrowania systemami, kierowania projektami i zespołami w celu zwiększenia wzmocnienia i dostępności systemu oraz | **Wiedza**: Uczniowie zdobędą praktyczną wiedzę na temat administrowania i zabezpieczania systemów operacyjnych, baz danych, sieci, chmur i systemów cyberfizycznych przed powszechnymi zagrożeniami cybernetycznymi, takimi jak phishing, ransomware i ataki DDoS, przy jednoczesnym wdrażaniu skutecznych zasad zarządzania ryzykiem.<br>**Umiejętności**: Uczniowie będą wykwalifikowani w identyfikowaniu potencjalnych zagrożeń i luk w zabezpieczeniach cybernetycznych na różnych platformach systemowych, korzystaniu ze specjalistycznych narzędzi i oprogramowania w celu zwiększenia wzmocnienia i dostępności systemu oraz wdrażaniu podstawowych praktyk cyberbezpieczeństwa, takich jak bezpieczne tworzenie haseł, bezpieczne przeglądanie i bezpieczne obchodzenie się z danymi wrażliwymi.<br>**Kompetencje**: Uczniowie będą kompetentni w zakresie oceny i łagodzenia zagrożeń bezpieczeństwa w ramach administrowania systemem, |

| | | | |
|---|---|---|---|
| | | podejmowania etycznych decyzji w zakresie utrzymania solidnych praktyk w zakresie cyberbezpieczeństwa w różnych domenach administracyjnych. | skutecznego komunikowania problemów związanych z cyberbezpieczeństwem oraz szybkiego zgłaszania wszelkich zagrożeń i naruszeń do odpowiednich kanałów organizacyjnych. |
| **Umiejętności analityczne** | | | |
| - **Nastawienie na krytyczne myślenie** | **Narzędzia analityczne**<br>- Pomiary wydajności (metryki)<br>- Analityka danych<br>- Analiza zabezpieczeń | **Wiedza**: Uczniowie zdobędą zaawansowaną wiedzę na temat krajowych i międzynarodowych przepisów, standardów i wymagań dotyczących zgodności z przepisami dotyczącymi cyberbezpieczeństwa oraz innych istotnych dla ich konkretnej branży.<br>**Umiejętności**: Uczniowie będą umieć korzystać z pomiarów wydajności, analizy danych i analizy bezpieczeństwa w celu projektowania i wdrażania skutecznych strategii zarządzania ryzykiem.<br>**Kompetencje**: Uczniowie będą kompetentni w korzystaniu z narzędzi analitycznych w celu opracowania strategicznych polityk | **Wiedza**: Uczniowie zdobędą praktyczną wiedzę na temat stosowania pomiarów wydajności, analizy danych i analizy zabezpieczeń w celu ochrony zasobów organizacji.<br>**Umiejętności**: Uczniowie będą umieć korzystać z narzędzi analitycznych w celu identyfikacji potencjalnych zagrożeń i luk w zabezpieczeniach cybernetycznych, stosować spostrzeżenia oparte na danych w celu wzmocnienia praktyk cyberbezpieczeństwa oraz wykorzystywać wskaźniki wydajności do oceny i zwiększania bezpieczeństwa haseł, przeglądania, poczty e-mail i obsługi danych.<br>**Kompetencje**: Uczniowie będą kompetentni w ocenie i łagodzeniu |

| | | | |
|---|---|---|---|
| | | cyberbezpieczeństwa z krytycznym nastawieniem oraz podejmowania decyzji w zakresie praktyk cyberbezpieczeństwa zgodnych z celami organizacyjnymi i zobowiązaniami w zakresie zgodności. | potencjalnych zagrożeń bezpieczeństwa za pomocą narzędzi analitycznych, dokładnym zgłaszaniu zagrożeń i naruszeń do odpowiednich kanałów w organizacji. |
| - **Analiza i zrozumienie lokalnych zagrożeń, sposobów ich powstawania, osób zagrożonych itp.** | **Operacje bezpieczeństwa**<br>- Konwergencja zabezpieczeń<br>- Globalne centra operacji bezpieczeństwa (GSOC) | **Wiedza**: Uczniowie zdobędą zaawansowaną wiedzę na temat lokalnych zagrożeń cybernetycznych, korzystając z informacji z globalnych centrów operacji bezpieczeństwa i aktualnych trendów w strategiach obrony cyberbezpieczeństwa.<br>**Umiejętności**: Uczniowie będą umieć korzystać z zaawansowanych metodologii i narzędzi w globalnych centrach operacji bezpieczeństwa w celu projektowania skutecznych strategii zarządzania ryzykiem i opracowywania planów skutecznego łagodzenia lokalnych zagrożeń cybernetycznych.<br>**Kompetencje**: Uczniowie będą kompetentni w opracowywaniu i wdrażaniu strategicznych polityk cyberbezpieczeństwa, które odnoszą się do lokalnych zagrożeń poprzez wykorzystanie globalnych centrów operacji bezpieczeństwa. | **Wiedza**: Uczniowie zdobędą praktyczną wiedzę na temat lokalnych zagrożeń cybernetycznych i ich pochodzenia, ocenią, w jaki sposób zagrożenia te wpływają na zasoby organizacji.<br>**Umiejętności**: Uczniowie będą wykwalifikowani w identyfikowaniu lokalnych zagrożeń i luk w zabezpieczeniach cybernetycznych, korzystając z narzędzi i oprogramowania, takich jak bezpieczne tworzenie haseł, bezpieczne przeglądanie i bezpieczna obsługa danych dostosowana do ich konkretnych środowisk.<br>**Kompetencje**: Uczniowie będą kompetentni w ocenie i łagodzeniu lokalnych zagrożeń bezpieczeństwa, korzystając z informacji z globalnych centrów operacji bezpieczeństwa, skutecznie komunikując problemy związane z cyberbezpieczeństwem oraz dokładnie zgłaszając zagrożenia i |

