Załącznik nr 3
do Programu studiów na kierunku bezpieczeństwo narodowe - studia drugiego stopnia o profilu praktycznym,
stanowiącego załącznik do Uchwały Nr 14/000/2022 Senatu AJP
z dnia 21 czerwca 2022 r.

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Drugiego stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		ZC.1

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Uregulowania prawne i taktyka prowadzenia wybranych czynności dowodowych**
Punkty ECTS	**3**
Rodzaj zajęć	**Obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępstw**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	**Liczba godzin Stacjonarne/niestacjonarne**	**Rok studiów/semestr**	**Punkty ECTS** (zgodnie z programem studiów)
wykład	**30/15**	**II/III**	**3**
ćwiczenia	**15/12**	**II/III**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych

4. Cele kształcenia

C1 – Rozszerzenie dotychczasowej wiedzy na temat krajowych i międzynarodowych uregulowań prawnych zwalczania cyberprzestępczości.
C2 – Rozwinięcie umiejętności analizowania i wyjaśniania problemów prawnych i dowodowych przestępstw popełnianych w cyberprzestrzeni.
C3 – Nabycie umiejętności radzenia sobie z problemami wynikający ze specyfiki prowadzenia wybranych czynności dowodowych.

5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	**Opis efektu uczenia się**	**Odniesienie do efektu kierunkowego**
WIEDZA		
W_01	Słuchacz zna i rozumie uregulowania prawne i taktykę dowodową w zwalczaniu cyberprzestępczości oraz potrafi wykorzystać zdobyty zasób wiedzy w praktyce.	K_W08
UMIEJĘTNOŚCI		

U_01	Słuchacz potrafi zabezpieczyć fizycznie oraz przeprowadzić oględziny sprzętu komputerowego i elektronicznych nośników danych oraz sporządzić w tym zakresie dokumentację.	K_U06
KOMPETENCJE SPOŁECZNE		
K_01	Słuchacz posiada zdolność do efektywnego radzenia sobie z problemami prawnymi, dowodowymi i sprzętowymi w specyfice przestępstw popełnianych w cyberprzestrzeni.	K_K13

6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć (zgodnie z programem studiów):

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Znamiona i specyfika wybranych przestępstw popełnianych w cyberprzestrzeni wraz z ich kwalifikacją prawną.	7	3
W2	Pojęcie dowodu elektronicznego w aspekcie art. 115 §14 KK oraz przepisów KPK - definicje. Oględziny: pojęcie oględzin, przedmiot oględzin. Przeszukanie: pojęcie przeszukania, sposób prowadzenia przeszukania.	7	4
W3	Krajowe i międzynarodowe uregulowania prawne (m.in. Konwencja Rady Europy, Europejski Nakaz Dochodzeniowy).	7	4
W4	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.	9	4
	Razem liczba godzin wykładów	30	15

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Określanie na podstawie praktycznych przykładów (case study) ustawowych znamion przestępstw popełnianych w cyberprzestrzeni.	3	3
C2	Interpretowanie na podstawie praktycznych przykładów (case study) różnych pojęć, zwłaszcza dowodu elektronicznego i cyfrowego, oględzin, przeszukania.	4	3
C3	Przeprowadzanie oględzin sprzętu komputerowego i elektronicznych nośników danych oraz tworzenie dokumentacji - praktyczne przykłady (case study).	4	3
C4	Przeprowadzanie przeszukania (pomieszczenia, systemu komputerowego) - praktyczne przykłady (case study).	4	3
	Zabezpieczanie fizyczne sprzętu elektronicznego i nośników danych - praktyczne przykłady (case study).		
	Razem liczba godzin ćwiczeń	15	12

7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M2 – metoda** problemowa: wykład problemowy **M4 – metoda programowa**: wykład z wykorzystaniem materiałów multimedialnych.	projektor multimedialny, oprogramowanie specjalistyczne

Ćwiczenia	**M5 – metoda praktyczna**: ćwiczenia przedmiotowe	projektor multimedialny, oprogramowanie specjalistyczne

8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta

8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	Ocena formująca (F)	Ocena podsumowująca (P) –
Wykład	----------	**F1 – sprawdzian** pisemny.
Ćwiczenia	**F2 – obserwacja/aktywność** podczas realizacji ćwiczeń wykonywanych podczas zajęć **F5 – ćwiczenia praktyczne:** ocena ćwiczeń wykonywanych podczas zajęć.	**Ocena podsumowująca** jest sumą ocen formułujących.

8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Symbol efektu	Wykład	Ćwiczenia	
	F1	F2	F5
W_01	x	x	x
U_01	x	x	x
K_01	x	x	x

9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Ocena formułująca - ćwiczenia:
Student realizuje prace/ćwiczenia/projekty za które prowadzący przyznaje punkty (prace/ćwiczenia/projekty terminowe lub na zajęciach). W toku zajęć student może uzyskać max 100 pkt.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

Ocena podsumowująca oceny jest sumą ocen formułujących.

Student, który nie uzyskał wymaganej minimalnej liczby punktów potrzebnej do zaliczenia ćwiczeń może w czasie sesji przystąpić do kolokwium poprawkowego. Kolokwium poprawkowe obejmuje materiał z całego semestru.

Ocena podsumowująca – wykład
Ocena ze sprawdzianu ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Egzamin

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	**na studiach niestacjonarnych**
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**45**	**27**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do egzaminu	10	16
przygotowanie do realizacji zajęć	7	13
wykonanie ćwiczeń	8	14
zapoznanie z literaturą	5	5
suma godzin:	**75**	**75**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**3**	**3**

12. Literatura zajęć

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*, 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,* Warszawa 2015.
2. Jaroszewska I.A., *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017.
3. Opitek P., *Skimming – aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Warszawa 2017.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Joanna Lubimow
data sporządzenia / aktualizacji	10 czerwca 2022 r.
dane kontaktowe (e-mail)	jlubimow@ajp.edu.pl
podpis	

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Drugiego stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		ZC.2

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Działania operacyjne w Internecie**
Punkty ECTS	**3**
Rodzaj zajęć	**Obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępstw**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	**Liczba godzin Stacjonarne/niestacjonarne**	**Rok studiów/semestr**	**Punkty ECTS** (zgodnie z programem studiów)
wykład	**30/15**	**II/III**	**3**
ćwiczenia	**12/15**	**II/III**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych

4. Cele kształcenia

C1 – Rozszerzenie dotychczasowej wiedzy na metod operacyjnych w Internecie.
C2 – Nabycie umiejętności przeprowadzenia ukierunkowanego rozpoznania internetowego.
C3 – Nabycie umiejętności radzenia sobie z problemami wynikającymi ze specyfiki działań operacyjnych w Internecie.

5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	**Opis efektu uczenia się**	**Odniesienie do efektu kierunkowego**
	WIEDZA	
W_01	Słuchacz zna i rozumie problemy związane z działaniami operacyjnymi oraz potrafi wykorzystać zdobyty zasób wiedzy w praktyce.	K_W07
	UMIEJĘTNOŚCI	
U_01	Słuchacz potrafi przeprowadzić rozpoznanie internetowe oraz	K_U07

	zweryfikować uzyskane informacje.	
KOMPETENCJE SPOŁECZNE		
K_01	Słuchacz posiada zdolność do efektywnego radzenia sobie z problemami działań operacyjnych w Internecie.	K_K09

6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć (zgodnie z programem studiów):

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Pojęcie czynności operacyjno-rozpoznawczych w systemie prawa polskiego. Katalog metod pracy operacyjnej – odniesienie do współczesnych rozwiązań prawnych. Ryzyko w czynnościach operacyjno-rozpoznawczych Policji.	3	2
W2	Możliwości prowadzenia pracy operacyjnej w Internecie.	4	2
W3	Metody pozyskiwania danych z Internetu przy użyciu ogólnodostępnych baz danych, ustalenia teleinformatyczne i internetowe.	4	2
W4	Zaawansowane metody pozyskiwania informacji z Internetu przy użyciu wyszukiwarek Internetowych.	4	2
W5	Tożsamość internetowa.	4	2
W6	Weryfikacja autentyczności uzyskanych informacji.	4	2
W7	Ustalenia w trybie art.20 i art.20c Ustawy o Policji, oraz procedura przekazywania uzyskanych danych do postępowania karnego.	4	2
W8	Zasady składania wniosków do operatorów i podmiotów zagranicznych (Facebook, Twitter, Instagram, etc.).	3	1
	Razem liczba godzin wykładów	30	15

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Określanie na podstawie praktycznych przykładów (case study) możliwości pracy operacyjnej w Internecie oraz jej ograniczeń.	3	3
C2	Uzyskiwanie, interpretowanie i analizowanie danych z otwartych źródeł informacji na praktycznych przykładach (case study).	4	3
C3	Wykorzystywanie narzędzi do zaawansowanego wyszukiwania informacji.	4	3
C4	Weryfikowanie autentyczności uzyskanych danych. Tworzenie, wykorzystywanie, weryfikowanie i interpretowanie tożsamości internetowej.	4	3
	Razem liczba godzin ćwiczeń	15	12

7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M2 – metoda** problemowa: wykład problemowy **M4 – metoda programowa**: wykład z wykorzystaniem materiałów multimedialnych.	projektor multimedialny, oprogramowanie specjalistyczne
Ćwiczenia	**M5 – metoda praktyczna**: ćwiczenia z wykorzystaniem dostępnych wyszukiwarek internetowych, storn agregujących informacje o	projektor multimedialny, oprogramowanie specjalistyczne

	użytkownikach Internetu z otwartych źródeł.	

8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta

8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	Ocena formująca (F)	Ocena podsumowująca (P) –
Wykład	----------	F1 – sprawdzian pisemny
Ćwiczenia	**F2 – obserwacja/aktywność** podczas realizacji ćwiczeń wykonywanych podczas zajęć **F5 – ćwiczenia praktyczne:** ocena ćwiczeń wykonywanych podczas zajęć.	**Ocena podsumowująca** jest sumą ocen formułujących.

8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Symbol efektu	Wykład	Ćwiczenia	
	F1	F2	F5
W_01	x	x	x
U_01	x	x	x
K_01	x	x	x

9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Ocena formułująca - ćwiczenia:
Student realizuje prace/ćwiczenia/projekty za które prowadzący przyznaje punkty (prace/ćwiczenia/projekty terminowe lub na zajęciach). W toku zajęć student może uzyskać max 100 pkt.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

Ocena podsumowująca oceny jest sumą ocen formułujących.

Student, który nie uzyskał wymaganej minimalnej liczby punktów potrzebnej do zaliczenia ćwiczeń może w czasie sesji przystąpić do kolokwium poprawkowego. Kolokwium poprawkowe obejmuje materiał z całego semestru.

Ocena podsumowująca – wykład
Ocena ze sprawdzianu ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Zaliczenie z oceną

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	**na studiach niestacjonarnych**
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**45**	**27**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do sprawdzianu	8	14
przygotowanie do zajęć	8	14
przygotowanie do wykonywania ćwiczeń, wykonanie ćwiczeń	9	15
zapoznanie z literaturą	5	5
suma godzin:	**75**	**75**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**3**	**3**

12. Literatura zajęć

Literatura obowiązkowa:

1. Kudła J., Kosmaty P.*, Ryzyko w czynnościach operacyjno-rozpoznawczych Policji. Aspekty kryminalistyczne i prawnodowodowe,* Warszawa 2018.
2. Sprengel B., *Praca operacyjna Policji*, Toruń 2018.
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,* Warszawa 2019.
2. Darren R. Hayes, *Informatyka w kryminalistyce. Praktyczny przewodnik*, Gliwice 2021.
3. Nikkel B.,, *Metody zabezpieczenia cyfrowego*, Warszawa 2021.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Joanna Lubimow
data sporządzenia / aktualizacji	10 czerwca 2022 r.
dane kontaktowe (e-mail)	jlubimow@ajp.edu.pl
podpis	

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Drugiego stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		ZC.3

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Wstęp do informatyki**
Punkty ECTS	**2**
Rodzaj zajęć	**Obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępstw**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	**Liczba godzin Stacjonarne/niestacjonarne**	**Rok studiów/semestr**	**Punkty ECTS** (zgodnie z programem studiów)
wykład	**15/15**	**II/III**	**2**
ćwiczenia	**10/8**	**II/III**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych

4. Cele kształcenia

C1 – Rozszerzenie dotychczasowej wiedzy na temat podstaw informatyki.
C2 – Rozszerzenie umiejętności analizowania i wyjaśniania problemów związanych z informatyką
C3 – Nabycie umiejętności radzenia sobie z problemami wynikający ze specyfiki informatyki

5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	**Opis efektu uczenia się**	**Odniesienie do efektu kierunkowego**
	WIEDZA	
W_01	Słuchacz zna i rozumie podstawy informatyki i potrafi wykorzystać zdobyty zasób wiedzy w specyfice zwalczania cyberprzestępczości.	K_W07
	UMIEJĘTNOŚCI	
U_01	Słuchacz potrafi analizować systemy operacyjne i sieci komputerowe, pozyskiwać i wykorzystywać zapisane w nich dane informatyczne w	K_U03

	zwalczaniu cyberprzestępczości.	
KOMPETENCJE SPOŁECZNE		
K_01	Słuchacz posiada zdolność do efektywnego radzenia sobie z problemami związanymi z informatyką w specyfice zwalczania cyberprzestępczości.	K_K09

6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć (zgodnie z programem studiów):

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Wprowadzenie do teorii informatyki.	3	2
W2	Wstęp do systemów operacyjnych z rodziny Windows	3	2
W3	Wstęp do systemów operacyjnych z rodziny Linux	3	2
W4	Wstęp do systemów operacyjnych z rodziny macOs	3	2
W5	Wstęp do sieci komputerowych (adresacja IP, DNS, TOR).	3	2
	Razem liczba godzin wykładów	15	10

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Korzystanie z systemów operacyjnych pracujących na maszynach wirtualnych.	3	2
C2	Wykonywanie cech charakterystycznych dla systemów operacyjnych Windows, Linux, macOs, oraz podstawowych poleceń systemowych.	4	2
C3	Wykonywanie operacji związanych z uzyskaniem informacji nt. sprzętowej konfiguracji komputera, interfejsów sieciowych, artefaktów systemu.	4	2
C4	Interpretacja zapisów logów systemowych, plików konfiguracyjnych, zapisów rejestrów	4	2
	Razem liczba godzin ćwiczeń	15	8

7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M2 – metoda** problemowa: wykład problemowy **M4 – metoda programowa**: wykład z wykorzystaniem materiałów multimedialnych.	projektor multimedialny, oprogramowanie specjalistyczne
Ćwiczenia	**M5 – metoda praktyczna**: ćwiczenia przedmiotowe	projektor multimedialny, oprogramowanie specjalistyczne

8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta

8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	Ocena formująca (F)	Ocena podsumowująca (P) –
Wykład	----------	**F1** – sprawdzian (ustny lub pisemny)
Ćwiczenia	**F2 – obserwacja/aktywność** podczas realizacji ćwiczeń wykonywanych podczas zajęć **F5 – ćwiczenia praktyczne:** ocena	**Ocena podsumowująca** jest sumą ocen formułujących.

