PROGRAM STUDIÓW PODYPLOMOWYCH

1. Informacje o studiach

Nazwa studiów podyplomowych: **Inspektor Ochrony Danych**
Przyporządkowanie do dyscypliny naukowej: **nauki o bezpieczeństwie**.
Czas trwania studiów: **2 semestry**
Język wykładowy: **polski**
Poziom umożliwiający uzyskanie kwalifikacji cząstkowych (6, 7 albo 8 PRK): **Poziom 6**
Szczegółowe warunki rekrutacji na studia, z uwzględnieniem: 1. wymogu posiadanego dyplomu (studia pierwszego stopnia, studia drugiego stopnia, jednolite studia magisterskie): **studia pierwszego, drugiego stopnia lub jednolite studia magisterskie** 2. zasad kwalifikacji w wypadku, gdy liczba kandydatów przekracza liczbę miejsc: **kolejność zgłoszeń**
Liczba osób przyjętych, która pozwala na uruchomienie studiów: **15**
Warunki ukończenia studiów podyplomowych (uzyskanie minimum 30 punktów ECTS oraz np. praca dyplomowa, egzamin dyplomowy o ile program studiów to przewiduje): **uzyskanie 30 punktów ECTS oraz praca dyplomowa**
Przewidywany termin rozpoczęcia zajęć: **październik 2020 r.**
Propozycja bazy dydaktycznej niezbędnej do realizacji programu studiów: **sale dydaktyczne PWSTE wyposażone w komputer z oprogramowaniem MS Office oraz rzutniki do prezentacji multimedialnych, zdalne nauczanie za pośrednictwem narzędzi teleinformatycznych.**

Opis efektów uczenia się dla studiów podyplomowych wraz z informacją o sposobach ich weryfikacji.

Lp.	Symbol efektu uczenia się	Treść efektu uczenia się	Kod składnika opisu- Uniwersalne charakterystyki poziomów w PRK	Kategoria opisowa – aspekty o podstawowym znaczeniu	Kod składnika opisu- charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8PRK	Sposób weryfikacji efektów uczenia się
1.	K_W01	Uczestnik studiów podyplomowych ma pogłębioną i uporządkowaną wiedzę w zakresie zagadnień prawnych i procedur związanych z bezpieczeństwem informacji przetwarzanych przy użyciu systemów informatycznych	P6U_W	**Zakres i głębia** – kompletność perspektywy poznawczej i zależności **Kontekst** – uwarunkowania, skutki	P6S_WG P6S_WK	E lub Z
2.	K_W02	Uczestnik studiów podyplomowych zna zagadnienia związane z kontrolą systemów informacyjnych w sektorze publicznym oraz zna zasady planowania, organizacji i kontroli systemów informatycznych	P6U_W	**Zakres i głębia** – kompletność perspektywy poznawczej i zależności **Kontekst** – uwarunkowania, skutki	P6S_WG P6S_WK	E lub Z
3.	K_W03	Uczestnik studiów podyplomowych posiada wiedzę z zakresu technik zarządzania usługami IT	P6U_W	**Zakres i głębia** – kompletność perspektywy poznawczej i zależności **Kontekst** – uwarunkowania, skutki	P6S_WG P6S_WK	E lub Z
4.	K_W04	Uczestnik studiów podyplomowych zna i rozumie zagadnienia związane z zarządzaniem projektami informatycznymi	P6U_W	**Zakres i głębia** – kompletność perspektywy poznawczej i zależności **Kontekst** – uwarunkowania, skutki	P6S_WG P6S_WK	E lub Z
5.	K_W05	Uczestnik studiów podyplomowych posiada wiedzę na temat kontroli legalności oprogramowania oraz wykrywania i zapobiegania oszustwom i nadużyciom komputerowym	P6U_W	**Zakres i głębia** – kompletność perspektywy poznawczej i zależności **Kontekst** – uwarunkowania, skutki	P6S_WG P6S_WK	E lub Z
6.	K_U01	Uczestnik studiów podyplomowych potrafi analizować i wykrywać problemy jakie pojawiają się w praktyce funkcjonowania systemu zarządzania bezpieczeństwem informacji	P6U_U	**Wykorzystanie wiedzy** – rozwiązywane problemy i wykonywane zadania **Uczenie się** – planowanie własnego rozwoju i rozwoju innych osób	P6S_UW P6S_UO P6S_UU	E lub Z
5.	K_U02	Uczestnik studiów podyplomowych potrafi zaplanować i przeprowadzić audyt bezpieczeństwa informacji, legalności oprogramowania, systemów oraz infrastruktury teleinformatycznej w instytucji zgodnie z międzynarodowymi standardami audytu.	P6U_U	**Wykorzystanie wiedzy** – rozwiązywane problemy i wykonywane zadania **Uczenie się** – planowanie własnego rozwoju i rozwoju innych osób	P6S_UW P6S_UO P6S_UU	E lub Z
6.	K_U03	Uczestnik studiów podyplomowych potrafi opracować plan i procedurę realizacji audytów wewnętrznych.	P6U_U	**Wykorzystanie wiedzy** – rozwiązywane problemy i wykonywane zadania **Uczenie się** – planowanie własnego rozwoju i rozwoju innych osób	P6S_UW P6S_UO P6S_UU	E lub Z

7.	K_U04	Uczestnik studiów podyplomowych potrafi wykorzystać narzędzia informatyczne do przeprowadzenia audytu systemów informatycznych i do wykrywania oszustw i nadużyć komputerowych.	P6U_U	**Wykorzystanie wiedzy** – rozwiązywane problemy i wykonywane zadania **Uczenie się** – planowanie własnego rozwoju i rozwoju innych osób	P6S_UW P6S_UO P6S_UU	
8.	K_K01	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawniania funkcjonowania organizacji, zgodnie z prawem i zasadami etyki.	P6U_K	**Oceny** - krytyczne podejście **Odpowiedzialność** – wypełnianie zobowiązań społecznych i działanie na rzecz interesu publicznego **Rola zawodowa –** niezależność i rozwój etosu	P6S_KK P6S_KO P6S_KR	E lub Z
9.	K_K02	Uczestnik studiów podyplomowych wykazuje się obiektywnością i niezależnością w formułowaniu ocen, stanowiących podstawę do rozstrzygania sytuacji konfliktowych	P6U_K	**Oceny** - krytyczne podejście **Odpowiedzialność** – wypełnianie zobowiązań społecznych i działanie na rzecz interesu publicznego **Rola zawodowa –** niezależność i rozwój etosu	P6S_KK P6S_KO P6S_KR	E lub Z
10.	K _K03	Uczestnik studiów podyplomowych ma świadomość znaczenia komunikacji w procesie podejmowania decyzji i rozstrzygania sporów	P6U_K	**Oceny** - krytyczne podejście **Odpowiedzialność** – wypełnianie zobowiązań społecznych i działanie na rzecz interesu publicznego **Rola zawodowa –** niezależność i rozwój etosu	P6S_KK P6S_KO P6S_KR	E lub Z

