KARTA ZAJĘĆ (SYLABUS)

I. Zajęcia i ich usytuowanie w harmonogramie realizacji programu

1. Jednostka prowadząca kierunek studiów	Instytut Nauk Społecznych i Ochrony Zdrowia
2. Nazwa kierunku studiów	Stosunki transgraniczne
3. Forma prowadzenia studiów	stacjonarne
4. Profil studiów	praktyczny
5. Poziom kształcenia	studia II stopnia
6. Nazwa zajęć	Cyberbezpieczeństwo i bezpieczeństwo informacyjne
7. Kod zajęć	ST.F.6
8. Poziom/kategoria zajęć	zajęcia kierunkowe do wyboru
9. Status zajęć	fakultatywne
10. Usytuowanie zajęć w harmonogramie realizacji zajęć	semestr II
11. Język wykładowy	polski
12. Liczba punktów ECTS	3
13. Koordynator zajęć	
14. Odpowiedzialny za realizację zajęć	dr Tomasz Olejarz

2 Formy zajęć dydaktycznych i ich wymiar w harmonogramie realizacji programu

Wykład W	Ćwiczenia C	Konwersatorium K	Laboratorium L	Projekt P	Praktyka PZ	Inne
30	-	-	-	-	-	-

3. Cele zajęć

Celem przedmiotu jest przekazanie studentom wiedzy teoretycznej i praktycznej w zakresie stosowania technologii informacyjnej, informatycznej w działaniach administracji publicznej z uwzględnieniem bezpieczeństwa danych.

C1 –Student zna i identyfikuje zagrożenia systemów informatycznych i danych w nich przechowywanych oraz ma wiedzę z zakresu praktycznych aspektów bezpieczeństwa w cyberprzestrzeni, z uwzględnieniem determinantów prawno-politycznych i ekonomicznych

C2 –Potrafi analizować typowe problemy bezpieczeństwa informacyjnego i cyberbezpieczeństwa

C3 –Potrafi inicjować działania na rzecz rozwiązywania problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa myśląc i działając w sposób przedsiębiorczy

4. Wymagania wstępne dla studenta w zakresie wiedzy, umiejętności i innych kompetencji.

Brak

5. Efekty uczenia się dla zajęć, wraz z odniesieniem do kierunkowych efektów uczenia się

Lp.	*Opis efektów uczenia się dla zajęć*	*Odniesienie do kierunkowych efektów uczenia się - Identyfikator kierunkowych efektów uczenia się*
K_W01	Ma pogłębioną wiedzę w zakresie identyfikacji zagrożeń systemów informatycznych i danych w nich przechowywanych	K_W03
K_W02	Ma pogłębioną wiedzę na temat prawno-politycznych i ekonomicznych determinantów problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa	K_W04 K_W05
K_U01	Potrafi analizować, syntetyzować i interpretować dane dotyczące zagrożeń bezpieczeństwa informacyjnego i cyberbezpieczeństwa	K_U02
K_U02	Prognozuje zagrożenia bezpieczeństwa informacyjnego i cyberbezpieczeństwa	K_U05
K_K01	Inicjuje działania na rzecz rozwiązywania problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa myśląc i działając w sposób przedsiębiorczy	K_K05

6. Treści kształcenia – oddzielnie dla każdej formy zajęć dydaktycznych (W- wykład, K- konwersatorium, P- projekt, C-ćwiczenia)

Lp.	**Wykład**	**Liczba godzin**
W1	Wprowadzenie do problematyki bezpieczeństwa informacyjnego i cyberbezpieczeństwa. Geneza i rozwój zagrożeń bezpieczeństwa informacyjnego i cyberbezpieczeństwa.	2
W2	Podstawowe informacje o systemach i oprogramowaniach wprowadzanych w administracji państwowej na podstawie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne: *informatyzacja postępowania administracyjnego; informatyzacja jako środek doskonalenia relacji między administracją publiczną a jednostką.*	4
W2	System informatyczny i jego zagrożenia wewnętrzne i zewnętrzne	4
W3	Systemy zarządzania bezpieczeństwem informacji. Infrastruktura przechowywania danych i jej bezpieczeństwo. Przykładowe Sieci konwergentne LAN/SAN i ich niezawodności i awarie.	4
W4	Ciągłość działania systemu informatycznego. Projektowanie bezpiecznej architektury sieci. Model ECNM. Protokoły rodziny STP. Ochrona infrastrukturalna. Gra IT Defender.	4
W5	Sieci lokalne bezprzewodowe. Konstrukcja, architektura, działanie i bezpieczeństwo. Protokoły zdalnego dostępu. Tunelowanie. Protokół SSH	4

