Program studiów podyplomowych
Antyterroryzm i zaawansowane cyberbezpieczeństwo

Liczba zjazdów	minimum 6 w semestrze
Liczba godzin	220 godzin
ECTS	60 punktów

Semestr 1: Podstawy i kluczowe aspekty bezpieczeństwa

Moduł 1: Wprowadzenie do antyterroryzmu

- Historia i typologie terroryzmu
- Ewolucja organizacji terrorystycznych.
- Typologie działań terrorystycznych (religijny, polityczny, cyberterroryzm).
- Strategie przeciwdziałania terroryzmowi
- Globalne inicjatywy antyterrorystyczne (ONZ, NATO).
- Rola służb specjalnych i międzynarodowej współpracy.

Moduł 2: Cyberbezpieczeństwo – podstawy

- Wprowadzenie do cyberzagrożeń
- Rodzaje zagrożeń: malware, phishing, ransomware.
- Analiza rzeczywistych cyberataków.
- Prawo i regulacje w cyberbezpieczeństwie
- RODO (GDPR), NIS2, i inne regulacje unijne.
- Międzynarodowe prawo w zwalczaniu cyberprzestępczości.

Moduł 3: Zarządzanie kryzysowe

- Zarządzanie sytuacjami kryzysowymi w antyterroryzmie
- Tworzenie planów działania w sytuacjach nadzwyczajnych.
- Negocjacje z terrorystami – psychologiczne aspekty.
- Reagowanie na incydenty cybernetyczne
- Tworzenie planu reagowania na cyberincydenty (IRP).
- Analiza ryzyka i ocena skutków naruszeń.

Moduł 4: Technologie w bezpieczeństwie

- Technologie antyterrorystyczne
- Drony, systemy monitoringu, biometryczne technologie identyfikacji.
- Systemy ochrony w dużych obiektach publicznych.

- Podstawy kryptografii
- Symetryczne i asymetryczne algorytmy szyfrowania.
- Zastosowanie blockchain w ochronie danych.

Zajęcia praktyczne i warsztaty

- Symulacje sytuacji kryzysowych (atak terrorystyczny, cyberatak).
- Praca z systemami IDS/IPS do wykrywania zagrożeń.

Semestr 2: Zaawansowane techniki i specjalizacja

Moduł 1: Zaawansowane cyberbezpieczeństwo

- Etyczny hacking i testy penetracyjne
- Narzędzia do testów penetracyjnych (np. Metasploit, Kali Linux).
- Wykrywanie i eliminowanie luk w zabezpieczeniach.
- Analiza złośliwego oprogramowania
- Techniki analizy malware (statyczna, dynamiczna).
- Tworzenie raportów i przeciwdziałanie zagrożeniom.

Moduł 2: Antyterroryzm – zaawansowane działania

- Profilowanie terrorystów i analiza behawioralna
- Techniki wykrywania zagrożeń na podstawie zachowań.
- Identyfikacja schematów działań organizacji terrorystycznych.
- Zarządzanie operacjami antyterrorystycznymi
- Planowanie operacji prewencyjnych.
- Przykłady udanych interwencji antyterrorystycznych.

Moduł 3: Sztuczna inteligencja w bezpieczeństwie

- Zastosowanie AI w cyberbezpieczeństwie
- Automatyczne wykrywanie zagrożeń (SIEM, ML).
- Analiza danych big data w ochronie systemów IT.
- AI w prewencji i antyterroryzmie
- Rozpoznawanie obrazów i analizowanie treści online.
- Predykcja zagrożeń na podstawie danych.

Moduł 4: Zarządzanie bezpieczeństwem w organizacjach

- Tworzenie polityk bezpieczeństwa
- Procedury zabezpieczania systemów IT.
- Polityka prywatności i zarządzanie danymi.

- Ochrona infrastruktury krytycznej
- Identyfikacja kluczowych zasobów i ich ochrona.
- Zarządzanie incydentami w infrastrukturze krytycznej.

Zajęcia praktyczne i warsztaty

- Ćwiczenia w zakresie testów penetracyjnych na systemach rzeczywistych.
- Warsztaty z wykorzystania SIEM (Security Information and Event Management).
- Symulacja operacji antyterrorystycznej – współpraca zespołowa.

Projekt dyplomowy i zaliczenie

- Opracowanie kompleksowego projektu z zakresu cyberbezpieczeństwa lub antyterroryzmu:

Sylwetka absolwenta

Absolwent studiów ***Antyterroryzm i zaawansowane cyberbezpieczeństwo*** to specjalista łączący wiedzę z zakresu przeciwdziałania zagrożeniom terrorystycznym z zaawansowanymi umiejętnościami w obszarze ochrony cyberprzestrzeni.

Absolwent zna:

- Zasady i mechanizmy współczesnego terroryzmu
- Podstawy prawne i procedury antyterrorystyczne
- Cyberbezpieczeństwo w kontekście zagrożeń terrorystycznych

. Absolwent potrafi:

- Identyfikować zagrożenia terrorystyczne i cyberzagrożenia
- Analizować i oceniać ryzyko
- Stosować zaawansowane technologie obronne
- Zarządzać incydentami
- Tworzyć strategię ochrony przed zagrożeniami terrorystycznymi i cybernetycznymi
- Współpracować z zespołami reagowania kryzysowego oraz służbami bezpieczeństwa
- Ocenić wpływ nowoczesnych technologii, takich jak sztuczna inteligencja czy blockchain, na kwestie bezpieczeństwa