Program studiów podyplomowych

Kierunek: Cyberbezpieczeństwo w praktyce

Spis treści

Program studiów podyplomowych

Informacje podstawowe

Nazwa wydziału:	Wydział Informatyki, Elektroniki i Telekomunikacji
Nazwa studiów podyplomowych:	Cyberbezpieczeństwo w praktyce
Poziom:	studia podyplomowe
Liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie:	31
Termin rozpoczęcia cyklu:	2021/2022
Czas trwania studiów (liczba semestrów):	2

Warunki rekrutacji, w tym wymagania wstępne

Znajomość obsługi komputera i podstawowych rozwiązań w zakresie IT.

Limit przyjęć na studia podyplomowe wraz ze wskazaniem minimalnej liczby osób przyjętych, warunkującej uruchomienie edycji studiów podyplomowych

76 osób (minimum 18).

Wymagane dokumenty oraz miejsce ich złożenia

- Formularz zgłoszeniowy,
- poświadczona przez Uczelnię kopia dyplomu ukończenia studiów wyższych,
- poświadczenie wniesienia opłaty wpisowej w wysokości 100 zł,
- poświadczenie wniesienia opłaty za studia podyplomowe za pierwszy semestr studiów, nie później niż w terminie 14 dni przed rozpoczęciem zajęć dydaktycznych w ramach studiów podyplomowych.

Dokumenty można składać bezpośrednio w sekretariacie studiów lub drogą elektroniczną na adres: chmo@agh.edu.pl (z obowiązkiem późniejszego - przed rozpoczęciem zajęć - osobistego przedstawienia oryginałów do potwierdzenia z wersjami skanowanymi złożonych dokumentów).

Ogólne cele kształcenia w ramach studiów podyplomowych

Oferta Studiów skierowana jest do wszystkich, którzy chcą pogłębić swoją wiedzę z zakresu zarządzania i administrowania bezpieczeństwem systemów komputerowych. Ze względu na specyfikę tematu, duży nacisk położony jest na nabycie umiejętności pozwalających na prowadzenie działalności praktycznej w tym obszarze. Celem Studiów jest przygotowanie absolwenta do podjęcia pracy zawodowej związanej z cyberbezpieczeństwem. Program studiów obejmuje 200 godzin wykładów i zajęć laboratoryjnych. Dzieli się na dwie fazy kształcenia: część ogólną, realizowaną w pierwszym semestrze, prezentującą najważniejsze składniki wiedzy dotyczącej cybezpieczeństwa systemów komputerowych, z uwzględnieniem zagadnień teoretycznych i praktycznych, prawnych, informatycznych i socjotechnicznych. W drugim semestrze słuchacze będą mogli wybrać jeden z czterech profili: ad-ministrowanie cyberbezpieczeństwem, bezpieczeństwo infrastruktury, zarządzanie cyberbezpieczeństwem i bezpieczeństwo informacji. Kluczowe zajęcia będą realizowane w obu profilach. W pierwszym jest jednak więcej zajęć praktycznych związanych z administrowaniem systemami komputerowymi, drugi koncentruje się na bezpieczeństwie sieci, w trzecim nacisk położony jest na zarządzanie, a czwarty dotyczy głównie procedur zapewniających bezpieczeństwo przechowywanych danych. Wiedza i umiejętności pozyskane w czasie studiów pozwolą absolwentowi na specjalizację w ramach swojej pracy w organach ścigania, instytucjach państwowych oraz w biznesie w obszarze związanym z cyberbezpieczeństwem. Wiedza, świadomość zagrożeń oraz konieczności inwestycji w tym obszarze pomoże szefom firm lub instytucji oraz osobom odpowiedzialnym za procesy decyzyjne w zakresie bezpieczeństwa teleinformatycznego.