3. Harmonogram realizacji programu studiów podyplomowych.

Lp.	Nazwa zajęć	Liczba godzin (ogółem)	Wykład (liczba godzin)	Ćwiczenia/ Seminaria (liczba godzina)	Laboratorium/ Pracownia (liczba godzin)	Forma Zaliczenia (E/Z)	Punkty ECTS
Rok I – semestr I							
1.	**Wprowadzenie do zagadnień związanych z kontrolą systemów informacyjnych i ochroną danych osobowych** – Podstawowe definicje i funkcje związane z obszarem bezpieczeństwa informacji i ochrony danych osobowych – Podejście do kontroli i priorytetyzacja zadań kontrolnych w obszarze przetwarzania danych – Zasoby organizacji i proces ich kontroli w podejściu praktycznych do wymienionych zabezpieczeń. – Rola kontroli w przeciwdziałaniu zagrożeniom związanym z obszarem informacyjnym. – Analiza najbardziej popularnych zagrożeń i podatności związanych z systemami teleinformatycznymi – Wprowadzenie do standardów, wytycznych, najlepszych praktyk, kodeksów związanych z bezpieczeństwem informacji i ochroną danych osobowych.	20	Wykład 20 godzin			Zaliczenie na ocenę	3
2.	**Prawne aspekty ochrony danych osobowych** – wprowadzenie do regulacji prawnych Unii Europejskiej oraz prawa krajowego i międzynarodowego po wprowadzenie ogólnego rozporządzenia o ochronie danych (RODO) i nowelizacji innych przepisów związanych z tematyką ochrony danych osobowych, – Obowiązki nałożone na administratora oraz podmiot przetwarzający, – Status i rola IOD – uprawnienia i obowiązki w zakresie ochrony danych osobowych, – Status i zasady działania organów nadzorczych, – Monitorowanie przestrzegania przepisów w zakresie ochrony danych osobowych przez pracowników i	20	wykład (20 godzin)			Egzamin na ocenę	3

	osoby trzecie oraz działania zapewniające w przedmiotowym zakresie – Konsekwencje wykonywania działań w zakresie szacowania ryzyka związanego z przetwarzaniem danych osobowych. – Przestępstwa przeciwko ochronie informacji wynikające z kodeksu karnego.						
3.	**Planowanie i realizacja kontroli, sprawdzeń i audytów w zakresie związanym z zabezpieczeniem informacji** – Plan roczny i plany strategiczne – Etapy tworzenia planu audytu – Identyfikacja obszarów ryzyka – Analiza ryzyka na potrzeby planowania – Audyt poza planem – Realizacja audytu IT – program audytu, techniki gromadzenia dowodów, próbkowanie i dokumentowanie wyników – Krajowe i międzynarodowe standardy audytu wewnętrznego – Krajowe i międzynarodowe wytyczne dla Inspektorów ochrony danych osobowych – Znaczenie audytu IT w organizacji – Kodeks etyki audytora	20	wykład (20 godzin)			Zaliczenie na ocenę	2
4.	**Planowanie i organizacja systemów informatycznych służących do przetwarzania danych osobowych** – Plan strategiczny – Architektura informatyczna i kierunek technologiczny – Zarządzanie zasobami ludzkimi w IT – Zarządzanie inwestycjami – Zarządzanie projektami IT	10	Wykład (10 godzin)			Zaliczenie na ocenę	1
5.	**Zarządzanie ryzykiem w obrębie danych osobowych** – Metodyka zarządzania ryzykiem w zakresie bezpieczeństwa informacji, – Organizacja i odpowiedzialności w zakresie procesu oceny i szacowania ryzyka, – Szacowanie ryzyka – warsztaty praktyczne, – Tworzenie planów postępowania z ryzykiem	10	Wykład (5 godzin)	Ćwiczenia (5 godzin)		Zaliczenie na ocenę	1

	– Informowanie o ryzyku, – Monitoring i przegląd ryzyka.						
6.	**Inspektor ochrony danych - realizacja zadań ustawowych - warsztaty praktyczne** – Zasady prowadzenia i weryfikacji podstawowych rejestrów. – Działania nadzorcze i kontrolne związane z udostępnianiem i powierzaniem danych osobowych – Działania doradcze IOD w obszarze zamówień publicznych oraz zasad weryfikacji podmiotu przetwarzającego. – Weryfikacja procesu rekrutacyjnego oraz procesów związanych z zatrudnieniem – Prawne aspekty stosowania monitoringu. – Zagrożenia związane z przetwarzaniem danych osobowych w organizacji i rola IOD w tym zakresie.	20	Wykład (10 godzin)	Ćwiczenia (10 godzin)		Zaliczenie na ocenę	3
Razem semestr I		**100**					**13**
			Rok I – semestr II				
7.	**Projektowanie i kontrola obszaru bezpieczeństwa fizycznego i środowiskowego** – Ustawa o ochronie osób i mienia – Pracownicy ochrony, ochrona wewnętrzna, SUFO, koncesjonowane podmioty realizujące usługi z zakresu bezpieczeństwa – Zagrożenia dla bezpieczeństwa, w zależności od uwarunkowań geograficznych, instytucjonalnych, obiektowych – Plany a instrukcje ochrony obiektów – ochrona mienia i osób, pracownik kwalifikowany, ustawa o broni i amunicji – Ochrona osobista i VIP – Agencje detektywistyczne w służbie biznesu – Konwoje i inkaso – Cash processing we współczesnej firmie – Technika w służbie bezpieczeństwa: SSWiN, CCTV, KD, RCP, inteligentne budynki – Współczesne systemy zarządzania i kontroli w logistyce (RFID) oraz nadzór nad personelem	20	Wykład (10 godzin)	Ćwiczenia (10 godzin)		Zaliczenie na ocenę	2

