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:	33
Czas trwania studiów (liczba semestrów):	2
Odniesienie do poziomu PRK:	7 PRK

Opis studiów podyplomowych

Cele kształcenia, opis grupy odbiorców

Celem głównym studiów podyplomowych „Menedżer Bezpieczeństwa Informacji i Ochrony Danych Osobowych” jest przygotowanie słuchacza studiów do pracy zawodowej w zakresie bezpieczeństwa informacji i ochrony danych osobowych, jak również podniesienie kwalifikacji osób już zatrudnionych w tej dziedzinie.

Do celów szczegółowych należy przekazanie wiedzy teoretycznej i umiejętności praktycznych w zakresie: regulacji prawnych w obszarze bezpieczeństwa informacji i ochrony danych osobowych, zarządzania ryzykiem w organizacji, identyfikacji i analizy zagrożeń dla bezpieczeństwa informacji i danych osobowych oraz oceny ryzyka związanego z tymi zagrożeniami; tworzenia polityki bezpieczeństwa informacji w organizacji, prowadzenia audytów; bieżącego monitorowania stanu bezpieczeństwa informacji i danych osobowych, przestrzegania przepisów i zasad; eliminacji albo ograniczania zagrożeń; prowadzenia dokumentacji w obszarze bezpieczeństwa informacji i ochrony danych osobowych, a także podejmowania odpowiednich działań profilaktycznych; technologii bezpieczeństwa teleinformatycznego, zarządzania ciągłością działania; zarządzania bezpieczeństwem informacji i ochroną danych osobowych zgodnie z najnowszymi osiągnięciami teorii i praktyki.

„Menedżer Bezpieczeństwa Informacji i Ochrony Danych Osobowych” to 2-semestralne studia podyplomowe adresowane do:

- osób pracujących lub chcących nauczyć się wykonywania zadań Inspektora Ochrony Danych lub Menedżera Bezpieczeństwa Informacji, bądź podnieść swoje kwalifikacje w tym zakresie,
- osób pragnących uzyskać specjalistyczne, przyszłościowe kwalifikacje zawodowe bądź poszerzyć swoją wiedzę z zakresu nowych przepisów obowiązujących od 25 maja 2018 r. na temat ochrony danych osobowych,
- osób zajmujących się doradztwem, audytem z zakresu bezpieczeństwa informacji i ochrony danych osobowych,
- kadry menedżerskiej wyższego i średniego szczebla zainteresowanych poszerzeniem wiedzy i umiejętności,
- osób zainteresowanych problematyką bezpieczeństwa informacji i ochrony danych osobowych,
- wszystkich zainteresowanych samodoskonaleniem i podnoszeniem własnych kwalifikacji,
- absolwentów wszystkich kierunków studiów, zainteresowanych nowoczesnymi rozwiązaniami z zakresu bezpieczeństwa informacji i ochrony danych osobowych, pragnących uzyskać nową specjalność zawodową,
- osób wyznaczonych w firmie do pełnienia funkcji Inspektora Ochrony Danych lub Oficera Bezpieczeństwa Informacji, lub do wykonywania zadań w zakresie ochrony danych osobowych.

Charakterystyka studiów podyplomowych

Studia umożliwią przygotowanie do praktycznej, efektywnej i skutecznej realizacji wyzwań z zakresu zarządzania bezpieczeństwem informacji, przed którymi stoją współczesne przedsiębiorstwa i zakłady pracy. Założeniem studiów jest także, aby absolwenci na podstawie zdobytej wiedzy podczas studiów podyplomowych, potrafili pomóc przedsiębiorstwom przygotować się do polskich i unijnych procedur regulujących obszar ochrony danych osobowych oraz przyczynić się do wzrostu ich konkurencyjności. Ukończenie studiów przygotowuje do pracy na stanowisku Inspektora Ochrony Danych lub Menedżera Bezpieczeństwa Informacji oraz prowadzenia szkoleń z zakresu ochrony danych osobowych i bezpieczeństwa informacji.

Analizując potrzeby edukacyjne w zakresie ochrony danych osobowych i zarządzania bezpieczeństwem informacji warto podkreślić znaczenie umiejętnego i praktycznego zastosowania metod oraz technik do rozwiązywania problemów dotyczących bezpieczeństwa danych. W tym celu założono podział zajęć w toku studiów na część wykładową i część ćwiczeniową. Część wykładowa prowadzona będzie metodą audytoryjną z wykorzystaniem różnych technik audiowizualnych (PowerPoint, foliogramy, flipchart). Część ćwiczeniowa prowadzona będzie w oparciu o studia przypadków (case studies), ćwiczenia i prace w grupach. Zajęcia teoretyczne, jak i praktyczne będą prowadzone z wykorzystaniem technik kształcenia na odległość, w tym co najmniej jeden zjazd odbędzie się w formie stacjonarnej.