| | | | |
|---|---|---|---|
| | | | naruszenia do odpowiednich kanałów w swojej organizacji. |
| **Zarządzanie ryzykiem** | | | |
| - **Zaznajomienie w miejscach pracy w MŚP z procedurami cyberbezpieczeństwa** | **Zarządzanie ryzykiem**<br>- Identyfikacja ryzyka<br>- Ocena i analiza ryzyka<br>- Zagrożenia wewnętrzne<br>- Modele i metodologie pomiaru i oceny ryzyka<br>- Kontrola ryzyka | **Wiedza**: Uczniowie zdobędą zaawansowaną wiedzę na temat procesów zarządzania ryzykiem, w tym identyfikacji, oceny i kontroli ryzyka, co umożliwi im ustanowienie i opisanie skutecznych procedur cyberbezpieczeństwa dostosowanych do konkretnych potrzeb miejsc pracy MŚP zgodnie z normami krajowymi i międzynarodowymi.<br>**Umiejętności**: Uczniowie będą umieć stosować zaawansowane metodologie i narzędzia do przeprowadzania kompleksowych ocen ryzyka, projektowania i wdrażania skutecznych strategii zarządzania ryzykiem oraz opracowywania solidnych procedur cyberbezpieczeństwa dostosowanych specjalnie do miejsc pracy MŚP.<br>**Kompetencje**: Osoby uczące się będą kompetentne w zakresie opracowywania i wdrażania strategicznych polityk cyberbezpieczeństwa dla miejsc pracy MŚP. | **Wiedza**: Uczniowie zdobędą praktyczną wiedzę na temat procesów identyfikacji, oceny i kontroli ryzyka oraz strategii zarządzania ryzykiem w celu skutecznej ochrony miejsc pracy MŚP.<br>**Umiejętności**: Uczniowie będą wykwalifikowani w identyfikowaniu i analizowaniu potencjalnych zagrożeń dla cyberbezpieczeństwa w środowiskach MŚP, korzystaniu z odpowiednich narzędzi i oprogramowania do łagodzenia zagrożeń oraz promowaniu i wdrażaniu podstawowych praktyk w zakresie cyberbezpieczeństwa, w tym bezpiecznego tworzenia haseł, bezpiecznego przeglądania i bezpiecznego obchodzenia się z danymi wrażliwymi.<br>**Kompetencje**: Uczniowie będą kompetentni w zakresie oceny i łagodzenia zagrożeń bezpieczeństwa w miejscach pracy MŚP, skutecznego komunikowania kwestii i procedur związanych z cyberbezpieczeństwem oraz dokładnego zgłaszania istotnych zagrożeń |

| | | | |
|---|---|---|---|
| | | | i naruszeń do odpowiednich kanałów organizacyjnych. |
| - **Stworzenie własnego podręcznika dla MŚP w zakresie cyberbezpieczeństwa w miejscu pracy i sposobów jego realizacji** | **Ciągłość działania, odzyskiwanie danych po awarii oraz zarządzanie incydentami i bezpieczeństwo personelu**<br>- Reagowanie na incydenty<br>- Odzyskiwanie po awarii<br>- Ciągłości działania<br>- Świadomość, szkolenie i edukacja w zakresie bezpieczeństwa<br>- Praktyki zatrudniania w zakresie bezpieczeństwa<br>- Praktyki w zakresie kończenia zabezpieczeń<br>- Zabezpieczenia innych firm<br>- Bezpieczeństwo w procesach recenzowania<br>- Specjalne zagadnienie dotyczące prywatności danych osobowych pracowników | **Wiedza**: Uczniowie zdobędą zaawansowaną wiedzę na temat tego, jak stworzyć i wdrożyć kompleksowy podręcznik cyberbezpieczeństwa w miejscu pracy dla MŚP, zawierający zaawansowane zasady cyberbezpieczeństwa, najnowsze mechanizmy obronne oraz przestrzeganie krajowych i międzynarodowych przepisów i standardów w zakresie zarządzania incydentami, ciągłości działania i bezpieczeństwa personelu.<br>**Umiejętności**: Uczniowie będą umieć tworzyć i utrzymywać podręcznik cyberbezpieczeństwa w miejscu pracy dla MŚP, wykorzystując zaawansowane metodologie do oceny ryzyka, projektowania skutecznych strategii zarządzania ryzykiem i reagowania na incydenty oraz opracowywania kompleksowych planów ciągłości działania dostosowanych do potrzeb ich organizacji.<br>**Kompetencje**: Uczniowie będą kompetentni w zakresie opracowywania i wdrażania | **Wiedza**: Uczniowie zdobędą praktyczną wiedzę na temat tworzenia kompleksowego podręcznika cyberbezpieczeństwa w miejscu pracy dla MŚP, który obejmuje strategie reagowania na incydenty, odzyskiwania po awarii, ciągłości działania i bezpieczeństwa personelu, ochrony zasobów organizacji i danych wrażliwych.<br>**Umiejętności**: Uczniowie będą wykwalifikowani w zakresie identyfikowania potencjalnych zagrożeń dla cyberbezpieczeństwa, korzystania z narzędzi i oprogramowania w celu ochrony przed zagrożeniami oraz stosowania najlepszych praktyk w zakresie cyberbezpieczeństwa w celu opracowania i utrzymywania podręcznika dla MŚP, który dotyczy bezpiecznego tworzenia haseł, przeglądania, bezpieczeństwa poczty e-mail i ochrony danych.<br>**Kompetencje**: Uczniowie będą kompetentni w zakresie oceny i łagodzenia zagrożeń bezpieczeństwa, skutecznego komunikowania zasad i praktyk w zakresie cyberbezpieczeństwa oraz systematycznego zgłaszania |

| | | | |
|---|---|---|---|
| | | podręcznika cyberbezpieczeństwa dla MŚP, skutecznego kierowania projektami i zespołami ds. bezpieczeństwa, zapewniając zgodność z celami organizacyjnymi i obowiązkami w zakresie zgodności. | incydentów związanych z bezpieczeństwem w MŚP, zgodnie z opisem zawartym w dostosowanym do ich potrzeb podręczniku cyberbezpieczeństwa. |
| **Umiejętności organizacyjne** | | | |
| - **Jak wdrożyć nowe procedury i sposób pracy w obszarze cyberbezpieczeństwa na stanowiskach pracy MŚP** | **Zarządzanie bezpieczeństwem i polityka**<br>- Kontekst organizacyjny<br>- Prywatność<br>- Prawo, etyka i zgodność z przepisami<br>- Zarządzanie zabezpieczeniami<br>- Komunikacja na poziomie kierownictwa i zarządu<br>- Polityka zarządcza | **Wiedza**: Uczniowie zdobędą zaawansowaną wiedzę na temat wdrażania nowych procedur i przepływów pracy w zakresie cyberbezpieczeństwa w miejscach pracy MŚP, z uwzględnieniem aktualnych zasad, trendów i zgodności z krajowymi i międzynarodowymi przepisami dotyczącymi ich branży.<br>**Umiejętności**: Uczniowie będą biegli w korzystaniu z zaawansowanych metodologii do przeprowadzania ocen ryzyka, projektowania i wdrażania nowych procedur cyberbezpieczeństwa oraz przygotowywania strategii reagowania, zapewniając skuteczne zarządzanie i zgodność w miejscach pracy MŚP.<br>**Kompetencje**: Uczniowie będą kompetentni w opracowywaniu i wdrażaniu strategicznych polityk | **Wiedza**: Uczniowie zdobędą praktyczną wiedzę na temat tego, jak zintegrować nowe procedury i praktyki w zakresie cyberbezpieczeństwa w miejscach pracy MŚP, zgodnie z przepisami, standardami, strategiami i politykami dotyczącymi bezpieczeństwa informacji, zarządzania ryzykiem i ochrony danych.<br>**Umiejętności**: Uczniowie będą wykwalifikowani w stosowaniu narzędzi i oprogramowania cyberbezpieczeństwa w celu wdrażania nowych procedur bezpieczeństwa, identyfikowania i ograniczania ryzyka oraz promowania podstawowych praktyk w zakresie cyberbezpieczeństwa, takich jak bezpieczne tworzenie haseł, przeglądanie i przetwarzanie danych w ramach zarządzania miejscami pracy MŚP.<br>**Kompetencje**: Uczniowie będą kompetentni w zakresie oceny i |

