Program studiów

Kierunek: Cyberbezpieczeństwo i zarządzanie bezpieczeństwem informacji

Spis treści

Program studiów podyplomowych

Informacje podstawowe

Nazwa wydziału:	Wydział Zarządzania
Nazwa kierunku:	Cyberbezpieczeństwo i zarządzanie bezpieczeństwem informacji
Poziom:	Studia podyplomowe
Liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie:	30
Termin rozpoczęcia cyklu:	2023/2024
Czas trwania studiów (liczba semestrów):	2

Warunki rekrutacji, w tym wymagania wstępne

Rekrutacja na studia obejmuje elektroniczną rejestrację kandydatów poprzez stronę https://www.cyberbezpieczenstwo.zarz.agh.edu.pl/rekrutacja/ oraz:

- złożenie przez kandydata deklaracji przystąpienia do kwalifikacji,
- kwalifikacji kandydatów,
- złożenie przez kandydata wymaganych dokumentów.

Podstawą kwalifikacji jest kolejność zgłoszeń.

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

Maksymalna liczba uczestników to 30 osób. Uruchomienie studiów nastąpi pod warunkiem zgłoszenia się minimum 16 osób.

Wymagane dokumenty oraz miejsce ich złożenia

Wymagane dokumenty:

- formularz zgłoszeniowy,
- poświadczona przez uczelnię kserokopia dyplomu ukończenia studiów I stopnia (licencjackich lub inżynierskich) lub dyplomu ukończenia studiów II stopnia lub dyplomu ukończenia jednolitych studiów magisterskich,
- 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.

Zgłoszenia na studia przyjmowane są w biurze studiów – Wydział Zarządzania, ul. Gramatyka 10 (budynek D-14) pok. 202.

Ogólne cele kształcenia w ramach studiów podyplomowych

Celem głównym kształcenia jest przygotowanie słuchaczy do pełnienia wyższych funkcji managerskich w biznesie, administracji państwowej oraz służbach państwa.
Cele cząstkowe:

- zrozumienie istoty informacji dla bezpiecznego funkcjonowania organizacji,
- organizacja i funkcjonowanie Krajowego systemu Cyberbezpieczeństwa,
- praktyczne wykorzystanie dokumentów standaryzacyjnych wykorzystywanych w cyberbezpieczeństwie.

Sylwetka absolwenta studiów podyplomowych

Uczestnicy nabywają niezbędnej, nowoczesnej wiedzy dotyczącej bezpiecznego zarządzania informacją na etapie jej tworzenia, przetwarzania, przesyłania i gromadzenia.
Uczestnicy otrzymają również praktyczne umiejętności w rozwiązywaniu problemów związanych z bezpieczeństwem informacji na przykładzie zajęć warsztatowych i ćwiczeń praktycznych.

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 na studiach podyplomowych „Cyberbezpieczeństwo i zarządzanie bezpieczeństwem informacji" w okresie od października 2023 r. do września 2024 r. odbywać się będą w formie dwudniowych sesji dydaktycznych organizowanych raz w miesiącu.
Warunkiem zaliczenia zajęć jest obecność uczestników studiów na zajęciach realizowanych w sposób tradycyjny, hybrydowy bądź on-line oraz ich aktywność dyskusyjna w trakcie zajęć, która pozwoli na realizację efektów kształcenia i zdobycie zaliczenia. Uczestnicy studiów, w razie usprawiedliwionej nieobecności na zajęciach, mogą zdobyć zaliczenie po uzgodnieniu z prowadzącym dany przedmiot sposobu uzupełnienia wiadomości i ich zaliczenia. W trakcie studiów jedynym egzaminem jest egzamin końcowy. Wpis słuchacza na kolejny semestr dokonywany jest na podstawie obecności i zaliczeń zajęć realizowanych w pierwszym semestrze studiów.

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

Nie przewiduje się odbywania praktyk w okresie trwania studiów podyplomowych.

