Załącznik nr 4 do programu studiów,
Uchwała nr 34/000/2021 Senatu AJP
z dnia 22 czerwca 2021 r. Kryminologia stosowana

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Kryminologia stosowana
	Poziom studiów	Studia Pierwszego stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil kształcenia	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**Z.C.1.**

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Przestępstwa komputerowe i przeciwko ochronie informacji**
2. Punkty ECTS	**1**
3. Rodzaj przedmiotu	**Specjalnościowy**
4. Język przedmiotu	**polski**
5. Rok studiów	**II**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**dr Sylwia Gwoździewicz** **dr Paweł Tomaszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	**Studia stacjonarne**	**Studia niestacjonarne**
Semestr 4	**Ćw:** (15)	**Ćw:** (10)
Liczba godzin ogółem	**15**	**10**

C - Wymagania wstępne

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

D - Cele kształcenia

	Wiedza
CW1	**Wyposażenie studenta w wiedzę z prawa karnego materialnego w zakresie przestępstw komputerowych i przeciwko ochronie informacji.**
	Umiejętności
CU1	**Zdobycie przez studenta umiejętności interpretowania i wyjaśniania zjawiska przestępczości komputerowej i przestępczości przeciwko ochronie informacji.**
CU2	**Zdobycie przez studenta umiejętności posługiwania się przepisami prawa krajowego i europejskiego do rozwiązania konkretnych problemów przestępstw komputerowych i przeciwko ochronie informacji.**
	Kompetencje społeczne
CK1	**Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności odnośne zjawiska przestępczości komputerowej i przestępczości przeciwko ochronie informacji.**

E - Efekty uczenia się przedmiotowe i kierunkowe

Przedmiotowy efekt uczenia się (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt uczenia się
Wiedza (EPW…)		
EPW1	Student ma zaawansowaną wiedzę o charakterze nauk prawnych, w szczególności prawa karnego materialnego w zakresie przestępstw komputerowych i przeciwko ochronie informacji.	K_W01 K_W13
Umiejętności (EPU…)		
EPU1	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
EPU2	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 (EPK…)		
EPK1	Student uzupełnienia i doskonali nabytą wiedzę i umiejętności odnośne zjawiska przestępczości komputerowej i przestępczości przeciwko ochronie informacji.	K_K06

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	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, Finlandia, Francja, Litwa, Bułgaria, Hiszpania, Niemcy, Norwegia, Szwajcaria, Rosja, Ukraina).	3	2

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**

G – 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.

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

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Ćwiczenia	**F2 - obserwacja/aktywność** (ocena ćwiczeń wykonywanych podczas zajęć). **F5 – ćwiczenia praktyczne** (analiza i rozstrzygnięcie stanów faktycznych, rozwiązywanie kazusów).	**P2 - zaliczenie** (pisemne w formie testowej zamkniętej).

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

Efekty przedmiotowe	Ćwiczenia		
	F2	**F5**	**P2**
EPW1	x	x	x
EPU1	x	x	x
EPU2	x	x	x
EPK1	x		

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt uczenia się (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student zna wybrane terminy, uwarunkowania i regulacje prawne (w szczególności prawa karnego materialnego) w zakresie przestępstw komputerowych i przeciwko ochronie informacji	Student zna większość wymaganych terminów, uwarunkowań i regulacji prawnych (w szczególności prawa karnego materialnego) w zakresie przestępstw komputerowych i przeciwko ochronie informacji	Student zna wszystkie wymagane terminy, uwarunkowania i regulacje prawne (w szczególności prawa karnego materialnego) w zakresie przestępstw komputerowych i przeciwko ochronie informacji.

EPU1	Student wykonuje niektóre zadania dotyczące interpretowania i wyjaśniania zjawisk przestępczości komputerowej i przestępczości przeciwko ochronie informacji w oparciu o posiadane dane i wiedzę w tym zakresie.	Student wykonuje większość wymaganych zadań dotyczących interpretowania i wyjaśniania zjawisk przestępczości komputerowej i przestępczości przeciwko ochronie informacji w oparciu o posiadane dane i wiedzę w tym zakresie.	Student wykonuje wszystkie wymagane zadania dotyczące interpretowania i wyjaśniania zjawisk przestępczości komputerowej i przestępczości przeciwko ochronie informacji w oparciu o posiadane dane i wiedzę w tym zakresie.
EPU2	Student potrafi wykorzystać niektóre poznane rozwiązania i przepisy prawa krajowego i europejskiego do rozwiązania konkretnych problemów przestępstw komputerowych i przeciwko ochronie informacji, szanując normy etyczne i przestrzegając praw człowieka.	Student potrafi wykorzystać większość poznanych rozwiązań i przepisów prawa krajowego i europejskiego do rozwiązania konkretnych problemów przestępstw komputerowych i przeciwko ochronie informacji, szanując normy etyczne i przestrzegając praw człowieka.	Student potrafi wykorzystać wszystkie poznane rozwiązania i przepisy prawa krajowego i europejskiego do rozwiązania konkretnych problemów przestępstw komputerowych i przeciwko ochronie informacji, szanując normy etyczne i przestrzegając praw człowieka.
EPK1	Student rozumie znaczenie aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne zjawiska przestępczości komputerowej i przestępczości przeciwko ochronie informacji.	Student rozumie i widzi znaczenie swojej aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne zjawiska przestępczości komputerowej i przestępczości przeciwko ochronie informacji.	Student rozumie i widzi znaczenie swojej aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne zjawiska przestępczości komputerowej i przestępczości przeciwko ochronie informacji i podejmuje dalsze działania w tym zakresie.

J – Forma zaliczenia przedmiotu

Zaliczenie z oceną

K – Literatura przedmiotu

Literatura obowiązkowa:

1. M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej,* Wydawnictwo: CeDeWu Warszawa 2016 r.
2. J. Kosiński, *Paradygmaty cyberprzestępczości,* Difin Warszawa 2015.
3. M. Sawicki, *Cyberprzestępczość.* Seria monografie prawnicze. Wydawnictwo C.H.BECK, Warszawa 2013 r.
4. *Konwencja Rady Europy o cyberprzestępczości,* sporządzona w Budapeszcie dnia 23 listopada 2001 r.
5. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny.*

Literatura zalecana / fakultatywna:

1. S. Gwoździewicz i in., *Determinanty rozwoju cyberprzestępczych ataków na systemy informatyczne firm i klientów indywidualnych instytucji finansowych* [w] Prawne i społeczne aspekty cyberbezpieczeństwa (red.) S. Gwoździewicz i K. Tomaszyckiego, Wyd. Międzynarodowy Instytut Innowacji, Warszawa 201
2. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Wolters Kluwer 2016.
3. Fischer B., *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000.

Ł – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	15	10
Czytanie literatury	3	5
Przygotowanie do zajęć	4	5
Przygotowanie do zaliczenia	3	5
Suma godzin:	**25**	**25**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**1**	**1**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Paweł Tomaszewski
Data sporządzenia / aktualizacji	10.06.2022 r.
Dane kontaktowe (e-mail)	ptomaszewski@ajp.edu.pl
Podpis	Tomaszewski

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Kryminologia stosowana
	Poziom studiów	Studia pierwszego stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil kształcenia	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.C.2.**

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Techniki i analiza kanałów społecznościowych w profilaktyce cyberprzestępczości**
2. Punkty ECTS	**2**
3. Rodzaj przedmiotu	**Specjalnościowy**
4. Język przedmiotu	**polski**
5. Rok studiów	**II, III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**dr Sylwia Gwoździewicz** **dr Paweł Tomaszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 4	**W**: (15)	**W**: (10)
Semestr 5	**Ćw:** (15)	**Ćw:** (10)
Liczba godzin ogółem	**30**	**20**

C - Wymagania wstępne

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

D - Cele kształcenia

	Wiedza
CW1	**Wyposażenie studenta w wiedzę w zakresie technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości.**
	Umiejętności
CU1	**Zdobycie przez studenta umiejętności zastosowania technik analizy kanałów społecznościowych w profilaktyce cyberprzestępczości**
	Kompetencje społeczne
CK1	**Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności z technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości**

E - Efekty uczenia się przedmiotowe i kierunkowe

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

Wiedza (EPW…)		
EPW1	Student ma zaawansowaną wiedzę w zakresie technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości.	K_W01 K_W13
Umiejętności (EPU…)		
EPU1	Student potrafi prawidłowo zastosować techniki i analizy kanałów społecznościowych w profilaktyce cyberprzestępczości	K_U01 K_U04 K_U07
Kompetencje społeczne (EPK…)		
EPK1	Student uzupełnienia i doskonali nabytą wiedzę i umiejętności odnośne technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości.	K_K06 K_K03

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Zapoznanie studentów z planem i programem nauczania przedmiotu, celami i efektami uczenia się oraz formą zaliczenia.	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 (Ustawa o świadczeniu usług drogą elektroniczną).	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 wykładów	**15**	**10**

G – 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.

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

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład	**F2 - obserwacja/aktywność** (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 sumę ocen formujących**

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

Efekty przedmiotowe	Wykład			**Ćwiczenia**		
	F2	**F5**	**P2**	**F2**	**F3**	**F5**
EPW1	x	x	x		x	x
EPU1				x	x	x
EPK1	x	x	x	x	x	x

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt uczenia się (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student zna wybrane techniki analiz kanałów społecznościowych w profilaktyce cyberprzestępczości.	Student zna większość wymaganych technik, analiz kanałów społecznościowych w profilaktyce cyberprzestępczości.	Student zna wszystkie wymagane techniki i analizy kanałów społecznościowych w profilaktyce cyberprzestępczości.
EPU1	Student wykonuje niektóre zadania dotyczące technik i analiz kanałów społecznościowych	Student wykonuje większość wymaganych zadań dotyczących technik i analiz kanałów społecznościowych	Student wykonuje wszystkie wymagane zadania dotyczące technik i analiz kanałów społecznościowych

	w profilaktyce cyberprzestępczości. w oparciu o posiadane dane i wiedzę w tym zakresie.	w profilaktyce cyberprzestępczości w oparciu o posiadane dane i wiedzę w tym zakresie.	w profilaktyce cyberprzestępczości w oparciu o posiadane dane i wiedzę w tym zakresie.
EPK1	Student rozumie znaczenie aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości.	Student rozumie i widzi znaczenie swojej aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości.	Student rozumie i widzi znaczenie swojej aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne technik i analiz kanałów społecznościowych w profilaktyce cyberprzestępczości i podejmuje dalsze działania w tym zakresie.

J – Forma zaliczenia przedmiotu

Zaliczenie z oceną

K – Literatura przedmiotu

Literatura obowiązkowa:

1. *Media społecznościowe w pracy organów ścigania,* red. Waszkiewicz P., Warszawa 2021.
2. W.A. Kasprzak, *Ślady cyfrowe. Studium prawno-kryminalistyczne,* Difin, 2015 r.
3. R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku : zarys problematyki*; Wyższa Szkoła Cła i Logistyki, wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011.

Literatura zalecana / fakultatywna:

1. J. Lovett, *Sekrety pomiarów w mediach społecznościowych,* Helion 2013 r.
2. Dąbrowska I., *Media społecznościowe*, Lublin 2019.
3. M. Sadowski, *Rewolucja social media,* Wydawnictwo Onepress, 2012 r.
4. S. Gwoździewicz i D. Prokopowicz, *Prawno-społeczne determinanty bezpieczeństwa gromadzenia i transferu danych niejawnych w internetowych portalach społecznościowych* [w] Pravo Ekonomija Menadžment I Međunarodni naučni zbornik, Srbske Rozvojove Udruženie, Bački Petrovac, Srbija 2016 - str. 80
5. S.Gwoździewicz, *Prawny wymiar kryminogennych zachowań w cyberprzestrzeni. Zjawisko sekstingu w badaniach osób nieletnich* [w] (red.) M. Goc, T. Tomaszewski, R. Lewandowski „Kryminalistyka – jedność nauki i praktyki, przegląd zagadnień z zakresu zwalczania przestępczości", Wyd. Polskie Towarzystwo Kryminalistyczne, ISBN: 978-83-7867-334-7, Warszawa 2016 r .

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	30	20
Czytanie literatury	3	4
Przygotowanie do zajęć	3	7
Przygotowanie projektu przeprowadzenia analizy kanałów społecznościowych w profilaktyce cyberprzestępczości.	9	9
Przygotowanie do zaliczenia	5	10
Suma godzin:	**50**	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**	**2**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	10.06.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl

Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Kryminologia stosowana
	Poziom studiów	Studia pierwszego stopnia
	Forma studiów	Studia stacjonarne/niestacjonarne
	Profil kształcenia	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.C.3.**

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Strategie cyberbezpieczeństwa RP i UE oraz wybranych państw świata.**
2. Punkty ECTS	**2**
3. Rodzaj przedmiotu	**Specjalnościowy**
4. Język przedmiotu	**polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**dr Sylwia Gwoździewicz**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 5	**W**: (15); **Ć:** (15)	**W**: (10); **Ć:** (10)
Liczba godzin ogółem	**30**	**10**

C - Wymagania wstępne

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

D - Cele kształcenia

	Wiedza
CW1	Przekazanie studentom wiedzy na temat różnych rodzajów struktur, organów i instytucji odpowiedzialnych za cyberbezpieczeństwo Polski, UE, wybranych krajów świata.
	Umiejętności
CU1	Wykształcenie umiejętności identyfikowania szans , zagrożeń oraz racjonalizacji podejmowanych koncepcji i strategii cyberbezpieczeństwa RP, UE i wybranych organizacji międzynarodowych dbających o bezpieczeństwo w cyberprzestrzeni.
	Kompetencje społeczne
CK1	Kształtowanie kompetencji zdobywania i doskonalenia zdobytej wiedzy odnośne podejmowanych przez państwa strategii i koncepcji bezpieczeństwa w cyberprzestrzeni.
CK2	Wykształcenie postawy poszanowania prawa i bezpieczeństwa w cyberprzestrzeni oraz kompetencji zwalczania jego naruszeń.

