Załącznik nr 1
do *Programu studiów podyplomowych Zwalczanie cyberprzestępczości*
stanowiącego załącznik do Uchwały Nr 35/000/2022 Senatu AJP
z dnia 20 września 2022 r.

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Wstęp do informatyki

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 20**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 10** **Ćwiczenia (Ć): 10**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz posiada pogłębioną wiedzę na temat podstaw informatyki.
Umiejętności (CU):
Słuchacz potrafi analizować i wyjaśnić problemy związane z informatyką.
Kompetencje społeczne (CK):
Słuchacz posiada zdolność radzenia sobie z problemami wynikający ze specyfiki informatyki.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1 - Słuchacz zna i rozumie podstawy informatyki i potrafi wykorzystać zdobyty zasób wiedzy w specyfice zwalczania cyberprzestępczości.

Umiejętności

EPU1 - Słuchacz potrafi analizować systemy operacyjne i sieci komputerowe, pozyskiwać i wykorzystywać zapisane w nich dane informatyczne w zwalczaniu cyberprzestępczości.

Kompetencje społeczne

EPK1 - Słuchacz posiada zdolność do efektywnego radzenia sobie z problemami związanymi z informatyką w specyfice zwalczania cyberprzestępczości.

E - Treści programowe oraz literatura

Forma zajęć wykład: 1. Wprowadzenie do teorii informatyki. 2. Wstęp do systemów operacyjnych z rodziny Windows 3. Wstęp do systemów operacyjnych z rodziny Linux. 4. Wstęp do systemów operacyjnych z rodziny macOs. 5. Wstęp do sieci komputerowych (adresacja IP, DNS, TOR). **Razem liczba godzin wykładów**	**10**
Forma zajęć ćwiczenia: 1. Korzystanie z systemów operacyjnych pracujących na maszynach wirtualnych. 2. Wykonywanie cech charakterystycznych dla systemów operacyjnych Windows, Linux, macOs, oraz	**10**

podstawowych poleceń systemowych. 3. Wykonywanie operacji związanych z uzyskaniem informacji nt. sprzętowej konfiguracji komputera, interfejsów sieciowych, artefaktów systemu. 4. Interpretacja zapisów logów systemowych, plików konfiguracyjnych, zapisów rejestrów. **Razem liczba godzin wykładów**	
Ogółem liczba godzin przedmiotu:	**20**

Literatura przedmiotu

Literatura obowiązkowa:

1. Bensel P, *Systemy i sieci komputerowe*, Gliwice 2010
2. Lembas J, Kawa R, *Wstęp do informatyki*, Warszawa 2017

Literatura zalecana / fakultatywna:

1. Kurose J, Ross K, *Sieci komputerowe. Ujęcie całościowe*. Wydanie VII, Gliwice 2018
2. Serafin M, *Wirtualizacja w praktyce*, Gliwice 2012
3. White R, Banks E, *Sieci komputerowe. Najczęstsze problemy i ich rozwiązania*, Gliwice 2018

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia przedmiotowe)

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**

Wykłady:

F1 – Sprawdzian (ustny lub pisemny)	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów i ćwiczeń

Ćwiczenia:

F2 - Obserwacja/aktywność (podczas realizacji ćwiczeń wykonywanych podczas zajęć) **F5 - Ćwiczenia praktyczne** (ocena ćwiczeń wykonywanych podczas zajęć)	-

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**						
	Wykład		Ćwiczenia				
	F1		**F2**	**F5**			
EPW1	X		X	X			
EPU1	X		X	X			
EPK1	X		X	X			

G.4. Forma i warunki zaliczenia przedmiotu:

Zaliczenie z oceną

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	20

Czytanie literatury	10
Przygotowanie do ćwiczeń	10
Przygotowanie do sprawdzianu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin: 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

Załącznik nr 1
do *Programu studiów podyplomowych Zwalczanie cyberprzestępczości*
stanowiącego załącznik do Uchwały Nr 35/000/2022 Senatu AJP
z dnia 20 września 2022 r.

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Uregulowania prawne i taktyka prowadzenia wybranych czynności dowodowych

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 20**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 10** **Ćwiczenia (Ć): 10**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz posiada pogłębioną wiedzę na temat krajowych i międzynarodowych uregulowań prawnych zwalczania cyberprzestępczości.
Umiejętności (CU):
Słuchacz potrafi analizować i wyjaśnić problemy prawne i dowodowe przestępstw popełnianych w cyberprzestrzeni.
Kompetencje społeczne (CK):
Słuchacz posiada zdolność radzenia sobie z problemami wynikający ze specyfiki prowadzenia wybranych czynności dowodowych.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1 - Słuchacz zna i rozumie uregulowania prawne i taktykę dowodową w zwalczaniu cyberprzestępczości oraz potrafi wykorzystać zdobyty zasób wiedzy w praktyce.

Umiejętności

EPU1 - Słuchacz potrafi zabezpieczyć fizycznie oraz przeprowadzić oględziny sprzętu komputerowego i elektronicznych nośników danych oraz sporządzić w tym zakresie dokumentację.

Kompetencje społeczne

EPK1 - Słuchacz posiada zdolność do efektywnego radzenia sobie z problemami prawnymi, dowodowymi i sprzętowymi w specyfice przestępstw popełnianych w cyberprzestrzeni.

E - Treści programowe oraz literatura

Forma zajęć, wykład:

1. Znamiona i specyfika wybranych przestępstw popełnianych w cyberprzestrzeni wraz z ich kwalifikacją prawną.
2. Pojęcie dowodu elektronicznego w aspekcie art. 115 §14 KK oraz przepisów KPK - definicje. Oględziny: pojęcie oględzin, przedmiot oględzin. Przeszukanie: pojęcie przeszukania, sposób prowadzenia przeszukania.

3. Krajowe i międzynarodowe uregulowania prawne (m.in. Konwencja Rady Europy, Europejski Nakaz Dochodzeniowy). 4. Wybrane międzynarodowe uregulowania prawne i rozwiązania instytucjonalne istotne w kontekście pozyskiwania dowodów z chmur obliczeniowych. Gromadzenie dowodów elektronicznych. Wyzwania i problemy w obszarze pozyskiwania i analizy dowodów cyfrowych z chmur obliczeniowych. **Razem liczba godzin wykładów**	**10**
Forma zajęć, ćwiczenia: 1. Określanie na podstawie praktycznych przykładów (case study) ustawowych znamion przestępstw popełnianych w cyberprzestrzeni. 2. Interpretowanie na podstawie praktycznych przykładów (case study) różnych pojęć, zwłaszcza dowodu elektronicznego i cyfrowego, oględzin, przeszukania. 3. Przeprowadzanie oględzin sprzętu komputerowego i elektronicznych nośników danych oraz tworzenie dokumentacji - praktyczne przykłady (case study) 4. Przeprowadzanie przeszukania (pomieszczenia, systemu komputerowego) - praktyczne przykłady (case study) 5. Zabezpieczanie fizyczne sprzętu elektronicznego i nośników danych - - praktyczne przykłady (case study). **Razem liczba godzin wykładów**	**10**
Ogółem liczba godzin przedmiotu:	**20**

Literatura przedmiotu

Literatura obowiązkowa:

1. Białkowski M, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2016
2. Nikkel B.„ *Metody zabezpieczenia cyfrowego*, Warszawa 2021
3. Darren R. Hayes, *Informatyka w kryminalistyce. Praktyczny przewodnik*. Gliwice 2021
4. Olber P.. *Prawno-kryminalistyczne aspekty zabezpieczania i pozyskiwania dowodów elektronicznych z chmur obliczeniowych*, Szczytno 2021.
5. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny
6. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego
7. Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. wraz z protokołami dodatkowymi

Literatura zalecana / fakultatywna:

1. Kasprzak W., *Ślady cyfrowe. Studium prawno-kryminalistyczne,* Difin 2015.
2. Jaroszewska I.A, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne,* Olsztyn 2017 r.
3. Opitek P, *Skimming – aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Beck 2017 r.

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**
Wykłady:	
-	**P1 – Egzamin** (ustny lub pisemny) Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów

	i ćwiczeń
Ćwiczenia:	
F2 - Obserwacja/aktywność (podczas realizacji ćwiczeń) **F5 - Ćwiczenia praktyczne** (ocena ćwiczeń wykonywanych podczas zajęć)	**-**

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**						
	Wykład		Ćwiczenia				
	P1		**F2**	**F5**			
EPW1	X		X	X			
EPU1	X		X	X			
EPK1	X		X	X			

G.4. Forma i warunki zaliczenia przedmiotu:

Egzamin

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	20
Czytanie literatury	10
Przygotowanie do ćwiczeń	10
Przygotowanie do egzaminu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

Załącznik nr 1
do *Programu studiów podyplomowych Zwalczanie cyberprzestępczości*
stanowiącego załącznik do Uchwały Nr 35/000/2022 Senatu AJP
z dnia 20 września 2022 r.

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Działania operacyjne w Internecie

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 20**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 10** **Ćwiczenia (Ć): 10**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz posiada pogłębioną wiedzę na temat metod operacyjnych w Internecie.
Umiejętności (CU):
Słuchacz potrafi przeprowadzić ukierunkowane rozpoznanie internetowe.
Kompetencje społeczne (CK):
Słuchacz posiada zdolność radzenia sobie z problemami wynikającymi ze specyfiki działań operacyjnych w Internecie.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1 - Słuchacz zna i rozumie problemy związane z działaniami operacyjnymi oraz potrafi wykorzystać zdobyty zasób wiedzy w praktyce.

Umiejętności

EPU1 - Słuchacz potrafi przeprowadzić rozpoznanie internetowe oraz zweryfikować uzyskane informacje.

Kompetencje społeczne

EPK1 - Słuchacz posiada zdolność do efektywnego radzenia sobie z problemami działań operacyjnych w Internecie.

E - Treści programowe oraz literatura

Forma zajęć, wykład:

1. Pojęcie czynności operacyjno-rozpoznawczych w systemie prawa polskiego. Katalog metod pracy operacyjnej – odniesienie do współczesnych rozwiązań prawnych. Ryzyko w czynnościach operacyjno-rozpoznawczych Policji.
2. Możliwości prowadzenia pracy operacyjnej w Internecie.
3. Metody pozyskiwania danych z Internetu przy użyciu ogólnodostępnych baz danych, ustalenia teleinformatyczne i internetowe.
4. Zaawansowane metody pozyskiwania informacji z Internetu przy użyciu wyszukiwarek Internetowych.
5. Tożsamość internetowa.
6. Weryfikacja autentyczności uzyskanych informacji.

7. Ustalenia w trybie art.20 i art.20c Ustawy o Policji, oraz procedura przekazywania uzyskanych danych do postępowania karnego. 8. Zasady składania wniosków do operatorów i podmiotów zagranicznych (Facebook, Twitter, Instagram, etc.). **Razem liczba godzin wykładów**	**10**
Forma zajęć, ćwiczenia: 1. Określanie na podstawie praktycznych przykładów (case study) możliwości pracy operacyjnej w Internecie oraz jej ograniczeń. 2. Uzyskiwanie, interpretowanie i analizowanie danych z otwartych źródeł informacji na praktycznych przykładach (case study). 3. Wykorzystywanie narzędzi do zaawansowanego wyszukiwania informacji. 4. Weryfikowanie autentyczności uzyskanych danych. Tworzenie, wykorzystywanie, weryfikowanie i interpretowanie tożsamości internetowej. **Razem liczba godzin wykładów**	**10**
Ogółem liczba godzin przedmiotu:	**20**

Literatura przedmiotu

Literatura obowiązkowa:

1. Kudła J., Kosmaty P.*, Ryzyko w czynnościach operacyjno-rozpoznawczych Policji. Aspekty kryminalistyczne i prawnodowodowe.* Wydanie II uzupełnione i uaktualnione, Difin 2018
2. Sprengel B., *Praca operacyjna Policji*, UMK –Toruń, 2018 r.
3. Ustawa z dnia 6 kwietnia 1990 r. o Policji.
4. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego

Literatura zalecana / fakultatywna

1. Czaplicki K., Szpor G., (red.) *Internet. Analityka danych,* Beck 2019
2. Darren R. Hayes, *Informatyka w kryminalistyce. Gliwice* 2021
3. Nikkel B.*„ Metody zabezpieczenia cyfrowego*, Warszawa, 2021

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia z wykorzystaniem dostępnych wyszukiwarek internetowych, stron agregujących informacje o użytkownikach Internetu z otwartych źródeł).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**
Wykłady:	
F1 – Sprawdzian (ustny lub pisemny)	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów i ćwiczeń.
Ćwiczenia:	
F2 - Obserwacja/aktywność (podczas realizacji ćwiczeń) **F5 - Ćwiczenia praktyczne** (ocena ćwiczeń wykonywanych podczas zajęć)	-

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**		
	Wykład	Ćwiczenia	

	F1	…….	**F2**	**F5**			
EPW1	X	…….	X	X			
EPU1	X	…….	X	X			
EPK1	X	…….	X	X			

G.4. Forma i warunki zaliczenia przedmiotu:	
Zaliczenie z oceną	

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	20
Czytanie literatury	10
Przygotowanie do ćwiczeń	10
Przygotowanie do sprawdzianu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Podstawy informatyki śledczej cz.1

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 20**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 10** **Ćwiczenia (Ć): 10**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz zna i rozumie narzędzia wykorzystywane w informatyce śledczej.
Umiejętności (CU):
Słuchacz potrafi ujawniać i zabezpieczać ślady i dowody zgodnie ze specyfiką informatyki śledczej.
Kompetencje społeczne (CK):
Słuchacz posiada zdolność krytycznej oceny sytuacji i efektywnego radzenia sobie z problemami wynikającymi z realizacji powierzonych zadań.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się
Wiedza
EPW1 - Słuchacz zna i rozumie specyfikę informatyki śledczej.
Umiejętności
EPU1 - Słuchacz potrafi ujawnić i zabezpieczyć cyfrowy materiał dowodowy.
Kompetencje społeczne
EPK1 - Słuchacz posiada zdolność do krytycznej oceny materiału dowodowego oraz do efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań informatyki śledczej.

