	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Kryminologia stosowana
	Poziom studiów	Studia pierwszego stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil kształcenia	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**B.6.**

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Informatyka śledczo – sądowa**
2. Punkty ECTS	**5**
3. Rodzaj przedmiotu	**Kierunkowy**
4. Język przedmiotu	**Polski**
5. Rok studiów	**I, II**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**dr Paweł Tomaszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 2	**W**: (15); **Ćw.**: (15);	**W**: (10); **Ćw.**: (8);
Semestr 3	**W:(15); Ćw.** (15)	**W**: (10); **Ćw.**: (8);
Liczba godzin ogółem	**60**	**36**

C - Wymagania wstępne

Student powinien posiadać wiedzę o prawie karnym materialnym i procesowym. Powinien znać elementy informatyki funkcjonowania sieci, sieci Internet.

D - Cele kształcenia

	Wiedza
CW1	**Przekazanie studentom wiedzy z zakresu informatyki śledczej w systemie prawnym.**
	Umiejętności
CU1	**Zdobycie umiejętności pozyskiwania danych do analizowania konkretnych procesów przestępczych w cyberświecie.**
CU2	**Wykształcenie umiejętności identyfikowania szans lub zagrożeń oraz podejmowania adekwatnych działań w zapobieganiu przestępstwom popełnianych w cyberświecie.**
	Kompetencje społeczne
CK1	**Ukształtowanie odpowiedniej postawy społecznej i etycznej opartej na prawidłowych zachowaniach w cyberświecie.**
CK2	**Wykształcenie postawy poszanowania prawa jednostki i kompetencji zwalczania jego naruszeń w cyberświecie.**

E - Efekty uczenia się przedmiotowe i kierunkowe

Przedmiotowy efekt uczenia się (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)	**Kierunkowy efekt uczenia się**
Wiedza (EPW…)	

EPW1	Student ma podstawową wiedzę na temat informatyki śledczej w systemie prawnym.	K_W01
EPW2	Student ma wiedzę na temat współczesnych zjawisk przestępczych związanych z zagrożeniami bezpieczeństwa państwa w aspekcie cyberświata.	K_W09
Umiejętności (EPU…)		
EPU1	Student potrafi wykorzystać i stosować w praktyce wiedze teoretyczną dotyczącą zwalczania przestępstw popełnianych w cyberświecie.	K_U02
EPU2	Student przewiduje implikacje konkretnych czynów zabronionych popełnianych przez cyber-przestępców.	K_U04
Kompetencje społeczne (EPK…)		
EPK1	Absolwent jest gotów odpowiednio określić priorytety służące ochronie prawa w cyberświecie, realizowanych zespołowo w aktywności społeczno-gospodarczej.	K_K03 K_K07
EPK2	Absolwent jest gotów do identyfikacji problemów z zakresu zapobiegania i wykrywania sprawców czynów zabronionych w cyberświecie oraz podjęcia własnych reakcji.	K_K05

F – Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	Niestacjonarnych
W1	Zapoznanie studentów z planem i programem nauczania przedmiotu, celami i efektami uczenia się oraz formą zaliczenia Informatyka śledcza w systemie prawnym	2	2
W2	Cyberprzestępcy, modus operandi, i motywy działania	3	2
W3	Rodzaje aktów na systemy informacyjne ,a informatyka śledcza	3	2
W4	Podstawy informatyki śledczej	5	2
W5	Cyfrowe nośniki danych	3	2
W6	Zabezpieczanie dowodów cyfrowych	2	2
W7	Rola dowodu cyfrowego	3	2
W8	Instytucja biegłego z zakresu informatyki	3	2
W9	Analiza śledcza nośników danych (offline)	3	2
W10	Analiza śledcza danych w „chmurze”	3	2
	Razem liczba godzin wykładów	**30**	**20**

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	Zapoznanie studentów z programem kształcenia Podstawy informatyki śledczej	3	3
C2	Wymagania informatyki śledczej	2	2
C3	Oprogramowanie do analizy systemu operacyjnego	3	2
C4	Rodzaje cyfrowych nośników danych w praktyce	4	3
C5	Metody zabezpieczania nośników danych – przykłady	5	2
C6	Błędy przy zabezpieczaniu dowodów cyfrowych – studium przypadku	4	2
C7	Właściwe formułowanie pytań do biegłego	4	2
C8	Analiza śledcza nośników danych (offline) przykłady	3	2
C9	Analiza śledcza danych w „chmurze” studium przypadków	2	2
		30	**16**

G – Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M1 Metoda podająca** (wykład informacyjny) **M2 Metoda problemowa** (wykład z elementami analizy problemowej i dyskusji).	Projektor multimedialny, system informacji prawnej.
Ćwiczenia	**M2 Metoda problemowa** (analiza przypadku, case study) **M5 Metoda praktyczna** (czytanie i analiza tekstu źródłowego, prezentacja różnych form wypowiedzi).	System informacji prawnej, dostęp do internetowego systemu aktów prawnych.

H - Metody oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	Ocena formująca (F) – wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	Ocena podsumowująca (P) – podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład	**F2 – obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć).	**P1 – egzamin pisemny w formie testowej z elementami opisu**
Ćwiczenia	**F2 – Obserwacja/aktywność**: (obserwacja poziomu przygotowania do zajęć). **F3 – Praca pisemna** (przygotowanie referatu lub prezentacji). **F4 – Wypowiedź/wystąpienie**: (sposób prezentacji multimedialnej z komentarzem).	**Ocena podsumowująca stanowi sumę ocen formujących.**

H-1 Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Efekty przedmiotowe	Wykład		Ćwiczenia		
	P1	F2	F2	F3	F4
EPW1	X	X	X		X
EPW2		X	X	X	X
EPU1	X	X	X		X
EPU2		X	X	X	X
EPK1	X	X	X		X
EPK2		x	x	X	X

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt uczenia się (EP..)	**Dostateczny dostateczny plus 3/3,5**	**Dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student ma podstawową wiedzę na temat znaczenia informatyki śledczej w systemie prawnym.	Student ma wiedzę o aspektach informatyki śledczej w systemie prawnym.	Student wyróżnia się wiedzą na temat informatyki śledczej w systemie prawnym.
EPW2	Student ma wiedzę podstawową na temat współczesnych zjawisk przestępczych związanych z zagrożeniami dla BN w aspekcie cyberbezpieczeństwa.	Student ma wiedzę na temat współczesnych zjawisk przestępczych związanych z zagrożeniami dla bezpieczeństwa państwa w aspekcie cyberbepieczeństwa.	Student wyróżnia się wiedzą na temat współczesnych zjawisk przestępczych związanych z zagrożeniami dla bezpieczeństwa państwa w aspekcie cyberbepieczeństwa.
EPU1	Student z pomocą innych potrafi wykorzystywać i stosować w praktyce wiedzę teoretyczną dotycząca zwalczania	Student potrafi wykorzystywać i stosować w praktyce wiedzę teoretyczną dotycząca zwalczania przestępstw popełnianych w cyberświecie.	Student wyróżnia się wykorzystywaniem i stosowaniem w praktyce wiedzy teoretycznej dotyczącej zwalczania przestępstw popełnianych w cyberświecie.

	przestępstw popełnianych w cyberświecie.		
EPU2	Student przy wsparciu innych określa implikacje konkretnych czynów zabronionych popełnianych przez cyberprzestępców.	Student przewiduje implikacje konkretnych czynów zabronionych popełnianych przez cyberprzestępców.	Student wyróżnia się w przewidywaniu implikacji konkretnych czynów zabronionych popełnianych przez cyberprzestępców.
EPK1	Student jest gotów określać priorytety służące ochronie prawa w cyberświecie, w ramach pracy zespołowej.	Student przejawia aktywność w zespołowej pracy mającej na celu określanie priorytetów służących ochronie prawa w cyberświecie.	Student potrafi przejmować kierownicze role w pracach zespołów określających priorytety służące ochronie prawa w cyberświecie.
EPK2	Student jest gotów do identyfikacji problemów z zakresu zapobiegania i wykrywania sprawców czynów zabronionych w cyberświecie.	Student jest gotów do identyfikacji problemów z zakresu zapobiegania i wykrywania sprawców czynów zabronionych w cyberświecie oraz podejmowania własnych reakcji z tym związanych.	Student jest gotów do identyfikacji problemów z zakresu zapobiegania i wykrywania sprawców czynów zabronionych w cyberświecie samodzielnego reagowania oraz wspierania innych w tym zakresie.

J – Forma zaliczenia przedmiotu

Egzamin

K – Literatura przedmiotu

Literatura obowiązkowa:

4. Olber P., *Prawo-kryminalistyczne aspekty zabezpieczania i pozyskiwania dowodów elektronicznych z chmur obliczeniowych*, Szczytno 2021.
5. C. Altheide, H. Carvey, Informatyka śledcza, Helion, Warszawa, 2015 r.

Literatura zalecana / fakultatywna:

1. Chojnowski A., *Informatyka sądowa w praktyce*, Gliwice 2020.
2. Harlan C., *Altheide C., Informatyka śledcza – przewodnik po narzędziach open source* , Gliwice 2014.
3. A. Kalinowski, Metody inwigilacji i element informatyki śledczej, CSH, 2011 r.
4. Konwencja Rady Europy o cyberprzestępczości.

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	60	36
Czytanie literatury	15	22
Przygotowanie referatu / prezentacji	17	23
Przygotowanie do ćwiczeń / do zaliczenia ćwiczenia	17	22
Przygotowanie do egzaminu	16	22
Suma godzin:	**125**	**125**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**5**	**5**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Paweł Tomaszewski
Data sporządzenia / aktualizacji	11.06.2022 r.
Dane kontaktowe (e-mail)	ptomaszewski@ajp.edu.pl
Podpis	Tomaszewski