

KARTA PRZEDMIOTU

I. OGÓLNE INFORMACJE O PRZEDMIOCIE						
PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA IM. WITELONA W LEGNICY WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH						
Kierunek studiów:		BEZPIECZEŃSTWO WEWNĘTRZNE				
Profil studiów:		Praktyczny				
Forma studiów:		Stacjonarne/niestacjonarne				
Nazwa przedmiotu:		Bezpieczeństwo informatyczne				
Język wykładowy:		Język polski				
Kod przedmiotu kształcenia:		BW2AB01				
Poziom studiów:		II stopień				
Rok studiów:	II	Formy prowadzenia zajęć i liczba godzin w planie studiów:				
Semestr:	3	Wykład	Ćwiczenia	Warsztaty	Seminarium	Praktyka zawodowa
Liczba punktów ECTS:	3	14/8	-	20/10	-	-
Forma zaliczenia:		Zaliczenie na ocenę				
Wymagania wstępne w zakresie wiedzy oraz umiejętności:		Wiedza na poziomie studiów licencjackich w zakresie nauk społecznych				
II. CELE KSZTAŁCENIA						
Cele kształcenia:						
C1 – Wyposażyć studenta w odpowiednią aparaturę pojęciową adekwatną do wybranych teorii badania bezpieczeństwa pozamilitarnego oraz zapoznać go z naukowymi metodami poszukiwania i przetwarzania informacji w celu analizowania zjawisk w sferze bezpieczeństwa – kształtowania sektorowych strategii tego bezpieczeństwa; C2 – Nabycie przez studentów wiedzy dotyczącej zagadnień w zakresie zagrożeń związanych z funkcjonowaniem systemów informatycznych, które mają bezpośredni wpływ na bezpieczeństwo: światowe, państwowe, korporacyjne, ludzkie, itd. Rozpoznawania przestępczości zorganizowanej oraz penalizacji cyberprzestępstw C3 – Pozyskanie niezbędnej wiedzy dotyczącej: unikania zidentyfikowanych zagrożeń, działań prewencyjnych, budowy systemów ochrony oraz reagowania na zaistniałe incydenty.						
III. PRZEDMIOTOWE EFEKTY UCZENIA SIĘ WRAZ Z ODNIESIENIEM DO EFEKTÓW KIERUNKOWYCH ORAZ METODY WERYFIKACJI EFEKTÓW						
Efekt	Student, który zaliczył przedmiot w zakresie:			Odniesienie do efektów kierunkowych	Metody weryfikacji	
wiedzy:						
W01	Student ma pogłębioną wiedzę w zakresie zasad ochrony informacji niejawnej i wrażliwej oraz obiegu dokumentacji, utrzymaniu bezpieczeństwa informacyjnego oraz zastosowania praktycznego tej wiedzy w działalności zawodowej;			K_W09	esej lub prezentacja na wybrane tematy dotyczące bezpieczeństwa systemów informatycznych	
umiejętności:						
U01	Student potrafi samodzielnie planować własne uczenie się, organizować swoją pracę, rozwiązywać problemy, gromadzić, przetwarzać oraz udostępniać informacje z wykorzystaniem nowoczesnych technologii informatycznych a także zastosować praktyczne nabyte umiejętności do tworzenia, rozwoju form indywidualnej przedsiębiorczości, wykorzystując wiedzę z zakresu nauk o bezpieczeństwie;			K_U08	odpowiedź ustna na podstawie analizy literatury przedmiotu, ocena prowadzenia merytorycznej dyskusji, ocena realizacji zadań przygotowanych w ramach warsztatów	

