Program studiów

Kierunek: Bezpieczeństwo sieci teleinformatycznych

Spis treści

Opis studiów podyplomowych

Ogólne informacje o studiach podyplomowych

Wydział:	Wydział Informatyki, Elektroniki i Telekomunikacji
Nazwa studiów podyplomowych (w j. polskim):	Bezpieczeństwo sieci teleinformatycznych
Nazwa studiów podyplomowych (w j. angielskim):	Security of ICT networks
Poziom:	Studia podyplomowe
Termin rozpoczęcia cyklu:	2026/2027, semestr zimowy
Czas trwania jednej edycji studiów podyplomowych (liczba semestrów):	2
Język wykładowy:	polski
Liczba punktów ECTS wymagana do ukończenia studiów podyplomowych:	32
w tym: liczba punktów ECTS przypisanych do zajęć kształtujących umiejętności praktyczne:	22
w tym: liczba punktów ECTS przypisanych do zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość:	14

Data planowanego rozpoczęcia i zakończenia pierwszej edycji studiów podyplomowych

1.10.2026 - 30.09.2027

Zakres tematyczny

Program studiów obejmuje podstawy technologii sieci teleinformatycznych oraz powiązane z nim aspekty bezpieczeństwa sieci i systemów. Program obejmuje podstawy sieci IP z rozszerzeniem w kierunku bezpieczeństwa sieci, system operacyjny Linux i jego bezpieczeństwo, lokalne sieci komputerowe z aspektami bezpieczeństwa, podstawy bezpiecznych, rozległych sieci teleinformatycznych z uwzględnieniem rutingu, programowanie w języku Python ukierunkowane na aspekty bezpieczeństwa sieci i systemów, wirtualizację sieci teleinformatycznych. Dodatkowo w programie studiów przewidziano wykłady wprowadzające w tematykę architektury sieci teleinformatycznych, prawnych zagadnień bezpieczeństwa sieci i systemów oraz podstaw bezpieczeństwa sieciowego.

Do kogo adresowane są studia podyplomowe

Studia adresowane są do osób z wyższym wykształceniem pierwszego lub drugiego stopnia, niekoniecznie wykształceniem technicznym. Program umożliwia zdobycie niezbędnych umiejętności osobom nie mającym wykształcenia z zakresu informatyki, teleinformatyki, telekomunikacji. Wymagana jest ogólna wiedza i umiejętności z zakresu obsługi komputera, ugruntowana wiedza informatyczna z zakresu szkoły średniej oraz silna motywacja do intensywnej pracy w ramach oferowanych zajęć.

Kierownik studiów podyplomowych: dr inż. Artur Lasoń
tel.: 12 617 40 37
mail: alason@agh.edu.pl

Organizator studiów podyplomowych: Wydział Informatyki, Elektroniki i Telekomunikacji, Instytut Telekomunikacji
tel.: 12 617 40 37, alason@agh.edu.pl
mail: alason@agh.edu.pl

Osoba do kontaktu: mgr Joanna Putała
tel.: tel. 12 617 48 07
mail: joanna.putala@agh.edu.pl

Dodatkowe informacje

-

Warunki rekrutacji na studia podyplomowe

Na studia podyplomowe Bezpieczeństwo sieci teleinformatycznych przyjmowani są kandydaci posiadający dyplom ukończenia studiów wyższych (inżyniera, licencjata, magistra). O przyjęciu decyduje kolejność zgłoszeń oraz dokonanie wymaganych wpłat na konto studiów.

Program studiów podyplomowych

Ogólne cele kształcenia w ramach studiów podyplomowych

Studia podyplomowe Bezpieczeństwo sieci teleinformatycznych mają na celu przygotowanie specjalistów z obszaru teleinformatyki, w szczególności zdobycie wiedzy i umiejętności z zakresu konfiguracji, testowania i utrzymania bezpiecznych sieci teleinformatycznych.

