KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE								
COLLEGIUM WITELONA UCZELNIA PAŃSTWOWA WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH								
Kierunek studiów:		Bezpieczeństwo wewnętrzne						
Poziom studiów:		Studia drugiego stopnia						
Profil studiów:		praktyczny						
Forma studiów:		stacjonarne						
Nazwa modułu:		**Bezpieczeństwo w cyberprzestrzeni w ujęciu indywidualnym oraz instytucjonalnym**						
Rodzaj modułu:		moduł kształcenia kierunkowego						
Język wykładowy:		język polski						
Rok studiów:	1	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**						
Semestr:	2	Wykład	Warsztaty	**	**	**	**	**
Liczba punktów ECTS ogółem:	4	24	36	S/N	S/N	S/N	S/N	S/N
Forma zaliczenia:		Egzamin						
Wymagania wstępne:		Znajomość konstytucyjnych organów państwa odpowiedzialnych za bezpieczeństwo wewnętrzne. Znajomość instytucji państwowych odpowiedzialnych za zapewnienie porządku publicznego. Znajomość sieci oraz komunikacji interpersonalnej w Internecie.						

II. CELE KSZTAŁCENIA
Cele kształcenia:
Cel 1: Nabycie podstawowej wiedzy w zakresie funkcjonowania globalnych oraz lokalnych sieci oraz zagrożeń wynikających z funkcjonowaniem stosunków międzyludzkich w cyberprzestrzeni. **Cel 2:** Pozyskanie niezbędnej wiedzy w zakresie rozpoznawania zagrożeń w obrębie cyberprzestrzeni, które mają bezpośredni wpływ na bezpieczeństwo: światowe, państwowe, korporacyjne, ludzkie, tworzenia polityk bezpieczeństwa z uwzględnieniem specyfiki systemu informatycznego. **Cel 3:** Pozyskanie niezbędnej wiedzy dotyczącej rozpoznawania przestępczości zorganizowanej, penalizacji cyberprzestępstw, efektywnej współpracy z organami powołanymi do zapewnienia bezpieczeństwa i zwalczania przestępczości w cyberprzestrzeni.

III. EFEKTY UCZENIA SIĘ WRAZ Z ODNIESIENIEM DO EFEKTÓW KIERUNKOWYCH		
Efekt uczenia się	Student, który zaliczył moduł w zakresie:	Odniesienie do efektów kierunkowych
wiedzy:		

W01	student zna i rozumie znaczenie nauk o bezpieczeństwie oraz powiązanych z nimi nauk prawnych, nauk o zarządzaniu, jakości, polityki i administracji w kontekście funkcjonowania państwa, ze szczególnym uwzględnieniem uwarunkowań instytucjonalnych, systemowych i prawnych bezpieczeństwa wewnętrznego i zewnętrznego oraz potrafi odnieść tę wiedzę do praktyki zawodowej.	K2BW_W02
W02	student zna i rozumie systemy, procesy oraz uwarunkowania działalności w obszarze bezpieczeństwa społecznego, politycznego, ekonomicznego i gospodarczego, w tym strukturę instytucji odpowiedzialnych za zapewnienie bezpieczeństwa oraz praktyczne zastosowanie tej wiedzy.	K2BW_W04

W03	student zna i rozumie rodzaje oraz źródła zagrożeń bezpieczeństwa, a także procesy determinujące ich powstawanie, eskalację, identyfikację i neutralizację, zarówno w ujęciu rzeczywistym, jak i potencjalnym, z uwzględnieniem ich znaczenia dla działalności zawodowej.	K2BW_W05
W04	student zna i rozumie organizację oraz zasady funkcjonowania państwa w zakresie budowania i utrzymywania bezpieczeństwa ochronnego i obronnego, a także uwarunkowania prawne i organizacyjne tych działań oraz ich praktyczne implikacje.	K2BW_W07
umiejętności:		
U01	student potrafi wykorzystać wiedzę teoretyczną do pogłębionego opisu oraz analizy zjawisk i procesów zachodzących w obszarze nauk o bezpieczeństwie, prawa, zarządzania, polityki i administracji, a także formułować samodzielne, uzasadnione opinie.	K2BW_U01
U02	student potrafi stosować zasady, metody oraz środki techniczne służące rozpoznawaniu i wykrywaniu negatywnych zjawisk społecznych o charakterze prawnym, a także analizować powiązania między osobami i zdarzeniami w kontekście działań zawodowych.	K2BW_U14
U03	student potrafi wykorzystywać dostępne techniki, metody i systemy w zakresie zapobiegania przestępczości, wykrywania zagrożeń oraz organizacji bezpiecznych zgromadzeń i imprez masowych, z uwzględnieniem praktycznych aspektów bezpieczeństwa.	K2BW_U15
kompetencji społecznych:		
K01	student jest gotów do krytycznej oceny posiadanej wiedzy, analizowania odbieranych treści oraz ciągłego doskonalenia kompetencji osobistych i zawodowych w obszarze bezpieczeństwa.	K2BW_K01