| | | | |
|---|---|---|---|
| | | cyberbezpieczeństwa, przewodzeniu inicjatywom mającym na celu ustanowienie nowych procedur i przepływów pracy w miejscach pracy MŚP oraz podejmowaniu etycznych decyzji, które są zgodne z celami organizacyjnymi i wymaganiami dotyczącymi zgodności. | łagodzenia potencjalnych zagrożeń bezpieczeństwa, skutecznego komunikowania zmian i polityk cyberbezpieczeństwa oraz dokładnego zgłaszania incydentów bezpieczeństwa w MŚP zgodnie z wymogami dotyczącymi zarządzania i zgodności. |
| - **Prowadzenie wsparcia lidera w zakresie cyberbezpieczeństwa.** | **Planowanie cyberbezpieczeństwa**<br>- Planowanie strategiczne<br>- Zarządzanie operacyjne i taktyczne | **Wiedza**: Uczniowie zdobędą zaawansowaną wiedzę na temat tego, jak zintegrować zaawansowane zasady cyberbezpieczeństwa i aktualne trendy z planowaniem strategicznym i zarządzaniem operacyjnym.<br>**Umiejętności**: Uczniowie będą posiadać umiejętności w zakresie planowania strategicznego i zarządzania operacyjnego, co umożliwi im skuteczne projektowanie i wdrażanie strategii cyberbezpieczeństwa, które przeciwdziałają pojawiającym się zagrożeniom i zapewniają solidne reakcje taktyczne.<br>**Kompetencje**: Uczniowie będą kompetentni w zakresie opracowywania i wdrażania strategicznych ram cyberbezpieczeństwa, kierowania | **Wiedza**: Uczniowie zdobędą praktyczną wiedzę na temat tego, jak zintegrować planowanie strategiczne i zarządzanie operacyjne w cyberbezpieczeństwie w celu ochrony zasobów organizacji, przestrzegania odpowiednich przepisów i standardów oraz wdrażania skutecznych strategii bezpieczeństwa informacji i polityk zarządzania ryzykiem.<br>**Umiejętności**: Uczniowie będą wykwalifikowani w identyfikowaniu zagrożeń związanych z cyberbezpieczeństwem, korzystaniu z narzędzi planowania strategicznego i zarządzania operacyjnego w celu ochrony przed zagrożeniami oraz promowaniu wdrażania podstawowych praktyk w zakresie cyberbezpieczeństwa w ramach swoich ról wspierających przywództwo.<br>**Kompetencje**: Uczniowie będą kompetentni w zakresie oceny i |

| | | | |
|---|---|---|---|
| | | inicjatywami w zakresie cyberbezpieczeństwa i zarządzania nimi. | łagodzenia zagrożeń bezpieczeństwa, skutecznego komunikowania strategii i problemów związanych z cyberbezpieczeństwem oraz rzetelnego zgłaszania incydentów i luk w zabezpieczeniach do odpowiednich kanałów w swoich organizacjach. |

# 6. STRATEGIA OCENIANIA KURSU

Ewaluacja wiedzy jest integralną częścią procesu uczenia się i sprzyja głębszemu uczeniu się. W tym rozdziale opisano podejście do oceny kursu, które jest potrzebne, aby wszyscy uczestnicy kursów CyberAgent osiągnęli wymagane efekty uczenia się i kompetencje. Proces oceniania w kursie podzielony jest na dwie główne części: samoocenę i testy oceny wiedzy, które są dostosowane zarówno do studentów szkół wyższych, jak i kształcenia i szkolenia zawodowego (VET), biorąc pod uwagę ich różne potrzeby i cele uczenia się.

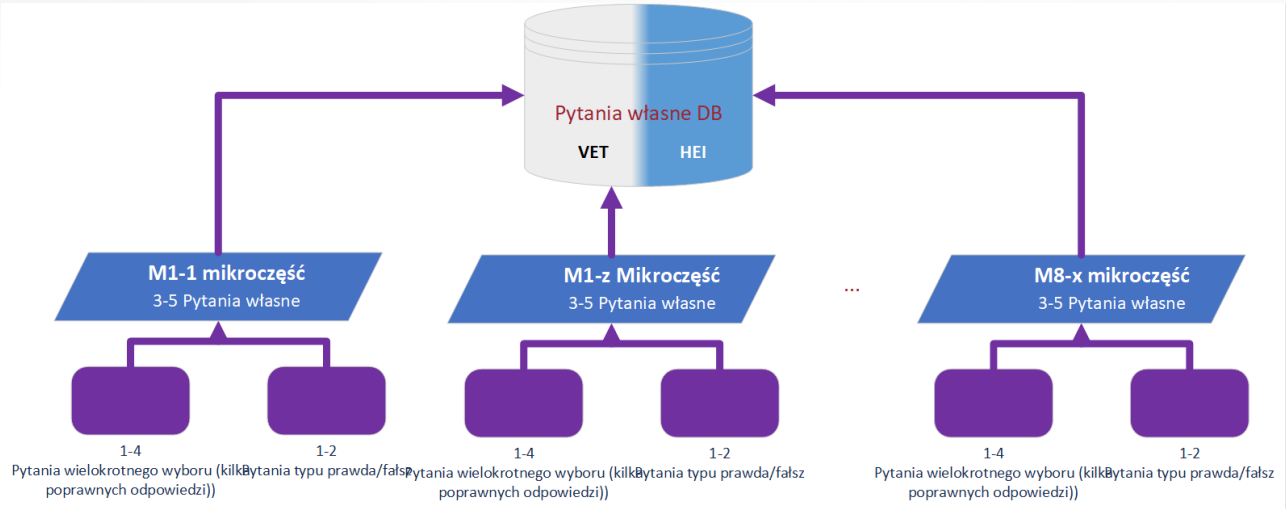
Ponieważ tematyka modułów może być taka sama zarówno dla uczelni, jak i dla kształcenia i szkolenia zawodowego, niektóre pytania mogą być odpowiednie zarówno dla kursów szkolnictwa wyższego, jak i kształcenia i szkolenia zawodowego. W związku z tym przy opracowywaniu pytań będzie można określić, czy pytanie jest przeznaczone wyłącznie dla kształcenia i szkolenia zawodowego lub uczelni, czy też dla obu. Ten sposób oznaczania będzie używany tylko podczas projektowania pytań, ponieważ ułatwi projektowanie pytań. Po zaimportowaniu pytań na platformę bazy danych będą się różnić w przypadku kształcenia i szkolenia zawodowego oraz szkolnictwa wyższego.


*Rysunek 12. Bazy danych do samooceny i oceny wiedzy*

**1. Testy samooceny**: Po ukończeniu każdego tematu w ramach kursu studenci przystąpią do testów samooceny. Oceny te mają na celu dostarczenie natychmiastowej informacji zwrotnej, pomagając uczniom ocenić ich zrozumienie ostatnio omówionego materiału. Ten etap zachęca do autorefleksji i pomaga we wzmocnieniu celów uczenia się każdego tematu. Ponadto pozwala uczniom zidentyfikować obszary, w których mogą potrzebować dalszych badań lub wyjaśnień, promując proaktywne podejście do ich podróży edukacyjnej.