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

Warunkiem ukończenia studiów podyplomowych jest zdanie egzaminu końcowego. Weryfikuje on zdobytą wiedzę i umiejętności w trakcie całych studiów podyplomowych.

Efekty uczenia się

Kierunek : Cyberbezpieczeństwo i zarządzanie bezpieczeństwem informacji

Wiedza

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CZBSP_W01	systemy, zasady, metody i narzędzia związane z zarządzaniem istotą informacji we współczesnych organizacjach i ich bezpieczeństwem	P7Z_WT
CZBSP_W02	różnice pomiędzy systemami zarządzania bezpieczeństwem informacji w organizacjach, a cyberbezpieczeństwem	P7Z_WT
CZBSP_W03	straty spowodowane złym funkcjonowaniem systemów zarządzania bezpieczeństwem informacji w organizacjach	P7Z_WZ
CZBSP_W04	przepisy, normy i elementy systemów zarządzania bezpieczeństwem informacji oraz zasadami cyberbezpieczeństwa	P7Z_WO
CZBSP_W05	wyzwania pojawiające się w zarządzaniu cyberbezpieczeństwem organizacji	P7Z_WO

Umiejętności

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CZBSP_U01	rozpoznawać zasady, przepisy, normy, metody oraz narzędzia wykorzystywane w zarządzaniu bezpieczeństwem organizacji	P7Z_UN
CZBSP_U02	rozpoznawać elementy systemów zarządzania bezpieczeństwem informatycznym w organizacji	P7Z_UO
CZBSP_U03	wyjaśniać przyczyny powstawania zagrożeń w cyberprzestrzeni i proponuje sposoby ich eliminacji	P7Z_UN
CZBSP_U04	korzystać z norm i przepisów dotyczących zarządzania cyberbezpieczeństwem i bezpieczeństwem teleinformatycznym organizacji	P7Z_UO

Kompetencje społeczne

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CZBSP_K01	współpracy w grupie, przewidywania wielokierunkowych skutków swojej działalności oraz ponosić za nie odpowiedzialność oraz potrafi budować projekty społeczne	P7Z_KW
CZBSP_K02	przyjmowania różnych ról w grupie, w tym potrafi kierować zespołami ludzkimi, proponować kształt prawny i organizacyjny	P7Z_KW
CZBSP_K03	samodzielnego i krytycznego uzupełniania wiedzy i umiejętności, poszerzonych o wymiar interdyscyplinarny	P7Z_KW
CZBSP_K04	samodzielnego myślenia, profesjonalizmu, przestrzegania zasad etyki zawodowej oraz dążenia do doskonalenia	P7Z_KW

Plany studiów

Nazwa kierunku: Cyberbezpieczeństwo i zarządzanie bezpieczeństwem informacji

Semestr 1

Przedmiot	Liczba godzin	Punkty ECTS	Forma weryfikacji	
Istota bezpieczeństwa informacji we współczesnych organizacjach oraz cyberbezpieczeństwo	Wykład: 40 Konwersatorium: 20	10,0	Zaliczenie	O
Standardy zarządzania bezpieczeństwem informacji	Wykład: 40	6,0	Egzamin	O
Suma	**100**	**16,0**		

Semestr 2

Przedmiot	Liczba godzin	Punkty ECTS	Forma weryfikacji	
Bezpieczeństwo fizyczne i środowiskowe systemów teleinformatycznych	Wykład: 25 Zajęcia warsztatowe: 5	5,0	Egzamin	O
Rozwiązania techniczne w zarządzaniu bezpieczeństwem informacji	Wykład: 20	3,0	Egzamin	O
Praktyka w zarządzaniu bezpieczeństwem informatycznym	Wykład: 20 Konwersatorium: 10 Zajęcia warsztatowe: 10	6,0	Egzamin	O
Suma	**90**	**14,0**		

O - Obowiązkowy
W - Do wyboru