E - Treści programowe oraz literatura

Forma zajęć, wykład:

1. Wstęp do informatyki śledczej.
2. Informatyka śledcza i narzędzia typu open source. Cele dochodzeń informatyki śledczej. Proces cyfrowej analizy śledczej. Informatyk śledczy – rola w procesie wykrywczym.
3. Problematyka ujawniania i zabezpieczania materiału dowodowego z Internetu.
4. Problematyka ujawniania i zabezpieczania materiału dowodowego pozyskiwanego z komputerów.
5. Problematyka ujawniania i zabezpieczania materiału dowodowego z urządzeń mobilnych (tablety, telefony).
6. Problematyka ujawniania i zabezpieczania materiału dowodowego z rejestratorów CCTV.

Razem liczba godzin wykładów	**10**
Forma zajęć, ćwiczenia: 1. Zasady, charakterystyka, stosowane narzędzia i oprogramowanie wykorzystywane w praktyce informatyki śledczej - praktyczne przykłady (case study). 2. Praktyczne przykłady (case study) ujawniania i zabezpieczania materiałów dowodowych z Internetu. 3. Praktyczne przykłady (case study) ujawniania i zabezpieczania materiałów dowodowych z komputerów, 4. Praktyczne przykłady (case study) ujawniania i zabezpieczania materiałów dowodowych z urządzeń mobilnych 5. Praktyczne przykłady (case study) ujawniania i zabezpieczania materiałów dowodowych z z rejestratorów CCTV **Razem liczba godzin wykładów**	**10**
Ogółem liczba godzin przedmiotu:	**20**

Literatura przedmiotu

Literatura obowiązkowa:

1. Altheide C, Carvey H, *Informatyka śledcza. Przewodnik po narzędziach open source, Gliwice* 2014
2. R. Hayes D, *Informatyka w kryminalistyce. Praktyczny przewodnik*. Gliwice2021
3. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny*
4. Ustawa z dnia 6 czerwca 1997 r. *Kodeks postępowania karnego*

Literatura zalecana / fakultatywna:

1. Chojnowski A., *Informatyka sądowa w praktyce,* Gliwice 2019
2. Nikkel B.,, *Metody zabezpieczenia cyfrowego*, Warszawa 2021
3. Stefański R. A., *Metodyka pracy prokuratora w sprawach karnych,* Warszawa 2017 r.
4. Rozporządzenie Ministra Sprawiedliwości z dnia 11 stycznia 2017 r. *w sprawie utrwalania obrazu lub dźwięku dla celów procesowych w postępowaniu karnym* (Dz.U. 2017 poz. 93)

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**
Wykłady:	
F1 – Sprawdzian (pisemny lub ustny)	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów i ćwiczeń
Ćwiczenia:	
F2 - Obserwacja/aktywność (realizacji zadań) **F5 - Ćwiczenia praktyczne** (ocena wykonywanych zadań)	-

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**		
	Wykład	Ćwiczenia	Laboratoria

	F1	…….	**F2**	**F5**			
EPW1	X	…….	X	X			
EPU1	X	…….	X	X			
EPK1	X	…….	X	X			

G.4. Forma i warunki zaliczenia przedmiotu:	
Zaliczenie z oceną	

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	20
Czytanie literatury	10
Przygotowanie do ćwiczeń	10
Przygotowanie do sprawdzianu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Analiza śledcza w sprawach związanych z cyberprzestępczością

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 20**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 10** **Ćwiczenia (Ć): 10**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz posiada pogłębioną wiedzę na temat analizy śledczej w sprawach związanych z cyberprzestępczością.
Umiejętności (CU):
Słuchacz potrafi analizować i wyjaśnić sprawy/stan faktyczny w realizacji zadań dotyczących analizy śledczej w sprawach związanych z cyberprzestępczością.
Kompetencje społeczne (CK):
Słuchacz posiada zdolność krytycznej oceny sytuacji i efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań dotyczących analizy śledczej w sprawach związanych z cyberprzestępczością.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1 - Słuchacz zna i rozumie metody i techniki analizy śledczej w sprawach związanych z cyberprzestępczością.

Umiejętności

EPU1 - potrafi przeprowadzić ukierunkowane rozpoznanie w sprawach związanych z cyberprzestępczością z wykorzystaniem analizy śledczej w sprawach związanych z cyberprzestępczością.

Kompetencje społeczne

EPK1 - Słuchacz posiada zdolność do krytycznej oceny materiału dowodowego do efektywnego radzenia sobie z problemami wynikającymi z analizy śledczej w sprawach związanych z cyberprzestępczością.

E - Treści programowe oraz literatura

Forma zajęć, wykład: 1. Problematyka, metody i techniki analizy śledczej w sprawach związanych z cyberprzestępczością. 2. Wstępna ocena cyfrowego materiału dowodowego. 3. Kryptowaluty w sprawach związanych z cyberprzestępczością 4. Sieci anonimizujące w sprawach związanych z cyberprzestępczością. **Razem liczba godzin wykładów**	**10**
Forma zajęć, ćwiczenia:	

5. Przygotowanie darmowego oprogramowania forensics do zajęć . 6. Ujawnianie i zabezpieczanie śladów korzystania z kryptowalut. Wykorzystanie portfeli do zobrazowania przepływów kryptowalut. Wykorzystanie opracowanej metodyki zabezpieczania kryptowalut - praktyczne przykłady (case study). 7. Ujawnianie i zabezpieczanie śladów korzystania z sieci anonimizujących. Korzystanie z sieci VPN, Tor i Darknetu - ujawnienia śladów pozostałych po korzystaniu z ww. rozwiązań - praktyczne przykłady (case study). 8. Przeprowadzanie podstawowej oceny zabezpieczonego materiału dowodowego - praktyczne przykłady (case study). 9. Opisywanie, dokumentowanie czynności - praktyczne przykłady (case study).	
Razem liczba godzin wykładów	**10**
Ogółem liczba godzin przedmiotu:	**20**

Literatura przedmiotu

Literatura obowiązkowa:

3. Carvey H, *Analiza śledcza i powłamaniowa. Zaawansowane techniki prowadzenia analizy w systemie Windows 7*. Gliwice 2013
4. R. Hayes D, *Informatyka w kryminalistyce. Praktyczny przewodnik*. Gliwice 2021
5. Nikkel B., *Metody zabezpieczenia cyfrowego*, Warszawa 2021

Literatura zalecana / fakultatywna:

4. Serafin M., *Sieci VPN. Zdalna praca i bezpieczeństwo danych*. Gliwice 2013
5. Song J., *Zrozumieć Bitcoin. Programowanie kryptowalut od podstaw*, Gliwice 2020
6. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny*
7. Ustawa z dnia 6 czerwca 1997 r. *Kodeks postępowania karnego*

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**
Wykłady:	
-	**P1 – Egzamin** (pisemny lub ustny) Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów i ćwiczeń
Ćwiczenia:	
F2 - Obserwacja/aktywność (realizacji zadań) **F5 - Ćwiczenia praktyczne** (ocena wykonywanych zadań)	**-**

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**						
	Wykład		Ćwiczenia				
	P1	……..	**F2**	**F5**	……..		
EPW1	X	……..	X	X	……..		

EPU1	X	……...	X	X	……....		
EPK1	X	……...	X	X	……....		

G.4. Forma i warunki zaliczenia przedmiotu:	
Zaliczenie z oceną	

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	20
Czytanie literatury	10
Przygotowanie do ćwiczeń	10
Przygotowanie do egzaminu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Live Forensics, metody TRIAGE

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 20**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 10** **Ćwiczenia (Ć): 10**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz posiada pogłębioną wiedzę na temat sposobów, metod i technik pracy dotyczącej zwalczania cyberprzestępczości.
Umiejętności (CU):
Słuchacz potrafi ujawniać i zabezpieczać ślady i dowody cyberprzestępczości wraz z ich wstępną weryfikacją.
Kompetencje społeczne (CK):
Słuchacz postępuje zgodnie ze standardami i regulacjami prawnymi dotyczącymi zwalczania cyberprzestępczości.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się
Wiedza
EPW1 - Słuchacz zna i rozumie metodologię Live Forensic/Triage w problematyce zwalczania cyberprzestępczości.
Umiejętności
EPU1 - Słuchacz potrafi wykorzystać i zastosować metodologię Live Forensic/Triage w zwalczaniu cyberprzestępczości.
Kompetencje społeczne
EPK1 - Słuchacz potrafi w praktyce stosować właściwe standardy prawne i etyczne, a także wykazywać się odpowiednią postawą z realizacji zadań dotyczących zwalczania cyberprzestępczości**.**

E - Treści programowe oraz literatura

Forma zajęć, wykład:

1. Specyfika, potrzeba oraz znaczenie metodologii Live Forensic/Triage w problematyce zabezpieczania dowodów elektronicznych. Zasady, charakterystyka, stosowane narzędzia i oprogramowanie.
2. Wstępna weryfikacja danych pozyskiwanych w ramach Live Forensics, metod Triage'owych.
3. Rozpoznawanie oprogramowania antiforensics i szyfrującego dane.

Razem liczba godzin wykładów	**10**
Forma zajęć, ćwiczenia: 1. Przygotowanie sprzętu, oprogramowanie i nośników wykorzystywanych do ćwiczeń. 2. Wykorzystanie maszyn wirtualnych z zainstalowanymi systemami operacyjnymi. 3. Przeprowadzanie sprawdzenia uruchomionego systemu - Live Forensics, 4. Korzystanie z oprogramowania Triage, 5. Ujawnianie oprogramowania antiforensics oraz szyfrującego dane. **Razem liczba godzin wykładów**	**10**
Ogółem liczba godzin przedmiotu:	**20**

Literatura przedmiotu

Literatura obowiązkowa:

1. Chojnowski A., *Informatyka sądowa w praktyce,* Helion 2019
2. Ziaja A., *Praktyczna analiza powłamaniowa. Aplikacja webowa w środowisku Linux*, Wydawnictwo Naukowe PWN 2017.

Literatura zalecana / fakultatywna:

1. Altheide C,Carvey H, *Informatyka śledcza. Przewodnik po narzędziach open source*, Gliwice 2014
2. Hayes D.R., *Informatyka w kryminalistyce. Praktyczny przewodnik*. Gliwice 2021
3. Nikkel B.,, *Metody zabezpieczenia cyfrowego*, Warszawa 2021
4. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny*
5. Ustawa z dnia 6 czerwca 1997 r. *Kodeks postępowania karnego*

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**
Wykłady:	
F1 – Sprawdzian (pisemny lub ustny)	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów i ćwiczeń
Ćwiczenia:	
F2 - Obserwacja/aktywność (realizacji zadań) **F5 - Ćwiczenia praktyczne** (ocena wykonywanych zadań)	**-**

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**						
	Wykład		Ćwiczenia			Laboratoria	
	F1	……...	**F2**	**F5**	……...		
EPW1	X	……...	X	X	……...		
EPU1	X	……...	X	X	……...		

EPK1	X	……...	X	X	……....		

G.4. Forma i warunki zaliczenia przedmiotu:	
Zaliczenie z oceną	
H. Nakład pracy studenta	
Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	20
Czytanie literatury	10
Przygotowanie do ćwiczeń	10
Przygotowanie do sprawdzianu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe	
Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Seminarium		
2. Punkty ECTS: 8 (3 - I semestr; 5 – 2 semestr)		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y:** 1 i 2	**7. Liczba godzin ogółem: 30** (10h - I semestr, 20h – 2 semestr)
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Seminarium (S): 30**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		**Dr Sylwia Gwoździewicz**

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz posiada pogłębioną wiedzę na temat sposobów, metod i technik pracy dotyczącej zwalczania cyberprzestępczości.
Umiejętności (CU):
Słuchacz potrafi analizować i wyjaśnić sprawy/stan faktyczny w realizacji zadań dotyczących zwalczania cyberprzestępczości.
Kompetencje społeczne (CK):
Słuchacz postępuje zgodnie ze standardami i regulacjami prawnymi dotyczącymi zwalczania cyberprzestępczości.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się
Wiedza
EPW1 - Słuchacz zna i rozumie specyfikę pracy związanej ze zwalczaniem cyberprzestępczości.
Umiejętności
EPU1 - Słuchacz potrafi zastosować różne narzędzia np. informatyczne, prawne w zwalczaniu cyberprzestępczości.
Kompetencje społeczne
EPK1 - Słuchacz postępuje zgodnie ze standardami i regulacjami prawnymi dotyczącymi zwalczania cyberprzestępczości.

E - Treści programowe oraz literatura

Forma zajęć, seminarium:

1. Metodologia i konstrukcja pracy pisemnej.
2. Określenie indywidualnej problematyki pracy.
3. Analiza przydatności literatury przedmiotu oraz innych źródeł.
4. Precyzowanie tematów prac i zatwierdzenie zebranej literatury.
5. Analiza, korekta i porównanie tematu, celu i całej koncepcji pracy.
6. Szczegółowa analiza techniki pisania pracy na indywidualnych przykładach.
7. Prezentacja celów prac.
8. Analiza literatury źródłowej z weryfikacją repozytoriów naukowych dostępnych w Internecie

pod kątem tematyki i koncepcji pracy. 9. Analiza najważniejszych problemów z dostępem do źródeł informacji oraz ich wykorzystaniem. 10. Analiza metodyki formułowania wniosków, komentowania i oceny opisywanych treści. 11. Prezentacja głównych wniosków. 12. Analiza najważniejszych problemów metodologicznych badań. 13. Ostateczny przegląd oraz prezentacja prac.	
Razem liczba godzin seminarium	**30**
Ogółem liczba godzin przedmiotu:	**30**

Literatura przedmiotu

Literatura obowiązkowa:

1. Siuda P, Wasylczyk P, *Publikacje naukowe. Praktyczny poradnik dla studentów, doktorantów i nie tylko*, Warszawa 2018.

Literatura zalecana / fakultatywna:

1. Sztumski J, *Wstęp do metod i technik badań społecznych*, Śląsk, 2020.

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład z elementami analizy źródłowej i dyskusji).
M5 – Metoda praktyczna (przygotowanie pracy pisemnej).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**

Seminarium:

F3 – Praca pisemna (przygotowanie pracy pisemnej tj. artykułu naukowego na podstawie materiału źródłowego z elementami analiz i lub badań własnych) **F4 – Wypowiedź/wystąpienie** (dyskusja, sposób prezentacji prac pisemnych)	**P5 – Ocena pracy pisemnej** (artykułu naukowego)

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**						
	Wykład		Seminarium			Laboratoria	
	……..	……..	**F3**	**F4**	**P5**	……..	……..
EPW1	……..	……..	X	X	X	……..	……..
EPU1	……..	……..	X	X	X	……..	……..
EPK1	……..	……..	X	X	X	……..	……..

G.4. Forma i warunki zaliczenia przedmiotu:

Zaliczenie (zal) - 1 semestr
Zaliczenie z oceną pracy pisemnej – 2 semestr

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na**

	realizację
Godziny zajęć z nauczycielem/ami	30
Czytanie i analiza literatury związanej z wybraną tematyką pracy pisemnej	70
Przygotowanie i prezentacja pracy pisemnej	100
Suma godzin:	**200**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**8**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Podstawy informatyki śledczej cz.2

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 2**	**7. Liczba godzin ogółem: 16**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 8** **Ćwiczenia (Ć): 8**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz zna i rozumie narzędzia wykorzystywane w informatyce śledczej.
Umiejętności (CU):
Słuchacz potrafi ujawniać i zabezpieczać ślady i materiał dowody zgodnie ze specyfiką informatyki śledczej.
Kompetencje społeczne (CK):
Słuchacz posiada zdolność krytycznej oceny sytuacji i efektywnego radzenia sobie z problemami wynikającymi z realizacji powierzonych zadań.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się
Wiedza
EPW1 - Słuchacz zna i rozumie specyfikę informatyki śledczej.
Umiejętności
EPU1 - Słuchacz potrafi odzyskiwać dane i zweryfikować zawartość materiału dowodowego oraz dokonać opisów czynności i je dokumentować.
Kompetencje społeczne
EPK1 - Słuchacz posiada zdolność do krytycznej oceny materiału dowodowego oraz do efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań informatyki śledczej.

E - Treści programowe oraz literatura

Forma zajęć, wykład:

1. Opiniowanie sądowo-informatyczne. Postanowienie o zasięgnięciu opinii. Dowód z opinii biegłego. Struktura opinii sądowo-informatycznej. Struktura opinii dotyczących badań nośników i informatyki śledczej. Struktura opinii dotycząca oceny systemów komputerowych i teleinformatycznych. Metodyka pracy biegłego. Specyfika opisów czynności i ich dokumentowania. Wnioski z ekspertyzy, opinii.
2. Automatyzacja procesów analizy śledczej i bezpłatne narzędzia wspomagające analizę śledczą oraz powłamaniową Środowisko do analizy i analiza zdarzeń w osi czasu.
3. Problemy odzyskiwania danych i problemy z weryfikacją zawartości materiału dowodowego

Razem liczba godzin wykładów	**8**
Forma zajęć, ćwiczenia: 1. Przygotowanie sprzętu, oprogramowania i nośników wykorzystywanych do ćwiczeń. 2. Przygotowanie i wykorzystanie maszyn wirtualnych z zainstalowanymi systemami operacyjnymi. 4. Odzyskiwanie i weryfikacja zawartości pozyskanego materiału dowodowego z komputerów, z urządzeń mobilnych i rejestratorów CCTV z wykorzystaniem automatyzacji procesów analizy śledczej i bezpłatnych narzędzi wspomagające analizę śledczą oraz powłamaniową - praktyczne przykłady (case study). 3. Opisywanie, dokumentowanie czynności - praktyczne przykłady (case study). 4. Przykłady opinii sądowych z zakresu informatyki: włamanie do systemu teleinformatycznego; kradzież z włamaniem na rachunek bankowy; badanie w sprawie o czyn z art. 200 § 1k.k; badanie oprogramowania - praktyczne przykłady (case study). **Razem liczba godzin wykładów**	**8**
Ogółem liczba godzin przedmiotu:	**16**

Literatura przedmiotu

Literatura obowiązkowa:

1. Altheide C, Carvey H, *Informatyka śledcza. Przewodnik po narzędziach open source*, Gliwice 2014
2. Chojnowski A., *Informatyka sądowa w praktyce,* Gliwice 2019
3. Darren R. Hayes, *Informatyka w kryminalistyce. Praktyczny przewodnik*. Gliwice 2021
4. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny*
5. Ustawa z dnia 6 czerwca 1997 r. *Kodeks postępowania karnego*

Literatura zalecana / fakultatywna:

1. Nikkel B.„ *Metody zabezpieczenia cyfrowego*, Warszawa, 2021
2. Rozporządzenie Ministra Sprawiedliwości z dnia 11 stycznia 2017 r. *w sprawie utrwalania obrazu lub dźwięku dla celów procesowych w postępowaniu karnym* (Dz.U. 2017 poz. 93)

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**
Wykłady:	
-	**P1 – Egzamin** (pisemny lub ustny) Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów i ćwiczeń
Ćwiczenia:	
F2 - Obserwacja/aktywność (realizacji zadań) **F5 - Ćwiczenia praktyczne** (ocena wykonywanych zadań)	-

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty	**Forma zajęć / Metoda oceniania**

przedmiotowe	Wykład		Ćwiczenia				
	P1	……...	**F2**	**F5**	……....		
EPW1	X	……...	X	X	……....		
EPU1	X	……...	X	X	……....		
EPK1	X	……...	X	X	……....		

G.4. Forma i warunki zaliczenia przedmiotu:

Zaliczenie z oceną

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	16
Czytanie literatury	12
Przygotowanie do ćwiczeń	12
Przygotowanie do egzaminu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

Załącznik nr 1
do *Programu studiów podyplomowych Zwalczanie cyberprzestępczości*
stanowiącego załącznik do Uchwały Nr 35/000/2022 Senatu AJP
z dnia 20 września 2022 r.

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Metodyka testów penetracyjnych z elementami socjotechniki

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 2**	**7. Liczba godzin ogółem: 16**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 8** **Ćwiczenia (Ć): 8**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz posiada pogłębioną wiedzę na temat sposobów, metod i technik pracy dotyczącej zwalczania cyberprzestępczości.
Umiejętności (CU):
Słuchacz potrafi wykorzystać dostępne narzędzia informatyczne w zwalczaniu cyberprzestępczości.
Kompetencje społeczne (CK):
Słuchacz postępuje zgodnie ze standardami i regulacjami prawnymi w zwalczania cyberprzestępczości.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1 - Słuchacz zna i rozumie metodykę testów penetracyjnych i specyfikę socjotechniki w problematyce zwalczania cyberprzestępczości.

Umiejętności

EPU1 - Słuchacz potrafi wykorzystać narzędzia informatyczne do testów penetracyjnych jak i znajomość specyfiki socjotechniki w problematyce zwalczania cyberprzestępczości.

Kompetencje społeczne

EPK1 - Słuchacz potrafi w praktyce stosować właściwe standardy prawne i etyczne, a także wykazywać się odpowiednią postawą z realizacji zadań dotyczących zwalczania cyberprzestępczości**.**

E - Treści programowe oraz literatura

Forma zajęć, wykład:

1. Specyfika, potrzeba oraz znaczenie testów penetracyjnych w analizie cyberprzestępczości.
2. Zasady, charakterystyka, stosowane narzędzia i oprogramowanie.
3. Automatyzacja procesów testów penetracyjnych.
4. Testy penetracyjne ze strony ofensywnej (Blue Flag).
5. Rekonesans. Skanowanie - narzędzie ping i przeczesywanie sieci za jego pomoc; skanowanie portów; skanowanie systemu pod kątem jego podatności na atak.

6. Wykorzystanie luk w zabezpieczeniach. Wykorzystywanie luk w zabezpieczeniach za pomocą przeglądarki internetowej. 7. Utrzymanie dostępu poprzez backdoor i rootkity. 8. Problematyka weryfikacji danych pozyskanych z testów penetracyjnych. 9. Socjotechnika - metody zasady działania sprawcy i oddziaływania na ofiarę. **Razem liczba godzin wykładów**	**8**
Forma zajęć, ćwiczenia: 1. Przygotowanie sprzętu, oprogramowanie i nośników wykorzystywanych do ćwiczeń. 2. Wykorzystanie maszyn wirtualnych z zainstalowanymi systemami operacyjnymi. 3. Wykorzystanie narzędzi udostępnionych poprzez platformę Linux Kali. 4. Skanowanie portów - praktyczne przykłady (case study). 5. Wykorzystanie luk w zabezpieczeniach - praktyczne przykłady (case study). 6. Analiza podsłuchanego ruchu sieciowego w poszukiwaniu wrażliwych danych - praktyczne przykłady (case study). 7. Przeszukiwanie infrastruktury w celu odnalezienia logów z loginami i hasłami - praktyczne przykłady (case study). 8. Aplikacje do łamania haseł - praktyczne przykłady (case study). 9. Tworzenie dokumentacji testów penetracyjnych pod kątem cyberprzestępczości - praktyczne przykłady (case study). **Razem liczba godzin wykładów**	**8**
Ogółem liczba godzin przedmiotu:	**16**

Literatura przedmiotu

Literatura obowiązkowa:

1. Engebretson P, *Hacking i testy penetracyjne. Podstawy*, Gliwice 2013.
2. Ziaja A., *Praktyczna analiza powłamaniowa. Aplikacja webowa w środowisku Linux*, Warszawa 2017.

Literatura zalecana / fakultatywna:

1. Altheide C,Carvey H, *Informatyka śledcza. Przewodnik po narzędziach open source*, Gliwice 2014
2. Hayes D.R., *Informatyka w kryminalistyce. Praktyczny przewodnik*. Gliwice 2021

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**
Wykłady:	
F1 – Sprawdzian (pisemny lub ustny)	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów i ćwiczeń
Ćwiczenia:	
F2 - Obserwacja/aktywność (realizacji zadań) **F5 - Ćwiczenia praktyczne** (ocena wykonywanych zadań)	-

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty	**Forma zajęć / Metoda oceniania**

przedmiotowe	Wykład		Ćwiczenia				
	F1	……...	**F2**	**F5**	…….....		
EPW1	X	……...	X	X	…….....		
EPU1	X	……...	X	X	…….....		
EPK1	X	……...	X	X	…….....		

G.4. Forma i warunki zaliczenia przedmiotu:
Zaliczenie z oceną

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	16
Czytanie literatury	10
Przygotowanie do ćwiczeń, korzystanie z repozytorium narzędzi informatycznych	14
Przygotowanie do sprawdzianu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Biały wywiad i Cyber Threat Intelligence

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 2**	**7. Liczba godzin ogółem: 16**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 8** **Ćwiczenia (Ć): 8**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz posiada pogłębioną wiedzę na temat sposobów, metod i technik pracy dotyczącej zwalczania cyberprzestępczości.
Umiejętności (CU):
Słuchacz potrafi dokonać oceny zachowania sprawcy cyberprzestępstwa i możliwości jego identyfikacji.
Słuchacz potrafi przeprowadzić ukierunkowane rozpoznanie internetowe oraz dokumentować ww. czynności.
Kompetencje społeczne (CK):
Słuchacz posiada zdolność krytycznej oceny sytuacji i efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań dotyczących zwalczania cyberprzestępczości.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się
Wiedza
EPW1 - Słuchacz zna i rozumie specyfikę pracy związanej ze zwalczaniem cyberprzestępczości.
Umiejętności
EPU1 - Słuchacz potrafi dokonać oceny zachowania sprawcy znając możliwości jego identyfikacji również za pomocą różnych środków i narzędzi.
EPU2 - Słuchacz potrafi przeprowadzić ukierunkowane rozpoznanie internetowe oraz dokumentować te czynności.
Kompetencje społeczne
EPK1 - Słuchacz posiada zdolność do krytycznej oceny sytuacji oraz efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań dotyczących zwalczania cyberprzestępczości**.**

E - Treści programowe oraz literatura

<u>Forma zajęć, wykład:</u>

1. Specyfika, potrzeba oraz znaczenie i rola Cyber Threat Intelligence w zwalczaniu cyberprzestępczości. Wprowadzenie do CTI i cyklu intelligence. Zadania i wsparcie CTI. Modele analityczne. DFIR – baza dla CTI. Profilowanie grup APT. Śledzenie grup APT. Modele zagrożeń.

Atrybucja. Techniki krytycznego myślenia. Analiza narzędzi, infrastruktury i danych z incydentów. Analiza powłamaniowa i interpretowanie wyników analizy powłamaniowej jako podstawowe atrybuty pracy analityka CTI. 2. Specyfika, potrzeba oraz znaczenie i rola Białego wywiadu w zwalczaniu cyberprzestępczości. Metody wydobywania i analizy danych. Przykłady otwartych źródeł informacji. Analiza otwartych źródeł internetowych z zastosowaniem metodologii sieci społecznych. Wybór źródeł danych. Proces pobierania i wydobywania informacji. Analiza sieci powiązań. Kryteria wyszukiwania. Analiza sentymentu. Śledzenie trendów. **Razem liczba godzin wykładów**	**8**
Forma zajęć, ćwiczenia: 1. Przygotowanie sprzętu, oprogramowania i nośników wykorzystywanych do ćwiczeń. 2. Wykorzystanie specyficznych narzędzi informatycznych do analizy OSINT i CTI - praktyczne przykłady (case study). Zalety oprogramowania Python do automatyzowania czynności, obliczeń scrapowania, analizowania danych w pracy OSINT-owców. 3. Analiza otwartych źródeł internetowych z zastosowaniem metodologii sieci społecznych - praktyczne przykłady (case study). 4. Przeprowadzenie ukierunkowanego rozpoznania internetowego - praktyczne przykłady (case study). 5. Dokumentowanie czynności ukierunkowanego rozpoznania internetowego - praktyczne przykłady (case study). Tworzenie raportu OSINT - praktyczne przykłady (case study). 6. Analiza powłamaniowa i interpretowanie wyników analizy powłamaniowej. Dokumentowanie czynności z analiz i śledzenia cyberzagrożeń (CTI) - praktyczne przykłady (case study). **Razem liczba godzin wykładów**	**8**
Ogółem liczba godzin przedmiotu:	**16**

Literatura przedmiotu

Literatura obowiązkowa:

1. Carvey H, *Analiza śledcza i powłamaniowa. Zaawansowane techniki prowadzenia analizy w systemie Windows 7*. Gliwice 2013.
2. Hayes D.R, *Informatyka w kryminalistyce. Praktyczny przewodnik*. Wydanie II, Gliwice 2021.
3. Filipkowski W, Mądrzejowski W, *Biały wywiad. Otwarte źródła informacji - wokół teorii i praktyk*i, Beck 2011.

Literatura zalecana / fakultatywna:

1. Liedel K, Serafin T, *Otwarte źródła informacji w działalności wywiadowczej*, Difin 2011.

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**
Wykłady:	
F1 – Sprawdzian (pisemny lub ustny)	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów i ćwiczeń
Ćwiczenia:	

F2 - Obserwacja/aktywność (realizacji zadań) **F5 - Ćwiczenia praktyczne** (ocena wykonywanych zadań)	**-**

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**						
	Wykład		Ćwiczenia				
	F1		**F2**	**F5**			
EPW1	X		X	X			
EPU1	X		X	X			
EPU2	X		X	X			
EPK1	X		X	X			

G.4. Forma i warunki zaliczenia przedmiotu:

Zaliczenie z oceną

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	16
Czytanie literatury	10
Przygotowanie do ćwiczeń, korzystanie z repozytorium narzędzi informatycznych	14
Przygotowanie do sprawdzianu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Wprowadzenie do analizy malware

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 2**	**7. Liczba godzin ogółem: 16**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 8** **Ćwiczenia (Ć): 8**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz posiada pogłębioną wiedzę na temat sposobów, metod i technik pracy dotyczącej zwalczania cyberprzestępczości.
Umiejętności (CU):
Słuchacz potrafi wykorzystać dostępne narzędzia informatyczne w zwalczaniu cyberprzestępczości.
Kompetencje społeczne (CK):
Słuchacz postępuje zgodnie ze standardami i regulacjami prawnymi w zwalczania cyberprzestępczości.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się
Wiedza
EPW1 - Słuchacz zna i rozumie problematykę informatycznej analizy złośliwego oprogramowania w problematyce zwalczania cyberprzestępczości.
Umiejętności
EPU1 - Słuchacz potrafi wykorzystać narzędzia informatyczne do specyfiki analizy złośliwego oprogramowania w problematyce zwalczania cyberprzestępczości.
Kompetencje społeczne
EPK1 - Słuchacz potrafi w praktyce stosować właściwe standardy prawne i etyczne, a także wykazywać się odpowiednią postawą z realizacji zadań dotyczących zwalczania cyberprzestępczości**.**

E - Treści programowe oraz literatura

Forma zajęć, wykład:

1. Specyfika, potrzeba oraz znaczenie analizy złośliwego oprogramowania w analizie przestępczości komputerowej.
2. Rodzaje złośliwego oprogramowania. Ogólne zasady analizy malware. Funkcjonalności malware
3. Zasady, charakterystyka, stosowane narzędzia i oprogramowanie do analizy złośliwego oprogramowania.
4. Ukryte uruchamianie malware – wstęp do analizy pamięci RAM.

5. Szyfrowanie danych na przykładzie ransomware. 6. Automatyzacja procesów analizy złośliwego oprogramowania. 7. Analiza statyczna i analiza dynamiczna złośliwego oprogramowania - podstawowe narzędzia. 8. Raporty z analizy złośliwego oprogramowania. **Razem liczba godzin wykładów**	**8**
Forma zajęć, ćwiczenia: 1. Przygotowanie sprzętu, oprogramowanie i nośników wykorzystywanych do ćwiczeń. 2. Wykorzystanie maszyn wirtualnych z zainstalowanymi systemami operacyjnymi. 3. Przygotowanie środowiska do analizy automatycznej złośliwego oprogramowania. - praktyczne przykłady (case study). 4. Podstawowe narzędzia w analizie statycznej i dynamicznej złośliwego oprogramowania - praktyczne przykłady (case study). 5. Analiza malware na maszynach wirtualnych. Wykorzystanie narzędzi VmWare Workstation Pro lub VirtualBox firmy Oracle - praktyczne przykłady (case study). 6. Analiza wyników - praktyczne przykłady (case study). 7. Tworzenie raportów - praktyczne przykłady (case study). **Razem liczba godzin wykładów**	**8**
Ogółem liczba godzin przedmiotu:	**16**

Literatura przedmiotu

Literatura obowiązkowa:

1. Sikorski M, Honig A, *Praktyczna Analiza Malware. Przewodnik po usuwaniu złośliwego oprogramowania,* Warszawa 2021

Literatura zalecana / fakultatywna:

1. Hickey M, Arcur Ji, *Warsztat hakera. Testy penetracyjne i inne techniki wykrywania podatności*, Gliwice, 2022
2. Hayes D.R., *Informatyka w kryminalistyce. Praktyczny przewodnik.* , Gliwice 2021

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**

Wykłady:

F1 – Sprawdzian (pisemny lub ustny)	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów i ćwiczeń

Ćwiczenia:

F2 - Obserwacja/aktywność (realizacji zadań) **F5 - Ćwiczenia praktyczne** (ocena wykonywanych zadań)	-

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**						
	Wykład		Ćwiczenia			Laboratoria	
	F1	……...	**F2**	**F5**	…….....	……...	……...
EPW1	X	……...	X	X	…….....	……...	……...

EPU1	X	……...	X	X	……....	……...	……....
EPK1	X	……...	X	X	……....	……...	……....

G.4. Forma i warunki zaliczenia przedmiotu:

Zaliczenie z oceną

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	16
Czytanie literatury	10
Przygotowanie do ćwiczeń, korzystanie z repozytorium narzędzi informatycznych	14
Przygotowanie do sprawdzianu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek studiów podyplomowych	Zwalczane cyberprzestępczości

PROGRAM PRZEDMIOTU

A - Informacje ogólne

1. Przedmiot: Wymiar sprawiedliwości i pomoc prawna w dochodzeniach karnych w cyberprzestrzeni

2. Punkty ECTS: 2

3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: 1	**6. Semestr/y: 2**	**7. Liczba godzin ogółem: 16**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (W): 8** **Ćwiczenia (Ć): 8**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia:		**Dr Sylwia Gwoździewicz**

B - Wymagania wstępne

Brak wymagań wstępnych

C - Cele kształcenia

Wiedza(CW):
Słuchacz posiada pogłębioną wiedzę na temat krajowych i międzynarodowych uregulowań prawnych zwalczania cyberprzestępczości.
Umiejętności (CU):
Słuchacz potrafi analizować i wyjaśnić problemy współpracy w zwalczania cyberprzestępczości.
Kompetencje społeczne (CK):
Słuchacz posiada zdolność radzenia sobie z problemami prawnymi wynikającymi ze specyfiki zwalczania przestępczości w cyberprzestrzeni

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1 - Słuchacz zna i rozumie problemy współpracy z wymiarem sprawiedliwości i pomocą prawną w dochodzeniach karnych w cyberprzestrzeni.

Umiejętności

EPU1 - Słuchacz potrafi stosować narzędzia prawne współpracy z wymiarem sprawiedliwości w dochodzeniach karnych w cyberprzestrzeni.

Kompetencje społeczne

EPK1 - Słuchacz potrafi w praktyce stosować właściwe standardy prawne i etyczne współpracy z wymiarem sprawiedliwości i pomocą prawną w dochodzeniach karnych w cyberprzestrzeni.

E - Treści programowe oraz literatura

Forma zajęć, wykład:

1. Narzędzia prawne oraz prawna organizacja wyspecjalizowanych agencji i organów UE w obszarze przeciwdziałania cyberprzestępczości.
2. Wybrane inicjatywy europejskie w walce z cyberprzestępczością. Działania Rady Europy w kontekście

problematyki transgranicznego dostępu do danych elektronicznych i jurysdykcji. Działania Unii Europejskiej w kontekście problematyki transgranicznego dostępu do danych i jurysdykcji 3. Problematyka jurysdykcji w cyberprzestrzeni. 4. Usprawnienie wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni 5. Prawne instrumenty finansowego i technologicznego wsparcia dla współpracy policyjnej w zapobieganiu i zwalczaniu przestępczości oraz zarządzania kryzysowego. **Razem liczba godzin wykładów**	**8**
Forma zajęć, ćwiczenia: 1. Analiza obszarów działań i współpracy międzynarodowej na przykładzie np. Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) oraz Eurojust i Europejskie Centrum do spraw Walki z Cyberprzestępczością (EC3). 2. Jurysdykcja w cyberprzestrzeni – analiza wybranych przykładów(case study). 3. Współpraca pomiędzy organami policyjnymi, sądowniczymi i ekspertami ds. cyberprzestępczości - praktyczne przykłady (case study). **Razem liczba godzin wykładów**	**8**
Ogółem liczba godzin przedmiotu:	**16**

Literatura przedmiotu

Literatura obowiązkowa:

1. Białkowski M, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Wydawnictwo: CEDEWU, 2016
2. Gwoździewicz S. *Wymiar sprawiedliwości i pomoc prawna w dochodzeniach karnych w cyberprzestrzen*i, [w:] Prawa człowieka i zrównoważony rozwój. Konwergencja czy dywergencja idei i polityki, red. Bieńkowska D. Kozłowski R, Beck Warszawa 2020
3. Gwoździewicz S, *Problematyka cyberataków w dobie Przemysłu 4.0 a ściganie przestępstw dotyczących sieci i systemów informatycznych w dochodzeniach karnych w cyberprzestrzeni* [w] Perspektywy bezpieczeństwa. Wybrane zagadnienia teorii i praktyki (red.) Chodak P,Krassowski K, Winogrodzki G, AGH Kraków 2021.
4. Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. wraz z protokołami dodatkowymi.
5. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol)
6. Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych.

Literatura zalecana / fakultatywna:

1. Jaroszewska I.A, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne,* Wydanie Uniwersytet Warmińsko-Mazurski, Olsztyn 2017 r.
2. Olber P *Prawno-kryminalistyczne aspekty zabezpieczania i pozyskiwania dowodów elektronicznych z chmur obliczeniowych,* Wyższa Szkoła Policji, Szczytno 2021.
3. Opitek P, *Skimming – aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Beck 2017 r.
4. Stefański R.A, *Metodyka pracy prokuratora w sprawach karnych,* Wyd. Wolters Kluwer, Warszawa 2017 r.
5. Samborski E, *Zarys metodyki pracy sędziego w sprawach karnych*, Wyd. LexisNexis, Warszawa 2013 r.
6. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny
7. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego

F – Metody kształcenia oraz środki dydaktyczne

M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia).

G - Weryfikacja osiągnięcia efektów uczenia się

G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu	**Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.**

studentów, a studentowi pomaga w uczeniu się.	
Wykłady:	
-	**P1 – Egzamin** (ustny lub pisemny) Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych z wykładów i ćwiczeń.
Ćwiczenia:	
F2 - Obserwacja/aktywność (podczas realizacji ćwiczeń) **F5 - Ćwiczenia praktyczne** (ocena ćwiczeń wykonywanych podczas zajęć)	-

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	Forma zajęć / Metoda oceniania						
	Wykład		Ćwiczenia			Laboratoria	
	P1	……...	**F2**	**F5**	……...	……...	……...
EPW1	X	……...	X	X	……...	……...	……...
EPU1	X	……...	X	X	……...	……...	……...
EPK1	X	……...	X	X	……...	……...	……...

G.4. Forma i warunki zaliczenia przedmiotu:

Egzamin

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	16
Czytanie i analiza literatury przedmiotu	14
Przygotowanie do ćwiczeń	10
Przygotowanie do egzaminu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	Dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	08.09.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz