KARTA PRZEDMIOTU

Nazwa przedmiotu w języku polskim: **CYBERPRZESTĘPCZOŚĆ W PRAWIE KARNYM**		*Kod przedmiotu:* **KNS/BW-IIP/BC/58**
Nazwa przedmiotu w języku angielskim: **CYBERCRIME IN CRIMINAL LAW**		
Kierunek studiów: **Bezpieczeństwo wewnętrzne**	*Profil:* **praktyczny**	*Poziom studiów:* **II stopień**
Specjalność/specjalizacja: **Bezpieczeństwo cyberprzestrzeni**	*Forma zaliczenia przedmiotu:* **zaliczenie na ocenę**	*Semestr studiów:* **3**
Nazwa grupy zajęć: **zajęcia specjalnościowe**	*Język w jakim prowadzone są zajęcia:* **polski**	

Tryb studiów	*Forma zajęć*							*Ogólna liczba godzin*	*Liczba punktów ECTS:*
	W	*Ćw.*	*Konw.*	*Lab.*	*Proj.*	*Sem.*	*Zajęcia terenowe*		
Tryb stacjonarny	**-**	**-**	**15**	**-**	**15**	**-**	**-**	**30**	**3**
Tryb niestacjonarny	**-**	**-**	**9**	**-**	**9**	**-**	**-**	**18**	

Jednostka realizująca przedmiot, wydział:
Kolegium Nauk Społecznych

Odpowiedzialny za opracowanie karty przedmiotu (tytuł/stopień naukowy, imię i nazwisko, adres e-mail):
dr Arkadiusz P. Szajna, aszajna@wszop.edu.pl

CEL PRZEDMIOTU

C1.	Zapoznanie studentów z zagadnieniami dotyczącymi: wieloaspektowej struktury przestępstwa, podziału typów czynów zabronionych.
C2.	Zapoznanie studentów z wybranymi obszarami wiedzy odnoszącymi się do cyberbezpieczeństwa, cyberprzestrzeni i cyberprzestępczości.
C3.	Nabycie przez studentów wiedzy na temat poszczególnych cyberprzestępstw (przestępstwa *stricte* komputerowe, przestępstwa związane z wykorzystaniem sieci i systemów teleinformatycznych oraz nowych technologii, przestępstwa związane z treścią informacji).
C4.	Nabycie umiejętności stosowania przepisów prawa karnego materialnego (odnoszących się do cyberprzestępstw) w kontekście kwalifikacji prawnej czynów.
C5.	Nabycie kompetencji koniecznych przy wykonywaniu zawodu wykorzystującego przepisy prawa karnego materialnego (odnoszące się do cyberprzestępczości).

WYMAGANIA WSTĘPNE

1.	Wiedza z zakresu podstaw prawa karnego materialnego i procesowego.
2.	Umiejętność pracy samodzielnej oraz pracy w grupie. Umiejętność posługiwania się aktami prawnymi, orzecznictwem oraz bazami danych takimi jak np. Legalis.

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ		METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ	ODNIESIENIE DO:	
			TREŚCI PROGRAMOWYCH	KIERUNKOWYCH EFEKTÓW UCZENIA SIĘ
EU1	Student ma pogłębioną wiedzę z zakresu m.in.: przestępstw *stricte* komputerowych, przestępstw związanych z wykorzystaniem sieci i systemów teleinformatycznych. Potrafi wykorzystać zdobytą wiedzę w praktyce przy dokonywaniu subsumpcji i dalszego prowadzenia sprawy.	test - pytania zamknięte i otwarte	K1 – K6	BW K_W 05
EU2	Student ma pogłębioną wiedzę z zakresu cyberprzestrzeni jako środowiska, w którym można zetknąć się z szeregiem zachowań kryminalnych. Dzięki temu jest w stanie skutecznie je identyfikować i neutralizować.	test - pytania zamknięte i otwarte	K1 – K6	BW K_W 06
EU3	Student potrafi identyfikować zagrożenia w cyberprzestrzeni. Przy konstruowaniu pism procesowych, podczas kontaktu z funkcjonariuszami np. policji, posługuje się właściwą terminologią. Ponadto umie formułować własne stanowisko podczas czynności związanych z zakwalifikowaniem danego czynu pod przepis prawa karnego odnoszący się do problematyki cyberprzestępczości.	test - pytania zamknięte i otwarte	K1 – K6	BW K_U 01
EU4	Student jest gotów do nieustannego poszerzania swojej wiedzy i kwalifikacji w zakresie działalności podejmowanej przez cyberprzestępców. Ponadto jest gotów do podjęcia działań uświadamiających społeczeństwo z zakresu bezpiecznego korzystania z sieci.	test - pytania zamknięte i otwarte	K1 – K6	BW K_K 01
EU5	Student ma świadomość znaczenia zdobytej wiedzy, kreatywności i asertywności w funkcjonowaniu zespołu projektowego. Umie współpracować z innymi osobami, komunikować się z nimi, wysłuchiwać ich argumentów, podejmować słuszne decyzje. Dzięki powyższemu (w razie konieczności) jest gotów do kierowania zespołem projektowym.	projekt	L1 – L5	BW K_K 03

TREŚCI PROGRAMOWE			
L.p.	KONWERSATORIUM	Liczba godzin	
		S	N

K1	**Wieloaspektowa struktura przestępstwa i podział typów czynów zabronionych** 1. Wieloaspektowa struktura przestępstwa: a) zachowanie się człowieka, b) czyn, c) bezprawność czynu, d) karalność czynu, e) karygodność czynu, f) zawinienie czynu. 2. Podział typów czynów zabronionych na: a) zasadnicze, kwalifikowane (przez okoliczności i następstwo), uprzywilejowane, b) nazwowe, opisowe, nazwowo-opisowe, c) zupełne, niezupełne, blankietowe, d) zbrodnie, występki.	4	2
K2	**Cyberprzestrzeń i cyberbezpieczeństwo:** 1. Cyberprzestrzeń: a) pojęcie cyberprzestrzeni, b) cyberprzestrzeń a cybernetyka. 2. Cyberbezpieczeństwo: a) pojęcie cyberbezpieczeństwa, b) strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej.	1	1
K3	**Cyberprzestępczość w ujęciu definicyjnym:** 1. cyberprzestępczość, przestępczość komputerowa, przestępstwa związane z wykorzystaniem komputera, 2. cyberprzestępczość – etymologia, 3. najistotniejsze cechy cyberprzestępczości, 4. cyberprzestępstwo a przestępstwo internetowe.	2	1
K4	**Typy przestępstw *stricte* komputerowych:** 1. analiza art. 267 k.k., 268 k.k., 268a k.k., 269 k.k., 269a k.k., 269b k.k., 2. analiza orzecznictwa do ww. typów czynów zabronionych.	2	1
K5	**Przestępstwa związane z wykorzystaniem sieci i systemów teleinformatycznych oraz nowych technologii:** 1. przestępstwa skierowane przeciwko mieniu (analiza np. art. 286 k.k., 278 k.k., 287 k.k., 285 k.k. oraz analiza orzecznictwa do wskazanych typów czynów zabronionych), 2. przestępstwa przeciwko wiarygodności dokumentów (analiza np. art. 270 § 1 k.k., 276 k.k., 303 k.k., 310 k.k. oraz analiza orzecznictwa do wskazanych typów czynów zabronionych), 3. przestępstwa skierowane przeciwko bezpieczeństwu powszechnemu oraz Rzeczypospolitej Polskiej (analiza np. art. 165 § 1 pkt 4 k.k., 130 § 2 k.k. oraz analiza orzecznictwa do wskazanych typów czynów zabronionych), 4. cyberstalking oraz podszywanie się pod inną osobę (analiza art. 190a § 1 i 2 k.k. oraz orzecznictwa).	4	2
K6	**Przestępstwa związane z treścią informacji:** 1. analiza art. 200a k.k., 202 k.k., 212 k.k., 216 k.k., 2. analiza orzecznictwa do ww. typów czynów zabronionych.	2	2
RAZEM		**15**	**9**

FORMA I KRYTERIA ZALICZENIA KONWERSATORIUM: test - pytania zamknięte i otwarte - ocena ilościowa.

L.p.	**PROJEKT**	**Liczba godzin**	
		S	**N**
L1	**Forma projektu i grupy robocze:** 1. podział studentów na grupy robocze (maksymalnie 2-osobowe), 2. przedstawienie wytycznych dot. procesu tworzenia projektów, 3. prezentacja przykładowych form realizacji projektu (np. pisemna, nagranie, organizacja seminarium naukowego, przeprowadzenie ciekawej lekcji w Szkołach Partnerskich Uczelni).	1	1

L2	**Prezentacja przykładowych zagadnień do opracowania:** 1. badania dot. poczucia bezpieczeństwa w cyberprzestrzeni, 2. badania dot. realizacji płatności z wykorzystaniem nowoczesnych technologii z perspektywy cyberbezpieczeństwa, 3. „CyberSafety" - specjalistyczny program szkolenia z zakresu bezpieczeństwa w sieci, 4. „CyberEkspert" - wywiady ze specjalistami, 5. cyberprzemoc w grupie młodych użytkowników Internetu - skala zjawiska, 6. cyberterroryzm - prezentacja specyfiki zjawiska na podstawie analizy działalności wybranych grup cyberprzestępczych.	2	1
L3	**Ustalenie zagadnienia do opracowania oraz wybór formy realizacji projektu:** 1. wybór (przez grupy robocze) problemu możliwego do opracowania, 2. uzasadnienie wyboru danego zagadnienia przez poszczególne grupy robocze, 3. wybór formy realizacji projektu przez grupy robocze, 4. akceptacja tematu projektu i formy jego realizacji przez prowadzącego zajęcia.	1	1
L4	**Tworzenie projektów i weryfikacja poprawności ich przygotowywania przez prowadzącego zajęcia.**	8	4
L5	**Prezentacja projektów.**	3	2
	RAZEM	**15**	**9**

FORMA I KRYTERIA ZALICZENIA PROJEKTU: projekt - ocena ilościowa.

METODY I FORMY DYDAKTYCZNE

1.	wykład informacyjny
2.	wykład problemowy
3.	wykład konwersatoryjny
4.	wytworzenie sytuacji problemowej, formułowanie i weryfikacja pomysłów ich rozwiązania
5.	studium przypadków
6.	dyskusja
7.	praca z tekstem
8.	praca zespołowa
9.	metoda projektów

NARZĘDZIA DYDAKTYCZNE

1.	platforma e-learningowa
2.	laboratorium komputerowe
3.	prezentacja multimedialna

OPROGRAMOWANIE

1.	system informacji prawnej - Legalis

OBCIĄŻENIE STUDENTA PRACĄ

	Forma aktywności	**Liczba godzin na zrealizowanie aktywności**	
		tryb stacjonarny	*tryb niestacjonarny*
1.	godziny kontaktowe z nauczycielem akademickim	30	18
2.	samodzielne przygotowanie do zajęć	15	20
3.	przygotowanie do kolokwium, egzaminu i innych form	15	18
4.	udział w konsultacjach	2	2
5.	zapoznanie się z literaturą przedmiotu	13	17
	SUMA GODZIN	**75**	**75**
	LICZBA PUNKTÓW ECTS	**3**	**3**

LITERATURA PODSTAWOWA

1.	A. Grześkowiak, K. Wiak (red.), *Kodeks karny. Komentarz*, Warszawa 2024. Wersja elektroniczna z Systemu Informacji Prawnej – Legalis.
2.	M. Siwicki, *Cyberprzestępczość*, Warszawa 2013. Wersja elektroniczna z Systemu Informacji Prawnej – Legalis.

3.	F. Radoniewicz, *Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w kodeksie karnym – propozycje zmian,* 2024, wyd. 1, Legalis
LITERATURA UZUPEŁNIAJĄCA I ŹRÓDŁA PRAWA	
1.	A.P. Szajna, *Transakcja zbliżeniowa zrealizowana cudzą kartą płatniczą do kwoty niewymagającej autoryzacji kodem PIN – kradzież (art. 278 § 1 k.k., art. 119 § 1 k.w.) czy kradzież z włamaniem (art. 279 § 1 k.k.)?*, Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury 2022, nr 1(45).
2.	P. Opitek, *Skimming - aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Warszawa 2017. Wersja elektroniczna z Systemu Informacji Prawnej – Legalis.
3.	P. Lewulis, *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, Prokuratura i Prawo 2021, nr 3.
4.	Ł. Krysiński, *Identyfikacja cyberprzestępców*, Prokuratura i Prawo 2020, nr 2.
5.	M. Smarzewski, *Cyberterroryzm a cyberprzestępstwa o charakterze terrorystycznym*, IUS NOVUM 2017, nr 1.
6.	Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej dokument aktualny).
7.	Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (aktualny tekst jednolity).
INNE PRZYDATNE INFORMACJE O PRZEDMIOCIE:	
1.	PLATFORMA MOODLE zawiera: ▪ materiały dydaktyczne do przedmiotu ▪ przedmiotowe efekty uczenia się ▪ zalecaną literaturę ▪ warunki i kryteria zaliczenia przedmiotu
2.	BIBLIOTEKA WSZOP zapewnia literaturę podstawową do przedmiotu oraz wybrane pozycje literatury uzupełniającej, w tym dostęp do zbiorów cyfrowych i Platformy IBUK Libra
3.	ELEKTRONICZNY NIEZBĘDNIK STUDENTA zawiera: ▪ kierunkowe efekty uczenia się ▪ karty przedmiotów ▪ terminy konsultacji nauczycieli akademickich
4.	WIRTUALNY DZIEKANAT zawiera: ▪ harmonogram zajęć na bieżący semestr ▪ harmonogram sesji egzaminacyjnej ▪ ogłoszenia dotyczące organizacji roku akademickiego
5.	Ocena osiągnięcia zakładanych efektów uczenia się z wykorzystaniem metod weryfikacji wymagających oceny jakościowej oznacza, że zakładane efekty zostały osiągnięte: ▪ w pełni – ocena bardzo dobry ▪ z niewielkimi niedociągnięciami – ocena dobry plus ▪ z brakami, które można uzupełnić – ocena dobry ▪ z istotnymi brakami, które można uzupełnić – ocena dostateczny plus ▪ z istotnymi brakami na minimalnym poziomie – ocena dostateczny lub ▪ nie zostały osiągnięte – ocena niedostateczny.
6.	Ocena osiągnięcia zakładanych efektów uczenia się z wykorzystaniem metod weryfikacji wymagających oceny ilościowej oznacza, że zakładane efekty zostały osiągnięte: ▪ 91-100% sumy – ocena bardzo dobry ▪ 81-90% – ocena dobry plus ▪ 71-80% – ocena dobry ▪ 61-70% – ocena dostateczny plus ▪ 51-60% – ocena dostateczny lub ▪ 50% i mniej – ocena niedostateczny.
7.	Terminy egzaminów uzgadnia starosta roku z prowadzącym zajęcia
8.	Karta przedmiotu obowiązuje od roku akademickiego 2024/25