Załącznik nr 3
do Programu studiów na kierunku kryminologia stosowana - studia pierwszego stopnia o profilu praktycznym,
stanowiącego załącznik do Uchwały Nr 42/2026 Senatu AJP
z dnia 23 czerwca 2026 r.

	Wydział	Prawa i Bezpieczeństwa
	Kierunek	Kryminologia Stosowana
	Poziom studiów	pierwszego stopnia
	Forma studiów	stacjonarna/niestacjonarna
	Profil studiów	praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.1.**

KARTA ZAJĘĆ

1. Informacje ogólne

Nazwa zajęć	**Przestępstwa komputerowe i przeciwko ochronie informacji**
Punkty ECTS	**1**
Rodzaj zajęć	**obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępczości**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Szybowska** **dr Paweł Opitek**

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	**15/10**	**II/4**	**1**

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Student przedmiotu przestępstwa komputerowe i przeciwko ochronie informacji posiada wiedzę, umiejętności oraz kompetencje społeczne, które nabył podczas realizacji przedmiotu Prawo karne materialne.

4. Cele kształcenia

C1 - Wyposażenie studenta w wiedzę z prawa karnego materialnego w zakresie przestępstw komputerowych i przeciwko ochronie informacji.

C2 - Zdobycie przez studenta umiejętności interpretowania i wyjaśniania zjawiska przestępczości komputerowej i przestępczości przeciwko ochronie informacji.

C3 - Zdobycie przez studenta umiejętności posługiwania się przepisami prawa krajowego i europejskiego do rozwiązania konkretnych problemów przestępstw komputerowych i przeciwko ochronie informacji.

C4 - Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności odnośne zjawiska przestępczości komputerowej i przestępczości przeciwko ochronie informacji.

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	Student ma zaawansowaną wiedzę o charakterze nauk prawnych, w szczególności prawa karnego materialnego w zakresie przestępstw komputerowych i przeciwko ochronie informacji.	K_W01 K_W13

UMIEJĘTNOŚCI		
U_01	Student potrafi prawidłowo interpretować i wyjaśniać zjawisko przestępczości komputerowej i przestępczości przeciwko ochronie informacji oraz dokonać krytycznej analizy własnych zachowań i zakresu posiadanej wiedzy, wykorzystując wiedzę i umiejętności nabyte w toku studiów.	K_U01 K_U12
U_02	Student posługuje się przepisami prawa krajowego i europejskiego do rozwiązania konkretnych problemów przestępstw komputerowych i przeciwko ochronie informacji, szanując normy etyczne i przestrzegając praw człowieka.	K_U03
KOMPETENCJE SPOŁECZNE		
K_01	Student uzupełnienia i doskonali nabytą wiedzę i umiejętności odnośne zjawiska przestępczości komputerowej i przestępczości przeciwko ochronie informacji.	K_K06

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

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	Zapoznanie studentów z planem i programem nauczania przedmiotu, celami i efektami uczenia się oraz formą zaliczenia.	0,5	0,5
C2	Wprowadzenie do problematyki przestępstw komputerowych: pojęcie przestępstwa komputerowego, klasyfikacja przestępstw komputerowych, zarys historii kryminalizacji zjawiska przestępczości komputerowej, podstawowe pojęcia (pojęcie informacji, informacje a dane, program komputerowy, poufność, integralność i dostępność danych komputerowych itp.). Katalog przestępstw komputerowych wg Interpolu i innych agencji i instytucji międzynarodowych. Katalog wg Konwencji o cyberprzestępczości.	1,5	1
C3	Charakterystyka podmiotowa i przedmiotowa przestępstw przeciwko ochronie informacji za pomocą sieci i systemów teleinformatycznych *(ujawnienie tajemnicy państwowej, ujawnienie tajemnicy służbowej i zawodowej, naruszenie tajemnicy korespondencji, udaremnienie lub utrudnienie korzystania z informacji, niszczenie danych informatycznych, sabotaż komputerowy, wytwarzanie programu komputerowego do popełnienia przestępstwa).*	2	1,5
C4	Charakterystyka podmiotowa i przedmiotowa tzw. przestępstw komputerowych *(przestępstwa przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji w tym: nielegalny dostęp do systemu komputerowego, nielegalny podsłuch komputerowy, naruszenie integralności danych komputerowych i systemu komputerowego; botnet; fałszerstwo i oszustwo komputerowe; cyberstalking; kradzież tożsamości; zniesławienie i zniewaga za pomocą sieci, grooming oraz posiadania, produkowanie i dystrybucja pornografii dziecięcej itp.).*	4	2
C5	Prawna ochrona informacji i dóbr osobistych w prawie cywilnym.	1	1
C6	Wybrane problemy prawno-porównawcze przestępstw komputerowych w wybranych krajach europejskich (analiza np.: Albania, Czechy, Estonia,	3	2

	Finlandia, Francja, Litwa, Bułgaria, Hiszpania, Niemcy, Norwegia, Szwajcaria, Rosja, Ukraina).		
C7	Rozwiązywanie kazusów (prawo karne materialne, orzecznictwo krajowe i europejskie) w zakresie przestępstw przeciwko ochronie informacji, przestępstw związanych z użyciem komputera, sieci i systemów teleinformatycznych.	3	2
	Razem liczba godzin ćwiczeń	**15**	**10**

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

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia przedmiotowe** (analiza problemowa i rozwiązywania kazusów).	Kazusy przygotowanie przez wykładowcę. Projektor multimedialny, komputer.

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)** – wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Ćwiczenia	**F1 – Sprawdzian** (pisemny w formie testowej zamkniętej). **F2 - obserwacja/aktywność** (ocena ćwiczeń wykonywanych podczas zajęć). **F5 – ćwiczenia praktyczne** (analiza i rozstrzygnięcie stanów faktycznych, rozwiązywanie kazusów).	Ocena podsumowująca stanowi wypadkową ocen formujących.

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

Symbol efektu	Ćwiczenia		
	F1	F2	F5
W_01	X	X	X
U_01	X	X	X
U_02	X	X	X
K_01		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 wypadkową 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.

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**
Zajęcia realizowane z udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia (zgodnie z planem studiów)	**15**	**10**
Praca własna studenta		
przygotowanie do kolokwium zaliczeniowych	3	5
przygotowanie do zajęć	4	5
zapoznanie z literaturą	3	5
suma godzin:	**25**	**25**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**1**	**1**

12. Literatura zajęć

Literatura obowiązkowa:

1. F. Radoniewicz, „Przestępstwa komputerowe w polskim Kodeksie karnym", Cybersecurity and Law, nr 1, 2019.
2. J. Kosiński, „Paradygmaty cyberprzestępczości", Difin Warszawa 2015.
3. P. Opitek, „Cyberprzestępczość w pracy prokuratora", Wydawnictwo Prokuratura i Prawo. Wydanie Specjalne, Prokuratura Krajowa 2018.
4. P. Opitek, „Kwalifikacja prawna i opis czynów zabronionych dotyczących przestępczości teleinformatycznej (zagadnienia wybrane)", Consilium Iuridicum, Kwartalnik naukowy Krajowej Rady Sądownictwa nr 1-2, 2022.