Korzystając z testów samooceny, uczestnicy kursu będą mogli określić początkowy poziom wiedzy i będą mogli sprawdzać postępy po każdym temacie szkolenia.

Zalecany jest quiz samooceny składający się z 3-5 pytań, z mieszanką pytań typu prawda/fałsz, dopasowywanie i/lub pytania wielokrotnego wyboru. Kolejny temat powinien zostać odblokowany dopiero po udzieleniu poprawnych odpowiedzi na wszystkie pytania. Nie powinno być żadnych ograniczeń czasowych ani ograniczeń dotyczących prób. Próba powinna losowo wybrać pytania z odpowiedniej bazy danych.




***Rysunek 13. Struktura bazy danych samooceny***

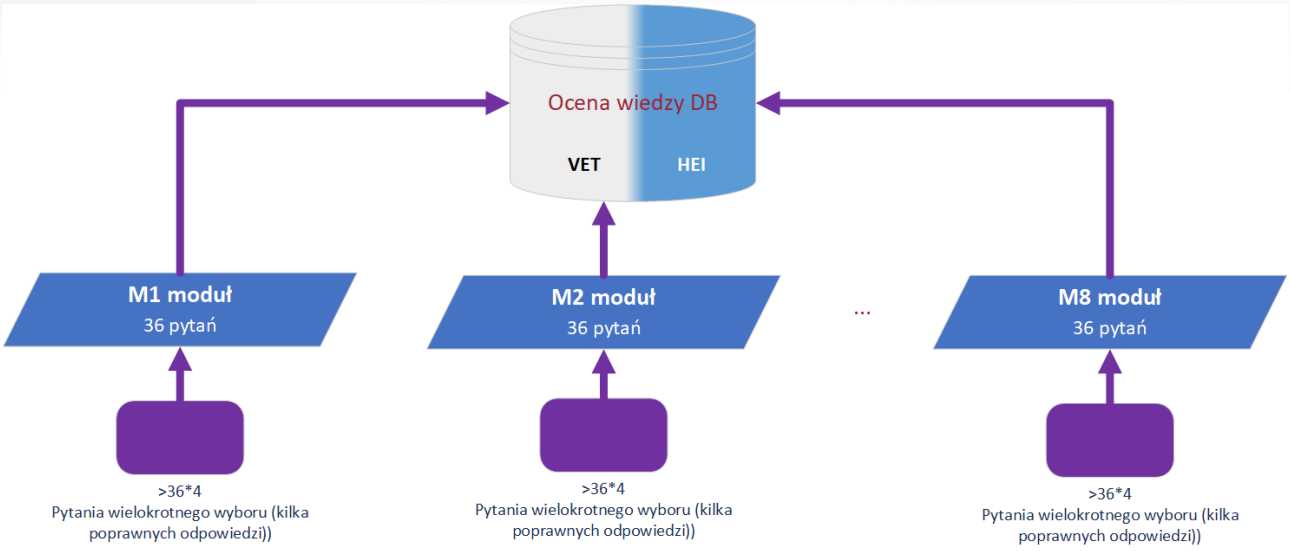
**2. Test sprawdzający wiedzę***: Po ukończeniu wszystkich tematów kursu studenci będą musieli przystąpić do testu końcowego w celu uzyskania certyfikatu ukończenia kursu. Ta kompleksowa ocena ocenia ich ogólne zrozumienie i opanowanie treści kursu. Test końcowy ocenia zapamiętywanie materiału przez uczniów i określa, jak dobrze mogą zastosować swoją wiedzę w szerszym kontekście.

* Podczas opracowywania programu nauczania i materiałów zostaną wzięte pod uwagę inne metodologie oceny ukończenia kursu i oceny wiedzy, takie jak studia przypadków, ćwiczenia praktyczne i refleksyjne raporty, które pozwolą na bardziej kompleksową ocenę umiejętności analitycznego i krytycznego myślenia uczestników. Podejście to będzie również dostępne dla wykładowców dla studentów uczelni wyższych i kształcenia i szkolenia zawodowego w trakcie realizacji kursu.

Korzystając z testu sprawdzającego wiedzę, uczestnicy będą mogli określić swój końcowy poziom wiedzy, a w przypadku pozytywnego zaliczenia – otrzymać odznakę (certyfikat) ukończenia kursu.

Zalecany jest test sprawdzający wiedzę składający się z 36 pytań, z mieszanką pytań typu prawda/fałsz, dopasowywanie i pytań wielokrotnego wyboru. Powinien istnieć limit czasu 45 minut i dozwolona jest tylko jedna próba. Test powinien być przeprowadzany poprzez losowe wybieranie pytań z bazy danych.

Ponadto ocena powinna również uwzględniać zapobieganie oszustwom, w związku z czym należy opracować około czterech zestawów pytań. Niektóre pytania testowe dotyczące wiedzy zarówno dla kształcenia i szkolenia zawodowego, jak i uczelni mogą się pokrywać, więc w momencie opracowywania będziemy mieli trzy atrybuty: VET, HEI lub VET i HEI.




***Rysunek 14. Struktura bazy danych ewaluacji wiedzy***

Ta dwuetapowa strategia oceny nie tylko wspiera efektywne uczenie się, zapewniając wiele pętli informacji zwrotnych, ale także umożliwia uczniom odgrywanie aktywnej roli w szkoleniu.

Testy samooceny oraz testy służące do oceny wiedzy zostaną opracowane zgodnie z programem kursów oraz na podstawie wyników i zaleceń opracowanych w ramach niniejszego projektu.

**SKŁAD BAZY PYTAŃ**

Aby zapewnić wystarczająco dużą i zrównoważoną bazę pytań, dla każdego tematu na kursie kształcenia i szkolenia zawodowego lub szkolnictwa wyższego zostanie utworzonych co najmniej 5 pytań typu prawda/fałsz lub pytań typu dopasuj odpowiedź oraz 5 pytań wielokrotnego wyboru.

Zakładając, że na każdym kursie będzie co najmniej 10 tematów, ogólna baza dla każdego kursu VET lub HEI powinna zawierać co najmniej 10-20% pytań typu prawda/fałsz lub dopasowanie oraz 90-80% pytań wielokrotnego wyboru. Jest to ogólna wytyczna, ale nauczyciel będzie miał możliwość wyboru struktury pytań zgodnie z tematyką kursu.

Biorąc pod uwagę różnice w celach i efektach uczenia się w ramach kształcenia i szkolenia zawodowego / szkolnictwa wyższego, ogólny skład bazy pytań dla pojedynczego kursu powinien zawierać to, co pokazano w poniższej tabeli.

*Tabela 6. Rodzaje pytań*

| | Pytania typu prawda/fałsz lub dopasowanie | Pytania wielokrotnego wyboru |
|---|---|---|
| Część ogólna kursu | 20% | 80% |
| VET konkretna część kursu | 20% | 80% |
| HEI konkretna część kursu | 20% | 80% |
| Łączna liczba dla kursów VET i HEI: | 20% | 80% |

**WSKAZÓWKI DOTYCZĄCE KONSTRUOWANIA PYTAŃ**

Pytania do samooceny i testów sprawdzających wiedzę muszą być przygotowane w języku angielskim, a następnie przetłumaczone na języki partnerskie.

