

## PROGRAM STUDIÓW PODYPLOMOWYCH

### 1. Informacje o studiach

<b>Nazwa studiów podyplomowych:</b>  CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI
<b>Przyporządkowanie do dyscypliny naukowej lub dyscyplin naukowych. W przypadku przyporządkowania do więcej niż jednej dyscypliny należy wskazać dyscyplinę wiodącą:</b> <ul style="list-style-type: none"><li>▪ nauki o bezpieczeństwie 17%</li><li>▪ nauki prawne 23%</li><li>▪ informatyka techniczna i telekomunikacja 60% (<i>dyscyplina wiodąca</i>)</li></ul>
<b>Czas trwania studiów:</b> Dwa semestry
<b>Język wykładowy:</b> Język polski
<b>Poziom umożliwiający uzyskanie kwalifikacji częściowych (6, 7 albo 8 PRK):</b> Poziom 6 PRK
<b>Szczegółowe warunki rekrutacji na studia podyplomowe:</b>  <b>Adresaci i główne założenia studiów podyplomowych:</b> Studia podyplomowe kierowane są zarówno do osób wykonujących pośrednio lub bezpośrednio zadania związane z zarządzaniem i administrowaniem bezpieczeństwa systemów komputerowych oraz ochrony informacji, jak i poszukujących zatrudnienia na stanowiskach w powyższym obszarze, w szczególności w urzędach administracji rządowej i samorządowej oraz jednostkach im podległych, a także w służbach mundurowych. Zakres merytoryczny oraz sposób prezentacji treści umożliwi pozyskanie wiedzy i nabycie umiejętności pozwalających na efektywniejsze wykonywanie obowiązków służbowych związanych m.in. z opracowywaniem polityk bezpieczeństwa, ich wdrażania, utrzymania oraz rozwoju. Zakłada się przy tym, że kandydat nie posiada stopnia zawodowego informatyka, jednakże dysponuje w tym zakresie odpowiednimi predyspozycjami i pewnym doświadczeniem. W ramach programu uczestnicy analizują studia przypadków związane z przestępczością komputerową (symulacje ataków na żywo), poznają również możliwości technologiczne wspomagające bezpieczeństwo informatyczne firm i instytucji. Absolwenci studiów podyplomowych z zakresu <i>cyberbezpieczeństwa i ochrony informacji</i> są przygotowani do certyfikowanych egzaminów z zakresu E-URZĘDNIK oraz IT SECURITY. Egzaminy te zostaną przeprowadzone w PWSTE w Jarosławiu dla chętnych osób bezpośrednio po zakończonych studiach.

**Zasady rekrutacji:**

Postępowanie kwalifikacyjne na studia podyplomowe przeprowadza Komisja Rekrutacyjna powołana przez Rektora PWSTE w Jarosławiu. Postępowanie kwalifikacyjne odbywa się przy użyciu systemu USOS oraz poprzez złożenie wymaganych dokumentów. Rekrutacja odbywa się na zasadzie kolejności zgłoszeń. W przypadku zgłoszenia się liczby kandydatów przekraczającej limit miejsc o przyjęciu na studia podyplomowe decyduje termin zgłoszenia. Kierownik studiów podyplomowych wraz z Komisją Rekrutacyjną określa zasady postępowania kwalifikacyjnego, w tym szczegółowe terminy, wymagane dokumenty oraz warunki przyjęcia. Warunkiem uruchomienia studiów z zakresu *cyberbezpieczeństwa i ochrony informacji* jest zebranie grupy liczącej min. 15 osób.

**Wymagania:**

Studia podyplomowe z zakresu *cyberbezpieczeństwa i ochrony informacji* przeznaczone są dla osób legitymujących się dyplomem ukończenia studiów wyższych (pierwszego lub drugiego stopnia lub jednolitych studiów magisterskich). Przyjęcie na studia warunkuje: złożenie kompletu dokumentów oraz decyzja Komisji Rekrutacyjnej. Wymagane dokumenty:

- kwestionariusz osobowy kandydata na studia (generowany w systemie Internetowej Rejestracji Kandydatów - IRK)
- odpis dyplomu ukończenia studiów lub uwierzytelniona kserokopia ukończonych studiów wyższych
- kserokopia dowodu osobistego,
- dowód wpłaty wpisowej
- jedno zdjęcie

**Miejsce składania dokumentów:**

Dział Obsługi Studentów (DOS), bud. J-2  
Państwowa Wyższa Szkoła Techniczno-Ekonomiczna  
ul. Czarnieckiego 16  
37-500 Jarosław

**Oplaty:**

Uczestnik studiów podyplomowych ponosi opłaty za świadczone usługi edukacyjne związane z prowadzeniem studiów podyplomowych na zasadach określonych w przepisach obowiązujących w PWSTE w Jarosławiu. Uczestnik zakwalifikowany na studia podyplomowe wnosi opłatę za każdy semestr w terminie 14 dni od daty rozpoczęcia semestru. Nieuiszczenie w terminie opłat za świadczone usługi edukacyjne może stanowić podstawę do skreślenia z listy studiów podyplomowych

**Liczba osób przyjętych, która pozwala na uruchomienie studiów:** 15 osób

**Warunki ukończenia studiów podyplomowych:**

Warunkiem ukończenia studiów podyplomowych jest osiągnięcie efektów uczenia się założonych w programie studiów, aktywne i systematyczne uczestnictwo w zajęciach, złożenie wszystkich egzaminów i uzyskanie zaliczeń z zajęć, uzyskanie co najmniej 30 punktów ECTS oraz przystąpienie i uzyskanie pozytywnej oceny z egzaminu końcowego.

Szczegółowe warunki i zasady przeprowadzania egzaminu końcowego, jego oceniania oraz sposób obliczania ostatecznego wyniku studiów podyplomowych

określa Regulamin studiów podyplomowych w PWSTE w Jarosławiu. Absolwent studiów podyplomowych otrzymuje świadectwo ukończenia studiów podyplomowych w zakresie cyberbezpieczeństwa i ochrony informacji niejawnych. Program studiów zapewnia przygotowanie do certyfikowanych egzaminów z zakresie E-URZĘDNIK, IT SECURITY i zdobycie przez absolwentów dodatkowych kwalifikacji.

**Przewidywany termin rozpoczęcia zajęć:** 1 października 2021 r.

**Propozycja sal dydaktycznych niezbędnych do realizacji programu studiów:**

Dwie sale wykładowe w Instytucie Inżynierii Technicznej, wyposażone w rzutnik multimedialny i komputer, trzy sale informatyczne ze stanowiskami komputerowym, wyposażone w rzutnik multimedialny, w tym jedna sala, która zostanie dostosowana przez ekspertów Exatel S.A. w zakresie niezbędnego oprogramowania do prowadzenia specjalistycznych zajęć w ramach studiów podyplomowych.

## 2. 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 opisu – aspekty o podstawowym znaczeniu	Kod składnika opisu – charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 7 PRK	Sposób weryfikacji efektów uczenia się
<b>WIEDZA</b>						
1.	E_W01 NP-1	<p>Student zna i rozumie uporządkowaną wiedzę o normach i zasadach prawnych w zakresie ochrony własności przemysłowej i prawa autorskiego oraz ochrony informacji mających wpływ na bezpieczeństwo państwa (w tym cyberbezpieczeństwa).</p> <p><i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i></p> <p><b>Koncepcje i uregulowania prawne w zakresie cyberbezpieczeństwa (2), Udostępnianie informacji publicznej (2), Ochrona informacji niejawnych (3)</b></p>	P6U_W	Kontekst – uwarunkowania, skutki	P6S_WK	<p><i>Egzamin pisemny, praca zaliczeniowa,</i></p> <p><i>Zaliczenie z oceną (ustne), Zaliczenie z oceną - praca zaliczeniowa,</i></p> <p><i>Egzamin pisemny, Zaliczenie z oceną - praca zaliczeniowa</i></p>
2.	E_W02	Student ma wiedzę w zakresie sieci komputerowych, typowych usług sieciowych, zasad udostępniania zasobów sieciowych, systemów i sieci komputerowych (podstawowe metody, techniki, narzędzia stosowane	P6U_W	Zakres i głębia – kompletność perspektywy poznawczej i zależności	P6S_WG	<p><i>Egzamin pisemny, Zaliczenie z oceną - zadania cząstkowe,</i></p>

	NI-1	<p>przy korzystaniu z sieci Internet, podstawowe portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji )</p> <p><i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i></p> <p>Pozyskiwanie i weryfikacja danych z Internetu (4), Zarządzanie usługami sieciowymi w kontekście bezpieczeństwa (3)</p>		Kontekst – uwarunkowania skutki	P6S_WK	<i>Pisemne kolokwium zaliczeniowe, krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych, weryfikacja poprawności realizacji ćwiczenia</i>
3.	E_W03  NI-1	<p>Student ma wiedzę w zakresie podstaw cyklu życia i trendach rozwojowych systemów informatycznych sprzętowych lub programowych</p> <p><i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i></p> <p>Podstawy technologii sieci i intersieci (3)</p>	P6U_W	<p>Zakres i głębia – kompletność perspektywy poznawczej i zależności</p> <p>Kontekst – uwarunkowania skutki</p>	P6S_WG  P6S_WK	<i>Egzamin pisemny, Zaliczenie z oceną - krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych, weryfikacja poprawności realizacji ćwiczenia</i>
	E_W04  NI-0,9 NB-0,1	<p>Student zna i rozumie zagadnienia związane z bezpieczeństwem systemów i sieci, podstawowe narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń</p> <p><i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i></p> <p>Bezpieczeństwo systemów teleinformatycznych (3), Incydenty teleinformatyczne (2), Cyberprzestępczość (2), Pozyskiwanie i weryfikacja danych z Internetu (4), Zarządzanie usługami sieciowymi w kontekście bezpieczeństwa (3)</p>	P6U_W	<p>Zakres i głębia – kompletność perspektywy poznawczej i zależności</p> <p>Kontekst – uwarunkowania skutki</p>	P6S_WG  P6S_WK	<p><i>Zaliczenie z oceną – realizacja projektu</i></p> <p><i>Zaliczenie z oceną – realizacja projektu</i></p> <p><i>Zaliczenie z oceną - kolokwium pisemne</i> <i>Zaliczenie z oceną - praca zaliczeniowa</i></p> <p><i>Egzamin pisemny, Zaliczenie z oceną - zadania cząstkowe,</i></p> <p><i>Egzamin - pisemne kolokwium zaliczeniowe, Zaliczenie z oceną - krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych, weryfikacja poprawności realizacji ćwiczenia</i></p>

	E_W05	Student zna i rozumie fakty, teorie, metody z zakresu dyscyplin naukowych powiązanych z działalnością zawodową w zakresie bezpieczeństwa wewnętrznego.	P6U_W	Zakres i głębia – kompletność perspektywy poznawczej i zależności	P06S_WG	Zaliczenie z oceną (ustne), Zaliczenie z oceną (ustne), aktywność podczas zajęć  Zaliczenie z oceną – kolokwium pisemne, Zaliczenie z oceną – zadania cząstkowe
	NB-1	Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:  Psychologiczne aspekty cyberbezpieczeństwa (1), Organizacja i zarządzanie bezpieczeństwem w administracji publicznej (2)				
	E_W06	Student zna i rozumie zagadnienia związane z systemami teleinformatycznymi dla audytorów IT, standardy, metodologie i metodyki prowadzenia audytu, proces audytu (utrzymanie systemów teleinformatycznych, zarządzanie kryzysowe).	P6U_W	Zakres i głębia – kompletność perspektywy poznawczej i zależności	P06S_WG	Egzamin pisemny, Zaliczenie z oceną - projekt
	NI-1	Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:  Audyt informatyczny (3)				
<b>UMIEJĘTNOŚCI</b>						
	E_U01	Student potrafi rozpoznać i przeciwdziałać przestępczości w cyberprzestrzeni. Wskazuje kierunki rozwoju oraz podstawowe uregulowania prawne w zakresie cyberbezpieczeństwa.	P6U_U	Wykorzystanie wiedzy – rozwiązywane problemy i wykonywane zadania	P6S_UW	Egzamin pisemny, praca zaliczeniowa,  Zaliczenie z oceną - kolokwium pisemne Zaliczenie z oceną - praca zaliczeniowa
	NB-0,5 NP-0,5	Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:  Koncepcje i uregulowania prawne w zakresie cyberbezpieczeństwa (2), Cyberprzestępczość (2)				
	E_U02	Potrafi wykorzystać podstawowe narzędzia i techniki do rozpoznawania zagrożeń, zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów, obsługiwać incydenty bezpieczeństwa w oparciu o systemy teleinformatyczne oraz sporządzać raporty.	P6U_U	Wykorzystanie wiedzy – rozwiązywane problemy i wykonywane zadania	P6S_UW	Zaliczenie z oceną – realizacja projektu  Zaliczenie z oceną – realizacja projektu
	NI-1	Nazwa zajęć, na których będzie realizowany efekt oraz				

		<p><i>liczba punktów ECTS przypisana do zajęć:</i></p> <p><b>Bezpieczeństwo systemów teleinformatycznych (3), Incydenty teleinformatyczne (2)</b></p>				
E_U03	NI-1	<p>Student potrafi tworzyć program audytu oraz dokonać oceny ryzyka i bezpieczeństwa baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe.</p> <p><i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i></p> <p><b>Audyt informatyczny (3)</b></p>	P6U_U	Wykorzystanie wiedzy – rozwiązywane problemy i wykonywane zadania	P6S_UW	<i>Egzamin pisemny, Zaliczenie z oceną - projekt</i>
E_U04	NI-1	<p>Potrafi pozyskiwać dane, a także umiejętnie interpretować otrzymane wyniki. Potrafi użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych.</p> <p><i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i></p> <p><b>Pozyskiwanie i weryfikacja danych z Internetu (4)</b></p>	P6U_U	Wykorzystanie wiedzy – rozwiązywane problemy i wykonywane zadania	P6S_UW	<i>Egzamin pisemny, Zaliczenie z oceną - zadania cząstkowe,</i>
E_U05	NI-1	<p>Student potrafi zaprojektować i skonfigurować prostą sieć, potrafi nią administrować, konfigurować, zabezpieczać i udostępniać podstawowe usługi sieciowe, wykrywać i rozwiązywać problemy pojawiające się w sieci.</p> <p><i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i></p> <p><b>Zarządzanie usługami sieciowymi w kontekście bezpieczeństwa (3)</b></p>	P6U_U	Wykorzystanie wiedzy – rozwiązywane problemy i wykonywane zadania	P6S_UW	<i>Pisemne kolokwium zaliczeniowe, krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych, weryfikacja poprawności realizacji ćwiczenia</i>
E_U06	NB-1	<p>Student potrafi wykorzystywać posiadaną wiedzę interdyscyplinarną do podejmowania decyzji, kierowania procesami, zarządzania zasobami oraz formułowania i rozwiązywania praktycznych problemów</p> <p><i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i></p> <p><b>Psychologiczne aspekty cyberbezpieczeństwa (1), Or-</b></p>	P6U_U	Wykorzystanie wiedzy – rozwiązywane problemy i wykonywane zadania	P6S_UW	<p><i>Zaliczenie z oceną (ustne), Zaliczenie z oceną (ustne), aktywność podczas zajęć</i></p> <p><i>Zaliczenie z oceną – kolokwium pisemne, Zaliczenie z oceną – zadania cząstkowe</i></p>

		ganizacja i zarządzanie bezpieczeństwem w administracji publicznej (2)				
E_U07 NI-1	Potrafi na poziomie podstawowym administrować systemami komputerowymi, potrafi sformułować specyfikację prostych systemów informatycznych w odniesieniu do sprzętu, oprogramowania systemowego i cech funkcjonalnych aplikacji.  <i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i>  Podstawy technologii sieci i intersieci (3)	P6U_U	Wykorzystanie wiedzy – rozwiązywane problemy i wykonywane zadania	P6S_UW	<i>Egzamin pisemny, Zaliczenie z oceną - krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych, weryfikacja poprawności realizacji ćwiczenia</i>	
E_U08 NP-1	Student potrafi wskazać zasady i uregulowania prawne w zakresie udostępniania informacji publicznej, dokonać klasyfikacji informacji niejawnych oraz wskazać ich klauzule tajności, sposoby ochrony informacji stanowiących tajemnicę państwową, zasady postępowania w sytuacjach zagrożenia dla informacji niejawnych lub w przypadku ich ujawnienia.  <i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i>  Ochrona informacji niejawnych (3), Udostępnianie informacji publicznej (2)	P6U_U	Wykorzystanie wiedzy – rozwiązywane problemy i wykonywane zadania	P6S_UW	<i>Egzamin pisemny, Zaliczenie z oceną - praca zaliczeniowa</i>  <i>Zaliczenie z oceną (ustne), Zaliczenie z oceną - praca zaliczeniowa,</i>	
<b>KOMPETENCJE SPOŁECZNE</b>						
E_K01 NP-0,5 NI-0,5	Student jest świadomy potrzeby uzupełniania i doskonalenia nabytej wiedzy i umiejętności, ich krytycznej oceny i konieczności korzystania z opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu  <i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i>  Udostępnianie informacji publicznej (2), Ochrona informacji niejawnych (3), Podstawy technologii sieci i intersieci (3), Incydenty teleinformatyczne (2)	P6U_K	Oceny – krytyczne podejście	P6S_KK	<i>Zaliczenie z oceną (ustne), Zaliczenie z oceną - praca zaliczeniowa,</i>  <i>Egzamin pisemny, Zaliczenie z oceną - praca zaliczeniowa</i>  <i>Egzamin pisemny, Zaliczenie z oceną - krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych,</i>	

