Załącznik nr 1
do *Programu studiów podyplomowych pn. Cybersecurity – techniczne aspekty cyberbezpieczeństwa,*
stanowiącego załącznik do Uchwały Nr 44/000/2023 Senatu AJP
z dnia 27 czerwca 2023 r.

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Koncepcje i uregulowania prawne w zakresie cyberbezpieczeństwa		
2. Punkty ECTS: 2		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: **polski**
5. Rok studiów: I	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 30**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15** **Ćwiczenia (Ćw):15**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

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

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: Słuchacz zagadnienia z zakresu prawa międzynarodowego i norm odpowiedzialnego postępowania w cyberprzestrzeni, wpływających na prawa i obowiązki państw na płaszczyźnie międzynarodowej.

EPW2: Słuchacz zna zagrożenia dla gospodarki oraz systemów politycznych płynących z nieodpowiedzialnego wykorzystania cyberprzestrzeni przez państwa.

Umiejętności

EPU1: Słuchacz potrafi analizować międzynarodowe akty prawne oraz normy kluczowe z punktu widzenia cyberbezpieczeństwa oraz implementować wynikające z nich obowiązki.

Kompetencje społeczne

EPK1: Słuchacz ma świadomość wagi podejmowania działań na rzecz interesu publicznego

EPK2: Słuchacz ma świadomość odpowiedzialnej realizacji powierzanych zadań

E - Treści programowe oraz literatura

<u>Forma zajęć: wykład</u>	
Wyk1 Państwa jako podmioty prawa międzynarodowego, źródła praw i zobowiązań w prawie międzynarodowym.	**2**
Wyk2 „Cyber normy" jako nowy element regulacji postępowania państw w cyberprzestrzeni pomiędzy „klasycznymi" normami prawnomiędzynarodowymi a soft law.	**2**
Wyk3 Naruszenie bezpieczeństwa informacyjnego systemów komputerowych w świetle konkretnych norm prawa międzynarodowego regulujące odpowiedzialność międzynarodową państwa za działania indywidualnych hakerów i grup hakerskich. (Zasady poszanowania suwerenności terytorialnej. Zakaz interwencji w sprawy wewnętrzne. Zakaz użycia siły. Nakaz przeciwdziałania wykorzystaniu własnego	

terytorium do czynności szkodliwych dla drugiego państwa (zasada dobrego sąsiedztwa)).	**5**
Wyk4 Prywatność w sieci w ujęciu przepisów prawa.	**2**
Wyk5 Rozwój złośliwego oprogramowania ransomware jako nowy wymiar cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków.	**2**
Wyk6 System dozoru elektronicznego w Polsce.	**2**
Razem liczba godzin wykładów	**15**
<u>Ćwiczenia:</u>	
Ćw1 Analiza cyberoperacji: Cyberoperacja przeciwko irańskiej instalacji nuklearnej Natanz za wykorzystaniem robaka Stuxnet	**3**
Ćw2 Analiza cyberoperacji: Wirusy Flame, Wiper i Shamoon	**2**
Ćw3 Analiza cyberoperacji: Cyberoperacje przeciwko Ukrainie	**2**
Ćw4 Analiza cyberoperacji: Cyberataki za wykorzystaniem ransomware WannaCry oraz NotPetya	**2**
Ćw5 Analiza cyberoperacji: Ingerencja w wybory prezydenckie w USA. Amerykańskie cyberoperacje przeciwko ISIS oraz przeciwko Rosji i Chinom w oparciu o nową doktrynę Departamentu Obrony USA	**4**
	2
Razem liczba godzin ćwiczeń	**15**
Ogółem liczba godzin przedmiotu:	**30**

Literatura przedmiotu

Literatura obowiązkowa:

1. Gwoździewicz S., Tomaszycki K., Prawne I społeczne aspekty cyberbezpieczeństwa, Wydaw. Międzynarodowy Instytut Innowacji "Nauka-Edukacje-Rozwój", Warszawa 2017.
2. Roguski P., Użycie siły w cyberprzestrzeni: "cyberwojna" jako wyzwanie dla systemu Narodów Zjednoczonych w XXI w., System Narodów Zjednoczonych z polskiej perspektywy, 2017. – S. 401-410.
3. Roguski P., Overcoming the damage of disinformation, New Eastern Europe, 2019, Public intellectuals. What is their place, role and responsibility today? no. 1 (35), p. 69-76.

Literatura zalecana / fakultatywna:

1. Tsagourias N., Buchan R. (red.), Research Handbook on International Law and Cyberspace, Edward Elgar 2017;
2. Schmitt M., Vihul L. (red.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press 2017;
3. Ziolkowski K. (red.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, NATO CCDCoE Publications 2012.

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się			
Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**		
	Wykład	Ćwiczenia	
	F1	F2	F5
EPW1	x		X
EPW2	x		X
EPU1		x	X
EPK1		x	X
EPK2	x	x	X

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

H. Nakład pracy studenta	
Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	30
Czytanie literatury	5
Przygotowanie do ćwiczeń	10
Przygotowanie do zaliczenia	5
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe	
Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Udostępnianie informacji publicznej		
2. Punkty ECTS: 1		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 15**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza(CW): Słuchacz zna i rozumie podstawowe pojęcia określone w ustawie o dostępie do informacji publicznej, a także związanych z ochroną danych osobowych oraz zasad funkcjonowania podstawowych instytucji w przedmiotowym zakresie.

Umiejętności (CU): Słuchacz potrafi napisać wniosek o udostępnienie informacji publicznej, uzyskać informacje z Biuletynu Informacji Publicznej

Kompetencje społeczne (CK): Słuchacz ma świadomość wagi podejmowania działań na rzecz interesu publicznego oraz odpowiedzialnej realizacji powierzanych zadań

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: Słuchacz zna i rozumie podstawowe pojęcia z zakresu dostępu do informacji publicznej, działania polskiego systemu w zakresie dostępu do informacji publicznej.

EPW2: Słuchacz rozumie znaczenie wiedzy z zakresu dostępu do informacji publicznej w funkcjonowaniu współczesnego państwa i społeczeństwa.

Umiejętności

EPU1: Słuchacz potrafi napisać wniosek o udostępnienie informacji publicznej, uzyskać informacje z Biuletynu Informacji Publicznej

Kompetencje społeczne

EPK1: Słuchacz ma świadomość wagi podejmowania działań na rzecz interesu publicznego

EPK2: Słuchacz ma świadomość odpowiedzialnej realizacji powierzanych zadań

E - Treści programowe oraz literatura

Forma zajęć: wykład **Wyk1** Informacja publiczna (Pojęcie informacji publicznej i informacji przetworzonej w ustawie o dostępie do informacji publicznej. Sposoby regulacji zakresu przedmiotowego ustaw normujących zasady dostępu do informacji o wykonywaniu zadań administracji publicznej na świecie). Generalna klauzula dostępu do informacji publicznej. Katalog podmiotów zobowiązanych do udostępniania informacji publicznej i katalog podmiotów uprawnionych do uzyskania tej informacji. **Wyk2** Granice prawa do informacji publicznej (Sposób regulacji granic prawa do informacji w	**5**

ustawodawstwie europejskim i ustawach wybranych krajów europejskich i pozaeuropejskich. Granice prawa do informacji w Konstytucji RP. Granice prawa do informacji wprowadzone ustawą o dostępie do informacji publicznej). Kontrola administracyjna i sądowa realizacji prawa dostępu do informacji publicznej (Modele kontroli administracyjnej. Kontrola administracyjna w ustawie o dostępie do informacji publicznej. Kontrola sądowa prawa do informacji publicznej).	
Wyk3 Tryb i formy udostępniania informacji publicznej na gruncie ustawy o dostępie do informacji publicznej (Katalog form udostępnienia informacji publicznej. Zasady dostępu do dokumentu urzędowego. Zasady dostępu do informacji przetworzonej. Biuletyn Informacji Publicznej. Prawo uczestnictwa w posiedzeniach organów kolegialnych pochodzących z powszechnych wyborów. Dostęp do informacji publicznej na wniosek).	**5**
Razem liczba godzin wykładów	**5** **15**
Ogółem liczba godzin przedmiotu:	**15**

Literatura przedmiotu

Literatura obowiązkowa:

1. P. Szustakiewicz (red.), Dostęp do informacji publicznej, Wydawnictwo C. H. Beck, Warszawa 2014.
2. P.Sitniewski, Dostęp do informacji publicznej. Pytania i odpowiedzi, Lex a Wolters Cluwer business, Warszawa 2014.
3. J.Taczkowska-Olszewska, Dostęp do informacji publicznej w polskim systemie prawnym, Wydawnictwo C. H. Beck, Warszawa 2014.
4.

Literatura uzupełniająca/fakultatywna:

1. A, Dmochowska, M. Zadrożny, Unijna reforma ochrony danych osobowych. Analiza zmian, wyd. C. H. Beck, Warszawa 2016.
2. Ogólne rozporządzenie o ochronie danych. Podręczny zbiór przepisów o ochronie danych osobowych, zestawień, schematów oraz wzorów rejestru czynności przetwarzania, pod red. G. Sibiga, K. Syska, wyd. C. H. Beck, Warszawa 2017.

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**
	Wykład
	F1
EPW1	x
EPW2	x
EPU1	x
EPK1	x
EPK2	X

G.4. Forma i warunki zaliczenia przedmiotu:

Zaliczenie z oceną	
H. Nakład pracy studenta	
Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	15
Czytanie literatury	5
Przygotowanie do zaliczenia	5
Suma godzin:	**25**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**1**
I – Informacje dodatkowe	
Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Ochrona informacji niejawnych		
2. Punkty ECTS: 2		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 30**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15** **Laboratorium (Lab):15**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza (CW): Słuchacz zna i rozumie zasady ochrony informacji niejawnych
Umiejętności (CU): Słuchacz ma umiejętność stosowania procedur określających nadawanie i kontrolowanie/weryfikację uprawnień dostępu do informacji niejawnych, a także procedur ochrony informacji niejawnych w ramach ich przetwarzania, obiegu, dystrybucji/transportu.
Kompetencje społeczne (CK): Słuchacz ma świadomość wagi podejmowania działań na rzecz interesu publicznego oraz odpowiedzialnej realizacji powierzanych zadań

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: Słuchacz zna system ochrony informacji kwalifikowanych jako niejawne, uregulowania prawne w tym zakresie.

EPW2: Słuchacz zna problematykę informacji i jej znaczenie we współczesnym świecie oraz bezpieczeństwo informacyjne państwa.

Umiejętności

EPU1: Słuchacz ma umiejętność stosowania procedur stanowienia i oznaczania informacji jako niejawnych, uwzględniając poziomy i rodzaje zagrożeń dla bezpieczeństwa państwa oraz ogniwa instytucjonalne delegowane do tych zadań.

EPU2: Słuchacz ma umiejętność zapobiegania nieuprawnionemu ujawnianiu materiałów niejawnych.

Kompetencje społeczne

EPK1: Słuchacz ma świadomość konieczności poszerzania swojej wiedzy i umiejętności

EPK2: Słuchacz ma świadomość odpowiedzialnej realizacji powierzanych zadań

E - Treści programowe oraz literatura

<u>Forma zajęć: wykład</u> **Wyk1** Pojęcie informacji i jej znaczenie w czasach współczesnych. Ustawa o ochronie informacji niejawnych jako podstawa prawna systemu zabiegów o zapewnienie tajności wybranym kategoriom informacji i związane z nią inne akty prawne.	**3**
Wyk2 Kategoria informacji niejawnych, ich klasyfikacja oraz sposoby oznaczania w RP. Bezpieczeństwo informacji niejawnych jako element systemu bezpieczeństwa państwa.	**3**
Wyk3 Rodzaje zagrożeń dla informacji prawnie chronionych. Wybrane elementy systemu ochrony	

informacji niejawnych w RP. **Wyk4** Postępowanie sprawdzające w zakresie dostępu do informacji niejawnych w tym zwykłe, poszerzone. **Wyk5** Instrumenty ochrony informacji niejawnych: kancelarie tajne, kontrola obiegu dokumentów, ochrona materiałów niejawnych w trakcie ich transportowania (przenoszenia, przewożenia). **Razem liczba godzin wykładów**	**3** **3** **15**
Forma zajęć: laboratorium: **Lab1** Zasady klasyfikowania informacji niejawnych - przykłady. **Lab2** Nadawanie materiałom klauzul tajności - przykłady. **Lab3** Identyfikowanie zagrożeń dla informacji prawnie chronionych. **Lab4** Postępowanie sprawdzające w sprawie dostępu do informacji niejawnych – możliwe sytuacje. **Lab5** Stosowanie instrumentów ochrony informacji niejawnych. **Razem liczba godzin ćwiczeń**	 **3** **3** **3** **3** **3** **15**
Ogółem liczba godzin przedmiotu:	**30**

Literatura przedmiotu

Literatura obowiązkowa:

1. Liderman K., Bezpieczeństwo informacyjne. Nowe wyzwania. PWN, Warszawa 2017.
2. Stankowska L., Ustawa o ochronie informacji niejawnych. Komentarz, LexisNexis Polska, Warszawa 2014.
3. Iwaszko B., Ochrona informacji w praktyce, Presscom, Wrocław 2012.
4. Thiem P., Instrukcja postępowania z materiałami niejawnymi z komentarzem, ODDK, Gdańsk 2012.
5. Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010.
6. Rozporządzenie Prezesa Rady Miniostróa. w sprawie nadawania, przyjmowania, przewozenia, wydawania i ochrony materiałów zawierajacych infromacje nijawne z dnia 7 grudnia 2011 r.
7. Rozporządzenie Prezesa rady Min istróa. w sprawie organizacji I funkcjonowania kancelarii tajnych oraz sposobu I trybu przetwarzania informacji niejawnych z dnia 7 grudnia 2011 r.

Literatura zalecana/fakultatywna:

1. Kwieciński M. (red.), Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane, Kraków 2010.
2. Denning D. E., Wojna informacyjna i bezpieczeństwa informacji, WNT, Warszawa 2002.
3. Pipkin D., Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa, WNT, Warszawa 2002.

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**		
	Wykład	Laboratoria	
	F1	F2	F5
EPW1	x		X
EPW2	x		X
EPU1		x	X
EPU2		x	X
EPK1		x	X
EPK2	x	x	X

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

H. Nakład pracy studenta	
Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	30
Czytanie literatury	5
Przygotowanie do laboratoriów	10
Przygotowanie do zaliczenia	5
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe	
Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Cyberprzestępczość		
2. Punkty ECTS: 3		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 45**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15** **Laboratoria (Lab):30**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza (CW): Słuchacz zna i rozumie pojęcia w zakresie europejskiego i krajowego systemu cyberbezpieczeństwa, identyfikacji współczesnych zagrożeń systemów teleinformatycznych oraz stosowania odpowiednich zabezpieczeń.
Umiejętności (CU): Słuchacz ma pogłębione umiejętności w zakresie europejskiego i krajowego systemu cyberbezpieczeństwa oraz identyfikacji współczesnych zagrożeń systemów teleinformatycznych i stosowania odpowiednich zabezpieczeń.
Kompetencje społeczne (CK): Słuchacz rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze cyberzagrożeń.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: europejski i krajowy system cyberbezpieczeństwa, organizację krajowego systemu cyberbezpieczeństwa.

EPW2: prawne możliwości ścigania cyberprzestepstw.

Umiejętności

EPU1: rozpoznać i przeciwdziałać zagrożeniom w cyberprzestrzeni, wskazuje podstawowe kierunki rozwoju cyberprzestępczości.

