SZKOŁA GŁÓWNA
GOSPODARSTWA
WIEJSKIEGO

Program studiów podyplomowych

Menedżer bezpieczeństwa informacji i ochrony danych osobowych

Spis treści

Informacje podstawowe

Nazwa wydziału:	Wydział Ekonomiczny
Nazwa studiów podyplomowych:	Menedżer bezpieczeństwa informacji i ochrony danych osobowych
Poziom:	studia podyplomowe
Liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie:	30
Czas trwania studiów (liczba semestrów):	2
Odniesienie do poziomu PRK:	7 PRK

Opis studiów podyplomowych

Cele kształcenia, opis grupy odbiorców

Celem studiów podyplomowych „Menedżer Bezpieczeństwa Informacji i Ochrony Danych Osobowych” jest przygotowanie uczestników do pracy zawodowej w obszarze bezpieczeństwa informacji i ochrony danych osobowych oraz podniesienie kwalifikacji osób już związanych z tą tematyką. Program studiów łączy wiedzę teoretyczną z praktycznymi kompetencjami niezbędnymi do skutecznego zarządzania bezpieczeństwem informacji we współczesnych organizacjach.

W trakcie studiów słuchacze zdobywają wiedzę i umiejętności z zakresu m.in. regulacji prawnych dotyczących ochrony danych osobowych i bezpieczeństwa informacji, zarządzania ryzykiem, identyfikacji i analizy zagrożeń, prowadzenia audytów, tworzenia i wdrażania polityk bezpieczeństwa, monitorowania zgodności z przepisami oraz zarządzania ciągłością działania. Program obejmuje również zagadnienia związane z bezpieczeństwem teleinformatycznym oraz nowoczesnymi metodami zarządzania bezpieczeństwem informacji zgodnie z aktualnymi standardami i wymaganiami rynku.

"Menedżer Bezpieczeństwa Informacji i Ochrony Danych Osobowych” to dwusemestralne studia adresowane są do:

- osób pracujących lub planujących rozwój zawodowy w obszarze bezpieczeństwa informacji i ochrony danych osobowych,
- kandydatów na Inspektorów Ochrony Danych oraz Menedżerów Bezpieczeństwa Informacji,
- osób zajmujących się doradztwem i audytem w zakresie ochrony danych osobowych i bezpieczeństwa informacji,
- kadry menedżerskiej zainteresowanej poszerzeniem kompetencji w zakresie zarządzania bezpieczeństwem informacji,
- pracowników odpowiedzialnych za zgodność organizacji z wymaganiami prawnymi i organizacyjnymi,
- absolwentów wszystkich kierunków studiów zainteresowanych zdobyciem nowoczesnych i praktycznych kwalifikacji zawodowych,
- osób wyznaczonych w organizacjach do realizacji zadań związanych z ochroną danych osobowych i bezpieczeństwem informacji,
- wszystkich zainteresowanych podnoszeniem kwalifikacji i zdobyciem specjalistycznej wiedzy w tym obszarze.

Charakterystyka studiów podyplomowych

Współczesne organizacje funkcjonują w środowisku dynamicznych zmian technologicznych i rosnących zagrożeń związanych z bezpieczeństwem informacji oraz ochroną danych osobowych. Skuteczne zarządzanie bezpieczeństwem danych stało się jednym z kluczowych elementów budowania stabilności organizacji, zapewniania zgodności z przepisami prawa oraz wzmacniania zaufania klientów i partnerów biznesowych.

Studia podyplomowe „Menedżer Bezpieczeństwa Informacji i Ochrony Danych Osobowych” przygotowują uczestników do praktycznej realizacji zadań związanych z ochroną danych i zarządzaniem bezpieczeństwem informacji w przedsiębiorstwach, instytucjach publicznych oraz organizacjach reprezentujących różne sektory gospodarki. Absolwenci zdobywają kompetencje umożliwiające wdrażanie procedur zgodnych z krajowymi i unijnymi regulacjami, identyfikowanie zagrożeń oraz budowanie skutecznych systemów zarządzania bezpieczeństwem informacji.