Opracowując pytania testowe zarówno do samooceny, jak i oceny wiedzy w ramach kursu, ważne jest, aby pytania były jasne, zwięzłe i dostępne dla wszystkich kandydatów, niezależnie od ich pochodzenia. Takie podejście zapewnia, że oceny dokładnie odzwierciedlają zrozumienie przez uczniów treści kursu oraz ich zdolność do osiągnięcia określonych umiejętności i celów określonych w programach kursu.

**Ogólne wytyczne dotyczące konstruowania pytań:**

Przy opracowywaniu pytań testowych stosowane będą jasne wytyczne: pytania muszą być zrozumiałe i bezpośrednio związane z celami nauczania kursu, bez użycia skomplikowanej terminologii lub mylących sformułowań. Unikane będą również pytania specyficzne kulturowo lub mylące, aby zapewnić uczciwość i dostępność dla wszystkich uczestników kursu. Dalsze wskazówki dotyczące projektowania pytań znajdują się poniżej.

**Jasność i prostota:** pytania muszą być proste, unikając użycia skomplikowanego języka lub żargonu, który mógłby zmylić lub wprowadzić w błąd kandydatów. Celem jest ocena wiedzy i zrozumienia tematu przez kandydatów, a nie ich zdolności do rozszyfrowywania skomplikowanych pytań.

**Bezpośredniość i trafność**: każde pytanie powinno bezpośrednio odnosić się do kluczowych umiejętności i celów programów kursu. Należy unikać nieistotnych lub stycznych treści, aby utrzymać koncentrację na ocenie zamierzonych efektów uczenia się.

**Wrażliwość kulturowa i kontekstowa**: dopilnuj, aby pytania nie zakładały konkretnej wiedzy lub doświadczeń kulturowych, dzięki czemu byłyby dostępne i sprawiedliwe dla kandydatów z różnych środowisk.

**Żadnych podchwytliwych pytań:** intencja każdego pytania powinna być jasna, bez prób wprowadzenia w błąd lub oszukania kandydatów. Pytania mające na celu złapanie kandydatów lub sprawdzenie ich zdolności do dostrzegania podstępów nie oceniają skutecznie ich zrozumienia tematu.

**Jednoznaczna i zwięzła prezentacja**: pytania powinny być sformułowane w sposób, który nie pozostawia miejsca na interpretację, zapewniając, że wszyscy kandydaci rozumieją pytanie w ten sam sposób. Pytania powinny być zwięzłe, unikając niepotrzebnej długości, która mogłaby zaciemnić główny punkt.

**Sformułowanie pozytywne**: unikaj używania zwrotów negatywnych w pytaniach (np. "Które z poniższych jest NIE..."). Negatywne sformułowania mogą prowadzić do nieporozumień i błędnej interpretacji, zwłaszcza w warunkach egzaminacyjnych. Zamiast tego formułuj wszystkie pytania pozytywnie, aby promować jasność.

**Szczegółowe wytyczne dotyczące konstruowania pytań:**

**Pytania wielokrotnego wyboru**: upewnij się, że wszystkie opcje są wiarygodne i odnoszą się do pytania. Prawidłowa odpowiedź powinna być bezdyskusyjnie poprawna, podczas gdy dystraktory powinny być wyraźnie niepoprawne dla kogoś, kto rozumie materiał.

**Pytania typu prawda/fałsz**: przedstaw jasne, oparte na faktach stwierdzenia, które bezpośrednio odnoszą się do treści kursu, upewniając się, że nie ma niejasności co do ich wartości prawdy.

**Pytania dotyczące dopasowania**: upewnij się, że obie listy (np. terminy po jednej stronie i definicje po drugiej) są wyraźnie powiązane i że istnieje prosta podstawa do dopasowania każdej z nich. Unikaj nierównych list, na których liczba elementów nie jest wyrównana, chyba że wyraźnie zaznaczono, że niektóre elementy nie będą używane lub mogą być używane wielokrotnie.

W ramach szkolenia pilotażowego przeanalizowane zostaną informacje na temat metodologii oceny wiedzy i procesu oceniania poprzez zebranie informacji zwrotnych zarówno od osób uczących się, jak i trenerów. Pozwoli to ocenić adekwatność metod oceny wiedzy oraz, w razie potrzeby, uzupełnić lub udoskonalić podejście do oceny.

**GRYWALIZACJA**

W tej sekcji przedstawiono opis elementów grywalizacji zaimplementowanych w kursach CyberAgent. Grywalizacja to proces włączania zasad grywalizacji do tradycyjnych działań edukacyjnych w celu zwiększenia motywacji i zaangażowania uczestników. Elementy te zostały dobrane na podstawie najnowszych badań nad technologiami edukacyjnymi, z których wynika, że grywalizacja może znacząco poprawić wyniki w nauce, zwiększyć motywację uczniów do nauki oraz zwiększyć ich zaangażowanie w proces uczenia się.

Elementy grywalizacji, które zostaną zintegrowane z kursami, obejmują odznaki, punkty, rangi i kolorowe pseudonimy, które odzwierciedlają doświadczenie i osiągnięcia uczestnika.

**- Odznaki będą przyznawane za:**

- **Zakończenie modułu**.
- **Za zaliczenie testu na podstawie procentu zdawalności**. Na przykład uczestnik otrzyma brązową odznakę za minimalny wynik zaliczenia testu końcowego, srebrną odznakę za minimalny wynik zaliczenia 75%, złotą odznakę za wynik zaliczenia 76%-90% i platynową odznakę za wynik zaliczenia 90%-100%. W takim przypadku jeden uczestnik może posiadać 8 odznak tego typu.
- **Uzupełnienie tematu**.
- **Logowanie do systemu codziennie przez dziesięć dni**.
- **Mentor/instruktor kursu przyzna również** specjalną odznakę aktywności dla każdego tematu.

- **Punkty i punktacja** obliczona zostanie na podstawie wyników testów samooceny + wyników testu końcowego z mnożnikiem.

Uczestnicy kursu CyberAgent nie będą mogli zobaczyć swoich postępów indywidualnie, ale będą mogli rywalizować z innymi uczestnikami w grupach lub zespołach (na podstawie największej liczby zdobytych punktów, ale także na podstawie największej liczby odznak). Zachęca to nie tylko do rywalizacji indywidualnej, ale także zespołowej i współpracy, co jest ważne w rozwijaniu umiejętności współpracy.

Każdy uczestnik zobaczy swój nick po zalogowaniu się do kursu, który zostanie oznaczony kolorami zgodnie z postępami w kursie i zdobytym doświadczeniem (ukończone/nagrane kursy).

Pomoże to uczestnikom kursu lepiej zaangażować się w proces szkolenia. Uczestnicy kursu mogą powtarzać ten sam test kilka razy, aby poprawić swój wynik (punkty przyznawane są za największą liczbę poprawnie wykonanych testów samooceny).