						<p>weryfikacja poprawności realizacji ćwiczenia</p> <p>Zaliczenie z oceną – realizacja projektu</p>
E_K02	<p>Student jest świadomy odpowiedzialności powierzanych mu zadań zawodowych w zakresie bezpieczeństwa wewnętrznego oraz konieczności ustalania priorytetów w ich realizacji i dbałości o dorobek i tradycje zawodu.</p> <p><i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i></p> <p>Koncepcje i uregulowania prawne w zakresie cyberbezpieczeństwa (2), Udostępnianie informacji publicznej (2), Ochrona informacji niejawnych (3), Zarządzanie usługami sieciowymi w kontekście bezpieczeństwa (3)</p>	P6U_K	<p>Odpowiedzialność – wypełnianie zobowiązań społecznych i działanie na rzecz interesu publicznego</p>	P6S_KO	<p>Egzamin pisemny, praca zaliczeniowa,</p> <p>Zaliczenie z oceną (ustne), Zaliczenie z oceną - praca zaliczeniowa,</p> <p>Egzamin pisemny, Zaliczenie z oceną - praca zaliczeniowa</p>	
E_K03	<p>Student jest gotów do rozstrzygania dylematów związanych z wykonywaniem zawodu, zgodnie z podstawowymi zasadami etyki i normami moralnymi.</p> <p><i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i></p> <p>Organizacja i zarządzanie bezpieczeństwem w administracji publicznej (2), Audyt informatyczny (3), Bezpieczeństwo systemów teleinformatycznych (3), Cyberprzestępczość (2), Koncepcje i uregulowania prawne w zakresie cyberbezpieczeństwa (2)</p>	P6U_K	<p>Rola zawodowa – niezależność i rozwój etosu</p>	P6S_KR	<p>Zaliczenie z oceną – kolokwium pisemne, Zaliczenie z oceną – zadania cząstkowe</p> <p>Egzamin pisemny, Zaliczenie z oceną – projekt</p> <p>Zaliczenie z oceną – realizacja projektu</p> <p>Zaliczenie z oceną - kolokwium pisemne Zaliczenie z oceną - praca zaliczeniowa</p> <p>Egzamin pisemny, praca zaliczeniowa,</p>	
E_K04	<p>Student jest świadomy konieczności podejmowania działań na rzecz interesu publicznego, konieczności myślenia i działania w sposób przedsiębiorczy.</p>	P6U_K	<p>Odpowiedzialność – wypełnianie zobowiązań spo-</p>	P6S_KO	<p>Egzamin pisemny, praca zaliczeniowa,</p>	



NB-0,1 NI-0,6 NP-0,3	<i>Nazwa zajęć, na których będzie realizowany efekt oraz liczba punktów ECTS przypisana do zajęć:</i>  Koncepcje i uregulowania prawne w zakresie cyberbezpieczeństwa (2), Psychologiczne aspekty cyberbezpieczeństwa (1), Pozyskiwanie i weryfikacja danych z Internetu (4)		łącznych i działanie na rzecz interesu publicznego		<i>Zaliczenie z oceną (ustne), Zaliczenie z oceną (ustne), aktywność podczas zajęć</i>  <i>Egzamin pisemny, Zaliczenie z oceną - zadania cząstkowe,</i>
----------------------------	--	--	--	--	---

### 3. Harmonogram realizacji programu studiów podyplomowych

Lp.	Nazwa zajęć	wykład (liczba godzin)	ćwiczenia (liczba godzin)	laboratorium (liczba godzin)	Forma zaliczenia	Punkty ECTS
Rok I - semestr 1						
1	Koncepcje i uregulowania prawne w zakresie cyberbezpieczeństwa	20	5	-	E	2
2	Udostępnianie informacji publicznej	15	10	-	ZO	2
3	Ochrona informacji niejawnych	15	15	-	E	3
4	Cyberprzestępczość	10	15	-	ZO	2
5	Podstawy technologii sieci i intersieci	15	-	15	E	3
6	Organizacja i zarządzanie w administracji publicznej w kontekście bezpieczeństwa jednostki	10	10	-	ZO	2
Razem semestr 1		85	55	15		14
Rok I - semestr 2						
1	Psychologiczne aspekty cyberbezpieczeństwa	10	5	-	ZO	1

2	Pozyskiwanie i weryfikacja danych z Internetu	15	-	30	E	4
3	Zarządzanie usługami sieciowymi w kontekście bezpieczeństwa	15	-	15	E	3
4	Audyt informatyczny	15	15	-	E	3
5	Bezpieczeństwo systemów teleinformatycznych	-	10	15	ZO	3
6	Incydenty teleinformatyczne	-	10	5	ZO	2
Razem semestr 2		55	40	65		16
Łącznie rok I	315	140	95	80		30

dyscypliny naukowe:

nauki o bezpieczeństwie

nauki prawne

informatyka

#### 4. Obowiązująca literatura

Literatura została ujęta w kartach zajęć (sylabusach)

# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Koncepcje i uregulowania prawne w zakresie cyberbezpieczeństwa</b>			
Nazwa studiów podyplomowych		CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI	
Język wykładowy: polski			
Rok studiów: I	Semestr: 1	Liczba punktów ECTS przypisana zajęciom: 2	Data aktualizacji sylabusu: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:			
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	20		
Ćwiczenia:	5		
Laboratorium:	-		
<b>RAZEM:</b>	<b>25</b>		
II. INFORMACJE SZCZEGÓLNE			
Cel (cele) prowadzenia zajęć: wprowadzenie studenta w obszar cyberbezpieczeństwa w prawie międzynarodowym. Celem wykładu jest przybliżenie studentom regulacji określających prawa i obowiązki oraz zasady odpowiedzialnego postępowania państw, analizie naruszeń bezpieczeństwa informacyjnego systemów komputerowych w świetle konkretnych norm prawa międzynarodowego oraz przypisaniu cyberoperacji (w szczególności działań zorganizowanych grup hakerskich typu APT) państwu.			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu #	
<b>Wiedzy - zna i rozumie</b>			
KiUP_W01	zagadnienia z zakresu prawa międzynarodowego i norm odpowiedzialnego postępowania w cyberprzestrzeni, wpływających na prawa i obowiązki państw na płaszczyźnie międzynarodowej.	E_W01	
KiUP_W02	zagrożenia dla gospodarki oraz systemów politycznych płynących z nieodpowiedzialnego wykorzystania cyberprzestrzeni przez państwa .	E_W01	
<b>Umiejętności - potrafi</b>			
KiUP_U01	analizować międzynarodowe akty prawne oraz normy kluczowe z punktu widzenia cyberbezpieczeństwa oraz implementować wynikające z nich obowiązki.	E_U01	
<b>Kompetencji społecznych - jest gotów do</b>			
KiUP_K01	podjmowania działań na rzecz interesu publicznego	E_K04	
KiUP_K02	odpowiedzialnej realizacji powierzonych zadań	E_K02	
KiUP_K03	rozstrzygania dylematów związanych z wykonywaniem zawodu	E_K03	
* kod zajęć, # efekty uczenia się dla określonego kierunku studiów, poziomu i profilu (np. K_W01, K_U01, ..) W- wiedza, U- umiejętności, K- kompetencje społeczne			

01, 02...- numer efektu uczenia się

**UWAGA!**

Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 4-7, ale są to wartości umowne.

**TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO 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	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>wykład</b>		
TP-01	Państwa jako podmioty prawa międzynarodowego, źródła praw i zobowiązań w prawie międzynarodowym. „Cyber normy” jako nowy element regulacji postępowania państw w cyberprzestrzeni pomiędzy „klasycznymi” normami prawnomiędzynarodowymi a soft law. Naruszenie bezpieczeństwa informacyjnego systemów komputerowych w świetle konkretnych norm prawa międzynarodowego regulujące odpowiedzialność międzynarodową państwa za działania indywidualnych hakerów i grup hakerskich. (Zasady poszanowania suwerenności terytorialnej. Zakaz interwencji w sprawy wewnętrzne. Zakaz użycia siły. Nakaz przeciwdziałania wykorzystaniu własnego terytorium do czynności szkodliwych dla drugiego państwa (zasada dobrego sąsiedztwa)).	x	5	KiUP_W01
TP-02	Prywatność w sieci w ujęciu przepisów prawa . Rozwój złośliwego oprogramowania ransomware jako nowy wymiar cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków. System dozoru elektronicznego w Polsce.	x	6	KiUP_W02
		<b>ćwiczenia</b>		
TP-03	Analiza poszczególnych cyberoperacji (Cyberoperacja przeciwko irańskiej instalacji nuklearnej Natanz za wykorzystaniem robaka Stuxnet. Wirusy Flame, Wiper i Shamoon. Cyberoperacje przeciwko Ukrainie. Cyberataki za wykorzystaniem ransomware WannaCry oraz NotPetya. Ingerencja w wybory prezydenckie w USA. Amerykańskie cyberoperacje przeciwko ISIS oraz przeciwko Rosji i Chinom w oparciu o nową doktrynę Departamentu Obrony USA).	x	5	KiUP_U01 KiUP_K01 KiUP_K02 KiUP_K03

**ZALECANA LITERATURA (w tym pozycje w języku obcym)**

**Literatura podstawowa przedmiotu** (powinna być dostępna dla studenta w uczelnianej bibliotece):

1. Gwoździwicz S., Tomaszycy K., Prawne I społeczne aspekty cyberbezpieczeństwa, Wydaw. Międzynarodowy Instytut Innowacji “Nauka-Edukacja-Rozwój”, Warszawa 2017.
2. P. Roguski, Użycie siły w cyberprzestrzeni : “cyberwojna” jako wyzwanie dla systemu Narodów Zjednoczonych w XXI w., System Narodów Zjednoczonych z polskiej perspektywy, 2017. – S. 401-410.
3. P. Roguski, Overcoming the damage of disinformation, New Eastern Europe, 2019, Public intellectuals. What is their place, role and responsibility today? no. 1 (35), p. 69-76.

**Literatura uzupełniająca przedmiotu:**

1. N. Tsagourias, R. Buchan (red.), Research Handbook on International Law and Cyberspace, Edward Elgar 2017;

2. M. Schmitt, L. Vihul (red.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press 2017;
3. K. Ziolkowski (red.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, NATO CCDCoE Publications 2012.

INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU

-

### III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

**Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.**

\* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy

# np. egzamin ustny, test, prezentacja, projekt

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
<b>WIEDZA</b>			
KiUP_W01	TP-01	wykład, prezentacja multimedialna	Egzamin pisemny
KiUP_W02	TP-02	wykład, prezentacja multimedialna	Egzamin pisemny
<b>UMIEJĘTNOŚCI</b>			
KiUP_U01	TP-3	ćwiczenia, studium przypadków	Zaliczenie z oceną - praca zaliczeniowa
<b>KOMPETENCJE SPOŁECZNE</b>			
KiUP_K01	TP-3	ćwiczenia, studium przypadków	Zaliczenie z oceną - praca zaliczeniowa
KiUP_K02	TP-3	ćwiczenia, studium przypadków	Zaliczenie z oceną - praca zaliczeniowa
KiUP_K03	TP-3	ćwiczenia, studium przypadków	Zaliczenie z oceną - praca zaliczeniowa

#### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności *
Godziny zajęć (według harmonogramu) z nauczycielem	25
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)	-
Praca własna studenta #	<ul style="list-style-type: none"> <li>▪ przygotowanie do egzaminu pisemnego (15 godzin)</li> <li>▪ przygotowanie pracy zaliczeniowej (10 godzin)</li> </ul>
<b>SUMA GODZIN</b>	50

#### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)

		Liczba punktów ECTS *	
SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPI-SANYCH DO ZAJĘĆ	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	2	1
	Liczba punktów ECTS przypisana praktykom zawodowym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe	2	-
	Praca własna studenta	2	1

\* godziny lekcyjne, czyli 1 godz. oznacza 45 min.

# przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu,...

## KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE

### Wykład:

Na ocenę dostateczną słuchacz potrafi wymienić regulacje prawne państw w zakresie ochrony cyberbezpieczeństwa, opisać zagrożenia dla gospodarki oraz systemów politycznych płynących z nieodpowiedzialnego wykorzystania cyberprzestrzeni przez państwa .

Na ocenę dobrą słuchacz potrafi opisać regulacje prawne państw w zakresie ochrony cyberbezpieczeństwa, zagrożenia dla gospodarki oraz systemów politycznych płynących z nieodpowiedzialnego wykorzystania cyberprzestrzeni przez państwa, odpowiedzialność międzynarodową państwa za działania indywidualnych hakerów i grup hakerskich. Podać przykłady złośliwego oprogramowania ransomware.

Na ocenę bardzo dobrą słuchacz potrafi opisać regulacje prawne państw w zakresie ochrony cyberbezpieczeństwa, zagrożenia dla gospodarki oraz systemów politycznych płynących z nieodpowiedzialnego wykorzystania cyberprzestrzeni przez państwa , odpowiedzialność międzynarodową państwa za działania indywidualnych hakerów i grup hakerskich. Opisać rozwój złośliwego oprogramowania ransomware jako nowego wymiaru cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków oraz system dozoru elektronicznego w Polsce.

### Ćwiczenia:

Na ocenę dostateczną student ma podstawową wiedzę i potrafi wymienić wybrane cyberoperacje na świecie oraz międzynarodowe akty prawne i normy kluczowe z punktu widzenia cyberbezpieczeństwa.

Na ocenę dobrą student ma podstawową wiedzę i potrafi opisać wybrane cyberoperacje na świecie oraz międzynarodowe akty prawne i normy kluczowe z punktu widzenia cyberbezpieczeństwa, implementować wynikające z nich obowiązki.

Na ocenę bardzo dobrą student ma podstawową wiedzę i potrafi dokonać analizy poszczególnych cyberoperacji (Cyberoperacja przeciwko irańskiej instalacji nuklearnej Natanz za wykorzystaniem robaka Stuxnet. Wirusy Flame, Wiper i Shamoon. Cyberoperacje przeciwko Ukrainie. Cyberataki za wykorzystaniem ransomware WannaCry oraz NotPetya. Ingerencja w wybory prezydenckie w USA. Amerykańskie cyberoperacje przeciwko ISIS oraz przeciwko Rosji i Chinom w oparciu o nową doktrynę Departamentu Obrony USA), opisać międzynarodowe akty prawne i normy kluczowe z punktu widzenia cyberbezpieczeństwa, implementować wynikające z nich obowiązki.