Literatura zalecana / fakultatywna:

1. A. Lebiedowicz, „Wybrane aspekty prawnokarne, kryminalistyczne i kryminologiczne
2. Cyberprzestępczości", Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury nr 1, 2022.
3. P. Opitek, „Przestępstwo skimmingu", Prokuratura i Prawo nr 11, 2015.
4. P. Opitek, „Kwalifikacja prawna i opis znamion przestępstw teleinformatycznych. Studium prawno-kryminalistyczne", Monografia, Wydawnictwo Krajowej Szkoły Sądownictwa i Prokuratury, grudzień 2023.
5. P. Opitek, A. Butor-Keler, K. Kanclerz, „Wybrane aspekty przestępczości z wykorzystaniem walut wirtualnych", czasopismo naukowe Agencji Bezpieczeństwa Wewnętrznego „Terroryzm – studia, analizy, prewencja" nr 4, 20

13. Informacje dodatkowe

imię i nazwisko sporządzającego	Paweł Opitek
data sporządzenia / aktualizacji	02.06.2025 r.
dane kontaktowe (e-mail)	popitek@ajp.edu.pl
podpis	P. Opitek
Czytelny podpis osoby upoważnionej do weryfikacji karty	

	Wydział	Prawa i Bezpieczeństwa
	Kierunek	Kryminologia Stosowana
	Poziom studiów	pierwszego stopnia
	Forma studiów	stacjonarna/niestacjonarna
	Profil studiów	praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.2.**

KARTA ZAJĘĆ

1. Informacje ogólne

Nazwa zajęć	**Techniki i analiza kanałów społecznościowych w profilaktyce cyberprzestępczości**
Punkty ECTS	**2**
Rodzaj zajęć	**obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępczości**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II , III**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Szybowska - koordynator specjalności Zwalczanie cyberprzestępczości** **dr Paweł Opitek – prowadzący 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	**15/10**	**II/4**	**2**
ćwiczenia	**15/10**	**III/5**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Student posiada wiedzę, umiejętności oraz kompetencje społeczne, które nabył podczas realizacji przedmiotu Prawo karne materialne.

4. Cele kształcenia

C1 - Wyposażenie studenta w wiedzę w zakresie technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości.

C2 - Zdobycie przez studenta umiejętności zastosowania technik analizy kanałów społecznościowych w profilaktyce cyberprzestępczości

C3 - Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności z technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości

5. Efekty uczenia siędla zajęć wraz z odniesieniem do efektów kierunkowych

Symbol efektu uczenia się	Opis efektu uczenia się	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Student ma zaawansowaną wiedzę w zakresie technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości.	K_W01 K_W13

UMIEJĘTNOŚCI		
U_01	Student potrafi prawidłowo zastosować techniki i analizy kanałów społecznościowych w profilaktyce cyberprzestępczości	K_U01, K_U04 K_U07
KOMPETENCJE SPOŁECZNE		
K_01	Student uzupełnienia i doskonali nabytą wiedzę i umiejętności odnośne technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości.	K_K06 K_K03

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

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Zapoznanie studentów z planem i programem nauczania przedmiotu, celami i efektami uczenia się oraz formą zaliczenia.	0,5	0,5
W2	Wolność słowa i etyka w cyfryzacji.	2	1,5
W3	Odpowiedzialność transgranicznych dostawców mediów społecznościowych (social media) w zakresie naruszeń wolności słowa według prawa krajowego i przed polskimi sądami	2	2
W4	Promocja odpowiedzialnego korzystania z internetu oraz monitoring problemów związanych z wykorzystywaniem mediów społecznościowych do działań przestępczych	1,5	2
W5	Promocja dobrych praktyk w sieci, w tym poszanowania własności intelektualnej. Ograniczenia analizy social media. Współpraca z dostawcami narzędzi.	5	2
W6	Wykorzystywanie serwisów społecznościowych przez organy ścigania jako cenne narzędzie do identyfikacji i lokalizacji osób, zbieraniu dowodów, odkrywaniu działalności przestępczej, zasięgnięciu wskazówek dot. przestępstwa.	4	2
	Razem liczba godzin wykładów	**15**	**10**

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	Zapoznanie studentów z programem kształcenia.	0,5	0,5
C2	Zawansowane techniki analityczne (np. wizualizacja, analiza mediów społecznościowych, metody statystyczne) w śledczej analizie danych	1,5	1,5
C3	Analiza różnych mediów społecznościowych pod względem rozprzestrzeniania fałszywych informacji (fake newsów), mowy nienawiści, samobójstwa itd.	4	3
C4	Analiza wybranych mediów społecznościowych: Twittea, Instagram, Facebook, LinkedIn, Pinterest w profilaktyce cyberprzestępczości.	5	3
C5	Techniki monitoringu dyskusji i opinii w portalach branżowych, blogach, forach dyskusyjnych i mediach społecznościowych.	4	2
	Razem liczba godzin ćwiczeń	**15**	**10**

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

Forma zajęć	**Metody dydaktyczne(wybór z listy)**	**Środki dydaktyczne**

Wykład	**M4 – Metoda programowa** (wykład z wykorzystaniem materiałów multimedialnych). **M2 – Metoda problemowa / metody aktywizujące** (dyskusja, pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia przedmiotowe** (analiza problemowa i rozwiązywania kazusów	Projektor multimedialny, komputer. Kazusy przygotowanie przez wykładowcę
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia laboratoryjne** (ćwiczenia doskonalące umiejętności pozyskiwania informacji ze źródeł internetowych; ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji).	Projektor multimedialny, komputer.

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)** – wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład	**F2 - obserwacja/aktywność** (ocena przygotowania do zajęć zajęć). **F5 – ćwiczenia praktyczne** (analiza i rozstrzygnięcie stanów faktycznych).	**P2 – Zaliczenie** (pisemne w formie testowej z elementami opisu)
Ćwiczenia	**F2 - obserwacja/aktywność** (ocena ćwiczeń wykonywanych podczas zajęć). **F3 – praca pisemna** (przygotowanie raportu na określony temat lub innej formy pisemnej o charakterze sprawozdawczym z elementami badań własnych). **F5 – ćwiczenia praktyczne** (przygotowanie projektu o konkretne założenia).	Ocena podsumowująca stanowi wypadkową ocen formujących

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

Symbol efektu	Wykład			Ćwiczenia		
	F2	F5	P2	F2	F3	F5
W_01	x	x	x		x	x
U_03				x	x	x
K_01	x	x	x	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 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
Zajęcia realizowane z udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia (zgodnie z planem studiów)	**30**	**20**
Praca własna studenta		
Przygotowanie projektu przeprowadzenia analizy kanałów społecznościowych w profilaktyce cyberprzestępczości.	10	11
przygotowanie do zajęć	4	8
przygotowanie do zaliczenia	3	7
zapoznanie z literaturą	3	4
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. *B. Saramak, „Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy", Uniwersytet Warszawski, Warszawa 2015 (https://wnpism.uw.edu.pl/wp-content/uploads/2019/08/Wykorzystanie-otwartych-zrodel.pdf).*
2. *D. Mider, „Wywiad jawnoźródłowy w internecie – kategoryzacja i ewaluacja narzędzi wyszukiwawczych", Przegląd Bezpieczeństwa Wewnętrznego nr 31, 2024 (file:///C:/Users/Opitek/Downloads/5_Mider_Przeglad-Bezpieczenstwa-Wewnetrznego_31-2024.pdf).*
3. *J. Dzikowski, „Wyszukiwanie danych osobowych w internecie dla celów informatyki śledczej, „Studia Oeconomica Posnaniensia" nr 1, 2013.*

Literatura zalecana / fakultatywna:

1. M. Witczak, „Biały wywiad w zarządzaniu bezpieczeństwem informacji", Przegląd Bezpieczeństwa Wewnętrzne nr 30, 2024 (https://www.abw.gov.pl/ftp/foto/Wydawnictwo/PBW/pbw30/16_-_ppk_-_M__Witczak.pdf).