Specjalny algorytm obliczy wynik każdego uczestnika, biorąc pod uwagę czas potrzebny na udzielenie odpowiedzi, liczbę powtórzeń testu i inne parametry, minimalizując w ten sposób możliwość oszustwa.

Wszystkie zasady grywalizacji zostaną jasno opisane i zakomunikowane uczestnikom, aby każdy mógł łatwo zrozumieć, w jaki sposób można osiągnąć różne poziomy grywalizacji i jak są obliczane.

# 7. PROCES UCZENIA SIĘ/NAUCZANIA CYBERAGENT

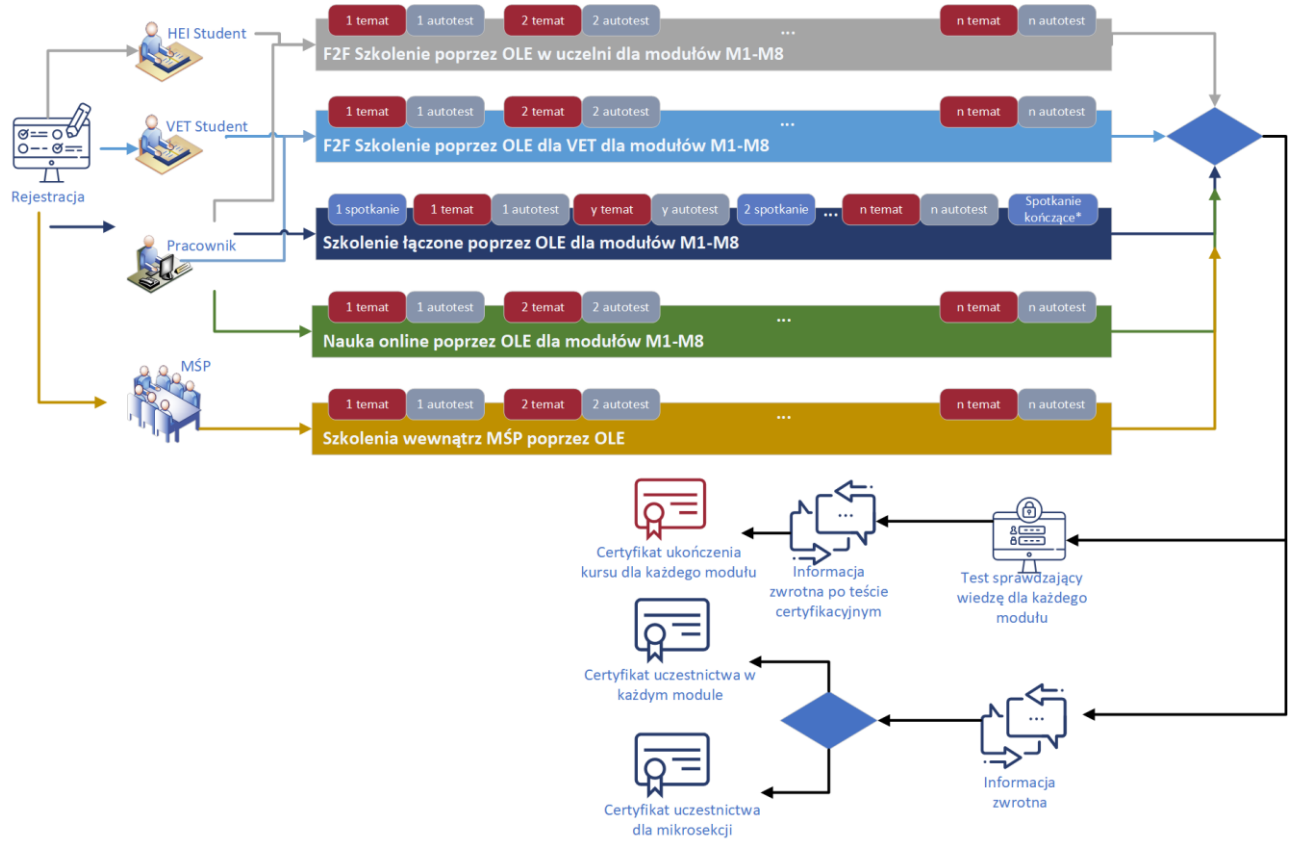
Ta sekcja podsumowuje informacje ze wszystkich rozdziałów tego dokumentu i szczegółowo opisuje proces uczenia się/nauczania, począwszy od zapisania się na kurs CyberAgent na platformie edukacyjnej, a skończywszy na ukończeniu kursu lub wydaniu certyfikatu.

Kursy CyberAgent są przeznaczone dla zróżnicowanego grona uczniów, w tym studentów z instytucji szkolnictwa wyższego (HEI), studentów kształcenia i szkolenia zawodowego (VET), a także pracowników z MŚP. Dążymy do tego, aby każdy uczestnik miał możliwość wyboru sposobu uczenia się, który najbardziej mu odpowiada, biorąc pod uwagę jego sytuację osobistą i politykę organizacyjną instytucji szkoleniowej.

Pomimo wybranej metody nauki/szkolenia, uczestnicy rejestrują się na platformie CyberAgent i korzystają z niej w trakcie szkolenia.

**Rejestracja**

Potencjalni uczestnicy zainteresowani zapisaniem się na kurs CyberAgent muszą wypełnić formularz rejestracyjny, wybierając pożądane moduły i preferowaną metodę nauki. Przedstawiono diagram koncepcyjny, który prowadzi uczestników przez ścieżkę szkoleniową od pierwszego do ósmego modułu CyberAgent.




*Rysunek 15. Ścieżka uczenia się / nauczania CyberAgent*

Poufność informacji o uczestnikach zostanie zapewniona podczas procesu rejestracji, w szczególności z uwzględnieniem wymogów RODO. Podczas rejestracji uczestnicy będą mieli możliwość zapoznania się z regulaminem platformy szkoleniowej, zasadami prywatności i ochrony danych.

Dane rejestracyjne uczestników są dostępne tylko dla wyznaczonych osób w organizacji partnerskiej, zgodnie z wewnętrznymi politykami organizacji. Podczas pilotażowych sesji szkoleniowych dane uczestników od partnerów projektu mogą być dostępne dla koordynatora CyberAgent, a pozostali partnerzy nie mogą wzajemnie przeglądać swoich danych uczestników. Po zakończeniu projektu koordynator może uzyskać dostęp wyłącznie do zanonimizowanych danych innych partnerów w celu monitorowania rezultatów projektu, określonych we wniosku projektowym, przez okres do 5 lat po zakończeniu projektu.

Oferujemy szkolenia dostosowane do potrzeb naszych zróżnicowanych grup docelowych. Studenci uczelni wyższych i kształcenia i szkolenia zawodowego mogą uczestniczyć w szkoleniu poprzez uniwersyteckie sesje kontaktowe. Pracownicy MŚP mogą wybrać metodę nauczania, która najlepiej odpowiada ich potrzebom: nauczanie mieszane, wyłącznie online lub, rzadziej, udział w zajęciach na uczelni lub w kształceniu i szkoleniu zawodowym.

