OPISY PRZEDMIOTÓW OBIERALNYCH

Nazwa kierunku studiów	Cyberbezpieczeństwo Informatyka
Poziom studiów	studia drugiego stopnia
Rocznik	2025/2026
Semestr, w którym przedmioty są wybierane	**1**
Semestr, w którym przedmioty są realizowane	**2**

Przedmioty obieralne umożliwiają zdobywanie wiedzy i rozwijanie umiejętności ważnych dla kierunku, ale z uwzględnieniem indywidualnych zainteresowań studenta.
W tym semestrze macie Państwo możliwość wyboru części przedmiotów obieralnych, a wybrane przedmioty będą realizowane w kolejnym semestrze.
Przedmiot może być realizowany jeśli zbierze się wystarczająca liczba chętnych studentów (nie mniej niż 66% studentów dokonujących wyboru).
W tym semestrze wyboru dokonacie Państwo za pomocą ankiety, która zostanie udostępniona 20. kwietnia (ankieta będzie aktywna przez tydzień). Studenci którzy nie dokonają wyboru, zostaną administracyjnie dopisani do przedmiotów które będą realizowane.

W semestrze letnim 2025/26 wybieracie Państwo 2 przedmioty kierunkowe z 4 oferowanych:

METODY WYSZUKIWANIA INFORMACJI W DUŻYCH ZBIORACH DANYCH

Wymagania wstępne (wynikające z następstwa przedmiotów):
- Algorytmy i struktury danych, Matematyka w zakresie algebry

Treści kształcenia:
- Samoorganizujące się struktury danych: listy, B-drzewa
- Mieszanie (hashing): metody usuwania kolizji, konstrukcja funkcji mieszających, klasa uniwersalna funkcji mieszających.
- Wyszukiwanie wzorca, w tym przypadek wielowymiarowy

BIG DATA I TRANSFORMACJA CYFROWA

Treści kształcenia:
- Big data i cyfrowa transformacja – wprowadzenie do dziedziny oraz definicja podstawowych pojęć
- Dane – podstawa działania nowoczesnych firm
- Big data – architektura rozwiązań. Przegląd środowisk programowych dostępnych na rynku. Charakterystyka architektury i funkcjonalności
- Transformacja cyfrowa procesów biznesowych
- Wsparcie big data dla łańcucha wartości. Konkurowanie w oparciu o analitykę w procesach wewnętrznych

- Metody deklaratywnie i programistyczne w implementacji CRM
- Wsparcie big data dla procesu podejmowania decyzji menedżerskich. Poziomy zarządzania i typy decyzji
- Planowanie strategii big data w organizacji. Podnoszenie kompetencji analitycznych organizacji
- Praktyczne zastosowania AI w aplikacjach biznesowych
- Aspekty prawne związane z big data i transformacją cyfrową

INFORMATYKA ŚLEDCZA

Treści kształcenia:

- Wprowadzenie do informatyki śledczej – pojęcia i zagadnienia
- Rodzaje przestępstw i związane z nimi zagrożenia
- Rodzaje dochodzeń w informatyce śledczej
- Proces analizy śledczej w środowisku cyfrowym
- Techniki i narzędzia wykorzystywane w informatyce śledczej
- Zabezpieczenie dowodów i analiza danych cyfrowych
- Ocena podatności na ataki oraz identyfikacja luk w zabezpieczeniach aplikacji i systemów operacyjnych
- Trendy i istotne osiągnięcia w zakresie wykorzystania technologii informatycznych w informatyce śledczej

ANALIZA RYZYKA

Treści kształcenia:

- Wprowadzenie do analizy ryzyka w kontekście systemów informatycznych: specyfika ryzyka IT, różnice między ryzykiem IT a ryzykiem biznesowym.
- Proces zarządzania ryzykiem IT: identyfikacja aktywów IT, identyfikacja zagrożeń i luk w systemach informatycznych, analiza podatności.
- Metody analizy ryzyka IT:
- Jakościowe: macierze ryzyka, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation);
- Ilościowe: FAIR (Factor Analysis of Information Risk), analiza kosztów i korzyści.
- Ocena ryzyka IT: określanie akceptowalnego poziomu ryzyka, analiza wpływu na biznes (Business Impact Analysis - BIA).
- Reagowanie na ryzyko IT: strategie minimalizacji ryzyka w projektach IT, planowanie awaryjne i odzyskiwanie po awarii (Disaster Recovery Planning - DRP).
- Standardy i dobre praktyki w analizie ryzyka IT: ISO 27005, NIST Risk Management Framework.
- Analiza ryzyka w cyklu życia oprogramowania (Software Development Life Cycle - SDLC): modelowanie zagrożeń (Threat Modeling), analiza ryzyka w testowaniu penetracyjnym.
- Ryzyko cybernetyczne: analiza ryzyka związanego z atakami cybernetycznymi, metody oceny ryzyka w cyberprzestrzeni.
- Studium przypadków: analiza rzeczywistych przykładów incydentów bezpieczeństwa i związanych z nimi ryzyk.