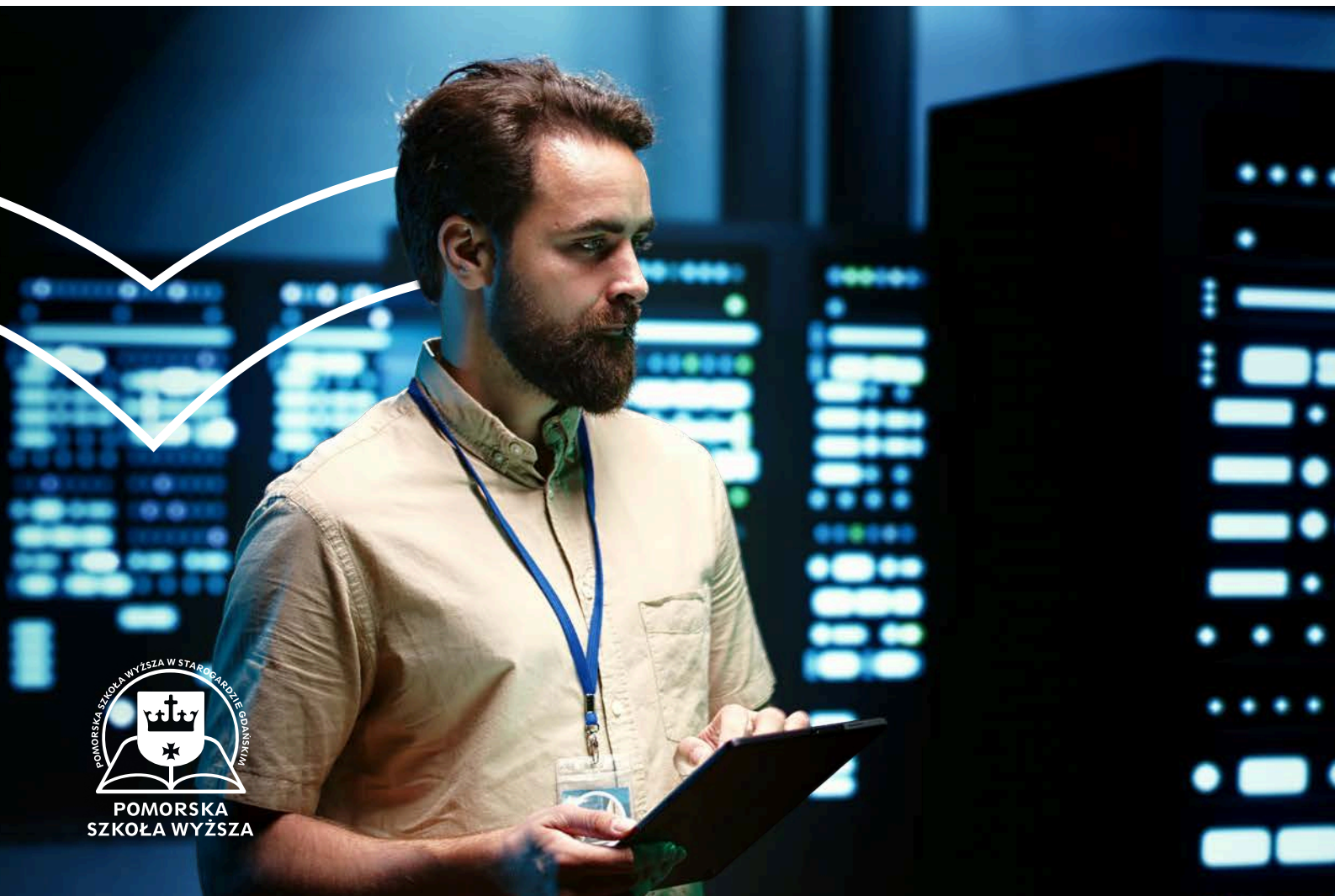


PROGRAM STUDIÓW



kierunek

CYBERBEZPIECZEŃSTWO

studia I stopnia



wskz.pl



CYBERBEZPIECZEŃSTWO

studia I stopnia

I SEMESTR

- Szkolenie BHP
- Język obcy specjalistyczny (angielski, niemiecki)
- Psychologia bezpieczeństwa
- Zajęcia humanistyczne do wyboru 1 (Filozofia z elementami etyki / Kultura współczesna)"
- Zajęcia humanistyczne do wyboru 2 (Historia kultury/ Historia cywilizacji)
- Ochrona własności intelektualnej w środowisku cyfrowym
- Współczesne zagrożenia cyberprzestrzeni Rzeczypospolitej
- Bezpieczeństwo energetyczne i infrastruktura krytyczna – wprowadzenie
- Metodologia badań w naukach o bezpieczeństwie

II SEMESTR

- Język obcy specjalistyczny (angielski, niemiecki)
- Podstawy prawa i regulacji bezpieczeństwa cyfrowego
- Administracja bezpieczeństwa cyfrowego państwa
- Podstawy technologii informacyjnych w bezpieczeństwie cyfrowym
- Psychologia zachowań cyfrowych – metody diagnozy i analizy
- Analiza i projektowanie polityk bezpieczeństwa informacji

III SEMESTR

- Język obcy specjalistyczny (angielski, niemiecki)
- Cyberprzestrzeń w bezpieczeństwie narodowym
- Bezpieczeństwo cyfrowe człowieka i organizacji
- Analiza informacji i OSINT w bezpieczeństwie
- Polityki bezpieczeństwa informacji i zarządzanie zasobami informacyjnymi
- Analiza danych cyberbezpieczeństwa i modelowanie zagrożeń

IV SEMESTR

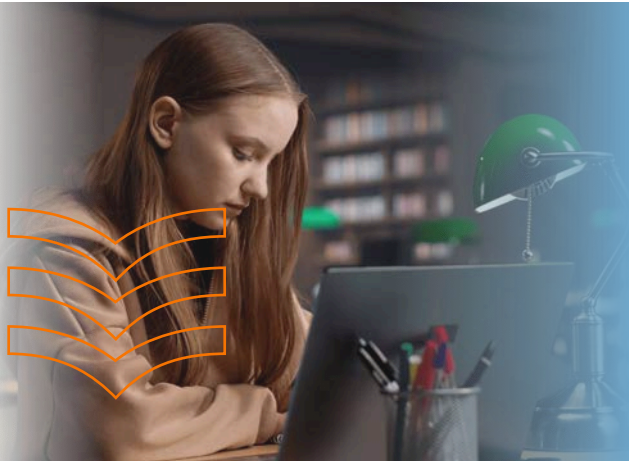
- Zajęcia do wyboru w języku obcym: Cybersecurity governance in National Security / Cyber Power and International Security / Cybersecurity-Governance in der nationalen Sicherheit / Cybermacht und internationale Sicherheit
- Kultura bezpieczeństwa cyfrowego i kompetencje cyfrowe obywateli
- Zajęcia do wyboru: Podstawy programowania / Internet rzeczy
- Zajęcia do wyboru: Geopolityka / Samorząd terytorialny w systemie bezpieczeństwa
- Analiza dezinformacji i operacji wpływu w środowisku cyfrowym
- Zajęcia specjalnościowe 1
- Zajęcia specjalnościowe 2

V SEMESTR

- Zajęcia do wyboru (Podstawy socjologii w przestrzeni cyfrowej / Podstawy ekonomii w przestrzeni cyfrowej)
- Systemy monitoringu i detekcji zagrożeń w bezpieczeństwie państwa
- Analiza ryzyka w bezpieczeństwie informacji
- Grupowy projekt badawczy
- Zajęcia specjalnościowe 3
- Zajęcia specjalnościowe 4
- Zajęcia specjalnościowe 5
- Projekt badawczy i przygotowanie do egzaminu dyplomowego I

VI SEMESTR

- Analiza zagrożeń cyfrowych w systemach bezpieczeństwa
- Analiza danych w bezpieczeństwie informacji i cyberzagrożeniach
- Zajęcia specjalnościowe 6
- Zajęcia specjalnościowe 7
- Zajęcia specjalnościowe 8
- Projekt badawczy i przygotowanie do egzaminu dyplomowego II



MODUŁY SPECJALNOŚCIOWE CYBERBEZPIECZEŃSTWO

1 specjalność w standardowej cenie studiów

+ możliwość realizacji dodatkowej specjalności
(dodatkowo płatna)

Bezpieczeństwo cyfrowe organizacji i użytkowników

- Inżynieria społeczna i zagrożenia dla użytkowników
- Projekt: Polityka bezpieczeństwa organizacji
- Podstawy bezpieczeństwa cyfrowego
- Bezpieczeństwo informacji w organizacji
- Polityki bezpieczeństwa organizacji
- Ryzyko bezpieczeństwa i metody jego oceny
- Prywatność i ochrona danych jako element bezpieczeństwa publicznego
- Komunikacja kryzysowa i reagowanie na incydenty

Bezpieczeństwo informacji i ochrona danych

- Ochrona danych jako element bezpieczeństwa publicznego
- Projekt: System ochrony informacji w organizacji
- Bezpieczeństwo informacji — podstawy
- Polityki ochrony danych w organizacjach
- Bezpieczeństwo przechowywania i przetwarzania informacji
- Zarządzanie tożsamością i dostępem w systemach bezpieczeństwa
- Bezpieczeństwo usług cyfrowych administracji
- Dowody cyfrowe w postępowaniu bezpieczeństwa