Program studiów łączy zajęcia teoretyczne z praktycznymi formami kształcenia. Część wykładowa realizowana jest z wykorzystaniem nowoczesnych technik dydaktycznych, natomiast zajęcia praktyczne prowadzone są w formie warsztatów, studiów przypadków oraz pracy zespołowej. Kształcenie odbywa się z wykorzystaniem metod nauczania na odległość, przy czym co najmniej jeden zjazd realizowany jest w formie stacjonarnej.

Zajęcia prowadzone są przez doświadczonych praktyków, ekspertów z zakresu bezpieczeństwa informacji i ochrony danych osobowych oraz przedstawicieli firm i instytucji będących partnerami merytorycznymi studiów. Dzięki temu uczestnicy zdobywają aktualną wiedzę oraz praktyczne kompetencje odpowiadające realnym wyzwaniom współczesnych organizacji.

Wymiar, zasady i forma odbywania oraz zaliczania praktyk

Na studiach podyplomowych nie są realizowane praktyki.

Warunki ukończenia studiów podyplomowych

1. Uzyskanie pozytywnych wyników zaliczeń z zajęć objętych programem studiów, zgodnie z kryteriami i warunkami określonymi w ich opisie;
2. Złożenie pracy dyplomowej obejmującej zestaw zadań projektowych oraz jej zakwalifikowanie do egzaminu końcowego;

3. Uzyskanie pozytywnego wyniku z egzaminu końcowego.

Praca dyplomowa
Praca dyplomowa jest zwartym opracowaniem w formie projektu, o charakterze przekrojowym i problemowym, odnoszącym się do treści realizowanych w ramach zajęć przewidzianych w programie studiów. Opis projektu i zasady jego przygotowania Słuchacze otrzymują podczas pierwszego zjazdu.

Praca dyplomowa wykonywana jest samodzielnie, a w przypadku gdy Słuchacze pochodzą z tej samej organizacji może być wykonywana w zespole maksymalnie dwuosobowym.

Przygotowanie prac dyplomowych słuchaczy wspiera opiekun lub zespół opiekunów merytorycznych odpowiedzialnych za promowanie pracy, których wskazuje Kierownik Studiów. O kwalifikacji pracy do egzaminu końcowego decyduje opiekun/opiekunowie pracy.

Praca dyplomowa składana jest do Kierownika studiów nie później niż siedem dni po zakończeniu ostatnich zajęć w programie studiów. Opiekun/opiekunowie pracy nie później niż trzy tygodnie po zakończeniu zajęć podejmują decyzję o zakwalifikowaniu złożonej pracy dyplomowej do egzaminu końcowego.

Egzamin końcowy
Do egzaminu końcowego dopuszczony jest Słuchacz, który uzyska pozytywne wyniki zaliczeń ze wszystkich zajęć objętych programem studiów, złoży pracę dyplomową zakwalifikowaną przez opiekuna/opiekunów do egzaminu końcowego oraz ma uregulowaną opłatę za studia określoną w warunkach rekrutacji.

Egzamin końcowy odbywa się nie później niż trzy miesiące od zakończenia ostatnich zajęć w programie studiów i przeprowadzany jest przez Komisję powołaną przez Dziekana. Egzamin końcowy jest dyskusją przygotowanej przez słuchacza pracy dyplomowej. Z egzaminu końcowego słuchacz otrzymuje ocenę w skali określonej w Regulaminie studiów podyplomowych.

Końcowy wynik studiów
Wynik końcowy studiów jest ustalany jako średnia arytmetyczna ocen uzyskanych z poszczególnych przedmiotów objętych programem studiów oraz oceny z egzaminu końcowego, zgodnie z poniższą skalą:

- ocena dostateczna - średnia arytmetyczna w przedziale (≥3,0 ≤ 3,25);
- ocena dostateczna plus - średnia arytmetyczna w przedziale (>3,25 ≤ 3,75);
- ocena dobra - średnia arytmetyczna w przedziale (>3,75 ≤ 4,25);
- ocena dobra plus - średnia arytmetyczna w przedziale (>4,25 ≤ 4,75);
- ocena bardzo dobra - średnia arytmetyczna w przedziale (>4,75).

Zasady i tryb rekrutacji

Kandydaci muszą mieć ukończone studia co najmniej pierwszego stopnia (6 poziom Polskiej Ramy Kwalifikacji).

Przyjęcie na studia podyplomowe następuje po:

1. dokonaniu rejestracji w systemie IRK,
2. złożeniu wymaganych dokumentów,
3. odnotowaniu wniesienia opłaty za studia podyplomowe lub pierwszej raty tej opłaty.

W procesie rekrutacji wymagane jest złożenie następujących dokumentów:

1. podanie/ankieta o przyjęcie na studia podyplomowe,
2. odpis lub poświadczoną przez uczelnię kopię dyplomu ukończenia studiów uprawniających do podjęcia studiów podyplomowych. W przypadku ukończenia studiów wyższych za granicą kandydat składa oryginał dyplomu oraz jego tłumaczenie na język polski potwierdzone przez upoważnione instytucje, a także dokument potwierdzający nostryfikację dyplomu lub zaświadczenie o zwolnieniu z postępowania nostryfikacyjnego,
3. dowód wpłaty za pierwszy semestr studiów lub za dwa semestry.

O przyjęciu na studia decydują kolejność zgłoszeń, dostarczenie kompletu dokumentów i dokonanie wymaganych opłat.

Efekty uczenia się

Wiedza

Kod	Treść	PRK
InspOch_K6_W01	Absolwent zna i rozumie terminologię stosowaną zakresie bezpieczeństwa informacji i ochrony danych oraz przepisy prawa w tym zakresie. Zna i rozumie zasady ochrony danych, źródłach zagrożeń dla bezpieczeństwa informacji oraz metody ich ochrony, w tym informacji niejawnych. Zna różne zabezpieczenia fizyczne i techniczne w organizacji w celu ochrony informacji i danych. Zna i rozumie technologie bezpieczeństwa teleinformatycznego i te związane ze sztuczną inteligencją. Zna i rozumie wymogi kontrolne UODO.	P7S_WG
InspOch_K6_W02	Absolwent zna i rozumie różne rodzaje ryzyka dla bezpieczeństwa informacji oraz danych osobowych. Zna i rozumie zasady przeprowadzania oceny i audytu bezpieczeństwa informacji oraz wdrażania systemu ochrony danych osobowych. Zna i rozumie zadania i kompetencje Menedżera Bezpieczeństwa Informacji i Inspektora Ochrony Danych. Zna i rozumie zasady ochrony danych w poszczególnych branżach gospodarki i w działach o szczególnym znaczeniu dla bezpieczeństwa informacji i danych.	P7S_WG
InspOch_K6_W03	Absolwent zna i rozumie współczesne teorie dotyczące zarządzania ciągłością działania oraz techniki i narzędzia wykorzystywane w zarządzaniu informacją a także w zarządzaniu incydentami i naruszeniami bezpieczeństwa informacji. Zna i rozumie polityki bezpieczeństwa informacji w organizacji oraz dokumentację w zakresie bezpieczeństwa informacji i ochrony danych, wymaganą przepisami prawa w organizacji.	P7S_WK

Umiejętności

Kod	Treść	PRK
InspOch_K6_U01	Absolwent potrafi ocenić stan bezpieczeństwa informacji w organizacji oraz przeprowadzić analizę ryzyka w tym zakresie. Potrafi zaplanować system pracy Inspektora Ochrony Danych.	P7S_UK, P7S_UW
InspOch_K6_U02	Absolwent potrafi sporządzić dokumentację i raporty z zakresu bezpieczeństwa informacji i ochrony danych osobowych oraz przeprowadzić audyt wewnętrzny systemu zarządzania bezpieczeństwem informacji ISO 27001.	P7S_UO
InspOch_K6_U03	Absolwent potrafi sporządzić politykę bezpieczeństwa informacji oraz regulamin ochrony danych. Potrafi komunikować się z UODO zgodnie z obowiązującymi przepisami prawa, m.in. w zakresie zgłaszania incydentów i naruszeń.	P7S_UU

Kompetencje społeczne

Kod	Treść	PRK
InspOch_K6_K01	Absolwent jest gotów do tworzenia i rozwijania wzorców właściwego postępowania w zakresie ochrony informacji i danych osobowych.	P7S_KR
InspOch_K6_K02	Absolwent jest gotów do podejmowania różnych inicjatyw służących bezpieczeństwu informacji i ochronie danych.	P7S_KO
InspOch_K6_K03	Absolwent jest gotów do krytycznej oceny siebie oraz organizacji, w której pracuje. Rozumie potrzebę dokształcania się zawodowego i rozwoju osobistego.	P7S_KK

Plan studiów

Semestr 1

Przedmiot	Liczba godzin	Punkty ECTS	Forma weryfikacji	Obligatoryjność
Wykład Inauguracyjny	Wykład: 2	0	-	Przedmioty do wyboru
Pojęcie informacji i metody zarządzania informacją	Wykład: 4	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Przykłady nadużyć i przestępstw w obszarze bezpieczeństwa informacji i danych osobowych	Wykład: 2 Ćwiczenia audytoryjne: 2	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Regulacje prawne w zakresie bezpieczeństwa informacji i ochrony danych osobowych	Wykład: 8	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Menedżer Bezpieczeństwa Informacji i Inspektor Ochrony Danych - zadania	Wykład: 4, w tym zajęcia zdalne: • Wykład synchroniczny: 4 Ćwiczenia audytoryjne: 4, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 4	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Ocena stanu bezpieczeństwa informacji w organizacji	Wykład: 4, w tym zajęcia zdalne: • Wykład synchroniczny: 4 Ćwiczenia audytoryjne: 4, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 4	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Polityka bezpieczeństwa informacji w organizacji	Wykład: 6, w tym zajęcia zdalne: • Wykład synchroniczny: 6 Ćwiczenia audytoryjne: 2, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 2	2	Zaliczenie na ocenę	Przedmioty obowiązkowe
Pozostała dokumentacja w zakresie danych osobowych	Wykład: 2, w tym zajęcia zdalne: • Wykład synchroniczny: 2 Ćwiczenia audytoryjne: 2, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 2	1	Zaliczenie na ocenę	Przedmioty obowiązkowe

Przedmiot	Liczba godzin	Punkty ECTS	Forma weryfikacji	Obligatoryjność
Umowa powierzenia przetwarzania danych osobowych	Wykład: 2, w tym zajęcia zdalne: • Wykład synchroniczny: 2 Ćwiczenia audytoryjne: 2, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 2	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Rejestr czynności przetwarzania danych osobowych	Wykład: 2, w tym zajęcia zdalne: • Wykład synchroniczny: 2 Ćwiczenia audytoryjne: 2, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 2	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Ochrona danych w procesach kadrowych	Wykład: 2, w tym zajęcia zdalne: • Wykład synchroniczny: 2 Ćwiczenia audytoryjne: 2, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 2	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Zabezpieczenia fizyczne i techniczne w organizacji	Wykład: 4, w tym zajęcia zdalne: • Wykład synchroniczny: 4 Ćwiczenia audytoryjne: 4, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 4	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Cyberbezpieczeństwo informacji i technologie bezpieczeństwa teleinformatycznego	Wykład: 12, w tym zajęcia zdalne: • Wykład synchroniczny: 12 Ćwiczenia audytoryjne: 4, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 4	2	Zaliczenie na ocenę	Przedmioty obowiązkowe
Suma	**82**	**14**		

Semestr 2

Przedmiot	Liczba godzin	Punkty ECTS	Forma weryfikacji	Obligatoryjność
Zarządzanie incydentami i naruszeniami bezpieczeństwa informacji	Wykład: 4, w tym zajęcia zdalne: • Wykład synchroniczny: 4 Ćwiczenia audytoryjne: 4, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 4	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Wymogi i kontrole UODO	Wykład: 6, w tym zajęcia zdalne: • Wykład synchroniczny: 6 Ćwiczenia audytoryjne: 2, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 2	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Auditor wiodący systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001	Wykład: 30, w tym zajęcia zdalne: • Wykład synchroniczny: 30 Ćwiczenia audytoryjne: 10, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 10	5	Zaliczenie na ocenę	Przedmioty obowiązkowe
Zarządzanie ciągłością działania (analiza ryzyka)	Wykład: 2, w tym zajęcia zdalne: • Wykład synchroniczny: 2 Ćwiczenia audytoryjne: 2, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 2	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Bezpieczeństwo informacji a sztuczna inteligencja	Wykład: 2, w tym zajęcia zdalne: • Wykład synchroniczny: 2 Ćwiczenia audytoryjne: 2, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 2	1	Zaliczenie na ocenę	Przedmioty obowiązkowe
Ochrona informacji niejawnych	Wykład: 4, w tym zajęcia zdalne: • Wykład synchroniczny: 4 Ćwiczenia audytoryjne: 4, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 4	1	Zaliczenie na ocenę	Przedmioty obowiązkowe

Przedmiot	Liczba godzin	Punkty ECTS	Forma weryfikacji	Obligatoryjność
Ochrona danych – studium przypadku (samorząd terytorialny, szkolnictwo, służba zdrowia, biznes, marketing, e-commerce, social-media)	Wykład: 12, w tym zajęcia zdalne: • Wykład synchroniczny: 12 Ćwiczenia audytoryjne: 8, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 8	3	Zaliczenie	Przedmioty obowiązkowe
Projekt dyplomowy	Wykład: 2, w tym zajęcia zdalne: • Wykład synchroniczny: 2 Ćwiczenia audytoryjne: 2, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 2	3	Zaliczenie	Przedmioty obowiązkowe
Suma	**96**	**16**		

Matryca efektów uczenia się

2026/27/N_Z/6/EKR/InspOch/all

Przedmiot	Specjalność	Obligatoryjność	Semestr	InspOch_K6_W01	InspOch_K6_W02	InspOch_K6_W03	InspOch_K6_U01	InspOch_K6_U02	InspOch_K6_U03	InspOch_K6_K01	InspOch_K6_K02	InspOch_K6_K03
Wykład Inauguracyjny		F	1s	x								x
Pojęcie informacji i metody zarządzania informacją		O	1s			x						
Przykłady nadużyć i przestępstw w obszarze bezpieczeństwa informacji i danych osobowych		O	1s	x								
Regulacje prawne w zakresie bezpieczeństwa informacji i ochrony danych osobowych		O	1s	x				x				
Menedżer Bezpieczeństwa Informacji i Inspektor Ochrony Danych - zadania		O	1s		x		x			x	x	x
Ocena stanu bezpieczeństwa informacji w organizacji		O	1s		x		x					
Polityka bezpieczeństwa informacji w organizacji		O	1s			x			x			
Pozostała dokumentacja w zakresie danych osobowych		O	1s			x		x				
Umowa powierzenia przetwarzania danych osobowych		O	1s			x		x				
Rejestr czynności przetwarzania danych osobowych		O	1s			x		x				
Ochrona danych w procesach kadrowych		O	1s		x					x		
Zabezpieczenia fizyczne i techniczne w organizacji		O	1s	x								
Cyberbezpieczeństwo informacji i technologie bezpieczeństwa teleinformatycznego		O	1s	x			x				x	x
Zarządzanie incydentami i naruszeniami bezpieczeństwa informacji		O	2s			x			x		x	
Wymogi i kontrole UODO		O	2s	x								
Auditor wiodący systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001		O	2s		x			x				

Przedmiot	Specjalność	Obligatoryjność	Semestr	InspOch_K6_W01	InspOch_K6_W02	InspOch_K6_W03	InspOch_K6_U01	InspOch_K6_U02	InspOch_K6_U03	InspOch_K6_K01	InspOch_K6_K02	InspOch_K6_K03
Zarządzanie ciągłością działania (analiza ryzyka)		O	2s			x	x					
Bezpieczeństwo informacji a sztuczna inteligencja		O	2s	x			x				x	
Ochrona informacji niejawnych		O	2s	x			x				x	
Ochrona danych – studium przypadku (samorząd terytorialny, szkolnictwo, służba zdrowia, biznes, marketing, e-commerce, social-media)		O	2s		x			x	x	x	x	x
Projekt dyplomowy		O	2s	x	x	x	x	x	x	x	x	x
Suma (obowiązkowy):				8	6	8	7	7	4	4	7	4
Suma (fakultatywny):				1	0	0	0	0	0	0	0	1
Suma:				9	6	8	7	7	4	4	7	5