Sylwetka absolwenta studiów podyplomowych

Absolwent zna i rozumie ogólną architekturę sieci teleinformatycznych, podstawowe regulacje prawne dotyczące bezpieczeństwa sieci, rozumie podstawowe terminy, problemy i narzędzia bezpieczeństwa sieciowego. Absolwent studiów podyplomowych Bezpieczeństwo sieci teleinformatycznych posiada wiedzę i podstawowe umiejętności z zakresu bezpieczeństwa lokalnych i rozległych sieci teleinformatycznych, sieci IP, potrafi efektywnie i bezpiecznie korzystać z funkcji i narzędzi systemu operacyjnego Linux, potrafi napisać i uruchomić program w języku Python. Absolwent poprzez przygotowanie pracy końcowej o wybranej tematyce posiada pogłębioną wiedzę i umiejętności z wybranego zakresu bezpieczeństwa sieci teleinformatycznych. Szczegółowe umiejętności wyszczególnione zostały w zdefiniowanych efektach uczenia się. Efekty uczenia się będą weryfikowane przez poszczególnych prowadzących w trakcie prowadzonych zajęć laboratoryjnych i właściwie dokumentowane dzięki prowadzonej przez wszystkich prowadzących dokumentacji.

Zasady odbywania studiów podyplomowych, w tym zasady udziału w zajęciach, zasady zaliczania zajęć i zasady składania egzaminów, zasady zaliczania i wpisu na kolejny semestr

Obecność na wykładach jest obowiązkowa, zaliczenie wykładu następuje na postawie prowadzonej listy obecności. Obecność na ćwiczeniach laboratoryjnych jest obowiązkowa. Zaliczenie ćwiczeń laboratoryjnych odbywa się na podstawie indywidualnej oceny aktywności oraz postępów uczestników studiów dokonywanej podczas zajęć laboratoryjnych.

Warunkiem uzyskania pozytywnej oceny końcowej z przedmiotu jest obecność na wykładach przewidzianych w programie danego przedmiotu. W przypadku usprawiedliwionej nieobecności na wykładach stanowiących 50% lub mniej wykładów przewidzianych w programie danego przedmiotu uczestnik zobowiązany jest samodzielnie uzupełnić swą wiedzę na podstawie udostępnionych uczestnikom studiów podyplomowych materiałów oraz przedstawić wyniki swej indywidualnej pracy prowadzącemu przedmiot lub kierownikowi studiów podyplomowych. W przypadku usprawiedliwionej nieobecności na więcej niż 50% wykładów uczestnik jest zobowiązany do zaliczenia wykładów w indywidualnym trybie ustalonym z prowadzącym przedmiot lub kierownikiem studiów podyplomowych. W przypadku przedmiotów, w ramach których nie przewidziano zajęć laboratoryjnych zaliczenie przedmiotu (wykładu) odbywa się bez ustalenia oceny. Zaliczenie wykładu nie wlicza się do średniej uzyskanej w toku studiów.
Obowiązującą formą zaliczenia ćwiczeń laboratoryjnych jest ocena. Ocena z kolejnych ćwiczeń laboratoryjnych wystawiana jest przez prowadzącego przedmiot na podstawie indywidualnej oceny aktywności oraz postępów uczestnika studiów.
Dokumentacja uzyskiwanych ocen jest prowadzona przez prowadzącego przedmiot i przekazywana na koniec semestru kierownikowi studiów podyplomowych. Ocena końcowa z przedmiotu jest średnią arytmetyczną ocen uzyskanych z poszczególnych ćwiczeń laboratoryjnych pod warunkiem uzyskania zaliczenia z wykładu przewidzianego dla danego przedmiotu.
Wpis na kolejny semestr następuje po zaliczeniu wszystkich przedmiotów semestru poprzedniego.

Wymiar, zasady , forma i miejsce odbywania praktyk, w tym w szczególności warunki ich realizacji, system kontroli praktyk i ich zaliczania (jeżeli są wymagane)

W ramach studiów podyplomowych Bezpieczeństwo sieci teleinformatycznych nie przewiduje się praktyk.