2. P. Opitek, „Rosyjska koncepcja wojny informacyjnej na przykładzie amerykańskich wyborów prezydenckich", Wojskowy Przegląd Prawniczy, styczeń-luty 2019.
3. P. Waszkiewicz (red.), „Media społecznościowe w pracy organów ścigania", Warszawa 2021 (https://www.researchgate.net/profile/Pawel-Waszkiewicz/publication/350836786_Media_spolecznosciowe_w_pracy_organow_scigania/links/60755a1a29f56d520c61/Media-spolecznosciowe-w-pracy-organow-scigania.pdf).

13. Informacje dodatkowe

imię i nazwisko sporządzającego	Dr Sylwia Szybowska / dr Paweł Opitek
data sporządzenia / aktualizacji	02.06.2025 r.
dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl/popitek@ajp.edu.pl
podpis	Sylwia Szybowska/Paweł Opitek
Czytelny podpis osoby upoważnionej do weryfikacji karty	

	Wydział	Prawa i Bezpieczeństwa
	Kierunek	Kryminologia Stosowana
	Poziom studiów	pierwszego stopnia
	Forma studiów	stacjonarna/niestacjonarna
	Profil studiów	praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.3.**

KARTA ZAJĘĆ

1. Informacje ogólne

Nazwa zajęć	**Strategie cyberbezpieczeństwa RP i UE oraz wybranych państw świata**
Punkty ECTS	**2**
Rodzaj zajęć	**obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępczości**
Język, w którym prowadzone są zajęcia	**Polski**
Rok studiów	**III**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Szybowska**

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	**15/10**	**III /5**	**2**
ćwiczenia	**15/10**	**III/5**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Student posiada wiedzę, umiejętności oraz kompetencje społeczne, które nabył podczas realizacji przedmiotów kierunkowych.

4. Cele kształcenia

C1 - Przekazanie studentom wiedzy na temat różnych rodzajów struktur, organów i instytucji odpowiedzialnych za cyberbezpieczeństwo Polski, UE, wybranych krajów świata.

C2 - Wykształcenie umiejętności identyfikowania szans , zagrożeń oraz racjonalizacji podejmowanych koncepcji i strategii cyberbezpieczeństwa RP, UE i wybranych organizacji międzynarodowych dbających o bezpieczeństwo w cyberprzestrzeni.

C3 - Kształtowanie kompetencji zdobywania i doskonalenia zdobytej wiedzy odnośne podejmowanych przez państwa strategii i koncepcji bezpieczeństwa w cyberprzestrzeni.

C4 - Wykształcenie postawy poszanowania prawa i bezpieczeństwa w cyberprzestrzeni oraz kompetencji zwalczania jego naruszeń.

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	Student ma wiedzę na temat różnych rodzajów struktur, organów i instytucji odpowiedzialnych za cyberbezpieczeństwo w skali krajowej, europejskiej i międzynarodowej.	K_W06
UMIEJĘTNOŚCI		
U_01	Student potrafi wykorzystywać posiadany zasób wiedzy teoretycznej do analizowania, diagnozowania i formułowania opinii na temat koncepcji i strategii cyberbezpieczeństwa RP, UE i wybranych organizacji międzynarodowych dbających o bezpieczeństwo w cyberprzestrzeni.	K_U02
KOMPETENCJE SPOŁECZNE		
K_01	Student uzupełnienia i doskonali nabytą wiedzę i umiejętności odnośnie podejmowanych przez państwa strategii i koncepcji cyberbezpieczeństwa w ramach pracy własnej oraz innych zorganizowanych formach kształcenia.	K_K06
K_02	Student diagnozuje i rozpoznaje zasady poszanowania prawa i bezpieczeństwa w cyberprzestrzeni oraz projektuje działania mogące zapobiegać ich naruszeniom.	K_K08

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

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Zapoznanie studentów z planem i programem wykładów, celami i efektami uczenia się oraz metodami oceniania.	1	1
W2	Międzynarodowa problematyka cyberbezpieczeństwa i wzrastającej skali cyberataków. Klasyfikacja prawnych definicji w zakresie tematyki zajęć	2	2
W3	Polityka NATO i UE w zakresie cyberobrony i cyberbezpieczeństwa. Europejska Strategia cyberbezpieczeństwa. Akt o cyberbezpieczeństwie i certyfikacja. Zadania ENISA w zakresie cyberbezpieczeństwa PCUE.	6	3
W4	Strategia cyberbezpieczeństwa RP. Koncepcje cyberbezpieczeństwa MON, zadania CISIRT i innych instytucji państwowych odpowiedzialnych za cyberbezpieczeństwa RP. Problematyka podziału kompetencji w zapewnianiu cyberbezpieczeństwa	6	4
	Razem liczba godzin wykładów	**15**	**10**

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	Zapoznanie studentów z planem i programem ćwiczeń, celami i efektami uczenia się oraz formą zaliczenia. Strategie i koncepcje cyberbezpieczeństwa na przykładzie wybranych państw europejskich (Słowacja, Czechy, Wielka Brytania, Niemcy, Francja, Estonia, Gruzja)	8	5
C2	Strategie i koncepcje cyberbezpieczeństwa na przykładzie: USA, Rosji, Chin.	7	5
	Razem liczba godzin ćwiczeń	**15**	**10**

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

Forma zajęć	**Metody dydaktyczne(wybór z listy)**	**Środki dydaktyczne**
Wykład	**M1 – Metoda podająca** (wykład informacyjny).	Projektor multimedialny, komputer.

	M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).	
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi).	Projektor multimedialny, komputer.

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)** – wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć).	**P2 – Zaliczenie** (pisemny w formie testowej).
Ćwiczenia	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć). **F3 – Praca pisemna** (przygotowanie prezentacji). Oraz sposób prezentacji multimedialnej z komentarzem). **F5 – Ćwiczenia praktyczne** (analiza, dyskusja obserwacja pracy indywidualnej i grupowej oraz ocena wykonywanych zadań indywidualnych i grupowych realizowanych podczas zajęć)	Ocena podsumowująca stanowi wypadkową ocen formujących

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

Symbol efektu	Wykład		Ćwiczenia		
	F2.	P2	F2	F3	F5
W_01	x	x	x	x	x
U_01	x	x	x	x	x
K_01	x	x	x	x	x
K_02	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 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**
Zajęcia realizowane z udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia (zgodnie z planem studiów)	**30**	**20**
Praca własna studenta		
przygotowanie do zaliczenia	4	8
przygotowanie do zajęć	4	7
zapoznanie z literaturą	8	8
przygotowanie prezentacji	4	7
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. C. Banasiński, *Cyberbezpieczeństwo*. Zarys wykładu. Wolters Kluwer, 2018.
2. Encyklopedia Bezpieczeństwa Narodowego, (red.) J. Itrich-Drabarek, A.Misiuk, Sz.Mitkow, P. Bryczek-Wróbel, S. Gwoździewicz - autor i współautor haseł: Cyberatak, Cyberbezpieczeństwo, Cyberprzestrzeń, Cyberwojna, Cyberzagrożenie, Krajowy System Cyberbezpieczeństwa, Strategia Cyberbezpieczeństwa, ELIPSA 2023
3. *Źródła prawa np. :*

- Rozporządzenie 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (akt o cyberbezpieczeństwie).
- Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę;
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- Strategia cyberbezpieczeńswa RP – aktualna
- Polityka i koncepcje dotyczące cyberbezpieczeństwa (NATO, organizacji Unii Europejskiej i innych organizacji międzynarodowych).