U02	Student potrafi wykorzystywać posiadaną wiedzę do właściwego doboru źródeł i informacji z nich pochodzących, dokonywania oceny, krytycznej analizy, syntezy, twórczej interpretacji i prezentacji tych informacji oraz komunikowania się tematy specjalistyczne z odbiorcami i prowadzenia debaty a także zastosować praktyczne umiejętności w działalności zawodowej;	K_U09	odpowiedź ustna na podstawie analizy literatury przedmiotu, ocena prowadzenia merytorycznej dyskusji, ocena realizacji zadań przygotowanych w ramach warsztatów
U03	Student potrafi wykorzystywać posiadaną wiedzę do ochrony informacji przed nieuprawnionym ujawnieniem, niezależnie od formy i sposobu ich wyrażania, także w trakcie opracowywania oraz posługiwać się specjalistyczną terminologią w zakresie informacji objętych klauzulami niejawności a także zastosować praktyczne umiejętności w działalności zawodowej	K_U10	odpowiedź ustna na podstawie analizy literatury przedmiotu, ocena prowadzenia merytorycznej dyskusji, ocena realizacji zadań przygotowanych w ramach warsztatów
kompetencji społecznych:			
K01	Student jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści;	K_K01	ocena realizacji zadań przygotowanych w ramach ćwiczeń, ocena zaangażowania w pracę grupy, ocena zachowań i aktywności w trakcie wykładów i ćwiczeń, ocena prowadzenia merytorycznej dyskusji
IV. TREŚCI KSZTAŁCENIA			
Treści kształcenia (tematyka zajęć, zaprezentowana z podziałem na poszczególne formy zajęć z określeniem liczby godzin potrzebnych na ich realizację)			
Wykłady:			
Kod	Tematyka zajęć	Liczba godzin	
W1	- Środowisko systemów informatycznych – cyberprzestrzeń - Cechy cyberprzestrzeni (omówienie) - Różne ujęcia cyberprzestrzeni (w zależności od dziedziny nauki) - Zasadnicze elementy cyberprzestrzeni - Różnice w podejściu do definiowania cyberprzestrzeni w różnych krajach i instytucjach - Definicja cyberprzestrzeni według polskiego prawa - Rola systemów informatycznych w obszarze bezpieczeństwa państwa - Materiały Ministerstwa Rozwoju, Pracy i Technologii (dawniej Ministerstwa Cyfryzacji) na temat systemów informatycznych	4/2	
W2	- Ministerstwo Rozwoju, Pracy i Technologii (dawniej Ministerstwo Cyfryzacji) podstawy prawne - Wizja, misja, wartości Ministerstwa Rozwoju, Pracy i Technologii (dawniej Ministerstwa Cyfryzacji) - Zadania Ministerstwa Rozwoju, Pracy i Technologii (dawniej Ministerstwa Cyfryzacji) - Współpraca międzynarodowa Ministerstwa Rozwoju, Pracy i Technologii (dawniej Ministerstwa Cyfryzacji) - Działania Departamentu Cyberbezpieczeństwa Ministerstwa Rozwoju, Pracy i Technologii (dawniej Ministerstwa Cyfryzacji) - Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polski na lata 2017-2022 - Ustawa o krajowym systemie cyberbezpieczeństwa - Strategia Krajowego Systemu Cyberbezpieczeństwa	2/1	