**Kryteria różnicowania ocen w powiązaniu ze stopniem realizacji efektów uczenia się, muszą być: precyzyjne i czytelne.**

# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Udostępnianie informacji publicznej</b>			
Nazwa studiów podyplomowych		<b>CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI</b>	
Język wykładowy: polski			
Rok studiów: I	Semestr: 1	Liczba punktów ECTS przypisana zajęciom: 2	Data aktualizacji sylabusu: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:			
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	15		
Ćwiczenia:	10		
Laboratorium:	-		
<b>RAZEM:</b>	<b>25</b>		
II. INFORMACJE SZCZEGÓLNE			
Cel (cele) prowadzenia zajęć: Przystwojenie i rozumienie podstawowych pojęć określonych w ustawie o dostępie do informacji publicznej, a także związanych z ochroną danych osobowych oraz zasad funkcjonowania podstawowych instytucji w przedmiotowym zakresie.			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu #	
<b>Wiedzy - zna i rozumie</b>			
UIP_W01	podstawowe pojęcia z zakresu dostępu do informacji publicznej, działania polskiego systemu w zakresie dostępu do informacji publicznej.	E_W01	
UIP_W02	znaczenie wiedzy z zakresu dostępu do informacji publicznej w funkcjonowaniu współczesnego państwa i społeczeństwa.	E_W01	
<b>Umiejętności - potrafi</b>			
UIP_U01	napisać wniosek o udostępnienie informacji publicznej, uzyskać informacje z Biuletynu Informacji Publicznej	E_U08	
<b>Kompetencji społecznych - jest gotów do</b>			
UIP_K01	poszerzania swojej wiedzy i umiejętności	E_K01	
UIP_K02	odpowiedzialnej realizacji powierzanych zadań	E_K02	
* kod zajęć, # efekty uczenia się dla określonego kierunku studiów, poziomu i profilu (np. K_W01, K_U01, ..) W- wiedza, U- umiejętności, K- kompetencje społeczne 01, 02...- numer efektu uczenia się <b>UWAGA!</b> Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 4-7, ale są to wartości umowne.			
<b>TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO ZAJĘĆ</b>			

**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	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>wykład</b>		
TP-01	Informacja publiczna (Pojęcie informacji publicznej i informacji przetworzonej w ustawie o dostępie do informacji publicznej. Sposoby regulacji zakresu przedmiotowego ustaw normujących zasady dostępu do informacji o wykonywaniu zadań administracji publicznej na świecie). Generalna klauzula dostępu do informacji publicznej. Katalog podmiotów zobowiązanych do udostępniania informacji publicznej i katalog podmiotów uprawnionych do uzyskania tej informacji.	x	7	UIP_W01 UIP_W02
TP-02	Granice prawa do informacji publicznej (Sposób regulacji granic prawa do informacji w ustawodawstwie europejskim i ustawach wybranych krajów europejskich i pozaeuropejskich. Granice prawa do informacji w Konstytucji RP. Granice prawa do informacji wprowadzone ustawą o dostępie do informacji publicznej). Kontrola administracyjna i sądowa realizacji prawa dostępu do informacji publicznej (Modele kontroli administracyjnej. Kontrola administracyjna w ustawie o dostępie do informacji publicznej. Kontrola sądowa prawa do informacji publicznej).	x	8	UIP_W01 UIP_W02
		<b>ćwiczenia</b>		
TP-03	Tryb i formy udostępniania informacji publicznej na gruncie ustawy o dostępie do informacji publicznej (Katalog form udostępnienia informacji publicznej. Zasady dostępu do dokumentu urzędowego. Zasady dostępu do informacji przetworzonej. Biuletyn Informacji Publicznej. Prawo uczestnictwa w posiedzeniach organów kolegialnych pochodzących z powszechnych wyborów. Dostęp do informacji publicznej na wniosek).	x	10	UIP_U01 UIP_K01 UIP_K02

**ZALECANA LITERATURA (w tym pozycje w języku obcym)**

**Literatura podstawowa przedmiotu** (powinna być dostępna dla studenta w uczelnianej bibliotece):

1. P. Szustakiewicz (red.), Dostęp do informacji publicznej, Wydawnictwo C. H. Beck, Warszawa 2014.
2. P. Sitniewski, Dostęp do informacji publicznej. Pytania i odpowiedzi, Lex a Wolters Cluwer business, Warszawa 2014.
3. J. Taczowska-Olszewska, Dostęp do informacji publicznej w polskim systemie prawnym, Wydawnictwo C. H. Beck, Warszawa 2014.

**Literatura uzupełniająca przedmiotu:**

1. A, Dmochowska, M. Zadrożny, Unijna reforma ochrony danych osobowych. Analiza zmian, wyd. C. H. Beck, Warszawa 2016.
2. Ogólne rozporządzenie o ochronie danych. Podręczny zbiór przepisów o ochronie danych osobowych, zestawień, schematów oraz wzorów rejestru czynności przetwarzania, pod red. G. Sibiga, K. Syska, wyd. C. H. Beck, Warszawa 2017.

INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU



### III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

**Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.**

\* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy

# np. egzamin ustny, test, prezentacja, projekt

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
<b>WIEDZA</b>			
UIP_W01	TP-01, TP-02	wykład, prezentacja multimedialna	Zaliczenie z oceną (ustne)
UIP_W02	TP-01, TP-02	wykład, prezentacja multimedialna	Zaliczenie z oceną (ustne)
<b>UMIEJĘTNOŚCI</b>			
UIP_U01	TP-3	ćwiczenia, studium przypadków, analiza orzeczeń sądowych	Zaliczenie z oceną - praca zaliczeniowa
<b>KOMPETENCJE SPOŁECZNE</b>			
UIP_K01	TP-3	ćwiczenia, studium przypadków, analiza orzeczeń sądowych	Zaliczenie z oceną - praca zaliczeniowa
UIP_K02	TP-3	ćwiczenia, studium przypadków, analiza orzeczeń sądowych	Zaliczenie z oceną - praca zaliczeniowa

#### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności *
Godziny zajęć (według harmonogramu) z nauczycielem	25
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)	-
Praca własna studenta #	<ul style="list-style-type: none"> <li>▪ przygotowanie do egzaminu ustnego (15 godzin)</li> <li>▪ przygotowanie pracy zaliczeniowej (10 godzin)</li> </ul>
<b>SUMA GODZIN</b>	50

#### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)

		Liczba punktów ECTS *	
<b>SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPI-SANYCH DO ZAJĘĆ</b>	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	<b>2</b>	<b>1</b>
	Liczba punktów ECTS przypisana praktykom zawodowym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe		-
	Praca własna studenta		<b>1</b>

\* godziny lekcyjne, czyli 1 godz. oznacza 45 min.

# przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu,...

#### KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE

##### Wykład:

Na ocenę dostateczną student potrafi zdefiniować podstawowe pojęcia z zakresu dostępu do informacji publicznej, opisać znaczenie wiedzy z zakresu dostępu do informacji publicznej w funkcjonowaniu współczesnego państwa i społeczeństwa.

działania polskiego systemu w zakresie dostępu do informacji publicznej.

Na ocenę dobrą słuchacz potrafi zdefiniować podstawowe pojęcia z zakresu dostępu do informacji publicznej, opisać znaczenie wiedzy z zakresu dostępu do informacji publicznej w funkcjonowaniu współczesnego państwa i społeczeństwa oraz scharakteryzować działania polskiego systemu w zakresie dostępu do informacji publicznej.

Na ocenę bardzo dobrą słuchacz potrafi opisać znaczenie wiedzy z zakresu dostępu do informacji publicznej w funkcjonowaniu współczesnego państwa i społeczeństwa, scharakteryzować polski system, w tym procedury w zakresie dostępu do informacji publicznej.

### **Ćwiczenia:**

Na ocenę dostateczną student ma podstawową wiedzę i potrafi opisać tryb i formy udostępniania informacji publicznej na gruncie ustawy o dostępie do informacji publicznej.

Na ocenę dobrą student ma podstawową wiedzę i potrafi opisać katalog form udostępnienia informacji publicznej, zasady dostępu do dokumentu urzędowego, zasady dostępu do informacji przetworzonej, Biuletyn Informacji Publicznej.

Na ocenę bardzo dobrą student ma podstawową wiedzę i potrafi napisać wniosek o udostępnienie informacji publicznej, uzyskać informacje z Biuletynu Informacji Publicznej.

**Kryteria różnicowania ocen w powiązaniu ze stopniem realizacji efektów uczenia się, muszą być: precyzyjne i czytelne.**

# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Ochrona informacji niejawnych</b>			
Nazwa studiów podyplomowych		CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI	
Język wykładowy: polski			
Rok studiów: I	Semestr: 1	Liczba punktów ECTS przypisana zajęciom: 3	Data aktualizacji sylabusu: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:			
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	15		
Ćwiczenia:	15		
Laboratorium:	-		
<b>RAZEM:</b>	<b>30</b>		
II. INFORMACJE SZCZEGÓLNE			
Cel (cele) prowadzenia zajęć: wprowadzenie studenta w obszar zasad ochrony informacji niejawnych, zapoznanie z procedurami określającymi nadawanie i kontrolowanie/weryfikację uprawnień dostępu do informacji niejawnych, a także ze sposobami ochrony informacji niejawnych w ramach ich przetwarzania, obiegu, dystrybucji/transportu.			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu #	
	<b>Wiedzy - zna i rozumie</b>		
OIN_W01	system ochrony informacji kwalifikowanych jako niejawne, uregulowania prawne w tym zakresie.	E_W01	
OIN_W02	problematykę informacji i jej znaczenie we współczesnym świecie oraz bezpieczeństwo informacyjne państwa.	E_W01	
	<b>Umiejętności - potrafi</b>		
OIN_U01	stosować procedury stanowienia i oznaczania informacji jako niejawnych, uwzględniając poziomy i rodzaje zagrożeń dla bezpieczeństwa państwa oraz ogniwa instytucjonalne delegowane do tych zadań.	E_U08	
OIN_U02	zapobiegać nieuprawnionemu ujawnianiu materiałów niejawnych.	E_U08	
	<b>Kompetencji społecznych - jest gotów do</b>		
OIN_K01	poszerzania swojej wiedzy i umiejętności	E_K01	
OIN_K02	odpowiedzialnej realizacji powierzonych zadań	E_K02	
* kod zajęć, # efekty uczenia się dla określonego kierunku studiów, poziomu i profilu (np. K_W01, K_U01, ..) W- wiedza, U- umiejętności, K- kompetencje społeczne 01, 02...- numer efektu uczenia się <b>UWAGA!</b> Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 4-7, ale są to wartości			

umowne.

## TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO 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	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>wykład</b>		
TP-01	Pojęcie informacji i jej znaczenie w czasach współczesnych. Ustawa o ochronie informacji niejawnych jako podstawa prawna systemu zabiegów o zapewnienie tajności wybranym kategoriom informacji i związane z nią inne akty prawne. Kategoria informacji niejawnych, ich klasyfikacja oraz sposoby oznaczania w RP. Bezpieczeństwo informacji niejawnych jako element systemu bezpieczeństwa państwa. Rodzaje zagrożeń dla informacji prawnie chronionych. Wybrane elementy systemu ochrony informacji niejawnych w RP.	x	8	OIN_W01
TP-02	Postępowanie sprawdzające w zakresie dostępu do informacji niejawnych w tym zwykłe, poszerzone. Instrumenty ochrony informacji niejawnych: kancelarie tajne, kontrola obiegu dokumentów, ochrona materiałów niejawnych w trakcie ich transportowania (przenoszenia, przewożenia).	x	7	OIN_W02
		<b>ćwiczenia</b>		
TP-03	Zasady klasyfikowania informacji niejawnych - przykłady. Nadawanie materiałom klauzul tajności - przykłady.	x	7	OIN_U01 OIN_K01 OIN_K02
TP-04	Identyfikowanie zagrożeń dla informacji prawnie chronionych. Postępowanie sprawdzające w sprawie dostępu do informacji niejawnych – możliwe sytuacje. Stosowanie instrumentów ochrony informacji niejawnych.	x	8	OIN_U01 OIN_K01 OIN_K02

### ZALECANA LITERATURA (w tym pozycje w języku obcym)

**Literatura podstawowa przedmiotu** (powinna być dostępna dla studenta w uczelnianej bibliotece):

- Liderman K., Bezpieczeństwo informacyjne. Nowe wyzwania. PWN, Warszawa 2017.
- Stankowska L., Ustawa o ochronie informacji niejawnych. Komentarz, LexisNexis Polska, Warszawa 2014.
- Iwaszko B., Ochrona informacji w praktyce, Presscom, Wrocław 2012.
- Thiem P., Instrukcja postępowania z materiałami niejawnymi z komentarzem, ODDK, Gdańsk 2012.
- Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010.
- Rozporządzenie Prezesa Rady Ministrów. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne z dnia 7 grudnia 2011 r.
- Rozporządzenie Prezesa rady Ministrów. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych z dnia 7 grudnia 2011 r.

**Literatura uzupełniająca przedmiotu:**

- Kwieciński M. (red.), Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane, Kraków 2010.
- Denning D. E., Wojna informacyjna i bezpieczeństwa informacji, WNT, Warszawa 2002.
- Pipkin D., Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa, WNT, Warszawa 2002.

INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU

-

### III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

**Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.**

\* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy

# np. egzamin ustny, test, prezentacja, projekt

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
<b>WIEDZA</b>			
OIN_W01	TP-01	wykład, prezentacja multimedialna	Egzamin pisemny
OIN_W02	TP-02	wykład, prezentacja multimedialna	Egzamin pisemny
<b>UMIEJĘTNOŚCI</b>			
OIN_U01	TP-3	ćwiczenia, studium przypadków	Zaliczenie z oceną - praca zaliczeniowa
OIN_U02	TP-4	ćwiczenia, studium przypadków	Zaliczenie z oceną - praca zaliczeniowa
<b>KOMPETENCJE SPOŁECZNE</b>			
OIN_K01	TP-3, TP-4	ćwiczenia, studium przypadków	Zaliczenie z oceną - praca zaliczeniowa
OIN_K02	TP-3, TP-4	ćwiczenia, studium przypadków	Zaliczenie z oceną - praca zaliczeniowa

#### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności *
Godziny zajęć (według harmonogramu) z nauczycielem	30
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)	-
Praca własna studenta #	<ul style="list-style-type: none"> <li>▪ przygotowanie do egzaminu pisemnego (15 godzin)</li> <li>▪ przygotowanie pracy zaliczeniowej (10 godzin)</li> <li>▪ przygotowanie do ćwiczeń – czytanie wskazanej literatury (15 godz.)</li> </ul>
<b>SUMA GODZIN</b>	75

#### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)

		Liczba punktów ECTS *	
SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPI-SANYCH DO ZAJĘĆ	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	3	1,2
	Liczba punktów ECTS przypisana praktykom zawodowym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe		-
	Praca własna studenta		1,8

\* godziny lekcyjne, czyli 1 godz. oznacza 45 min.

# przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu,...

#### KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE

**Wkład:**

Na ocenę dostateczną student potrafi zdefiniować informacje niejawne, potrafi określić regulacje prawne obowiązujące w tym zakresie.

Na ocenę dobrą słuchacz potrafi zakwalifikować informacje do grupy niejawnych, potrafi określić regulacje prawne obowiązujące w tym zakresie, potrafi określić znaczenie informacji we współczesnym świecie.

Na ocenę bardzo dobrą słuchacz potrafi zakwalifikować informacje do grupy niejawnych, potrafi określić regulacje prawne obowiązujące w tym zakresie, potrafi określić znaczenie informacji we współczesnym świecie oraz bezpieczeństwa informacyjnego państwa.

#### **Ćwiczenia:**

Na ocenę dostateczną student ma podstawową wiedzę i potrafi opisać procedury stanowienia i oznaczania informacji jako niejawnych, uwzględniając poziomy i rodzaje zagrożeń dla bezpieczeństwa państwa oraz ogniwa instytucjonalne delegowane do tych zadań.

Na ocenę dobrą student ma podstawową wiedzę i potrafi opisać procedury stanowienia i oznaczania informacji jako niejawnych, dokonać identyfikacji informacji niejawnych, uwzględniając poziomy i rodzaje zagrożeń dla bezpieczeństwa państwa oraz ogniwa instytucjonalne delegowane do tych zadań.

Na ocenę bardzo dobrą student ma podstawową wiedzę i potrafi stosować procedury stanowienia i oznaczania informacji jako niejawnych, uwzględniając poziomy i rodzaje zagrożeń dla bezpieczeństwa państwa, zapobiegać nieuprawnionemu ujawnianiu materiałów niejawnych.