Wykłady prowadzone będą przez specjalistów z SGGW, zaproszonych wykładowców z innych uczelni oraz praktyków, zajmujących się ochroną danych osobowych i bezpieczeństwem informacji.

Wymiar, zasady i forma odbywania oraz zaliczania praktyk

Na studiach podyplomowych nie są realizowane praktyki.

Warunki ukończenia studiów podyplomowych

§1

Zajęcia dydaktyczne w ramach Studiów Podyplomowych „Menedżer bezpieczeństwa informacji i ochrony danych osobowych" kończą się Zaliczeniem na ocenę z poszczególnych przedmiotów. W przypadku niektórych przedmiotów wskazanych w planie i programie studiów, warunkiem dopuszczenia do Zaliczenia na ocenę jest złożenie pracy projektowej. Warunkiem ukończenia studiów jest także wypełnienie Testu Kompetencji Społecznych po zdaniu Zaliczeń na ocenę i po wykonaniu prac projektowych. Wypełnienie Testu Kompetencji Społecznych jest równoznaczne z jego zaliczeniem. W programie studiów nie ma pracy dyplomowej.

§2

Słuchacze otrzymają świadectwo ukończenia studiów podyplomowych po spełnieniu następujących warunków:

- ukończą studia z pozytywnym wynikiem, to znaczy uzyskają z każdego przedmiotu przewidzianego programem studiów co najmniej ocenę dostateczną;
- złożą prace projektowe wskazane w planie i programie studiów;
- wypełnią Test Kompetencji Społecznych;
- uiszczą opłatę za studia określoną w warunkach rekrutacji.

§3

Wynik końcowy ze studiów będzie ustalany w oparciu o średnią arytmetyczną ocen uzyskanych z poszczególnych przedmiotów przewidzianych programem studiów i zgodnie z poniższymi przedziałami:

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

Wyniki końcowe ze studiów są zgodne ze skalą ocen zawartą w regulaminie studiów podyplomowych.

Zasady i tryb rekrutacji

O przyjęcie na studia podyplomowe mogą ubiegać się kandydaci posiadający dyplom ukończenia studiów pierwszego stopnia, drugiego stopnia lub jednolitych studiów magisterskich. Kandydaci przyjmowani są wg kolejności zgłoszeń.

W terminach określonych w harmonogramie rekrutacji, kandydat:

- rejestruje się w systemie rekrutacyjnym SGGW i dołącza w nim skany dokumentów niezbędnych do kwalifikacji,
- otrzymuje informację o zakwalifikowaniu lub nie,
- dostarcza wymagane dokumenty,
- wnosi na wskazany numer konta, właściwy danym studiom podyplomowym opłatę za pierwszy semestr lub za całe studia,
- po dostarczeniu wymaganych dokumentów, zgodnych z przedstawionymi do kwalifikacji w systemie rekrutacyjnym oraz potwierdzeniu wniesienia opłaty - otrzymuje informację o przyjęciu na studia podyplomowe.

W przypadku nieuruchomienia danej edycji studiów podyplomowych kandydat otrzymuje informację w tej sprawie oraz zwrot wniesionych opłat. Harmonogram przebiegu rekrutacji określany jest odrębnie dla każdej edycji studiów podyplomowych.

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
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	2	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	2	Zaliczenie na ocenę	Przedmioty obowiązkowe
Ocena stanu 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
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: 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
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	**80**	**18**		

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	2	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	2	Zaliczenie na ocenę	Przedmioty obowiązkowe
Auditor wiodący systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji – Wymagania”	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: 16, w tym zajęcia zdalne: • Wykład synchroniczny: 16 Ćwiczenia audytoryjne: 8, w tym zajęcia zdalne: • Ćwiczenia audytoryjne synchroniczne: 8	3	Zaliczenie na ocenę	Przedmioty obowiązkowe
Suma	**96**	**15**		

Matryca efektów uczenia się

2025/26/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
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								
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							
Zabezpieczenia fizyczne i techniczne w organizacji		O	1s	x								
Cyberbezpieczeństwo informacji i technologie bezpieczeństwa teleinformatycznego		O	1s	x								
Zarządzanie incydentami i naruszeniami bezpieczeństwa informacji		O	2s			x			x			
Wymogi i kontrole UODO		O	2s	x								
Auditor wiodący systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji – Wymagania”		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	1s lub 2s			x	x					
Bezpieczeństwo informacji a sztuczna inteligencja		O	2s	x								
Ochrona informacji niejawnych		O	2s	x								
Ochrona danych – studium przypadku (samorząd terytorialny, szkolnictwo, służba zdrowia, biznes, marketing, e-commerce, social-media)		O	2s		x							
Suma (obowiązkowy):				7	5	7	3	4	2	1	1	1
Suma (fakultatywny):				0	0	0	0	0	0	0	0	0
Suma:				7	5	7	3	4	2	1	1	1