Szkolenia mogą być również oferowane większym firmom zatrudniającym wielu pracowników. W takich przypadkach metoda szkoleniowa zostanie dostosowana do konkretnych potrzeb, przy jednoczesnym uwzględnieniu kursów modułowych CyberAgent.

Po zarejestrowaniu się na platformie uczestnicy wybierają metodę nauki i rozpoczynają naukę. Po ukończeniu modułu lub jego części mogą zakwalifikować się do otrzymania Certyfikatu Uczestnictwa lub Certyfikatu Ukończenia Kursu, który jest wydawany, jeśli uczestnik zda test modułowy z wynikiem co najmniej 75%.

Na koniec uczestnicy są zobowiązani do wypełnienia formularza informacji zwrotnej przed otrzymaniem jakiegokolwiek certyfikatu. Ta informacja zwrotna ma kluczowe znaczenie dla ciągłego doskonalenia naszej oferty szkoleniowej i zapewnienia satysfakcji uczestników.

**Sposoby uczenia się/szkolenia**

**Pracownicy** mają kilka możliwości angażowania się w treść kursu:

- Jeśli uczelnie lub instytucje kształcenia i szkolenia zawodowego zezwalają pracownikom na udział w wykładach jako uczestnik gościnny, pracownik może uczestniczyć w wykładach razem z zapisanymi studentami. Takie zewnętrzne sesje uczestników mogą być organizowane 1-2 razy w roku, w oparciu o opublikowany harmonogram wykładów.
- Pracownicy mogą zdecydować się na szkolenie mieszane, w którym sesje szkoleniowe są prowadzone w określonych terminach z zalecanym czasem trwania 2-4 miesięcy. Wskazane są grupy liczące co najmniej 10 uczestników, maksymalnie 30 uczestników w grupie. Szkolenie mieszane obejmuje zarówno konsultacje bezpośrednie, jak i online na początku, w trakcie i na końcu kursu, aby ułatwić bezpośrednią informację zwrotną i przygotowanie się do oceny końcowej.

- Pracownicy mogą wybrać sposób nauki online do nauki we własnym tempie, bez ustalonego czasu trwania kursu.
- Więcej szczegółów na temat modułów CyberAgent znajduje się w sekcji 1. Ścieżka nauki.

**Zaangażowanie uczniów**

Studenci zapisani na program studiów z zakresu cyberbezpieczeństwa mogą napotkać różne ścieżki w zależności od przepisów obowiązujących w ich instytucji akademickiej. Mogą być zobowiązani do ukończenia niektórych lub wszystkich modułów CyberAgent lub, w zależności od wewnętrznych zasad uczelni, studenci, którzy spełniają kryteria, mogą zdecydować się na studiowanie jednego lub wielu modułów CyberAgent. Studenci szkół wyższych lub kształcenia i szkolenia zawodowego zazwyczaj angażują się w przedmioty poprzez tradycyjne nauczanie w klasie, zapewniane przez ich instytucję, lub mogą zdecydować się na metody samodzielnej nauki, aby przygotować się do końcowego testu sprawdzającego wiedzę.

**Zaangażowanie MŚP**

W organizacjach, w których szkolenie z zakresu cyberbezpieczeństwa jest konieczne, przedstawiciel firmy może zarejestrować organizację na wewnętrzne sesje szkoleniowe. W takich przypadkach, po odrębnym uzgodnieniu z uczelnią i/lub wykładowcami, sposób szkolenia, harmonogram i wydawanie certyfikatów mogą być dostosowane do specyficznych potrzeb organizacji w oparciu o istniejące moduły.

**Zbieranie opinii**

Po ukończeniu modułu uczestnicy są zobowiązani do wypełnienia anonimowego formularza opinii dostępnego online. Dane zwrotne są dostępne tylko dla upoważnionego personelu w organizacji partnera, przy czym podobne środki poufności są stosowane podczas pilotażowych sesji szkoleniowych i wykorzystania danych po zakończeniu projektu.

Informacje zwrotne będą zbierane głównie od uczestników kursu, ale zbierane będą również informacje zwrotne od mentorów/trenerów. Zebrane informacje zwrotne ocenią organizacyjny poziom satysfakcji uczestników, aspekty organizacji kursu, proces uczenia się, wykorzystanie zdobytych kompetencji w praktyce, treść kursu, strategie oceny, włączenie elementów grywalizacji, obszary do poprawy itp.

Wyniki informacji zwrotnej będą regularnie przeglądane i przedstawiane zespołowi zarządzającemu projektem, aby szybko reagować i ulepszać strategie szkoleniowe zgodnie z rzeczywistymi potrzebami i zmianami rynkowymi.

Dopiero po wypełnieniu tego formularza uczestnicy są uprawnieni do otrzymania certyfikatu uczestnictwa lub certyfikatu ukończenia kursu lub certyfikatu uczestnictwa.

**Certyfikat ukończenia kursu**

Pozytywne zaliczenie testu oceniającego skutkuje wygenerowaniem certyfikatu ukończenia kursu dla uczestnika. W każdym module odbywa się jeden test końcowy.

**Certyfikat uczestnictwa**

Uczestnicy, którzy nie zdecydują się na udział w teście sprawdzającym wiedzę, mogą otrzymać certyfikat uczestnictwa. Potwierdzenie to może zostać wydane po ukończeniu pojedynczego modułu lub kilku mikroczęści w ramach kursu.

## WNIOSKI I PODSUMOWANIE

W niniejszym sprawozdaniu z powodzeniem opracowano ustrukturyzowane ścieżki szkoleniowe dla podmiotów odpowiedzialnych za zmiany w zakresie cyberbezpieczeństwa MŚP, dostosowane do konkretnych potrzeb na różnych poziomach edukacyjnych i zawodowych, od instytucji szkolnictwa wyższego po kształcenie i szkolenie zawodowe oraz bezpośrednie szkolenia pracowników MŚP. Opracowany program nauczania, składający się z ośmiu kompleksowych modułów, integruje umiejętności techniczne, analityczne, organizacyjne i zarządzania ryzykiem, które są kluczowe dla skutecznego wzmocnienia pozycji przyszłych specjalistów ds. cyberbezpieczeństwa.

Ustrukturyzowane podejście do ścieżek edukacyjnych zapewnia kompleksową podróż edukacyjną dla pracowników MŚP. Poprzez etapy wstępnego nauczania, nauki i etapu po nauce, wspiera zapamiętywanie wiedzy i praktyczne zastosowanie. Mikromoduły oferują elastyczność i możliwość dostosowania do indywidualnych potrzeb, wzbogacając naukę o mikropoświadczenia, które zapewniają uznane kwalifikacje. To dostosowanie do standardów branżowych znacząco przyczynia się do wzmocnienia zdolności w zakresie cyberbezpieczeństwa w MŚP, przygotowując pracowników do sprostania obecnym wyzwaniom i przyszłym postępom. Poniższa analiza Ścieżki Kariery nakreśliła progresję ról związanych z cyberbezpieczeństwem zgodnie z definicją w ramach ESCO, ułatwiając ukierunkowane podejście edukacyjne, które przygotowuje osoby do skutecznej integracji z pracownikami zajmującymi się cyberbezpieczeństwem, ostatecznie zwiększając ich perspektywy kariery i rozwój zawodowy.

Zbadana różnorodność podejść pedagogicznych w ramach programu nauczania cyberbezpieczeństwa powinna umożliwić stworzenie dynamicznego i elastycznego środowiska uczenia się, które uwzględnia różne style uczenia się i potrzeby. Włączenie różnych metod nauczania, w tym wykładów teoretycznych, laboratoriów praktycznych, grywalizacji i projektów opartych na współpracy, zapewnia, że uczniowie są nie tylko odbiorcami wiedzy, ale także aktywnymi uczestnikami swojej podróży edukacyjnej. Ta kompleksowa strategia powinna zwiększyć zaangażowanie, zrozumienie i lepiej przygotować uczniów do rzeczywistych wyzwań związanych z cyberbezpieczeństwem. Możliwość dostosowania metod nauczania do wymagań specyficznych dla modułu powinna jeszcze bardziej spersonalizować doświadczenie uczenia się, zapewniając, że efekty edukacyjne są maksymalizowane dla każdego ucznia.

Dzięki systematycznemu mapowaniu podtematów i modułów projektu CyberAgent na uznane na całym świecie jednostki wiedzy, program nauczania nie tylko spełnia, ale i wyprzedza dynamiczne wymagania w dziedzinie cyberbezpieczeństwa. To metodyczne podejście zapewnia, że każdy efekt uczenia się jest strategicznie powiązany z rzeczywistymi kompetencjami, które mają kluczowe znaczenie dla skutecznego zarządzania zagrożeniami cybernetycznymi. Zdolność adaptacji programu nauczania pozwala mu pełnić różne role zawodowe w branży, przygotowując uczniów nie tylko do bezpośrednich wyzwań, ale także do długoterminowego rozwoju kariery w cyberbezpieczeństwie.

Nakreślona strategia oceny kursu oferuje ramy oceny biegłości i postępów studentów w programach cyberbezpieczeństwa. Dwuetapowe podejście, łączące testy samooceny i

kompleksowe testy oceny wiedzy, pozwala uczniom aktywnie angażować się w materiał, stale oceniać swoje zrozumienie i odpowiednio dostosowywać strategie uczenia się. Opracowując ocenę w taki sposób, aby zarówno instytucje szkolnictwa wyższego, jak i studenci kształcenia i szkolenia zawodowego zadawali pytania dostosowane do indywidualnych potrzeb, strategia zapewnia adekwatność i adekwatność dla każdego poziomu kształcenia, poprawiając doświadczenie edukacyjne. Metoda ta umożliwia wyraźną miarę opanowania i gotowości ucznia do praktycznego zastosowania wiedzy. Co więcej, wprowadzenie elementów grywalizacji, takich jak odznaki i systemy punktacji, nie tylko motywuje uczniów, ale także sprzyja konkurencyjnemu, ale opartemu na współpracy środowisku uczenia się.

Wreszcie, proces uczenia się i nauczania CyberAgent zapewnia kompleksowe i elastyczne ramy edukacyjne odpowiednie dla zróżnicowanego grona uczniów z uczelni wyższych, instytucji kształcenia i szkolenia zawodowego oraz MŚP. System ten pozwala na różne metody partycypacyjne, w tym uczenie się twarzą w twarz, mieszane i online, zapewniając elastyczność w sposobie prowadzenia szkoleń z zakresu cyberbezpieczeństwa i dostępu do nich. Rejestracja na platformie CyberAgent inicjuje ścieżkę, w której uczestnicy wybierają preferowane moduły i metody nauczania, a jej zwieńczeniem jest wydanie certyfikatów po pomyślnym ukończeniu i ocenie. Struktura ta nie tylko wspiera spersonalizowane trajektorie uczenia się, ale także jest zgodna z rygorystycznymi standardami prywatności niezbędnymi do zachowania poufności uczestników w całym procesie szkoleniowym.

Zalecenia i wskazówki zawarte w tym dokumencie zostaną wykorzystane w następnej fazie do opracowania kompleksowych programów szkoleniowych CyberAgent, materiałów szkoleniowych, testów wiedzy i ocen, ćwiczeń praktycznych i innych treści szkoleniowych, które zostaną zintegrowane z platformą szkoleniową CyberAgent.

## ZAŁĄCZNIK 1. OPIS MODUŁU

**OPIS MODUŁU**

| Tytuł modułu | Kod modułu |
|---|---|
| ... | |

| Wykładowca (-y) | Instytucja lub dział, w którym dostarczany jest moduł |
|---|---|
| ... | ... |

| Sposób dostawy | Język |
|---|---|
| *Konsultacje bezpośrednie, online, mieszane,* | *Angielski, ...* |

| Warunki wstępne |
|---|
| ... |

| Liczba przyznanych punktów ECTS | Nakład pracy studenta | Czas pracy kontaktowej | Indywidualny czas pracy |
|---|---|---|---|
| 5 | ... | ... | ... |

| Cel i rezultaty modułu | | |
|---|---|---|
| ... | | |
| **Efekty kształcenia modułu** | **Metody nauczania i uczenia się** | **Metody oceniania** |
| Umiejętności techniczne | | |
| Umiejętności analityczne | | |
| Umiejętności związane z ryzykiem | | |
| Umiejętności organizacyjne | | |

| Ułatwienia korzystania z zasobów (sprzęt, oprogramowanie, technologia) |
|---|
| ... |

| Zawartość modułu: podział tematów | Kontaktowe godziny pracy | | | | | Indywidualne godziny pracy i zadania | |
|---|---|---|---|---|---|---|---|
| | Wykładowcy (HEI/VET) | Konsultacje (MŚP) | Praktyka (HEI/VET) | Testy | **Łącznie wszystkie godziny** | **Praca indywidualna** | **Zadania** |
| 1 | | | | | | | |
| ... | | | | | | | |
| n | | | | | | | |
| **Łącznie** | | | | | | | |

| Strategia oceny | Porównawcza wartość procentowa wagi | Kryteria oceniania |
|---|---|---|
| Autotest I | | ... |
| ... | | ... |
| Autotest n | | ... |
| Test sprawdzający wiedzę | | ... |
| | | |
| **HEI/VET certyfikacja -> Autotest I + ...+ Autotest n + Test sprawdzający wiedzę** | | |
| **MŚP/Certyfikacja samodzielnej nauki -> Autotest I + ...+ Autotest n + Test sprawdzający wiedzę** | | |
| **Mikromoduły, mikrosekcje -> Autotest I (opcjonalny), Autotest n (opcjonalny)** | | |

| **Materiały do nauki** *(nazwisko, inicjał. (Rok, Miesiąc, Dzień). Tytuł artykułu. Tytuł czasopisma/czasopisma/gazety, numer tomu (numer wydania), numery stron całego artykułu, wydawca, adres URL)* |
|---|
| **Lektura obowiązkowa** |
| ... |
| **Rekomendowane lektury** |
| ... |

CyberAgent

Co-funded by the European Union

# Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

## Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau