Tabela opisu efektów uczenia się studiów podyplomowych

Politechnika Krakowska im. Tadeusza Kościuszki w Krakowie

Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń

Dziedzina lub dziedziny nauki/~~sztuki~~[1]: Dziedzina nauk inżynieryjno-technicznych (100%)

Poziom Polskiej Ramy Kwalifikacji[2] 6 PRK

Symbole efektów uczenia się	KIERUNKOWE EFEKTY UCZENIA SIĘ STUDIÓW PODYPLOMOWYCH	Odniesienie do		
		uniwersalnych charakterystyk pierwszego stopnia PRK[3]	charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 PRK typowych dla kwalifikacji uzyskiwanych w ramach systemu szkolnictwa wyższego i nauki po uzyskaniu kwalifikacji pełnej na poziomie 4[4]	charakterystyk drugiego stopnia PRK typowych dla kwalifikacji o charakterze zawodowym – poziomy 6-8[5]
1	2	3	4	5
	WIEDZA: ABSOLWENT ZNA I ROZUMIE	**Kod składnika opisu**	**Kod składnika opisu**	**Kod składnika opisu**
CYB_W01	pojęcia dotyczące bezpieczeństwa informacji (danych) oraz sieci komputerowych	P6U_W	P6S_WG	P6Z_WT
CYB_W02	zaawansowane mechanizmy oraz algorytmy zabezpieczania informacji cyfrowych	P6U_W	P6S_WG	P6Z_WT
CYB_W03	problemy bezpiecznej komunikacji poprzez publiczne kanały wymiany informacji	P6U_W	P6S_WG	P6Z_WO
CYB_W04	wybrane typy zagrożeń i ataków na systemy i sieci	P6U_W	P6S_WG	P6Z_WZ
CYB_W05	protokoły transmisji w sieciach	P6U_W	P6S_WG	P6Z_WT
CYB_W06	zaawansowane mechanizmy zabezpieczeń wybranych systemów	P6U_W	P6S_WG	P6Z_WT
CYB_W07	metodyki, techniki i narzędzia niezbędne do implementacji skryptów	P6U_W	P6S_WG	P6Z_WZ
CYB_W08	zasady tworzenia i wykorzystania polityki bezpieczeństwa	P6U_W	P6S_WG	P6Z_WO

CYB_W09	wybrane metody przeprowadzania testów penetracyjnych	P6U_W	P6S_WG	P6Z_WZ
CYB_W10	wybrane narzędzia administratora systemów i sieci	P6U_W	P6S_WG	P6Z_WN
	UMIEJĘTNOŚCI: ABSOLWENT POTRAFI	**Kod składnika opisu**	**Kod składnika opisu**	**Kod składnika opisu**
CYB_U01	wybrać oraz wykorzystać odpowiednie mechanizmy ochrony informacji cyfrowych w kontekście określonego problemu	P6U_U	P6S_UW	P6Z_UO
CYB_U02	skonfigurować i zabezpieczyć system operacyjny	P6U_U	P6S_UW	P6Z_UU
CYB_U03	przeprowadzić analizę ruchu w sieciach	P6U_U	P6S_UW	P6Z_UI
CYB_U04	skonfigurować wybrane usługi w systemach i sieciach	P6U_U	P6S_UW	P6Z_UU
CYB_U05	implementować skrypty powłoki systemów operacyjnych	P6U_U	P6S_UW	P6Z_UI
CYB_U06	przygotować dokumentację techniczną zrealizowanych rozwiązań	P6U_U	P6S_UW	P6Z_UO
CYB_U07	wykonać analizę bezpieczeństwa środowiska IT	P6U_U	P6S_UW	P6Z_UI
CYB_U08	wykrywać popularne ataki na systemy i sieci oraz odpowiednio zareagować na zaistniały incydent	P6U_U	P6S_UW	P6Z_UO
CYB_U09	używać wybranych narzędzi administratora systemów i sieci	P6U_U	P6S_UW	P6Z_UN
CYB_U10	przeprowadzać testy penetracyjne	P6U_U	P6S_UW	P6Z_UN
	KOMPETENCJE SPOŁECZNE: ABSOLWENT JEST GOTÓW DO	**Kod składnika opisu**	**Kod składnika opisu**	**Kod składnika opisu**
CYB_K01	kierowania się w swojej pracy profesjonalizmem i etyką zawodową	P6U_K	P6S_KK	P6Z_KO P6Z_KP
CYB_K02	realizacji swoich działań z uwzględnieniem aspektów ekonomicznych	P6U_K	P6S_KK	P6Z_KW P6Z_KP

Objaśnienia używanych symboli:

SP = symbol studiów podyplomowych
01, 02, 03 i kolejne = numer efektu uczenia się
W = wiedza
U = umiejętności
K = kompetencje społeczne
Przykłady: **SP_W01**, **SP_U01**, **SP_K01**

1. Uniwersalne charakterystyki poziomów 6-8 PRK pierwszego stopnia:

P = poziom PRK (6, 7, 8)
U = charakterystyka uniwersalna
W = wiedza
U = umiejętności

K = kompetencje społeczne
Przykłady: **P6U_W**, **P7U_W**

2. Charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 PRK typowe dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego i nauki po uzyskaniu kwalifikacji pełnej na poziomie 4:

P = poziom PRK (6, 7, 8)
S = charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego

W = wiedza	**U = umiejętności**	**K = kompetencje społeczne**
G = głębia i zakres	W = wykorzystanie wiedzy	K = krytyczna ocena
K = kontekst	K = komunikowanie się	O = odpowiedzialność
	O = organizacja pracy	R = rola zawodowa
	U = uczenie się	

Przykłady: **P6S_WG**, **P7S_WG**

3. Charakterystyki drugiego stopnia PRK typowe dla kwalifikacji o charakterze zawodowym – poziomy 6-8:

P = poziom PRK (6, 7, 8)
Z = charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach kształcenia i szkolenia zawodowego

W = wiedza	**U = umiejętności**	**K = kompetencje społeczne**
T = teorie i zasady	I = informacje	P = przestrzeganie reguł
Z = zjawiska i procesy	O = organizacja pracy	W = współpraca
O = organizacja pracy	N = narzędzia i materiały	O = odpowiedzialność
N = narzędzia i materiały	U = uczenie się i rozwój zawodowy	

Przykłady:
P6Z_UO,
P7Z_K

---

[1] W przypadku więcej niż jednej dziedziny nauki/sztuki należy wpisać wszystkie, zgodnie z rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. 2018 r. poz. 1818).
[2] Należy podać właściwy poziom Polskiej Ramy Kwalifikacji, zgodnie z ustawą z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz.U. z.2020 r. poz. 226).
[3] Opis zakładanych efektów uczenia się dla kierunku studiów wyższych, poziomu i profilu kształcenia uwzględnia wszystkie uniwersalne charakterystyki pierwszego stopnia określone w ustawie z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji, właściwe dla danego poziomu Polskiej Ramy Kwalifikacji.
[4] Charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomie 6-8 PRK typowe dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego i nauki po uzyskaniu kwalifikacji pełnej na poziomie 4, określone w rozporządzeniu Ministra Nauki i Szkolnictwa Wyższego z dnia 14 listopada 2018 r. w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji (Dz.U. 2018 r. poz. 2218).
[5] Charakterystyki drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji o charakterze zawodowym – poziomy 6-8 określone w rozporządzeniu Ministra Edukacji Narodowej z dnia 13 kwietnia 2016 r. w sprawie charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji o charakterze zawodowym – poziomy 1-8 (Dz.U. 2016 r. poz. 537).

PLAN STUDIÓW PODYPLOMOWYCH
Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Wydział Inżynierii Elektrycznej i Komputerowej E-0
0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Obowiązuje od roku akademickiego 2023/2024

Lp.	Nazwa przedmiotu	RAZEM									semestry															
											I								II							
		Liczba godzin RAZEM	W	C	L	K	P	S	ECTS	E/Z	W	C	L	K	P	S	ECTS	E/Z	W	C	L	K	P	S	ECTS	E/Z
1	Bezpieczeństwo systemów Linux	48	16			32			5	Z	16			32			5	Z								
2	Bezpieczeństwo systemów Windows	48	16			32			5	Z	16			32			5	Z								
3	Platforma analizy zagrożeń 1	10				10			2	Z				10			2	Z								
4	Zagrożenia w obszarze cyberbezpieczeństwa	10	10						2	Z	10						2	Z								
5	Zarządzanie bezpieczeństwem informacji	10	10						1	Z	10						1	Z								
6	Bezpieczeństwo LDAP	30	10			20			4	Z									10			20			4	Z
7	Mechanizmy zabezpieczeń komunikacji	18	8			10			3	Z									8			10			3	Z
8	Narzędzia typu SIEM	24	8			16			3	Z									8			16			3	Z
9	Testy penetracyjne	30	10			20			3	Z									10			20			3	Z
10	Platforma analizy zagrożeń 2 - egzamin końcowy*	10				10			2	E												10			2	E
Ogółem		238	88	0	0	150	0	0	30		52	0	0	74	0	0	15		36	0	0	76	0	0	15	
Liczba egzaminów/zaliczeń		1/9																								

Legenda: W - wykłady, C - ćwiczenia, L - laboratoria, K - laboratoria komputerowe, P - projekty, S - seminaria, E - egzamin, Z - zaliczenie przedmiotu

* Platforma analizy zagrożeń 2 - zajęcia z egzaminem końcowym sprawdzającym zagadnienia omawiane również podczas pozostałych zajęć.
Egzamin kończący się uzyskaniem certyfikatu cyberbezpieczeństwa, wymagane 60% poprawnych rozwiązań zadań praktycznych na platformie CDeX

…….....……. kierownik studiów podyplomowych

…….. kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

…..……. Pełnomocnik Rektora Politechniki Krakowskiej ds. Kształcenia

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek:
Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Bezpieczeństwo systemów Linux
Nazwa przedmiotu w języku angielskim	Security of Linux systems
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	5
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: Platforma analizy zagrożeń 1 (CYB_CTF1),
Zagrożenia w obszarze cyberbezpieczeństwa (CYB_ZOC),

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności praktycznych związanych z budową i konfiguracją systemów Linux oraz popularnymi atakami na te systemy i wybrane usługi.

Efekty uczenia się:
EU1: zna budowę systemu, wybrane jego usługi oraz rodzaje zagrożeń, na które są narażone (CYB_W01, CYB_W04, CYB_W06, CYB_W07, CYB_W10).
EU2: potrafi konfigurować interfejsy sieciowe oraz wybrane usługi systemowe (CYB_U02, CYB_U09).
EU3: potrafi wykrywać i usuwać zagrożenia poprzez wprowadzenie zabezpieczeń zapobiegających atakom (CYB_U02, CYB_U04, CYB_U08, CYB_U09).
EU4: potrafi implementować skrypty powłoki systemowej (CYB_U05).
EU5: jest przygotowany do optymalizacji środowiska sprzętowego i programowego oraz konfiguracji systemu (CYB_K02).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	Z	16			32		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. System pomocy. 2. Zarządzanie lokalnymi użytkownikami i grupami. 3. Kontrola dostępu do plików i ACL. 4. Zarządzanie procesami i usługami. 5. Zarządzanie logami. 6. Zarządzanie partycjami i systemami plików. 7. Harminogram uruchmiania zadań. 8. Zarządzanie SELinux. 9. Konfiguracja interfejsów sieciowych. 11. Konfiguracja FTP i SSH. 12. Elementy hardeningu. 13. Programowanie w bash.	16
	1. Konfiguracja interfejsów sieciowych. 2. Konfiguracja usług SSH i FTP. 3. Wykrywanie najpopularniejszych ataków na usługi SSH i FTP oraz	

K	zapobieganie im. 4. Wykrywanie najpopularniejszych ataków na aplikacje webowe, m.in. SQL Injection, JWT cracking, Path traversal, CSRF Cross Site Request Forgery, XSS Cross-Site Scripting, oraz praktyczne wykorzystanie wybranych metod zapobiegania. 3. Identyfikacja i usuwanie zagrożeń poprzez wprowadzenie zabezpieczeń zapobiegających atakom. 4. Implementacja skryptów w powłoce bash.	32

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 60% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 60% zadań praktycznych.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja do platformy CDeX.
3. Linux Professional Institute: https://learning.lpi.org.
4. Dokumentacja systemu Kali Linux: https://www.kali.org/docs.

Zatwierdzenie karty przedmiotu:

…….	……	……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek:
Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Bezpieczeństwo systemów Windows
Nazwa przedmiotu w języku angielskim	Security of Windows systems
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	5
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: Platforma analizy zagrożeń 1 (CYB_CTF1),
Zagrożenia w obszarze cyberbezpieczeństwa (CYB_ZOC),

Cele przedmiotu: Celem przedmiotu jest nabycie wiedzy i umiejętności praktycznych związanych z budową i konfiguracją systemów Windows. Omówione zostaną popularne ataki na te systemy i ich wybrane usługi oraz zostaną przeprowadzone konfiguracje utwardzające system.

Efekty uczenia się:
EU1: zna budowę systemu, wybrane jego usługi oraz rodzaje zagrożeń, na które są narażone (CYB_W01, CYB_W04, CYB_W06, CYB_W07, CYB_W10).
EU2: potrafi wykrywać najpopularniejsze ataki na wybrane usługi oraz je zabezpieczyć (CYB_U02, CYB_U09).
EU3: potrafi wykrywać i usuwać zagrożenia poprzez wprowadzenie zabezpieczeń zapobiegających atakom (CYB_U02, CYB_U04, CYB_U08, CYB_U09).
EU4: potrafi implementować skrypty powłoki systemowej (CYB_U05).
EU5: jest przygotowany do optymalizacji środowiska sprzętowego i programowego oraz konfiguracji systemu (CYB_K02).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	Z	16			32		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Podstawy administracji systemami Windows. Konfiguracja interfejsów sieciowych. 2. Implementacja skryptów w powłoce systemowej. 3. Popularne ataki na usługi w systemach Windows. 4. Konfiguracja usługi katalogowej Active Directory. 5. Konfiguracja serwera Microsoft Exchange. 6. Analiza logów w dzienniku zdarzeń. 7. Bezpieczeństwo aplikacji pakietu Microsoft Office.	16
	1. Zarządzanie bezpieczeństwem rzeczywistego środowiska IT w warunkach codziennej pracy, w szczególności Microsoft Exchange i Active Directory. 2. Rozpoznanie i ocena infrastruktury IT pod kątem metod ochrony	

K	przed atakami cybernetycznymi. 3. Poznanie popularnych metod ataków na Microsoft Exchange i Active Directory. 4. Wykrywanie ataków brute-force i password spraying na podstawie analizy logów w Dzienniku Zdarzeń systemu Windows. 5. Konfiguracja zabezpieczeń dla kont użytkowników poprzez polityki Active Directory. 6. Wdrażanie zabezpieczeń dla aplikacji pakietu Microsoft Office. 7. Implementacja skryptów powłoki.	32

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 60% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 60% zadań praktycznych.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja do platformy CDeX.
3. J. Mielnik, Microsoft Windows Server 2022, Helion, 2023.
4. K. Wołk, Biblia Windows Server 2019. Podręcznik Administratora, Helion, 2020.

Zatwierdzenie karty przedmiotu:

…….	……	……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek:
Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Platforma analizy zagrożeń 1
Nazwa przedmiotu w języku angielskim	Threat Intelligence Platform 1
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	2
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: bez wymagań

Cele przedmiotu: Celem przedmiotu jest zdobycie umiejętności pozwalających na poruszanie się po środowisku laboratoryjnym, lokalizowanie flag ukrytych w systemach operacyjnych oraz wykorzystywanie popularnych narzędzi do przeprowadzania działań ukierunkowanych na bezpieczeństwo systemów (Linux, Windows).

Efekty uczenia się:
EU1: potrafi rozwiązywać zadania w formule Capture The Flag (CYB_U02, CYB_U09).
EU2: potrafi wykonywać operacje w środowisku platformy laboratoryjnej (CYB_U09).
EU3: potrafi odnajdować i odczytywać informacje przydatne do analizy zdarzeń (CYB_U03, CYB_U07, CYB_U09).
EU4: potrafi wykorzystywać popularne narzędzia do analizy stanu systemów (CYB_U03, CYB_U07, CYB_U09).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	Z				10		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
K	1. Praktyczne zapoznanie z platformą cybernetyczną. Zestawianie połączeń VPN i SSH. 2. Algorytmy budowy hashy haseł. 3. Szyfrowanie i deszyfrowanie ciągów znaków z wykorzystaniem m.in. base64, ROT-X, klucza publicznego/prywatnego. 4. Analiza ruchu sieciowego z wykorzystaniem Wireshark. 5. Podstawowe umiejętności programowania i uruchamiania skryptów. 6. Wykorzystanie gotowych podatności i backdoorów. 7. Zapoznanie i wprowadzenie do wykorzystania narzędzi rekonesansu np. NMAP, John The Ripper, DirBuster. 8. Łamanie haseł z wykorzystaniem popularnych narzędzi. 9. Wykorzystywanie wbudowanych narzędzi do analizy stanu systemów.	10