	ćwiczeń wykonywanych podczas zajęć.	

8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Symbol efektu	Wykład	Ćwiczenia	
	F1	F2	F5
W_01	x	x	x
U_01	x	x	x
K_01	x	x	x

9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Ocena formułująca - ćwiczenia:
Student realizuje prace/ćwiczenia/projekty za które prowadzący przyznaje punkty (prace/ćwiczenia/projekty terminowe lub na zajęciach). W toku zajęć student może uzyskać max 100 pkt.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

Ocena podsumowująca oceny jest sumą ocen formułujących.

Student, który nie uzyskał wymaganej minimalnej liczby punktów potrzebnej do zaliczenia ćwiczeń może w czasie sesji przystąpić do kolokwium poprawkowego. Kolokwium poprawkowe obejmuje materiał z całego semestru.

Ocena podsumowująca – wykład
Ocena ze sprawdzianu ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Zaliczenie z oceną

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**30**	**18**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		

przygotowanie do sprawdzianu	7	13
przygotowanie do realizacji zajęć, wykonanie ćwiczeń,	8	14
zapoznanie z literaturą	5	5
suma godzin:	**50**	**50**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**2**	**2**

12. Literatura zajęć

Literatura obowiązkowa:

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

Literatura zalecana / fakultatywna:

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

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Joanna Lubimow
data sporządzenia / aktualizacji	10 czerwca 2022 r.
dane kontaktowe (e-mail)	jlubimow@ajp.edu.pl
podpis	

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Drugiego stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		ZC.4

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Analiza śledcza w sprawach związanych z cyberprzestępczością**
Punkty ECTS	**3**
Rodzaj zajęć	**Obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępstw**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	**Liczba godzin Stacjonarne/niestacjonarne**	**Rok studiów/semestr**	**Punkty ECTS** (zgodnie z programem studiów)
wykład	**30/15**	**II/III**	**3**
ćwiczenia	**15/12**	**II/III**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych

4. Cele kształcenia

C1 – Zdobycie wiedzy na temat analizy śledczej w sprawach związanych z cyberprzestępczością.
C2 – Nabycie umiejętności analizowania i wyjaśniania sprawy/stanu faktycznego w realizacji zadań dotyczących analizy śledczej w sprawach związanych z cyberprzestępczością.
C3 – Nabycie zdolności krytycznej oceny sytuacji i efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań dotyczących analizy śledczej w sprawach związanych z cyberprzestępczością.

5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	**Opis efektu uczenia się**	**Odniesienie do efektu kierunkowego**
	WIEDZA	
W_01	Słuchacz zna i rozumie metody i techniki analizy śledczej w sprawach związanych z cyberprzestępczością.	K_W08
	UMIEJĘTNOŚCI	

U_01	Słuchacz potrafi przeprowadzić ukierunkowane rozpoznanie w sprawach związanych z cyberprzestępczością z wykorzystaniem analizy śledczej w sprawach związanych z cyberprzestępczością.	K_U06
KOMPETENCJE SPOŁECZNE		
K_01	Słuchacz posiada zdolność do krytycznej oceny materiału dowodowego do efektywnego radzenia sobie z problemami wynikającymi z analizy śledczej w sprawach związanych z cyberprzestępczością.	K_K07

6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć (zgodnie z programem studiów):

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Problematyka, metody i techniki analizy śledczej w sprawach związanych z cyberprzestępczością.	7	3
W2	Wstępna ocena cyfrowego materiału dowodowego.	7	4
W3	Kryptowaluty w sprawach związanych z cyberprzestępczością	8	4
W4	Sieci anonimizujące w sprawach związanych z cyberprzestępczością.	8	4
	Razem liczba godzin wykładów	30	15

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Przygotowanie darmowego oprogramowania forensics do zajęć .	3	2
C2	Ujawnianie i zabezpieczanie śladów korzystania z kryptowalut. Wykorzystanie portfeli do zobrazowania przepływów kryptowalut. Wykorzystanie opracowanej metodyki zabezpieczania kryptowalut - praktyczne przykłady (case study).	3	2
C3	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).	3	2
C4	Przeprowadzanie podstawowej oceny zabezpieczonego materiału dowodowego - praktyczne przykłady (case study).	3	3
C5	Opisywanie, dokumentowanie czynności - praktyczne przykłady (case study).	3	3
	Razem liczba godzin ćwiczeń	15	12

7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M2 – metoda** problemowa: wykład problemowy **M4 – metoda programowa**: wykład z wykorzystaniem materiałów multimedialnych.	projektor multimedialny, oprogramowanie specjalistyczne
Ćwiczenia	**M5 – metoda praktyczna**: ćwiczenia praktyczne	projektor multimedialny, oprogramowanie specjalistyczne

8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta

8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	Ocena formująca (F)	Ocena podsumowująca (P) –

Wykład	**----------**	**F1 – sprawdzian** (pisemny)
Ćwiczenia	**F2 – obserwacja/aktywność** podczas realizacji ćwiczeń wykonywanych podczas zajęć **F5 – ćwiczenia praktyczne:** ocena ćwiczeń wykonywanych podczas zajęć.	**Ocena podsumowująca** jest sumą ocen formułujących.

8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Symbol efektu	Wykład	Ćwiczenia	
	F1	F2	F5
W_01	x		x
U_01	x	x	x
K_01	x	x	

9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Ocena formułująca - ćwiczenia:
Student realizuje prace/ćwiczenia/projekty za które prowadzący przyznaje punkty (prace/ćwiczenia/projekty terminowe lub na zajęciach). W toku zajęć student może uzyskać max 100 pkt.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

Ocena podsumowująca oceny jest sumą ocen formułujących.

Student, który nie uzyskał wymaganej minimalnej liczby punktów potrzebnej do zaliczenia ćwiczeń może w czasie sesji przystąpić do kolokwium poprawkowego. Kolokwium poprawkowe obejmuje materiał z całego semestru.

