KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE								
PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA IM. WITELONA W LEGNICY WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH								
Kierunek studiów:		Bezpieczeństwo wewnętrzne						
Poziom studiów:		drugiego stopnia						
Profil studiów:		praktyczny						
Forma studiów:		stacjonarne/niestacjonarne						
Nazwa modułu:		**Bezpieczeństwo informatyczne**						
Rodzaj modułu:		obowiązkowy						
Język wykładowy:		Język polski*						
Rok studiów:	2	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**						
Semestr:	3	Wykłady	Warsztaty	Ćwiczenia	Seminaria	Lektorat	Praktyka zawodowa	**
Liczba punktów ECTS ogółem:	3	14/8	20/10	-	-	-	-	-
Forma zaliczenia:		Zaliczenie						
Wymagania wstępne:		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. EFEKTY UCZENIA SIĘ WRAZ Z ODNIESIENIEM DO EFEKTÓW KIERUNKOWYCH ORAZ METODY WERYFIKACJI EFEKTÓW

Efekt	Student, który zaliczył moduł 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 umiejętnoścido 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	K_U09	odpowiedź ustna na podstawie

	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;		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 PROGRAMOWE

Treści programowe (tematyka zajęć, zaprezentowana z podziałam 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 cybeprzestrzeni - 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 Cyfryzacji na temat systemów informatycznych	4/2
W2	- Ministerstwo Cyfryzacji podstawy prawne - Wizja, misja, wartości Ministerstwa Cyfryzacji - Zadania MinisterstwaCyfryzacji - Współpraca międzynarodowa MinisterstwaCyfryzacji - Działania Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji - Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na latach 2019-2024 - Cele szczegółowe Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na latach 2019-2024	2/1
W3	- Ustawa o krajowym systemie cyberbezpieczeństwa - Strategia Krajowego Systemu Cyberbezpieczeństwa - Definicje określane przez Ustawa 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 - Program Współpracy w Cyberbezpieczeństwie (PWCyber)	2/1

	- Raporty o stanie bezpieczeństwa cyberprzestrzeni RP CSIRT GOV	
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 bezpieczeństwai 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 - 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	2/1

	- Normy i wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Inne akty prawne obowiązujące w Polsce związane z polityką bezpieczeństwa - Omówienie przykładowej Polityki Bezpieczeństwa	
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 poczuciu 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 MODUŁU

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

Ocena podsumowująca:

- średnia ocen z wykładów i warsztatów

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 innych formach zajęć (**)	20/10
Inne (jakie?)	-
Samodzielna praca studenta (godziny niekontaktowe)	**41/57**
Przygotowanie do wykładu	
Przygotowanie do ćwiczeń, warsztatów,	15/25
Gromadzenie materiałów do projektu	8/10

Kwerenda internetowa	8/10
Opracowanie prezentacji multimedialnej	10/12
Łączna liczba godzin	**75**
Punkty ECTS za moduł	**3**

VIII. ZALECANA LITERATURA

Literatura podstawowa:

1. William Stallings, Lawrie Brown – Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 1; wyd. Helion 2019,
2. K. Linderman – Bezpieczeństwo informacyjne. Nowe wyzwania; wyd. PWN SA, Warszawa 2017
3. 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:

1. Praca zbiorowa pod red. J. Kosińskiego – Przestępczość teleinformatyczna; Wyd. WSPol Szczytno 2015
2. T. Trejderowski – Kradzież tożsamości: terroryzm informatyczny: cyberprzestępstwa, internet, telefon, Facebook; wyd. Eneteia Wydawnictwo Psychologii i Kultury, Warszawa 2013