Metody dydaktyczne: ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: Poprawne wykonanie minimum 60% zadań praktycznych.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:

Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja do platformy CDeX.
3. Dokumentacja Metasploit: https://docs.metasploit.com.
4. V. Costa-Gazcón, Aktywne wykrywanie zagrożeń w systemach IT w praktyce. Wykorzystywanie analizy danych, frameworku ATT&CK oraz narzędzi open source, Helion, 2022.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek:
Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Zagrożenia w obszarze cyberbezpieczeństwa
Nazwa przedmiotu w języku angielskim	Threats in the area of cyber security
Kategoria przedmiotu	Specjalnościowy
Liczba punktów ECTS	2
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: brak wymagań

Cele przedmiotu: Zapoznanie z kategoriami i rodzajami przestępstw oraz zagrożeń w cyberprzestrzeni. Opisanie różnych typów ataków i ich cech charakterystycznych.

Efekty uczenia się:
EU1: zna i rozumie istotę oraz określenie cyberterroryzmu (CYB_W01, CYB_W03).
EU2: zna kategorie i rodzaje przestępstw oraz zagrożeń w cyberprzestrzeni (CYB_W04).
EU3: zna rodzaje ataków i podatności (CYB_W04).
EU4: rozumie na czym polega ochrona cyberprzestrzeni (CYB_W03, CYB_W04).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	Z	10					

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Istota i określenie cyberterroryzmu. Motywacje i techniki. 2. Model przeciwnika (zasoby, zdolności, zamiar, motywacja, awersja do ryzyka, dostęp). 3. Rodzaje ataków i podatności, które je umożliwiają m.in.: łamanie haseł, backdoory, trojany, wirusy, ataki bezprzewodowe, sniffing, spoofing, przejęcie sesji, denial of service, BOTs, MAC spoofing, ataki na aplikacje internetowe, Advanced Persistent Threat (APT). 4. Zdarzenia wskazujące na przeprowadzenie ataku. 5. Czas ataku. 6. Powierzchnia ataku. 7. Ukryte kanały. 8. Socjotechnika. 9. Problem czynnika wewnętrznego w bezpieczeństwie. 10. Źródła informacji o zagrożeniach. 11. Zagadnienia prawne związane z zagrożeniami cybernetycznymi.	10

Metody dydaktyczne: wykład problemowy, wykład informacyjny

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.

Kryteria oceny: odpowiedzieć poprawnie na minimum 60% pytań na kolokwium z wiadomości przekazywanych na wykładach.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:

Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. D. Graham, Etyczny haking. Praktyczne wprowadzenie do hakingu, Helion, 2022.
3. N.H. Tanner, Blue team i cyberbezpieczeństwo. Zestaw narzędzi dla specjalistów od zabezpieczeń w sieci, Helion, 2021.
4. G. Khawaja, Kali Linux i testy penetracyjne. Biblia, Helion, 2022.
5. Opracowanie zbiorowe, Cyberbezpieczeństwo. Zarys wykładu, Wolters Kluwer, 2018.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek:
Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Zarządzanie bezpieczeństwem informacji
Nazwa przedmiotu w języku angielskim	Information security management
Kategoria przedmiotu	Specjalnościowy
Liczba punktów ECTS	1
Semestry	I
Język wykładowy	Polski

Wymagania wstępne: brak wymagań

Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowych umiejętności pozwalających na zarządzanie bezpieczeństwem informacji w odniesieniu do wymagań norm ISO/IEC 27001.

Efekty uczenia się:
EU1: zna rodziny norm ISO/IEC 27xxxx oraz rozumie zachodzące między nimi relacje (CYB_W01, CYB_W08).
EU2: zna poszczególne obszary SZBI umożliwiające zarządzanie bezpieczeństwem (CYB_W08).
EU3: zna podstawowe zasady opracowywania dokumentacji SZBI (CYB_W08).
EU4: zna podstawowe zasady wykorzystywania zabezpieczeń organizacyjno-proceduralnych na potrzeby innych wymagań prawnych np. KRI, KSC, RODO (CYB_W08).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
I	Z	10					

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Zdobycie ogólnej wiedzy o relacjach i zawartości rodziny norm ISO/IEC 27xxx. 2. Zrozumienie znaczenia Systemu Zarządzania Bezpieczeństwem Informacji w Organizacji. 3. Wiedza umożliwiająca zaplanowanie wdrożenia SZBI w Organizacji.	10

Metody dydaktyczne: wykład problemowy, wykład informacyjny

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.