Kompetencje społeczne

EPK1: świadomość konieczności podnoszenia kwalifikacji w zakresie cyberzagorżeń

E - Treści programowe oraz literatura

Forma zajęć: wykład	
Wyk1 Cyberbezpieczeństwo państwa. Europejski i krajowy system cyberbezpieczeństwa (Podstawy ustrojowe europejskiego cyberbezpieczeństwa. Dyrek-tywa NIS. Organizacja krajowego systemu cyberbezpieczeństwa. Doktryna i strategia cyberbezpieczeństwa RP na tle innych krajów).	**3**
Wyk2 Przedmioty ochrony i zagrożenia systemów informatycznych.	**3**
Wyk3 Cyberprzestępstwa (Phishing. Kradzież tożsamości. Oszustwo telekomunikacyjne. Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych).	**6**
Wyk4 Charakterystyka cyberprzestępczości w Polsce (Współczesne trendy i mody w zakresie cyberprzestępczości. Nowy wymiar Cyberbezpieczeństwa. Profilaktyka w zakresie cyberprzestępczości).	**3**

Razem liczba godzin wykładów	**15**
Forma zajęć: laboratorium	
Lab1 Instalacja wirtualnej maszyny CyberOps Workstation (Studia przypadków dotyczące cyberbezpieczeństwa, poznawanie szczegółów ataków, wizualizacja czarnych kapeluszy, jak zostać obrońcą)	**3**
Lab2 Eksploracja procesów, wątków, uchwytów i rejestru systemu Windows (Tworzenie kont użytkowników, korzystanie z Windows PowerShell, menedżer zadań Windows, monitoruj i zarządzaj zasobami systemowymi w systemie Windows)	**3**
Lab3 Praca z plikami tekstowymi w CLI (Zapoznanie się z powłoką Linuksa, Serwery Linux, lokalizowanie plików dziennika, poruszanie się po systemie plików Linux i ustawieniach uprawnień, śledzenie trasy)	**2**
Lab4 Wprowadzenie do Wireshark (Używanie Wireshark do badania ramek Ethernet, używanie Wireshark do obserwacji trójstronnego uzgadniania TCP)	**2**
Lab5 Odkrywanie Nmap, używanie programu Wireshark do badania przechwycenia DNS przez UDP, używanie programu Wireshark do badania przechwytywania TCP i UDP, używanie Wireshark do badania HTTP i HTTPS.	**2**
Lab6 Packet Tracer (Demonstracja ACL, identyfikacja przepływu pakietów)	**2**
Lab7 Anatomia złośliwego oprogramowania, inżynieria społeczna	**2**
Lab8 Aktywność klasowa – co się dzieje (Badanie ruchu DNS, atakowanie bazy danych mySQL, odczytywanie dzienników serwera, Packet Tracer – rejestrowanie aktywności sieci)	**2**
Lab9 Szyfrowanie i odszyfrowywanie danych za pomocą narzędzia hakerskiego (Badanie Telnet i SSH w Wireshark, haszowanie rzeczy, magazyny urzędów certyfikacji)	**2**
Lab10 Konfiguracja środowiska z wieloma maszynami wirtualnymi (Packet Tracer – poznaj implementację NetFlow, Packet Tracer – logowanie z wielu źródeł)	**2**
Lab11 Zasady Snort i zapory, konwersja danych do formatu uniwersalnego, samouczek dotyczący wyrażeń regularnych	**2**
Lab12 Wyodrębnij plik wykonywalny z PCAP, interpretacja danych HTTP i DNS w celu wyizolowania podmiotu stanowiącego zagrożenie	**2**
Lab13 Izolowanie zaatakowanego hosta za pomocą 5-krotnego	**2**
Lab14 Obsługa incydentów	**2**
Razem liczba godzin laboratorium	**30**
Ogółem liczba godzin przedmiotu:	**45**

Literatura przedmiotu

Literatura obowiązkowa:

1. Materiały na platformie netacad.com kurs Cisco Certified CyberOps 2020.
2. C. Banasiński, M. Rojszczak, Cyberbezpieczeństwo , Wolters Kluwer Polska Sp. z o.o., 2020

Literatura zalecana / fakultatywna:

1. O. Santos, Cisco Cyberops Associate Cbrops 200-201 Official Cert Guide, CISCO, 2020
2. G. D. Singh, Cisco Certified CyberOps Associate 200-201 Certification Guide, Packt Publishing Limited, 2021

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

się.	
Wykłady:	
F1 – Sprawdzian (ustny lub pisemny)	Ocena podsumowująca powstała na podstawie ocen formułujących
Laboratorium:	
F2 - Obserwacja/aktywność (podczas realizacji ćwiczeń wykonywanych podczas zajęć) F5 - Ćwiczenia praktyczne (ocena ćwiczeń wykonywanych podczas zajęć)	

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**		
	Wykład	Laboratorium	
	F1	F2	F5
EPW1	x		X
EPW2	x		X
EPU1		x	X
EPK2	x	x	X

G.4. Forma i warunki zaliczenia przedmiotu:

egzamin z oceną

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	45
Czytanie literatury	5
Przygotowanie do laboratoriów	15
Przygotowanie do egzaminu	10
Suma godzin:	**75**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**3**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Podstawy technologii sieci i intersieci		
2. Punkty ECTS: 3		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 45**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15** **Laboratorium (Lab): 30**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza (CW): Słuchacz zna zagadnienia dotyczące budowy topologii sieciowych i intersieciowych z wykorzystaniem technologii przewodowej Ethernet oraz wybrane mechanizmy i protokoły implementowane w urządzeniach sieciowych Ethernet w warstwie II oraz III modelu OSI

Umiejętności (CU): Słuchacz ma umiejętność zarządzania urządzeniami sieciowymi tj. przełącznikami i routerami, budowania topologii sieciowych i intersieciowych, a także w tym wdrażania mechanizmów routingu oraz implementowania mechanizmów protokołu IEEE 802.1q w kontekście bezpieczeństwa sieciowego

Kompetencje społeczne (CK): Słuchacz rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze sieci komputerowych

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: zasady budowy podstawowych topologii oraz mechanizmy funkcjonowania sieci i intersieci na poziomie warstwy II i III

EPW2: mechanizmy wybranych protokołów bezpieczeństwa sieciowego

Umiejętności

EPU1: w zakresie zaawansowanym zarządzać urządzeniami sieciowymi tj. przełącznikami i routerami

EPU2: zbudować topologię sieciową i intersieciową, a także w tym wdrożyć mechanizmy routingu

EPU3: potrafi zaimplementować mechanizmy protokołu IEEE 802.1q w kontekście bezpieczeństwa sieciowego

Kompetencje społeczne

EPK1: rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze sieci komputerowych

E - Treści programowe oraz literatura

<u>Forma zajęć: wykład</u>	
Wyk1 Wybrane aspekty warstwy fizycznej technologii przewodowej Ethernet. Elementy systemów okablowania strukturalnego.	**3**
Wyk2 Budowa ramki Ethernet, charakterystyka parametrów nagłówka ramki. Wykorzystanie analizatora sieciowego do badania nagłówka. Budowa adresów podwarstwy MAC.	**3**
Wyk3 Przełączanie w warstwie II, zasada działania przełączników Ethernet, warstwy II. Algorytmy i	

tabele przełączania - wpisy statyczne i dynamiczne.	**3**
Wyk4 Adresowanie IP v4 oraz IPv6, interfejsy IP i ich rola w komunikacji sieciowej i intersieciowej. Podstawy routingu IP, routing statyczny i dynamiczny (RIP, OSPF).	**3**
Wyk5 Mechanizmy protokołu IEEE 802.1q - elementy bezpiecznej infrastruktury sieciowej z wykorzystaniem technologii sieci wirtualnych.	**3**
Razem liczba godzin wykładów	**15**
Forma zajęć: laboratorium	
Lab1 Media i urządzenia transmisyjne w sieciach LAN, standard Ethernet, topologie sieci, przygotowanie okablowania strukturalnego dla Ethernetu w oparciu o normę TIA/EIA-568-B, elementy instalatorstwa światłowodowego – praktyczne zajęcia instalatorskie.	**5**
Lab2 Zarządzanie urządzeniami sieciowymi na przykładzie systemu operacyjnego CISCO IOS	**5**
Lab3 Idea kapsułkowania pakietów, wykorzystanie analizatora sieciowego *wireshark* do badania nagłówków ramki Ethernet.	**5**
Lab4 Zasady adresowania w sieciach IPv4 i IPv6; obliczanie puli adresowych dla przykładowych rozwiązań sieciowych.	**5**
Lab5 Wdrażanie mechanizmów routingu statycznego i dynamicznego w intersieciach IPv4 oraz IPv4 dla przykładowych topologii.	**5**
Lab6 Wdrażanie technologii sieci wirtualnych VLAN. Rola protokołu VTP. Routing między sieciami VLAN.	**5**
Razem liczba godzin laboratorium	**30**
Ogółem liczba godzin przedmiotu:	**45**

Literatura przedmiotu

Literatura obowiązkowa:

1. Józefiok A.: CCNA 200-301. *Zostań administratorem sieci komputerowych CISCO*, wyd. Helion 2020r.
2. Banks E., White R.: *Sieci komputerowe. Najczęstsze problemy i ich rozwiązania*, wyd. Helion 2019r.
3. Empson S.: CCNA: pełny przegląd poleceń, Akademia sieci Cisco, PWN 2009r.