E - Efekty uczenia się przedmiotowe i kierunkowe

Przedmiotowy efekt uczenia się (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt uczenia się
Wiedza (EPW…)		
EPW1	Student ma wiedzę na temat różnych rodzajów struktur, organów i instytucji odpowiedzialnych za cyberbezpieczeństwo w skali krajowej, europejskiej i międzynarodowej.	K_W06
Umiejętności (EPU…)		
EPU1	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 (EPK…)		
EPK1	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
EPK2	Student diagnozuje i rozpoznaje zasady poszanowania prawa i bezpieczeństwa w cyberprzestrzeni oraz podejmuje działania zapobiegające ich naruszeniom.	K_K08

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Zapoznanie studentów z planem i programem wykładów, celami i efektami uczenia się oraz metodami oceniania.	1	1
W2	Międzynarodowa problematyka cyberbezpieczeństwa i wzrastającej skali cyberataków.	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**

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

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M1 – Metoda podająca** (wykład informacyjny). **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 kreacyjne** (przygotowanie i analiza prezentacji przedstawianych przez studentów).	Projektor multimedialny, komputer.

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

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć).	**P2 – zaliczenie** (pisemny w formie testowej).
Ćwiczenia	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć). **F3 – Praca pisemna** (przygotowanie prezentacji). **F4 – Wypowiedź/wystąpienie** (sposób prezentacji multimedialnej z komentarzem).	Ocena podsumowująca stanowi sumę ocen formujących

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

Efekty przedmiotowe	Wykład		Ćwiczenia		
	F2	**P2**	**F2**	**F3**	**F4**
EPW1	x	x	x	x	x
EPU1	x	x	x	x	x
EPK1	x	x	x	x	x
EPK2			x		

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt uczenia się (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student zna wybrane rodzaje struktur, organów i instytucji odpowiedzialnych za cyberbezpieczeństwo w skali krajowej, europejskiej i międzynarodowej.	Student zna większość wymaganych struktur, organów i instytucji odpowiedzialnych za cyberbezpieczeństwo w skali krajowej, europejskiej i międzynarodowej.	Student zna wszystkie wymagane rodzaje struktur, organów i instytucji odpowiedzialnych za cyberbezpieczeństwo w skali krajowej, europejskiej i międzynarodowej.
EPU1	Student wykonuje niektóre zadania dotyczące analizowania, diagnozowania i formułowania opinii na temat koncepcji i strategii cyberbezpieczeństwa RP, UE i wybranych organizacji międzynarodowych dbających o bezpieczeństwo w cyberprzestrzeni w	Student wykonuje większość wymaganych zadań dotyczących analizowania, diagnozowania i formułowania opinii na temat koncepcji i strategii cyberbezpieczeństwa RP, UE i wybranych organizacji międzynarodowych dbających o bezpieczeństwo w cyberprzestrzeni w oparciu o posiadany zasób wiedzy teoretycznej.	Student wykonuje wszystkie wymagane zadania dotyczące analizowania, diagnozowania i formułowania opinii na temat koncepcji i strategii cyberbezpieczeństwa RP, UE i wybranych organizacji międzynarodowych dbających o bezpieczeństwo

	oparciu o posiadany zasób wiedzy teoretycznej.	.	w cyberprzestrzeni w oparciu o posiadany zasób wiedzy teoretycznej.
EPK1	Student rozumie znaczenie aktywności w zakresie uzupełniania i doskonalenia nabytej wiedzy i umiejętności odnośnie podejmowanych przez państwa strategii i koncepcji cyberbezpieczeństwa w ramach pracy własnej oraz innych zorganizowanych formach kształcenia.	Student rozumie i widzi znaczenie swojej aktywności w zakresie uzupełniania i doskonalenia nabytej wiedzy i umiejętności odnośnie podejmowanych przez państwa strategii i koncepcji cyberbezpieczeństwa w ramach pracy własnej oraz innych zorganizowanych formach kształcenia.	Student rozumie i widzi znaczenie swojej aktywności w zakresie uzupełniania i doskonalenia nabytej wiedzy i umiejętności odnośnie podejmowanych przez państwa strategii i koncepcji cyberbezpieczeństwa w ramach pracy własnej oraz innych zorganizowanych formach kształcenia.i podejmuje dalsze działania w tym zakresie.
EPK2	Student rozpoznaje zasady poszanowania prawa i bezpieczeństwa w cyberprzestrzeni oraz zna zasady działań zapobiegających ich naruszeniom.	Student rozpoznaje zasady poszanowania prawa i bezpieczeństwa w cyberprzestrzeni oraz zna zasady i widzi potrzebę podejmowania działań zapobiegających ich naruszeniom.	Student rozpoznaje zasady poszanowania prawa i bezpieczeństwa w cyberprzestrzeni oraz wg znanych mu zasad podejmuje próby działań zapobiegających ich naruszeniom.

J – Forma zaliczenia przedmiotu

Zaliczenie z oceną

K – Literatura przedmiotu

Literatura obowiązkowa:

4. C. Banasiński, *Cyberbezpieczeństwo*. Zarys wykładu. Wolters Kluwer, 2018.
5. *Prawodawstwo:*
   - 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 na lata 2019-2024;
   - Polityka i koncepcje dotyczące cyberbezpieczeństwa (NATO, organizacji Unii Europejskiej i innych organizacji międzynarodowych).

Literatura zalecana / fakultatywna:

(publikacje udostępniane dla studentów przez wykładowcę podczas zajęć)

1. 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
2. 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.
3. 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
4. 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

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	**na studiach niestacjonarnych**
Godziny zajęć z nauczycielem/ami	30	20
Czytanie literatury	8	8
Przygotowanie do zajęć	4	7
Przygotowanie prezentacji / referatu	4	7
Przygotowanie do zaliczenia	4	8
Suma godzin:	**50**	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**	**2**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	10.06.2022 r.
Dane kontaktowe (e-mail, telefon)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Kryminologia stosowana
	Poziom studiów	Studia pierwszego stopnia
	Forma studiów	Studia stacjonarne/niestacjonarne
	Profil kształcenia	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.C.4.**

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Ujawnianie i zwalczanie przestępstw przy użyciu sieci**
2. Punkty ECTS	**3**
3. Rodzaj przedmiotu	**obieralny**
4. Język przedmiotu	**polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Łukasz Lemieszewski, Mariusz Kowalski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 5	**W**: (30); **Ć:** (15)	**W**: (10); **Ć:** (8)
Liczba godzin ogółem	**45**	**18**

C - Wymagania wstępne

-

D - Cele kształcenia

	Wiedza
CW1	Wyposażenie studenta w wiedzę w zakresie ujawniania i zwalczania przestępstw przy użyciu sieci.
	Umiejętności
CU1	Zdobycie przez studenta umiejętności ujawniania i zwalczania przestępstw przy użyciu sieci.
CU2	Zdobycie przez studenta umiejętności posługiwania się przepisami prawa w aspekcie ujawniania i zwalczania przestępstw przy użyciu sieci.
	Kompetencje społeczne
CK1	Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności odnośne ujawniania i zwalczania przestępstw przy użyciu sieci.