W6	Informacja i informatyka a ochrona danych osobowych w administracji publicznej: ochrona danych osobowych – podstawy prawne; ochrona danych osobowych na gruncie Konstytucji; charakterystyka i założenia ustawy o ochronie danych osobowych; ochrona danych osobowych w przepisach szczególnych (usługi drogą elektroniczną, prawo telekomunikacyjne); szczególne problemy prawne ochrony danych osobowych w procesie informatyzacji administracji publicznej.	6
	Razem	**30**

7. Metody weryfikacji efektów uczenia się /w odniesieniu do poszczególnych efektów/

Symbol efektu uczenia się	*Forma weryfikacji*						
	Egzamin ustny	*Egzamin pisemny*	*Kolokwium*	*Projekt*	*Sprawdzian wejściowy*	*Sprawozdanie*	*Inne*
K_W01			X				
K_W02			X				
K_U01							X ocena aktywności
K_U02							X ocena aktywności
K_K01							X ocena aktywności

8. Narzędzia dydaktyczne

Symbol	Forma zajęć
N1 - Metody podające – wykład informacyjny	W1-W6
N2 – Metody poddające - anegdota	W1-W6
N3 –Metody poddające – objaśnienie lub wyjaśnienie	W1-W6
N4 – Metody problemowe – wykład problemowy	W2-W6
N5 – Metody problemowe – wykład konwersatoryjny	W2-W6
N6– Metody eksponujące - film	W2, W3, W4,W5, W6

9. Ocena osiągniętych efektów uczenia się

9.1. Sposoby oceny

Ocena formująca

F1	Kolokwium
F2	Ocena aktywności

Ocena podsumowująca

P1	zaliczenie przedmiotu na podstawie średniej zwykłej (F1+F2)

9.2. Kryteria oceny

symbol efektu uczenia	Na ocenę 3	Na ocenę 3,5	Na ocenę 4	Na ocenę 4,5	Na ocenę 5
W_01;	Ma bardzo podstawową wiedzę w zakresie identyfikacji zagrożeń systemów informatycznych i danych w nich przechowywanych na zaliczenie przedmiotu: 51%-60% pkt.	Ma podstawową wiedzę w zakresie identyfikacji zagrożeń systemów informatycznych i danych w nich przechowywanych zaliczenie przedmiotu: 61%-70% pkt.	Ma średnią wiedzę w zakresie identyfikacji zagrożeń systemów informatycznych i danych w nich przechowywanych zaliczenie przedmiotu: 71%-80% pkt.	Ma zaawansowaną wiedzę w zakresie identyfikacji zagrożeń systemów informatycznych i danych w nich przechowywanych zaliczenie przedmiotu: 81% - 90% pkt.	Ma bardzo zaawansowaną wiedzę w zakresie identyfikacji zagrożeń systemów informatycznych i danych w nich przechowywanych zaliczenie przedmiotu: 91% - 100% pkt.
W_02	Ma bardzo podstawową wiedzę na temat prawno-politycznych i ekonomicznych determinantów problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 51%-60% pkt.	Ma podstawową wiedzę na temat prawno-politycznych i ekonomicznych determinantów problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu:61%-70% pkt.	Ma średnią wiedzę na temat prawno-politycznych i ekonomicznych determinantów problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu71%-80% pkt.	Ma zaawansowaną wiedzę na temat prawno-politycznych i ekonomicznych determinantów problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu:81% - 90% pkt.	Ma bardzo zaawansowaną wiedzę na temat prawno-politycznych i ekonomicznych determinantów problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 91%-100% pkt.
U_01;	Potrafi w bardzo ograniczonym zakresie analizować, syntetyzować i interpretować dane dotyczące zagrożeń bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 51%-60% pkt.	Potrafi w ograniczonym zakresie analizować, syntetyzować i interpretować dane dotyczące zagrożeń bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 61%-70% pkt.	Potrafi w znacznym zakresie analizować, syntetyzować i interpretować dane dotyczące zagrożeń bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 71%-80% pkt.	Potrafi w dużym zakresie analizować, syntetyzować i interpretować dane dotyczące zagrożeń bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 81%-90% pkt.	Potrafi w pogłębiony sposób analizować, syntetyzować i interpretować dane dotyczące zagrożeń bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 91%-100% pkt.
U_02	W bardzo minimalnym stopniu prognozuje zagrożenia bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 51%-60% pkt.	W minimalnym stopniu prognozuje zagrożenia bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 61%-70%	W znacznym stopniu prognozuje zagrożenia bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 71%-80%	W dużym stopniu prognozuje zagrożenia bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 81%-91%	W pogłębionym stopniu prognozuje zagrożenia bezpieczeństwa informacyjnego i cyberbezpieczeństwa zaliczenie przedmiotu: 91%-100%