Literatura zalecana / fakultatywna:

1. oficjalny serwis: *www.cisco.com*
2. serwis internetowy: *www.computerworld.pl*

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty	**Forma zajęć / Metoda oceniania**

przedmiotowe	Wykład	Laboratorium	
	F1	F2	F5
EPW1	x		X
EPW2	x		X
EPU1		x	X
EPK1		x	X
EPK3		x	x
EPK2	x	x	X

G.4. Forma i warunki zaliczenia przedmiotu:	
Zaliczenie z oceną	
H. Nakład pracy studenta	
Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	45
Czytanie literatury	5
Przygotowanie do laboratorium	15
Przygotowanie do zaliczenia	10
Suma godzin:	**75**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**3**

I – Informacje dodatkowe	
Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Organizacja i zarządzanie bezpieczeństwem		
2. Punkty ECTS: 3		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 45**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15** **Laboratorium (Lab): 30**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza (CW): Słuchacz zna i rozumie teorie i techniki organizacji i zarządzania bezpieczeństwem, istotę i funkcje zarządzania publicznego traktowanego jako społeczny system funkcjonujący według określonego porządku, tworzącego złożone i dynamiczne struktury społeczne.
Umiejętności (CU): Słuchacz ma umiejętność organizowania i zarządzania systemami bezpieczeństwa
Kompetencje społeczne (CK): Słuchacz rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: pojęcia z zakresu obejmującego przetwarzanie informacji, architekturę i organizację systemów komputerowych, bezpieczeństwo systemów komputerowych, budowę sieci i aplikacji sieciowych

Umiejętności

EPU1: opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania

EPU2: ocenić przydatność rutynowych metod i narzędzi służących do rozwiązywania prostych zadań inżynierskich, typowych dla wybranego zadania oraz wybierać i stosować właściwe metody i narzędzia

Kompetencje społeczne

EPK1: rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze sieci komputerowych

E - Treści programowe oraz literatura

Forma zajęć: wykład	
Wyk1 Możliwości zarządzania siecią. Najpopularniejsze rozwiązania i oprogramowanie dedykowane do monitoringu, zarządzania i raportowania.	**3**
Wyk2 Konfiguracja infrastruktury sieciowej w ujęciu zarządzania. Perspektywa możliwości zarządzania programu Zentyl.	**3**
Wyk3 Projektowanie i wdrażanie sieci o wysokiej dostępności. Rozwiązania VPN i pulpitu zdalnego. Zarządzanie siecią z perspektywy cyber nomada.	**3**
Wyk4 Projektowanie sieci rozproszonych i zarządzanie poprzez dedykowane oprogramowanie Grafana.	

Zarządzanie i monitorowanie wydajności sieci w perspektywie programu Zabbix. **Wyk5** Implementacja i konfiguracja bezpieczeństwa sieciowego. Identyfikacja zagrożeń, analiza pracy i ruchu z wykorzystaniem OpenNMS. Analiza wymagań i projektowanie sieci komputerowej dla firm. **Razem liczba godzin wykładów**	**3** **3** **15**
Forma zajęć: laboratorium: **Lab1** Wprowadzenie do oprogramowania Zentyal, instalacja, przedstawienie funkcji, konfiguracja wstępna. Zarządzanie usługami za pomocą Zentyal. **Lab2** Instalacji i wdrożenie aplikacji Zabbix, monitoring i analiza sieci z użyciem zabixxa. Rejstracja zasobów i sygnałowanie awarii z urzyciem narzędzia Zabbix. **Lab3** Wprowadzenie do zarządzania siecią z użyciem OpenNMS. Konfiguracja i monitorowanie sieciowych urządzeń. **Lab4** Tworzenie własnych skryptów i rozszerzeń w OpenNMS. **Lab5** Tworzenie interaktywnych i spersonalizowanych paneli w OpenNMS. **Razem liczba godzin ćwiczeń**	 **6** **6** **6** **6** **6** **30**
Ogółem liczba godzin przedmiotu:	**45**

Literatura przedmiotu

Literatura obowiązkowa:

1. Rob VandenBrink, Linux i obsługa sieci dla profesjonalistów. Konfiguracja i stosowanie bezpiecznych usług sieciowych.
2. Adam Józefiok, CCNA 200-301. Zostań administratorem sieci komputerowych Cisco, Helion, Gliwice 2020
3. Adam Józefiok, CCNA 200-125. Zostań administratorem sieci, Helion, Gliwice 2017
4. James Kurose, Keith Ross, Sieci komputerowe. Ujęcie całościowe. Wydanie VII

Literatura zalecana / fakultatywna:

1.Nathan Liefting, Brian van Baekel, Dmitry Lambert, Zabbix 6 IT Infrastructure Monitoring Cookbook - Second Edition, Packt Publishing, 2023.
2. Prince Kevin Nyam A Ngon, Zentyal adventure, OmniScriptum 2023.

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**		
	Wykład	Laboratorium	
	F1	F2	F5

EPW1	x		X
EPU1		x	X
EPU2		x	X
EPK1		x	X

G.4. Forma i warunki zaliczenia przedmiotu:	
egzamin z oceną	
H. Nakład pracy studenta	
Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	45
Czytanie literatury	5
Przygotowanie do laboratorium	15
Przygotowanie do egzaminu	10
Suma godzin:	**75**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**3**

I – Informacje dodatkowe	
Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Seminarium		
2. Punkty ECTS: 2		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 1,2**	**7. Liczba godzin ogółem: 30**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Seminarium (Sem): I semestr 15, II semestr 15**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

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

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: zna metody, narzędzia i techniki wykorzystywane do rozpoznawania i zwalczania cyberzagrożeń

Umiejętności

EPU1: wykorzystuje metody, narzędzia i techniki do rozpoznawania zagrożeń, obsługuje incydenty bezpieczeństwa w oparciu o systemy teleinformatyczne oraz sporządza raporty

Kompetencje społeczne

EPK1: rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze przeciwdziałania cyberzagrożeniom

E - Treści programowe oraz literatura

Forma zajęć: seminarium	
Semestr I	
Sem1 Podstawowe reguły dotyczące pisania prac dyplomowych. Opracowanie tematów i zdefiniowanie zadania oraz harmonogramu czynności pracy dyplomowej.	**4**
Sem2 Badanie literatury przedmiotu, prezentacje z badań literaturowych. Opracowanie wniosków z badań literaturowych.	**4**
Sem3 Planowanie eksperymentów dla potrzeb zadania.	**4**
Sem4 Realizacja poszczególnych etapów zadania. Opracowanie wyników eksperymentu dla potrzeb zadania. Modelowanie procesów i systemów dla potrzeb zadania. Symulacja procesów i systemów. Elementy zadania inżynierskiego. Analiza. Specyfikacja. Projekt. Wdrożenie. Testowanie.	**3**
Razem godzin seminarium semestr I	**15**
Semestr II	

Sem1 Realizacja poszczególnych etapów zadania. Opracowanie wyników eksperymentu dla potrzeb zadania. Modelowanie procesów i systemów dla potrzeb zadania. Symulacja procesów i systemów. Elementy zadania inżynierskiego. Analiza. Specyfikacja. Projekt. Wdrożenie. Testowanie.	**10**
Sem2 Prezentacja głównych wniosków. Analiza najważniejszych problemów metodologicznych badań.	**2**
Sem3 Przygotowanie do obrony pracy dyplomowej. Przygotowanie prezentacji pracy dyplomowej	**3**
Razem liczba godzin seminarium semestr II	**15**
Ogółem liczba godzin przedmiotu:	**30**

Literatura przedmiotu

Literatura obowiązkowa:

1. J. Biernat, *Profesjonalne przygotowanie publikacji,* Instytut Cybernetyki Technicznej Politechniki Wrocławskiej, Wrocław 2003
2. K. S. Berezowski, *Profesjonalne przygotowanie dokumentów technicznych i naukowych,* Politechnika Wrocławska, Wrocław 2006.
3. Z. Knecht, Metody uczenia się i zasady pisania prac dyplomowych: poradnik jak się uczyć, jak pisać pracę dyplomową, Wyższa Szkoła Zarządzania EDYKACJA, Wrocław, 1999.
4. J. Majchrzak, T. Mendel, Metodyka pisania prac magisterskich i dyplomowych: poradnik pisania prac promocyjnych oraz innych opracowań naukowych wraz z przygotowaniem ich do obrony lub publikacji, Wyd. 2 popr., Akademia Ekonomiczna w Poznaniu, Poznań, 1996,

Literatura zalecana/fakultatywna

1. www.sztukaprezentacji.pl
2. T. Rawa, Metodyka wykonywania inżynierskich i magisterskich prac dyplomowych, Akademia RolniczoTechniczna w Olsztynie, Olsztyn, 1999.
3. A. Pabian, W. Gworys, Pisanie i redagowanie prac dyplomowych: poradnik dla studentów, Politechnika Częstochowska, Częstochowa, 1997.
4. K. Wójcik, Piszę pracę magisterską: poradnik dla autorów akademickich prac promocyjnych licencjackich, magisterskich, doktorskich, Wyd. 5 zm., Szkoła Głowna Handlowa, Warszawa, 2000.