E - Efekty kształcenia przedmiotowe i kierunkowe

Przedmiotowy efekt kształcenia (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EPW…)		
EPW1	Student ma zaawansowaną wiedzę na temat ujawniania i zwalczania przestępstw przy użyciu sieci oraz wiedzę na temat instytucji organów ochrony porządku prawnego z ich współpracy innymi podmiotami w tym zakresie.	K_W02 K_W13 K_W06
Umiejętności (EPU…)		
EPU1	Student potrafi prawidłowo interpretować i wyjaśniać zasady i metody ujawniania i zwalczania przestępstw przy użyciu sieci.	K_U01 K_U02
EPU2	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 (EPK…)		
EPK1	Student uzupełnienia i doskonali nabytą wiedzę i umiejętności odnośne ujawniania i zwalczania przestępstw przy użyciu sieci.	K_K06
EPK2	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

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

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.	5	1
W2	Prawne i pozaprawne źródła wymagań dla systemów cyberbezpieczeństwa oraz praktyczne aspekty cyberbezpieczeństwa. Krajowy system cyberbezpieczeństwa. Dobre praktyki w zakresie bezpieczeństwa IT .	5	2
W3	Postępowanie w przypadku podejrzenia popełnienia cyberprzestępstwa. Służby w Polsce odpowiedzialne za ujawnianie i zwalczanie przestępstw przy użyciu sieci i ich statystyki.	5	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.	5	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.	5	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.	5	2
	Razem liczba godzin wykładów	**30**	**10**

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	Narzędzia sieciowe w systemie Windows	4	2
C2	Ujawnianie i zabezpieczanie śladów. Obserwacja i analiza mechanizmu uzgadniania trójetapowego.	2	1
C3	Biały wywiad teoretycznie i praktycznie.	4	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.	2	1
C5	Rodzaje danych zapisywanych w sieci, wykorzystanie geolokalizacji w procesie wykrywczym . Zabezpieczanie danych z sieci.	3	2
	Razem liczba godzin ćwiczeń	**15**	**8**

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

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

H - Metody oceniania osiągnięcia efektów kształcenia 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 kształcenia **(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.).	**P3-** Ocena podsumowująca na podstawie sumy ocen formułujących

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

Efekty przedmiotowe	Wykład		Ćwiczenia		
	F2	P1	F2	F3	P5
EPW1	x	x	x	x	x
EPU1	x	x	x	x	x
EPU2	x	x	x	x	x
EPK1	x	x	x	x	x

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student zna wybrane pojęcia, zasady, metody, uwarunkowania oraz instytucje organów ochrony porządku prawnego z ich współpracą z innymi podmiotami w zakresie ujawniania i zwalczania przestępstw przy użyciu sieci.	Student zna większość wymaganych pojęć, zasad, metod, uwarunkowań oraz instytucji organów ochrony porządku prawnego z ich współpracą z innymi podmiotami w zakresie ujawniania i zwalczania przestępstw przy użyciu sieci.	Student zna wszystkie wymagane pojęcia, zasady, metody, uwarunkowania oraz instytucje organów ochrony porządku prawnego z ich współpracą z innymi podmiotami w zakresie ujawniania i zwalczania przestępstw przy użyciu sieci.
EPU1	Student wykonuje niektóre zadania dotyczące interpretowania i wyjaśniania zasad i metod ujawniania i zwalczania przestępstw przy użyciu sieci w oparciu o posiadane dane i wiedzę w tym zakresie.	Student wykonuje większość wymaganych zadań dotyczących interpretowania i wyjaśniania zasad i metod ujawniania i zwalczania przestępstw przy użyciu sieci w oparciu o posiadane dane i wiedzę w tym zakresie.	Student wykonuje wszystkie wymagane zadania dotyczące interpretowania i wyjaśniania zasad i metod ujawniania i zwalczania przestępstw przy użyciu sieci w oparciu o posiadane dane i wiedzę w tym zakresie.
EPU2	Student potrafi wykorzystać niektóre poznane sposoby rozwiązania konkretnych problemów dotyczących ujawniania i zwalczania przestępstw przy użyciu sieci z poszanowaniem norm prawnych i etycznych.	Student potrafi wykorzystać większość poznanych sposobów rozwiązania konkretnych problemów dotyczących ujawniania i zwalczania przestępstw przy użyciu sieci z poszanowaniem norm prawnych i etycznych.	Student potrafi wykorzystać wszystkie poznane sposoby rozwiązania konkretnych problemów dotyczących ujawniania i zwalczania przestępstw przy użyciu sieci z poszanowaniem norm prawnych i etycznych.
EPK1	Student rozumie znaczenie aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne ujawniania i zwalczania przestępstw przy użyciu sieci.	Student rozumie i widzi znaczenie swojej aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne ujawniania i zwalczania przestępstw przy użyciu sieci.	Student rozumie i widzi znaczenie swojej aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne ujawniania i zwalczania przestępstw przy użyciu sieci oraz podejmuje dalszą aktywność w tym zakresie.
EPK2	Student posiada umiejętność analizowania złożonych relacji pomiędzy aspektami prawnymi w zakresie funkcjonowania ujawniania i zwalczania przestępstw przy użyciu sieci.	Student posiada umiejętność analizowania złożonych relacji pomiędzy aspektami prawnymi i pozaprawnymi w zakresie funkcjonowania ujawniania i zwalczania przestępstw przy użyciu sieci	Student posiada umiejętność analizowania i rozumienia złożonych relacji pomiędzy aspektami prawnymi i pozaprawnymi w zakresie funkcjonowania ujawniania i zwalczania przestępstw przy użyciu sieci

J – Forma zaliczenia przedmiotu

Wykład – Egzamin, ćwiczenia – zaleczenie z oceną

K – Literatura przedmiotu

Literatura obowiązkowa: 6. C. Banasiński, M. Rojszczak, *Cyberbezpieczeństwo* Wydawnictwo Wolters Kluwer Polska 2020 r. 7. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Wydawnictwo Wolters Kluwer Polska 2016 r. 8. 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 2004 r.