	– Bezpieczeństwo pożarowe i BHP – Archiwizacja i bezpieczeństwo dokumentów fizycznych – Zasady postępowania w sytuacjach kryzysowych, napad, włamanie, pożar, podłożenie ładunku wybuchowego, z pierwszej pomocy przedmedycznej – Organizacja kancelarii tajnych i procesu kontroli informacji niejawnych						
8.	**System zarządzania bezpieczeństwem informacji zgodny z wymaganiami ISO/IEC 27001:2013** – Struktura i podstawy ISMS – Organizacja bezpieczeństwa – Bezpieczeństwo zasobów ludzkich – Zarządzanie aktywami – Kontrola dostępu – Kryptografia – Bezpieczeństwo fizyczne oraz środowiskowe – Bezpieczna eksploatacja. Zarządzanie sieciami i systemami informatycznymi – Bezpieczeństwo komunikacji – Pozyskiwanie, rozwój oraz utrzymanie systemów – Relacje z dostawcami – Zarządzanie incydentami – Aspekty bezpieczeństwa w zarządzaniu ciągłością działania – Zgodność z przepisami prawa i standardami	30	Wykład (30 godzin)			Egzamin na ocenę	3
9.	**Audyt infrastruktury teleinformatycznej** – Techniki przeprowadzania audytu infrastruktury informatycznej, – Podejście do mobilności i przetwarzania danych w chmurach obliczeniowych; – Techniki kontroli warstwy sieciowej, systemowej i aplikacyjnej, – Tworzenie audytowych list kontrolnych: CASE STUDY – Najczęściej występujące niezgodności i problemy identyfikowane w trakcie audytów.	10	Wykład (10 godzin)			Zaliczenie na ocenę	2
10.	**Wykrywanie i zapobieganie oszustwom i nadużyciom skutkującym wyciekiem danych osobowych**	10			Laboratorium (10 godzin)	Zaliczenie na ocenę	2

	– Zajęcia laboratoryjne – Metody analizy podatności i luk w oprogramowaniu, zabezpieczania systemów i struktur IT, bezpieczeństwo sieci bezprzewodowych, zarządzanie backupem, niszczenie i odzyskiwanie danych, analiza materiału dowodowego						
11.	**Ochrona organizacji przed wyciekiem danych osobowych** – Zajęcia laboratoryjne – Wdrażanie i możliwości administracyjne systemów klasy DLP (Data Leakage Prevention/Prevention)	10			Laboratorium (10 godzin)	Zaliczenie na ocenę	2
12.	**Kontynuacja działalności po awarii. Zarządzanie ciągłością działania.** – Role i odpowiedzialności – Plany awaryjne – Plany przywracania systemów po awarii – Testowanie planów awaryjnych – Odtwarzanie techniki teleinformatycznej po katastrofie.	10	Wykład (10 godzin)			Zaliczenie na ocenę	1
13.	**Zarządzanie kryzysowe. Krajowy system cyberbezpieczeństwa** – Działania w czasie kryzysu. – Działania lokalnych komórek CSIRT – Obowiązki operatorów usług kluczowych i dostawców usług cyfrowych – Organizacja systemu zarządzania cyberbezpieczeństwem – Architektura cyberbezpieczeństwa – określenie i powołanie struktur wewnętrznych – Współpraca z sektorowymi zespołami cyberbezpieczeństwa	10	Wykład (10 godzin)			Zaliczenie na ocenę	2
14.	**Bezpieczeństwo prawne – rozszerzone podejście**	10	Wykład (10 godzin)			Zaliczenie na ocenę	1

	– Kodeks karny – Przestępstwa przeciwko ochronie informacji – Odpowiedzialność z tytułu naruszenia przepisów ODO – Analiza projektów i nowelizacji – Prawa autorskie i zasady ochrony własności intelektualnej. – Dowód elektroniczny na potrzeby postępowania sądowego w postępowaniach karnych oraz postępowaniach cywilnych. – Tajemnica przedsiębiorstwa i inne tajemnice prawnie chronione.						
15.	**Seminarium dyplomowe (projektowe)**	10		Seminarium dyplomowe (projektowe) 10 godzin		Zaliczenie na ocenę	2
Razem semestr II		**120**					**17**
Razem Rok I (Suma godzin)		**220**					**30**

3. Formy odbywania praktyk zawodowych (liczba godzin, efekty uczenia się, sposoby weryfikacji założonych efektów uczenia się, sposób oceny instytucji, w której uczestnicy studiów podyplomowych odbywają praktyki zawodowe).

Nie przewiduje się (nie dotyczy)

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Wprowadzenie do zagadnień związanych z kontrolą systemów informacyjnych i ochroną danych osobowych **(**WKSIODO)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: I	Liczba punktów ECTS przypisana zajęciom:	ECTS: 3

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**20**
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**20**

II. INFORMACJE SZCZEGÓŁOWE	
UWAGA: Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
WKSIODO_W_01	Uczestnik studiów podyplomowych nabywa wiedzę na temat podstawowych funkcji związanych z obszarem bezpieczeństwa informacji i ochrony danych osobowych, definiuje podstawowe funkcje związane z obszarem bezpieczeństwa informacji i ochrony danych osobowych.
WKSIODO_W _02	Uczestnik studiów podyplomowych definiuje podstawowe funkcje związane z obszarem bezpieczeństwa informacji i ochrony danych osobowych, zna zasoby organizacji i proces ich kontroli w podejściu praktycznym do wymienionych zabezpieczeń
Umiejętności - potrafi	
WKSIODO _U_03	Uczestnik studiów podyplomowych potrafi dokonać analizy najbardziej popularnych zagrożeń i podatności związanych z systemami teleinformatycznymi

Kompetencji społecznych - jest gotów do	
WKSIODO _K_04	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
wykład		
TP-01	Podstawowe definicje i funkcje związane z obszarem bezpieczeństwa informacji i ochrony danych osobowych	wykład
TP-02	Podejście do kontroli i priorytetyzacja zadań kontrolnych w obszarze przetwarzania danych	wykład
TP-03	Zasoby organizacji i proces ich kontroli w podejściu praktycznym do wymienionych zabezpieczeń	wykład
TP-04	Rola kontroli w przeciwdziałaniu zagrożeniom związanym z obszarem informacyjnym	wykład
TP-05	Analiza najbardziej popularnych zagrożeń i podatności związanych z systemami teleinformatycznymi	wykład
TP-06	Wprowadzenie do standardów, wytycznych, najlepszych praktyk, kodeksów związanych z bezpieczeństwem informacji i ochroną danych osobowych	wykład

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
WKSIODO_W_01 WKSIODO_W _02 WKSIODO _U_03 WKSIODO _K_04	zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Prawne aspekty ochrony danych osobowych (PAODO)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: I	Liczba punktów ECTS przypisana zajęciom:	ECTS: 3

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**20**
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**20**

II. INFORMACJE SZCZEGÓŁOWE	
UWAGA: Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
PAODO_W_01	Uczestnik studiów podyplomowych nabywa wiedzę w zakresie nadzoru nad dokumentacją dotyczącą bezpieczeństwa informacji oraz monitorowania przestrzegania przepisów w zakresie ochrony danych osobowych i szacowania ryzyka związanego z przetwarzaniem danych osobowych
PAODO_W _02	Uczestnik studiów podyplomowych nabywa wiedzę dotyczącą zasad ochrony i przetwarzania danych osobowych oraz praw i obowiązków administratora i inspektora ochrony danych osobowych (audytora) w przedmiotowym zakresie.
PAODO_W _03	Uczestnik studiów podyplomowych definiuje i opisuje zasady ochrony i przetwarzania danych osobowych i informacji niejawnych oraz prawa i obowiązki podmiotów w przedmiotowym zakresie, scharakteryzuje przestępstwa przeciwko ochronie informacji wynikające z kodeksu karnego, skrytykuje, podsumuje, wymienia kryteria, przedstawi zagadnienie prawne dotyczące zabezpieczenia systemów teleinformatycznych i ochrony własności intelektualnej.
Umiejętności - potrafi	