F – Metody kształcenia oraz środki dydaktyczne

M5 – Metoda praktyczna (metoda projektu)

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

Wykłady:

F2 – obserwacja/aktywność (ocena aktywności podczas zajęć i jako pracy własnej). **F3 – praca pisemna** (dokumentacja projektu, pisemna analiza problemu w ramach pracy dyplomowej.).	**P3 –** ocena podsumowująca powstała na podstawie ocen formujących, uzyskanych w semestrze. **P5 –** wystąpienie/rozmowa (prezentacja, omówienie pracy dyplomowej).

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**			
	Seminarium			
	F2	F3	P3	P4
EPW1	X	X	X	X
EPU1	X	X	X	X
EPK1	X	X	X	X

G.4. Forma i warunki zaliczenia przedmiotu:

egzamin z oceną

H. Nakład pracy studenta	
Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	30
Czytanie literatury	10
Przygotowanie do egzaminu	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe	
Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Psychologiczne aspekty cyberbezpieczeństwa		
2. Punkty ECTS: 1		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 2**	**7. Liczba godzin ogółem: 15**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza (CW): Słuchacz zna i rozumie zjawiska psychologiczne w sieci oraz psychologicznego funkcjonowania użytkowników Internetu

Umiejętności (CU): Słuchacz ma umiejętność odnajdywania źródeł nieprawidłowego zachowania użytkowników w kontekście cyberzagrożeń.

Kompetencje społeczne (CK): Słuchacz ma świadomość wagi podejmowania działań na rzecz interesu publicznego oraz odpowiedzialnej realizacji powierzanych zadań

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: zagrożenia dla użytkowników płynące z upowszechniania nowoczesnych technologii w kontekście zachowań jednostki, mechanizmy i efekty poznania społecznego poprzez Internet, jego wpływ na relacje interpersonalne oraz na funkcjonowanie grup.

Umiejętności

EPU1: analizować i interpretować ludzkie zachowania oraz przyczyn problemów w funkcjonowaniu jednostek, grup, organizacji i społeczności w dobie Internetu.

Kompetencje społeczne

EPK1: podejmowania działań na rzecz interesu publicznego

EPK2: odpowiedzialnej realizacji powierzanych zadań

E - Treści programowe oraz literatura

<u>Forma zajęć: wykład</u>	
Wyk1 Psychologiczny wymiar Internetu nowa przestrzeń funkcjonowania człowieka. Psychologiczna charakterystyka użytkowników Internetu. Jednostka w wirtualnej rzeczywistości w kontekście cyberzagrożeń. Problematyka tożsamości sieciowej - psychologiczne konsekwencje konstruowania wirtualnej tożsamości. Kontakty społeczne - analiza punktu widzenia zaspokajania potrzeb użytkowników.	**5**
Wyk2 Poradnictwo sieciowe - pozytywne i negatywne aspekty zjawiska. Wpływ Internetu: modele wyjaśniające mechanizmy wpływu. Psychomanipulacja w sieci - zagrożenia dla użytkowników.	**5**
Wyk3 Wpływ technologii na zachowania społeczne poszczególnych jednostek, grup i organizacji.	

Cyberhigiena. Tendencje oceny ryzyka (nadmierny optymizm, heurystyka dostępności, zakotwiczenia, reprezentatywności.	**5**
Razem liczba godzin wykładów	**15**
Ogółem liczba godzin przedmiotu:	**15**

Literatura przedmiotu

Literatura podstawowa:

1. Wallace, P., Psychologia Internetu, Poznań 2005.
2. Castells M., Społeczeństwo sieci, Warszawa 2011.
3. Wojciszke B., Człowiek wśród ludzi. Zarys psychologii społecznej, Wydawnictwo Naukowe Scholar, Warszawa 2009.
4. Nęcka E., Orzechowski J., $ Szymura B., Psychologia poznawcza, Wydawnictwo Szkoły Wyższej Psychologii Społecznej „Academica", 2008.

Literatura zalecana/fakultatywna:

1. Majgier K., Internet jako przestrzeń komunikacyjna, Lublin 2002.
2. Sokołowski M.(red.), Oblicza Internetu, Elbląg 2004.
3. M. Castells, Galaktyka Internetu, Warszawa 2004.

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

Wykłady:

F1 – Sprawdzian (ustny lub pisemny)	Ocena podsumowująca powstała na podstawie ocen formułujących

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**
	Wykład
	F1
EPW1	x
EPU1	x
EPK1	X
EPK2	X

G.4. Forma i warunki zaliczenia przedmiotu:

Zaliczenie z oceną

H. Nakład pracy studenta

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

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	

Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Pozyskiwanie i weryfikacja danych z Internetu		
2. Punkty ECTS: 2		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 30**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15** **Laboratorium (Lab):15**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza (CW): Słuchacz zna podstawowe metody, techniki i narzędzia stosowane przy pozyskiwaniu informacji ze specjalistycznych źródeł.
Umiejętności (CU): Słuchacz ma umiejętność implementacji podstawowych metod, technik i narzędzia stosowanych przy pozyskiwaniu informacji ze specjalistycznych źródeł.
Kompetencje społeczne (CK): Słuchacz rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: podstawowe metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet

EPW2: podstawowe portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji

Umiejętności

EPU1: pozyskiwać dane, a także umiejętnie interpretować otrzymanie wyniki.

EPU2: użyć ogólnodostępnych narzędzi, m.in. wyszukiwarek internetowych i portali społecznościowych, jako źródła danych operacyjnych.

Kompetencje społeczne

EPK1: rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych

E - Treści programowe oraz literatura

<u>Forma zajęć: wykład</u> **Wyk1** Podstawowe metody, techniki, narzędzia stosowane przy korzystaniu z sieci Internet. Wyszukiwarka Google (google hacking, google grafika). Rejestr domen internetowych – WhoIs. WiGLE.net. **Wyk2** Informacje specjalistyczne ze źródeł publicznych takich jak zbiory orzeczeń sądowych, czy interpretacji podatkowych. Bazy przedsiębiorców – Centralna Ewidencja i Informacja o Działalności Gospodarczej, Krajowy Rejestr Sądowy, Elektroniczne Księgi Wieczyste, inne. Informacje o pojazdach – sprawdzanie numeru VIN. Baza polis i szkód ubezpieczeniowych. Mapy i zdjęcia, geolokalizacja. Narzędzia do analizy metadanych, zdjęć.	**6** **9**

Razem liczba godzin wykładów	**15**
Forma zajęć: laboratorium **Lab1** Podstawowe portale, metody, techniki i narzędzia wykorzystywane przy gromadzeniu informacji – praktyczne zadania. **Lab2** Wyszukiwanie informacji w sieci WWW. Ściąganie oprogramowania i innych plików. **Lab3** Kontaktowanie się ze światem. Wyszukiwanie w social mediach, wyszukiwanie ludzi. **Lab4** Poczta elektroniczna - wysyłanie i odbieranie wiadomości oraz zarzadzanie nimi. Najnowsze wiadomości z sieci WWW. Zarządzanie pieniędzmi online. **Lab5** Informacje specjalistyczne ze źródeł publicznych – praktyczne zadania. **Razem liczba godzin laboratorium**	 **2** **2** **2** **2** **7** **15**
Ogółem liczba godzin przedmiotu:	**30**

Literatura przedmiotu

Literatura podstawowa:

1. Kasser B., Internet praktycznie, Wydaw. „Intersoftland, Warszawa 2000.
2. Leś B., ABC… Internetu, Wydaw. Edition Kraków 2005.
3. Michałowska A., Michałowski S., Ćwiczenia z Internetu, Wydaw. MIKOM, Warszawa 2000.
4. Kent P., tł. Szymczyk W., Internet nie tylko dla orłów, Wydaw. Intersoftland, Warszawa 2000.
5. Żabicki P., Technologiczna codzienność. Internet – BANK – Telewizja, Wydaw. Trio, Warszawa 2007.