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	45	18
Konsultacje	2	2
Czytanie literatury	8	10
Przygotowanie prezentacji	5	10
Przygotowanie do zajęć	5	15
Przygotowanie do egzaminu	10	20
Suma godzin:	**75**	**75**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**3**	**3**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz modyfikacja: Łukasz Lemieszewski, Mariusz Kowalski (7 października 2021 r.)
Data ~~sporządzenia~~ / aktualizacji	10.06.2022 r.
Dane kontaktowe (e-mail, telefon)	sylwiagwozdziewicz@gmail.com, llemieszewski@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Kryminologia stosowana
	Poziom studiów	Studia pierwszego stopnia
	Forma studiów	Studia stacjonarne/niestacjonarne
	Profil kształcenia	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.C.5.**

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Postępowanie w zwalczaniu cyberprzestępstw**
2. Punkty ECTS	**2**
3. Rodzaj przedmiotu	**obieralny**
4. Język przedmiotu	**polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**Łukasz Lemieszewski, Mariusz Kowalski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 5	**W**: (15); **Ć:** (15)	**W**: (10); **Ć:** (14)
Liczba godzin ogółem	**30**	**24**

C - Wymagania wstępne

-

D - Cele kształcenia

	Wiedza
CW1	Wyposażenie studenta w wiedzę w zakresie postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.
	Umiejętności
CU1	Zdobycie przez studenta umiejętności postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.
CU2	Zdobycie przez studenta umiejętności posługiwania się przepisami prawa i odpowiednimi metodami kryminalistycznymi w aspekcie postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.
	Kompetencje społeczne
CK1	Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności odnośne postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.

E - Efekty kształcenia przedmiotowe i kierunkowe

Przedmiotowy efekt kształcenia (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt kształcenia
Wiedza (EPW…)		
EPW1	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 (EPU…)		
EPU1	Student potrafi prawidłowo interpretować i wyjaśniać zasady i metody postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.	K_U01 K_U02
EPU2	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 (EPK…)		
EPK1	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

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach		
		stacjonarnych		Niestacjonarnych
W1	Internet – charakterystyka i ewolucja. Powstanie społeczeństwa informacyjnego. Próby międzynarodowej regulacji internetu.	1	1	
W2	Terminologia związana z cyberprzestępczością. Historia kontroli nadużyć w cyberprzestrzeni.	2	1	
W3	Wybrane międzynarodowe inicjatywy z zakresu przeciwdziałania cyberprzestępczości: Unia Europejska, Organizacja Współpracy Gospodarczej i Rozwoju, Międzynarodowy Związek Telekomunikacyjny.	4	2	
W4	Zjawisko czyberprzestępczości – charakter, rozmiary, tendencje. Odpowiedzialność za przestępstwa w cyberprzestrzeni.	2	1	
W5	Cyberprzestępczość – wykrywalność, działalność Policji, prokuratury i sądów. Czynniki utrudniające ściganie.	2	1	
W6	Procedury techniczne służące przeciwdziałaniu cyberprzestępczości. Współpraca z wyspecjalizowanymi organizacjami. Świadomość użytkowników.	2	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.	2	2	
	Razem liczba godzin wykładów	**15**	**10**	

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych

C1	Wyszukiwanie danych na cyfrowych nośnikach danych. Odzysk i niszczenie danych	4	2
C2	Analiza metadanych	2	1
C3	Ustalenia dotyczące adresów IP. Techniczne aspekty wymiany informacji z operatorami udostepniającymi Internet.	2	1
C4	Dowód elektroniczny – charakterystyka. Informatyka śledcza jako gałąź nauk sądowych. Badania ich podział i możliwości.	2	1
C5	Wykonywanie kopii binarnych (klonowanie, wykonywanie obrazów) dowodowych nośników danych cyfrowych z wykorzystaniem środowiska Windows i Linux	2	1
C6	Zabezpieczanie i transport sprzętu informatycznego i cyfrowych nośników danych. Opracowanie projektu prawidłowego zabezpieczenia sprzętu informatycznego na miejscu zdarzenia.	3	2
		15	**8**

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

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

H - Metody oceniania osiągnięcia efektów kształcenia 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 kształcenia **(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 i prezentacji, sprawozdań z ćwiczeń **F5 – ćwiczenia praktyczne** (przeprowadzenie symulacji w laboratorium sieci komputerowych WT AJP.).	**P3-** Ocena podsumowująca na podstawie sumy ocen formułujących

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

Efekty przedmiotowe	Wykład			Ćwiczenia		
	F2	**P1**	**P4**	**F2**	**F3**	**F5**
EPW1	x	x	x	x	x	x
EPU1	x	x	x	x	x	x
EPU2	x	x	x	x	x	x

EPK1	x	x	x	x	x	x

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt kształcenia (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student zna wybrane pojęcia, zasady, metody, uwarunkowania oraz instytucje organów ochrony porządku prawnego z ich współpracą z innymi postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.	Student zna większość wymaganych pojęć, zasad, metod, uwarunkowań oraz instytucji organów ochrony porządku prawnego z ich współpracą z innymi podmiotami w zakresie postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.	Student zna wszystkie wymagane pojęcia, zasady, metody, uwarunkowania oraz instytucje organów ochrony porządku prawnego z ich współpracą z innymi podmiotami w zakresie postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.
EPU1	Student wykonuje niektóre zadania dotyczące interpretowania i wyjaśniania zasad i metod postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw w oparciu o posiadane dane i wiedzę w tym zakresie.	Student wykonuje większość wymaganych zadań dotyczących interpretowania i wyjaśniania zasad i metod postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw w oparciu o posiadane dane i wiedzę w tym zakresie.	Student wykonuje wszystkie wymagane zadania dotyczące interpretowania i wyjaśniania zasad i metod postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw. w oparciu o posiadane dane i wiedzę w tym zakresie.
EPU2	Student potrafi wykorzystać niektóre poznane sposoby rozwiązania konkretnych problemów dotyczących postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw z poszanowaniem norm prawnych i etycznych.	Student potrafi wykorzystać większość poznanych sposobów rozwiązania konkretnych problemów dotyczących postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw z poszanowaniem norm prawnych i etycznych.	Student potrafi wykorzystać wszystkie poznane sposoby rozwiązania konkretnych problemów dotyczących postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw z poszanowaniem norm prawnych i etycznych.
EPK1	Student rozumie znaczenie aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.	Student rozumie i widzi znaczenie swojej aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw.	Student rozumie i widzi znaczenie swojej aktywności w zakresie uzupełnienia i doskonalenia nabytej wiedzę i umiejętności odnośne postępowania w przestępstwach komputerowych w zwalczaniu cyberprzestępstw oraz podejmuje dalszą aktywność w tym zakresie.

J – Forma zaliczenia przedmiotu

Egzamin

K – Literatura przedmiotu

Literatura obowiązkowa:

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

Literatura zalecana / fakultatywna:

3. R. A. Stefański, *Metodyka pracy prokuratora w sprawach karnych*, Wyd. Wolters Kluwer, Warszawa 2017 r.
4. E. Samborski, *Zarys metodyki pracy sędziego w sprawach karnych*, Wyd. LexisNexis Polska Sp. z o.o., Warszawa 2013 r.
5. A. Gryszczyńska, G. Szpor (red.) *Internet. Strategie bezpieczeństwa*. Wydawnictwo C.H. Beck, Warszawa 2017 r.
6. I.A. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Wydanie Uniwersytet Warmińsko-Mazurski w Olsztynie, Olsztyn 2017 r.

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	30	24
Konsultacje	2	2
Czytanie literatury	2	4
Przygotowanie raportu	6	6
Przygotowanie do zajęć	3	4
Przygotowanie do egzaminu	7	10
Suma godzin:	**50**	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**	**2**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz modyfikacja: Łukasz Lemieszewski, Mariusz Kowalski (7 października 2021 r.)
Data sporządzenia / aktualizacji	10.06.2022 r.
Dane kontaktowe (e-mail, telefon)	sylwiagwozdziewicz@gmail.com, llemieszewski@ajp.edu.pl
Podpis	Sylwia Gwoździewicz

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

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Informatyka śledcza i dowody w postaci elektronicznej w wykrywaniu cyberprzestępstw**
2. Punkty ECTS	**5**
3. Rodzaj przedmiotu	**Specjalnościowy**
4. Język przedmiotu	**Polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 5	**W**: (15); **Ćw.**: (15);	**W**: (10); **Ćw.**: (8);
Semestr 6	**W:**(15) **Ćw:.**(15)	**W**: (8); **Ćw.**: (10)
Liczba godzin ogółem	**60**	**36**

C - Wymagania wstępne

Podstawowa wiedza z zakresu prawa karnego

D - Cele kształcenia

	Wiedza
CW1	**Wyposażenie studentów w interdyscyplinarną wiedzę niezbędną do właściwego podejmowania decyzji oraz efektywnego wykonywania aktywności zawodowej**
	Umiejętności
CU1	**Wykształcenie umiejętności identyfikowania szans lub zagrożeń oraz podejmowania adekwatnych działań w zakresie wykrywania cyberprzestępstw**
	Kompetencje społeczne
CK1	**Wykształcenie postawy poszanowania prawa i kompetencji zwalczania jego naruszeń , w szczególności cyberprzestępstw**
CK2	**Uwrażliwienie na potrzebę profesjonalnego zachowania się w ramach prowadzonej informatyki śledczej i przygotowanie do ponoszenia odpowiedzialności za podjęte działania w wykrywaniu cyberprzestępstw**

E - Efekty uczenia się przedmiotowe i kierunkowe

Przedmiotowy efekt uczenia się (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		Kierunkowy efekt uczenia się
Wiedza (EPW…)		
EPW1	Student zna w stopniu zaawansowanym zasady zdobywania i przeprowadzania dowodów w postacie elektronicznej w wykrywaniu cyberprzestępstw w postępowaniu karnym na etapie sądowym,	K_W03
EPW2	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 śledzczej	K_W06
Umiejętności (EPU…)		
EPU1	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
EPU2	Potrafi prawidłowo prognozować potrzebę uczenia się przez całe życie z uwzględnieniem perspektywy własnej kariery zawodowej	K_U10
Kompetencje społeczne (EPK…)		
EPK1	Student potrafi współdziałać i pracować w grupie na różnych etapach realizowanych projektów, wykorzystując odpowiednie kanały i sposoby komunikacji.	K_K01
EPK2	Student uzupełnia i doskonali wiedzę i umiejętności w różnych dziedzinach zarówno w ramach pracy własnej, jak i zorganizowanych form kształcenia	K_K06
EPK3	Student potrafi prawidłowo identyfikować ryzyka oraz szanse prowadzonej aktywności oraz podejmuje działania w oparciu o przeprowadzoną diagnozę.	K_K08

F – Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	Niestacjonarnych
W1	Zapoznanie studentów z planem i programem nauczania przedmiotu, celami i efektami uczenia się oraz formą zaliczenia 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 danych informatycznym	4	2
C2	Przestępstwa komputerowe	6	3
C3	Przestępstwa ze względu na charakter zawartych informacji, prawa autorskie	4	3
C4	Zabezpieczanie dowodów cyfrowych	4	2
C6	Analiza danych na dowodach cyfrowych	4	2

C7	Analiza aktywności internetowej użytkownika komputera	4	3
C8	Wykorzystanie sieci w procesie wykrywczym	4	3
		30	**18**

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

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

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

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

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

Efekty przedmiotowe	**Wykład**		**Ćwiczenia**		
	P2	F2	F2	F3	F4
EPW1	X	X	X		X
EPW2		X	X	X	X
EPU1	X	X	X		X
EPU2		X	X	X	X
EPK1	X	X	X		X
EPK2		x	x	X	X
EPK3		x	x		

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt uczenia się (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student ma wiedzę o charakterze nauk prawnych w aspekcie ochrony środowiska.	Student ma wiedzę o charakterze nauk prawnych, a szczególności prawa karnego oraz potrafi ustalić	Student wyróżniająco potrafi określić relacje pomiędzy naukami prawnymi a a innymi naukami zajmującymi się

		relacje z naukami o ochronie środowiska.	kwestiami prawnymi w zakresie ochrony środowiska.
EPW2	Student potrafi określić struktury i organy zajmujące się kwestiami ochrony środowiska.	Student ma wiedzę na temat różnych struktur, organów i instytucji związanych z ochroną środowiska oraz ich wzajemnych relacji.	Student wyróżnia się wiedzą na temat różnych struktur, organów i instytucji związanych z ochroną środowiska oraz ich wzajemnych relacji.
EPU1	Student z pomocą innych potrafi wykorzystywać posiadany zasób wiedzy do analizowania faktycznego stanu ochrony środowiska.	Student potrafi wykorzystywać posiadany zasób wiedzy do analizowania faktycznego stanu ochrony środowiska.	Student wyróżnia się w wykorzystywaniu posiadanego zasobu wiedzy do analizowania faktycznego stanu ochrony środowiska.
EPU2	Student musi korzystać ze wsparcia przy posługiwaniu się przepisami prawa krajowego i wspólnotowego do rozwiązywania problemów związanych z ochroną środowiska.	Student posługuje się przepisami prawa krajowego i wspólnotowego do rozwiązywania problemów związanych z ochroną środowiska.	Student wyróżnia się w posługiwaniu przepisami prawa krajowego i wspólnotowego do rozwiązywania problemów związanych z ochroną środowiska.
EPK1	Student potrafi współpracować w grupie w zakresie realizacji programów związanych z ochroną środowiska.	Student przejawia aktywność w zespołowej realizacji projektów związanych z oceną zagrożeń realizowanych projektów związanych z ochroną środowiska.	Student potrafi przejmować kierownictwo w grupach realizujących projekty związane z oddziaływaniem na środowisko.
EPK2	Student potrafi identyfikować ryzyka związane z realizacją projektów związanych ze środowiskiem.	Student potrafi identyfikować ryzyka i dokonywać diagnozy w zakresie oddziaływania na środowisko.	Student wyróżnia się w identyfikowaniu ryzyk i dokonywaniu diagnozy w zakresie oddziaływania na środowisko.
EPK3	Student potrafi identyfikować ryzyka oraz szanse prowadzonej aktywności nie zawsze prawidłowo.	Student potrafi prawie w każdym przypadku prawidłowo identyfikować ryzyka.	Student potrafi prawidłowo identyfikować ryzyka oraz szanse prowadzonej aktywności oraz podejmuje działania w oparciu o przeprowadzoną diagnozę.