**Kryteria różnicowania ocen w powiązaniu ze stopniem realizacji efektów uczenia się, muszą być: precyzyjne i czytelne.**

# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Cyberprzestępczość</b>			
Nazwa studiów podyplomowych		CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI	
Język wykładowy: polski			
Rok studiów: I	Semestr: 1	Liczba punktów ECTS przypisana zajęciom: 2	Data aktualizacji sylabusu: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:			
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	10		
Ćwiczenia:	15		
Laboratorium:	-		
<b>RAZEM:</b>	<b>25</b>		
II. INFORMACJE SZCZEGÓLNE			
Cel (cele) prowadzenia zajęć: przekazanie wiedzy i pogłębienie umiejętności w zakresie europejskiego i krajowego systemu cyberbezpieczeństwa, identyfikacji współczesnych zagrożeń systemów teleinformatycznych oraz stosowania odpowiednich zabezpieczeń.			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu #	
	<b>Wiedzy - zna i rozumie</b>		
C_W01	europejski i krajowy system cyberbezpieczeństwa, organizację krajowego systemu cyberbezpieczeństwa.	E_W04	
C_W02	prawne możliwości ścigania cyberprzestępstw.	E_W04	
	<b>Umiejętności - potrafi</b>		
C_U01	rozpoznać i przeciwdziałać zagrożeniom w cyberprzestrzeni, wskazuje podstawowe kierunki rozwoju cyberprzestępczości.	E_U01	
	<b>Kompetencji społecznych - jest gotów do</b>		
C_K01	rozstrzygania dylematów związanych z wykonywaniem zawodu	E_K03	
* kod zajęć, # efekty uczenia się dla określonego kierunku studiów, poziomu i profilu (np. K_W01, K_U01, ..) W- wiedza, U- umiejętności, K- kompetencje społeczne 01, 02...- numer efektu uczenia się			
<b>UWAGA!</b> Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 4-7, ale są to wartości umowne.			
TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO ZAJĘĆ			
<b>Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):</b>			

Symbol treści programowych	Opis treści programowych	Forma zajęć	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>wykład</b>		
TP-01	Cyberbezpieczeństwo państwa. Europejski i krajowy system cyberbezpieczeństwa (Podstawy ustrojowe europejskiego cyberbezpieczeństwa. Dyrektywa NIS. Organizacja krajowego systemu cyberbezpieczeństwa. Doktryna i strategia cyberbezpieczeństwa RP na tle innych krajów). Przedmioty ochrony i zagrożenia systemów informatycznych. Cyberprzestępstwa (Phishing. Kradzież tożsamości. Oszustwo telekomunikacyjne. Przystępczość z wykorzystaniem elektronicznych instrumentów płatniczych).	x	7	C_W01 C_W02
TP-02	Charakterystyka cyberprzestępczości w Polsce (Współczesne trendy i mody w zakresie cyberprzestępczości. Nowy wymiar Cyberbezpieczeństwa. Profilaktyka w zakresie cyberprzestępczości).	x	3	C_W01 C_W02
		<b>ćwiczenia</b>		
TP-03	Prywatność i poufność w środowisku chmurowym. Transakcje elektroniczne. Kryteria wyboru zabezpieczeń. (Zasady ogólne. Polityka dotycząca haseł. Wytoczne dotyczące różnych platform technologicznych. Przetwarzanie transakcyjne. Technologie biometryczne).	x	15	C_U01 C_K01

#### ZALECANA LITERATURA (w tym pozycje w języku obcym)

##### Literatura podstawowa przedmiotu (powinna być dostępna dla studenta w uczelnianej bibliotece):

1. Krawiec J., Cyberbezpieczeństwo. Podejście systemowe, Politechnika Warszawska. Warszawa 2019.
2. Banasiński C., Cyberbezpieczeństwo. Zarys wykładu, Wydaw. Wolters Kluwer, Warszawa 2018.
3. Górka M, Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Difin, Warszawa 2014.

##### Literatura uzupełniająca przedmiotu:

1. Hoffman T., Wybrane aspekty cyberbezpieczeństwa w Polsce, Wydaw. Fnc, Warszawa 2018.
2. Kluczewski J., Bezpieczeństwo sieci komputerowych. Praktyczne przykłady i ćwiczenia w symulatorze Cisco Packet Tracer, Wydaw. itstart, Warszawa 2019.
3. McNab Chris, Ocena bezpieczeństwa sieci, Wydaw. APN Promise. Warszawa 2017.

#### INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU

-

### III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

**Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.**

\* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy

# np. egzamin ustny, test, prezentacja, projekt

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
<b>WIEDZA</b>			
C_W01	TP-01, TP-02	wykład, prezentacja multimedialna	Zaliczenie z oceną - kolokwium pisemne
C_W02	TP-01, TP-02	wykład, prezentacja multimedialna	Zaliczenie z oceną - kolokwium pisemne



UMIEJĘTNOŚCI			
C_U01	TP-3	ćwiczenia, studium przypadków,	Zaliczenie z oceną - praca zaliczeniowa
KOMPETENCJE SPOŁECZNE			
C_K01	TP-3	ćwiczenia, studium przypadków,	Zaliczenie z oceną - praca zaliczeniowa
MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)			
Forma aktywności		Średnia liczba godzin na zrealizowanie aktywności *	
Godziny zajęć (według harmonogramu) z nauczycielem		25	
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)		-	
Praca własna studenta #		<ul style="list-style-type: none"> <li>▪ przygotowanie do egzaminu pisemnego (15 godzin)</li> <li>▪ przygotowanie pracy zaliczeniowej (10 godzin)</li> </ul>	
<b>SUMA GODZIN</b>		50	
MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)			
		Liczba punktów ECTS *	
SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPI-SANYCH DO ZAJĘĆ	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	2	1
	Liczba punktów ECTS przypisana praktykom zawodowym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe		-
	Praca własna studenta		1
* godziny lekcyjne, czyli 1 godz. oznacza 45 min.			
# przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu,...			
KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE			
<b><u>Wykład:</u></b>			
Na ocenę dostateczną student ma wiedzę i potrafi wymienić zagrożenia cyberbezpieczeństwa i opisać Europejski i krajowy system cyberbezpieczeństwa.			
Na ocenę dobrą student ma wiedzę i potrafi opisać Europejski i krajowy system cyberbezpieczeństwa, organizację krajowego systemu cyberbezpieczeństwa, zagrożenia cyberbezpieczeństwa.i prawne możliwości ścigania cyberprzestępstw.			
Na ocenę bardzo dobrą student ma wiedzę i potrafi opisać Europejski i krajowy system cyberbezpieczeństwa, organizację krajowego systemu cyberbezpieczeństwa. Potrafi identyfikować współczesne zagrożenia systemów teleinformatycznych oraz stosować odpowiednie zabezpieczenia.			
<b><u>Ćwiczenia:</u></b>			
Na ocenę dostateczną student ma podstawową wiedzę i potrafi opisać podstawowe kierunki rozwoju cyberprzestępczości			
Na ocenę dobrą student ma podstawową wiedzę i potrafi opisać podstawowe kierunki rozwoju cyberprzestępczości, wskazać metody zabezpieczeń.			
Na ocenę bardzo dobrą student ma podstawową wiedzę i potrafi wskazać podstawowe kierunki rozwoju cyberprzestępczości, rozpoznać i przeciwdziałać zagrożeniom w cyberprzestrzeni.			
<b>Kryteria różnicowania ocen w powiązaniu ze stopniem realizacji efektów uczenia się, muszą być: precyzyjne i czytelne.</b>			

# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Podstawy technologii sieci i intersieci</b>			
Nazwa studiów podyplomowych		<b>CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI</b>	
Język wykładowy: polski			
Rok studiów: I	Semestr: 1	Liczba punktów ECTS przypisana zajęciom: 3	Data aktualizacji sylabusu: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:		dr Robert Pękala mgr Marek Zarychta	
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	15		
Ćwiczenia:	-		
Laboratorium:	15		
<b>RAZEM: 30</b>			
II. INFORMACJE SZCZEGÓLNE			
Cel (cele) prowadzenia zajęć: zapoznanie słuchaczy z podstawowymi zagadnieniami dotyczącymi budowy topologii sieciowych i intersieciowych z wykorzystaniem technologii przewodowej Ethernet, zapoznanie z wybranymi mechanizmami i protokołami implementowanymi w urządzeniach sieciowych Ethernet w warstwie II oraz III modelu OSI			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu	
<b>Wiedzy - zna i rozumie</b>			
PTSiI_W_01	zasady budowy podstawowych topologii oraz mechanizmy funkcjonowania sieci i intersieci na poziomie warstwy II i III	E_W03	
PTSiI_W_02	mechanizmy wybranych protokołów bezpieczeństwa sieciowego	E_W03	
<b>Umiejętności - potrafi</b>			
PTSiI_U_01	w zakresie podstawowym zarządzać urządzeniami sieciowymi tj. przełącznikami i routerami	E_U07	
PTSiI_U_02	zbudować topologię sieciową i intersieciową, a także w tym wdrożyć mechanizmy routingu	E_U07	
PTSiI_U_03	potrafi zaimplementować mechanizmy protokołu IEEE 802.1q w kontekście bezpieczeństwa sieciowego	E_U07	
<b>Kompetencji społecznych - jest gotów do</b>			
PTSiI_K_01	samodzielnego zdobywania wiedzy w nieustannie rozwijającej się dziedzinie techniki	E_K01	

TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO 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	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>wykład</b>		
TP-01	Wybrane aspekty warstwy fizycznej technologii przewodowej Ethernet. Elementy systemów okablowania strukturalnego.	x	1	PTSiI_W_01
TP-02	Budowa ramki Ethernet, charakterystyka parametrów nagłówka ramki. Wykorzystanie analizatora sieciowego do badania nagłówka. Budowa adresów podwarstwy MAC.	x	1	PTSiI_W_01
TP-03	Przełączanie w warstwie II, zasada działania przełączników Ethernet, warstwy II. Algorytmy i tabele przełączania - wpisy statyczne i dynamiczne.	x	2	PTSiI_W_01
TP-04	Adresowanie IP v4 oraz IPv6, interfejsy IP i ich rola w komunikacji sieciowej i intersieciowej. Podstawy routingu IP, routing statyczny i dynamiczny (RIP, OSPF).	x	3	PTSiI_W_01
TP-05	Mechanizmy protokołu IEEE 802.1q - elementy bezpiecznej infrastruktury sieciowej z wykorzystaniem technologii sieci wirtualnych.	x	3	PTSiI_W_01, PTSiI_W_02
		<b>laboratorium</b>		
TP-06	Media i urządzenia transmisyjne w sieciach LAN, standard Ethernet, topologie sieci, przygotowanie okablowania strukturalnego dla Ethernetu w oparciu o normę TIA/EIA-568-B, elementy instalatorstwa światłowodowego – praktyczne zajęcia instalatorskie.	x	2	PTSiI_W_01, PTSiI_U_02
TP-07	Zarządzanie urządzeniami sieciowymi na przykładzie systemu operacyjnego CISCO IOS	x	1	PTSiI_W_01, PTSiI_U_01
TP-08	Idea kapsułkowania pakietów, wykorzystanie analizatora sieciowego <i>wireshark</i> do badania nagłówków ramki Ethernet.	x	2	PTSiI_W_01, PTSiI_U_01
TP-09	Zasady adresowania w sieciach IPv4 i IPv6; obliczanie puli adresowych dla przykładowych rozwiązań sieciowych.	x	3	PTSiI_W_01, PTSiI_U_02
TP-10	Wdrażanie mechanizmów routingu statycznego i dynamicznego w intersieciach IPv4 oraz IPv4 dla przykładowych topologii.	x	4	PTSiI_W_01, PTSiI_U_01 PTSiI_U_02
TP-11	Wdrażanie technologii sieci wirtualnych VLAN. Rola protokołu VTP. Routing między sieciami VLAN.	x	3	PTSiI_W_01, PTSiI_W_02 PTSiI_U_01 PTSiI_U_02 PTSiI_U_03 PTSiI_K_01

**ZALECANA LITERATURA (w tym pozycje w języku obcym)**

**Literatura podstawowa przedmiotu** (powinna być dostępna dla studenta w uczelnianej bibliotece):

1. Józefiak A.: CCNA 200-301. *Zostań administratorem sieci komputerowych CISCO*, wyd. Helion 2020r.
2. Banks E., White R.: *Sieci komputerowe. Najczęstsze problemy i ich rozwiązania*, wyd. Helion 2019r.
3. Empson S.: CCNA: pełny przegląd poleceń, Akademia sieci Cisco, PWN 2009r.

**Literatura uzupełniająca przedmiotu:**

1. oficjalny serwis: [www.cisco.com](http://www.cisco.com)
2. serwis internetowy: [www.computerworld.pl](http://www.computerworld.pl)

**INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU**

istnieje możliwość przeprowadzenia zajęć wykładowych z wykorzystaniem technologii wspierających e-learning

**III. INFORMACJE DODATKOWE**

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć
<b>WIEDZA</b>			
PTSiI_W_01	TP-01÷TP-11	wykład podający	Egzamin pisemny
PTSiI_W_02	TP-05, TP-11	wykład podający	Egzamin pisemny
<b>UMIEJĘTNOŚCI</b>			
PTSiI_U_01	TP-07, TP-08, TP-10, TP-11	zajęcia laboratoryjne z wykorzystaniem sprzętu sieciowego i analizatora sieciowego <i>wireshark</i>	Zaliczenie z oceną - krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych, weryfikacja poprawności realizacji ćwiczenia
PTSiI_U_02	TP-06, TP-09, TP-10, TP-11	zajęcia laboratoryjne z wykorzystaniem sprzętu sieciowego	Zaliczenie z oceną - krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych, weryfikacja poprawności realizacji ćwiczenia
PTSiI_U_03	TP-11	zajęcia laboratoryjne z wykorzystaniem sprzętu sieciowego	Zaliczenie z oceną - krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych, weryfikacja poprawności realizacji ćwiczenia
<b>KOMPETENCJE SPOŁECZNE</b>			
PTSiI_K_01	TP-05, TP-11	wykład, pogadanka w trakcie zajęć laboratoryjnych	wyniki zaliczeń kolokwiów oraz egzaminu

**MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)**

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny zajęć (według harmonogramu) z nauczycielem	30
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)	-
Praca własna studenta	<ul style="list-style-type: none"> <li>▪ przygotowanie do zajęć laboratoryjnych (10 godzin)</li> <li>▪ czytanie wskazanej literatury (5 godzin)</li> <li>▪ przygotowanie do egzaminu (15 godzin)</li> <li>▪ napisanie raportu z zajęć laboratoryjnych (15 godzin)</li> </ul>
<b>SUMA GODZIN</b>	75

**MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)**

		Liczba punktów ECTS	
SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPI-SANYCH DO ZAJĘĆ	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	3	1,2
	Liczba punktów ECTS przy-		-

	pisana praktykom zawodowym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe		
	Praca własna studenta		<b>1,8</b>
<b>KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE</b>			
<b><u>Wykład:</u></b>			
Na ocenę dostateczną słuchacz potrafi wykorzystać w stopniu zadowalającym zdobytą wiedzę w zakresie budowy topologii sieciowych i intersieciowych oraz w zakresie teorii protokołów sieciowych			
Na ocenę dobrą słuchacz potrafi wykorzystać i uzupełnić zdobytą samodzielnie wiedzę w zakresie budowy topologii sieciowych i intersieciowych oraz w zakresie teorii protokołów sieciowych			
Na ocenę bardzo dobrą słuchacz potrafi posługiwać się zaawansowanymi aspektami wiedzy teoretycznej w zakresie mechanizmów i protokołów sieciowych			
<b><u>laboratorium:</u></b>			
Na ocenę dostateczną słuchacz wykorzystuje w stopniu zadowalającym zdobytą wiedzę i umiejętności praktyczne do budowy topologii sieciowych i intersieciowych oraz zarządzania urządzeniami sieciowymi w zakresie podstawowym, z pomocą prowadzącego zajęcia			
Na ocenę dobrą słuchacz samodzielnie zdobywa i wykorzystuje wiedzę oraz umiejętności praktyczne do samodzielnej budowy topologii sieciowych i intersieciowych oraz zarządzania urządzeniami sieciowymi			
Na ocenę bardzo dobrą słuchacz samodzielnie zdobywa i wykorzystuje wiedzę oraz umiejętności praktyczne do budowy topologii sieciowych i intersieciowych oraz zarządzania urządzeniami sieciowymi, biegle posługując się wszystkimi podstawowymi aspektami w tym zakresie.			

# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Organizacja i zarządzanie bezpieczeństwem w administracji publicznej</b>			
Nazwa studiów podyplomowych		CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI	
Język wykładowy: polski			
Rok studiów: I	Semestr: 1	Liczba punktów ECTS przypisana zajęciom: 2	Data aktualizacji sylabusu: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:			
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	10		
Ćwiczenia:	10		
Laboratorium:	-		
<b>RAZEM:</b>	<b>20</b>		
II. INFORMACJE SZCZEGÓLNE			
Cel (cele) prowadzenia zajęć: wprowadzenie studenta w obszar teorii i technik organizacji i zarządzania w administracji publicznej, istotę i funkcje zarządzania publicznego traktowanego jako społeczny system funkcjonujący według określonego porządku, tworzącego złożone i dynamiczne struktury społeczne.			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu #	
	<b>Wiedzy - zna i rozumie</b>		
OiZB_W01	podstawową terminologię właściwą dla administracji, podstawę prawną, orzecznictwo i literaturę dotyczącą podstawowych materii administracyjnych.	E_W05	
	<b>Umiejętności - potrafi</b>		
OiZB_U01	dokonać analizy organizacji w strukturach administracji publicznej oraz sposobu zarządzania zadaniami wykonywanymi przez jej organy zgodnie z systemami normatywnymi oraz wybranymi normami i regułami (prawnymi, zawodowymi, moralnymi).	E_U06	
	<b>Kompetencji społecznych - jest gotów do</b>		
OiZB_K01	rozstrzygania dylematów związanych z wykonywaniem zawodu, zgodnie z podstawowymi zasadami etyki i normami moralnymi.	E_K03	
* kod zajęć, # efekty uczenia się dla określonego kierunku studiów, poziomu i profilu (np. K_W01, K_U01, ..) W- wiedza, U- umiejętności, K- kompetencje społeczne 01, 02...- numer efektu uczenia się <b>UWAGA!</b> Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 4-7, ale są to wartości umowne.			
TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO 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	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>wykład</b>		
TP-01	Istota i funkcje zarządzania publicznego. Administracja publiczna jako organizacja. Teorie i techniki organizacji i zarządzania w administracji publicznej. Regulacje prawne w zakresie funkcjonowania usług elektronicznych administracji publicznej (w szczególności ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne). Rola podpisu elektronicznego w administracji publicznej.	x	5	OiZB_W01
TP-02	Rewolucja technologiczna w zarządzaniu publicznym. E-administracja (Technologie informacyjne wewnątrz administracji. Technologie informacyjne w relacjach administracji z obywatelem. Cyberzagrożenia). Usługi elektroniczne w administracji publicznej (specyfika usług elektronicznych. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną).	x	5	OiZB_W01
		<b>ćwiczenia</b>		
TP-03	Zasady realizacji zadań z zakresu administracji publicznej w kontekście bezpieczeństwa jednostki. Systemy informacyjne jednostki (Informacja - strona BIP. Interakcja – możliwość ściągnięcia formularzy. Transakcja – możliwość przeprowadzenia transakcji elektronicznej np. serwis ePodatki. Personalizacja – posiadanie spersonalizowanego konta (np. Platforma ePUAP).	x	5	OiZB_U01 OiZB_K01
TP-04	Usługi elektroniczne świadczone pomiędzy jednostkami administracji. Usługi elektroniczne świadczone przez administrację na rzecz banku (np. podatki VAT i CIT). Usługi elektroniczne świadczone przez administrację na rzecz obywateli (np. aplikacje o dowody osobiste, prawa jazdy, podatek PIT).	x	5	OiZB_U01 OiZB_K01

**ZALECANA LITERATURA (w tym pozycje w języku obcym)**

**Literatura podstawowa przedmiotu** (powinna być dostępna dla studenta w uczelnianej bibliotece):

11. Niziołek M., Sześciło D., Jakubek-lalik J., Mednis A, Administracja i zarządzanie publiczne nauka o współczesnej administracji, Wyd. Sawpiau, Warszawa 2014.
12. Kożuch B., red. nauk.: Problemy zarządzania organizacjami publicznymi, Fundacja Współczesne
13. Zarządzanie, Instytut Spraw Publicznych UJ, Kraków 2006
14. Bednarczyk M., Organizacje publiczne. Zarządzanie konkurencyjnością, Warszawa-Kraków, 2001
15. Hausner J., Zarządzanie publiczne, Wydawnictwo Naukowe Scholar, Warszawa 2008
16. Władek Z., Organizacja i zarządzanie w administracji publicznej. Zarys wykładu, Difin, 2013.
17. Mazur S. (red.), Współzarządzanie publiczne, Wydawnictwo Naukowe Scholar, Warszawa 2015
18. Kisilowska I., Kisilowski M., Administracja - jak osiągnąć sukces osobisty zarządzając w administracji publicznej, Studio Emka 2016.

**Literatura uzupełniająca przedmiotu:**

7. Zawicki M., Nowe zarządzanie publiczne, PWE, Warszawa 2011.
8. Zybala A., Polityki publiczne. Doświadczenia w tworzeniu i wykonywaniu programów publicznych w Polsce i w innych krajach. Jak działa państwo gdy zamierza rozwiązać problemy zbiorowe swoich obywateli, Warszawa 2012.
9. Kulesza M., Sześciło D., Polityka administracyjna i zarządzanie publiczne, Warszawa 2013.

INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU

### III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

**Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.**

\* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy

# np. egzamin ustny, test, prezentacja, projekt

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
<b>WIEDZA</b>			
OiZB_W01	TP-01, TP-02	Wykład problemowy, prezentacja multimedialna	Zaliczenie z oceną – kolokwium pisemne
<b>UMIEJĘTNOŚCI</b>			
OiZB_U01	TP-03, TP-04	Ćwiczenia, praktyczne zadania, studium przypadków	Zaliczenie z oceną – zadania cząstkowe
<b>KOMPETENCJE SPOŁECZNE</b>			
OiZB_K01	TP-03, TP-04	Ćwiczenia, praktyczne zadania, studium przypadków	Zaliczenie z oceną – zadania cząstkowe

#### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności *
Godziny zajęć (według harmonogramu) z nauczycielem	20
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)	-
Praca własna studenta #	<ul style="list-style-type: none"> <li>▪ przygotowanie do zajęć, w tym realizacja zadań cząstkowych (20 godzin)</li> <li>▪ przygotowanie do zaliczenia pisemnego z wykładów (10 godzin)</li> </ul>
<b>SUMA GODZIN</b>	50

#### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)

		Liczba punktów ECTS *	
SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPI-SANYCH DO ZAJĘĆ	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	2	0,8
	Liczba punktów ECTS przypisana praktykom zawodowym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe		-
	Praca własna studenta		1,2

\* godziny lekcyjne, czyli 1 godz. oznacza 45 min.

# przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu,...

#### KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE

##### Wykład:

Na ocenę dostateczną słuchacz potrafi zdefiniować podstawową terminologię właściwą dla administracji, wymienić podstawę prawną, orzecznictwo i literaturę dotyczącą podstawowych materii administracyjnych.

Na ocenę dobrą słuchacz potrafi opisać istotę zarządzania w administracji publicznej, scharakteryzować teorie i techniki organizacji i zarządzania w administracji publicznej, regulacje prawne w zakresie funkcjonowania usług elektronicznych administracji publicznej.

Na ocenę bardzo dobrą słuchacz potrafi rozwiązać konkretne problemy związane z zarządzaniem w administracji publicznej w kontekście



cyberzagrożeń i w oparciu o orzecznictwo i literaturę dotyczącą podstawowych materii administracyjnych.

### **Ćwiczenia:**

Na ocenę dostateczną student ma podstawową wiedzę i potrafi opisać zasady realizacji zadań z zakresu administracji publicznej w kontekście bezpieczeństwa jednostki.

Na ocenę dobrą student ma podstawową wiedzę i potrafi opisać zasady realizacji zadań z zakresu administracji publicznej w kontekście bezpieczeństwa jednostki oraz systemy informacyjne jednostki (Informacja - strona BIP. Interakcja – możliwość ściągnięcia formularzy. Transakcja – możliwość przeprowadzenia transakcji elektronicznej np. serwis ePodatki. Personalizacja – posiadanie spersonalizowanego konta (np. Platforma ePUAP).

Na ocenę bardzo dobrą student ma podstawową wiedzę i potrafi realizować podstawowe usługi w zakresie: usługi elektronicznych świadczonych pomiędzy jednostkami administracji, usług elektronicznych świadczonych przez administrację na rzecz banku (np. podatki VAT i CIT), usług elektronicznych świadczonych przez administrację na rzecz obywateli (np. aplikacje o dowody osobiste, prawa jazdy, podatek PIT).

**Kryteria różnicowania ocen w powiązaniu ze stopniem realizacji efektów uczenia się, muszą być: precyzyjne i czytelne.**

# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Psychologiczne aspekty cyberbezpieczeństwa</b>			
Nazwa studiów podyplomowych		<b>CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI</b>	
Język wykładowy: polski			
Rok studiów: I	Semestr: 2	Liczba punktów ECTS przypisana zajęciom: 1	Data aktualizacji sylabusu: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:		Mgr Kamil Obłodecki	
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	10		
Ćwiczenia:	5		
Laboratorium:	-		
<b>RAZEM:</b>	<b>15</b>		
II. INFORMACJE SZCZEGÓLNE			
Cel (cele) prowadzenia zajęć: dostarczenie studentom wiedzy na temat zjawisk psychologicznych w sieci oraz psychologicznego funkcjonowania użytkowników Internetu, odnalezienie źródeł nieprawidłowego zachowania użytkowników w kontekście cyberzagrożeń.			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu #	
<b>Wiedzy - zna i rozumie</b>			
PAC_WO1	zagrożenia dla użytkowników płynące z upowszechniania nowoczesnych technologii w kontekście zachowań jednostki, mechanizmy i efekty poznania społecznego poprzez Internet, jego wpływ na relacje interpersonalne oraz na funkcjonowanie grup.	E_W05	
<b>Umiejętności - potrafi</b>			
PAC_UO1	analizować i interpretować ludzkie zachowania oraz przyczyn problemów w funkcjonowaniu jednostek, grup, organizacji i społeczności w dobie Internetu.	E_U06	
<b>Kompetencji społecznych - jest gotów do</b>			
PAC_KO1	przedsiębiorczego i kreatywnego myślenia i działania	E_K04	
* kod zajęć, # efekty uczenia się dla określonego kierunku studiów, poziomu i profilu (np. K_W01, K_U01, ..) W- wiedza, U- umiejętności, K- kompetencje społeczne 01, 02...- numer efektu uczenia się <b>UWAGA!</b> Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 4-7, ale są to wartości umowne.			
TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO 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	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>wykład</b>		
TP-01	Psychologiczny wymiar Internetu nowa przestrzeń funkcjonowania człowieka. Psychologiczna charakterystyka użytkowników Internetu. Jednostka w wirtualnej rzeczywistości w kontekście cyberzagrożeń. Problematyka tożsamości sieciowej - psychologiczne konsekwencje konstruowania wirtualnej tożsamości. Kontakty społeczne - analiza punktu widzenia zaspokajania potrzeb użytkowników..	x	6	PAC_WO1
TP-02	Poradnictwo sieciowe - pozytywne i negatywne aspekty zjawiska. Wpływ Internetu: modele wyjaśniające mechanizmy wpływu. Psychomanipulacja w sieci - zagrożenia dla użytkowników.	x	4	PAC_WO1
		<b>ćwiczenia</b>		
TP-03	Wpływ technologii na zachowania społeczne poszczególnych jednostek, grup i organizacji. Cyberhigiena. Tendencje oceny ryzyka (nadmierny optymizm, heurystyka dostępności, zakotwiczenia, reprezentatywności	x	5	PAC_UO1 PAC_KO1

**ZALECANA LITERATURA (w tym pozycje w języku obcym)**

**Literatura podstawowa przedmiotu (powinna być dostępna dla studenta w uczelnianej bibliotece):**

19. Wallace, P., Psychologia Internetu, Poznań 2005.
20. Castells M., Społeczeństwo sieci, Warszawa 2011.
21. Wojciszke B., Człowiek wśród ludzi. Zarys psychologii społecznej, Wydawnictwo Naukowe Scholar, Warszawa 2009.
22. Nęcka E., Orzechowski J., Szymura B., Psychologia poznawcza, Wydawnictwo Szkoły Wyższej Psychologii Społecznej „Academica”, 2008.

**Literatura uzupełniająca przedmiotu:**

10. Majgier K., Internet jako przestrzeń komunikacyjna, Lublin 2002.
11. Sokołowski M.(red.), Oblicza Internetu, Elbląg 2004.
12. M. Castells, Galaktyka Internetu, Warszawa 2004.

**INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU**

-

**III. INFORMACJE DODATKOWE**

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

**Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.**

\* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy

# np. egzamin ustny, test, prezentacja, projekt

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
<b>WIEDZA</b>			
PAC_WO1	TP-01, TP-02	Wykład problemowy, prezentacje multimedialne	Zaliczenie z oceną (ustne)
<b>UMIEJĘTNOŚCI</b>			
PAC_UO1	TP-03	Ćwiczenia, studium przypad-	Zaliczenie z oceną (ustne), ak-

		ków	tywność podczas zajęć
<b>KOMPETENCJE SPOŁECZNE</b>			
PAC_KO1	TP-03	Ćwiczenia, studium przypadków	Zaliczenie z oceną (ustne), aktywność podczas zajęć

**MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)**

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności *
Godziny zajęć (według harmonogramu) z nauczycielem	15
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)	-
Praca własna studenta #	<ul style="list-style-type: none"> <li>▪ przygotowanie do zaliczenia z wykładów (5 godzin)</li> <li>▪ przygotowanie do zaliczenia z ćwiczeń (5 godzin)</li> </ul>
<b>SUMA GODZIN</b>	25

**MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)**

		Liczba punktów ECTS *	
SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPI-SANYCH DO ZAJĘĆ	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	1	0,5
	Liczba punktów ECTS przypisana praktykom zawodowym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe		-
	Praca własna studenta		0,5

\* godziny lekcyjne, czyli 1 godz. oznacza 45 min.

# przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu,...

**KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE**

**Wykład:**

Na ocenę dostateczną słuchacz potrafi opisać zagrożenia płynące z upowszechniania nowoczesnych technologii w kontekście zachowań jednostki.

Na ocenę dobrą słuchacz potrafi na przykładach opisać zagrożenia dla użytkowników płynące z upowszechniania nowoczesnych technologii oraz mechanizmy i efekty poznania społecznego poprzez Internet.

Na ocenę bardzo dobrą student ma podstawową wiedzę i potrafi na przykładach scharakteryzować zjawisko psychomanipulacji w sieci w kontekście cyberzagrożeń.

**Ćwiczenia:**

Na ocenę dostateczną student ma podstawową wiedzę i potrafi opisać zachowania jednostek, grup, organizacji i społeczności w dobie Internetu.

Na ocenę dobrą student ma podstawową wiedzę i potrafi dokonać analizy ludzkich zachowań oraz przyczyn problemów w funkcjonowaniu jednostek, grup, organizacji i społeczności w dobie Internetu.

Na ocenę bardzo dobrą słuchacz potrafi dokonać analizy ludzkich zachowań, przyczyn problemów w dobie Internetu oraz ocenić wpływ nowoczesnych technologii na zachowania jednostki, relacje interpersonalne oraz na funkcjonowanie grup.

**Kryteria różnicowania ocen w powiązaniu ze stopniem realizacji efektów uczenia się, muszą być: precyzyjne i czytelne.**

# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Pozyskiwanie i weryfikacja danych z Internetu</b>			
Nazwa studiów podyplomowych		CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI	
Język wykładowy: polski			
Rok studiów: I	Semestr: 2	Liczba punktów ECTS przypisana zajęciom: 4	Data aktualizacji sylabusa: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:		Mgr Kamil Obłodecki	
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	15		
Ćwiczenia:	-		
Laboratorium:	30		
<b>RAZEM:</b>	<b>45</b>		
II. INFORMACJE SZCZEGÓLNE			
Cel (cele) prowadzenia zajęć: zapoznanie słuchaczy z			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu #	
<b>Wiedzy - zna i rozumie</b>			
PiWD_WO1	podstawowe metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet	E_W02, E_W04	
PiWD_WO2	podstawowe portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji	E_W02, E_W04	
<b>Umiejętności - potrafi</b>			
PiWD_UO1	pozyskiwać dane, a także umiejętnie interpretować otrzymane wyniki.	E_U04	
PiWD_UO2	użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych.	E_U04	
<b>Kompetencji społecznych - jest gotów do</b>			
PiWD_KO1	przedsiębiorczego i kreatywnego myślenia i działania	E_K04	
* kod zajęć, # efekty uczenia się dla określonego kierunku studiów, poziomu i profilu (np. K_W01, K_U01, ..) W- wiedza, U- umiejętności, K- kompetencje społeczne 01, 02...- numer efektu uczenia się <b>UWAGA!</b> Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 4-7, ale są to wartości umowne.			
TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO 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	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>wykład</b>		
TP-01	Podstawowe metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet. Wyszukiwarka Google (google hacking, google grafika). Rejestr domen internetowych – WhoIs. WiGLE.net.	x	6	PiWD_WO1
TP-02	Informacje specjalistyczne ze źródeł publicznych takich jak zbiory orzeczeń sądowych, czy interpretacji podatkowych. Bazy przedsiębiorców – Centralna Ewidencja i Informacja o Działalności Gospodarczej, Krajowy Rejestr Sądowy, Elektroniczne Księgi Wieczyste, inne. Informacje o pojazdach – sprawdzanie numeru VIN. Baza polis i szkód ubezpieczeniowych. Mapy i zdjęcia, geolokalizacja. Narzędzia do analizy metadanych, zdjęć.	x	9	PiWD_WO2
		<b>laboratorium</b>		
TP-03	Podstawowe portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji – praktyczne zadania. Własne sposoby surfowania po sieci WWW. Wyszukiwanie informacji w sieci WWW. Ściąganie oprogramowania i innych plików.	x	15	PiWD_UO2 PiWD_KO1
TP-04	Kontaktowanie się ze światem. Wyszukiwanie w social mediach, wyszukiwanie ludzi. Poczta elektroniczna - wysyłanie i odbieranie wiadomości oraz zarządzanie nimi. Najnowsze wiadomości z sieci WWW. Zarządzanie pieniędzmi online. Informacje specjalistyczne ze źródeł publicznych – praktyczne zadania.	x	15	PiWD_UO1 PiWD_KO1

**ZALECANA LITERATURA (w tym pozycje w języku obcym)**

**Literatura podstawowa przedmiotu** (powinna być dostępna dla studenta w uczelnianej bibliotece):

23. Kasser B., Internet praktycznie, Wydaw. „Intersoftland, Warszawa 2000.
24. Leś B., ABC... Internetu, Wydaw. Edition Kraków 2005.
25. Michałowska A., Michałowski S., Ćwiczenia z Internetu, Wydaw. MIKOM, Warszawa 2000.
26. Kent P., tł. Szymczyk W., Internet nie tylko dla orłów, Wydaw. Intersoftland, Warszawa 2000.
27. Żabicki P., Technologiczna codzienność. Internet – BANK – Telewizja, Wydaw. Trio, Warszawa 2007.

**Literatura uzupełniająca przedmiotu:**

13. Michałowska A., Michałowski S., Internet w Windows 98PL, Wydaw. MIKOM, Warszawa 2000.
14. Fabicki D., Poczta elektroniczna. Szkoła, internet, intranet, Wydaw. MIKOM, Warszawa 2000.
15. Sławik M., Komunikacja w Internecie dla każdego, Wydaw. Videograf Edukacja, Chorzów 2006.

INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU

### III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

**Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.**

\* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy

# np. egzamin ustny, test, prezentacja, projekt

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
<b>WIEDZA</b>			
PiWD_WO1	TP-01	Wykład, prezentacja multimedialna, pogadanka	Egzamin pisemny
PiWD_WO2	TP-02	Wykład, prezentacja multimedialna, pogadanka	Egzamin pisemny
<b>UMIEJĘTNOŚCI</b>			
PiWD_UO1	TP-04	Laboratorium, praktyczne zadania	Zaliczenie z oceną - zadania cząstkowe
PiWD_UO2	TP-03	Laboratorium, praktyczne zadania	Zaliczenie z oceną - zadania cząstkowe
<b>KOMPETENCJE SPOŁECZNE</b>			
PiWD_KO1	TP-03, TP-04	Laboratorium, praktyczne zadania	Zaliczenie z oceną - zadania cząstkowe

#### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności *
Godziny zajęć (według harmonogramu) z nauczycielem	45
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)	-
Praca własna studenta #	<ul style="list-style-type: none"> <li>▪ przygotowanie zadań cząstkowych (25 godzin)</li> <li>▪ przygotowanie do zajęć (15 godzin)</li> <li>▪ przygotowanie do egzaminu pisemnego (15 godzin)</li> </ul>
<b>SUMA GODZIN</b>	100

#### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)

		Liczba punktów ECTS *	
<b>SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPI-SANYCH DO ZAJĘĆ</b>	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	<b>4</b>	<b>1,8</b>
	Liczba punktów ECTS przypisana praktykom zawodowym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe		-
	Praca własna studenta		<b>2,2</b>

\* godziny lekcyjne, czyli 1 godz. oznacza 45 min.

# przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu,...

#### KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE

##### Wykład:

Na ocenę dostateczną słuchacz potrafi wymienić podstawowe metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet.

Na ocenę dobrą słuchacz potrafi opisać podstawowe metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet. Opisać źródła pozyskiwania specjalistycznych informacji (Zbiory orzeczeń sądowych, czy interpretacji podatkowych. Bazy przedsiębiorców – Centralna Ewidencja i Informacja o Działalności Gospodarczej, Krajowy Rejestr Sądowy, Elektroniczne Księgi Wieczyste, inne. Informacje o pojazdach – sprawdzanie numeru VIN. Baza polis i szkód ubezpieczeniowych. Mapy i zdjęcia, geolokalizacja. Narzędzia do analizy metadanych, zdjęć).

Na ocenę bardzo dobrą słuchacz potrafi opisać podstawowe metody, techniki, narzędzia oraz źródła pozyskania wskazanych informacji.

#### **laboratorium:**

Na ocenę dostateczną student ma podstawową wiedzę i potrafi wskazać portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji (Wyszukiwanie informacji w sieci WWW. Ściąganie oprogramowania i innych plików) – praktyczne zadanie

Na ocenę dobrą student ma podstawową wiedzę i potrafi pozyskać określone dane przy użyciu odpowiednich metod i narzędzi – praktyczne zadanie.

Na ocenę bardzo dobrą student ma podstawową wiedzę i potrafi użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych i zinterpretować otrzymane wyniki.

**Kryteria różnicowania ocen w powiązaniu ze stopniem realizacji efektów uczenia się, muszą być: precyzyjne i czytelne.**



# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Zarządzanie usługami sieciowymi w kontekście bezpieczeństwa</b>			
Nazwa studiów podyplomowych		<b>CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI</b>	
Język wykładowy: polski			
Rok studiów: I	Semestr: 2	Liczba punktów ECTS przypisana zajęciom: 3	Data aktualizacji sylabusa: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:		dr Robert Pękala mgr Marek Zarychta	
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	15		
Ćwiczenia:	-		
Laboratorium:	15		
<b>RAZEM:</b>	<b>30</b>		
II. INFORMACJE SZCZEGÓLNE			
Cel (cele) prowadzenia zajęć: zapoznanie słuchaczy z wybranymi mechanizmami i protokołami bezpieczeństwa sieciowego, stosowanych w sieciowych systemach operacyjnych w tym w systemach urządzeń sieciowych LAN			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu	
<b>Wiedzy - zna i rozumie</b>			
ZUS_W_01	zasady bezpiecznego zarządzania przełącznikami i routerami w sieciach LAN	E_W02, E_W04	
ZUS_W_02	mechanizmy wybranych protokołów bezpieczeństwa sieciowego, implementowanych w sieciowych systemach operacyjnych, w tym systemach wbudowanych urządzeń sieciowych	E_W02, E_W04	
<b>Umiejętności - potrafi</b>			
ZUS_U_01	wdrożyć protokoły bezpieczeństwa sieciowego umożliwiające bezpieczne, zdalne zarządzanie urządzeniami sieciowymi	E_U05	
ZUS_U_02	wdrożyć protokoły poprawiające bezpieczeństwo przesyłanych danych zarówno w skali LAN jak i Internetu	E_U05	
<b>Kompetencji społecznych - jest gotów do</b>			
ZUS_K_01	odpowiedzialnej realizacji powierzanych zadań	E_K02	
TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO 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	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>wykład</b>		
TP-01	Problematyka bezpiecznego, zdalnego zarządzania infrastrukturą sieciową - mechanizmy protokołu SSH.	x	2	ZUS_W_01
TP-02	Filtrowanie ruchu sieciowego w warstwie II - wykorzystanie protokołu <i>port-security</i> w systemie sieciowym IOS.	x	1	ZUS_W_01, ZUS_W_02
TP-03	Rola protokołu RADIUS w realizacji polityki bezpieczeństwa i jego implementacja w operacyjnych systemach sieciowych.	x	2	ZUS_W_01, ZUS_W_02
TP-04	Charakterystyka i zastosowanie protokołów technologii VPN - przykłady rozwiązań.	x	2	ZUS_W_01, ZUS_W_02
TP-05	Infrastruktura klucza publicznego PKI, rola urzędów certyfikacji. Aspekty techniczne wdrażania protokołu TLS/SSL w usłudze WWW w systemach Windows Server oraz GNU/Linux.	x	3	ZUS_W_02, ZUS_K_01
		<b>laboratorium</b>		
TP-06	Konfiguracja usługi SSH w sieciowym systemie operacyjnym CISCO IOS.	x	2	ZUS_W_01, ZUS_W_02, ZUS_U_01
TP-07	Wdrożenie protokołu <i>port security</i> w przełączniku CISCO.	x	1	ZUS_W_02, ZUS_U_01
TP-08	Instalacja i konfiguracja usługi <i>Free Radius</i> w systemie GNU/Linux. Implementacja usługi bezpieczeństwa z wykorzystaniem przełącznika CISCO.	x	2	ZUS_W_02, ZUS_U_01
TP-09	Konfiguracja usługi VPN w architekturze <i>punkt-punkt</i> w systemie CISCO IOS.	x	3	ZUS_W_01, ZUS_W_02, ZUS_U_02
TP-10	Wdrożenie bezpiecznego serwera WWW na przykładzie systemu GNU/Linux i serwera <i>Apache</i> .	x	2	ZUS_W_01, ZUS_W_02, ZUS_U_02, ZUS_K_01

**ZALECANA LITERATURA (w tym pozycje w języku obcym)**

**Literatura podstawowa przedmiotu** (powinna być dostępna dla studenta w uczelnianej bibliotece):

1. McNab Ch.: *Ocena bezpieczeństwa sieci* wyd. 3, wyd. APN Promise 2017r.
2. Santos O, Stuppi J.: *CCNA Security. Oficjalny podręcznik*, wyd. PWN 2016r.

**Literatura uzupełniająca przedmiotu:**

1. oficjalny serwis: [www.cisco.com](http://www.cisco.com)
2. oficjalny serwis: [httpd.apache.org](http://httpd.apache.org)

**INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU**

istnieje możliwość przeprowadzenia zajęć wykładowych z wykorzystaniem technologii wspierających e-learning

### III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć
<b>WIEDZA</b>			
ZUS_W_01	TP-01÷TP-04 TP-06, TP-09, TP-10	wykład podający	Egzamin - pisemne kolokwium zaliczeniowe
ZUS_W_02	TP-02÷TP-10	wykład podający	Egzamin - pisemne kolokwium zaliczeniowe
<b>UMIĘJĘTNOŚCI</b>			
ZUS_U_01	TP-06÷TP-08	zajęcia laboratoryjne z wykorzystaniem sprzętu sieciowego oraz zwirtualizowanego systemu GNU/Linux	Zaliczenie z oceną - krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych, weryfikacja poprawności realizacji ćwiczenia
ZUS_U_02	TP-09, TP-10,	zajęcia laboratoryjne z wykorzystaniem sprzętu sieciowego oraz zwirtualizowanego systemu GNU/Linux	Zaliczenie z oceną - krótkie kolokwium przed rozpoczęciem zajęć laboratoryjnych, weryfikacja poprawności realizacji ćwiczenia
<b>KOMPETENCJE SPOŁECZNE</b>			
ZUS_K_01	TP-05, TP-10	wykład, pogadanka w trakcie zajęć laboratoryjnych	wyniki zaliczeń kolokwiów

**MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)**

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny zajęć (według harmonogramu) z nauczycielem	30
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)	-
Praca własna studenta	<ul style="list-style-type: none"> <li>▪ przygotowanie do zajęć laboratoryjnych (10 godzin)</li> <li>▪ czytanie wskazanej literatury (5 godzin)</li> <li>▪ przygotowanie do zaliczenia kolokwium zaliczeniowego z wykładu (15 godzin)</li> <li>▪ napisanie raportu z zajęć laboratoryjnych (15 godzin)</li> </ul>
<b>SUMA GODZIN</b>	75

**MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)**

		Liczba punktów ECTS	
<b>SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPI-SANYCH DO ZAJĘĆ</b>	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	<b>3</b>	<b>1,2</b>
	Liczba punktów ECTS przypisana praktykom zawodowym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe		-
	Praca własna studenta		<b>1.8</b>

#### KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE

**Wkład:**

Na ocenę dostateczną słuchacz potrafi wykorzystać w stopniu zadowalającym zdobytą wiedzę w zakresie protokołów bezpieczeństwa sieciowego.

Na ocenę dobrą słuchacz potrafi wykorzystać i uzupełnić zdobytą samodzielnie wiedzę w zakresie protokołów bezpieczeństwa sieciowego

Na ocenę bardzo dobrą słuchacz potrafi posługiwać się zaawansowanymi aspektami wiedzy teoretycznej w zakresie mechanizmów i protokołów bezpieczeństwa sieciowego.

**laboratorium:**

Na ocenę dostateczną słuchacz wykorzystuje zdobytą wiedzę oraz wykorzystuje swoje umiejętności do konfiguracji protokołów i usług bezpieczeństwa w zakresie podstawowym, z pomocą prowadzącego zajęcia.

Na ocenę dobrą słuchacz zdobywa i wykorzystuje wiedzę oraz umiejętności praktyczne do samodzielnej konfiguracji protokołów i usług bezpieczeństwa w zakresie przewidzianym tematyką ćwiczeń

Na ocenę bardzo dobrą słuchacz zdobywa i wykorzystuje wiedzę oraz umiejętności praktyczne do samodzielnej konfiguracji protokołów i usług bezpieczeństwa, biegle posługując się wszystkimi podstawowymi aspektami zarządzania.

# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Audyt informatyczny</b>			
Nazwa studiów podyplomowych		CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI	
Język wykładowy: polski			
Rok studiów: I	Semestr: 2	Liczba punktów ECTS przypisana zajęciom: 3	Data aktualizacji sylabusu: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:		mgr Kamil Obłodecki	
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	15		
Ćwiczenia:	15		
Laboratorium:	-		
<b>RAZEM:</b>	<b>30</b>		
II. INFORMACJE SZCZEGÓLNE			
Cel (cele) prowadzenia zajęć: zapoznanie słuchaczy z metodologiami, metodykami i narzędziami prowadzenia audytu informatycznego			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu #	
<b>Wiedzy - zna i rozumie</b>			
AI_W01	zagadnienia związane z systemami teleinformatycznymi dla audytorów IT, standardy, metodologie i metodyki prowadzenia audytu, proces audytu (utrzymanie systemów teleinformatycznych).	E_W06	
<b>Umiejętności - potrafi</b>			
AI_U01	tworzyć program audytu oraz dokonać oceny ryzyka i bezpieczeństwa baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe.	E_U03	
<b>Kompetencji społecznych - jest gotów do</b>			
AI_K01	rozstrzygania dylematów związanych z wykonywaniem zawodu, zgodnie z podstawowymi zasadami etyki i normami moralnymi.	E_K03	
* kod zajęć, # efekty uczenia się dla określonego kierunku studiów, poziomu i profilu (np. K_W01, K_U01, ..) W- wiedza, U- umiejętności, K- kompetencje społeczne 01, 02...- numer efektu uczenia się <b>UWAGA!</b> Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 4-7, ale są to wartości umowne.			
TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO 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	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>wykład</b>		
TP-01	Zapoznanie studentów z istotą, założeniami i celem audytu. Omówione zostanie podstawowe rozumienie audytu, elementy wspólne i różniące od kontroli, ścieżki kariery i rozwoju, certyfikacje międzynarodowe ze szczególnym uwzględnieniem CISA, CompTIA oraz audytora JSFP, rynek pracy audytora w rozróżnieniu na sektor prywatny i publiczny, oczekiwane zarobki, typowe zadania audytora i jego umiejscowienie w strukturze podmiotu prywatnego lub publicznego	x	2	AI_W01
TP-02	Wykład gościnny - Dyrektor Departamentu Cyberbezpieczeństwa Exatel. Przedstawione zostanie podejście do prowadzenia badań odporności organizacji w konfrontacji ze zmotywowanym atakującym poprzez realizację rekonesansów bezpieczeństwa. Omówiona zostanie formuła rekonesansu, typowe realizacje i wnioski z pracy operacyjnej.	x	2	AI_W01
TP-03	Standardy, metodologie i metodyki prowadzenia audytu. Omówione zostaną standardy ISACA, INTOSAI, NIST, ISO z serii 27000 dobre praktyki NIK, COBIT 5, ITIL, Krajowe Ramy Interoperacyjności	x	4	AI_W01
TP-04	Proces audytu. Omówiony zostanie typowy cykl życia audytu, począwszy od planowania w oparciu o ocenę ryzyka, przygotowanie programu audytu, czynności audytowe, przygotowanie raportu z audytu, nadzór nad wykonaniem rekomendacji z audytu	x	2	AI_W01
TP-05	Podstawy wiedzy o systemach teleinformatycznych dla audytorów IT. Omówione zostaną m.in. zagadnienia z zakresu sieci, modelu OSI, protokołu TCP/IP, urządzeń i usług sieciowych, topologii sieci, technologii cloud, cyklu życia systemu informatycznego, audytu aplikacji,	x	2	AI_W01
TP-06	Ochrona informacji, utrzymanie systemów teleinformatycznych oraz zarządzanie kryzysowe. Omówione zostaną m.in. zagrożenia informatyczne, metody autentykacji, firewalle, IDS, IPS, infrastruktura PKI, zabezpieczenia na poziomie aplikacji, zarządzanie zmianą, incydentami, procesem tworzenia oprogramowania, dobre praktyki z zakresu utrzymania systemów teleinformatycznych	x	3	AI_W01
		<b>ćwiczenia</b>		
TP-07	Przygotowanie i planowanie audytu. Słuchacze ćwiczyć będą jak poprawnie tworzyć program audytu oraz analizę ryzyka	x	2	AI_U01 AI_K01
TP-08	OSINT i Information gathering. Przećwiczone zostaną techniki gromadzenia danych o audytowanym podmiocie na podstawie źródeł publicznie dostępnych. Omówiony zostanie OSINT framework, Nmap, whois, nslookup, Shodan, Maltego, theHarvester i inne	x	6	AI_U01 AI_K01
TP-09	Dowody z audytu oraz zasady sporządzania raportu z audytu. Przećwiczone zostaną zasady gromadzenia dowodów w trakcie czynności audytowych oraz najczęstsze błędy. Słuchacze sporządzą typowe elementy z raportu audytowego.	x	2	AI_U01 AI_K01

TP-10	Sytuacje nietypowe w audycie. Przeciwiczone zostaną typowe scenariusze niewłaściwej współpracy audytowanego z audytorem oraz omówione zostaną dobre praktyki po stronie audytorów	x	5	AI_U01 AI_K01
<b>ZALECANA LITERATURA (w tym pozycje w języku obcym)</b>				
<b>Literatura podstawowa przedmiotu</b> (powinna być dostępna dla studenta w uczelnianej bibliotece): 28. David L. Cannon Certified Information Systems Auditor, Wiley Publishing Inc., Indianapolis 2011 r. 29. Certified Information Systems Auditor – CISA Review Manual, ISACA, Rolling Meadows 2011 r. 30. INTOSAI Framework of Professional Pronouncements (IFPP), <a href="https://www.issai.org/">https://www.issai.org/</a>				
<b>Literatura uzupełniająca przedmiotu:</b> 16. Seria publikacji z zakresu COBIT 5, ISACA, <a href="https://www.isaca.org/resources/cobit">https://www.isaca.org/resources/cobit</a> 17. ITIL Foundation 4 edition, AXELOS 18. M. Chapple, CompTIA Pentest+, Sybex, Indianapolis 2019 r. 19. NIST standards, <a href="https://csrc.nist.gov/publications/sp800">https://csrc.nist.gov/publications/sp800</a>				
INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU				
-				
<b>III. INFORMACJE DODATKOWE</b>				
Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania <b>Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.</b>				
* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy # np. egzamin ustny, test, prezentacja, projekt				
Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #	
<b>WIEDZA</b>				
AI_W01	TP-01, TP-02, TP-03, TP-04, TP-05, TP-06	Wykład podający, prezentacja multimedialna	Egzamin pisemny	
<b>UMIEJĘTNOŚCI</b>				
AI_U01	TP-07, TP-08, TP-09, TP-10	Ćwiczenia, studium przypadków, praca z materiałami	Zaliczenie z oceną - projekt	
<b>KOMPETENCJE SPOŁECZNE</b>				
AI_K01	TP-07, TP-08, TP-09, TP-10	Ćwiczenia, studium przypadków, praca z materiałami	Zaliczenie z oceną - projekt	
<b>MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)</b>				
Forma aktywności		Średnia liczba godzin na zrealizowanie aktywności *		
Godziny zajęć (według harmonogramu) z nauczycielem		30		
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)		-		
Praca własna studenta #		<ul style="list-style-type: none"> <li>▪ przygotowanie do zajęć, w tym realizacja projektu (25 godzin)</li> <li>▪ przygotowanie do egzaminu pisemnego (20 godzin)</li> </ul>		
<b>SUMA GODZIN</b>		75		
<b>MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)</b>				
		Liczba punktów ECTS *		
SUMARYCZNA LICZBA	Praca studenta wymagająca	3	1,2	

PUNKTÓW ECTS PRZYPI- SANYCH DO ZAJĘĆ	bezpośredniego kontaktu z nauczycielem akademickim	
	Liczba punktów ECTS przy- pisana praktykom zawodo- wym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe	-
	Praca własna studenta	<b>1,8</b>

\* godziny lekcyjne, czyli 1 godz. oznacza 45 min.

# przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu,...

#### KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE

##### Wykład:

Na ocenę dostateczną słuchacz potrafi rozpoznać podstawowe standardy, metodologie i metodyki prowadzenia audytu informatycznego. Potrafi właściwie umiejscowić audyt w strukturze organizacyjnej oraz określić założenia formalno-organizacyjne wymagane do prawidłowego funkcjonowania audytu. Słuchacz zna podstawowe narzędzia OSINT i potrafi poprawnie korzystać z ich podstawowych funkcjonalności. Słuchacz ma podstawową wiedzę z obszaru informatyki pozwalającej na porozumiewanie się z personelem IT z wykorzystaniem terminologii technicznej. Potrafi poprawnie przygotować analizę ryzyka oraz program audytu i raport z audytu przy wsparciu bardziej doświadczonej osoby. Absolwent jest w stanie swobodnie wykonywać funkcje audytora wspierającego, młodsze audytora, członka zespołu audytu.

Na ocenę dobrą słuchacz potrafi samodzielnie wykorzystać podstawowe standardy, metodologie i metodyki prowadzenia audytu informatycznego, w tym także opracowane w języku angielskim. Potrafi właściwie umiejscowić audyt w strukturze organizacyjnej oraz opracować założenia formalno-organizacyjne wymagane do prawidłowego funkcjonowania audytu. Słuchacz zna narzędzia OSINT i potrafi samodzielnie korzystać z ich podstawowych funkcjonalności, w tym także dopasować narzędzia do wymagań podmiotu audytowanego. Słuchacz ma obszerną wiedzę z obszaru informatyki pozwalającej na porozumiewanie się z personelem IT z wykorzystaniem terminologii technicznej, wytłumaczenie zasad funkcjonowania systemów teleinformatycznych oraz szczegółowe uzasadnienie zaproponowanych rekomendacji audytowych. Potrafi samodzielnie przygotować analizę ryzyka, program audytu i raport z audytu. Absolwent jest w stanie swobodnie wykonywać funkcje audytora samodzielnego oraz kierownika zespołu audytu.

Na ocenę bardzo dobrą słuchacz potrafi samodzielnie wyszukać, krytycznie przeanalizować i dopasować do specyfiki audytu standardy, metodologie i metodyki prowadzenia audytu informatycznego, w tym także opracowane w języku angielskim. Potrafi właściwie umiejscowić audyt w strukturze organizacyjnej oraz opracować założenia formalno-organizacyjne wymagane do prawidłowego funkcjonowania audytu. Słuchacz zna narzędzia OSINT oraz wybrane narzędzia z zakresu testów penetracyjnych systemów teleinformatycznych, a także potrafi samodzielnie korzystać z ich podstawowych funkcjonalności, w tym także dopasować narzędzia do wymagań podmiotu audytowanego. Słuchacz ma obszerną wiedzę z obszaru informatyki pozwalającej na porozumiewanie się z personelem IT z wykorzystaniem terminologii technicznej, wytłumaczenie zasad funkcjonowania systemów teleinformatycznych oraz szczegółowe uzasadnienie zaproponowanych rekomendacji audytowych. Stanowi źródło wiedzy dla pozostałych członków zespołu audytowego. Potrafi samodzielnie przygotować analizę ryzyka, program audytu i raport z audytu, w tym także uzasadnić poszczególne uzasadnienia w oparciu o standardy audytu. Absolwent jest w stanie swobodnie wykonywać funkcje audytora samodzielnego, kierownika zespołu audytu oraz kierownika pionu audytu w podmiocie.

##### Ćwiczenia:

Na ocenę dostateczną student ma podstawową wiedzę i potrafi określić podstawowe błędy w zakresie programu audytu, dowodów audytowych, raportu z audytu. Dysponuje podstawowym warsztatem w zakresie prowadzenia audytu w oparciu o analizę ryzyka. Wykorzystuje w ograniczonym zakresie narzędzia automatyzacji planowania i czynności audytowych. Potrafi rozpoznać i podjąć czynności zaradcze w stosunku do podstawowych sytuacji nietypowych w audycie.

Na ocenę dobrą student ma podstawową wiedzę i potrafi swobodnie określić błędy w zakresie programu audytu, dowodów audytowych, raportu z audytu. Dysponuje warsztatem w zakresie prowadzenia audytu w oparciu o analizę ryzyka i potrafi samodzielnie przygotować dokumenty właściwe dla całego cyklu życia audytu. Wykorzystuje narzędzia automatyzacji planowania i czynności audytowych. Potrafi rozpoznać i podjąć czynności zaradcze w stosunku do wszystkich sytuacji nietypowych w audycie, omówionych na zajęciach.

Na ocenę bardzo dobrą student ma podstawową wiedzę i potrafi swobodnie określić błędy w zakresie programu audytu, dowodów audytowych, raportu z audytu, wraz z uzasadnieniem błędu w odniesieniu do międzynarodowych standardów audytu. Dysponuje warsztatem w zakresie prowadzenia audytu w oparciu o analizę ryzyka i potrafi samodzielnie przygotować dokumenty właściwe dla całego cyklu życia audytu. Wykorzystuje narzędzia automatyzacji planowania i czynności audytowych. Potrafi rozpoznać i podjąć czynności zaradcze w stosunku do wszystkich sytuacji nietypowych w audycie, omówionych na zajęciach.

**Kryteria różnicowania ocen w powiązaniu ze stopniem realizacji efektów uczenia się, muszą być: precyzyjne i czytelne.**



# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE			
Nazwa zajęć: <b>Bezpieczeństwo systemów teleinformatycznych</b>			
Nazwa studiów podyplomowych		CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI	
Język wykładowy: polski			
Rok studiów: I	Semestr: 2	Liczba punktów ECTS przypisana zajęciom: 3	Data aktualizacji sylabusu: 01.06.2021
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania	
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:		Łukasz Kurek Dawid Zięcina Tomasz Podłucki	
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN			
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:			
Wykład:	-		
Ćwiczenia:	10		
Laboratorium:	15		
<b>RAZEM:</b>	<b>25</b>		
II. INFORMACJE SZCZEGÓLWE			
Cel (cele) prowadzenia zajęć: zapoznanie słuchaczy ze stosowanymi na rynku narzędziami oraz technologiami służącymi do monitorowania i eliminacji zagrożeń w sieci i systemach informatycznych.			
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.			
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:	Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu #	
	<b>Wiedzy - zna i rozumie</b>		
BST_W01	zagadnienia związane z bezpieczeństwem systemów i sieci, podstawowe narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń	E_W04	
	<b>Umiejętności - potrafi</b>		
BST_U01	wykorzystać podstawowe narzędzia i techniki do rozpoznawania zagrożeń, zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów.	E_U02	
	<b>Kompetencji społecznych - jest gotów do</b>		
BST_K01	rozstrzygania dylematów związanych z wykonywaniem zawodu, zgodnie z podstawowymi zasadami etyki i normami moralnymi.	E_K03	
* kod zajęć, # efekty uczenia się dla określonego kierunku studiów, poziomu i profilu (np. K_W01, K_U01, ..) W- wiedza, U- umiejętności, K- kompetencje społeczne 01, 02...- numer efektu uczenia się <b>UWAGA!</b> Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 4-7, ale są to wartości umowne.			
TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO 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	Liczba godzin	Odniesienie do efektów uczenia się przypisanych do zajęć
		<b>ćwiczenia</b>		
TP-01	Wprowadzenie + Nowoczesne systemy firewall. Zakres wykładu obejmie ogólne omówienie komponentów nowoczesnego systemu klasy firewall oraz wykorzystywanych metod ochrony, sposoby implementacji systemu firewall, integrację systemów z pozostałymi elementami architektury bezpieczeństwa, przedstawienie rozwiązania klasy NGFW na przykładzie platformy jednego z wiodących producentów na rynku.	x	2h (DZ)	BST_W01
TP-02	Wykrywanie zagrożeń dzięki analizie NetFlow. Zakres wykładu obejmie wstęp do technologii NetFlow, zalety i wady monitorowania zagrożeń w oparciu o analizę NetFlow, prezentację komponentów środowiska do analizy, przedstawienie sposobu realizacji detekcji na przykładzie platformy jednego z wiodących producentów na rynku.	x	2h (DZ)	BST_W01
TP-03	Platformy Antymalware / Data Leak Prevention / Deception. Zakres wykładu obejmie omówienie działania platform oraz ich komponentów, sposoby implementacji monitoringu oraz zalety i wady w zależności od przyjętego modelu.	x	2h (ŁK)	BST_W01
TP-04	SIEM / Full Packet Capture. Zakres wykładu obejmie omówienie działania systemów klasy SIEM, sposobów implementacji monitoringu innych systemów informatycznych, procesu pozyskiwania logów i korelowania zdarzeń.	x	2h (ŁK)	BST_W01
TP-05	Bezpieczeństwo OT – wprowadzenie do zagadnień bezpieczeństwa systemów automatyki przemysłowej.	x	2h (TP)	BST_W01
		<b>laboratorium</b>		
TP-06	Ochrona sieci poprzez zaawansowane mechanizmy systemu firewall. Uczestnik ćwiczeń zapozna się z panelem zarządzania systemu firewall, przeprowadzi konfigurację wybranych mechanizmów i przetestuje ich skuteczność w ochronie sieci, zapozna się z praktycznymi zastosowaniami dekrypcji SSL realizowanej przez firewall oraz zweryfikuje sposoby bezpiecznego podłączania zdalnych użytkowników.	x	4h (DZ)	BST_U01 BST_K01
TP-07	Analiza ruchu sieciowego i wykrywanie zagrożeń. Uczestnik ćwiczeń zapozna się z panelem zarządzania platformy jednego z wiodących producentów na rynku, nabyte umiejętności analizy ruchu sieciowego w oparciu o NetFlow, pozna wybrane sposoby wykrywania ukrytej komunikacji, zrealizuje analizę przykładowego alarmu oraz przeprowadzi próbę analizy komunikacji SSL bez dekrypcji.	x	4h (DZ)	BST_U01 BST_K01
TP-08	Ochrona sieci poprzez zaawansowane mechanizmy systemu NIDS i Deception. Uczestnik zapozna się z panelem zarządzania platformą jednego z wiodących producentów na rynku, nabyte umiejętności projektowania i implementowania własnych reguł oraz polityk bezpieczeństwa, zrealizuje analizę przykładowego alarmu oraz przeprowadzi próbę analizy komunikacji.	x	4h (ŁK)	BST_U01 BST_K01
TP-09	Monitoring systemów za pomocą SIEM i Full Packet Capture. Uczestnik zapozna się z panelem za-	x	3h (ŁK)	BST_U01 BST_K01

	<p>rzządzania platformą SIEM, nabeździe umiejętności projektowania i implementowania reguł korelacyjnych, zrealizuje analizę przykładowego alarmu oraz przeprowadzi próbę analizy zdarzenia na podstawie zebranych logów z innych systemów.</p>			
--	---	--	--	--

### ZALECANA LITERATURA (w tym pozycje w języku obcym)

#### Literatura podstawowa przedmiotu (powinna być dostępna dla studenta w uczelnianej bibliotece):

1. Don Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter Paperback, 2019 r.
2. Don Murdoch, Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder, 2014 r.