PAODO _U_04	Uczestnik studiów podyplomowych potrafi sprawować nadzór nad dokumentacją dotyczącą bezpieczeństwa informacji, potrafi wykorzystywać dowód elektroniczny na potrzeby postępowania sądowego w postępowaniach karnych oraz cywilnych, posiada umiejętność w zakresie nadzorowania, nadzór dokumentacji dotyczącej bezpieczeństwa informacji.
PAODO _U_05	Uczestnik studiów podyplomowych samodzielnie wykona audyt w zakresie ochrony i przetwarzania danych osobowych, potrafi ocenić rolę i znaczenie administratora danych oraz audytora w zakresie ochrony informacji oraz jej zabezpieczenia
Kompetencji społecznych - jest gotów do	
PAODO _K_06	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
wykład		
TP-01	Wprowadzenie do regulacji prawnych Unii Europejskiej oraz prawa krajowego i międzynarodowego po wprowadzenie ogólnego rozporządzenia o ochronie danych (RODO) i nowelizacji innych przepisów związanych z tematyką ochrony danych osobowych,	wykład
TP-02	Obowiązki nałożone na administratora oraz podmiot przetwarzający,	wykład
TP-03	Status i rola IOD – uprawnienia i obowiązki w zakresie ochrony danych osobowych,	wykład
TP-04	Status i zasady działania organów nadzorczych,	wykład
TP-05	Monitorowanie przestrzegania przepisów w zakresie ochrony danych osobowych przez pracowników i osoby trzecie oraz działania zapewniające w przedmiotowym zakresie	wykład
TP-06	Konsekwencje wykonywania działań w zakresie szacowania ryzyka związanego z przetwarzaniem danych osobowych.	wykład
TP-07	Przestępstwa przeciwko ochronie informacji wynikające z kodeksu karnego.	wykład

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
PAODO _W_01 PAODO _W _02 PAODO _W _03 PAODO _U_04 PAODO_U_05 PAODO_K_06	Egzamin na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Planowanie i realizacja kontroli, sprawdzeń i audytów w zakresie związanym z zabezpieczeniem informacji (PRKSA)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: I	Liczba punktów ECTS przypisana zajęciom:	ECTS: 2

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**20**
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**20**

II. INFORMACJE SZCZEGÓŁOWE	
UWAGA: Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
PRKSA _W_01	Uczestnik studiów podyplomowych nabywa wiedzę w zakresie: zaplanowania, przygotowania i prowadzenia kontroli i audytu bezpieczeństwa informacji, zbierania dowodów oraz raportowania do kadry kierowniczej wyników
PRKSA _W _02	Uczestnik studiów podyplomowych omawia standardy prowadzenia kontroli i audytu bezpieczeństwa informacji oraz metodykę pracy specjalisty ds. audytu i kontroli bezpieczeństwa informacji
Umiejętności - potrafi	
PRKSA _U_03	Uczestnik studiów podyplomowych potrafi: zaplanować, przygotować i zrealizować zadanie kontrolne i audytowe w zakresie bezpieczeństwa informacji. Potrafi zebrać odpowiednie i wystarczające dowody z kontroli i audytu, sformułować zalecenia i przygotować raport z realizacji zadania.
Kompetencji społecznych - jest gotów do	

PRKSA _K_04	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
	wykład	
TP-01	Plan roczny i plany strategiczne	wykład
TP-02	Etapy tworzenia planu audytu	wykład
TP-03	Identyfikacja obszarów ryzyka	wykład
TP-04	Analiza ryzyka na potrzeby planowania	wykład
TP-05	Audyt poza planem	wykład
TP-06	Realizacja audytu IT – program audytu, techniki gromadzenia dowodów, próbkowanie i dokumentowanie wyników	wykład
TP-07	Krajowe i międzynarodowe standardy audytu wewnętrznego	wykład
TP-08	Krajowe i międzynarodowe wytyczne dla Inspektorów ochrony danych osobowych	wykład
TP-09	Znaczenie audytu IT w organizacji	wykład
TP-10	Kodeks etyki audytora	wykład

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
PRKSA _W_01 PRKSA _W_02 PRKSA _U_03 PRKSA _K_04	zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Planowanie i organizacja systemów informatycznych służących do przetwarzania danych osobowych (POSI)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: I	Liczba punktów ECTS przypisana zajęciom:	ECTS: 1

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**10**
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**10**

II. INFORMACJE SZCZEGÓŁOWE

Cele prowadzenia zajęć: poznanie technik: dopasowania strategicznego obszaru biznesu i obszaru IT oraz optymalizacji wykorzystania zasobów IT w organizacji. Zdobycie umiejętności pozwalających wykorzystywać strukturę ramową podczas definiowania architektury informacji oraz określania kierunku technologicznego. Pozyskanie kompetencji w wykorzystywaniu właściwego instrumentarium dotyczącego realizacji projektów i inicjatyw oraz zarządzania inwestycjami IT

UWAGA:

Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.

Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
POSI_W_01	Uczestnik studiów podyplomowych nabywa wiedzę w zakresie poznania technik: dopasowania strategicznego obszaru biznesu i obszaru IT oraz optymalizacji wykorzystania zasobów IT w organizacji. Definiuje misję, wizję, cele biznesowe, strategie IT, wskaźniki realizacji celu, wskazuje różnice pomiędzy strategią biznesową a strategią IT oraz wymienia cele budowy strategii IT w organizacji
POSI _W _02	Uczestnik studiów podyplomowych opisuje metody i techniki pozwalające zdefiniować architekturę informacji, wskaże procesy niezbędne do wyznaczenia kierunku technologicznego w organizacji oraz przedstawia sposoby osiągnięcia efektywności kosztowej przez obszar IT w organizacji.

POSI _W _03	Uczestnik studiów podyplomowych przedstawia sposoby pozyskiwania i zarządzania kompetentnymi i zmotywowanymi pracownikami IT, wymienia metody zapewnienia dostarczania przez projekty i inicjatywy IT rezultatów w uzgodnionych ramach czasowych, kosztowych i jakościowych.
Umiejętności - potrafi	
POSI _U_04	Uczestnik studiów podyplomowych potrafi wyznaczyć cele kontrolne i mierniki dla domeny strategia IT, architektura informacji, kierunek technologiczny, zarządzanie inwestycjami, zarządzanie projektami, zarządzanie zasobami ludzkimi
POSI _U_05	Uczestnik studiów podyplomowych potrafi zaplanować niezbędne do wykonania czynności podczas opracowania strategii IT, definiowania architektury informacji i kierunku technologicznego oraz przygotuje zestaw działań zapewniający, że zarządzanie inwestycjami, zasobami ludzkimi a także projektami w obszarze IT będzie efektywnie zaplanowane.
Kompetencji społecznych - jest gotów do	
POSI _K_06	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
wykład		
TP-01	Plan strategiczny	wykład
TP-02	Architektura informatyczna i kierunek technologiczny	wykład
TP-03	Zarządzanie zasobami ludzkimi w IT	wykład
TP-04	Zarządzanie inwestycjami	wykład
TP-05	Zarządzanie projektami IT	wykład

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
POSI_W_01 POSI _W_02 POSI _W_03 POSI _U_04 POSI _U_05 POSI _K_06	zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Zarządzanie ryzykiem w obrębie danych osobowych (ZRODO)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: I	Liczba punktów ECTS przypisana zajęciom:	ECTS: 1

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**5**
Ćwiczenia:		Ćwiczenia:	**5**
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**10**

II. INFORMACJE SZCZEGÓŁOWE

Cele prowadzenia zajęć: poznanie otoczenia regulacyjnego dla zarządzania ryzykiem w obszarze danych osobowych, zdobycie umiejętności identyfikacji, oceny i postępowania z ryzykiem. Pozyskanie kompetencji w wykorzystywaniu właściwego instrumentarium dotyczącego domeny ryzyka

UWAGA:

Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.

Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
ZRODO_W_01	Uczestnik studiów podyplomowych nabywa definiuje ryzyko, prawdopodobieństwo, wpływ (siłę oddziaływania), opisuje składowe ryzyka i składowe procesu zarządzania ryzykiem oraz opisuje ilościową i jakościową ocenę ryzyka oraz macierz ryzyka
ZRODO_W_02	Uczestnik studiów podyplomowych wskazuje różnice pomiędzy ryzykiem inherentnym a ryzykiem rezydualnym, wymienia normy ISO związane z zarządzaniem ryzykiem oraz wymienia kryteria wymagane podczas procesu zarządzania ryzykiem
ZRODO_W _03	Uczestnik studiów podyplomowych wskazuje normy ISACA powiązane z obszarem ryzyka, wskaże i wiąże przykładowe zasoby z podatnościami i możliwymi ryzykami oraz przedstawia możliwe ścieżki w planie postępowania z ryzykiem

Umiejętności - potrafi	
ZRODO_U _04	Uczestnik studiów podyplomowych potrafi wyznaczyć ryzyko w obszarze danych osobowych, ocenia ryzyko w projekcie, organizacji, w obszarze bezpieczeństwa oraz ocenia ryzyko w oparciu o analizę utraty poufności, integralności i dostępności.
ZRODO_U _05	Uczestnik studiów podyplomowych weryfikuje proces zarządzania ryzykiem w organizacji, projekcie, obszarze bezpieczeństwa, samodzielnie tworzy macierz oceny ryzyka oraz ocenia krytyczność aplikacji przetwarzającej dane osobowe w oparciu o analizę utraty poufności, integralności i dostępności oraz przypisze adekwatne mechanizmy bezpieczeństwa
Kompetencji społecznych - jest gotów do	
ZRODO_K_ 06	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki
ZRODO_K_ 07	Uczestnik studiów podyplomowych ma świadomość znaczenia komunikacji w procesie podejmowania decyzji i rozstrzygania sporów.

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
wykład		
TP-01	Metodyka zarządzania ryzykiem w zakresie bezpieczeństwa informacji	wykład
TP-02	Organizacja i odpowiedzialność w zakresie procesu oceny i szacowania ryzyka	wykład
ćwiczenia		
TP-03	Szacowanie ryzyka – warsztaty praktyczne	ćwiczenia
TP-04	Tworzenie planów postępowania z ryzykiem	ćwiczenia
TP-05	Informowanie o ryzyku	ćwiczenia
TP-06	Monitoring i przegląd ryzyka	ćwiczenia

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
ZRODO_W_01 ZRODO_W_02 ZRODO_W_03 ZRODO_U _04 ZRODO_U _05 ZRODO_K_ 06 ZRODO_K_ 07	Zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Inspektor ochrony danych – realizacja zadań ustawowych (IODRZU)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: I	Liczba punktów ECTS przypisana zajęciom:	ECTS: 3

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**10**
Ćwiczenia:		Ćwiczenia:	**10**
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**20**

II. INFORMACJE SZCZEGÓŁOWE

Cele prowadzenia zajęć: poznanie otoczenia regulacyjnego dla zarządzania ryzykiem w obszarze danych osobowych, zdobycie umiejętności identyfikacji, oceny i postępowania z ryzykiem. Pozyskanie kompetencji w wykorzystywaniu właściwego instrumentarium dotyczącego domeny ryzyka

UWAGA:

Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.

Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
IODRZU _W_01	Uczestnik studiów podyplomowych nabywa definiuje ryzyko, prawdopodobieństwo, wpływ (siłę oddziaływania), opisuje składowe ryzyka i składowe procesu zarządzania ryzykiem oraz opisuje ilościową i jakościową ocenę ryzyka oraz macierz ryzyka
IODRZU _W_02	Uczestnik studiów podyplomowych wskazuje różnice pomiędzy ryzykiem inherentnym a ryzykiem rezydualnym, wymienia normy ISO związane z zarządzaniem ryzykiem oraz wymienia kryteria wymagane podczas procesu zarządzania ryzykiem

IODRZU _W _03	Uczestnik studiów podyplomowych wskazuje normy ISACA powiązane z obszarem ryzyka, wskaże i wiąże przykładowe zasoby z podatnościami i możliwymi ryzykami oraz przedstawia możliwe ścieżki w planie postępowania z ryzykiem
Umiejętności - potrafi	
IODRZU _U _04	Uczestnik studiów podyplomowych potrafi wyznaczyć ryzyko w obszarze danych osobowych, ocenia ryzyko w projekcie, organizacji, w obszarze bezpieczeństwa oraz ocenia ryzyko w oparciu o analizę utraty poufności, integralności i dostępności.
IODRZU _U _05	Uczestnik studiów podyplomowych weryfikuje proces zarządzania ryzykiem w organizacji, projekcie, obszarze bezpieczeństwa, samodzielnie tworzy macierz oceny ryzyka oraz ocenia krytyczność aplikacji przetwarzającej dane osobowe w oparciu o analizę utraty poufności, integralności i dostępności oraz przypisze adekwatne mechanizmy bezpieczeństwa
Kompetencji społecznych - jest gotów do	
IODRZU _K_ 06	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki
IODRZU _K_ 07	Uczestnik studiów podyplomowych ma świadomość znaczenia komunikacji w procesie podejmowania decyzji i rozstrzygania sporów.