IV. TREŚCI PROGRAMOWE

Treści programowe (tematyka zajęć, zaprezentowana z podziałam na poszczególne formy zajęć z określeniem liczby godzin potrzebnych na ich realizację)

Wykład

Kod	Tematyka zajęć	Liczba godzin S
W1	Cyberprzestrzeń - pojęcie i zakres znaczeniowy, podstawowe cechy oraz elementy cyberprzestrzeni, definicja cyberprzestrzeni w świetle prawa polskiego, znaczenie definicji dla systemu bezpieczeństwa państwa, omówienie karty modułu, zasad zaliczenia oraz form weryfikacji efektów uczenia się.	4
W2	Ministerstwo Cyfryzacji - podstawy prawne, wizja, misja, wartości, zadania, współpraca międzynarodowa, Departament Cyberbezpieczeństwa, Strategia Cyberbezpieczeństwa Rzeczypospolitej, cele szczegółowe Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.	4
W3	Ustawa o krajowym systemie cyberbezpieczeństwa, określenie incydentu w cyberprzestrzeni ilość i podział incydentów, jednostki reagujące na incydenty w systemach informatycznych, Program Współpracy w Cyberbezpieczeństwie (PWCyber).	4

W4	Rządowe Programy Ochrony Cyberprzestrzeni, definicje przestępczości informatycznej według Interpolu, Rady Europy, Unii Europejskiej, ONZ, rodzaje przestępstw związanych z użytkowaniem systemów informatycznych, ich cechy, przestępstwa charakterystyczne dla cyberprzestępczości, penalizacja przestępstw informatycznych, zagrożenia asymetryczne, pornografia dziecięca w ujęciu Konwencji RE – art. 9 .	4
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	4
W6	Kopie i archiwa stron internetowych, „Maszyna czasu" – cele, dowody sądowe z archiwów stron internetowych.	4
Warsztaty		
Kod	Tematyka zajęć	Liczba godzin S
WT1	Zapewnienie autentyczności i integralności zapisów cyfrowych, funkcja skrótu, praktyczne wykorzystanie oprogramowania haszującego.	6
WT2	Podstawowe pojęcia dotyczące sieci komputerowych, budowa i złożoność Internetu, budowa sieci lokalnych, przykładowe pojęcia słowniczka cyberbezpieczeństwa, zagrożenia i przestępstwa, reagowanie na przemoc seksualną względem dziecka w sieci, gdzie zgłaszać i jak się zachować, omówienie przypadków, ogólne zasady bezpieczeństwa i higieny cyfrowej, bezpieczne hasła, programy peer-to-peer (P2P).	6
WT3	Instytucje powołane do zapewnienia cyberbezpieczeństwa, zwalczania cyberprzestępczości, struktura, zadania, kanały komunikacji.	6
WT4	Polityka bezpieczeństwa – definicja, etapy tworzenia, zarządzanie, monitorowanie i konserwacja, zakres, akty prawne obowiązujące w Polsce związane z polityką bezpieczeństwa, omówienie przykładowej Polityki Bezpieczeństwa.	5
WT5	Pozyskiwanie danych - biały wywiad, czym jest, czego szukamy, słowa kluczowe, parametry, operatory.	6
WT6	Bezpieczeństwo osobiste w cyberprzestrzeni, omówienie i konfigurowanie parametrów prywatności, rodzaje i podział zagrożeń, socjotechnika w cyberprzestrzeni, fałszywe poczucie bezpieczeństwa, analiza przykładów zidentyfikowanych incydentów w systemach informatycznych.	7

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. Metody kształcenia: wykład informacyjny, warsztaty oparte na wykorzystaniu różnych źródeł wiedzy, dyskusja.
2. Narzędzia (środki) dydaktyczne: wykład informacyjny, warsztaty oparte na wykorzystaniu różnych źródeł wiedzy, dyskusja.

VI. FORMA I KRYTERIA ZALICZENIA MODUŁU

1. Formy zaliczenia:

- egzamin

2. Sposób weryfikacji i oceniania efektów uczenia się:

1. Wykład – Egzamin – kryteria oceny:

- posiada podstawowe na temat funkcjonowania systemu zarządzania kryzysowego - ocena dostateczna,
- posiada podstawowe informacje na temat funkcjonowania systemu zarządzania kryzysowego i potrafi wymienić jego elementy składowe - ocena dostateczna plus,
- ma rozbudowaną wiedzę na temat funkcjonowania systemu zarządzania kryzysowego, w tym potrafi wskazać zależności między wybranymi organami administracji publicznej - ocena dobra,
- ma rozbudowaną wiedzę na temat funkcjonowania systemu zarządzania kryzysowego, w tym potrafi wskazać zależności między wybranymi organami administracji publicznej, a także wpływ otoczenia zewnętrznego i wewnętrznego na właściwe funkcjonowanie systemu - ocena dobra plus,
- ma rozbudowaną wiedzę na temat funkcjonowania systemu zarządzania kryzysowego, w tym potrafi wskazać zależności między wybranymi organami administracji publicznej, a także dokonywać praktycznej analizy jego funkcjonowania - ocena bardzo dobra.

2. Warsztaty – Przygotowanie prezentacji, kolokwium:

- **3,0 (dostateczny)** – przygotowanie i prezentacja na forum grupy,
- **3,5 (dostateczny plus)** – przygotowanie i prezentacja na forum prezentacji oraz znajomość literatury źródłowej,
- **4,0 (dobry)** – przygotowanie i prezentacja na forum prezentacji oraz znajomość literatury źródłowej, umiejętność analizy
  i syntezy treści źródłowych,
- **4,5 (dobry plus)** – przygotowanie i prezentacja na forum prezentacji oraz znajomość literatury źródłowej, umiejętność analizy i syntezy treści źródłowych, poprawność wnioskowania,
- **5,0 (bardzo dobry)** – przygotowanie i prezentacja na forum prezentacji oraz znajomość literatury źródłowej, umiejętność analizy i syntezy treści źródłowych, poprawność wnioskowania, pomysłowość proponowanych rozwiązań. Test wiedzy:
- 51% - 60% - ocena dostateczna,
- 61% - 70% - ocena dostateczna plus,
- 71% - 80% - ocena dobra,
- 81% - 90% - ocena dobra plus,
- 91% - 100% - ocena bardzo dobra.

3. 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.

Podstawowe kryteria oceny lub wymagania egzaminacyjne określane są indywidualnie, jednak powinny zachować adekwatność wobec zaplanowanych efektów uczenia się

VII. BILANS PUNKTÓW ECTS - NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	**60**
Udział w wykładach	24
Udział w innych formach zajęć (**)	36
Samodzielna praca studenta (godziny niekontaktowe)	**40**
Przygotowanie do wykładu	8
Przygotowanie do innych form zajęć (**)	10
Przygotowanie do egzaminu	22
Przygotowanie do zaliczenia innych form zajęć (**)	0

Łączna liczba godzin	**100**
Punkty ECTS za moduł	**4**

VIII. ZALECANA LITERATURA

Literatura podstawowa:

1. J. Kluczewski, *Bezpieczeństwo sieci komputerowych, praktyczne przykłady i ćwiczenia w symulatorze Cisco Packet,* Itstart Wydawnictwo Informatyczne, 2019.
2. J. Krawiec, Cyberbezpieczeństwo: *podejście systemowe,* Warszawa, Oficyna Wydawnicza Politechniki Warszawskiej, 2019.
3. P. Dela, *Teoria walki w cyberprzestrzeni*; Akademia Sztuki Wojennej, Warszawa 2020.

Literatura uzupełniająca:

1.A. Jamil, *Cyberbezpieczeństwo we współczesnych konfliktach na Bliskim Wschodzie*, FNCE Wydawnictwo, 2019.
2. R. Szpyra*, Cyberbezpieczeństwo militarne w amerykańskiej praktyce*, Oficyna Wydawnicza Politechniki Warszawskiej, 2019.
3. D. Szeligiewicz- Urban, B. Matusek., *Cyberprzestrzeń miejscem skutecznego nauczania-uczenia się*, Oficyna Wydawnicza "Humanitas". Pbl, 2021.