Warunki ukończenia studiów podyplomowych i uzyskania świadectwa ukończenia studiów podyplomowych, w tym warunki i wymagania związane z przygotowaniem prac końcowych oraz realizacją procesu dyplomowania, a także związane z organizacją i przebiegiem egzaminu końcowego (jego zakres, tryb i sposób jego przeprowadzenia, zasady ustalania oceny z egzaminu końcowego, wytyczne dotyczące jego przebiegu), jeżeli są wymagane, zasady ustalania ostatecznego wyniku ich ukończenia

Do ukończenia studiów podyplomowych Bezpieczeństwo sieci teleinformatycznych konieczne jest uzyskanie pozytywnej oceny ze wszystkich przedmiotów przewidzianych w planie studiów oraz złożenie pracy końcowej. Praca końcowa musi uzyskać pozytywną ocenę ze strony opiekuna pracy i zakończyć się jej pozytywną obroną. Obrona pracy końcowej przeprowadzana przed komisją powołaną przez kierownika studiów podyplomowych. Ocena pracy końcowej ustalana jest jako średnia arytmetyczna oceny pracy wystawionej przez jej opiekuna i oceny uzyskanej podczas jej obrony. Ocena końcowa ukończenia studiów podyplomowych wyznaczona będzie na podstawie średniej ważonej z uzyskanych ocen z poszczególnych przedmiotów i oceny pracy końcowej zgodnie z zapisami Regulaminu studiów podyplomowych AGH. W programie studiów podyplomowych nie zaplanowano egzaminów z przewidzianych planem studiów przedmiotów.

Informacja o możliwości odbycia kształcenia przygotowującego do wykonywania zawodu lub uzyskania uprawnień zawodowych w ramach nowo tworzonych studiów podyplomowych (o ile dotyczy)

Nie dotyczy.

Informacja o możliwości odbycia kształcenia zgodnie ze standardem kształcenia przygotowującego do wykonywania zawodu nauczyciela (o ile dotyczy)

Nie dotyczy.

Informacja o możliwości uzyskania przygotowania do wykonywania zawodu nauczyciela wraz ze wskazaniem przedmiotu lub rodzaju zajęć, które absolwent będzie mógł prowadzić po ukończeniu studiów podyplomowych (o ile dotyczy)

Nie dotyczy

Efekty uczenia się

Kierunek: Bezpieczeństwo sieci teleinformatycznych

Wiedza

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
BSTSP_W01	Uczestnik zna i rozumie zasady funkcjonowania bezpiecznych sieci IP	P6S_WG
BSTSP_W02	Uczestnik zna i rozumie zasady bezpiecznej transmisji danych w lokalnych i rozległych sieciach teleinformatycznych	P6S_WG
BSTSP_W03	Uczestnik zna i rozumie wybrane techniki testowania i wykonywania pomiarów w sieciach teleinformatycznych	P6S_WG
BSTSP_W04	Uczestnik zna i rozumie podstawy projektowania i tworzenia aplikacji w językach skryptowych	P6S_WG

Umiejętności

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
BSTSP_U01	Uczestnik potrafi skonfigurować, uruchomić i zapewnić bezpieczeństwo lokalnej i rozległej sieci teleinformatycznej w oparciu o wybrane techniki i protokoły	P6S_UW
BSTSP_U02	Uczestnik potrafi skonfigurować , uruchomić, zapewnić bezpieczeństwo transmisji danych w sieciach IP	P6S_UW
BSTSP_U03	Uczestnik potrafi posługiwać się systemem operacyjnym Linux z użyciem interfejsu tekstowego CLI, poprawić bezpieczeństwo systemu przez zastosowanie wybranych metod i narzędzi	P6S_UW
BSTSP_U04	Uczestnik potrafi napisać i uruchomić program w języku Python	P6S_UW
BSTSP_U05	Uczestnik potrafi zaplanować proces rozszerzania i rozwoju wiedzy w zakresie bezpieczeństwa sieci teleinformatycznych	P6S_UU

Kompetencje społeczne

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
BSTSP_K01	Uczestnik jest gotów do samodzielnego podejmowania decyzji dotyczących utrzymania bezpiecznych systemów teleinformatycznych	P6S_KK
BSTSP_K02	Uczestnik jest gotów do krytycznej oceny własnych działań i ich potencjalnych skutków w zakresie bezpieczeństwa sieci	P6S_KR, P6S_KK