J – Forma zaliczenia przedmiotu

Egzamin

K – Literatura przedmiotu

Literatura obowiązkowa:

1. Ustawa z dnia 6 czerwca 1997r. Kodeks karny,
2. Ustawa z dnia 6 czerwca 1997r. Kodeks postępowania karnego
3. Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001r. (Dz.U. poz. 728 z 2015r.)

Literatura zalecana / fakultatywna:

1. Rozporządzenie Ministra Sprawiedliwości z dnia 14 września 2012 r. w sprawie rodzaju urządzeń i środków technicznych służących do utrwalania obrazu lub dźwięku dla celów procesowych oraz sposobu przechowywania, odtwarzania i kopiowania zapisów
2. Dowody cyfrowe w postępowaniu karnym – *opracowania dowolnego autora*

L – Obciążenie pracą studenta:

	Liczba godzin na realizację

Forma aktywności studenta	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	30	18
Konsultacje	2	2
Czytanie literatury	25	25
Przygotowanie referatu / prezentacji	20	30
Przygotowanie rozwiązania zadania	15	27
Przygotowanie do egzaminu	25	25
Suma godzin:	**125**	**125**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**5**	**5**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Paweł Tomaszewski
Data sporządzenia / aktualizacji	10.06.2022 r.
Dane kontaktowe (e-mail)	ptomaszewski@ajp.edu.pl
Podpis	Tomaszewski

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Kryminologia stosowana
	Poziom studiów	Studia pierwszego stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil kształcenia	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.C.7.**

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Włamania do sieci i systemów informatycznych. Cyberataki.**
2. Punkty ECTS	**2**
3. Rodzaj przedmiotu	**Specjalnościowy**
4. Język przedmiotu	**polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**dr inż. Łukasz Lemieszewski** **dr Paweł Tomaszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 6	**W**: (15); **Ćw.**: (15);	**W**: (10); **Ćw.**: (8);
Liczba godzin ogółem	**30**	**18**

C - Wymagania wstępne

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

D - Cele kształcenia

	Wiedza
CW1	**Wyposażenie studentów w interdyscyplinarną wiedzę niezbędną do właściwego podejmowania decyzji oraz efektywnego wykonywania aktywności zawodowej**
	Umiejętności
CU1	**Wykształcenie umiejętności identyfikowania szans lub zagrożeń oraz podejmowania adekwatnych działań**
	Kompetencje społeczne
CK1	**Uwrażliwienie na potrzebę profesjonalnego zachowania się i przygotowanie do ponoszenia odpowiedzialności za podjęte działania**

E - Efekty uczenia się przedmiotowe i kierunkowe

Przedmiotowy efekt uczenia się (EP) w zakresie wiedzy (W), umiejętności (U) i kompetencji społecznych (K)		**Kierunkowy efekt uczenia się**
	Wiedza (EPW…)	
EPW1	Ma wiedzę na temat współczesnych zjawisk związanych z zagrożeniem bezpieczeństwa cybernetycznego	K_W09
	Umiejętności (EPU…)	

EPU1	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 (EPK...)		
EPK1	Identyfikacji głównych problemów podejmowanej działalności, przewidywania jej skutków, uwzględnia towarzyszących im ryzyk, rozpoznawania zagrożeń i patologii oraz podjęcia właściwej reakcji	K_K05
EPK2	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

F - Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Zapoznanie studentów z planem i programem nauczania przedmiotu, celami i efektami uczenia się oraz formą zaliczenia 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**

G – 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.

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

Forma zajęć	**Ocena formująca (F) –** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)**	**Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)**
Wykład		**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.**

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

Efekty przedmiotowe	Wykład	Ćwiczenia	
	P2	**F2**	**F3**
EPW1	X		
EPU1	X	X	X
EPK1	X		X
EPK2		X	X

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
	Ocena		
Przedmiotowy efekt uczenia się (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Zna wybrane terminy z zakresu metod stosowanych w atakach sieciowych na infrastrukturę Internetu	Zna większość terminów z zakresu metod stosowanych w atakach sieciowych na infrastrukturę Internetu	Zna wszystkie wymagane terminy metody narzędzia i techniki wykorzystywane w Cyberbezpieczeństwie i aktywnej ochronie zasobów sieciowych
EPU1	Wykonuje niektóre testy podatności oraz zna zasady i metody konfiguracji niektórych urządzeń sieciowych	Wykonuje większość testów podatności rozumie pojęcia z zakresu „siły" systemów kryptograficznych, zna zasady uwierzytelniania i bezpiecznej konfiguracji urządzeń	Wykonuje wszystkie wymagane analizy podatności oraz posługuje się narzędziami wspomagającymi testowanie podatności oraz wspomagającymi ochronę sieci przed Cyber zagrożeniami
EPK1	Rozumie, potrzebę ochrony użytkowników i infrastruktury Internetu	Rozumie potrzebę ochrony użytkowników i infrastruktury Internetu, rozpoznaje wybrane zagrożenia i świadomie stosuje wybrane narzędzia przeciwdziałania Cyberzagrożeniom	Rozumie potrzebę ochrony użytkowników i infrastruktury Internetu, rozpoznaje zagrożenia i świadomie stosuje narzędzia przeciwdziałania Cyberzagrożeniom
EPK2	Uzupełnienia, ale nie i doskonali nabytej wiedzy i umiejętności w dziedzinie włamania do sieci i systemów informatycznych	Uzupełnienia i doskonalenia nabytej wiedzy i umiejętności w dziedzinie włamania do sieci i systemów informatycznych	Uzupełnienia i doskonalenia nabytej wiedzy i umiejętności w dziedzinie włamania do sieci i systemów informatycznych w ramach pracy własnej, jak i zorganizowanych form kształcenia

J – Forma zaliczenia przedmiotu

Zaliczenie z oceną

K – Literatura przedmiotu

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.