Literatura zalecana / fakultatywna:

1. S. Szybowska, *Środki zarządzania ryzykiem w cyberbezpieczeństwie w polityce bezpieczeństwa ICT i wyzwaniach prawnych* - publikacja w ramach projektu badawczego *„The multi-dimensionality of cybersecurity and its relevance to the functioning of international institutions, national actors and socjety*". Referat wygłoszony na międzynarodowej konferencji naukowej pt. „The multidimensionality of cybersecurity" organizowanej dniach w 24-26 kwietnia 2024 r. przez Uczelnię Techniczno-Handlowa im. Heleny Chodkowskiej
2. S. Gwoździewicz, *Wymiar sprawiedliwości i pomoc prawna w dochodzeniach karnych w cyberprzestrzeni* [w:] Prawa człowieka i zrównoważony rozwój. Konwergencja czy dywergencja idei i polityki (red.) D. Bieńkowska,

R. Kozłowski, Wydawnictwo C.H.Beck, Warszawa 2020, Seria monografie prawnicze – (rozdział IV w części V s. 223-236), ISBN 978-83-8198-782-0, ISBN e-book 978-83-8198-783-7
3. S. Gwoździewicz, *Prawo i organizacja współdziałania instytucji i organów Unii Europejskiej na rzecz walki z cyberprzestępczością* [w:] Współdziałanie w administracji, (red.) Suwaj P., Kledzik P., Samulska K. Wyd. AJP, 2020, s. 175-188, ISBN 978-83-65466-93-8.
4. S. Gwoździewicz, *Problematyka cyberbezpieczeństwa i wzrastającej skali cyberataków, a dostęp do Internetu jako wartości dla realizacji praw człowieka* [w] D. Bieńkowska, R. Kozłowski (red.), Prawa człowieka i ludzkie bezpieczeństwo. Osiągnięcia i wyzwania. w 70. rocznicę ogłoszenia Powszechnej Deklaracji Praw Człowieka, Wyd. C.H.BECK, Warszawa 2019 (rozdział XIVs.157-168) ISBN 978-83-8158-613-9
5. S. Gwoździewicz, *Działania prawne Unii Europejskiej w zakresie cyberbezpieczeństwa* [w] Zagrożenia bezpieczeństwa w XXI wieku. Walka z przestępczością a profilaktyka społeczna. red. Z. Kuźniar, K. Tomaszycki, A. Łapińska, Wyd. Akademia Wojsk Lądowych imienia generała Tadeusza Kościuszki, Wrocław 2018, s. 25-44, ISBN 978-83-65422-82-8

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Sylwia Szybowska
data sporządzenia / aktualizacji	02.06.2025 r.
dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
podpis	Sylwia Szybowska
Czytelny podpis osoby upoważnionej do weryfikacji karty	

	Wydział	Prawa i Bezpieczeństwa
	Kierunek	Kryminologia Stosowana
	Poziom studiów	pierwszego stopnia
	Forma studiów	stacjonarna/niestacjonarna
	Profil studiów	praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.4.**

KARTA ZAJĘĆ

1. Informacje ogólne

Nazwa zajęć	**Ujawnianie i zwalczanie przestępstw przy użyciu sieci**
Punkty ECTS	**3**
Rodzaj zajęć	**obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępczości**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**III**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Szybowska** **dr inż. Łukasz Lemieszewski** **mgr inż. Mariusz Kowalski**

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	**15/10**	**III/5**	**3**
ćwiczenia	**15/8**	**III/5**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Student posiada wiedzę, umiejętności oraz kompetencje społeczne, które nabył podczas realizacji przedmiotów kierunkowych.

4. Cele kształcenia

C1 - Wyposażenie studenta w wiedzę w zakresie ujawniania i zwalczania przestępstw przy użyciu sieci.

C2 - Zdobycie przez studenta umiejętności ujawniania i zwalczania przestępstw przy użyciu sieci.

C3 - Zdobycie przez studenta umiejętności posługiwania się przepisami prawa w aspekcie ujawniania i zwalczania przestępstw przy użyciu sieci.

C4 - Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności odnośne ujawniania i zwalczania przestępstw przy użyciu sieci.

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	Student ma zaawansowaną wiedzę na temat ujawniania i zwalczania przestępstw przy użyciu sieci oraz wiedzę na temat instytucji organów	K_W02

	ochrony porządku prawnego z ich współpracy innymi podmiotami w tym zakresie.	K_W13 K_W06
UMIEJĘTNOŚCI		
U_01	Student potrafi prawidłowo interpretować i wyjaśniać zasady i metody ujawniania i zwalczania przestępstw przy użyciu sieci.	K_U01 K_U02
U_02	Student potrafi rozwiązywać konkretne problemy dotyczące ujawniania i zwalczania przestępstw przy użyciu sieci z poszanowaniem norm prawnych i etycznych.	K_U03 K_U04
KOMPETENCJE SPOŁECZNE		
K_01	Student uzupełnienia i doskonali nabytą wiedzę i umiejętności odnośne ujawniania i zwalczania przestępstw przy użyciu sieci.	K_K06
K_02	Student posiada umiejętność identyfikacji głównych problemów podejmowanej działalności, przewidywania jej skutków, uwzględnia towarzyszących im ryzyk, rozpoznawania zagrożeń i patologii oraz podjęcia właściwej reakcji w zakresie funkcjonowania ujawniania i zwalczania przestępstw przy użyciu sieci.	K_K05

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

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Zapoznanie studentów z efektami kształcenia, celem przedmiotu, warunkami i kryteriami zaliczenia. Wprowadzenie do problematyki ujawniania i zwalczania przestępstw przy użyciu sieci.	1	1
W2	Prawne i pozaprawne źródła wymagań dla systemów cyberbezpieczeństwa oraz praktyczne aspekty cyberbezpieczeństwa. Krajowy system cyberbezpieczeństwa. Dobre praktyki w zakresie bezpieczeństwa IT .	3	2
W3	Postępowanie w przypadku podejrzenia popełnienia cyberprzestępstwa. Służby w Polsce odpowiedzialne za ujawnianie i zwalczanie przestępstw przy użyciu sieci i ich statystyki.	2	1
W4	Współpraca z organami państwa i innymi podmiotami krajowymi i międzynarodowymi w zakresie wymiany informacji dotyczących nowych zjawisk przestępczych, związanych z rozwojem technik informatycznych dla potrzeb prowadzonej pracy operacyjnej.	3	2
W5	Podstawy pozyskiwania dowodów działalności użytkownika na komputerze. Siady pozostawione poza komputerem lokalnym. Na czym polega zbieranie podstawowych śladów działalności? Podstawowe zasady zbierania danych do analizy. Przygotowanie środowiska do analizy. Pułapki i błędy popełniane podczas niewłaściwego zbierania i analizy dowodów.	2	1
W6	Przegląd przykładowych ataków i popełnianych przestępstw. Rodzaje śladów pozostawianych w systemie. Najgroźniejsze ataki 2018-2021. Wybrane stany faktyczne. Czynności wykrywczo-dowodowe w zakresie oszustw z wykorzystaniem sieci.	4	2
	Razem liczba godzin wykładów	**15**	**10**

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**

		stacjonarnych	niestacjonarnych
C1	Zapoznanie studentów z efektami kształcenia, celem przedmiotu, warunkami i kryteriami zaliczenia. Narzędzia sieciowe w systemie Windows	3	2
C2	Ujawnianie i zabezpieczanie śladów. Obserwacja i analiza mechanizmu uzgadniania trójetapowego.	3	1
C3	Biały wywiad teoretycznie i praktycznie.	3	2
C4	Metodyka ujawniania i zwalczania przestępstw komputerowych: zabezpieczenie miejsca zdarzenia; oględziny - ujawnianie i zabezpieczanie śladów; przeszukanie i zabezpieczenie dowodów przestępstwa na podstawie analizy danych przeglądarki internetowej.	3	1
C5	Rodzaje danych zapisywanych w sieci, wykorzystanie geolokalizacji w procesie wykrywczym . Zabezpieczanie danych z sieci.	3	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	**M1 – Metoda podająca** (wykład informacyjny). **M4 – Metoda programowa** (wykład z wykorzystaniem materiałów multimedialnych).	Projektor multimedialny, komputer.
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia laboratoryjne** (ćwiczenia doskonalące umiejętności pozyskiwania informacji ze źródeł internetowych; ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji).	Projektor multimedialny, komputer, laboratorium systemów bezpieczeństwa WAiBN AJP.

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)** – wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład	**F2** – o**bserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć).	**P1** – **Egzamin** (pisemny w formie testowej z elementami opisu).
Ćwiczenia	**F2 - obserwacja/aktywność** (ocena ćwiczeń wykonywanych podczas zajęć). **F3** – przygotowanie referatu i prezentacji, sprawozdań z ćwiczeń **F5 – ćwiczenia praktyczne** (przeprowadzenie symulacji w laboratorium sieci komputerowych WT AJP.).	Ocena podsumowująca na podstawie sumy ocen formułujących

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

Symbol efektu	Wykład		Ćwiczenia		
	F2	P1	F2	F3	F5
W_01	X	X	x	X	X
U_01	X	X	X	X	X

U_02	X	X	X	X	X
K_01	X	X	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 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):		
Zajęcia realizowane z udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia (zgodnie z planem studiów)	**30**	**18**
Praca własna studenta		
Czytanie literatury	7	12
Przygotowanie prezentacji	8	12
Przygotowanie do zajęć	15	16
Przygotowanie do egzaminu	15	17

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. C. Banasiński, M. Rojszczak, *Cyberbezpieczeństwo* Wydawnictwo Wolters Kluwer Polska 2020 r.
2. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Wydawnictwo Wolters Kluwer Polska 2016 r.
3. M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Wydawnictwo: CEDEWU, 2016 r.

Literatura zalecana / fakultatywna:

1. A. Gryszczyńska, G. Szpor (red.) *Internet. Strategie bezpieczeństwa*. Wydawnictwo C.H. Beck, Warszawa 2017 r.
2. D. Littlejohn Shinder, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci.* Wydawnictwo Helion, Gliwice 20

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Sylwia Szybowska
data sporządzenia / aktualizacji	02.06.2025 r.
dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
podpis	Sylwia Szybowska
Czytelny podpis osoby upoważnionej do weryfikacji karty	

	Wydział	Prawa i Bezpieczeństwa
	Kierunek	Kryminologia Stosowana
	Poziom studiów	pierwszego stopnia
	Forma studiów	stacjonarna/niestacjonarna
	Profil studiów	praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.5.**

KARTA ZAJĘĆ

1. Informacje ogólne

Nazwa zajęć	**Postępowanie w zwalczaniu cyberprzestępstw**
Punkty ECTS	**3**
Rodzaj zajęć	**obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępczości**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**III**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Szybowska** **dr inż. Łukasz Lemieszewski** **mgr inż. Mariusz Kowalski**

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	**30/10**	**III/5**	**3**
ćwiczenia	**15/14**	**III/5**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Student posiada wiedzę, umiejętności oraz kompetencje społeczne, które nabył podczas realizacji przedmiotów kierunkowych.

4. Cele kształcenia

C1 - Wyposażenie studenta w wiedzę w zakresie postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.

C2 - Zdobycie przez studenta umiejętności postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.

C3 - Zdobycie przez studenta umiejętności posługiwania się przepisami prawa i odpowiednimi metodami kryminalistycznymi w aspekcie postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.

C4 - Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności odnośne postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw

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	Student ma zaawansowaną wiedzę na temat postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw oraz wiedzę na temat instytucji organów ochrony porządku prawnego z ich współpracy innymi podmiotami w tym zakresie.	K_W04 K_W06 K_W13
UMIEJĘTNOŚCI		
U_01	Student potrafi prawidłowo interpretować i wyjaśniać zasady i metody postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.	K_U01 K_U02
U_02	Student potrafi dokonać krytycznej analizy własnych zachowań i zakresu posiadanej wiedzy, wykorzystując wiedzę i umiejętności nabyte w toku studiów i podczas realizacji praktyki zawodowej w ramach rozwiązywania konkretnych problemy dotyczących postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw z poszanowaniem norm prawnych i etycznych.	K_U03 K_U04 K_U12
KOMPETENCJE SPOŁECZNE		
K_01	Student uzupełnienia i doskonali nabytą wiedzę i umiejętności odnośne postępowania w zwalczaniu cyberprzestępstw oraz student potrafi prawidłowo identyfikować ryzyka oraz szanse prowadzonej aktywności oraz podejmuje działania w oparciu o przeprowadzoną diagnozę.	K_K06 K_K08

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

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Zapoznanie studenta z planem i programem. Internet – charakterystyka i ewolucja. Powstanie społeczeństwa informacyjnego. Próby międzynarodowej regulacji internetu.	2	1
W2	Terminologia związana z cyberprzestępczością. Historia kontroli nadużyć w cyberprzestrzeni.	5	1
W3	Wybrane międzynarodowe inicjatywy z zakresu przeciwdziałania cyberprzestępczości: Unia Europejska, Organizacja Współpracy Gospodarczej i Rozwoju, Międzynarodowy Związek Telekomunikacyjny.	6	2
W4	Zjawisko cyberprzestępczości – charakter, rozmiary, tendencje. Odpowiedzialność za przestępstwa w cyberprzestrzeni.	5	1
W5	Cyberprzestępczość – wykrywalność, działalność Policji, prokuratury i sądów. Czynniki utrudniające ściganie.	4	1
W6	Procedury techniczne służące przeciwdziałaniu cyberprzestępczości. Współpraca z wyspecjalizowanymi organizacjami. Świadomość użytkowników.	4	2
W7	Konwencja Rady Europy z 23 listopada 2001 roku i polskie prawo karne. Przestępstwa przeciwko poufności, integralności oraz dostępności danych informatycznych i systemów komputerowych. Przestępstwa popełnione z wykorzystaniem komputera. Przestępstwa związane z naruszeniem praw autorskich i pokrewnych	4	2
	Razem liczba godzin wykładów	**30**	**10**

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**

C1	Zapoznanie studentów z programem kształcenia. Wyszukiwanie danych na cyfrowych nośnikach danych. Odzysk i niszczenie danych	4	4
C2	Analiza metadanych	2	2
C3	Ustalenia dotyczące adresów IP. Techniczne aspekty wymiany informacji z operatorami udostepniającymi Internet.	2	2
C4	Dowód elektroniczny – charakterystyka. Informatyka śledcza jako gałąź nauk sądowych. Badania ich podział i możliwości.	2	2
C5	Wykonywanie kopii binarnych (klonowanie, wykonywanie obrazów) dowodowych nośników danych cyfrowych z wykorzystaniem środowiska Windows i Linux	2	2
C6	Zabezpieczanie i transport sprzętu informatycznego i cyfrowych nośników danych. Opracowanie projektu prawidłowego zabezpieczenia sprzętu informatycznego na miejscu zdarzenia.	3	2
	Razem liczba godzin ćwiczeń	**15**	**14**

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

Forma zajęć	Metody dydaktyczne(wybór z listy)	Środki dydaktyczne
Wykład	**M1 – Metoda podająca** (wykład informacyjny). **M4 – Metoda programowa** (wykład z wykorzystaniem materiałów multimedialnych).	Projektor multimedialny, komputer.
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia laboratoryjne** (ćwiczenia doskonalące umiejętności pozyskiwania informacji ze źródeł internetowych; ćwiczenia doskonalące umiejętność selekcjonowania, grupowania i przedstawiania zgromadzonych informacji).	Projektor multimedialny, komputer, laboratorium systemów bezpieczeństwa WAiBN AJP.