Literatura zalecana/fakultatywna:

1. Michałowska A., Michałowski S., Internet w Windows 98PL, Wydaw. MIKOM, Warszawa 2000.
2. Fabicki D., Poczta elektroniczna. Szkoła, internet, intranet, Wydaw. MIKOM, Warszawa 2000.
3. Sławik M., Komunikacja w Internecie dla każdego, Wydaw. Videograf Edukacja, Chorzów 2006.

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**		
	Wykład	Laboratorium	
	F1	F2	F5
EPW1	x		X
EPW2	x		X

EPU1		x	X
EPU2		x	X
EPK1		x	X
G.4. Forma i warunki zaliczenia przedmiotu:			
Zaliczenie z oceną			
H. Nakład pracy studenta			
Forma aktywności studenta			**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami			30
Czytanie literatury			5
Przygotowanie do laboratorium			10
Przygotowanie do zaliczenia			5
Suma godzin:			**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):			**2**
I – Informacje dodatkowe			
Tytuł/stopień, Imię i nazwisko sporządzającego program			
Data sporządzenia / aktualizacji	10.06.2023		
Dane kontaktowe (e-mail)			
Podpis			

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Zarządzanie usługami sieciowymi w kontekście bezpieczeństwa		
2. Punkty ECTS: 3		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 2**	**7. Liczba godzin ogółem: 45**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15** **Laboratorium (Lab): 30**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza (CW): Słuchacz zna i rozumie wybrane mechanizmy i protokoły bezpieczeństwa sieciowego stosowane w sieciowych systemach operacyjnych w tym w systemach urządzeń sieciowych LAN
Umiejętności (CU): Słuchacz ma umiejętność implementacji wybranych mechanizmów i protokołów bezpieczeństwa sieciowego stosowanych w sieciowych systemach operacyjnych w tym w systemach urządzeń sieciowych LAN
Kompetencje społeczne (CK): Słuchacz rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: zasady bezpiecznego zarządzania przełącznikami i routerami w sieciach LAN

EPW2: mechanizmy wybranych protokołów bezpieczeństwa sieciowego, implementowanych w sieciowych systemach operacyjnych, w tym systemach wbudowanych urządzeń sieciowych

Umiejętności

EPU1: wdrożyć protokoły bezpieczeństwa sieciowego umożliwiające bezpieczne, zdalne zarządzanie urządzeniami sieciowymi

EPU2: wdrożyć protokoły poprawiające bezpieczeństwo przesyłanych danych zarówno w skali LAN jak i Internetu

Kompetencje społeczne

EPK1: rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych

E - Treści programowe oraz literatura

<u>Forma zajęć: wykład</u>	
Wyk1 Czynności post instalacyjne, zarządzanie procesorami i pamięcią operacyjną. Wprowadzenie do nazewnictwa i oznaczeń dla urządzeń MikroTik	**2**
Wyk2 MikroTik – konfigurowanie usług sieciowych DHCP, pula statyczna i dynamiczna	**2**
Wyk3 MikroTik – konfigurowanie usług sieciowych - bridge, routing, wireless, metody pomiaru	**2**
Wyk4 MikroTik – konfigurowanie usług sieciowych – firewall, bezpieczeństwo QOS, kolejkowanie, tunele	**2**
Wyk5 Budowanie sieci zbudowanej na wielu urządzeniach MikroTik	**2**
Wyk6 Analiza celów i kompromisów technicznych. Dostępność – przywrócenie sieci po awarii	**2**
Wyk7 Wydajność sieci – symulowanie i testowanie sieci MikroTik.Algorytmy opracowania sieci	

bezprzewodowych	**3**
Razem liczba godzin wykładów	**15**
Forma zajęć: laboratorium	
Lab1 Dostęp do urządzenia sieciowego MikroTik, przygotowanie stanowisk pracy	**3**
Lab2 Urządzenia sieciowe MikroTik – Konfiguracja portów LAN, WAN, DHCP- klient DHCP- serwer DHCP	**3**
Lab3 Urządzenia sieciowe MikroTik – Konfigurowanie NAT – Masquerade, Ustawienia DNS	**3**
Lab4 Urządzenia sieciowe MikroTik - Tworzenie użytkowników - uprawnienia. Aktualizacja RouterOS	**3**
Lab5 Urządzenia sieciowe MikroTik – konfigurowanie usług sieciowych. Tablica ARP - wpisy statyczne urządzeń sieciowych. Export backup konfiguracji.	**3**
Lab6 Urządzenia sieciowe MikroTik – QOS - kolejki simle queue,PCQ. Tunele - PPP, PPPoE,	**3**
Lab7 Urządzenia sieciowe MikroTik Praca z logami systemowymi	**3**
Lab8 Urządzenia sieciowe MikroTik. Wireless - tryb access point i station. Wireless - szyfrowanie i access list	**3**
Lab9 Bezpieczeństwo w dostępie do urządzenia i skonfigurowanych usług sieciowych. Pomiary sygnałów przewodowych urządzeń MikroTik. Pomiary sygnałów bezprzewodowych urządzeń MikroTik	**3**
Lab10 Instalacja oprogramowania NS2 – testowanie. Instalacja oprogramowania NS2 – symulacje ruchu. Porównanie modelowania z rzeczywistymi pomiarami	**3**
Razem liczba godzin laboratorium	**30**
Ogółem liczba godzin przedmiotu:	**45**

Literatura przedmiotu

Literatura obowiązkowa:

1. Paweł Zaręba, Projekty i rozwiązania sieciowe w praktyce, Helion 2023
2. MikroTik MTCNA - Student Guide: Prepare for the MikroTik MTCNA certification exam with step-by-step LABS on RouterOS v7, Maher Haddad, Independently published 2023

Literatura zalecana / fakultatywna:

1. MikroTik Scripting: Unleash the Power of RouterOS Task, Nigel Bowden, Independently published 2023
2. Theory, laboratories and exercises for Mikrotik RouterOS,
3. https://mikrotikacademy.pl/
4. https://forum.mikrotik.com

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się			
Efekty przedmiotowe	**Forma zajęć / Metoda oceniania**		
	Wykład	Laboratorium	
	F1	F2	F5
EPW1	x		X
EPW2	x		X
EPU1		X	X
EPU2		x	X
EPK1		X	X

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

H. Nakład pracy studenta	
Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	45
Czytanie literatury	5
Przygotowanie do laboratorium	10
Przygotowanie do zaliczenia	10
Przygotowanie do egzaminu	5
Suma godzin:	**75**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**3**

I – Informacje dodatkowe	
Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Audyt informatyczny		
2. Punkty ECTS: 2		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 30**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15** **Ćwiczenia (Ćw):15**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza (CW): Słuchacz zna metodologie, metodyki i narzędzia do prowadzenia audytu informatycznego
Umiejętności (CU): Słuchacz ma umiejętność implementacji metodologii, metodyk i narzędzi do prowadzenia audytu informatycznego
Kompetencje społeczne (CK): Słuchacz rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: zagadnienia związane z systemami teleinformatycznymi dla audytorów IT, standardy, metodologie i metodyki prowadzenia audytu, proces audytu (utrzymanie systemów teleinformatycznych).

Umiejętności

EPU1: tworzyć program audytu oraz dokonać oceny ryzyka i bezpieczeństwa baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe.