K_01;	Inicjuje w bardzo niewielkim stopniu działania na rzecz rozwiązywania problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa	Inicjuje w niewielkim stopniu działania na rzecz rozwiązywania problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa	Inicjuje w znacznym stopniu działania na rzecz rozwiązywania problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa myśląc i działając w sposób przedsiębiorczy	Inicjuje w dużym stopniu działania na rzecz rozwiązywania problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa myśląc i działając w sposób przedsiębiorczy	Inicjuje w bardzo dużym stopniu działania na rzecz rozwiązywania problemów bezpieczeństwa informacyjnego i cyberbezpieczeństwa myśląc i działając w sposób przedsiębiorczy

10. Literatura podstawowa i uzupełniająca

Literatura podstawowa:

1. Ganczar M., Informatyzacja *administracji publicznej*, CeDeWu Sp. z o.o., Warszawa 2009.
2. Hoc S., *Karnoprawna ochrona informacji*, Wyd. Uniwersytetu Opolskiego, Opole 2012.
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r., w sprawie Biuletynu Informacji Publicznej
4. Zalewski S., *Ochrona informacji niejawnych – wybrane zagadnienia bezpieczeństwa osobowego,* Płock 2014.

Literatura uzupełniająca:

1. Kamińska I. Rozbicka-Ostrowska M. *Ustawa o dostępie do informacji publicznej. Komentarz*, LexisNexis 2012.
2. OlakA., *Współczesnezagrożenia. Rola telewizji i Internetu w życiu młodzieży. Zarys problematyki*, AMELIA Rzeszów 2012.
3. Ustawa z dnia 10 maja 2018 r., o ochronie danych osobowych
4. Ustawa z dnia 17 lutego 2005 r., o informatyzacji działalności podmiotów realizujących zadania publiczne.
5. Ustawa z dnia 29 czerwca 20018 r., o dostępie do informacji publicznej.

11. Macierz realizacji zajęć

Symbol efektu kształcenia	Odniesienie efektu do efektów zdefiniowanych dla programu	Cele Przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
K_W01	K_W03	C1	W1-W6	N1, N4, N5,	F1
K_W02	K_W04 K_W05	C1	W1-W6	N1, N2, N3, N4, N5, N6	F1
K_U01	K_U02	C1, C2	W1-W6	N1, N4, N5	F1, F2
K_U02	K_U05	C1, C2	W1-W6	N1, N4, N5	F1, F2
K_K01	K_K05	C3	W1-W6	N1, N4, N5	F2

12. Obciążenie pracą studenta

Forma aktywności	**Średnia liczba godzin na zrealizowanie aktywności**
Udział w wykładach	30
Udział w ćwiczeniach	-
Udział w konwersatoriach/laboratoriach/projektach	-
Udział w praktyce zawodowej	-
Udział nauczyciela akademickiego w egzaminie	-
Udział w konsultacjach	-
Suma godzin kontaktowych	**30**
Samodzielne studiowanie treści wykładów	22
Samodzielne przygotowanie do zajęć kształtujących umiejętności praktyczne	-
Wykonanie projektu	-
Przygotowanie do egzaminu i kolokwiów	22
Suma godzin pracy własnej studenta	**44**
Sumaryczne obciążenie studenta	**74**
Liczba punktów ECTS za przedmiot	**3**
Obciążenie studenta zajęciami kształtującymi umiejętności praktyczne	-
Liczba punktów ECTS za zajęcia kształtujące umiejętności praktyczne	-

13. Zatwierdzenie karty przedmiotu do realizacji.

Odpowiedzialny za przedmiot: **Dyrektor Instytutu:**

Przemyśl, dnia 07.03.2022