| KIERUNEK STUDIÓW | LICZBA GODZIN WYKŁADÓW | LICZBA GODZIN ĆWICZEŃ / WARSZTATÓW | LICZBA PUNKTÓW ECTS |
|---|---|---|---|
| **1. Wprowadzenie do antyterroryzmu** | | | |
| Historia i typologie terroryzmu | 2 | 0 | 6 |
| Ewolucja organizacji terrorystycznych | 2 | 0 | |
| Typologie działań terrorystycznych (religijny, polityczny, cyberterroryzm) | 2 | 0 | |
| Typologie działań terrorystycznych (religijny, polityczny, cyberterroryzm) | 2 | 0 | |
| Strategie przeciwdziałania terroryzmowi | 2 | 0 | |
| Globalne inicjatywy antyterrorystyczne (ONZ, NATO | 2 | 0 | |
| Rola służb specjalnych i międzynarodowej współpracy | 2 | 0 | |
| RAZEM W MODULE | 14 | 0 | |
| | 14 | | |
| **2. Cyberbezpieczeństwo - podstawy** | | | |
| Wprowadzenie do cyberzagrożeń | 2 | 0 | 4 |
| Rodzaje zagrożeń: malware, phishing, ransomware | 2 | 0 | |
| Analiza rzeczywistych cyberataków | 0 | 5 | |
| Prawo i regulacje w cyberbezpieczeństwie | 2 | 0 | |
| RODO (GDPR), NIS2, i inne regulacje unijne | 2 | 0 | |
| Międzynarodowe prawo w zwalczaniu cyberprzestępczo | 2 | 0 | |
| RAZEM W MODULE | 10 | 5 | |
| | 15 | | |
| **3. Zarządzanie kryzysowe** | | | |
| Zarządzanie sytuacjami kryzysowymi w antyterroryzm | 2 | 0 | 4 |
| Tworzenie planów działania w sytuacjach nadzwyczajny | 0 | 5 | |
| Negocjacje z terrorystami - psychologiczne aspekty | 2 | 0 | |
| Reagowanie na incydenty cybernetyczne | 2 | 0 | |
| Tworzenie planu reagowania na cyberincydenty (IRP). | 0 | 5 | |
| Analiza ryzyka i ocena skutków naruszeń | 0 | 5 | |
| RAZEM W MODULE | 6 | 15 | |
| | 21 | | |
| **4. Technologie w bezpieczeństwie** | | | |
| Technologie antyterrorystyczne. | 3 | 0 | 4 |
| Drony, systemy monitoringu, biometryczne technologie | 5 | 0 | |
| Systemy ochrony w dużych obiektach publicznych | 5 | 0 | |
| Podstawy kryptografii | 5 | 0 | |
| Symetryczne i asymetryczne algorytmy szyfrowania | 5 | 0 | |
| Zastosowanie blockchain w ochronie danych | 5 | 0 | |
| RAZEM W MODULE | 28 | 0 | |
| | 28 | | |
| **5. Zajęcia praktyczne i warsztaty** | | | |
| Symulacje sytuacji kryzysowych (atak terrorystyczny, cyberatak) | 0 | 5 | 7 |
| Praca z systemami IDS/IPS do wykrywania zagrożeń | 0 | 5 | |
| RAZEM W MODULE | 0 | 10 | |
| | 10 | | |
| **6. Zaawansowane cyberbezpieczeństwo** | | | |
| Etyczny hacking i testy penetracyjne | 2 | 0 | 4 |
| Narzędzia do testów penetracyjnych (np. Metasploit, | 0 | 5 | |
| Wykrywanie i eliminowanie luk w zabezpieczeniach | 0 | 5 | |
| Analiza złośliwego oprogramowania | 0 | 5 | |
| Techniki analizy malware (statyczna, dynamiczna) | 5 | 0 | |
| Tworzenie raportów i przeciwdziałanie zagrożeniom | 0 | 5 | |
| RAZEM W MODULE | 7 | 20 | |
| | 27 | | |
| **7. Antyterroryzm - zaawansowane działania** | | | |
| Profilowanie terrorystów i analiza behawioralna | 0 | 5 | 5 |
| Techniki wykrywania zagrożeń na podstawie zachowań | 5 | 0 | |
| Identyfikacja schematów działań organizacji terrorys | 5 | 0 | |
| Zarządzanie operacjami antyterrorystycznymi | 5 | 0 | |
| Planowanie operacji prewencyjnych | 0 | 5 | |
| Przykłady udanych interwencji antyterrorystycznych | 5 | 0 | |
| RAZEM W MODULE | 20 | 10 | |
| | 30 | | |
| **8. Sztuczna inteligencja w bezpieczeństwie** | | | |
| Zastosowanie AI w cyberbezpieczeństwie | 5 | 0 | 5 |
| Automatyczne wykrywanie zagrożeń (SIEM, ML) | 5 | 0 | |
| Analiza danych big data w ochronie systemów IT | 0 | 5 | |
| AI w prewencji i antyterroryzmie | 5 | 0 | |
| Rozpoznawanie obrazów i analizowanie treści online | 0 | 5 | |
| Predykcja zagrożeń na podstawie danych | 0 | 5 | |
| RAZEM W MODULE | 15 | 15 | |
| | 30 | | |
| **9. Zarządzanie bezpieczeństwem w organizacjach** | | | |
| Tworzenie polityk bezpieczeństwa | 0 | 5 | 5 |
| Procedury zabezpieczania systemów IT | 5 | 0 | |
| Polityka prywatności i zarządzanie danymi | 5 | 0 | |
| Ochrona infrastruktury krytycznej | 5 | 0 | |
| Identyfikacja kluczowych zasobów i ich ochrona | 5 | 0 | |
| Zarządzanie incydentami w infrastrukturze krytycznej | 5 | 0 | |
| RAZEM W MODULE | 25 | 5 | |
| | 30 | | |
| **10. Zajęcia praktyczne i warsztaty** | | | |
| Ćwiczenia w zakresie testów penetracyjnych na systemach rzeczywistych | 0 | 5 | 8 |
| Warsztaty z wykorzystania SIEM (Security Information and Event Management) | 0 | 5 | |
| Symulacja operacji antyterrorystycznej – współpraca ze | 0 | 5 | |
| RAZEM W MODULE | 0 | 15 | |
| | 15 | | |
| 11. Projekt dyplomowy i zaliczenie | | | |
| Opracowanie kompleksowego projektu z zakresu cyberbezpieczeństwa lub antyterroryzmu | 0 | 5 | 8 |
| RAZEM W MODULE | 15 | 5 | |
| | 20 | | |
| **RAZEM GODZIN W TOKU** | 125 | 95 | 60 |
| **OGÓŁEM** | 220 | | |