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

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo narodowe
	Poziom studiów	Studia II stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**CYBER.1**

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Prawo UE i RP dotyczące cyberbezpieczeństwa**
Punkty ECTS	**3**
Rodzaj zajęć	**obieralny**
Moduł/specjalizacja	**cyberbezpieczeństwo**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Gwoździewicz - koordynator specjalności Cyberbezpieczeństwo** **dr Sylwia Gwoździewicz - prowadząca zajęcia**

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

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

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych.

4. Cele kształcenia

C1 - Wyposażenie studenta w wiedzę z prawa UE i RP dotyczącego cyberbezpieczeństwa.

C2 - Zdobycie przez studenta umiejętności interpretowania i wyjaśniania problemów z obszaru prawa UE i RP dotyczącego cyberbezpieczeństwa.

C3 - Zdobycie przez studenta umiejętności posługiwania się przepisami prawa do rozwiązania konkretnych problemów cyberbezpieczeństwa.

C4 - Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności odnośne prawa UE i RP dotyczącego cyberbezpieczeństwa.

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, zna i rozumie podstawowe pojęcia i zasady na temat działania na rzecz rozwiązywania problemów prawnych w zakresie cyberbezpieczeństwa państwa i jego systemu nadzoru , również w	K_W01

	wymiarze międzynarodowym.	
UMIEJĘTNOŚCI		
U_01	Student posługuje się w sposób pogłębiony normami i regułami umożliwiającymi rozwiązanie konkretnie postawionego problemu właściwego dla krajowego systemu cyberbezpieczeństwa.	K_U01
U_02	Student potrafi samodzielnie planować i realizować własne uczenie się przez całe życie oraz potrafi ukierunkować innych w tym zakresie, uwzględnia także ryzyko i przewiduje skutki podejmowanych decyzji opierając się na zdobytej wiedzy w zakresie prawa dotyczącego cyberbezpieczeństwa.	K_U02
KOMPETENCJE SPOŁECZNE		
K_01	Student potrafi współpracować w grupie i przyjmować w niej różne role, a przy tym docenia znaczenie i znajomość prawa w rozwiązywaniu problemów związanych z cyberbezpieczeństwem państwa.	K_K01

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.	0,5	0,5
W2	Kształtowanie się prawa i aktualna problematyka prawna cyberbezpieczeństwa UE, przedstawienie najważniejszych kwestii i ram prawnych w tym legalnych definicji, np.: system informatyczny, sieci i systemy informatyczne, cyberbezpieczeństwo, cyberzagrożenia, w systemie prawnym UE (analiza rozporządzeń i dyrektyw).	10	5
W3	Kształtowanie się prawa i aktualna problematyka prawna cyberbezpieczeństwa RP, przedstawienie najważniejszych kwestii i ram prawnych w tym legalnych definicji, np.: system informacyjny, system teleinformatyczny, cyberbezpieczeństwo, cyberzagrożenia, podatność, ryzyko cyberbezpieczeństwa, incydent - w systemie prawnym UE (analiza Ustawy o krajowym systemie cyberbezpieczeństwa i aktów wykonawczych i prawno-administracyjnych na aktualnych przykładach).	10	5
W4	Ramy prawne współpracy międzynarodowej w zakresie cyberbezpieczeństwa.	3,5	2,5
W5	Współpraca krajowych zespołów CISIRT z agencjami i instytucjami UE, w tym z ENISA, ONZ, NATO.	3	1
W6	Wymiar sprawiedliwości i pomoc prawna w dochodzeniach karnych w cyberprzestrzeni.	3	1
	Razem liczba godzin wykładów	**30**	**15**

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	Analiza wybranych problemów np. na podst. m.in. *Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.*	4	3
C2	Analiza wybranych problemów np. na podst. m.in. *Dyrektywy Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów*	4	3

	informatycznych na terytorium Unii (oraz po zmianach / Dyrektywa NIS 2)		
C2	Analiza wybranych praktycznych problemów prawno-administracyjnych jednostek organizacyjnych i osób fizycznych, dotyczących cyberbezpieczeństwa oraz dochodzeń karnych w cyberprzestrzeni.	4	3
C	Analiza wybranych praktycznych problemów prawno-administracyjnych jednostek organizacyjnych i osób fizycznych, dotyczących dochodzeń karnych w cyberprzestrzeni.	3	3
	Razem liczba godzin ćwiczeń	**15**	**12**

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

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M1 – Metoda podająca** (objaśnienie) **M2 – Metoda problemowa / metody aktywizujące** (dyskusja)	Projektor multimedialny, komputer.
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia przedmiotowe** (analizy problemowe związana z ćwiczeniami; pytania i odpowiedzi itp.).	Projektor multimedialny, komputer Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams

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	**-**	**P1 - Egzamin** (pisemny)
Ćwiczenia	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć; ocena ćwiczeń wykonywanych podczas zajęć) **F5 – Ćwiczenia praktyczne** (analiza i rozstrzygnięcie stanów faktycznych, dyskusje, rozwiązywanie testów cząstkowych przygotowanych przez prowadzącego w systemie np. MsTeams).	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych podczas realizacji ćwiczeń.

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

Symbol efektu	Wykład	Ćwiczenia	
	P1	F2	F5
W_01	x	x	x
U_01	x	x	
U_02	x	x	x
U_03	x		x
K_01	x	x	

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

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

Ocena podsumowująca oceny jest sumą ocen formułujących.

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

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

10. Forma zaliczenia zajęć

Egzamin

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

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	**na studiach niestacjonarnych**
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	45	27
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do kolokwium zaliczeniowych	5	4
przygotowanie do egzaminu	8	10
wykonanie ćwiczeń,	5	10
zapoznanie z literaturą	5	10
przygotowanie do zajęć	7	14
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. Banasiński C., Ratajczak M. (red.), *Cyberbezpieczeństwo*, Warszawa 2020.
2. Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.
3. Rozporządzenie 2019/881 *w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (akt o cyberbezpieczeństwie).*
4. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu i bezpieczeństwa sieci i systemów informatycznych na terytorium UE (oraz po zmianach / Dyrektywa NIS 2)*
5. *Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.*
6. Ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018 poz. 1560 z późn zm.).

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.

Literatura zalecana / fakultatywna:

1. Gwoździewicz S., *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, Wrocław 2018, s. 25-44, SBN 978-83-65422-82-8
2. Gwoździewicz S., *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, ISBN 978-83-8198-782-0, ISBN e-book 978-83-8198-7 7, (rozdział IV w części V s. 223-236).
3. Gwoździewicz S., *Problematyka cyberataków w dobie Przemysłu 4.0 a ściganie przestępstw dotyczących sieci i systemów informatycznych w dochodzeniach karnych w cyberprzestrzeni* [w] Perspektywy bezpieczeństwa – wybrane zagadnienia teorii i praktyki. Vol. I. (red.) P. Chodak, Wydawnictwo AGH, Kraków 2021 (w procesie wydawniczym)

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz i dr Andrzej Skwarski
data sporządzenia / aktualizacji	10.06.2022 r.
dane kontaktowe (e-mail)	sylwiagwozdziewicz@gmail.com
podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo narodowe
	Poziom studiów	Studia II stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**CYBER.2**

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Rozwój technologii ICT i certyfikacja cyberbezpieczeństwa**
Punkty ECTS	**3**
Rodzaj zajęć	**obieralny**
Moduł/specjalizacja	**cyberbezpieczeństwo**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Gwoździewicz - koordynator specjalności Cyberbezpieczeństwo** **dr Sylwia Gwoździewicz - prowadząca zajęcia**

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

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

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych.

4. Cele kształcenia

C1 - Wyposażenie studenta w wiedzę o nowych technologiach ICT i certyfikacji cyberbezpieczeństwa.

C2 - Zdobycie przez studenta umiejętności dobierania środków, metod pracy w obszarze doboru i stosowania bezpiecznych technologii ICT.

C3 - Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności odnośne rozwoju technologii ICT i certyfikacji cyberbezpieczeństwa oraz kształtowanie postawy podejmowania współpracy grupowej w analizie problematyki nowych technologii ICT.