Sylwetka absolwenta studiów podyplomowych

Absolwent posiądzie teoretyczną i praktyczną wiedzę z zakresu bezpieczeństwa systemów informatycznych, analizy i

informatyki śledczej, rodzajów zagrożeń i ataków oraz przeciwdziałania im, poszukiwania, gromadzenia i zabezpieczania materiału dowodowego oraz działań prewencyjnych. Absolwent pozna podstawy informatyki, budowę systemów operacyjnych, podstawy kryptografii. Nabędzie umiejętność programowania w języku Python. Pozna zasady zabezpieczania systemów komputerowych, aplikacji i sieci komputerowych. W przypadku profilu administracja, opanuje umiejętność dbania o bezpieczeństwo baz danych. Absolwent uzyska wiedzę i praktyczne umiejętności umożliwiające podjęcie pracy związanej z administracją i bezpieczeństwem systemów komputerowych, opracowywaniem polityk bezpieczeństwa, ich wdrażania, utrzymania oraz rozwoju. Pozna podstawy informatyki śledczej oraz najnowsze metody ataków i zagrożenia dla systemów informatycznych. Będzie potrafił przeciwdziałać ich rozprzestrzenianiu i skutkom. Będzie umiał poszukiwać, gromadzić i zabezpieczać materiał dowodowy. Absolwent pozna podstawy analizy kryminalnej, będzie potrafił analizować dane związane z wystąpieniem incydentu teleinformatycznego, wykrywać i identyfikować związki między nimi, określać przesłanki, wyciągać wnioski i oceniać ich wiarygodność. Będzie umiał sporządzić raport z przebiegu incydentu, jego faktycznych i prawdopodobnych skutków, podjętych działań oraz proponowanych działań zapobiegawczych na przyszłość. Pozna sposób postępowania w przypadku zgłaszania popełnienia przestępstwa organom ścigania oraz prawa pokrzywdzonego. Będzie potrafił współdziałać z organami przestrzegania prawa w zakresie rozpoznania i zwalczania cyberprzestępczości, jak również będzie przygotowany do prowadzenia szkoleń w zakresie bezpieczeństwa teleinformatycznego dla pracowników swojej firmy lub instytucji.

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

Zajęcia odbywają się w soboty i niedziele. Szczegółowy tryb zaliczenia jest ustalany indywidualnie dla każdego przedmiotu i podawany jest na pierwszych zajęciach z danego przedmiotu. W przypadku nieobecności należy uzgodnić z prowadzącym tryb odrobienia zaległości.

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

Brak

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

Dla zaliczenia przedmiotów wymagana jest obecność i aktywny udział w zajęciach, w szczególności wymagana jest realizacja zadań praktycznych na laboratoriach. Wymagana jest też ogólna obecność studentów na przynajmniej 75% wszystkich zajęć. Ocena końcowa uzyskiwana przez absolwentów Studiów Podyplomowych jest zgodna z przepisami Regulaminu Studiów podyplomowych na AGH. Ocena końcowa tworzona jest w oparciu o średnią z ocen uzyskanych zaliczeń. Wymagane jest zaliczenie wszystkich przedmiotów. Studenci Studiów po zaliczeniu wszystkich przedmiotów objętych planem studiów otrzymują świadectwo Ukończenia Studiów Podyplomowych „Cyberbezpieczeństwo w praktyce”.

Efekty uczenia się

Kierunek: Cyberbezpieczeństwo w praktyce

Wiedza

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CBPSP_W01	Podstawowe pojęcia związane z cyberbezpieczeństwem	P6S_WG
CBPSP_W02	Podstawy informatyki śledczej	P6S_WG
CBPSP_W03	Podstawowe pojęcia związane z analizą incydentów	P6S_WK
CBPSP_W04	Dostępne oprogramowanie wspomagające prace związane z cyberbezpieczeństwem	P6S_WK

Umiejętności

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CBPSP_U01	Porozumiewać się, w tym brać udział w dyskusji z użyciem specjalistycznej terminologii	P6S_UK
CBPSP_U02	Dokonać analizy incydentu teleinformatycznego	P6S_UW
CBPSP_U03	Zastosować odpowiednie narzędzia w obszarze cyberbezpieczeństwa	P6S_UW
CBPSP_U04	Zaplanować dalsze kierunki swojej nauki w obszarze cyberbezpieczeństwa	P6S_UU

Kompetencje społeczne

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CBPSP_K01	Stałego poszerzania wiedzy z zakresu cyberbezpieczeństwa	P6S_KK
CBPSP_K02	Krytycznej oceny swojej wiedzy	P6S_KK
CBPSP_K03	Wykorzystania zdobytej wiedzy do realizacji istotnych celów służących społeczeństwu	P6S_KO
CBPSP_K04	Przestrzegania zasad etyki zawodowej	P6S_KR