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
wykład		
TP-01	Zasady prowadzenia i weryfikacji podstawowych rejestrów.	wykład
TP-02	Działania nadzorcze i kontrolne związane z udostępnianiem i powierzaniem danych osobowych	wykład
TP-03	Działania doradcze IOD w obszarze zamówień publicznych oraz zasad weryfikacji podmiotu przetwarzającego.	wykład
ćwiczenia		
TP-04	Weryfikacja procesu rekrutacyjnego oraz procesów związanych z zatrudnieniem	ćwiczenia
TP-05	Prawne aspekty stosowania monitoringu	ćwiczenia
TP-06	Zagrożenia związane z przetwarzaniem danych osobowych w organizacji i rola IOD w tym zakresie.	ćwiczenia

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #

IODRZU _W_01 IODRZU _W_02 IODRZU _W_03 IODRZU _U _04 IODRZU _U _05 IODRZU _K_ 06 IODRZU _K_ 07	Zaliczenie na ocenę
# np. egzamin, zaliczenie	

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Projektowanie i kontrola obszaru bezpieczeństwa fizycznego i środowiskowego (PKOBFŚ)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: II	Liczba punktów ECTS przypisana zajęciom:	ECTS: 2

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**10**
Ćwiczenia:		Ćwiczenia:	**10**
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**20**

II. INFORMACJE SZCZEGÓŁOWE	
UWAGA: Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
PKOBFŚ_W_01	Uczestnik studiów podyplomowych zna podstawowe zapisy Ustawy o ochronie osób i mienia
Umiejętności - potrafi	
PKOBFŚ _U _02	Uczestnik studiów podyplomowych potrafi określić zagrożenia dla bezpieczeństwa, w zależności od uwarunkowań geograficznych, instytucjonalnych, obiektowych
Kompetencji społecznych - jest gotów do	
PKOBFŚ _K_ 03	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
	wykład	
TP-01	Ustawa o ochronie osób i mienia	wykład
TP-02	Pracownicy ochrony, ochrona wewnętrzna, SUFO, koncesjonowane podmioty realizujące usługi z zakresu bezpieczeństwa	wykład
TP-03	Zagrożenia dla bezpieczeństwa, w zależności od uwarunkowań geograficznych, instytucjonalnych, obiektowych	wykład
TP-04	Plany a instrukcje ochrony obiektów. Ochrona mienia i osób, pracownik kwalifikowany, ustawa o broni i amunicji.. Ochrona osobista i VIP	wykład
TP-05	Agencje detektywistyczne w służbie biznesu. Konwoje i inkaso. Cash processing we współczesnej firmie	wykład
	ćwiczenia	
TP-06	Technika w służbie bezpieczeństwa: SSWiN, CCTV, KD, RCP, inteligentne budynki	ćwiczenia
TP-07	Współczesne systemy zarządzania i kontroli w logistyce (RFID) oraz nadzór nad personelem	ćwiczenia
TP-08	Bezpieczeństwo pożarowe i BHP	ćwiczenia
TP-09	Archiwizacja i bezpieczeństwo dokumentów fizycznych	ćwiczenia
TP-10	Zasady postępowania w sytuacjach kryzysowych, napad, włamanie, pożar, podłożenie ładunku wybuchowego, z pierwszej pomocy przedmedycznej	ćwiczenia
TP-11	Organizacja kancelarii tajnych i procesu kontroli informacji niejawnych	ćwiczenia

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
PKOBFŚ_W_01 PKOBFŚ _U _02 PKOBFŚ _K_ 03	Zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: System zarządzania bezpieczeństwem informacji zgodny z wymogami ISO/IEC 27001:2013 (SZBI)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: II	Liczba punktów ECTS przypisana zajęciom:	ECTS: 3

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**30**
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**30**

II. INFORMACJE SZCZEGÓŁOWE	
cele zajęć: przygotowanie uczestnik studiów podyplomowych do certyfikacji Systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami ISO/IEC 27001:2013 **UWAGA:** Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
SZBI_W_01	Uczestnik studiów podyplomowych zna normy i standardy w zakresie bezpieczeństwa informacji
SZBI _W _02	Uczestnik studiów podyplomowych zna zasady zarządzania bezpieczeństwem informacji w oparciu o normę ISO/IEC 27001:2013
Umiejętności - potrafi	
SZBI _U_03	Uczestnik studiów podyplomowych posiada umiejętność opracowania regulacji i procedur bezpieczeństwa. Planuje i realizuje kontrolę systemu bezpieczeństwa informacyjnego przedsiębiorstwa zgodnie z międzynarodowymi standardami oraz audyt systemów i infrastruktury teleinformatycznej, potrafi być elastyczny i kreatywny skutecznie planując zamierzenia i projekty

Kompetencji społecznych - jest gotów do	
SZBI _K_04	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
wykład		
TP-01	Struktura i podstawy ISMS	wykład
TP-02	Organizacja bezpieczeństwa	wykład
TP-03	Bezpieczeństwo zasobów ludzkich	wykład
TP-04	Zarządzanie aktywami	wykład
TP-05	Kontrola dostępu	wykład
TP-06	Kryptografia	wykład
TP-07	Bezpieczeństwo fizyczne oraz środowiskowe	wykład
TP-08	Bezpieczna eksploatacja. Zarządzanie sieciami i systemami informatycznymi	wykład
TP-09	Bezpieczeństwo komunikacji	wykład
TP-10	Pozyskiwanie, rozwój oraz utrzymanie systemów	wykład
TP-11	Relacje z dostawcami	wykład
TP-12	Zarządzanie incydentami	wykład
TP-13	Aspekty bezpieczeństwa w zarządzaniu ciągłością działania	wykład
TP-14	Zgodność z przepisami prawa i standardami	wykład

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
SZBI _W_01 SZBI _W _02 SZBI _U_03 SZBI _K_04	Egzamin na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Audyt infrastruktury teleinformatycznej (AIT)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: II	Liczba punktów ECTS przypisana zajęciom:	ECTS: 2

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**10**
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**10**