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	Studenta ma pogłębioną wiedzę o współzależnościach między elementami struktury systemu certyfikacji cyberbezpieczeństwa w wymiarze narodowym i międzynarodowym, społecznym oraz wykorzystuje odpowiednie modele teoretyczne do opisów i analizowania nowych	K_W03 K_W12

	technologii ICT i certyfikacji cyberbezpieczeństwa	
UMIEJĘTNOŚCI		
U_01	Student samodzielnie wybiera i stosuje właściwy dla cyberbezpieczeństwa sposób postępowania, potrafi dobierać środki, metody pracy w celu efektywnego wykonywania pojawiających się zadań zawodowych również w obszarze doboru i stosowania odpowiednich i certyfikowanych technologii ICT.	K_U05 K_U07
KOMPETENCJE SPOŁECZNE		
K_01	Student rozumie potrzebę uczenia się przez całe życie oraz konieczność ciągłego rozwoju osobowego i zawodowego w obszarze rozwoju technologii ICT i certyfikacji cyberbezpieczeństwa, potrafi również współpracować w grupie i przyjmować w niej różne role.	K_K02 K_K04

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 wykładów i ćwiczeń.	0,5	0,5
W2	Terminologia i rozwój technologii ICT. Transformacja cyfrowa i wyzwania Przemysłu 4.0. Big Data a Data Science i Data Mining. Internet Rzeczy (IoT). Sieć 5G. Technologia Blockchain. Sztuczna Inteligencja (AI) i Machine Learning (ML).	5	2,5
W3	Wirtualna rzeczywistość. Rozwiązania chmurowe. Zastosowanie i problematyka dotycząca wyzwań i zagrożeń.	5	2,5
W4	Certyfikacja cyberbezpieczeństwa. Analiza legalnych definicji: europejski i krajowy program certyfikacji cyberbezpieczeństwa; europejski certyfikat cyberbezpieczeństwa; produkt ICT; usługa ICT; proces ICT; krajowa jednostka akredytująca; jednostka i poziomy oceniające zgodność; norma; specyfikacja techniczna; poziom uzasadnienia zaufania. ENISA - zadania, cele, budowanie zdolności, współpraca operacyjna na poziomie unijnym. Rynek, certyfikacja cyberbezpieczeństwa i normalizacja; Grupa Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa.	5,5	2,5
W5	Europejskie ramy certyfikacji cyberbezpieczeństwa. Przygotowanie, przyjęcie i przegląd europejskiego programu certyfikacji cyberbezpieczeństwa. Cele bezpieczeństwa europejskich programów certyfikacji cyberbezpieczeństwa.	5	3
W6	Poziomy uzasadnienia zaufania europejskich programów certyfikacji cyberbezpieczeństwa. Elementy europejskich programów certyfikacji cyberbezpieczeństwa. Cyberbezpieczeństwo certyfikowanych produktów ICT, usług ICT i procesów ICT. Certyfikacja cyberbezpieczeństwa.	5	2
W7	Krajowe programy certyfikacji cyberbezpieczeństwa i krajowe certyfikaty cyberbezpieczeństwa. Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa	4	2
	Razem liczba godzin wykładów	**30**	**15**

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

		stacjonarnych	niestacjonarnych
C1	Analiza wybranych problemów dotyczących produktów ICT, usług ICT i procesów ICT dla Internetu Rzeczy (IoT), Sieci 5G, Technologii Blockchain. Sztucznej Inteligencji (AI) i Machine Learningu (ML).	4	3
C2	Wirtualna rzeczywistość. Rozwiązania chmurowe. Wyzwania i zagrożenia a certyfikacja.	4	3
C3	Praktyczne przykłady wykorzystania systemów Big Data w procesach informatyzacji dla przykładowych sektorów i organizacji.	3,5	3
C4	Wyzwania, uwarunkowania i zagrożenia w zakresie wykorzystania systemów Big Data.	3,5	3
	Razem liczba godzin ćwiczeń	**15**	**12**

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

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M1 – Metoda podająca** (objaśnienie) **M2 – Metoda problemowa / metody aktywizujące** (dyskusja)	Projektor multimedialny, komputer. Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia przedmiotowe** (analizy problemowe związana z ćwiczeniami; pytania i odpowiedzi itp.).	Projektor multimedialny, komputer. Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams
Laboratoria	Np. ćwiczenia doskonalące obsługę programów edytorskich	

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	-	**P1 - Egzamin** (pisemny)
Ćwiczenia	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć; ocena ćwiczeń wykonywanych podczas zajęć) **F5 – Ćwiczenia praktyczne** (analiza i rozstrzygnięcie stanów faktycznych, dyskusje, rozwiązywanie problemów przygotowanych przez prowadzącego w systemie np. MsTeams, prezentacje wykonywane w grupach na wskazany przez prowadzącego temat).	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych podczas realizacji ćwiczeń.

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

Symbol	Wykład	Ćwiczenia

efektu	P1	F2	F5
W_01	**x**	**x**	**x**
U_01	**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 sumą ocen formułujących.

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

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

10. Forma zaliczenia zajęć

Egzamin

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

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

wykonanie ćwiczeń,	8	10
zapoznanie z literaturą	7	10
Przygotowanie do zajęć	7	14
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. V. Dhillon, D. Metcalf, M. Hooper, *Zastosowania technologii Blockchain*, Wolters Kluwer, 2018.
2. K. Flaga-Gieruszyńska, J. Gołaczyński, *Prawo nowych technologii*, Wolters Kluwer, 2021.
3. A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Wolters Kluwer, 2018.
4. M. Wrzosek (red.) *Akt o cyberbezpieczeństwie – nowy mandat ENISA i certyfikacja cyberbezpieczeństwa,* NASK 2019 / www.cyberpolicy.nask.pl
5. *Industry 4.0 - Cybersecurity Challenges and Recommendations,* Raport ENISA, 2019 / www.enisa.europa.eu
6. Rozporządzenie 2019/881 *w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (akt o cyberbezpieczeństwie).*

Literatura zalecana / fakultatywna:

1. A. Gorelik, *Korporacyjne jezioro danych. Wykorzystaj potencjał Big Data w swojej organizacji*, Helion, 2020
2. D. Prokopowicz, S. Gwoździewicz, J. Grzegorek, *Wykorzystanie platform analitycznych Big Data Analytics technologii informacyjnych ICT w analizie sentymentu dla wybranej problematyki związanej z Przemysłem 4.0* [w] Bezpieczeństwo informacyjne jednostek organizacyjnych. Wybrane problemy (pod red.) P. Suwaj, S. Gwoździewicz, K. Samulska, Wyd. Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim, 2021 r. (rozdział w monografii, p. 101-143)
3. S. Gwoździewicz, D. Prokopowicz, J. Grzegorek, *Zastosowanie zaawansowanych narzędzi przetwarzania danych w dobie cyfryzacji* [w] Cyfryzacja w zarządzaniu, (red.) Aleksandra Laskowska-Rutkowska, Wydawnictwo CeDeWu, Warszawa 2020, ISBN 978-83-8102-394-8 (rozdział IV, s. s. 93-126).
4. Nguyen Ngoc Thach, Hoang Thanh Hanh, Sylwia Gwoździewicz, Dinh Tran Ngoc Huy, Le Thi Viet Nga, Do Minh Thuy, Pham Van Hong, *Technology Quality Management of the Industry 4.0 and Cybersecurity Risk Management on Current Banking Activities in Emerging Markets - The Case in Vietnam*, International Journal for Quality Research, Volume 15, Number 3, 2021.
5. S. Gwoździewicz, Dinh Tran Ngoc Huy, Nguyen Thu Thuy, Nguyen Thuy Dung, Guyen Duy Mau, *Risk Assessment of Viet Nam Telecommunication Industry under Financial Leverage and Role of New ICT and Cybersecurity at the Sector Challenges*, International Journal of Mechanical and Production Engineering Research and Development , Vol. 10, Issue 3, Jun 2020, p. 1715-1722.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz i dr Andrzej Skwarski
data sporządzenia / aktualizacji	10.06.2022 r.
dane kontaktowe (e-mail)	sylwiagwozdziewicz@gmail.com
podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo narodowe
	Poziom studiów	Studia II stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**CYBER.3**

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Cyberzagrożenia i zarządzanie incydentem**
Punkty ECTS	**3**
Rodzaj zajęć	**obieralny**
Moduł/specjalizacja	**cyberbezpieczeństwo**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Gwoździewicz - koordynator specjalności Cyberbezpieczeństwo** **dr Sylwia Gwoździewicz - prowadząca zajęcia**

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

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

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych.

4. Cele kształcenia

C1 - Wyposażenie studenta w wiedzę w zakresie cyberzagrożeń i zarządzania incydentem.

C2 -Zdobycie przez studenta umiejętności interpretowania i wyjaśniania problematyki w zakresie cyberzagrożeń i zarządzania incydentem.

C3 - Zdobycie przez studenta umiejętności rozwiązania konkretnych problemów dotyczących cyberzagrożeń i zarządzania incydentem.

C4 - Kształtowanie kompetencji współpracy w grupie.

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 dysponuje wiedzą w zakresie cyberzagrożeń i zarządzania incydentem, która jest niezbędna w pracy zawodowej w podmiotach	K_W13

	państwowych, prywatnych czy też organizacjach społecznych.	
UMIEJĘTNOŚCI		
U_01	Student potrafi prawidłowo interpretować i wyjaśniać cyberzagrożenia oraz potrafi dobierać środki, metody pracy w celu efektywnego wykonywania zadań i efektywnego proponowania rozwiązań w zakresie zarządzania incydentem.	K_U05 K_U09
U_02	Student posługuje się ujęciami teoretycznymi i strategiami do rozwiązania praktycznych problemów dotyczących cyberzagrożeń i zarządzania incydentem, wykorzystuje rozwój techniki i narzędzi systemów informatycznych do analizy i oceny cyberzagrożeń i podejmowanych działań praktycznych w zarządzaniu incydentem.	K_U07 K_U12
KOMPETENCJE SPOŁECZNE		
K_01	Student potrafi współpracować w grupie i przyjmować w niej różne role.	K_K04

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.	0,5	0,5
W2	Definicje cyberzagrożeń w porządku prawnym UE i RP. Typologia cyberzagrożeń. Skala cyberzagrożeń.	6	3
W3	Omówienie problematyki i diagnoza cyberzagrożeń. Cyberzagrożenia danych osobowych (kradzieże i wyłudzenia; modyfikacje bądź niszczenie danych; kradzież tożsamości inne.).	5	3
W4	Cyberataki z użyciem szkodliwego oprogramowania (wirusy; robaki komputerowe) i inne rodzaje oprogramowania np. szantażującego (ransomware). Inne sposoby i metody cyberataków (socjotechnika, phishing; skimming; blokowanie dostępu do usług i inne).	5	3
W5	Definicje incydentu (krytyczny, poważny, istotny w podmiocie publicznym, obsługa i zarządzanie incydentem) w porządku prawnym UE i RP. Zadania, obowiązki zespołów CSIRT.	3,5	2
W6	Zarządzanie incydentami oraz współdzielenie informacji o incydentach - wytyczne, obowiązki, rozwiązania organizacyjne. Zarządzanie incydentami a ogólne rozporządzenie o ochronie danych (RODO) i UKSC.	3	1
W7	Obowiązki operatorów usług kluczowych, dostawców usług cyfrowych, podmiotów publicznych Raportowanie incydentów. Inne aspekty praktyczne w zakresie zarządzania incydentami.	3	1
W8	Międzynarodowa problematyka w zakresie przeciwdziałania cyberzagrożeniom.	3,5	1,5
	Razem liczba godzin wykładów	**30**	**15**

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

C1	Analiza wybranych cyberzagrożeń (np. ataki typu Ransomware; robaki i wirusy komputerowe na przykładzie: Stuxnet, Flame, Blaster, WannaCry; popularne ataki DDos i inne z wykorzystaniem Botnetu).	4	3
C2	Wybrane przykłady cyberataków. Jak wykrywać i neutralizować wciąż najgroźniejsze ataki typu Ransomware. Case stady, praktyczne przykłady, dyskusja.	4	3
C3	Zarządzanie incydentem: analiza i wykrywanie zagrożeń w czasie rzeczywistym oraz reakcja na zagrożenia.	3	2
C4	Standaryzacja w zarządzaniu incydentami oraz rola zapewnienia ciągłości działania (metodyka Cyber Kill Chain; metodyki PDCA; zarządzanie incydentami według standardu NIST oraz wytycznych ENISA).	2	2
C5	Identyfikacja incydentu (na wybranych przykładach np. infekcja złośliwym oprogramowaniem, wykryta próba włamania lub wyłudzenia danych), zabezpieczenie dowodów, zgłaszanie incydentu. Procedury. Case stady, praktyczne przykłady, dyskusja.	2	2
	Razem liczba godzin ćwiczeń	**15**	**12**

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

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	**M1 – Metoda podająca** (objaśnienie) **M2 – Metoda problemowa / metody aktywizujące** (dyskusja)	Projektor multimedialny, komputer. Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia przedmiotowe** (analiza problemowa).	Projektor multimedialny, komputer. Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams

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)
Ćwiczenia	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć; ocena ćwiczeń wykonywanych podczas zajęć) **F3 – Praca pisemna** (przygotowanie referatu lub prezentacji)	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych podczas realizacji ćwiczeń.

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

Symbol efektu	Wykład	Ćwiczenia	
	P2	F2	F3
W_01	x	x	x
U_01	x	x	x
U_02		x	x
K_01		x	x

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

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

Ocena podsumowująca oceny jest sumą ocen formułujących.

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

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

10. Forma zaliczenia zajęć

Zaliczenie z oceną

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

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	45	27
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
Przygotowanie do zaliczenia	5	7
przygotowanie do egzaminu	5	10

Przygotowanie do zajęć	5	8
zapoznanie z literaturą	5	10
Przygotowanie prezentacji / referatu	10	13
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. Cezary Banasiński, Marcin Rojszczak (red.), *Cyberbezpieczeństwo,* Wolters Kluwer Polska, 2020
2. J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin, 2015.
3. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024

Literatura zalecana / fakultatywna:

1. S. Gwoździewicz, K. Tomaszycki (red), *Legal and Social Aspects of Cybersecurity,* Difin SA, Warszawa 2020
2. S. Gwoździewicz, *Problematyka cyberbezpieczeństwa i wzrastającej skali cyberataków, a dostęp do Internetu jak 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, C.H.BECK, Warszawa 2019 (rozdział XIVs.157-168) ISBN 978-83-8158-613-9).
3. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na syst informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz i dr Andrzej Skwarski
data sporządzenia / aktualizacji	10.06.2022 r.
dane kontaktowe (e-mail)	sylwiagwozdziewicz@gmail.com
podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo narodowe
	Poziom studiów	Studia II stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**CYBER.4**

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Przestępczość komputerowa**
Punkty ECTS	**3**
Rodzaj zajęć	**obieralny**
Moduł/specjalizacja	**cyberbezpieczeństwo**
Język, w którym prowadzone są zajęcia	**Polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Gwoździewicz - koordynator specjalności Cyberbezpieczeństwo**

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

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

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych.

4. Cele kształcenia

C1 - 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 - Zdobycie przez studenta umiejętności posługiwania się przepisami prawa krajowego i europejskiego do rozwiązania konkretnych problemów przestępstw komputerowych i 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_W08 K_W11
UMIEJĘTNOŚCI		
U_01	Student potrafi prawidłowo interpretować i wyjaśniać zjawisko przestępczości komputerowej i przestępczości przeciwko ochronie informacji oraz potrafi dobierać środki, metody pracy w celu efektywnego wykonywania pojawiających się zadań zawodowych oraz zagrożeń.	K_U05 K_U09
U_02	Student posługuje się ujęciami teoretycznymi i przepisami prawa krajowego i europejskiego do rozwiązania praktycznych problemów dotyczących przestępstw komputerowych i przeciwko ochronie informacji, wykorzystuje rozwój techniki i narzędzi systemów informatycznych do analizy i oceny tych problemów.	K_U07
KOMPETENCJE SPOŁECZNE		
K_01	Student potrafi współpracować w grupie i przyjmować w niej różne role, a przy tym uzupełnienia i doskonali nabytą wiedzę, umiejętności odnośne zjawiska przestępczości komputerowej i przestępczości przeciwko ochronie informacji.	K_K04 K_K13

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

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Zapoznanie studentów z planem i programem zajęć, celami i efektami uczenia się oraz formą zaliczenia.	0,5	0,5
W2	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.).	5	2,5
W3	Katalog przestępstw komputerowych wg Interpolu i innych agencji i instytucji międzynarodowych. Katalog wg Konwencji o cyberprzestępczości. Współpraca transgraniczna w wykrywaniu cyberprzestępczości.	5	2,5
W4	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).*	6	3
W5	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,*	10	5

	produkowanie i dystrybucja pornografii dziecięcej itp.).		
W6	Prawna ochrona informacji i dóbr osobistych w prawie cywilnym.	3,5	1,5
	Razem liczba godzin wykładów	**30**	**15**

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	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).	5	4
C2	Rozwiązywanie kazusów (prawo karne materialne, orzecznictwo krajowe i europejskie) w zakresie przestępstw przeciwko ochronie informacji.	3	3
C3	Rozwiązywanie kazusów (prawo karne materialne, orzecznictwo krajowe i europejskie) w zakresie przestępstw związanych z użyciem komputera.	3	2
C4	Rozwiązywanie kazusów (prawo karne materialne, orzecznictwo krajowe i europejskie) w zakresie sieci i systemów teleinformatycznych.	3	2
	Razem liczba godzin ćwiczeń	**15**	**12**

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

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	**M1 – Metoda podająca** (objaśnienie) **M2 – Metoda problemowa / metody aktywizujące** (dyskusja)	Projektor multimedialny, komputer Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia przedmiotowe** (analiza problemowa wyroki / kazusów).	Kazusy /wyroki przygotowanie przez wykładowcę. Projektor multimedialny, komputer. Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams

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

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

Forma zajęć	**Ocena formująca (F)**	**Ocena podsumowująca (P)**
Wykład	-	**P2 - zaliczenie** (pisemne w formie testowej)
Ćwiczenia	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć; ocena ćwiczeń wykonywanych podczas zajęć) **F3 – Praca pisemna** (przygotowanie referatu lub prezentacji) **F5 – Ćwiczenia praktyczne** (analiza i	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych podczas realizacji ćwiczeń.

	rozstrzygnięcie stanów faktycznych / rozwiązywanie kazusów, analiza wyroków).	