Kompetencje społeczne

EPK1: rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych

E - Treści programowe oraz literatura

<u>Forma zajęć: wykład</u>	
Wyk1 Zapoznanie studentów z istotą, założeniami i celem audytu. Rodzaje audytu. Audyt informatyczny, audyt wewnętrzny, audyt bezpieczeństwa. Omówione zostanie podstawowe rozumienie audytu, elementy wspólne i różniące od kontroli, ścieżki kariery i rozwoju, certyfikacje międzynarodowe audytu: CISA, CIA. Podejście do audytu według ISACA a praktyka polska. Rynek pracy audytora w rozróżnieniu na sektor prywatny i publiczny, typowe zadania audytora i jego umiejscowienie w strukturze podmiotu prywatnego lub publicznego	**3**
Wyk2 Przedstawione zostanie podejście do prowadzenia badań odporności organizacji w konfrontacji ze zmotywowanym atakującym poprzez realizację rekonesansów bezpieczeństwa. Omówiona zostanie formuła rekonesansu, typowe realizacje i wnioski z pracy operacyjnej.	**3**
Wyk3 Standardy, metodologie i metodyki prowadzenia audytu. Omówione zostaną standardy ISACA, INTOSAI, NIST, ISO z serii 27000 dobre praktyki NIK, COBIT 5, ITIL, Krajowe Ramy Interoperacyjności	**3**

Wyk4 Proces audytu. Omówiony zostanie typowy cykl życia audytu, począwszy od planowania w oparciu o ocenę ryzyka, przygotowanie programu audytu, czynności audytowe, przygotowanie raportu z audytu, nadzór nad wykonaniem rekomendacji z audytu	**3**
Wyk5 Bezpieczeństwo informacji. Omówione zostaną rodzaje zagrożeń, które mogą mieć wpływ na bezpieczeństwo informacji w systemach teleinformatycznych. Zaprezentowane zostanę metody zabezpieczeń, omówione stosowane w praktyce narzędzia, rozwiązania techniczne i organizacyjno-prawne. Omówione będą dobre praktyki z zakresu zarządzania i utrzymania w ruchu systemów teleinformatycznych.	**3**
Razem liczba godzin wykładów	**15**
Forma zajęć: laboratorium	
Lab1 Analiza ryzyka jako podstawa do dalszych prac związanych z zapewnieniem bezpieczeństwa.	**3**
Lab2 Przeprowadzenie analizy ryzyka w oparciu o zaproponowaną metodę analizy ryzyka	**3**
Lab3 Opracowanie planu audytu w oparciu o wcześniej przygotowaną analizę ryzyka, przygotowanie listy zagadnień i pytań kontrolnych, opracowanie narzędzi ułatwiających prace: wzorów przydatnych dokumentów.	**3**
Lab4 Dyskusja zebranych dowodów z audytu. Analiza ich przydatności do dalszych postępowań, np. w razie stwierdzenia incydentów bezpieczeństwa informacji. Słuchacze zaprezentują wypełnione według wcześniej opracowanych wzorów dokumenty audytowe.	**3**
Lab5 Wprowadzenie do tematyki incydentów bezpieczeństwa. Zasady klasyfikacji incydentów i dalszego obiegu informacji o incydentach.	**3**
Razem liczba godzin laboratorium	**15**
Ogółem liczba godzin przedmiotu:	**30**

Literatura przedmiotu

Literatura obowiązkowa:

1. M.Forystek, Audyt informatyczny, InfoAudit, 2005,
2. M.Molski, M.Łacheta, Przewodnik audytora systemów informatycznych, Helion, 2006
3. T.Polaczek, Audyt bezpieczeństwa informacji w praktyce, Helion, 2006
4. Podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli, NIK, 2016
5. INTOSAI Framework of Professional Pronouncements (IFPP), https://www.issai.org/
6. K.Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN 2008,
7. K.Liderman, Bezpieczeństwo informacyjne, PWN, 2012

Literatura zalecana/fakultatywna:

1. Seria publikacji z zakresu COBIT 2019, ISACA, https://www.isaca.org/resources/cobit,
2. ITIL 4 Foundation, AXELOS,
3. CIA iia.org.pl/certyfikacja/certyfikat-ciar,
4. CISA Review Manual, 27th edition,
5. CISA Review Questions, Answers & Explanations Manual, 12th edition,
6. NIST standards, nist.gov/cybersecurity,
7. V.Troia, Upoluj cyberprzestępcę. Przewodnik dla hakerów prowadzących śledztwa online, Helion 2022,
8. V.Costa-Gazcon, Aktywne wykrywanie zagrożeń w systemach ITw praktyce. Wykorzystanie analizy danych, frameworku ATT&CK oraz narzędzi open source, Helion 2022

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

F – formująca	**P– podsumowująca**
Prowadzona na początku i w trakcie zajęć, przez	**Prowadzona pod koniec przedmiotu,**

nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.	**podsumowuje osiągnięte efekty uczenia się.**
Wykłady:	
F1 – Sprawdzian (ustny lub pisemny)	Ocena podsumowująca powstała na podstawie ocen formułujących
Laboratorium:	
F2 - Obserwacja/aktywność (podczas realizacji ćwiczeń wykonywanych podczas zajęć) F5 - Ćwiczenia praktyczne (ocena ćwiczeń wykonywanych podczas zajęć)	

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

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

G.4. Forma i warunki zaliczenia przedmiotu:

Zaliczenie z oceną

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	30
Czytanie literatury	5
Przygotowanie do laboratorium	5
Przygotowanie do zaliczenia	10
Suma godzin:	**50**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**2**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Bezpieczeństwo systemów teleinformatycznych		
2. Punkty ECTS: 3		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 2**	**7. Liczba godzin ogółem: 45**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15** **Laboratorium (Lab):30**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza (CW): Słuchacz zna definicje i standardy oraz unormowania dotycząc zagadnień odnoszących się do bezpieczeństwa systemów i sieci komputerowych
Umiejętności (CU): Słuchacz korzysta z poznanych narzędzi i metod oraz technik projektowania, konfigurowania, testowania w eliminowaniu podatności oraz przeciwdziałaniu skutkom incydentów bezpieczeństwa systemów i sieci komputerowych
Kompetencje społeczne (CK): Słuchacz rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: zagadnienia związane z bezpieczeństwem systemów i sieci, podstawowe narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń

Umiejętności

EPU1: wykorzystać podstawowe narzędzia i techniki do rozpoznawania zagrożeń, zaprojektować i wdrożyć procedury zapewniające bezpieczeństwo sieci i systemów.

Kompetencje społeczne

EPK1: rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych.

E - Treści programowe oraz literatura

<u>Forma zajęć: wykład</u>	
Wyk1 Elementy kryptografii. Omówione zostaną podstawy kryptografii w tym: metody i rodzaje szyfrowania symetrycznego i asymetrycznego, funkcje skrótów, podpis i certyfikaty cyfrowe oraz infrastruktura klucza publicznego.	**3**
Wyk2 Bezpieczeństwo infrastruktury sieciowej. Omówione zostaną podstawowe rodzaje ataków na infrastrukturę sieciową oraz metody i technologie zabezpieczania sieci korporacyjnych.	**3**
Wyk3 Bezpieczeństwo systemów operacyjnych. Omówione zostaną typowe rodzaje ataków oraz naruszenia bezpieczeństwa systemów operacyjnych (Windows, Linux), metody i rodzaje uwierzytelniania, kontroli dostępu do zasobów oraz przydzielania uprawnień w systemach operacyjnych, a także metody i narzędzie pozwalające na ochronę i podniesienie poziomu ich bezpieczeństwa.	**3**

Wyk4 Bezpieczeństwo aplikacji i usług. Omówione zostaną mechanizmy uwierzytelniania we współczesnych aplikacjach i systemach teleinformatycznych, metody separacji zasobów, dobre praktyki stosowane w projektowaniu redundantnych systemów wysokiej dostępności, sposoby wykonywania kopii zapasowych oraz metody i narzędzie pozwalające na ochronę i podniesienie poziomu ich bezpieczeństwa.	**3**
Wyk5 Systemy bezpieczeństwa. Omówione zostaną systemy bezpieczeństwa teleinformatycznego klasy SIEM, SOAR. NGFW. IPS/IDS, WAF, antymalware, EDR, Deception pozwalające na ochronę i podniesienie poziomu bezpieczeństwa infrastruktury sieciowej oraz systemowej przedsiębiorstwa.	**3**
Razem liczba godzin wykładów	**15**
Forma zajęć: laboratorium	
Lab1 Monitoring systemów za pomocą SIEM. Platformą SIEM - jednego z wiodących producentów na rynku, nabędzie umiejętności projektowania i implementowania reguł korelacyjnych, zrealizuje analizę przykładowego alarmu oraz przeprowadzi próbę analizy zdarzenia na podstawie zebranych logów.	**10**
Lab2 Monitoring sieci za pomocą platformy NDR. Platformą NDR (Antymalware/DLP) - jednego z wiodących producentów na rynku, nabędzie umiejętności projektowania i implementowania sposobu realizacji detekcji zagrożeń w infrastrukturze sieciowej, zrealizuje analizę przykładowego alarmu oraz przeprowadzi próbę analizy zdarzenia na podstawie zebranych danych sieciowych.	**10**
Lab3 EDR / Anty-DDoS (TAMA)	**10**
Razem liczba godzin ćwiczeń	**30**
Ogółem liczba godzin przedmiotu:	**45**

Literatura przedmiotu

Literatura obowiązkowa:

1. Marcin Karbowski „Podstawy Kryptografii", Helion
2. William Stallings, Lawrie Brown „Bezpieczeństwo systemów informatycznych", Helion
3. Mike Chapple, James Michael Stewart, Darril Gibson „Official $(ISC)^2$ CISSP Study Guide", Sybex
4. Ric Messier, „CEH v11 Cerified Ethical Hacker Study Guide", Sybex Don Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter Paperback, 2019 r.