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	30	18
Czytanie literatury	8	12
Przygotowanie raportu	6	10
Przygotowanie do zaliczenia	6	10
Suma godzin:	**50**	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**	**2**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Sylwia Gwoździewicz
Data sporządzenia / aktualizacji	10.06.2022 r.
Dane kontaktowe (e-mail)	sgwozdziewicz@ajp.edu.pl
Podpis	Sylwai Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Kryminologia stosowana
	Poziom studiów	Studia pierwszego stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil kształcenia	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**ZC.C.8.**

PROGRAM PRZEDMIOTU/MODUŁU

A - Informacje ogólne

1. Nazwa przedmiotu	**Bezpieczeństwo sieci i systemów informatycznych**
2. Punkty ECTS	**4**
3. Rodzaj przedmiotu	**Specjalnościowy**
4. Język przedmiotu	**polski**
5. Rok studiów	**III**
6. Imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia	**dr Paweł Tomaszewski**

B – Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Nr semestru	Studia stacjonarne	Studia niestacjonarne
Semestr 6	**W**: (15); **Ćw.**: (15);	**W**: (8); **Ćw.**: (10;
Liczba godzin ogółem	**30**	**18**

C - Wymagania wstępne

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

D - Cele kształcenia

	Wiedza
CW1	**Wyposażenie studentów w interdyscyplinarną wiedzę niezbędną do właściwego podejmowania decyzji oraz efektywnego wykonywania aktywności zawodowej**
	Umiejętności
CU1	**Wykształcenie umiejętności identyfikowania szans lub zagrożeń oraz podejmowania adekwatnych działań**
	Kompetencje społeczne
CK1	**Uwrażliwienie na potrzebę profesjonalnego zachowania się i przygotowania do ponoszenia odpowiedzialności za podjęte działania**

E - Efekty uczenia się przedmiotowe i kierunkowe

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

EPW1	Student ma wiedzę na temat współczesnych zjawisk związanych z zagrożeniem bezpieczeństwa cybernetycznego	K_W09
Umiejętności (EPU…)		
EPU1	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
EPU2	Student posiada umiejętność analizowania i rozumienia złożonych relacji pomiędzy aspektami prawnymi i pozaprawnymi w zakresie funkcjonowania sieci i systemów informatycznych	K_U14
Kompetencje społeczne (EPK…)		
EPK1	Student potrafi współdziałać i pracować w grupie na różnych etapach realizowanych projektów, wykorzystując odpowiednie kanały i sposoby komunikacji.	K_K01
EPK2	Student potrafi prawidłowo identyfikować ryzyka oraz szanse prowadzonej aktywności oraz podejmuje działania w oparciu o przeprowadzoną diagnozę.	K_K08
EKP3	Student potrafi identyfikować główne problemy podejmowanej działalności, przewidywania jej skutków, uwzględniania towarzyszących im ryzk, rozpoznawania zagrożeń i patologii oraz podjęcia właściwej reakcji	K_K05

F – Treści programowe oraz liczba godzin na poszczególnych formach zajęć

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	Niestacjonarnych
W1	Zapoznanie studentów z planem i programem nauczania przedmiotu, celami i efektami uczenia się oraz formą zaliczenia. 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).	1	1
W2	Prawne i etyczne aspekty cyberbezpieczeństwa.	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	2
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 kształcenia. 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 narażeniami i terroryzmem elektromagnetycznym	2	2
		15	**10**

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

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

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

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

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

Efekty przedmiotowe	Wykład		Ćwiczenia		
	P1	F2	F2	F3	F4
EPW1	X	X	X		X
EPU1	X	X	X		X
EPU2		X	X	X	X
EPK1	X	X	X		X
EPK2		X	x	X	X
EPK3			x		

I – Kryteria oceniania

Wymagania określające kryteria uzyskania oceny w danym efekcie			
Ocena			
Przedmiotowy efekt uczenia się (EP..)	**Dostateczny dostateczny plus 3/3,5**	**dobry dobry plus 4/4,5**	**bardzo dobry 5**
EPW1	Student ma wiedzę o charakterze nauk prawnych w aspekcie ochrony środowiska.	Student ma wiedzę o charakterze nauk prawnych, a szczególności prawa karnego oraz potrafi ustalić relacje z naukami o ochronie środowiska.	Student wyróżniająco potrafi określić relacje pomiędzy naukami prawnymi a a innymi naukami zajmującymi się kwestiami prawnymi w zakresie ochrony środowiska.
EPW2	Student potrafi określić struktury i organy	Student ma wiedzę na temat różnych struktur, organów i instytucji związanych z	Student wyróżnia się wiedzą na temat różnych struktur, organów i instytucji

	zajmujące się kwestiami ochrony środowiska.	ochroną środowiska oraz ich wzajemnych relacji.	związanych z ochroną środowiska oraz ich wzajemnych relacji.
EPU1	Student z pomocą innych potrafi wykorzystywać posiadany zasób wiedzy do analizowania faktycznego stanu ochrony środowiska.	Student potrafi wykorzystywać posiadany zasób wiedzy do analizowania faktycznego stanu ochrony środowiska.	Student wyróżnia się w wykorzystywaniu posiadanego zasobu wiedzy do analizowania faktycznego stanu ochrony środowiska.
EPU2	Student musi korzystać ze wsparcia przy posługiwaniu się przepisami prawa krajowego i wspólnotowego do rozwiązywania problemów związanych z ochroną środowiska.	Student posługuje się przepisami prawa krajowego i wspólnotowego do rozwiązywania problemów związanych z ochroną środowiska.	Student wyróżnia się w posługiwaniu przepisami prawa krajowego i wspólnotowego do rozwiązywania problemów związanych z ochroną środowiska.
EPK1	Student potrafi współpracować w grupie w zakresie realizacji programów związanych z ochroną środowiska.	Student przejawia aktywność w zespołowej realizacji projektów związanych z oceną zagrożeń realizowanych projektów związanych z ochroną środowiska.	Student potrafi przejmować kierownictwo w grupach realizujących projekty związane z oddziaływaniem na środowisko.
EPK2	Student potrafi identyfikować ryzyka związane z realizacją projektów związanych ze środowiskiem.	Student potrafi identyfikować ryzyka i dokonywać diagnozy w zakresie oddziaływania na środowisko.	Student wyróżnia się w identyfikowaniu ryzyk i dokonywaniu diagnozy w zakresie oddziaływania na środowisko.
EPK3	Student potrafi identyfikować niektóre problemy podejmowanej działalności, ale nie potrafi przewidywać jej skutków, uwzględniania towarzyszących im ryzk, rozpoznawania zagrożeń i patologii oraz podjęcia właściwej reakcji	Student potrafi identyfikować prawie wszystkie główne problemy podejmowanej działalności, przewidywania jej skutków, uwzględniania towarzyszących im ryzk, rozpoznawania zagrożeń i patologii oraz podjęcia właściwej reakcji	Student potrafi identyfikować wszystkie główne problemy podejmowanej działalności, przewidywania jej skutków, uwzględniania towarzyszących im ryzk, rozpoznawania zagrożeń i patologii oraz podjęcia właściwej reakcji

J – Forma zaliczenia przedmiotu

Egzamin

K – Literatura przedmiotu

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.
3. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022*, Warszawa 2017.

L – Obciążenie pracą studenta:

Forma aktywności studenta	Liczba godzin na realizację	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny zajęć z nauczycielem/ami	30	18
Czytanie literatury	15	15
Przygotowanie referatu	20	30
Przygotowanie rozwiązania zadania	15	17
Przygotowanie do egzaminu	20	20
Suma godzin:	**100**	**100**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**4**	**4**

Ł – Informacje dodatkowe

Imię i nazwisko sporządzającego	Paweł Tomaszewski
Data sporządzenia / aktualizacji	10.06.2022 r.
Dane kontaktowe (e-mail)	ptomaszewski@ajp.edu.pl
Podpis	Tomaszewski