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

Symbol efektu	Wykład	Ćwiczenia		
	P2	F2	F3	F5
W_01	x		x	x
U_01	x	x	x	x
U_02		x	x	x
K_01		x	x	x

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

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

Ocena podsumowująca oceny jest sumą ocen formułujących.

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

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

10. Forma zaliczenia zajęć

Zaliczenie z oceną

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

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny kontaktowe studenta (w ramach zajęć):		

liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**45**	**27**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
Przygotowanie do zaliczenia	5	7
przygotowanie do egzaminu	5	10
wykonanie ćwiczeń,	5	10
zapoznanie z literaturą	5	5
Przygotowanie prezentacji / referatu	5	8
Przygotowanie do zajęć	5	8
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. M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej,* Wydawnictwo: CeDeWu Warszawa 2016 r.
2. J. Kosiński, *Paradygmaty cyberprzestępczości,* Difin 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.

Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny.*

Literatura zalecana / fakultatywna:

1. 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, ISBN 978-83-8198-782-0, ISBN e-book 978-83-8198-783-7 Seria monografie prawnicze – (rozdział IV w części V s. 223-236)
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. Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim, 2020, s. 175-188, ISBN 978-83-65466-93-8

3. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemowi informatycznym*, Wolters Kluwer 2016.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz i dr Andrzej Skwarski
data sporządzenia / aktualizacji	10.06.2022 r.
dane kontaktowe (e-mail)	sylwiagwozdziewicz@gmail.com
podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo narodowe
	Poziom studiów	Studia II stopnia
	Forma studiów	Studia stacjonarne i niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**CYBER.5**

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Bezpieczeństwo informacji w organizacjach**
Punkty ECTS	**2**
Rodzaj zajęć	**obieralny**
Moduł/specjalizacja	**cyberbezpieczeństwo**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Gwoździewicz - koordynator specjalności Cyberbezpieczeństwo** **dr Juliusz Sikorski – 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/III**	**2**
ćwiczenia	**15/8**	**II/III**	

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych.

4. Cele kształcenia

C1 - Wyposażenie studenta w wiedzę z zakresu nauk o bezpieczeństwie oraz nauk pokrewnych, w szczególności w odniesieniu do istoty administrowania bezpieczeństwem i porządkiem publicznym, systemów bezpieczeństwa oraz funkcjonowania struktur społecznych w sytuacjach kryzysowych w wymiarze lokalnym, regionalnym i globalnym

C2 - przekazanie wiedzy na temat procesów dokonujących się we współczesnym świecie, ich analizy oraz prognozowania zmian i rozwiązań w środowisku bezpieczeństwa

C3 - Zdobycie umiejętności posługiwania się normami i regułami prawnymi w celu rozwiązywania problemów i zadań z zakresu bezpieczeństwa

C4 - Przygotowanie absolwenta do samodzielnej analizy i przetwarzania informacji oraz podejmowania decyzji i kierowania zespołami ludzkimi

C5 - Ukształtowanie postawy społecznej i etycznej opartej na poszanowaniu prawa i wartości moralnych powszechnie akceptowanych w społeczeństwie, w szczególności rozwinięcie wrażliwości na potrzebę zagwarantowania bezpieczeństwa oraz przestrzegania praw i wolności człowieka w sytuacjach kryzysowych

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 pogłębioną wiedzę o współzależnościach między elementami struktury systemu bezpieczeństwa w wymiarze narodowym i międzynarodowym, społecznym i kulturowym	K_W03
W_02	Ma pogłębioną wiedzę na temat analizowania i prognozowania zjawisk i procesów społecznych w sytuacjach zagrożenia bezpieczeństwa	K_W07
UMIEJĘTNOŚCI		
U_01	Analizuje przyczyny, przebieg procesów i zjawisk społecznych, rozwój zagrożeń dla bezpieczeństwa, formułuje własne opinie na ten temat oraz stawia proste hipotezy badawcze i je weryfikuje.	K_U04
U_02	Posługuje się w sposób pogłębiony normami i regułami umożliwiającymi rozwiązanie konkretnie postawionego problemu właściwego dla kierunku bezpieczeństwo.	K_U06
KOMPETENCJE SPOŁECZNE		
K_01	Rozumie potrzebę uczenia się przez całe życie oraz konieczność ciągłego rozwoju osobowego i zawodowego.	K_K02
K_02	Potrafi odpowiednio określić priorytety w realizacji zadań wyznaczonych przez siebie lub inne osoby.	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	I część zajęć (0,5 godz.): Zapoznanie studentów z celem zajęć, efektami kształcenia oraz metodami ich weryfikacji. II część zajęć: Rodzaje zasobów informacyjnych we współczesnych organizacjach.	3	2
W2	Zakres pojęciowy bezpieczeństwa informacyjnego.	3	2
W3	Zagrożenia bezpieczeństwa informacyjnego.	3	2
W4	Standardy i normy bezpieczeństwa informacyjnego.	3	2
W5	Wyzwania bezpieczeństwa informacyjnego.	3	2
	Razem liczba godzin wykładów	**15**	**10**

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	Dokumentacja bezpieczeństwa informacyjnego, aspekt normatywne.	5	2
C2	Dokumentacja bezpieczeństwa informacyjnego, praktyczna analiza przykładów.	6	2
C3	Prezentacje prac pisemnych przygotowanych przez studentów	4	4
	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** (objaśnienie)	Tablica, dokumenty źródłowe i literatura przedmiotu. Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams
Ćwiczenia	**M2 – Metoda problemowa** (metody aktywizujące: rozwiązywanie problemu) **M5 – Metoda praktyczna** (ćwiczenia przedmiotowe – czytanie i analiza tekstu źródłowego, analiza literatury przedmiotu; analiza referatów przedstawionych przez studentów)	Tablica, dokumenty źródłowe i literatura przedmiotu. Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams

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)
Ćwiczenia	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć; ocena ćwiczeń wykonywanych podczas zajęć) **F3 – Praca pisemna** (przygotowanie referatu lub prezentacji) **F4 – Wypowiedź/wystąpienie** (sposób prezentacji prac pisemnych)	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych podczas realizacji ćwiczeń.

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

Symbol efektu	Wykład	Ćwiczenia		
	P2	F2	F3	F4
W_01		x		
W_02	x		x	x
U_01	x	x	x	x
U_02		x	x	x
K_01				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 ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Zaliczenie z oceną

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

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	**na studiach niestacjonarnych**
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	30	18
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
Przygotowanie do zaliczenia	3	4
przygotowanie do egzaminu	3	3
wykonanie ćwiczeń,	3	3
zapoznanie z literaturą	6	10
Konsultacje	2	2
Przygotowanie referatu	3	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. Lidermann K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017.
2. *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Siedlce 2016.

Literatura zalecana / fakultatywna:

1. 1. Hetmański M., *Świat informacji*, Warszaw 2015.
2. Roman W. K., *Podstawy zarządzania informacją*, Toruń 2012.
3. P. Suwaj, S. Gwoździewicz, K. Samulska (red.), *Bezpieczeństwo informacyjne jednostek organizacyjnych. Wybrane problemy*, Wyd. Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim, 2021.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Juliusz Sikorski i dr Andrzej Skwarski
data sporządzenia / aktualizacji	10.06.2022 r.
dane kontaktowe (e-mail)	jsikorski@ajp.edu.pl
podpis	Juliusz Sikorski

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo narodowe
	Poziom studiów	Studia II stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**CYBER.6**

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Transgraniczna ochrona danych osobowych**
Punkty ECTS	**4**
Rodzaj zajęć	**obieralny**
Moduł/specjalizacja	**cyberbezpieczeństwo**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Gwoździewicz - koordynator specjalności Cyberbezpieczeństwo** **dr Sylwia Gwoździewicz - prowadząca zajęcia**

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

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

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych.

4. Cele kształcenia

C1 -Wyposażenie studenta w wiedzę z transgranicznej ochrony danych osobowych.

C2 - Zdobycie przez studenta umiejętności interpretowania i wyjaśniania problemów dotyczących transgranicznej ochrony danych osobowych.

C3 – Zdobycie przez studenta umiejętności posługiwania się przepisami prawa do rozwiązania konkretnych problemów transgranicznej ochrony danych osobowych.

C4 - Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności odnośne transgranicznej ochrony danych osobowych.

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 rozwiązywania problemów prawnych i współzależnościach transgranicznej ochrony danych osobowych w	K_W03 K_W08

	wymiarze społecznym, narodowym, międzynarodowym oraz rozumie wpływ integracji przepisów transgranicznej ochrony danych osobowych na bezpieczeństwo danych osobowych osób fizycznych.	K_W09
UMIEJĘTNOŚCI		
U_01	Student posługuje się w sposób pogłębiony normami i regułami umożliwiającymi rozwiązanie konkretnie postawionego problemu właściwego dla transgranicznej ochrony danych osobowych.	K_U06
U_02	Student potrafi samodzielnie planować i realizować własne uczenie się przez całe życie oraz potrafi ukierunkować innych w tym zakresie, uwzględnia także ryzyko i przewiduje skutki podejmowanych decyzji opierając się na zdobytej wiedzy teoretycznej i empirycznej dotyczącej transgranicznej ochrony danych osobowych.	K_U11 K_U16
KOMPETENCJE SPOŁECZNE		
K_01	Student potrafi współpracować w grupie i przyjmować w niej różne role, a przy tym docenia znaczenie i znajomość prawa w rozwiązywaniu problemów związanych z transgraniczną ochroną danych osobowych.	K_K04 K_K13

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

Lp.	Treści wykładów	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
W1	Zapoznanie studentów z planem i programem zajęć, celami i efektami uczenia się oraz formą zaliczenia.	0,5	0,5
W2	Wprowadzenie do problematyki ochrony danych osobowych w Unii Europejskiej. Idea, założenia i rozwój unijnej regulacji prawnej w odniesieniu do ochrony danych osobowych.	3,5	2,5
W3	Wybrane problemy ogólnego rozporządzenia o ochronie danych osobowych – podstawy ochrony danych osobowych w UE. Transgraniczne przetwarzanie danych osobowych.	3,5	2,5
W4	Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych (ogólna zasada przekazywania; przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony;).	5	3
W5	Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych (przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń; wiążące reguły korporacyjne; przekazywanie lub ujawnianie niedozwolone na mocy prawa UE; wyjątki w szczególnych sytuacjach).	5	3
W6	Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 10 października 2018 r. (umowa międzynarodowa jako prawnie wiążący międzynarodowy akt w obszarze ochrony danych osobowych; zmiany Konwencji ze względu na dynamiczny rozwój nowych technologii, globalizację)	5	2
W7	Kryteria ustalania głównej jednostki organizacyjnej administratora w przypadkach, gdy nie jest to miejsce jego centralnej administracji w UE; przedsiębiorstwa nieposiadające jednostki organizacyjnej w UE.	4,5	2,5
W8	Międzynarodowa współpraca na rzecz ochrony danych osobowych. Szczególny tryb transgranicznego przetwarzania danych osobowych w celu wykrywania i zwalczania przestępstw o charakterze	3	2

	terrorystycznym i innych przestępstw lub przestępstw skarbowych oraz zapobiegania im i ścigania ich sprawców. Umowy międzynarodowye UE z USA, Kanadą, Australią.		
	Razem liczba godzin wykładów	**30**	**18**

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	Analiza wybranych problemów np. na podst. *Ustawy z dnia 16 października 2019 r. o ratyfikacji Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonego w Strasburgu dnia 10 października 2018 r.;*	7,5	4,5
C2	Analiza wybranych problemów np. na podst. *Ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera; opinii Europejskiego Inspektora Ochrony Danych w sprawie wniosków dotyczących decyzji Rady w sprawie zawarcia i podpisania umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera*.	7,5	4,5
C3	Analiza wybranych praktycznych problemów prawno-administracyjnych, jednostek organizacyjnych i osób fizycznych dotyczących transgranicznej ochrony i dostępu do danych osobowych obywateli PCUE (np. ocena dostępu z terytorium państwa trzeciego do danych osobowych zgromadzonych w Unii Europejskiej na podst. *Wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie Lindquist* i inne wyroki).	15	9
	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** (objaśnienie) **M2 – Metoda problemowa / metody aktywizujące** (dyskusja)	Projektor multimedialny, komputer. Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams

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	-	**P1 - Egzamin** (pisemny)
Ćwiczenia	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć; ocena ćwiczeń wykonywanych podczas zajęć) **F3 – Praca pisemna** (przygotowanie referatu/prezentacji) **F5 – Ćwiczenia praktyczne** (analiza i rozstrzygnięcie stanów faktycznych, dyskusje, praca w grupach).	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych podczas realizacji ćwiczeń.

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

Symbol efektu	Wykład	Ćwiczenia		
	P1	F2	F3	F5
W_01	**x**	**x**	**x**	**x**
U_01	**x**	**x**	**x**	**x**
U_02	**x**	**x**		**x**
K_01		**x**	**x**	**x**

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

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

Ocena podsumowująca oceny jest sumą ocen formułujących.

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

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

10. Forma zaliczenia zajęć

Egzamin

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

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	**na studiach niestacjonarnych**
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**60**	**36**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		

przygotowanie do kolokwium zaliczeniowych		
przygotowanie do egzaminu	10	16
wykonanie ćwiczeń,	5	10
zapoznanie z literaturą	10	15
Przygotowanie prezentacji / referatu	10	13
Przygotowanie do zajęć	5	10
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. D. Karwala, *Komercyjne transfery danych osobowych do państw trzecich*, Wolters Kluwer 2018.
2. Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych* oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych.
3. Ustawa z dnia 16 października 2019 r. *o ratyfikacji Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*, sporządzonego w Strasburgu dnia 10 października 2018 r. (Dz.U. poz. 2284).
4. Ustawa z 14 grudnia 2018 r. *o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* (Dz.U. z 2019 r. poz. 125)
5. Ustawy z dnia 9 maja 2018 r. *o przetwarzaniu danych dotyczących przelotu pasażera.*

Literatura zalecana / fakultatywna:

1. 1. M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji,* Wolters Kluwer 2019.
2. S. Gwoździewicz, *Poszanowanie prawnej ochrony danych osobowych i prywatności w cyberprzestrzeni w działaniach Unii Europejskiej i Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej*. Univerzita Mateja Bela V Banskej Bystrici, Právnická Fakulta Katedra Dejín Štátu A Práva, Banská Bystrica 2017 r. (artykuł dostępny w Internecie)
3. S. Gwoździewicz i i in., *Prawo do ochrony danych osobowych w cyberprzestrzeni w dobie rozwoju bankowości internetowej* [w] Technologiczno-społeczne oblicza XXI wieku (pod red.) D. Gałuszka, G.Ptaszek, D. Żuchowska-Skiby, Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie i Wydawnictwo LIBRON – Filip Lohner, ISBN 978-83-65705-09-9, Kraków 2016. (s.391-421) (artykuł dostępny w Internecie).
4. Dyrektywa 2016/680 Parlamentu Europejskiego i Rady (UE) z 27.04.2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady* 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89)

5. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z 27.04.2016 r. *w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania* (Dz.Urz. UE 2016 r. Nr L 119, s. 132).

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz i dr Andrzej Skwarski
data sporządzenia / aktualizacji	10.06.2022 r.
dane kontaktowe (e-mail)	sylwiagwozdziewicz@gmail.com
podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo narodowe
	Poziom studiów	Studia drugiego stopnia
	Forma studiów	Studia stacjonarne/niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**CYBER.7**

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Ochrona cyberprzestrzeni RP w działaniach służb państwowych**
Punkty ECTS	**3**
Rodzaj zajęć	**obieralny**
Moduł/specjalizacja	**cyberbezpieczeństwo**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Gwoździewicz - koordynator specjalności Cyberbezpieczeństwo** **dr Sylwia Gwoździewicz - prowadząca zajęcia**

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

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

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Student przedmiotu Bezpieczeństwo cyberprzestrzeni RP w działaniach służb państwowych posiada wiedzę, umiejętności oraz kompetencje społeczne, które nabył podczas realizacji przedmiotu Zagrożenia bezpieczeństwa w sieciach teleinformacyjnych

4. Cele kształcenia

C1 - Przekazanie wiedzy na temat różnorodnych koncepcji dotyczących struktur społecznych i politycznych oraz rodzajów więzi społecznych, istotnych z punktu widzenia ochrony cyberprzestrzeni RP w działaniach służb państwowych.

C2 - Zdobycie umiejętności dokonywania wyboru i stosowania właściwych dla sytuacji kryzysowych rozwiązań, odpowiedniego doboru środków, narzędzi i metod pracy w celu efektywnego wykonywania zadań w obszarze ochrony cyberprzestrzeni RP w działaniach służb państwowych.

C3 - Zdobycie umiejętności posługiwania się normami i regułami prawnymi w celu rozwiązywania problemów i zadań z zakresu ochrony cyberprzestrzeni RP w działaniach służb państwowych.

C4 - Przygotowanie do twórczego współdziałania i pracy w grupie.

C5 - Uświadomienie potrzeby i rozwinięcie umiejętności uczenia się przez całe życie.

C6 - Ukształtowanie postawy społecznej i etycznej opartej na poszanowaniu prawa i wartości moralnych powszechnie akceptowanych w społeczeństwie, w szczególności rozwinięcie wrażliwości na potrzebę zagwarantowania bezpieczeństwa oraz przestrzegania praw i wolności człowieka w sytuacjach kryzysowych.