W3	- Definicje określone przez Ustawę Krajowy System Cyberbezpieczeństwa - Jednostki reagujące na incydenty w systemach informatycznych - Określenie incydentu w cyberprzestrzeni - Ilość i podział incydentów - Działania mające na celu wzmocnienie bezpieczeństwa użytkowników systemów informatycznych - Poradniki Ministerstwa Rozwoju, Pracy i Technologii (dawniej Ministerstwa Cyfryzacji) przybliżające problematykę bezpieczeństwa informatycznego oraz ułatwiające wdrażanie obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa - Projekt Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 Ministerstwa Rozwoju, Pracy i Technologii (dawniej Ministerstwa Cyfryzacji) i jej główne cele	2/1
W4	- Rządowe Programy Ochrony Cyberprzestrzeni - Definicje przestępczości informatycznej według Interpolu, Rady Europy, Unii Europejskiej, ONZ - Rodzaje przestępstw związanych z użytkowaniem systemów informatycznych - Przestępstwa charakterystyczne dla cyberprzestępczości - Przestępstwa popełniane z wykorzystaniem sieci Internet - Najważniejsze cechy przestępczości informatycznej - Zagrożenia asymetryczne - Penalizacja przestępstw informatycznych - Penalizacja przestępstw informatycznych – treści pornograficzne w tym z udziałem małoletnich - Pornografia dziecięca w ujęciu Konwencji RE – art. 9 - Nawoływanie do nienawiści na tle rasowym i treści ksenofobiczne, obrażanie uczuć religijnych - Groźby karalne, zmuszanie do określonego zachowania, cyberstalking, kradzież tożsamości i inne przestępstwa - Regulacje prawne ujęte w kodeksie wykroczeń	4/2
W5	- Prawo do bycia zapomnianym w Internecie - Geneza - Rozporządzenie unijnego RODO (art. 17 ust. 1) - Warunki usunięcia danych - Wyjątki od konieczności egzekwowania przez Administratora prawa do bycia zapomnianym - Kopie stron internetowych - Procedura usuwania danych z kopii stron z serwisu Google - Archiwa stron internetowych - „Maszyna czasu” – cele - Dowody sądowe z archiwów stron internetowych	2/2
Warsztaty:		
Kod	Tematyka zajęć	Liczba godzin
WT1	- Podstawowe pojęcia dotyczące sieci komputerowych - Budowa sieci lokalnych - Budowa i złożoność Internetu - Przykładowe pojęcia słownika informatycznego – zagrożenia i przestępstwa - Przykładowe pojęcia słownika informatycznego – stan zagrożenia - Jak reagować na przemoc seksualną względem dziecka w sieci – gdzie zgłaszać i jak się zachować - Jak reagować na przemoc seksualną względem dziecka w sieci – omówienie przypadków - Czym jest chmura i czy można mieć do niej zaufanie? - Ogólne zasady bezpieczeństwa i higieny cyfrowej – komputer, tablet, telefon, router sieci Wi-Fi, postępowanie własne - Bezpieczne hasła – podstawowe zasady, blokady urządzeń, klawiatury wirtualne - Programy peer-to-peer (P2P)	4/2
WT2	- Pozyskiwanie danych - Biały wywiad – jakie informacje pozostawiamy w cyberprzestrzeni - Czym jest biały wywiad - Czego wyszukujemy w internecie - Istotne elementy białego wywiadu internetowego - Słowa kluczowe - Znaczenie parametrów wyszukiwania - Jak tworzyć słowa kluczowe - Najważniejsze pytania przy definiowaniu zagadnienia do opracowania - Wykorzystanie operatorów logicznych - Operatory inne - Szukanie zaawansowane - Możliwości serwisu Google - Przykładowe ćwiczenia do pracy własnej	4/2

WT3	- Zapewnienie bezpieczeństwa informatycznego przez Policję - Struktura Biura i Wydziałów do Walki z Cyberprzestępczością - Zadania Biura do Walki z Cyberprzestępczością Komendy Głównej Policji - Zadania Wydziałów do Walki z Cyberprzestępczością Komend Wojewódzkich Policji - Zwalczanie cyberprzestępczości przez funkcjonariuszy Centralnego Laboratorium Kryminalistycznego Policji oraz Laboratoriów Kryminalistycznych Komend Wojewódzkich Policji - Zadania pracowni do badań informatycznych Laboratoriów Kryminalistycznych Komend Wojewódzkich Policji - Zadania wspólne Wydziałów do Walki z Cyberprzestępczością oraz Laboratoriów Kryminalistycznych	2/1
WT4	- Polityka bezpieczeństwa – definicja, etapy tworzenia - Zarządzanie, monitorowanie i konserwacja – jako proces - Zakres Polityki Bezpieczeństwa - Normy i wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Inne akty prawne obowiązujące w Polsce związane z polityką bezpieczeństwa - Omówienie przykładowej Polityki Bezpieczeństwa	2/1
WT5	- System informatyczny – definicje, elementy składowe - Podstawowe cele bezpieczeństwa informacji i systemów informatycznych - Zarządzani ryzykiem w systemach informatycznych - Określenie strategii bezpieczeństwa systemów informatycznych - Identyfikacja zasobów do ochrony - „Co chronić?” - Identyfikacja zagrożeń wystąpienia incydentu - „Przed czym chronić?” - Systemy zabezpieczeń – Podstawowe definicje - Zasady tworzenia systemu zabezpieczeń - Wielowarstwowe systemy zabezpieczeń – zalety i zagrożenia - Ogólne własności bezpieczeństwa C I A – zagrożenia i mechanizmy obrony	4/2
WT6	- Główne zagrożenia związane z wykorzystaniem systemów informatycznych - Rodzaje zagrożeń, historia, podział, omówienie rodzajów - Socjotechnika w cyberprzestrzeni, fałszywe poczucie bezpieczeństwa, obszary działania - Analiza przykładów zidentyfikowanych incydentów w systemach informatycznych	2/1
WT7	- Zasady bezpieczeństwa stosowane w systemach informatycznych - Kto, jak i jakie dane wprowadza do systemów informatycznych - Oszustwa w Internecie, typy, metody działania - Podstawowe zasady bezpieczeństwa przy wykorzystaniu komputerów stacjonarnych, urządzeń mobilnych, urządzeń USB, inteligentnych urządzeń, - Zasady bezpiecznego korzystania, budowy i przechowywania haseł	2/1

