

PROGRAM STUDIÓW



kierunek

CYBERBEZPIECZEŃSTWO

studia II stopnia



wskz.pl



CYBERBEZPIECZEŃSTWO

studia II stopnia

I SEMESTR

- Szkolenie BHP
- Język obcy specjalistyczny (angielski, niemiecki)
- Psychologia zachowań cyfrowych
- Zajęcia humanistyczne do wyboru 1 (Problematyka narracji mediów w kontekście manipulacji i dezinformacji / Współczesne przemiany kultury i życia społecznego)
- Zajęcia humanistyczne do wyboru 2 (Humanistyka przyszłości: człowiek, wartości, odpowiedzialność / Historia przemian społecznych XX i XXI wieku)
- Cyberzagrożenia asymetryczne i hybrydowe – analiza strategiczna
- Strategie bezpieczeństwa cyfrowego państwa i organizacji
- Zaawansowana analiza informacji i operacji informacyjnych
- Inteligentne systemy bezpieczeństwa i technologie autonomiczne
- Zaawansowane metody badań w cyberbezpieczeństwie

II SEMESTR

- Język obcy specjalistyczny (angielski, niemiecki)
- Zarządzanie ryzykiem łańcucha dostaw i nadzór nad dostawcami ICT
- Regulacje Unii Europejskiej w obszarze cyberbezpieczeństwa
- Zaawansowana analiza danych i wnioskowanie przyczynowe w cyberbezpieczeństwie
- Ilościowe modelowanie ryzyka w cyberbezpieczeństwie
- Analiza i projektowanie strategii bezpieczeństwa informacyjnego państwa
- Zajęcia specjalnościowe 1
- Seminarium magisterskie I

III SEMESTR

- Prawne aspekty cyberbezpieczeństwa
- Informatyczne systemy ochrony infrastruktury krytycznej
- Zespołowy projekt badawczo – publikacyjny
- Zajęcia specjalnościowe 2
- Zajęcia specjalnościowe 3
- Zajęcia specjalnościowe 4
- Seminarium magisterskie II

IV SEMESTR

- Nadzór i odpowiedzialność organów zarządzających w cyberbezpieczeństwie
- Big Data i analityka zagrożeń cyberbezpieczeństwa
- ZDW obcojęzyczne: Cybersecurity Compliance, Reporting and Regulatory Implementation (NIS2, DORA, CRA) / Regulatorische Vorgaben zur Cybersicherheit: Compliance, Melde- und Berichtspflichten sowie praktische Umsetzung (NIS2, DORA, CRA)
- Zajęcia specjalnościowe 5
- Zajęcia specjalnościowe 6
- Zajęcia specjalnościowe 7
- Seminarium magisterskie III



MODUŁY SPECJALNOŚCIOWE na kierunku Cyberbezpieczeństwo

1 specjalność w standardowej cenie studiów

+ możliwość realizacji dodatkowej specjalności
(dodatkowo płatna)

Cyberbezpieczeństwo i ochrona danych w administracji

- Bezpieczeństwo informacji w administracji publicznej
- Ochrona danych jako element bezpieczeństwa publicznego
- Zarządzanie ryzykiem informacji w instytucjach publicznych
- Dowody cyfrowe w postępowaniu bezpieczeństwa
- Zarządzanie tożsamością w systemach bezpieczeństwa publicznego
- Bezpieczeństwo usług cyfrowych administracji
- Projekt: Polityka bezpieczeństwa informacji w jednostce administracji

Zarządzanie cyberbezpieczeństwem i audyty bezpieczeństwa

- Audyt bezpieczeństwa organizacji
- Zarządzanie ryzykiem bezpieczeństwa
- Zarządzanie incydentami bezpieczeństwa i budowa zespołów reagowania
- Zaawansowane metody oceny bezpieczeństwa organizacji
- Zarządzanie projektami bezpieczeństwa i governance bezpieczeństwa
- Odporność organizacji na zagrożenia cybernetyczne
- Projekt: Audyt bezpieczeństwa organizacji

Cyberbezpieczeństwo infrastruktury krytycznej

- Zagrożenia cybernetyczne infrastruktury krytycznej
- Systemy infrastruktury krytycznej państwa – zagrożenia i odporność
- Analiza incydentów w środowiskach infrastruktury krytycznej
- Odporność infrastruktury krytycznej i zarządzanie kryzysowe
- Zarządzanie ciągłością działania infrastruktury krytycznej
- Ryzyko bezpieczeństwa infrastruktury krytycznej
- Projekt: Model bezpieczeństwa infrastruktury krytycznej