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 pogłębioną wiedzę na temat analizowania i prognozowania zjawisk i procesów społecznych ochrony cyberprzestrzeni RP w działaniach służb państwowych.	K_W07
UMIEJĘTNOŚCI		
U_01	Posługuje się w sposób pogłębiony normami i regułami umożliwiającymi rozwiązanie konkretnie postawionego problemu właściwego dla ochrony cyberprzestrzeni RP.	K_U06
U_02	Sprawnie posługuje się wybranymi ujęciami teoretycznymi i wykorzystuje strategie, rozwój techniki i narzędzi systemów informatycznych do analizy i oceny podejmowanych działań praktycznych dla ochrony cyberprzestrzeni RP.	K_U07
KOMPETENCJE SPOŁECZNE		
K_01	Potrafi współpracować w grupie i przyjmować w niej różne role także w sytuacjach kryzysowych w ochronie cyberprzestrzeni RP.	K_K04
K_02	Potrafi samodzielnie i krytycznie uzupełniać wiedzę i umiejętności ochrony cyberprzestrzeni RP w działaniach służb państwowych.	K_K12
K_03	Docenia znaczenie i znajomość prawa w rozwiązywaniu problemów związanych z bezpieczeństwem cyberprzestrzeni RP.	K_K13

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

Lp.	Treści ćwiczeń	Liczba godzin na studiach	
		stacjonarnych	niestacjonarnych
C1	**Zapoznanie studentów z efektami kształcenia, celem przedmiotu, warunkami i kryteriami zaliczenia.** Informacje wprowadzające.	2	2
C2	Podstawowe pojęcia w zakresie cyberprzestrzeni i cyberbezpieczeństwa. Strategie UE i RP w zakresie cyberbezpieczeństwa.	8	5
C3	Strategie i programy ochrony cyberprzestrzeni UE w instytucjach państwowych i agencjach odpowiedzialnych za cyberbezpieczeństwo Współpraca PCUE w zakresie cyberbezpieczeństwa.	8	5
C4	Strategie i programy ochrony cyberprzestrzeni RP w instytucjach państwowych i agencjach odpowiedzialnych za cyberbezpieczeństwo Współpraca krajowa w zakresie cyberbezpieczeństwa.	9	5
C5	Wdrażanie i rozwój systemowego podejścia do cyberbezpieczeństwa w wymiarze społecznym, prawnym, organizacyjnym i teleinformatycznym.	8	5
C6	Wybrane problemy związane z bezpieczeństwem cybernetycznym oraz innych cyberzagrożeń mających wpływ na bezpieczeństwo cyberprzestrzeni RP (referaty/prezentacje)	10	5
	Razem liczba godzin ćwiczeń	**45**	**27**

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

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład	Np. wykład informacyjny	Np. projektor
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (wykład z elementami analizy źródłowej i dyskusji; dyskusja związana z ćwiczeniami; metoda przypadków -case study; pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia przedmiotowe** (analiza źródeł prawa; przegląd form aktywności podmiotów zewnętrznych (np. orzecznictwa, piśmiennictwa, interpretacji organów administracji publicznej); analiza opracowanych referatów /prezentacji przedstawionych przez studentów).	Projektor multimedialny, komputer (analiza problemowa na podst. filmów dokumentalnych i konferencji naukowych). Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams

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		Np. egzamin ustny
Ćwiczenia	**F1 - Sprawdzian** pisemny w formie testowej **F2** – **Obserwacja/aktywność** (ocena ćwiczeń wykonywanych podczas zajęć, w tym np. ocena wygłoszonej prezentacji / referatu). **F3** – **Praca pisemna** (przygotowanie referatu lub prezentacji).	Ocena podsumowująca stanowi sumę ocen formujących.

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

Symbol efektu	Ćwiczenia		
	F1	F2	F3
W_01	**x**		**x**
U_01	**x**		**x**
U_02	**x**		**x**
K_01		**x**	
K_02	**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 ustnego/pisemnego stanowi podstawę zaliczenia wykładu. Skala ocen wg.
R > 91% bardzo dobry (5,0)
R > 81% ÷ 90% plus dobry (4,5)
R > 71% ÷ 80% dobry (4,0)
R > 61% ÷ 70% plus dostateczny (3,5)
R > 50% ÷ 60% dostateczny (3,0)
R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Zaliczenie na ocenę

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

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**45**	**27**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
Przygotowanie do sprawdzianu	5	10
przygotowanie do egzaminu	5	11
wykonanie ćwiczeń,	5	7
zapoznanie z literaturą	8	10
Konsultacje	2	2
Przygotowanie prezentacji/referatu oraz przygotowanie do zajęć	5	8
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. Banasiński C., Ratajczak M. (red.), *Cyberbezpieczeństwo*, Warszawa 2020.
2. Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.
3. Gwoździewicz S., Tomaszycki K, red), *Legal and Social Aspects of Cybersecurity*, Difin SA, Warszawa 2020.
4. Prawodawstwo krajowe (wybrane):

5. - Ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa.* *- Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.*2.
Literatura zalecana / fakultatywna: 1. 1. Gwoździewicz S., *Prawo i organizacja współdziałania instytucji i organów Unii Europejskiej na rzecz walki z cyberprzestępczością* [w:] Suwaj P., Kledzik P., Samulska K., (red.), Współdziałanie w administracji, Wyd. Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim, 2020, s. 175-188. 2. Gwoździewicz S., *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*, Warszawa 2019 (rozdział XIVs.157-168). 3. Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016. 4. Szpor G., Gryszczyńska A. (red.), *Internet. Strategie bezpieczeństwa*, Warszawa 2017.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz i dr Andrzej Skwarski
data sporządzenia / aktualizacji	10.06.2022 r.
dane kontaktowe (e-mail)	sylwiagwozdziewicz@gmail.com
podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo Narodowe
	Poziom studiów	Studia pierwszego stopnia
	Forma studiów	stacjonarna/niestacjonarna
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**CYBER.8.**

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Bezpieczeństwo sieci i systemów informatycznych**
Punkty ECTS	**3**
Rodzaj zajęć	**Specjalnościowy**
Moduł/specjalizacja	**cyber**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Paweł Tomaszewski**

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

Forma zajęć	**Liczba godzin stacjonarne/niestacjonarne**	**Rok studiów/semestr**	**Punkty ECTS** (zgodnie z programem studiów)
ćwiczenia	**45/27**	**II/4**	**3**

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	
K_W1	Ma pogłębioną wiedzę na temat analizowania i prognozowania zjawisk i procesów społecznych w sytuacjach zagrożenia bezpieczeństwa	P7U_W P7S_WG
	UMIEJĘTNOŚCI	

K_U1	Samodzielnie wybiera i stosuje właściwy dla sytuacji kryzysowej i zagrożenia bezpieczeństwa sposób postępowania, potrafi dobierać środki, metody pracy w celu efektywnego wykonywania pojawiających się zadań zawodowych	P7U_U P7S_UU
K_U2	Posługuje się w sposób pogłębiony normami i regułami umożliwiającymi rozwiązanie konkretnie postawionego problemu właściwego dla kierunku bezpieczeństwo	P7U_U P7S_UW
K_U3	Sprawnie posługuje się wybranymi ujęciami teoretycznymi i wykorzystuje strategie, rozwój techniki i narzędzi systemów informatycznych do analizy i oceny podejmowanych działań praktycznych w dziedzinie bezpieczeństwa	P7U_U P7S_UW, P7S_UU
KOMPETENCJE SPOŁECZNE		
K_K1	Rozumie potrzebę uczenia się przez całe życie oraz konieczność ciągłego rozwoju osobowego i zawodowego	P7U_K P7S_KK
K_K2	Potrafi samodzielnie i krytycznie uzupełniać wiedzę i umiejętności, rozszerzone o wymiar interdyscyplinarny	P7U_K P7S_KK

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 programem kształcenia. Standardy i organizacje standaryzacyjne.	1	1
C2	Bezpieczeństwo poczty elektronicznej. Bezpieczeństwo urządzeń mobilnych..	8	5
C3	Bezpieczeństwo sieci bezprzewodowych. Bezpieczeństwo systemów operacyjnych.	8	5
C4	Firewall'e – charakterystyka, typy, implementacje.	7	4
C5	Szyfrowanie – poznanie wybranych programów szyfrujących.	7	4
C6	Projektowanie zabezpieczenia systemu komputerowego.	7	4
C7	Ochrona sieci teleinformatycznych przed narażeniami i terroryzmem elektromagnetycznym	7	4
	Razem liczba godzin wykładów	**45**	**27**

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

Forma zajęć	**Metody dydaktyczne (wybór z listy)**	**Środki dydaktyczne**
Wykład	M-3 Metoda Eksponująca - Pokaz materiału audiowizualnego, pokaz prezentacji multimedialnej.	projektor , komputer
Ćwiczenia	M5 – Metoda praktyczna - Ćwiczenia przedmiotowe przy zastosowaniu oprogramowania i aplikacji.	komputer, telefon komórkowy

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 i wykonywanych zadań w grupach.	P2 – Kolokwium: test sprawdzający wiedzę z całego przedmiotu.
Ćwiczenia	F5 – ćwiczenia praktyczne	P3- aktywność, oceny zdobyte na podstawie ocen cząstkowych

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

Symbol efektu	Wykład		Ćwiczenia		
	P2	P3	F2	F5	
W1	x	x	x		
U_01	x	x	x		
U_02		x	x	x	
K_01	x	x	x		
K_02		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 sumą ocen formułujących.

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

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

10. Forma zaliczenia zajęć

- Egzamin

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

Forma aktywności studenta	Liczba godzin	
	na studiach stacjonarnych	na studiach niestacjonarnych
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	45	27
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do kolokwium zaliczeniowych	8	10
przygotowanie do egzaminu	7	11
przygotowanie do realizacji zajęć laboratoryjnych, wykonanie ćwiczeń,	6	7
zapoznanie z literaturą	5	10
Przygotowanie do sprawdzianu	4	10
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. 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.

Strużak R., *Problemy ochrony sieci teleinformatycznych przed zagrożeniami i terroryzmem elektromagnetycznym*, „Telekomunikacja i techniki informacyjne" 2010, nr 3-4.

4. Kluczewski J., Bezpieczeństwo sieci komputerowych: praktyczne przykłady i ćwiczenia na symulatorze Cisco Packet Tracker, Piekary Śląskie 2019.

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.

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

3. Kluczewski J., Bezpieczeństwo sieci komputerowych: praktyczne przykłady i ćwiczenia na symulatorze Cisco Packet Tracker, Piekary Śląskie 2019.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	Paweł Tomaszewski
data sporządzenia / aktualizacji	10.06.2022 r.
dane kontaktowe (e-mail)	cheerioss@wp.pl
podpis	Paweł Tomaszewski

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo narodowe
	Poziom studiów	Studia II stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**CYBER.9**

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Ochrona kryptograficzna**
Punkty ECTS	**3**
Rodzaj zajęć	**obieralny**
Moduł/specjalizacja	**cyberbezpieczeństwo**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Gwoździewicz - koordynator specjalności Cyberbezpieczeństwo**

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

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

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych.

4. Cele kształcenia

C1 - Wyposażenie studenta w wiedzę z zakresu ochrony kryptograficznej.
C2 -Zdobycie przez studenta umiejętności interpretowania i wyjaśniania problemów z obszaru kryptografii.
C3 - Kształtowanie kompetencji doskonalenia nabytej wiedzy i umiejętności w zakresie kryptografii..

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 dysponuje niezbędną wiedzę na temat analizowania i prognozowania ochrony kryptograficznej w procesach mających związek z bezpieczeństwem sieci i systemów informatycznych oraz potrafi wykorzystać tę wiedzę w praktyce.	K_W13
	UMIEJĘTNOŚCI	
U_01	Student proponuje oryginalne rozwiązania złożonych sytuacji kryzysowych i zagrożeń bezpieczeństwa oraz prognozuje przebieg ich rozwiązania a	K_U09

	także przewiduje skutki planowanych działań w określonych obszarach praktycznych ochrony kryptograficznej.	
U_02	Student sprawnie posługuje się wybranymi ujęciami teoretycznymi i wykorzystuje rozwój techniki i narzędzi systemów informatycznych do analizy i oceny podejmowanych działań praktycznych w dziedzinie ochrony kryptograficznej.	K_U07
KOMPETENCJE SPOŁECZNE		
K_01	Student rozumie potrzebę uczenia się przez całe życie oraz konieczność ciągłego rozwoju osobowego i zawodowego, samodzielnie uzupełnienia i doskonali nabytą wiedzę, umiejętności w zakresie ochrony kryptograficznej, rozszerzone o wymiar interdyscyplinarny.	K_K02 K_K12

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 zajęć, celami i efektami uczenia się oraz formą zaliczenia.	0,5	0,5
C2	Kluczowe pojęcia kryptografii np. bezpieczeństwo obliczeniowe, modele ataków oraz odporność na analizę wsteczną, mocne strony i ograniczenia protokołu TLS stosowanego w bezpiecznych witrynach HTTPS, komputery kwantowe i kryptografia post-kwantowa.	10	6
C3	Funkcja skrótu (ang. hash). Kryptograficzne utajnianie wiadomości. Przykładowe zastosowania kryptografii w teleinformatyce	5	3
C4	. Protokoły komunikacyjne. Ataki na protokoły komunikacyjne. Zastosowania kryptografii w protokołach warstwy aplikacji . Kryptografia symetryczna. Kryptografia asymetryczna.	5	3
C5	Hasło w kryptografii i uwierzytelnianiu. Metody ataków kryptograficznych na hasła.	5	3
C6	Atak siłowy. Atak słownikowy. Odwrócony atak siłowy. Tęczowe tablice.	5	3
C7	Obrona kryptograficzna przed atakami na hasła. Ciąg zaburzający, tzw. sól. Token kryptograficzny. Uwierzytelnianie za pomocą klucza. Infrastruktura klucza publicznego.	5	3
C8	Certyfikat podpisywania. Hierarchia urzędów certyfikacyjnych. Podpis cyfrowy. Znacznik czasu.	5	3
C9	Różne podatności poprzez badanie przykładów kodu i przypadków użycia, sposoby wybierania najlepszego algorytmu lub protokołu.	4,5	2,5
	Razem liczba godzin wykładów	**45**	**27**

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

Forma zajęć	Metody dydaktyczne (wybór z listy)	Środki dydaktyczne
Wykład		
Ćwiczenia	**M1 – Metoda podająca** (objaśnienie) **M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi).	Projektor multimedialny, komputer, oprogramowanie niezbędne do realizacji poszczególnych tematów zajęć.

	M5 - Metoda praktyczna / ćwiczenia przedmiotowe (analiza problemowa i zadania przygotowanane przez prowadzącego dla studentów).	Pomocniczo wykorzystanie systemu do organizacji zajęć zdalnych i kontaktów merytorycznych ze studentami - np. MsTeams

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** **F2 – Obserwacja/aktywność**: (obserwacja poziomu przygotowania do zajęć i realizowanych zadań)	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych podczas realizacji ćwiczeń.

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

Symbol efektu	Ćwiczenia	
	F1	F2
W_01	**x**	**x**
U_01	**x**	**x**
U_02	**x**	**x**
K_01	**x**	**x**

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

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

Ocena podsumowująca oceny jest sumą ocen formułujących.

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

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

R > 50% ÷ 60% dostateczny (3,0) R < 50% niedostateczny (2,0)

10. Forma zaliczenia zajęć

Zaliczenie z oceną

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

Forma aktywności studenta	**Liczba godzin**	
	na studiach stacjonarnych	**na studiach niestacjonarnych**
Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**45**	**27**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do sprawdzianu	5	8
przygotowanie do egzaminu	5	5
przygotowanie do realizacji zajęć laboratoryjnych, wykonanie ćwiczeń,	5	5
zapoznanie z literaturą	5	20
Przygotowanie do zajęć i realizacji wykonywanych zadań	10	10
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. J-P Aumasson, *Nowoczesna kryptografia Praktyczne wprowadzenie do szyfrowania*, Wydawnictwo Naukowe PWN, 2018 2. C. Banasiński, Marcin Rojszczak (red.), *Cyberbezpieczeństwo,* Wolters Kluwer Polska, 2020.
Literatura zalecana / fakultatywna: 1. W. Stallings., *Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji,* Gliv 2012.

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz i dr Andrzej Skwarski
data sporządzenia / aktualizacji	10.06.2022 r.
dane kontaktowe (e-mail)	sylwiagwozdziewicz@gmail.com
podpis	Sylwia Gwoździewicz

	Wydział	Administracji i Bezpieczeństwa Narodowego
	Kierunek	Bezpieczeństwo narodowe
	Poziom studiów	Studia II stopnia
	Forma studiów	Studia stacjonarne / niestacjonarne
	Profil studiów	Praktyczny
Pozycja w planie studiów (lub kod przedmiotu)		**CYBER.10**

KARTA ZAJĘĆ/MODUŁU

1. Informacje ogólne

Nazwa zajęć	**Zarządzanie ryzykiem i audyt cyberbezpieczeństwa**
Punkty ECTS	**4**
Rodzaj zajęć	**obieralny**
Moduł/specjalizacja	**cyberbezpieczeństwo**
Język, w którym prowadzone są zajęcia	**polski**
Rok studiów	**II**
Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia	**dr Sylwia Gwoździewicz - koordynator specjalności Cyberbezpieczeństwo** **dr Sylwia Gwoździewicz - wykłady**

2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze

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

3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć

Brak wymagań wstępnych.

4. Cele kształcenia

C1 - Wyposażenie studenta w wiedzę z zarządzania ryzykiem i audytu cyberbezpieczeństwa

C2 - Zdobycie przez studenta umiejętności wykorzystania w praktyce zdobytej wiedzy w zakresie zarządzania ryzykiem i audytu cyberbezpieczeństwa

C3 - Kształtowanie postawy podejmowania współpracy grupowej a także docenia znaczenie i znajomość wiedzy i prawa w rozwiązywaniu problemów związanych z zarządzaniem ryzykiem i audytem cyberbezpieczeństwa.

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	Studenta ma pogłębioną wiedzę o współzależnościach między elementami zarządzania ryzykiem i audytem cyberbezpieczeństwa w wymiarze narodowym i międzynarodowym oraz społecznym, wykorzystuje odpowiednie modele teoretyczne niezbędnych do zarządzania ryzykiem i	K_W03 K_W12

	audytem cyberbezpieczeństwa.	
UMIEJĘTNOŚCI		
U_01	Student sprawnie posługuje się wybranymi ujęciami teoretycznymi i wykorzystuje strategie, rozwój technik i narzędzi systemów informatycznych do analizy i oceny podejmowanych działań praktycznych dotyczących zarządzania ryzykiem i audytu cyberbezpieczeństwa, proponując przy tym oryginalne rozwiązania i przewidując skutki planowanych działań.	K_U07 K_U09
U_02	Student uwzględnia ryzyko i przewiduje skutki podejmowanych decyzji opierając się na zdobytej wiedzy teoretycznej i empirycznej, umiejętnościach rozumienia analizowania i pogłębionej oceny sytuacji kryzysowych, w zakresie audycie i zarządzania ryzykiem.	K_U11 K_U12
KOMPETENCJE SPOŁECZNE		
K_01	Student potrafi współpracować w grupie i przyjmować w niej różne role a także docenia znaczenie i znajomość prawa w rozwiązywaniu problemów związanych z zarządzaniem ryzykiem i audytem cyberbezpieczeństwa.	K_K04 K_K13

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

Lp.	**Treści wykładów**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
W1	Zapoznanie studentów z planem i programem zajęć, celami i efektami uczenia się oraz formą zaliczenia wykładów i ćwiczeń.	0,5	0,5
W2	Podstawy prawne, z których wynika obowiązek prowadzenia zarządzania ryzykiem. Zarządzanie ryzykiem – pojęcia i rodzaje ryzyka , istota ryzyka i źródła, Podstawy teoretyczne dotyczące ryzyka a niepewności.	10	6,5
W3	Metody zarządzania ryzykiem. Analiza szacowania poziomu ryzyka i stosowanych środków redukcji ryzyka. Uregulowania normy ISO 31000:2018 w procesie oceny ryzyka każdej organizacji. Postępowanie w sytuacji wystąpienia ryzyka i minimalizowanie skutków. Ciągłość działania Systemy wykorzystywane do zarządzania ryzykiem.	5,5	2,5
W4	Systematyzacja aparatu pojęciowego, typologia audytu i jego sprawność. Rodzaje badań audytowych. Planowanie i realizacja audytu.	4,5	2,5
W5	Podstawy prawne, z których wynika obowiązek audytu bezpieczeństwa sieci i systemów informatycznych a podstawowe pojęcia i zagadnienia norm z rodziny ISO 27000. Organizacja bezpieczeństwa informacji wg normy ISO 27001 7 i analiza normy ISO 27001 8.	4,5	2,5
W6	Cel, zakres i kryteria audytu. Role i odpowiedzialność w procesie audytu. Etapy audytu. Proces zbierania i ewidencjonowania dowodów audytowych. Proces przygotowania raportu końcowego. Problemy audytu.	5	4
	Razem liczba godzin wykładów	30	18

Lp.	**Treści ćwiczeń**	**Liczba godzin na studiach**	
		stacjonarnych	**niestacjonarnych**
C1	Praktyczne rozwiązania w zakresie zarządzania ryzykiem – polityka i dokumentacja szacowania ryzyka i przewidywanych sposobów redukcji,	5	3

	raportowanie itp.		
C2	Analiza dokonywana jest na wybranych przykładach np. różnych instytucji z obszaru infrastruktury krytycznej (np. służby zdrowia) i innych przedsiębiorstw i definiowania problematyki dotyczącej cyberbezpieczeństwa.	5	3
C3	Zastosowanie Normy ISO 31000:2018 w procesie oceny ryzyka. Praca grupowa, dyskusje i prezentacje.	5	3
C4	Planowanie i realizacja audytu Planowanie zakresu podmiotowego i przedmiotowego audytu . Planowanie czasu realizacji zadań audytowych. Określenie profilu kompetencji audytorów. Ustalenie istotności w procesie audytu. Ustalenie źródeł dowodów audytu i sposobu prezentacji wyników.	5	3
C5	Analiza wybranych problemów dotyczących kontroli i audytu cyberbezpieczeństwa – analiza bezpieczeństwa sieci i systemów informatycznych, bezpieczeństwa sprzętu, nośników, zbieranie i ewidencjonowania dowodów audytowych.	5	3
C6	Zarządzanie aktywami, ciągłością działania, incydentami w oparciu o załącznik A normy. Przygotowywanie raportu końcowego oraz organizacja bezpieczeństwa informacji wg normy ISO 27001 (dokumentacja, raporty, itp.) Praca grupowa, dyskusje i prezentacje.	5	3
	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** (objaśnienie) **M2 – Metoda problemowa / metody aktywizujące** (dyskusja)	Projektor multimedialny, komputer. Do realizacji zajęć pomocny będzie system do pracy zdalnej ze np. MsTeams
Ćwiczenia	**M2 – Metoda problemowa / metody aktywizujące** (dyskusja związana z ćwiczeniami; pytania i odpowiedzi). **M5 - Metoda praktyczna / ćwiczenia przedmiotowe** (analizy problemowe związane z realizacją ćwiczeń; pytania i odpowiedzi itp.).	Projektor multimedialny, komputer. Do realizacji zajęć pomocny będzie system do pracy zdalnej ze np. MsTeams

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	-	**P1 - Egzamin** (pisemny)
Ćwiczenia	**F2 – Obserwacja/aktywność** (obserwacja poziomu przygotowania do zajęć; ocena ćwiczeń wykonywanych podczas zajęć) **F5 – Ćwiczenia praktyczne** (analiza i rozstrzygnięcie stanów faktycznych, dyskusje,	Ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych podczas realizacji ćwiczeń.

	rozwiązywanie problemów przygotowanych przez prowadzącego, prezentacje wykonywane w grupach na wskazany przez prowadzącego temat).	

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

Symbol efektu	Wykład	Ćwiczenia	
	P1	F2	F5
W_01	**x**	**x**	**x**
U_01	**x**	**x**	**x**
U_02	**x**	**x**	**x**
K_01		**x**	**x**

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

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

Ocena podsumowująca oceny jest sumą ocen formułujących.

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

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

10. Forma zaliczenia zajęć

Egzamin

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

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

Godziny kontaktowe studenta (w ramach zajęć):		
liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**60**	**36**
Praca własna studenta (indywidualna praca studenta związana z zajęciami):		
przygotowanie do egzaminu	10	16
wykonanie ćwiczeń,	10	15
zapoznanie z literaturą	5	10
Przygotowanie do zajęć (w tym zadań wskazanych na ćwiczeniach)	5	10
Przygotowanie prezentacji/referatu	10	13
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. Z. Dobrowolski, *Audyt. Funkcje. Formułowanie ustaleń. Ryzyka*, Wolters Kluwer Polska, 2021
2. J. Sasak, *Zarządzanie ryzykiem w placówkach ochrony zdrowia*, Wolters Kluwer Polska, 2020
3. D. Wróblewski, *Zarządzanie ryzykiem. Przegląd wybranych metodyk. Wydanie rozszerzone (2018).* Wyd. Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego Państwowy Instytut Badawczy, Józefów 2018 / książka do pobrania - https://www.cnbop.pl/pl/wydawnictwa/ksiazki/zarzdzanie-ryzykiem-przegld-wybranych-metodyk-wydanie-rozszerzone_14398
4. Norma PN-EN ISO/IEC 27001:2017
5. Norma PN-EN ISO 31000:2018

Literatura zalecana / fakultatywna:

1. *Poradnik RODO. Podejście oparte na ryzyku cz.1 i cz. 2,* Urzędu Ochrony Danych Osobowych 2018 / Poradniki do pobrania - https://uodo.gov.pl/pl/123/208

13. Informacje dodatkowe

imię i nazwisko sporządzającego	dr Sylwia Gwoździewicz i dr Andrzej Skwarski
data sporządzenia / aktualizacji	10.06.2022 r.
dane kontaktowe (e-mail)	sylwiagwozdziewicz@gmail.com
podpis	Sylwia Gwoździewicz