Literatura zalecana/fakultatywna:

1. Norma ISO/IEC 27001:2017
2. Don Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter Paperback, 2019 r.
3. Don Murdoch, Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder, 2014 r.

F – Metody kształcenia oraz środki dydaktyczne

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

G - Weryfikacja osiągnięcia efektów uczenia się

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

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

wykonywanych podczas zajęć) F5 - Ćwiczenia praktyczne (ocena ćwiczeń wykonywanych podczas zajęć)	

G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się

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

G.4. Forma i warunki zaliczenia przedmiotu:

egzamin z oceną

H. Nakład pracy studenta

Forma aktywności studenta	**Liczba godzin na realizację**
Godziny zajęć z nauczycielem/ami	45
Czytanie literatury	5
Przygotowanie do laboratorium	10
Przygotowanie do zaliczenia	10
Przygotowanie do egzaminu	5
Suma godzin:	**75**
Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):	**3**

I – Informacje dodatkowe

Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	

	Wydział	**Techniczny**
	Kierunek studiów podyplomowych	**Cybersecurity – techniczne aspekty cyberbezpieczeństwa**

P R O G R A M P R Z E D M I O T U

A - Informacje ogólne

1. Przedmiot: Incydenty teleinformatyczne		
2. Punkty ECTS: 3		
3. Rodzaj przedmiotu: obowiązkowy		**4. Język wykładowy**: polski
5. Rok studiów: I	**6. Semestr/y: 1**	**7. Liczba godzin ogółem: 45**
8. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze:		**Wykład (Wyk): 15** **Laboratorium (Lab): 30**
9. Tytuł/stopień, imię i nazwisko koordynatora przedmiotu oraz prowadzących zajęcia		

B - Wymagania wstępne

C - Cele kształcenia

Wiedza(CW): Słuchacz zna narzędzia rozpoznawania incydentów teleinformatycznych
Umiejętności (CU): Słuchacz ma umiejętność obsługi narzędzi rozpoznawania incydentów teleinformatycznych
Kompetencje społeczne (CK): Słuchacz rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych.

D - Efekty uczenia się

Przedmiotowy efekt uczenia się

Wiedza

EPW1: podstawowe narzędzia i techniki wykorzystywane do rozpoznawania zagrożeń

Umiejętności

EPU1: wykorzystać podstawowe narzędzia i techniki do rozpoznawania zagrożeń, obsługiwać incydenty bezpieczeństwa w oparciu o systemy teleinformatyczne oraz sporządzać raporty

Kompetencje społeczne

EPK1: rozumie potrzebę uczenia się przez całe życie i podnoszenia swoich kompetencji w obszarze bezpieczeństwa danych.

E - Treści programowe oraz literatura

Forma zajęć: wykład	
Wyk1 Wprowadzenie do obsługi incydentów.	**2**
Wyk2 Omówienie jak wygląda typowy atak i czym jest incydent.	**3**
Wyk3 Procesy obsługi Incydentów na rzeczywistych przykładach.	**5**
Wyk4 Narzędzia wykorzystywane podczas obsługi incydentu. Narzędzia lokalne jak i dostępne online.	**5**
Razem liczba godzin wykładów	**15**
Forma zajęć: laboratorium	
Lab1 Obsługa incydentu bezpieczeństwa w oparciu o systemy teleinformatyczne. Ćwiczenia laboratoryjne mające na celu kompleksową obsługę incydentu od wykrycia alarmu, przez analizę, a kończąc na raporcie.	**30**
Razem liczba godzin ćwiczeń	**30**
Ogółem liczba godzin przedmiotu:	**45**

<table>
<tr><th colspan="4">Literatura przedmiotu</th></tr>
<tr><td colspan="4">Literatura obowiązkowa:
1. Don Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter Paperback, 2019 r.
2. Don Murdoch, Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder, 2014 r.</td></tr>
<tr><td colspan="4">Literatura zalecana/fakultatywna
1. Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone;
NIST Special Publication 800-61 Revision 2 - Computer SecurityIncident Handling Guide
2. Patrick Kral, The Incident Handlers Handbook, - SANS Institute</td></tr>
<tr><th colspan="4">F – Metody kształcenia oraz środki dydaktyczne</th></tr>
<tr><td colspan="4">M2 – Metoda problemowa (wykład problemowy).
M4 – Metoda programowa (wykład z wykorzystaniem materiałów multimedialnych).
M5 – Metoda praktyczna (ćwiczenia laboratoryjne)</td></tr>
<tr><th colspan="4">G - Weryfikacja osiągnięcia efektów uczenia się</th></tr>
<tr><th colspan="4">G.1. Metody oceniania i warunki zaliczenia poszczególnych form zajęć z przedmiotu:</th></tr>
<tr><td colspan="2">F – formująca
Prowadzona na początku i w trakcie zajęć, przez nauczycieli i studentów. Pomaga ukierunkować nauczanie do poziomu studentów, a studentowi pomaga w uczeniu się.</td><td colspan="2">P– podsumowująca
Prowadzona pod koniec przedmiotu, podsumowuje osiągnięte efekty uczenia się.</td></tr>
<tr><th colspan="4">Wykłady:</th></tr>
<tr><td colspan="2">F1 – Sprawdzian (ustny lub pisemny)</td><td colspan="2">Ocena podsumowująca powstała na podstawie ocen formułujących</td></tr>
<tr><th colspan="4">Laboratoria:</th></tr>
<tr><td colspan="2">F2 - Obserwacja/aktywność (podczas realizacji ćwiczeń wykonywanych podczas zajęć)
F5 - Ćwiczenia praktyczne (ocena ćwiczeń wykonywanych podczas zajęć)</td><td colspan="2"></td></tr>
<tr><th colspan="4">G.2. Metody weryfikacji osiągnięcia przedmiotowych efektów uczenia się</th></tr>
<tr><td rowspan="2">Efekty przedmiotowe</td><td colspan="3">Forma zajęć / Metoda oceniania</td></tr>
<tr><td>Wykład</td><td colspan="2">Laboratoria</td></tr>
<tr><td>EPW1</td><td>F1</td><td>F2</td><td>F5</td></tr>
<tr><td>EPW2</td><td>x</td><td></td><td>X</td></tr>
<tr><td>EPU1</td><td>x</td><td></td><td>X</td></tr>
<tr><td>EPK1</td><td></td><td>x</td><td>X</td></tr>
<tr><td>EPK2</td><td></td><td>x</td><td>X</td></tr>
<tr><td>EPK2</td><td>x</td><td>x</td><td>X</td></tr>
<tr><th colspan="4">G.4. Forma i warunki zaliczenia przedmiotu:</th></tr>
<tr><td colspan="4">Zaliczenie z oceną</td></tr>
<tr><th colspan="4">H. Nakład pracy studenta</th></tr>
<tr><td colspan="3">Forma aktywności studenta</td><td>Liczba godzin na realizację</td></tr>
<tr><td colspan="3">Godziny zajęć z nauczycielem/ami</td><td>45</td></tr>
<tr><td colspan="3">Czytanie literatury</td><td>5</td></tr>
<tr><td colspan="3">Przygotowanie do laboratorium</td><td>15</td></tr>
<tr><td colspan="3">Przygotowanie do zaliczenia</td><td>10</td></tr>
<tr><td colspan="3">Suma godzin:</td><td>75</td></tr>
<tr><td colspan="3">Liczba punktów ECTS dla przedmiotu (suma godzin : 25 godz.):</td><td>3</td></tr>
</table>

I – Informacje dodatkowe	
Tytuł/stopień, Imię i nazwisko sporządzającego program	
Data sporządzenia / aktualizacji	10.06.2023
Dane kontaktowe (e-mail)	
Podpis	