#### Literatura uzupełniająca przedmiotu:

1. Norma ISO/IEC 27001:2017

### INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU

-

### III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

**Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.**

\* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy

# np. egzamin ustny, test, prezentacja, projekt

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
<b>WIEDZA</b>			
BST_W01	TP-01, TP-02, TP-03 TP-04, TP-05	Ćwiczenia, metoda przypadków, prezentacje	Zaliczenie z oceną – realizacja projektu
<b>UMIEJĘTNOŚCI</b>			
BST_U01	TP-06, TP-07, TP-08, TP-09	Laboratorium, praktyczne zadania z wykorzystaniem narzędzi informatycznych	Zaliczenie z oceną – realizacja projektu
<b>KOMPETENCJE SPOŁECZNE</b>			
BST_K01	TP-06, TP-07, TP-08, TP-09	Laboratorium, praktyczne zadania z wykorzystaniem narzędzi informatycznych	Zaliczenie z oceną – realizacja projektu

### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (godziny)

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności *
Godziny zajęć (według harmonogramu) z nauczycielem	25
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)	-
Praca własna studenta #	<ul style="list-style-type: none"> <li>▪ przygotowanie do zajęć, czytanie wskazanej literatury (10 godz.)</li> <li>▪ realizacja projektu z ćwiczeń (20 godzin)</li> <li>▪ realizacja projektu z laboratorium (20 godzin)</li> </ul>
<b>SUMA GODZIN</b>	75

### MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)

		Liczba punktów ECTS *	
SUMARYCZNA LICZBA	Praca studenta wymagająca	3	1

PUNKTÓW ECTS PRZYPI- SANYCH DO ZAJĘĆ	bezpośredniego kontaktu z nauczycielem akademickim	
	Liczba punktów ECTS przy- pisana praktykom zawodo- wym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe	-
	Praca własna studenta	2

\* godziny lekcyjne, czyli 1 godz. oznacza 45 min.

# przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu,...

#### KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE

##### Ćwiczenia:

Na ocenę dostateczną student ma podstawową wiedzę potrafi rozróżnić klasy systemów bezpieczeństwa oraz wskazać różnicę w ich działaniu. Student posiada podstawową wiedzę dotyczącą reguł i polityk bezpieczeństwa w systemach informatycznych.

Na ocenę dobrą student ma podstawową wiedzę i potrafi rozróżnić klasy systemów bezpieczeństwa. Potrafi wskazać różnicę w ich działaniu. Student posiada wiedzę z projektowania i implementowania reguł i polityk bezpieczeństwa w systemach informatycznych. Potrafi korelować zdarzenia pochodzące z różnych systemów informatycznych.

Na ocenę bardzo dobrą student ma wiedzę i potrafi rozróżnić klasy systemów bezpieczeństwa. Potrafi wskazać różnicę w ich działaniu. Student posiada wiedzę z projektowania i implementowania reguł oraz polityk bezpieczeństwa w systemach informatycznych. Potrafi korelować zdarzenia z różnych systemów informatycznych, wskazać różne modele implementacji poszczególnych systemów bezpieczeństwa oraz ich wady i zalety, a także wyjaśnić ideę honeypotów.

##### laboratorium:

Na ocenę dostateczną student ma podstawową wiedzę i potrafi zaimplementować poprawne podstawowe reguły bezpieczeństwa w systemie informatycznym.

Na ocenę dobrą student ma podstawową wiedzę i potrafi zaimplementować poprawne reguły (w tym reguły korelacyjne) i polityki bezpieczeństwa w systemie informatycznym, na bazie wcześniej dostarczonej analizy wymagań. Potrafi wykonać analizę alarmu o zdarzeniu i odrzucić alarmy typu „false positive”.

Na ocenę bardzo dobrą student ma wiedzę i potrafi samodzielnie przeprowadzić analizę wymagań, zaprojektować oraz zaimplementować poprawne reguły (w tym reguły korelacyjne) i polityki bezpieczeństwa w systemach informatycznych. Potrafi wykonać analizę alarmu o zdarzeniu, odrzucić alarmy typu „false positive” oraz skorelować zdarzenia z innych systemów na podstawie zebranych logów.

**Kryteria różnicowania ocen w powiązaniu ze stopniem realizacji efektów uczenia się, muszą być: precyzyjne i czytelne.**

# Karta opisu zajęć - Sylabus

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

I. INFORMACJE OGÓLNE				
Nazwa zajęć: <b>Incydenty teleinformatyczne</b>				
Nazwa studiów podyplomowych		<b>CYBERBEZPIECZEŃSTWO I OCHRONA INFORMACJI</b>		
Język wykładowy: polski				
Rok studiów: I	Semestr: 2	Liczba punktów ECTS przypisana zajęciom: 2	Data aktualizacji sylabusa: 01.06.2021	
Instytut (Zakład) odpowiedzialny za zajęcia:		Instytut Ekonomii i Zarządzania		
Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/prowadzących zajęcia:		Rafał Litwińczuk Łukasz Kurek		
FORMA PROWADZENIA ZAJĘĆ I LICZBA GODZIN				
Ogólna liczba godzin zajęć dydaktycznych na studiach podyplomowych z podziałem na formy:				
Wykład:	-			
Ćwiczenia:	10			
Laboratorium:	5			
<b>RAZEM:</b>	<b>15</b>			
II. INFORMACJE SZCZEGÓLNE				
Cel (cele) prowadzenia zajęć: zapoznanie słuchaczy z metodologiami, metodykami i narzędziami prowadzenia audytu informatycznego				
Przypisane do zajęć efekty uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych i odniesienie ich do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu.				
Symbol efektów uczenia się przypisanego do zajęć*	Po zakończeniu zajęć i potwierdzeniu osiągnięcia efektów uczenia się, student w kategorii:		Odniesienie do efektów uczenia się dla określonego kierunku studiów, poziomu i profilu #	
<b>Wiedzy - zna i rozumie</b>				
IT_W01	podstawowe narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń		E_W04	
<b>Umiejętności - potrafi</b>				
IT_U01	wykorzystać podstawowe narzędzia i techniki do rozpoznawania zagrożeń, obsługiwać incydenty bezpieczeństwa w oparciu o systemy teleinformatyczne oraz sporządzać raporty.		E_U02	
<b>Kompetencji społecznych - jest gotów do</b>				
IT_K01	krytycznej oceny posiadanej wiedzy i umiejętności		E_K01	
* kod zajęć, # efekty uczenia się dla określonego kierunku studiów, poziomu i profilu (np. K_W01, K_U01, ..) W- wiedza, U- umiejętności, K- kompetencje społeczne 01, 02...- numer efektu uczenia się <b>UWAGA!</b> Zaleca się, aby w zależności od liczby godzin zajęć, liczba efektów uczenia się zawierała się w przedziale: 4-7, ale są to wartości umowne.				
TREŚCI PROGRAMOWE I ICH ODNIESIENIE DO EFEKTÓW UCZENIA SIĘ PRZYPISANYCH DO ZAJĘĆ				
<b>Treści programowe (uszczegółowione, zaprezentowane z podziałem na poszczególne formy zajęć tj. wykład, ćwiczenia, laboratoria, projekty, seminaria i inne):</b>				
<b>Symbol treści pro-</b>	<b>Opis treści programowych</b>	<b>Forma zajęć</b>	<b>Liczba godzin</b>	<b>Odniesienie do efektów uczenia</b>

gramowych				się przypisanych do zajęć
		<b>ćwiczenia</b>		
TP-01	Wprowadzenie do obsługi incydentów. Omówienie jak wygląda typowy atak i czym jest incydent.	x	1 (RL)	IT_W01 IT_U01 IT_K01
TP-02	Procesy obsługi Incydentów na rzeczywistych przykładach. Uczestnicy będą mieli możliwość poznać typowy proces obsługi incydentu i związane z nim dobre praktyki.	x	4 (RL)	IT_W01 IT_U01 IT_K01
TP-03	Narzędzia wykorzystywane podczas obsługi incydentu. Uczestnicy będą mieli możliwość zapoznać się z typowymi narzędziami wspomagającymi obsługę incydentów na przygotowanych przykładach. Narzędzia obejmowały będą zarówno rozwiązania lokalne jak i dostępne online.	x	5 (RL)	IT_W01 IT_U01 IT_K01
		<b>laboratorium</b>		
TP-04	Obsługa incydentu bezpieczeństwa w oparciu o systemy teleinformatyczne. Ćwiczenie mające na celu kompleksową obsługę incydentu od wykrycia alarmu, przez analizę, a kończąc na raporcie.	x	5 (RL, ŁK)	IT_W01 IT_U01 IT_K01

#### ZALECANA LITERATURA (w tym pozycje w języku obcym)

##### Literatura podstawowa przedmiotu (powinna być dostępna dla studenta w uczelnianej bibliotece):

- Don Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter Paperback, 2019 r.
- Don Murdoch, Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder, 2014 r.

##### Literatura uzupełniająca przedmiotu:

- Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone;  
NIST Special Publication 800-61 Revision 2 - Computer Security Incident Handling Guide
- Patrick Kral, The Incident Handlers Handbook, - SANS Institute

#### INFORMACJA O PRZEWIDYWANEJ MOŻLIWOŚCI WYKORZYSTANIA E-LEARNINGU

-

### III. INFORMACJE DODATKOWE

Odniesienie efektów uczenia się przypisanych do zajęć i treści programowych do form zajęć i metod oceniania

**Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć, powinny być zróżnicowane w zależności od kategorii, tj. inne dla kategorii wiedza i inne dla kategorii umiejętności i kompetencje społeczne.**

\* np. wykład podający, wykład problemowy, ćwiczenia oparte na wykorzystaniu różnych źródeł wiedzy

# np. egzamin ustny, test, prezentacja, projekt

Symbol efektu uczenia się przypisanego do zajęć	Symbol treści programowych realizowanych w trakcie zajęć	Formy zajęć i metody dydaktyczne prowadzenia zajęć umożliwiające osiągnięcie założonych efektów uczenia się *	Metody weryfikacji osiągnięcia efektów uczenia się przypisanych do zajęć #
<b>WIEDZA</b>			
IT_W01	TP-01, TP-02, TP-03, TP-04	Ćwiczenia, laboratorium, studium przypadków	Zaliczenie z oceną – realizacja projektu
<b>UMIĘJĘTNOŚCI</b>			
IT_U01	TP-01, TP-02, TP-03, TP-04	Ćwiczenia, laboratorium, studium przypadków	Zaliczenie z oceną – realizacja projektu
<b>KOMPETENCJE SPOŁECZNE</b>			
IT_K01	TP-01, TP-02, TP-03, TP-04	Ćwiczenia, laboratorium, studium przypadków	Zaliczenie z oceną – realizacja projektu

**MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ**

(godziny)

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności *
Godziny zajęć (według harmonogramu) z nauczycielem	15
w tym liczba godzin z praktyk zawodowych realizowanych w uczelni (według harmonogramu)	-
Praca własna studenta #	<ul style="list-style-type: none"><li>▪ przygotowanie do zajęć, w tym realizacja projektu (25 godzin)</li><li>▪ przygotowanie do zajęć (10 godzin)</li></ul>
<b>SUMA GODZIN</b>	<b>50</b>

**MIARA ŚREDNIEGO NAKŁADU PRACY STUDENTA NIEZBĘDNA DO UZYSKANIA EFEKTÓW UCZENIA SIĘ (punkty ECTS)**

		Liczba punktów ECTS *	
SUMARYCZNA LICZBA PUNKTÓW ECTS PRZYPI- SANYCH DO ZAJĘĆ	Praca studenta wymagająca bezpośredniego kontaktu z nauczycielem akademickim	2	1,2
	Liczba punktów ECTS przypisana praktykom zawodowym, jeśli formą zajęć dla tego przedmiotu są praktyki zawodowe		-
	Praca własna studenta		0,8

\* godziny lekcyjne, czyli 1 godz. oznacza 45 min.

# przykładowe formy aktywności: (1) przygotowanie do zajęć, (2) opracowanie wyników, (3) czytanie wskazanej literatury, (4) napisanie raportu z zajęć, (5) przygotowanie do egzaminu,...

#### **KRYTERIA OCENIANIA I WYMAGANIA EGZAMINACYJNE**

##### **Ćwiczenia:**

Na ocenę dostateczną student ma podstawową wiedzę i potrafi omówić jak wygląda typowy atak i czym jest incydent.

Na ocenę dobrą student ma podstawową wiedzę i potrafi omówić jak wygląda typowy atak i czym jest incydent, opisać narzędzia wykorzystywane podczas obsługi incydentu.

Na ocenę dostateczną student ma podstawową wiedzę i potrafi omówić jak wygląda typowy atak i czym jest incydent, opisać narzędzia wykorzystywane podczas obsługi incydentu, potrafi przedstawić dobre praktyki w zakresie typowych procesów obsługi incydentu.

##### **Laboratorium:**

Na ocenę dostateczną student ma podstawową wiedzę i potrafi scharakteryzować obsługę incydentu od wykrycia alarmu, przez analizę, aż do opracowania raportu.

Na ocenę dostateczną student ma podstawową wiedzę i potrafi scharakteryzować obsługę incydentu od wykrycia alarmu, przez analizę, aż do opracowania raportu, potrafi identyfikować zagrożenie.

Na ocenę dostateczną student ma podstawową wiedzę i potrafi obsługiwać incydenty bezpieczeństwa w oparciu o systemy teleinformatyczne oraz sporządzać raporty.

**Kryteria różnicowania ocen w powiązaniu ze stopniem realizacji efektów uczenia się, muszą być: precyzyjne i czytelne.**

**5. Zasady i formy odbywania praktyk zawodowych (liczba godzin, efekty uczenia się, sposoby weryfikacji założonych efektów uczenia się, sposobów oceny instytucji, w której uczestnicy studiów podyplomowych odbywają praktyki zawodowe).**

Studia podyplomowe nie przewidują praktyk zawodowych.

.....  
(data i podpis Kierownika Studiów Podyplomowych)

.....  
(data i podpis Dyrektora Instytutu)

Do wniosku należy dołączyć:

1. Uchwała Senatu w sprawie ustalenia programu studiów;
2. Kosztorys studiów sporządzony do minimalnej liczby słuchaczy warunkującej samofinansowanie się studiów;
3. W przypadku studiów podyplomowych prowadzonych wspólnie z innymi uczelniami lub instytucjami należy złożyć porozumienie zawarte między jednostkami;
4. Wniosek dyrektora instytutu o powołanie przez Rektora kierownika studiów podyplomowych.

**Opinia Prorektora do spraw Dydaktycznych**

.....  
.....  
.....  
(data i podpis)

**Decyzja Rektora w sprawie utworzenia studiów podyplomowych**

**Wyrażam zgodę/nie wyrażam zgody** na utworzenie studiów podyplomowych

.....  
(data i podpis Rektora PWSTE w Jarosławiu)