II. INFORMACJE SZCZEGÓŁOWE	
Cele zajęć: przygotowanie uczestnik studiów podyplomowych do prowadzenia audytu infrastruktury teleinformatycznej **UWAGA:** Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
AIT_W_01	Uczestnik studiów podyplomowych zna normy i standardy wykorzystywane w audycie wewnętrznym i kontroli wewnętrznej
AIT _W _02	Uczestnik studiów podyplomowych zna i omawia zadania audytora wewnętrznego w systemie zarządzania bezpieczeństwem informacji
Umiejętności - potrafi	
AIT _U_03	Uczestnik studiów podyplomowych potrafi omówić powszechnie znane techniki planowania i realizacji audytu wewnętrznego i kontroli wewnętrznej oraz wymagania dla sprawozdawczości
Kompetencji społecznych - jest gotów do	

AIT _K_04	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
wykład		
TP-01	Techniki przeprowadzania audytu infrastruktury informatycznej	wykład
TP-02	Podejście do mobilności i przetwarzania danych w chmurach obliczeniowych	wykład
TP-03	Techniki kontroli warstwy sieciowej, systemowej i aplikacyjnej	wykład
TP-04	Tworzenie audytowych list kontrolnych: case study	wykład
TP-05	Najczęściej występujące niezgodności i problemy identyfikowane w trakcie audytów	wykład

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
SZBI _W_01 SZBI _W _02 SZBI _U_03 SZBI _K_04	zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Wykrywanie i zapobieganie oszustwom i nadużyciom skutkującym wyciekiem danych osobowych (WZON)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: II	Liczba punktów ECTS przypisana zajęciom:	ECTS: 2

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	**10**
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**10**

II. INFORMACJE SZCZEGÓŁOWE	
Cele zajęć umiejętność zidentyfikowania procesów i zachowań prowadzących do nadużyć komputerowych oraz pozwalających na podejmowanie strategicznych decyzji w takich obszarach jak: przewidywanie zachowania pracowników, przeciwdziałanie dalszym wyciekom, zabezpieczenie danych, ciągłość organizacji. Poznanie najczęstszych kanałów wycieku danych, rodzajów śladów wycieku danych. **UWAGA:** Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
WZON_W_01	Uczestnik studiów podyplomowych zna najczęstsze kanały wycieku danych, rodzaje śladów wycieku danych.
Umiejętności - potrafi	
WZON _U_02	Uczestnik studiów podyplomowych potrafi zlokalizować punkty krytyczne w działaniu systemów informatycznych
WZON _U_03	Uczestnik studiów podyplomowych potrafi ustalić kanały wycieku danych, oraz ustalić techniczne metody zapobiegające wyciekom danych
WZON _U_04	Uczestnik studiów podyplomowych potrafi zabezpieczyć ślady wycieku w sposób pozwalający na wykorzystanie materiału w celach dowodowych.

Kompetencji społecznych - jest gotów do	
WZON_K_05	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
Laboratorium		
TP-01	Metody analizy podatności i luk w oprogramowaniu.	Laboratorium
TP-02	Zabezpieczania systemów i struktur IT.	Laboratorium
TP-03	Bezpieczeństwo sieci bezprzewodowych.	Laboratorium
TP-04	Zarządzanie backupem.	Laboratorium
TP-05	Niszczenie i odzyskiwanie danych.	Laboratorium
TP-06	Analiza materiału dowodowego.	Laboratorium

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
WZON_W_01 WZON_U_02 WZON_U_03 WZON_U_04 WZON_K_05	zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Ochrona organizacji przed wyciekiem danych osobowych (OOWDO)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: II	Liczba punktów ECTS przypisana zajęciom:	ECTS: 2

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	**10**
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**10**

II. INFORMACJE SZCZEGÓŁOWE	
Cele zajęć: poznanie sposobów ochrony organizacji przed wyciekiem danych osobowych **UWAGA:** Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
OOWDO_W_01	Uczestnik studiów podyplomowych zna sposoby ochrony organizacji przed wyciekiem danych osobowych
Umiejętności - potrafi	
OOWDO _U_02	Uczestnik studiów podyplomowych potrafi samodzielnie opracować i wdrożyć procedury i procesy minimalizujące wycieki danych
OOWDO _U_03	Uczestnik studiów podyplomowych potrafi zdefiniować i wskazać kierunki zabezpieczenia organizacji przed wyciekiem danych z wykorzystaniem znaczników DLP (Data Leakage Prevention/Prevention)
Kompetencji społecznych - jest gotów do	

OOWDO _K_04	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
Laboratorium		
TP-01	Wdrażanie i możliwości administracyjne systemów klasy DLP (Data Leakage Prevention/Prevention)	Laboratorium

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
OOWDO _W_01 OOWDO _U_02 OOWDO _U_03 OOWDO _K_04	zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Kontynuacja działalności po awarii. Zarządzanie ciągłością działania. (KDZCD)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: II	Liczba punktów ECTS przypisana zajęciom:	ECTS: 1

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**10**
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**10**

II. INFORMACJE SZCZEGÓŁOWE	
Cele zajęć: poznanie sposobów postępowania po awarii; poznanie sposobów odtwarzania techniki teleinformatycznej po katastrofie **UWAGA:** Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
KDZCD_W_01	Uczestnik studiów podyplomowych zna sposoby postępowania po awarii oraz sposoby odtwarzania techniki teleinformatycznej po katastrofie
Umiejętności - potrafi	
KDZCD_U_02	Uczestnik studiów podyplomowych potrafi opracować plan awaryjny
KDZCD_U_03	Uczestnik studiów podyplomowych potrafi określić sposoby postępowania po awarii
Kompetencji społecznych - jest gotów do	
KDZCD_K_04	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!
Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
	wykład	
TP-01	Role i odpowiedzialności.	**wykład**
TP-02	Plany awaryjne.	**wykład**
TP-03	Plany przywracania systemów po awarii	**wykład**
TP-04	Testowanie planów awaryjnych	**wykład**
TP-05	Odtwarzanie techniki teleinformatycznej po katastrofie	**wykład**

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
KDZCD_W_01 KDZCD_U_02 KDZCD_U_03 KDZCD_K_04	zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Zarządzanie kryzysowe. Krajowy system cyberbezpieczeństwa (ZKKSC)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: II	Liczba punktów ECTS przypisana zajęciom:	ECTS: 2

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**10**
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**10**

II. INFORMACJE SZCZEGÓŁOWE	
Cele zajęć: poznanie obowiązków operatorów usług kluczowych i dostawców usług cyfrowych. Poznanie organizacji systemu zarządzania cyberbezpieczeństwem **UWAGA:** Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
KDZCD_W_01	Uczestnik studiów podyplomowych zna działania lokalnych komórek CSIRT
KDZCD_W_02	Uczestnik studiów podyplomowych zna organizację systemu zarządzania ceberbezpieczeństwem
Umiejętności - potrafi	
KDZCD_U_03	Uczestnik studiów podyplomowych potrafi określić obowiązki operatorów usług kluczowych i dostawców usług cyfrowych.
Kompetencji społecznych - jest gotów do	
KDZCD_K_04	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!
Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
	wykład	
TP-01	Działania w czasie kryzysu.	**wykład**
TP-02	Działania lokalnych komórek CSIRT	**wykład**
TP-03	Obowiązki operatorów usług kluczowych i dostawców usług cyfrowych	**wykład**
TP-04	Organizacja systemu zarządzania cyberbezpieczeństwem	**wykład**
TP-05	Architektura cyberbezpieczeństwa - określenie i powołanie struktur wewnętrznych	**wykład**
TP-06	Współpraca z sektorowymi zespołami cyberbezpieczeństwa	**wykład**