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. Metody kształcenia: wykład informacyjny (konwencjonalny), wykład konwersatoryjny, pokaz, burza mózgów, ćwiczenia praktyczne, ćwiczeniowa oparta na wykorzystaniu różnych źródeł wiedzy, dyskusja, analiza literatury przedmiotu, metoda projektów.

2. Narzędzia (środki) dydaktyczne: prezentacje multimedialne, podręczniki, Internet, rzutniki multimedialne.

VI. FORMA I KRYTERIA ZALICZENIA PRZEDMIOTU

Forma zaliczenia przedmiotu. Kryteria oceny formującej:

1. Realizacja zleconego eseju lub prezentacji multimedialnej na temat „Środowisko pracy systemów informatycznych – cyberprzestrzeń - cechy i zagrożenia”.
2. Samodzielne wykonanie ćwiczeń warsztatowych.

Obserwacja i ocena postaw studenta wynikających z:

- Realizacji zadań przygotowanych w ramach warsztatów,
- Zaangażowania w pracę grupy,
- Zachowań i aktywności w trakcie wykładów i warsztatów,
- Prowadzenia merytorycznej dyskusji,
- Potrzeby ciągłego rozwoju osobistego i zawodowego.

Kryteria oceny podsumowującej:

- Średnia ocen formujących

VII. BILANS PUNKTÓW ECTS - NAKŁAD PRACY STUDENTA	
Kategoria	Obciążenie studenta
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	34/18
Udział w wykładach	14/8
Udział w ćwiczeniach, warsztatach	20/10
Udział w seminarium	
Udział w egzaminie	
Inne (jakie?)	
Samodzielna praca studenta (godziny niekontaktowe)	41/57
Przygotowanie do wykładu	
Przygotowanie do ćwiczeń, warsztatów,	20/30
Przygotowanie do kolokwium zaliczeniowego	
Przygotowanie do egzaminu	
Przygotowanie do seminarium	
Gromadzenie materiałów do projektu	10/16
Kwerenda internetowa	10/10
Opracowanie prezentacji multimedialnej	1/1
Przygotowanie do praktyki zawodowej	
Inne (jakie?)	
Łączna liczba godzin	75
Punkty ECTS za przedmiot	3
VIII. LITERATURA PRZEDMIOTU	
Literatura podstawowa: William Stallings, Lawrie Brown – Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 1; wyd. Helion 2019, K. Linderman – Bezpieczeństwo informacyjne. Nowe wyzwania; wyd. PWN SA, Warszawa 2017 A. Gałach, S. Hoc, A. Jędruszczak, K. Kędzierska, P. Kowalik, A. Kuszel, M. Kuźma, R. Marek, B. Nowakowski - Ochrona danych osobowych i informacji niejawnych w sektorze publicznym; Wyd. C. H. Beck, 2015	
Literatura uzupełniająca: Praca zbiorowa pod red. J. Kosińskiego – Przestępczość teleinformatyczna; Wyd. WSPol Szczytno 2015 T. Trejderowski – Kradzież tożsamości: terroryzm informatyczny: cyberprzestępstwa, internet, telefon, Facebook; wyd. Eneteia Wydawnictwo Psychologii i Kultury, Warszawa 2013	