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)** – wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład	**F2** – o**bserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć).	**P1** – **Egzamin** (ustny - wystąpienie z prezentacją, pytania do wystąpienia) **P4** – **praca pisemna** (referat, raport),.
Ćwiczenia	**F2 - obserwacja/aktywność** (ocena ćwiczeń wykonywanych podczas zajęć). **F3** – przygotowanie raportu / prezentacji / sprawozdań z ćwiczeń **F5 – ćwiczenia praktyczne** (przeprowadzenie symulacji w laboratorium sieci komputerowych WT AJP.).	Ocena podsumowująca na podstawie wypadkowej ocen formułujących

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

	Wykład	Ćwiczenia

Symbol efektu	F2	P1	P4	F2	F3	F5
W_01	x	x	x	x	x	x
U_01	x	x	x	x	x	x
U_02	x	x	x	x	x	
K_01	x	x	x	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 z egzaminu ustnego oraz pracy pisemnej stanowią 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
Zajęcia realizowane z udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia (zgodnie z planem studiów)	**45**	**24**
Praca własna studenta		
Czytanie literatury	9	15
Przygotowanie raportu	5	12
Przygotowanie do zajęć	6	12
Przygotowanie do egzaminu	10	12

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. D. R. Hayes - Informatyka w kryminalistyce. Praktyczny przewodnik. Wydanie II, Helion 2021 r.
2. M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Wydawnictwo: CEDEWU, 2016 r.

Literatura zalecana / fakultatywna:

1. R. A. Stefański, *Metodyka pracy prokuratora w sprawach karnych*, Wyd. Wolters Kluwer, Warszawa 2017 r.
2. E. Samborski, *Zarys metodyki pracy sędziego w sprawach karnych*, Wyd. LexisNexis Polska Sp. z o.o., Warszawa 2013 r.
3. A. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*,

13. Informacje dodatkowe

imię i nazwisko sporządzającego	Łukasz Lemieszewski
data sporządzenia / aktualizacji	02.06.2025 r.
dane kontaktowe (e-mail)	llemieszewski@ajp.edu.pl
podpis	Łukasz Lemieszewski
Czytelny podpis osoby upoważnionej do weryfikacji karty	

	Wydział	Prawa i Bezpieczeństwa
	Kierunek	Kryminologia Stosowana
	Poziom studiów	pierwszego stopnia
	Forma studiów	stacjonarna/niestacjonarna
	Profil studiów	praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.6.**

KARTA ZAJĘĆ

1. Informacje ogólne

Nazwa zajęć	**Informatyka śledcza i dowody w postaci elektronicznej w wykrywaniu cyberprzestępstw**
Punkty ECTS	**5**
Rodzaj zajęć	**obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępczości**
Język, w którym prowadzone są zajęcia	**Polski**
Rok studiów	**III**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Szybowska** **dr Paweł Opitek**

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**	**III / 5 i 6**	**5**
ćwiczenia	**30/18**	**III / 5 i 6**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Podstawowa wiedza z zakresu prawa karnego

4. Cele kształcenia

C1 - Wyposażenie studentów w interdyscyplinarną wiedzę niezbędną do właściwego podejmowania decyzji oraz efektywnego wykonywania aktywności zawodowej

C2 - Wykształcenie umiejętności identyfikowania szans lub zagrożeń oraz podejmowania adekwatnych działań w zakresie wykrywania cyberprzestępstw

C3 - Wykształcenie postawy poszanowania prawa i kompetencji zwalczania jego naruszeń, w szczególności cyberprzestępstw

C4 - Uwrażliwienie na potrzebę profesjonalnego zachowania się w ramach prowadzonej informatyki śledczej i przygotowanie do ponoszenia odpowiedzialności za podjęte działania w wykrywaniu cyberprzestępstw

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	Student zna w stopniu zaawansowanym zasady zdobywania i przeprowadzania dowodów w postacie elektronicznej w wykrywaniu cyberprzestępstw w postępowaniu karnym na etapie sądowym,	K_W03
W_02	Student ma wiedzę na temat różnych rodzajów struktur, organów i instytucji organów ochrony porządku prawnego oraz wymiaru sprawiedliwości, a także o relacjach zachodzących między tymi strukturami i instytucjami oraz między nimi a obywatelami w zakresie prowadzenia informatyki śledczej	K_W06
UMIEJĘTNOŚCI		
U_01	Student potrafi wykorzystywać posiadany zasób wiedzy teoretycznej do analizowania, diagnozowania i formułowania opinii na temat konkretnych stanów faktycznych związanych z przeprowadzaniem dowodów w postaci elektronicznej w wykrywaniu cyberprzestępstw	K_U02
U_02	Potrafi prawidłowo prognozować potrzebę uczenia się przez całe życie z uwzględnieniem perspektywy własnej kariery zawodowej	K_U10
KOMPETENCJE SPOŁECZNE		
K_01	Student potrafi współdziałać i pracować w grupie na różnych etapach realizowanych projektów, wykorzystując odpowiednie kanały i sposoby komunikacji.	K_K01
K_02	Student uzupełnia i doskonali wiedzę i umiejętności w różnych dziedzinach zarówno w ramach pracy własnej, jak i zorganizowanych form kształcenia	K_K06
K_03	Student potrafi prawidłowo identyfikować ryzyka oraz szanse prowadzonej aktywności oraz podejmuje działania w oparciu o przeprowadzoną diagnozę.	K_K08

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

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Zapoznanie studentów z planem i programem nauczania przedmiotu, celami i efektami uczenia się oraz formą zaliczenia Charakterystyka cyberprzestępczości	6	3
W2	Dowód cyfrowy, zabezpieczania i wykorzystanie	4	3
W3	Informatyk śledczy – rola w procesie wykrywczym	4	2
W4	Zabezpieczanie danych na miejscu zdarzenia	4	3
W5	Ślady przestępstw w sieci	4	3
W6	Analiza aktywności internetowej sprawcy	4	2
W7	Rodzaje analizy dowodów cyfrowych	4	2
	Razem liczba godzin wykładów	**30**	**18**

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	Zapoznanie studentów z programem kształcenia. Przestępstwa przeciwko danym informatycznym	4	2
C2	Przestępstwa komputerowe	6	3
C3	Przestępstwa ze względu na charakter zawartych informacji, prawa autorskie	4	3

C4	Zabezpieczanie dowodów cyfrowych	3	2
C5	Analiza danych na dowodach cyfrowych	3	2
C6	Analiza danych na dowodach cyfrowych	3	2
C7	Analiza aktywności internetowej użytkownika komputera	3	2
C8	Wykorzystanie sieci w procesie wykrywczym	4	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	**M1 Metoda podająca** (wykład informacyjny) **M2 Metoda problemowa** (wykład z elementami analizy problemowej i dyskusji).	Projektor multimedialny, system informacji prawnej.
Ćwiczenia	**M2 Metoda problemowa** (analiza przypadku, case study) **M5 Metoda praktyczna** (czytanie i analiza tekstu źródłowego, prezentacja różnych form wypowiedzi).	System informacji prawnej, dostęp do internetowego systemu aktów prawnych.

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)** – wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład	**F2 – obserwacja**/aktywność (obserwacja poziomu przygotowania do zajęć	**P1– Egzamin** (pisemny w formie opisowej)
Ćwiczenia	**F2 – Obserwacja/aktywność**: obserwacja poziomu przygotowania do zajęć. **F3 – Praca pisemna** (przygotowanie i wygłoszenie prezentacji). **F5 – Ćwiczenia praktyczne:** (analiza, dyskusja obserwacja pracy indywidualnej i grupowej oraz ocena wykonywanych zadań indywidualnych i grupowych podczas zajęć)	Ocena podsumowująca stanowi sumę ocen formujących.

