Program studiów podyplomowych
MBA Zarządzanie cyberbezpieczeństwem /+AI/ w edukacji

Liczba zjazdów	minimum 6 w semestrze
Liczba godzin	330 godzin
ECTS	94 punkty

Moduł 1: Podstawy cyberbezpieczeństwa i zarządzania AI w edukacji

1. Podstawy cyberbezpieczeństwa w instytucjach edukacyjnych
    - Wprowadzenie do zagadnień cyberbezpieczeństwa.
    - Podstawowe zagrożenia i sposoby ich identyfikacji (phishing, malware, ransomware).
    - Audyt bezpieczeństwa systemów edukacyjnych.
2. Prawo i regulacje w zakresie ochrony danych osobowych
    - RODO (GDPR) w instytucjach edukacyjnych.
    - Odpowiedzialność administracyjna i karna za naruszenia.
    - Polityka prywatności w placówkach oświatowych.
3. Wprowadzenie do sztucznej inteligencji w edukacji
    - Definicje i podstawowe koncepcje AI.
    - Rola AI w zarządzaniu placówkami edukacyjnymi.
    - Przegląd narzędzi AI wspierających procesy administracyjne i dydaktyczne.
4. Zarządzanie infrastrukturą IT w placówkach edukacyjnych
    - Planowanie i utrzymanie infrastruktury technologicznej.
    - Wdrożenie systemów zarządzania edukacją (e-dzienniki, platformy LMS).
    - Monitoring i aktualizacje systemów IT.

Moduł 2: Rozwój kompetencji zarządczych w cyberbezpieczeństwie i AI

1. Zarządzanie ryzykiem w cyberbezpieczeństwie
    - Identyfikacja, ocena i minimalizacja ryzyk w systemach IT.
    - Tworzenie i wdrażanie polityki bezpieczeństwa w placówkach edukacyjnych.
    - Zarządzanie kryzysowe w przypadku naruszenia bezpieczeństwa.
2. AI w personalizacji procesu nauczania
    - Algorytmy i systemy adaptacyjne wspierające nauczanie.
    - Personalizacja treści edukacyjnych przy użyciu AI.
    - Case studies: Zastosowanie AI w edukacji na różnych poziomach.
3. Szkolenie pracowników w zakresie cyberbezpieczeństwa
    - Programy podnoszenia świadomości bezpieczeństwa cyfrowego.
    - Metodyka szkoleń dla nauczycieli, uczniów i administracji.
    - Budowanie kultury bezpieczeństwa w środowisku szkolnym.
4. Zarządzanie danymi i analiza predykcyjna w edukacji
    - Analiza danych uczniów i nauczycieli przy użyciu narzędzi AI.
    - Ochrona danych wrażliwych w systemach edukacyjnych.
    - Wykorzystanie analityki predykcyjnej do poprawy wyników nauczania.

Moduł 3: Zastosowanie wiedzy i projektowanie rozwiązań

1. Etyka i odpowiedzialność w AI i cyberbezpieczeństwie
    - Problematyka uprzedzeń algorytmicznych.
    - Standardy etyczne w wykorzystaniu AI w edukacji.
    - Bezpieczeństwo psychologiczne uczniów w środowisku cyfrowym.
2. Zarządzanie incydentami i audyt bezpieczeństwa
    - Tworzenie planów reagowania na incydenty (IRP).
    - Przeprowadzanie audytów bezpieczeństwa w placówkach edukacyjnych.
    - Dokumentowanie i raportowanie naruszeń bezpieczeństwa.
3. Case study: Rozwiązania w edukacji cyfrowej
    - Analiza udanych wdrożeń systemów AI w edukacji.
    - Studium przypadków zarządzania incydentami w instytucjach edukacyjnych.
    - Projektowanie modelowych rozwiązań dla placówek edukacyjnych.

Moduł 4: Psychologia i kształtowanie kompetencji miękkich

1. Komunikacja interpersonalna w zarządzaniu edukacją
    - Techniki skutecznej komunikacji w zespole.
    - Budowanie relacji z rodzicami, nauczycielami i uczniami.
    - Zarządzanie konfliktami i mediacje.
2. Przywództwo i zarządzanie zespołami
    - Rola lidera w środowisku edukacyjnym.
    - Motywowanie i angażowanie zespołów w procesy transformacji cyfrowej.
    - Rozwój kompetencji lidera.
3. Zarządzanie stresem i emocjami
    - Techniki radzenia sobie ze stresem w pracy menedżera edukacji.
    - Wsparcie psychologiczne dla zespołów w sytuacjach kryzysowych.
    - Budowanie odporności psychicznej w środowisku zawodowym.
4. Kultura organizacyjna i innowacyjność
    - Tworzenie pozytywnej kultury organizacyjnej.
    - Promowanie innowacji w edukacji i zarządzaniu.
    - Zarządzanie zmianą i adaptacja do nowych technologii.

Moduł 5: Praca dyplomowa

1. Opracowanie strategii cyberbezpieczeństwa lub zastosowania AI w edukacji
    - Tworzenie kompleksowych strategii dla placówek edukacyjnych.
    - Konsultacje z ekspertami w zakresie wdrażania rozwiązań technologicznych.
2. Analiza studium przypadku wybranego wdrożenia technologicznego
    - Analiza danych i efektywności wdrożonych systemów.
    - Prezentacja wyników i rekomendacje dla praktyki edukacyjnej.
3. Obrona projektu przed komisją
    - Przygotowanie do prezentacji wyników.
    - Dyskusja i ocena praktycznego zastosowania opracowanych rozwiązań.

Sylwetka absolwenta

Absolwent posiada zaawansowaną wiedzę z zakresu zarządzania cyberbezpieczeństwem oraz zastosowania sztucznej inteligencji w sektorze edukacyjnym. Zna nowoczesne narzędzia i technologie ochrony danych oraz systemów informatycznych, z uwzględnieniem specyfiki instytucji edukacyjnych. Potrafi analizować ryzyka związane z cyberzagrożeniami, projektować strategie bezpieczeństwa oraz wdrażać polityki ochrony informacji w placówkach edukacyjnych. Wykazuje umiejętność wykorzystania sztucznej inteligencji w zarządzaniu procesami edukacyjnymi, w tym w personalizacji nauczania, analityce danych edukacyjnych oraz automatyzacji administracji. Dysponuje kompetencjami w zakresie zarządzania zespołami interdyscyplinarnymi, łączącymi specjalistów IT, pedagogów i administratorów, w celu budowania cyfrowo bezpiecznego środowiska edukacyjnego.