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
ZKKSC_W_01 ZKKSC_W_02 KDZCD_U_03 KDZCD_K_04	zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Bezpieczeństwo prawne – rozszerzone podejście (BP)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: II	Liczba punktów ECTS przypisana zajęciom:	ECTS: 1

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	**10**
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**10**

II. INFORMACJE SZCZEGÓŁOWE	
Cele zajęć: poznanie przestępstw przeciwko ochronie informacji. Znajomość odpowiedzialności z tytułu naruszania przepisów ODO **UWAGA:** Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.	
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
BP_W_01	Uczestnik studiów podyplomowych zna przestępstwa przeciwko ochronie informacji
BP_W_02	Uczestnik studiów podyplomowych zna odpowiedzialność z tytułu naruszenia przepisów ODO
Umiejętności - potrafi	
BP_U_03	Uczestnik studiów podyplomowych potrafi wykorzystać dowód elektroniczny na potrzeby postępowania sądowego w postępowaniach karnych oraz postępowaniach cywilnych.
Kompetencji społecznych - jest gotów do	

BP_K_04	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki

UWAGA!

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
wykład		
TP-01	Kodeks karny	**wykład**
TP-02	Przestępstwa przeciwko ochronie informacji	**wykład**
TP-03	Odpowiedzialność z tytułu naruszenia przepisów ODO	**wykład**
TP-04	Analiza projektów i nowelizacji	**wykład**
TP-05	Prawa autorskie i zasady ochrony własności intelektualnej	**wykład**
TP-06	Dowód elektroniczny na potrzeby postępowania sądowego w postępowaniach karnych oraz postępowaniach cywilnych	**wykład**
TP-07	Tajemnica przedsiębiorstwa i inne tajemnice prawnie chronione	**wykład**

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
BP_W_01 BP_W_02 BP_U_03 BP_K_04	zaliczenie na ocenę

np. egzamin, zaliczenie

Uproszczona karta opisu zajęć - Sylabus

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu

I. INFORMACJE OGÓLNE			
Nazwa zajęć: Seminarium dyplomowe (projektowe) (SD)			
Nazwa kierunku studiów, poziom i profil kształcenia:		Inspektor Ochrony Danych, studia podyplomowe	
Język wykładowy:	Język polski		
Rok studiów: I	Semestr: II	Liczba punktów ECTS przypisana zajęciom:	ECTS: 2

FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach stacjonarnych i niestacjonarnych z podziałem na formy:			
Studia stacjonarne		**Studia niestacjonarne**	
Wykład:		Wykład:	
Ćwiczenia:		Ćwiczenia:	
Laboratorium:		Laboratorium:	
Lektorat:		Lektorat:	
Projekt:		Projekt:	
Zajęcia praktyczne:		Zajęcia praktyczne:	
Seminarium:		Seminarium:	**10**
Zajęcia terenowe:		Zajęcia terenowe:	
Praktyki:		Praktyki:	
Inna forma (jaka):		Inna forma (jaka):	
RAZEM:		**RAZEM:**	**10**

II. INFORMACJE SZCZEGÓŁOWE

Cele zajęć: zapoznanie uczestników studiów podyplomowych z zasadami przygotowania pracy końcowej (zasady korzystania z literatury i cytowania jej) oraz nabycie umiejętności prezentowania wybranej tematyki z zakresu ochrony danych osobowych.

UWAGA:

Dzielimy efekty uczenia się przypisane do zajęć na kategorie wiedzy, umiejętności i kompetencji społecznych. Przypisane do zajęć efekty uczenia się nie muszą obejmować wszystkich trzech kategorii.

Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:
Wiedzy - zna i rozumie	
SD_W_01	Uczestnik studiów podyplomowych zna zasady przygotowania pracy końcowej.
Umiejętności - potrafi	
SD_U_02	Uczestnik studiów podyplomowych potrafi wykorzystać informacje pochodzące z różnych źródeł oraz stosuje dostępne techniki informatyczne, niezbędne do pozyskiwania, gromadzenia i przetwarzania danych.
SD_U_03	Uczestnik studiów podyplomowych potrafi zaplanować, opracować wybrane zagadnienie związane z ochroną danych osobowych i wyciągnąć wnioski końcowe
SD_U_04	Uczestnik studiów podyplomowych potrafi określić priorytety realizacji określonego zadania, rozumie potrzebę uczenia się przez całe życie.
Kompetencji społecznych - jest gotów do	

SD_K_05	Uczestnik studiów podyplomowych jest świadomy roli i zadań osoby odpowiedzialnej za realizację audytu bezpieczeństwa informacji i systemów informatycznych oraz wszelkich procedur, stosowanych dla usprawnienia funkcjonowania organizacji, zgodnie z prawem i zasadami etyki
SD_K_06	Uczestnik studiów podyplomowych ma świadomość znaczenia komunikacji w procesie podejmowania decyzji i rozstrzygania sporów.

UWAGA!
Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 3-7, ale są to wartości umowne w zależności od ogólnej liczby godzin zajęć.

Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):

Symbol treści programowych	Opis treści programowych	Forma zajęć
seminarium		
TP-01	Wymagania formalne i techniczne dotyczące redakcji pracy dyplomowej (korzystanie z literatury, umiejętność cytowania literatury, metody opracowania wyników lub danych źródłowych, kształcenie umiejętności ich przedstawiania, posługiwanie się specjalistycznym, fachowym językiem)	**seminarium**
TP-02	Podstawowe zasady i przykładowe sposoby prezentacji opracowania z zakresu studiowanego kierunku	**seminarium**
TP-03	Podstawowe zasady prowadzenia prezentacji w tym: postawa, emisja głosu, kontakt z odbiorcą, podstawowe zasady graficznego opracowania prezentacji multimedialnej	**seminarium**
TP-04	Multimedialna prezentacja wybranego przez słuchacza zagadnienia, związanego z jego pracą końcową oraz dyskusja na temat przedstawionych prezentacji.	**seminarium**

III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć do metod weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć

Symbol efektu uczenia się przypisanego do zajęć	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
SD_W_01 SD_U_02 SD_U_03 SD_U_04 SD_K_05 SD_K_06	zaliczenie na ocenę

np. egzamin, zaliczenie