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

Symbol efektu	Wykład		Ćwiczenia		
	P2	F2	F2	F3	F5
W_01	x	x	x		x
W_02		x	x	x	x
U_01	x	x	x		x
U_02		x	x	x	x
K_01		x	x		x
K_02	x	x	x	x	x
K_03		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 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
Zajęcia realizowane z udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia (zgodnie z planem studiów)	**60**	**36**
Praca własna studenta		
przygotowanie do egzaminu i do zajęć	15	21
Czytanie literatury	15	21
Przygotowanie referatu / prezentacji	17	23
Przygotowanie rozwiązania zadania	18	24
suma godzin:	**125**	**125**
liczba pkt ECTS przypisana do zajęć: (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta)	**5**	**5**

12. Literatura zajęć

Literatura obowiązkowa:
1. W. Kasprzak, „Ślady cyfrowe : studium prawno-kryminalistyczne”, Wydawnictwo Difin 2015.

2. P. Opitek, „Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych", Prokuratura i Prawo nr 7-8, 2018.
3. M. Niebrzydowska, R. Kotowicz, Wstęp do informatyki śledczej, Przegląd Bezpieczeństwa Wewnętrznego nr 4, 2012.
4. M. Szmit, O standardach informatyki śledczej, Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach nr 335, 2018.

Literatura zalecana / fakultatywna:

1. P. Opitek, A. Choroszewska, „Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany (cz. II)", Prokuratura i Prawo nr 10-11, 2020.
2. P. Opitek, A. Choroszewska, „Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany (cz. I)", Prokuratura i Prawo nr 9, 2020.
3. P. Opitek, D. Jaworski, „Cyberprzestępczość w prawie karnym i kryminalistyce", Wydawnictwo Difin 2025.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	Paweł Opitek
data sporządzenia / aktualizacji	02.06.2025 r.
dane kontaktowe (e-mail)	popitek@ajp.edu.pl
podpis	P. Opitek
Czytelny podpis osoby upoważnionej do weryfikacji karty	

	Wydział	Prawa i Bezpieczeństwa
	Kierunek	Kryminologia Stosowana
	Poziom studiów	pierwszego stopnia
	Forma studiów	stacjonarna/niestacjonarna
	Profil studiów	praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.7.**

KARTA ZAJĘĆ

1. Informacje ogólne

Nazwa zajęć	**Włamania do sieci i systemów informatycznych. Cyberataki.**
Punkty ECTS	**2**
Rodzaj zajęć	**obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępczości**
Język, w którym prowadzone są zajęcia	**Polski**
Rok studiów	**III**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Szybowska** **dr inż. Łukasz Lemieszewski** **mgr inż. Mariusz Kowalski**

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	**15/10**	**III/6**	**2**
ćwiczenia	**15/8**	**III/6**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Student przedmiotu powinien posiadać podstawową wiedzę z zakresu technologii informacyjnej, która nabył podczas kształcenia w szkole średniej oraz w trakcie studiów.

4. Cele kształcenia

C1 - Wyposażenie studentów w interdyscyplinarną wiedzę niezbędną do właściwego podejmowania decyzji oraz efektywnego wykonywania aktywności zawodowej

C2 - Wykształcenie umiejętności identyfikowania szans lub zagrożeń oraz podejmowania adekwatnych działań

C3 - Uwrażliwienie na potrzebę profesjonalnego zachowania się i przygotowanie do ponoszenia odpowiedzialności za podjęte działania

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	Ma wiedzę na temat współczesnych zjawisk związanych z zagrożeniem bezpieczeństwa cybernetycznego	K_W09
UMIEJĘTNOŚCI		

U_01	Posiada umiejętność analizowania i rozumienia złożonych relacji pomiędzy aspektami prawnymi i pozaprawnymi w zakresie funkcjonowania organizacji oraz dokonuje krytycznej analizy obserwowanych (badanych) zjawisk społecznych, stanów faktycznych i zdarzeń o znaczeniu prawnym, oceny ich uwarunkowań oraz konsekwencji dla organów ochrony porządku prawnego	K_U14 K_U07
KOMPETENCJE SPOŁECZNE		
K_01	Identyfikacji głównych problemów podejmowanej działalności, przewidywania jej skutków, uwzględnia towarzyszących im ryzyk, rozpoznawania zagrożeń i patologii oraz podjęcia właściwej reakcji	K_K05
K_02	Absolwent gotów jest do uzupełnienia i doskonalenia nabytej wiedzy i umiejętności w dziedzinie włamania do sieci i systemów informatycznych w ramach pracy własnej, jak i zorganizowanych form kształcenia	K_K06

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

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Zapoznanie studentów z planem i programem nauczania przedmiotu, celami i efektami uczenia się oraz formą zaliczenia Cyberbezpieczeństwo – definicje i architektura systemów WWW	2	1
W2	Podstawy Internetu - urządzenia sieciowe, sniffing spoofing hijacking	2	1
W3	Ataki DDoS, SQL-Injection, XSS - metody ochrony	4	2
W4	Kryptologia na usługach Cyberbezpieczeństwa	4	2
W5	Przyszłość Cyberbezpieczeństwa w obliczu QuantumComputing	3	2
	Razem liczba godzin wykładów	**15**	**10**

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	Zapoznanie studentów z programem kształcenia Wybrane przykłady aplikacji WWW i ich architektura	2	1
C2	Narzędzia zbierania informacji o sieci i użytkownikach	2	1
C3	Przykłady praktycznej realizacji ataków DDOS, SQL Injection, XSS i ochrona	4	2
C4	Instalacja i konfiguracja narzędzi typu Firewall oraz uwierzytelniania	4	2
C5	Kali Linux w analizie ruchu sieciowego i testowania podatności urządzeń sieciowych typu router Wi-fii	3	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	**M4-metoda programowa** (wykład z wykorzystaniem materiałów multimedialnych, wykład z bieżącym wykorzystaniem źródeł internetowych, wykład problemowy z wykorzystaniem materiałów multimedialnych.	Projektor multimedialny, Internet

Ćwiczenia	**M2 – Metoda problemowa** (analiza przypadku - case study)	Projektor multimedialny, laptop z dostępem do Internetu.

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)** – wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład	**……**	**P2 – zaliczenie** (pisemne w formie testowej z elementami opisu).
Ćwiczenia	**F2-obserwacja/aktywność** (ocena ćwiczeń wykonywanych podczas zajęć). **F3 – praca pisemna** (przygotowanie raportu na określony temat lub innej formy pisemnej o charakterze sprawozdawczym z elementami badan własnych).	**Ocena podsumowująca stanowi sumę ocen formujących.**

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

Symbol efektu	Wykład	Ćwiczenia	
	P2.	F2	F3
W_01	x		
U_01	x	x	x
K_01	x		x
K_02		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 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**
Zajęcia realizowane z udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia (zgodnie z planem studiów)	**30**	**18**
Praca własna studenta		
przygotowanie do zaliczenia	6	10
zapoznanie z literaturą	8	12
przygotowanie raportu	6	10
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. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii, Helion 2012.
2. J. Muniz, A. Lakhani, Kali Linux. Testy penetracyjne, Helion 2014.
3 J. Kluczewski, Bezpieczeństwo sieci komputerowych. Praktyczne przykłady i ćwiczenia w symulatorze. ITStart, 2019.