Ocena podsumowująca – wykład
Ocena ze sprawdzianu ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Egzamin

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

Forma aktywności studenta	**Liczba godzin**	
	na studiach stacjonarnych	**na studiach niestacjonarnych**

Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**45**	**27**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do egzaminu	8	14
przygotowanie do zajęć	8	14
przygotowanie do wykonywania ćwiczeń, wykonanie ćwiczeń	9	15
zapoznanie z literaturą	5	5
suma godzin:	**75**	**75**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**3**	**3**

12. Literatura zajęć

Literatura obowiązkowa:

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

Literatura zalecana / fakultatywna

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

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Joanna Lubimow
data sporządzenia / aktualizacji	10 czerwca 2022 r.
dane kontaktowe (e-mail)	jlubimow@ajp.edu.pl
podpis	

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Drugiego stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		ZC.5

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Podstawy informatyki śledczej**
Punkty ECTS	**3**
Rodzaj zajęć	**Obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępstw**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	**Liczba godzin Stacjonarne/niestacjonarne**	**Rok studiów/semestr**	**Punkty ECTS** (zgodnie z programem studiów)
wykład	**30/15**	**II/III**	**3**
ćwiczenia	**15/12**	**II/III**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych

4. Cele kształcenia

C1 – Zdobycie wiedzy na temat narzędzi wykorzystywanych w informatyce śledczej.
C2 – Nabycie umiejętności ujawniania i zabezpieczania śladów i dowodów zgodnie ze specyfiką informatyki śledczej.
C3 – Nabycie umiejętności krytycznej oceny sytuacji i efektywnego radzenia sobie z problemami wynikającymi z realizacji powierzonych zadań.

5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	**Opis efektu uczenia się**	**Odniesienie do efektu kierunkowego**
WIEDZA		
W_01	Słuchacz zna i rozumie specyfikę informatyki śledczej.	K_W07
UMIEJĘTNOŚCI		
U_01	Słuchacz potrafi ujawnić i zabezpieczyć cyfrowy materiał dowodowy.	K_U12

KOMPETENCJE SPOŁECZNE		
K_01	Słuchacz posiada zdolność do krytycznej oceny materiału dowodowego oraz do efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań informatyki śledczej.	K_K09

6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć (zgodnie z programem studiów):

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Wstęp do informatyki śledczej.	3	2
W2	Informatyka śledcza i narzędzia typu open source. Cele dochodzeń informatyki śledczej. Proces cyfrowej analizy śledczej. Informatyk śledczy – rola w procesie wykrywczym.	4	2
W3	Problematyka ujawniania i zabezpieczania materiału dowodowego z Internetu.	4	2
W4	Problematyka ujawniania i zabezpieczania materiału dowodowego pozyskiwanego z komputerów.	4	2
W5	Problematyka ujawniania i zabezpieczania materiału dowodowego pozyskiwanego z komputerów.	3	2
W6	Problematyka ujawniania i zabezpieczania materiału dowodowego z rejestratorów CCTV.	3	2
W7	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.	3	1
W8	Automatyzacja procesów analizy śledczej i bezpłatne narzędzia wspomagające analizę śledczą oraz powłamaniową. Środowisko do analizy i analiza zdarzeń w osi czasu.	3	1
W9	Problemy odzyskiwania danych i problemy z weryfikacją zawartości materiału	3	1
	Razem liczba godzin wykładów	30	15

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Zasady, charakterystyka, stosowane narzędzia i oprogramowanie	1	1
C2	Praktyczne przykłady (case study) ujawniania i zabezpieczania materiałów dowodowych z Internetu.	1	1
C3	Praktyczne przykłady (case study) ujawniania i zabezpieczania materiałów dowodowych z komputerów	1	1
C4	Praktyczne przykłady (case study) ujawniania i zabezpieczania materiałów dowodowychz urządzeń mobilnych	2	1
C5	Praktyczne przykłady (case study) ujawniania i zabezpieczania materiałów dowodowych z z rejestratorów CCTV	2	1
C6	Przygotowanie sprzętu, oprogramowania i nośników wykorzystywanych do ćwiczeń.	2	1
C7	Przygotowanie i wykorzystanie maszyn wirtualnych z zainstalowanymi systemami operacyjnymi.	2	2
C8	Opisywanie, dokumentowanie czynności - praktyczne przykłady (case study).	2	2

C9	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).	2	2
	Razem liczba godzin ćwiczeń	15	12

7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M2 – metoda** problemowa: wykład problemowy **M4 – metoda programowa**: wykład z wykorzystaniem materiałów multimedialnych.	projektor multimedialny, oprogramowanie specjalistyczne
Ćwiczenia	**M5 – metoda praktyczna**: ćwiczenia praktyczne	projektor multimedialny, oprogramowanie specjalistyczne

8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta

8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	Ocena formująca (F)	Ocena podsumowująca (P) –
Wykład	----------	F1 – sprawdzian (pisemny i
Ćwiczenia	**F2 – obserwacja/aktywność** podczas realizacji ćwiczeń wykonywanych podczas zajęć **F5 – ćwiczenia praktyczne:** ocena ćwiczeń wykonywanych podczas zajęć.	**Ocena podsumowująca** jest sumą ocen formułujących.

8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Symbol efektu	Wykład	Ćwiczenia	
	F1	F2	F5
W_01	x	x	
U_01	x	x	x
K_01	x		x

9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Ocena formułująca - ćwiczenia:
Student realizuje prace/ćwiczenia/projekty za które prowadzący przyznaje punkty (prace/ćwiczenia/projekty terminowe lub na zajęciach). W toku zajęć student może uzyskać max 100 pkt.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

Ocena podsumowująca oceny jest sumą ocen formułujących.

Student, który nie uzyskał wymaganej minimalnej liczby punktów potrzebnej do zaliczenia ćwiczeń może w czasie sesji przystąpić do kolokwium poprawkowego. Kolokwium poprawkowe obejmuje materiał z całego semestru.

Ocena podsumowująca – wykład
Ocena ze sprawdzianu ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Zaliczenie z oceną

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**45**	**27**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do sprawdzianu	8	14
przygotowanie do zajęć	8	14
przygotowanie do wykonywania ćwiczeń, wykonanie ćwiczeń	9	15
zapoznanie z literaturą	5	5
suma godzin:	**75**	**75**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**3**	**3**

12. Literatura zajęć

Literatura obowiązkowa:
1. Cory Altheide, Harlan Carvey, *Informatyka śledcza. Przewodnik po narzędziach open source*, Gliwice 2014.
2. Darren R. Hayes, *Informatyka w kryminalistyce. Praktyczny przewodnik,* Gliwice 2021.
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.
4. Rozporządzenie Ministra Sprawiedliwości z dnia 11 stycznia 2017 r. w sprawie utrwalania obrazu lub dźwięku dla celów procesowych w postępowaniu karnym.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Joanna Lubimow
data sporządzenia / aktualizacji	10 czerwca 2022 r.

dane kontaktowe (e-mail)	jlubimow@ajp.edu.pl
podpis	

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Drugiego stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		ZC.6

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Live Forensics, metody TRIAGE**
Punkty ECTS	**3**
Rodzaj zajęć	**Obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępstw**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	Liczba godzin Stacjonarne/niestacjonarne	Rok studiów/semestr	**Punkty ECTS** (zgodnie z programem studiów)
ćwiczenia	**45/27**	**II/IV**	**3**

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych

4. Cele kształcenia

C1 – Rozszerzenie dotychczasowej wiedzy na temat sposobów, metod i technik pracy dotyczącej zwalczania cyberprzestępczości.
C2 – Nabycie umiejętności ujawniania i zabezpieczania śladów i dowodów cyberprzestępczości wraz z ich wstępną weryfikacją.
C3 – Nabycie umiejętności postępowania zgodnie ze standardami i regulacjami prawnymi dotyczącymi zwalczania cyberprzestępczości.

5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	Opis efektu uczenia się	Odniesienie do efektu kierunkowego
	WIEDZA	
W_01	Słuchacz zna i rozumie metodologię Live Forensic/Triage w problematyce zwalczania cyberprzestępczości.	K_W12
	UMIEJĘTNOŚCI	

U_01	Słuchacz potrafi wykorzystać i zastosować metodologię Live Forensic/Triage w zwalczaniu cyberprzestępczości.	K_U10
KOMPETENCJE SPOŁECZNE		
K_01	Słuchacz potrafi w praktyce stosować właściwe standardy prawne i etyczne, a także wykazywać się odpowiednią postawą z realizacji zadań dotyczących zwalczania cyberprzestępczości**.**	K_K09

6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć (zgodnie z programem studiów):

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Specyfika, potrzeba oraz znaczenie metodologii Live Forensic/Triage w problematyce zabezpieczania dowodów elektronicznych. Zasady, charakterystyka, stosowane narzędzia i oprogramowanie.	7	4
W2	Wstępna weryfikacja danych pozyskiwanych w ramach Live Forensics, metod Triage'owych.	6	4
W3	Rozpoznawanie oprogramowania antiforensics i szyfrującego dane.	6	4
W4	Przygotowanie sprzętu, oprogramowanie i nośników wykorzystywanych do ćwiczeń.	5	4
W5	Wykorzystanie maszyn wirtualnych z zainstalowanymi systemami operacyjnymi.	6	4
W6	Przeprowadzanie sprawdzenia uruchomionego systemu - Live Forensics,	5	3
W7	Korzystanie z oprogramowania Triage	5	2
W8	Ujawnianie oprogramowania antiforensics oraz szyfrującego dane.	5	2
	Razem liczba godzin wykładów	45	27

7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	----------	----------
Ćwiczenia	**M5 – metoda praktyczna**: ćwiczenia z wykorzystaniem dostępnych wyszukiwarek internetowych, storn agregujących informacje o użytkownikach Internetu z otwartych źródeł.	projektor multimedialny, oprogramowanie specjalistyczne

8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta

8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F)**	**Ocena podsumowująca (P) –**
Wykład	----------	----------
Ćwiczenia	**F2 – obserwacja/aktywność** podczas realizacji ćwiczeń wykonywanych podczas zajęć **F5 – ćwiczenia praktyczne:** ocena ćwiczeń wykonywanych podczas zajęć.	**Ocena podsumowująca** jest sumą ocen formułujących.

8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Symbol efektu	Ćwiczenia	
	F2	F5
W_01	x	x
U_01	x	x
K_01	x	x

9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Ocena formułująca - ćwiczenia:
Student realizuje prace/ćwiczenia/projekty za które prowadzący przyznaje punkty (prace/ćwiczenia/projekty terminowe lub na zajęciach). W toku zajęć student może uzyskać max 100 pkt.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

Ocena podsumowująca oceny jest sumą ocen formułujących.

Student, który nie uzyskał wymaganej minimalnej liczby punktów potrzebnej do zaliczenia ćwiczeń może w czasie sesji przystąpić do kolokwium poprawkowego. Kolokwium poprawkowe obejmuje materiał z całego semestru.

Ocena podsumowująca – wykład
Ocena ze sprawdzianu ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Zaliczenie z oceną

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**45**	**27**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do sprawdzianu	8	14

przygotowanie do zajęć	8	14
przygotowanie do wykonywania ćwiczeń, wykonanie ćwiczeń	9	15
zapoznanie z literaturą	5	5
suma godzin:	**75**	**75**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**3**	**3**

12. Literatura zajęć

Literatura obowiązkowa:

1. Chojnowski A., *Informatyka sądowa w praktyce,* Gliwice 2019.
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.
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.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Joanna Lubimow
data sporządzenia / aktualizacji	10 czerwca 2022 r.
dane kontaktowe (e-mail)	jlubimow@ajp.edu.pl
podpis	

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Drugiego stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		ZC.7

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Wprowadzenie do analizy malware**
Punkty ECTS	**3**
Rodzaj zajęć	**Obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępstw**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	**Liczba godzin Stacjonarne/niestacjonarne**	**Rok studiów/semestr**	**Punkty ECTS** (zgodnie z programem studiów)
ćwiczenia	**45/27**	**II/IV**	**3**

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych

4. Cele kształcenia

C1 – Nabycie wiedzy na temat sposobów, metod i technik pracy dotyczącej zwalczania cyberprzestępczości.
C2 – Nabycie umiejętności wykorzystać dostępne narzędzia informatyczne w zwalczaniu cyberprzestępczości.
C3 – Nabycie umiejętności postępowania zgodnie ze standardami i regulacjami prawnymi w zwalczania cyberprzestępczości.

5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	**Opis efektu uczenia się**	**Odniesienie do efektu kierunkowego**
	WIEDZA	
W_01	Słuchacz zna i rozumie problematykę informatycznej analizy złośliwego oprogramowania w problematyce zwalczania cyberprzestępczości.	K_W07
	UMIEJĘTNOŚCI	
U_01	Słuchacz potrafi wykorzystać narzędzia informatyczne do specyfiki analizy złośliwego oprogramowania w problematyce zwalczania cyberprzestępczości.	K_U03

KOMPETENCJE SPOŁECZNE		
K_01	Słuchacz potrafi w praktyce stosować właściwe standardy prawne i etyczne, a także wykazywać się odpowiednią postawą z realizacji zadań dotyczących zwalczania cyberprzestępczości.	K_K13

6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć (zgodnie z programem studiów):

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Specyfika, potrzeba oraz znaczenie analizy złośliwego oprogramowania w analizie przestępczości komputerowej.	3	2
W2	Rodzaje złośliwego oprogramowania. Ogólne zasady analizy malware. Funkcjonalności malware.	3	2
W3	Zasady, charakterystyka, stosowane narzędzia i oprogramowanie do analizy złośliwego oprogramowania.	3	1
W4	Ukryte uruchamianie malware – wstęp do analizy pamięci RAM.	3	1
W5	Szyfrowanie danych na przykładzie ransomware.	2	1
W6	Automatyzacja procesów analizy złośliwego oprogramowania.	3	2
W7	Analiza statyczna i analiza dynamiczna złośliwego oprogramowania - podstawowe narzędzia.	3	2
W8	Raporty z analizy złośliwego oprogramowania.	3	2
W9	Przygotowanie sprzętu, oprogramowanie i nośników wykorzystywanych do ćwiczeń.	3	2
W10	Wykorzystanie maszyn wirtualnych z zainstalowanymi systemami operacyjnymi.	3	2
W11	Przygotowanie środowiska do analizy automatycznej złośliwego oprogramowania. - praktyczne przykłady (case study).	3	2
W12	Podstawowe narzędzia w analizie statycznej i dynamicznej złośliwego oprogramowania - praktyczne przykłady (case study).	3	2
W13	Podstawowe narzędzia w analizie statycznej i dynamicznej złośliwego oprogramowania - praktyczne przykłady (case study).	3	2
W14	Analiza malware na maszynach wirtualnych. Wykorzystanie narzędzi VmWare Workstation Pro lub VirtualBox firmy Oracle - praktyczne przykłady (case study).	3	2
W15	Analiza wyników - praktyczne przykłady (case study).	2	1
W16	Tworzenie raportów - praktyczne przykłady (case study).	2	1
	Razem liczba godzin wykładów	45	27

7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	----------	----------
Ćwiczenia	**M5 – metoda praktyczna**: ćwiczenia z wykorzystaniem dostępnych wyszukiwarek internetowych,, storn agregujących informacje o użytkownikach Internetu z otwartych źródeł.	projektor multimedialny, oprogramowanie specjalistyczne

8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta

8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	Ocena formująca (F)	Ocena podsumowująca (P) –
Wykład	----------	----------
Ćwiczenia	**F2 – obserwacja/aktywność** podczas realizacji ćwiczeń wykonywanych podczas zajęć **F5 – ćwiczenia praktyczne:** ocena ćwiczeń wykonywanych podczas zajęć.	**Ocena podsumowująca** jest sumą ocen formułujących.

8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Symbol efektu	Ćwiczenia	
	F2	F5
W_01	x	x
U_01	x	x
K_01	x	x

9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Ocena formułująca - ćwiczenia:
Student realizuje prace/ćwiczenia/projekty za które prowadzący przyznaje punkty (prace/ćwiczenia/projekty terminowe lub na zajęciach). W toku zajęć student może uzyskać max 100 pkt.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

Ocena podsumowująca oceny jest sumą ocen formułujących.

Student, który nie uzyskał wymaganej minimalnej liczby punktów potrzebnej do zaliczenia ćwiczeń może w czasie sesji przystąpić do kolokwium poprawkowego. Kolokwium poprawkowe obejmuje materiał z całego semestru.

Ocena podsumowująca – wykład
Ocena ze sprawdzianu ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Zaliczenie z oceną

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	**na studiach niestacjonarnych**
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**45**	**27**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do sprawdzianu	8	14
przygotowanie do zajęć	8	14
przygotowanie do wykonywania ćwiczeń, wykonanie ćwiczeń	9	15
zapoznanie z literaturą	5	5
suma godzin:	**75**	**75**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**3**	**3**

12. Literatura zajęć

Literatura obowiązkowa:

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

Literatura zalecana / fakultatywna

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

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Joanna Lubimow
data sporządzenia / aktualizacji	10 czerwca 2022 r.
dane kontaktowe (e-mail)	jlubimow@ajp.edu.pl
podpis	

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Drugiego stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		ZC.8

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Wymiar sprawiedliwości i pomoc prawna w dochodzeniach karnych w cyberprzestrzeni**
Punkty ECTS	**3**
Rodzaj zajęć	**Obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępstw**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	**Liczba godzin Stacjonarne/niestacjonarne**	**Rok studiów/semestr**	**Punkty ECTS** (zgodnie z programem studiów)
ćwiczenia	**45/27**	**II/IV**	**3**

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych

4. Cele kształcenia

C1 – Nabycie wiedzy na temat krajowych i międzynarodowych uregulowań prawnych zwalczania cyberprzestępczości.
C2 – Nabycie umiejętności analizowania i wyjaśniania problemów współpracy w zwalczaniu cyberprzestępczości.
C3 – Nabycie umiejętności radzenia sobie z problemami prawnymi wynikającymi ze specyfiki zwalczania przestępczości w cyberprzestrzeni.

5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	**Opis efektu uczenia się**	**Odniesienie do efektu kierunkowego**
WIEDZA		
W_01	Słuchacz zna i rozumie problemy współpracy z wymiarem sprawiedliwości i pomocą prawną w dochodzeniach karnych w cyberprzestrzeni.	K_W08
UMIEJĘTNOŚCI		

U_01	Słuchacz potrafi stosować narzędzia prawne współpracy z wymiarem sprawiedliwości w dochodzeniach karnych w cyberprzestrzeni.	K_U06
KOMPETENCJE SPOŁECZNE		
K_01	Słuchacz potrafi w praktyce stosować właściwe standardy prawne i etyczne współpracy z wymiarem sprawiedliwości i pomocą prawną w dochodzeniach karnych w cyberprzestrzeni.	K_K13

6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć (zgodnie z programem studiów):

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Narzędzia prawne oraz prawna organizacja wyspecjalizowanych agencji i organów UE w obszarze przeciwdziałania cyberprzestępczości.	7	4
W2	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	7	4
W3	Problematyka jurysdykcji w cyberprzestrzeni.	6	3
W4	Usprawnienie wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni	7	4
W5	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).	6	4
W6	Jurysdykcja w cyberprzestrzeni – analiza wybranych przykładów (case study).	6	4
W7	Współpraca pomiędzy organami policyjnymi, sądowniczymi i ekspertami ds. cyberprzestępczości - praktyczne przykłady (case study).	6	4
	Razem liczba godzin wykładów	45	27

7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	----------	----------
Ćwiczenia	**M5 – metoda praktyczna**: ćwiczenia z wykorzystaniem dostępnych wyszukiwarek internetowych, storn agregujących informacje o użytkownikach Internetu z otwartych źródeł.	projektor multimedialny, oprogramowanie specjalistyczne

8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta

8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	**Ocena formująca (F)**	**Ocena podsumowująca (P) –**
Wykład	----------	----------
Ćwiczenia	**F2 – obserwacja/aktywność** podczas realizacji ćwiczeń wykonywanych podczas zajęć **F5 – ćwiczenia praktyczne:** ocena	**Ocena podsumowująca** jest sumą ocen formułujących.

	ćwiczeń wykonywanych podczas zajęć.	

8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Symbol efektu	Ćwiczenia	
	F2	F5
W_01	x	x
U_01	x	x
K_01	x	x

9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Ocena formułująca - ćwiczenia:
Student realizuje prace/ćwiczenia/projekty za które prowadzący przyznaje punkty (prace/ćwiczenia/projekty terminowe lub na zajęciach). W toku zajęć student może uzyskać max 100 pkt.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

Ocena podsumowująca oceny jest sumą ocen formułujących.

Student, który nie uzyskał wymaganej minimalnej liczby punktów potrzebnej do zaliczenia ćwiczeń może w czasie sesji przystąpić do kolokwium poprawkowego. Kolokwium poprawkowe obejmuje materiał z całego semestru.

Ocena podsumowująca – wykład
Ocena ze sprawdzianu ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Zaliczenie z oceną

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**45**	**27**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		

przygotowanie do sprawdzianu	8	14
przygotowanie do zajęć	8	14
przygotowanie do wykonywania ćwiczeń, wykonanie ćwiczeń	9	15
zapoznanie z literaturą	5	5
suma godzin:	**75**	**75**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**3**	**3**

12. Literatura zajęć

Literatura obowiązkowa:

1. Białkowski M., *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Wydawnictwo, Warszawa 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. D. Bieńkowska, R. Kozłowski, 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. P. Chodak, K. Krassowski, 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,* Olsztyn 2017 r.
2. Olber P., *Prawno-kryminalistyczne aspekty zabezpieczania i pozyskiwania dowodów elektronicznych z chmur obliczeniowych,* Szczytno 2021.
3. Opitek P., *Skimming – aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Warszawa 2017 r.
4. Stefański R. A., *Metodyka pracy prokuratora w sprawach karnych,* Warszawa 2017.
5. Samborski E., *Zarys metodyki pracy sędziego w sprawach karnych*, Warszawa 2013.
6. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny.
7. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Joanna Lubimow
data sporządzenia / aktualizacji	10 czerwca 2022 r.
dane kontaktowe (e-mail)	jlubimow@ajp.edu.pl
podpis	

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Drugiego stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Biały wywiad i Cyber Threat Intelligence**
Punkty ECTS	**4**
Rodzaj zajęć	**Obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępstw**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	**Liczba godzin Stacjonarne/niestacjonarne**	**Rok studiów/semestr**	**Punkty ECTS** (zgodnie z programem studiów)
wykład	**30/18**	**II/IV**	**4**
ćwiczenia	**30/18**	**II/IV**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych

4. Cele kształcenia

C1 – Zdobycie wiedzy na temat sposobów, metod i technik pracy dotyczącej zwalczania cyberprzestępczości.
C2 – Nabycie umiejętności oceny zachowania sprawcy cyberprzestępstwa i możliwości jego identyfikacji.
C3 - Nabycie umiejętności przeprowadzania ukierunkowanego rozpoznania internetowego oraz dokumentowanie ww. czynności.
C4 – Słuchacz posiada zdolność krytycznej oceny sytuacji i efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań dotyczących zwalczania cyberprzestępczości.

5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	**Opis efektu uczenia się**	**Odniesienie do efektu kierunkowego**
	WIEDZA	
W_01	Słuchacz zna i rozumie specyfikę pracy związanej ze zwalczaniem cyberprzestępczości	K_W07
	UMIEJĘTNOŚCI	

U_01	Słuchacz potrafi dokonać oceny zachowania sprawcy znając możliwości jego identyfikacji również za pomocą różnych środków i narzędzi	K_U12
U_02	Słuchacz potrafi przeprowadzić ukierunkowane rozpoznanie internetowe oraz dokumentować te czynności.	
KOMPETENCJE SPOŁECZNE		
K_01	Słuchacz posiada zdolność do krytycznej oceny sytuacji oraz efektywnego radzenia sobie z problemami wynikającymi z realizacji zadań dotyczących zwalczania cyberprzestępczości**.**	K_K09

6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć (zgodnie z programem studiów):

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Specyfika, potrzeba oraz znaczenie i rola Cyber Threat Intelligence w zwalczaniu cyberprzestępczości. Wprowadzenie do CTI i cyklu intelligence.	3	2
W2	Zadania i wsparcie CTI. Modele analityczne. DFIR – baza dla CTI. Profilowanie grup APT. Śledzenie grup APT. Modele zagrożeń. Atrybucja.	3	2
W3	Techniki krytycznego myślenia.	3	1
W4	Analiza narzędzi, infrastruktury i danych z incydentów.	3	1
W5	Analiza powłamaniowa i interpretowanie wyników analizy powłamaniowej jako podstawowe atrybuty pracy analityka CTI.	3	2
W6	Specyfika, potrzeba oraz znaczenie i rola Białego wywiadu w zwalczaniu cyberprzestępczości.	3	2
W7	Metody wydobywania i analizy danych. Przykłady otwartych źródeł informacji.	3	2
W8	Analiza otwartych źródeł internetowych z zastosowaniem metodologii sieci społecznych.	3	2
W9	Wybór źródeł danych. Proces pobierania i wydobywania informacji	3	2
W10	Analiza sieci powiązań. Kryteria wyszukiwania. Analiza sentymentu. Śledzenie trendów.	3	2
	Razem liczba godzin wykładów	30	18

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Przygotowanie sprzętu, oprogramowania i nośników wykorzystywanych do ćwiczeń.	5	3
C2	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.	5	3
C3	Analiza otwartych źródeł internetowych z zastosowaniem metodologii sieci społecznych - praktyczne przykłady (case study).	5	3
C4	Przeprowadzenie ukierunkowanego rozpoznania internetowego - praktyczne przykłady (case study).	5	3
C5	Dokumentowanie czynności ukierunkowanego rozpoznania internetowego - praktyczne przykłady (case study). Tworzenie raportu OSINT - praktyczne przykłady (case study).	5	3
C6	Analiza powłamaniowa i interpretowanie wyników analizy powłamaniowej. Dokumentowanie czynności z analiz i śledzenia	5	3

	cyberzagrożeń (CTI) - praktyczne przykłady (case study).		
	Razem liczba godzin ćwiczeń	30	18

7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M2 – metoda** problemowa: wykład problemowy **M4 – metoda programowa**: wykład z wykorzystaniem materiałów multimedialnych.	projektor multimedialny, oprogramowanie specjalistyczne
Ćwiczenia	**M5 – metoda praktyczna**: ćwiczenia praktyczne	projektor multimedialny, oprogramowanie specjalistyczne

8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta

8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	Ocena formująca (F)	Ocena podsumowująca (P) –
Wykład	----------	F1 – sprawdzian (pisemny i
Ćwiczenia	**F2 – obserwacja/aktywność** podczas realizacji ćwiczeń wykonywanych podczas zajęć **F5 – ćwiczenia praktyczne:** ocena ćwiczeń wykonywanych podczas zajęć.	**Ocena podsumowująca** jest sumą ocen formułujących.

8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Symbol efektu	Wykład	Ćwiczenia	
	F1	F2	F5
W_01	x		x
U_01	x	x	x
K_01	x	x	

9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Ocena formułująca - ćwiczenia:
Student realizuje prace/ćwiczenia/projekty za które prowadzący przyznaje punkty (prace/ćwiczenia/projekty terminowe lub na zajęciach). W toku zajęć student może uzyskać max 100 pkt.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

Ocena podsumowująca oceny jest sumą ocen formułujących.

Student, który nie uzyskał wymaganej minimalnej liczby punktów potrzebnej do zaliczenia ćwiczeń może w czasie sesji przystąpić do kolokwium poprawkowego. Kolokwium poprawkowe obejmuje materiał z całego semestru.

Ocena podsumowująca – wykład

Ocena ze sprawdzianu ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg. R > 91% bardzo dobry (5,0) R > 81% ÷ 90% plus dobry (4,5) R > 71% ÷ 80% dobry (4,0) R > 61% ÷ 70% plus dostateczny (3,5) R > 50% ÷ 60% dostateczny (3,0) R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Egzamin

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

Forma aktywności studenta	**Liczba godzin**	
	na studiach stacjonarnych	**na studiach niestacjonarnych**
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**60**	**36**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do egzaminu	10	14
przygotowanie do zajęć	8	14
przygotowanie do zajęć	10	16
przygotowanie do wykonywania ćwiczeń	7	15
zapoznanie z literaturą	5	5
suma godzin:	**100**	**100**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**4**	**4**

12. Literatura zajęć

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*, Gliwice 2021.
3. Filipkowski W., Mądrzejowski W., *Biały wywiad. Otwarte źródła informacji - wokół teorii i praktyk*i, Warszawa 2011.

Literatura zalecana / fakultatywna

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

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Joanna Lubimow
data sporządzenia / aktualizacji	10 czerwca 2022 r.
dane kontaktowe (e-mail)	jlubimow@ajp.edu.pl
podpis	

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Drugiego stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		ZP.10

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Metodyka testów penetracyjnych z elementami socjotechniki**
Punkty ECTS	**4**
Rodzaj zajęć	**Obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępstw**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	Liczba godzin Stacjonarne/niestacjonarne	Rok studiów/semestr	**Punkty ECTS** (zgodnie z programem studiów)
wykład	**30/18**	**II/IV**	**4**
ćwiczenia	**30/18**	**II/IV**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych

4. Cele kształcenia

C1 – Zdobycie wiedzy na temat sposobów, metod i technik pracy dotyczącej zwalczania cyberprzestępczości.
C2 – Nabycie umiejętności wykorzystania dostępnych narzędzi informatycznych w zwalczaniu cyberprzestępczości.
C4 – Słuchacz posiada zdolność postępowania zgodnie ze standardami i regulacjami prawnymi w zwalczania cyberprzestępczości.

5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	Opis efektu uczenia się	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Słuchacz zna i rozumie metodykę testów penetracyjnych i specyfikę socjotechniki w problematyce zwalczania cyberprzestępczości.	K_W12
UMIEJĘTNOŚCI		

U_01	Słuchacz potrafi wykorzystać narzędzia informatyczne do testów penetracyjnych jak i znajomość specyfiki socjotechniki w problematyce zwalczania cyberprzestępczości.	K_U05
KOMPETENCJE SPOŁECZNE		
K_01	Słuchacz potrafi w praktyce stosować właściwe standardy prawne i etyczne, a także wykazywać się odpowiednią postawą z realizacji zadań dotyczących zwalczania cyberprzestępczości.	K_K13

6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć (zgodnie z programem studiów):

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Specyfika, potrzeba oraz znaczenie testów penetracyjnych w analizie cyberprzestępczości.	4	3
W2	Zasady, charakterystyka, stosowane narzędzia i oprogramowanie.	3	2
W3	Automatyzacja procesów testów penetracyjnych.	3	1
W4	Testy penetracyjne ze strony ofensywnej (Blue Flag).	3	1
W5	Rekonesans. Skanowanie - narzędzie ping i przeczesywanie sieci za jego pomoc; skanowanie portów; skanowanie systemu pod kątem jego podatności na atak.	4	3
W6	Wykorzystanie luk w zabezpieczeniach. Wykorzystywanie luk w zabezpieczeniach za pomocą przeglądarki internetowej.	3	2
W7	Utrzymanie dostępu poprzez backdoor i rootkity.	4	2
W8	Problematyka weryfikacji danych pozyskanych z testów penetracyjnych.	3	2
W9	Socjotechnika - metody zasady działania sprawcy i oddziaływania na ofiarę	3	2
	Razem liczba godzin wykładów	30	18

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	**Wprowadzenie do przedmiotu: cele, efekty, metody weryfikacji.** Specyfika, potrzeba oraz znaczenie testów penetracyjnych w analizie cyberprzestępczości.	3	1
C2	Zasady, charakterystyka, stosowane narzędzia i oprogramowanie	3	1
C3	Automatyzacja procesów testów penetracyjnych.	3	2
C4	Testy penetracyjne ze strony ofensywnej (Blue Flag).	3	2
C5	Rekonesans. Skanowanie - narzędzie ping i przeczesywanie sieci za jego pomoc; skanowanie portów; skanowanie systemu pod kątem jego podatności na atak.	3	2
C6	Rekonesans. Skanowanie - narzędzie ping i przeczesywanie sieci za jego pomoc; skanowanie portów; skanowanie systemu pod kątem jego podatności na atak.	3	2
C7	Wykorzystanie luk w zabezpieczeniach. Wykorzystywanie luk w zabezpieczeniach za pomocą przeglądarki internetowej.	3	2
C8	Utrzymanie dostępu poprzez backdoor i rootkity.	3	2
C9	Problematyka weryfikacji danych pozyskanych z testów penetracyjnych.	3	2
C10	Socjotechnika - metody zasady działania sprawcy i oddziaływania na ofiarę	3	2

	Razem liczba godzin ćwiczeń	30	18

7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M2 – metoda** problemowa: wykład problemowy **M4 – metoda programowa**: wykład z wykorzystaniem materiałów multimedialnych.	projektor multimedialny, oprogramowanie specjalistyczne
Ćwiczenia	**M5 – metoda praktyczna**: ćwiczenia praktyczne	projektor multimedialny, oprogramowanie specjalistyczne

8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta

8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć

Forma zajęć	Ocena formująca (F)	Ocena podsumowująca (P) –
Wykład	----------	F1 – sprawdzian (pisemny i
Ćwiczenia	**F2 – obserwacja/aktywność** podczas realizacji ćwiczeń wykonywanych podczas zajęć **F5 – ćwiczenia praktyczne:** ocena ćwiczeń wykonywanych podczas zajęć.	**Ocena podsumowująca** jest sumą ocen formułujących.

8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x")

Symbol efektu	Wykład	Ćwiczenia	
	F1	F2	F5
W_01	x		x
U_01	x	x	x
K_01	x	x	

9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Ocena formułująca - ćwiczenia:
Student realizuje prace/ćwiczenia/projekty za które prowadzący przyznaje punkty (prace/ćwiczenia/projekty terminowe lub na zajęciach). W toku zajęć student może uzyskać max 100 pkt.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

Ocena podsumowująca oceny jest sumą ocen formułujących.

Student, który nie uzyskał wymaganej minimalnej liczby punktów potrzebnej do zaliczenia ćwiczeń może w czasie sesji przystąpić do kolokwium poprawkowego. Kolokwium poprawkowe obejmuje materiał z całego semestru.

Ocena podsumowująca – wykład
Ocena ze sprawdzianu ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)

R > 81% ÷ 90% plus dobry (4,5) R > 71% ÷ 80% dobry (4,0) R > 61% ÷ 70% plus dostateczny (3,5) R > 50% ÷ 60% dostateczny (3,0) R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Egzamin

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

Forma aktywności studenta	**Liczba godzin**	
	na studiach stacjonarnych	**na studiach niestacjonarnych**
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**60**	**36**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do egzaminu	10	14
przygotowanie do zajęć	8	14
przygotowanie do zajęć	10	16
przygotowanie do wykonywania ćwiczeń	7	15
zapoznanie z literaturą	5	5
suma godzin:	**100**	**100**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**4**	**4**

12. Literatura zajęć

Literatura obowiązkowa: 1. Engebretson P., *Hacking i testy penetracyjne. Podstawy*, Gliwice2013. 2. Ziaja A., *Praktyczna analiza powłamaniowa. Aplikacja webowa w środowisku Linux*, Warszawa 2017.
Literatura zalecana / fakultatywna 1. Cory Altheide, Harlan Carvey, *Informatyka śledcza. Przewodnik po narzędziach open source*, Gliwice 2014. 2. Hayes D.R., *Informatyka w kryminalistyce. Praktyczny przewodnik*, Gliwice 2021.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Joanna Lubimow
data sporządzenia / aktualizacji	10 czerwca 2022 r.
dane kontaktowe (e-mail)	jlubimow@ajp.edu.pl
podpis	