Sylwetka absolwenta

Absolwent kierunku Cyberbezpieczeństwo będzie miał wiedzę dotyczącą budowy i działania współczesnych systemów transmisji informacji i systemów służących do jej przechowywania i udostępniania. Systemy te stanowią część infrastruktury krytycznej każdego państwa i każdej firmy, dlatego muszą być szczególnie chronione. Ze względu na wzrastające zagrożenia związane z atakami na tego typu systemy konieczne jest wykształcenie specjalistów umiejących je zabezpieczyć. Wzrasta również zapotrzebowanie rynku na tego typu specjalistów. Z tego względu absolwent ma możliwość znalezienia zatrudnienia wszędzie tam, gdzie względy i polityka bezpieczeństwa, szczególnie w odniesieniu do systemów informacyjnych, jest koniecznością. Absolwent znajdzie zatrudnienie w instytucjach związanych z informatyką i telekomunikacją ICT (Information and Communication Technologies), w tym w korporacjach, bankach, przemyśle, biurach projektowych i rozwojowych przedsiębiorstw oraz w jednostkach administracji. Jest również przygotowany do podjęcia pracy w firmach produkujących sprzęt informatyczny i telekomunikacyjny, u operatorów sieci teleinformatycznych i w centrach danych. Ponadto posiada umiejętności pozwalające na projektowanie, konfigurowanie, eksploatację i serwis sprzętu informatycznego i telekomunikacyjnego.

SPECJALNOŚCI

STUDIA I STOPNIA

Bezpieczeństwo sieci teleinformatycznych

Kształcenie przygotowuje do pracy przy zabezpieczaniu dostępu do informacji na wszystkich etapach życia systemu teleinformatycznego, obejmujących planowanie systemu zabezpieczeń, jego wdrażanie i utrzymywanie w gotowości podczas eksploatacji oraz wprowadzania niezbędnych modyfikacji dostosowujących system zabezpieczeń do występujących i ciągle ewoluujących zagrożeń.

Szczególny nacisk położono na bezpieczeństwo przenoszenia informacji i dostęp do niej przy użyciu nowoczesnych systemów transmisyjnych. Kształcenie obejmuje m. in. sposoby tworzenia bezpiecznych aplikacji mobilnych, kompresję informacji, kryptografię, elektromagnetyczne bezpieczeństwo systemów i sieci, chmury obliczeniowe, systemy biometryczne, systemy monitorowania i detekcji zagrożeń, bezpieczeństwo w sieciach komputerowych, internet rzeczy, audytowanie sieci teleinformatycznych, metody bezpiecznego dostępu do sieci i aspekty prawne i etyczne w obszarze bezpieczeństwa. W ramach specjalności studenci będą przygotowani również do uzyskania certyfikatów:

- CCNA (Cisco Certified Network Associate),
- CCNA Security.

Bezpieczeństwo danych

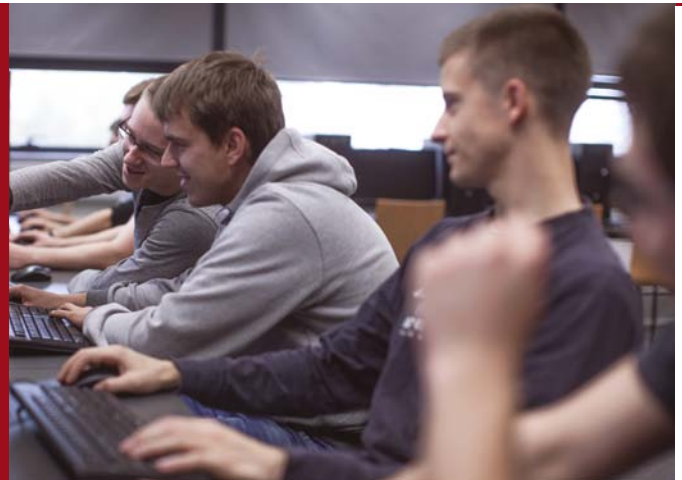
Kształcenie przygotowuje do pracy przy zabezpieczaniu informacji na wszystkich etapach jej życia, obejmujących planowanie systemu zabezpieczeń, jego wdrażanie i utrzymywanie w gotowości podczas eksploatacji oraz wprowadzania niezbędnych modyfikacji dostosowujących system zabezpieczeń do występujących i ciągle ewoluujących zagrożeń.

Szczególny nacisk położono na bezpieczeństwo przechowywanych informacji i dostęp do niej przy użyciu nowoczesnych systemów transmisyjnych. Kształcenie obejmuje m. in. sposoby tworzenia bezpiecznych usług multimedialnych, przetwarzanie dużych zbiorów informacji, struktury i działanie centrów przetwarzania danych, bazy danych, biometryczne zabezpieczanie dostępu, bezpieczeństwo w systemach rozproszonych, kryptografię, elektromagnetyczne bezpieczeństwo systemów i sieci, audytowanie sieci teleinformatycznych i bezpieczne usługi internetowe oraz informatykę śledczą związaną z analizą powłamaniową, zabezpieczaniem dowodów, zapewnianiem rzetelności i niezaprzeczalności dowodów cyfrowych. W ramach specjalności studenci będą przygotowani również do uzyskania certyfikatów:

- CCNA (Cisco Certified Network Associate),
- CCNA Security.

Bezpieczeństwo w energetyce

Specjalność międzywydziałowa, na której kształcenie przygotowuje do pracy przy zabezpieczaniu dostępu do informacji systemów: informatycznych ICT i sterowania przemysłowego OT, wchodzących w skład infrastruktury krytycznej systemów elektroenergetycznych. Szczególny nacisk położono na bezpieczeństwo przechowywanych informacji i ochrony dostępu do niej przy użyciu nowoczesnych systemów transmisyjnych.



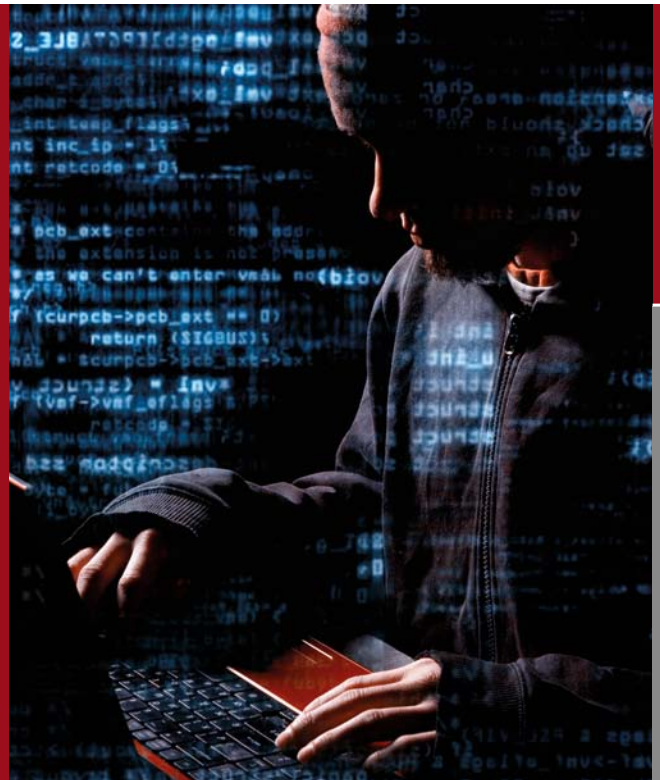
Kształcenie obejmuje m. in. zasady projektowania i funkcjonowania systemów elektroenergetycznych i inteligentnych sieci elektroenergetycznych (Smart Grid), wykorzystujących technologię ICT, w szczególności: mechanizmy zabezpieczeń infrastruktury krytycznej wytwarzania i przesyłu energii elektrycznej, klasyfikację systemów krytycznych, procesy wznowienia działania systemów po przerwie, niskoenergetyczne technologie komunikacyjne, cyfrowe stacje elektroenergetyczne, inteligentne sieci domowe, systemy zdalnego odczytu liczników energii elektrycznej (Smart Metering), zarządzanie rozproszonymi źródłami energii, prowadzenie ruchu stacji, automatyki stacyjnej oraz systemów sterowania i nadzoru (SSiN). W ramach specjalności studenci będą przygotowani również do uzyskania certyfikatów CCNA (Cisco Certified Network Associate) i CCNA Security.

Studia na kierunku Cyberbezpieczeństwo gwarantują wykształcenie w obszarze bezpieczeństwa sieci oraz systemów informatycznych i telekomunikacyjnych, a także ochrony danych. Kierunek jest silnie powiązany z aktualnymi potrzebami rynku pracy. Studenci uzyskują wszechstronne i gruntowne wykształcenie w dyscyplinach informatyka i telekomunikacja, w aspektach technicznych oraz prawnych i organizacyjnych, z naciskiem na pogłębioną wiedzę w zakresie bezpieczeństwa systemów operacyjnych, sieci komputerowych i telekomunikacyjnych oraz bezpieczeństwa przetwarzanych i przechowanych danych w centrach danych. Wiedza oraz umiejętności uzyskane w ramach niniejszego kierunku umożliwiają jego absolwentowi branie czynnego udziału w procesach związanych z szeroko pojętym bezpieczeństwem informacji związanym m.in. z audytowaniem systemów, sieci i magazynów danych pod kątem bezpieczeństwa oraz monitorowaniem, detekcją i analizą zagrożeń oraz naruszeń w systemach informatycznych.

Absolwenci I stopnia studiów będą mogli je kontynuować na przygotowywanym obecnie II stopniu studiów (magisterskich).

ABSOLWENT ZNAJDZIE ZATRUDNIENIE NA STANOWISKACH:

- specjalista bezpieczeństwa IT,
- administrator systemów transmisji danych,
- kierownik projektów IT,
- specjalista od wdrażania bezpiecznych sieci i systemów informatycznych,
- doradca w obszarze bezpieczeństwa IT, itp.



WYDZIAŁ ELEKTRONIKI
POLITECHNIKA WROCŁAWSKA
ul. Janiszewskiego 11/17, 50-372 Wrocław
tel. 71 320 35 74 (sekretariat)

OBSŁUGA STUDENTÓW
tel. 71 320 25 38 (kierownik dziekanatu)
tel. 71 320 40 65 (studia stacjonarne)
tel. 71 320 26 65 (studia stacjonarne)
tel. 71 320 25 27 (studia stacjonarne)
tel. 71 320 20 54 (studia niestacjonarne)

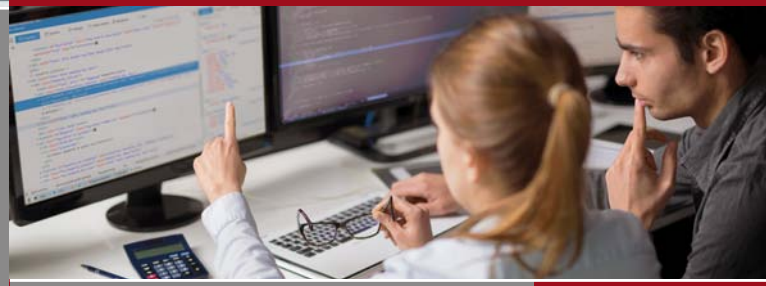
www.weka.pwr.edu.pl

Politechnika Wrocławska

WYDZIAŁ ELEKTRONIKI

KIERUNEK

CYBERBEZPIECZEŃSTWO



www.weka.pwr.edu.pl