Literatura zalecana / fakultatywna:

1. Pieprzyk, T. Hardjono, J. Seberry, Teoria bezpieczeństwa systemów komputerowych, Helion, Gliwice 2005.
2. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2006.
3. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Helion 2011.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	Dr Sylwia Szybowska
data sporządzenia / aktualizacji	02.06.2025 r.
dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
podpis	Sylwia Szybowska
Czytelny podpis osoby upoważnionej do weryfikacji karty	

	Wydział	Prawa i Bezpieczeństwa
	Kierunek	Kryminologia Stosowana
	Poziom studiów	pierwszego stopnia
	Forma studiów	stacjonarna/niestacjonarna
	Profil studiów	praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.8.**

KARTA ZAJĘĆ

1. Informacje ogólne

Nazwa zajęć	**Bezpieczeństwo sieci i systemów informatycznych**
Punkty ECTS	**4**
Rodzaj zajęć	**obieralne**
Moduł/specjalizacja	**Zwalczanie cyberprzestępczości**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**III**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Szybowska** **dr Paweł Opitek**

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	**15/8**	**III /6**	**4**
ćwiczenia	**15/10**	**III /6**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Student przedmiotu powinien posiadać podstawową wiedzę z zakresu technologii informacyjnej, którą nabył podczas kształcenia w szkole średniej oraz w trakcie studiów.

4. Cele kształcenia

C1 - Wyposażenie studentów w interdyscyplinarną wiedzę niezbędną do właściwego podejmowania decyzji oraz efektywnego wykonywania aktywności zawodowej

C2 - Wykształcenie umiejętności identyfikowania szans lub zagrożeń oraz podejmowania adekwatnych działań

C3 - Uwrażliwienie na potrzebę profesjonalnego zachowania się i przygotowania do ponoszenia odpowiedzialności za podjęte działania

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	Student ma wiedzę na temat współczesnych zjawisk związanych z zagrożeniem bezpieczeństwa cybernetycznego	K_W09
UMIEJĘTNOŚCI		

U_01	Student potrafi wykorzystywać posiadany zasób wiedzy teoretycznej do analizowania, diagnozowania i formułowania opinii na temat konkretnych stanów faktycznych w zakresie bezpieczeństwa sieci i systemów informatycznych oraz potrafi dokonać krytycznej analizy własnych zachowań i zakresu posiadanej wiedzy, wykorzystując wiedzę i umiejętności nabyte w toku studiów i podczas realizacji praktyki zawodowej	K_U02 K_U12
U_02	Student posiada umiejętność analizowania i rozumienia złożonych relacji pomiędzy aspektami prawnymi i pozaprawnymi w zakresie funkcjonowania sieci i systemów informatycznych	K_U14
KOMPETENCJE SPOŁECZNE		
K_01	Student potrafi współdziałać i pracować w grupie na różnych etapach realizowanych projektów, wykorzystując odpowiednie kanały i sposoby komunikacji.	K_K01
K_02	Student potrafi prawidłowo identyfikować ryzyka oraz szanse prowadzonej aktywności oraz podejmuje działania w oparciu o przeprowadzoną diagnozę.	K_K08
K_03	Student potrafi identyfikować główne problemy podejmowanej działalności, przewidywania jej skutków, uwzględniania towarzyszących im ryzk, rozpoznawania zagrożeń i patologii oraz podjęcia właściwej reakcji	K_K05

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

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Zapoznanie studentów z planem i programem zajęć, celami i efektami uczenia się oraz formą zaliczenia. Podstawowe pojęcia związane z ochroną i bezpieczeństwem systemów informatycznych (m.in. co to jest system informatyczny/komputerowy, wiarygodność systemu, własności bezpieczeństwa, zasady bezpieczeństwa, zarządzanie bezpieczeństwem, rodzaje zabezpieczeń, i.in.	1	1
W2	Prawne i etyczne aspekty bezpieczeństwo sieci i systemów informatycznych	2	1
W3	Podstawowe zagrożenia bezpieczeństwa sieci i systemów informatycznych i ich rodzaje.	4	2
W4	Narzędzia, aplikacje procedury do zabezpieczania sieci. Systemy wykrywania włamań. Zapory ogniowe, Honeypot, systemy IDS.	4	4
W5	Sposoby zbierania informacji o ataku na system.	2	1
W6	Elementy kryptografii.	2	1
	Razem liczba godzin wykładów	15	8

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	Zapoznanie studentów z programem ćwiczeń Standardy i organizacje standaryzacyjne.	1	1
C2	Bezpieczeństwo poczty elektronicznej. Bezpieczeństwo urządzeń mobilnych..	2	1

C3	Bezpieczeństwo sieci bezprzewodowych. Bezpieczeństwo systemów operacyjnych.	2	2
C4	Firewall'e – charakterystyka, typy, implementacje.	2	1
C5	Szyfrowanie – poznanie wybranych programów szyfrujących.	2	1
C6	Projektowanie zabezpieczenia systemu komputerowego.	4	2
C7	Ochrona sieci teleinformatycznych przed zagrożeniami i terroryzmem elektromagnetycznym	2	2
	Razem liczba godzin ćwiczeń	**15**	**10**

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

Forma zajęć	Metody dydaktyczne(wybór z listy)	Środki dydaktyczne
Wykład	**M1 Metoda podająca** (wykład informacyjny) **M2 Metoda problemowa** (wykład z elementami analizy problemowej i dyskusji).	Projektor multimedialny, tablica
Ćwiczenia	**M2 Metoda problemowa** (analiza przypadku, case study) **M5 Metoda praktyczna** (czytanie i analiza tekstu źródłowego, prezentacja różnych form wypowiedzi)	Projektor multimedialny

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)** – wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład	**F2 – obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć).	**P1 – Egzamin** (pisemny w formie testowej z elementami opisu).
Ćwiczenia	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć). **F3 – Praca pisemna** (przygotowanie referatu lub prezentacji). **F5 – Ćwiczenia praktyczne:** (analiza, dyskusja obserwacja pracy indywidualnej i grupowej oraz ocena wykonywanych zadań indywidualnych i grupowych podczas zajęć)	**Ocena podsumowująca stanowi wypadkową ocen formujących.**

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

Symbol efektu	Wykład		Ćwiczenia		
	P1	F2	F2	F3	F5
W_01	x	x	x		x
U_01	x	x	x		x
U_02		x	x	x	x
K_01	x	x	x		x
K_02		x	x	x	x
K_03			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 wypadkową 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 egzaminu 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**
Zajęcia realizowane z udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia (zgodnie z planem studiów)	**30**	**18**
Praca własna studenta		
Czytanie literatury	15	15
Przygotowanie referatu	20	30
Przygotowanie rozwiązania zadania	15	17
Przygotowanie do egzaminu	20	20
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. Byrska D., Gawkowski K., Liszkowska D., *Unia Europejska. Geneza, funkcjonowanie, wyzwania*, Wrocław 2017.
2. Chaładyniak D., *Wybrane zagadnienia bezpieczeństwa danych w sieciach komputerowych*, „Zeszyty Naukowe WWSI" 2015, vol. 9, no 13.
3. Stallings W., *Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji*, Gliwice 2012.
4. Strużak R., *Problemy ochrony sieci teleinformatycznych przed zagrożeniami i terroryzmem elektromagnetycznym*, „Telekomunikacja i techniki informacyjne" 2010, nr 3-4.

Literatura zalecana / fakultatywna:

1. Ziaja A., *Praktyczna analiza powłamaniowa*, Warszawa 2017.
2. Michał Kamiński M., Strużewska-Smirnow J., Wieczerza M., *Charakterystyka modeli systemów bezpieczeństwa teleinformatycznego oraz ochrony sieci teleinformatycznych z punktu widzenia służb specjalnych*, [w:] Burczaaniuk P. (red.) *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, Warszawa 2017.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	Paweł Opitek
data sporządzenia / aktualizacji	02.06.2025 r.
dane kontaktowe (e-mail)	popitek@ajp.edu.pl
podpis	P. Opitek
Czytelny podpis osoby upoważnionej do weryfikacji karty	