Kryteria oceny: odpowiedzieć poprawnie na minimum 60% pytań na kolokwium z wiadomości przekazywanych na wykładach.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. PN-EN ISO/IEC 27000 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia.

2. PN-EN ISO/IEC 27001 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania.
3. PN-EN ISO/IEC 27002 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji.
4. J. Krawiec, G. Ożarek, System Zarządzania Bezpieczeństwem Informacji w praktyce. Zabezpieczenia (Wydanie II zaktualizowane i rozszerzone), PKN, 2017.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek:
Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Bezpieczeństwo LDAP
Nazwa przedmiotu w języku angielskim	LDAP security
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	4
Semestry	II
Język wykładowy	Polski

Wymagania wstępne: bez wymagań

Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowych umiejętności pozwalających na bezpieczną konfigurację oraz reagowanie na incydenty bezpieczeństwa i ataki związane z LDAP.

Efekty uczenia się:
EU1: zna podstawowe pojęcia związane z LDAP (uwierzytelnianie, szyfrowanie itp.); zna podstawowe operacje związane z usługą (Bind, Search, Compare, Add, Delete, Modify, Modify DN, Unbind, Abandon, Extended); zna podstawowe struktury logiczne i fizyczne usługi AD; zna bazy danych usługi AD oraz schematy przechowywanych obiektów (CYB_W01; CYB_W02; CYB_W10).
EU2: potrafi zarządzać usługą Active Directory, potrafi używać narzędzi administracyjnych AD i zarządzać zasobami za pomocą grup IGDLA (CYB_U04, CYB_U09).
EU3: potrafi wykrywać ataki na Active Directory (CYB_U07, CYB_U08).
EU4: potrafi konfigurować zabezpieczenia w wykorzystaniem polityki Active Directory (CYB_U01, CYB_U02, CYB_U07, CYB_U09).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
II	Z	10			20		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Proces uwierzytelniania Kerberos. 2. Konfiguracja uwierzytelniania w LDAP. 3. Podstawowe operacje w LDAP (Bind, Search, Compare, Add, Delete, Modify, Modify DN, Unbind, Abandon, Extended). 4. Wprowadzenie i podstawy konfiguracji usługi Active Directory. 5. Podstawowe struktury logiczne i fizyczne usługi AD – domeny, drzewa domenowe, lasy, jednostki organizacyjne, kontrolery domeny, katalog globalny, RODC. 6. Baza danych usługi AD oraz schematy przechowywanych obiektów. 7. Instalacja kontrolera domeny. 8. Narzędzia administratora usługi AD. 9. Właściwości obiektów i zarządzanie obiektami: użytkownika, grupy, jednostki organizacyjnej, komputera. 10. Rodzaje grup, organizacja kontroli dostępu i zarządzanie zasobami za pomocą grup - IGDLA.	10

	11. Podłączanie komputera do kontrolera domeny w trybach offline i online. 12. Delegacja uprawnień administratora. 13. Rodzaje ataków (Password spraying, Pass-the-Hash, NLTM Relay, Kerberoast, Golden/ Silver Ticket, Group Policy Preferences, LDAP Injection).	
K	1. Zarządzanie bezpieczeństwem rzeczywistego środowiska IT w warunkach codziennej pracy, w szczególności Active Directory. 2. Rozpoznanie i ocena infrastruktury IT pod kątem metod ochrony przed cyberatakami. 3. Rozpoznanie popularnych metod ataków na infrastrukturę opartą o domenę Active Directory, w tym metod nadużywania protokołu Kerberos przez atakujących. 4. Wykrywanie ataków na Active Directory na podstawie analizy logów w Dzienniku Zdarzeń systemu Windows. 5. Konfiguracja zabezpieczeń poprzez polityki Active Directory.	20

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 60% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 60% zadań praktycznych.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja do platformy CDeX.
3. Dokumentacja openLDAP: https://www.openldap.org/doc.

Zatwierdzenie karty przedmiotu:

……..	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek:
Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Mechanizmy zabezpieczeń komunikacji
Nazwa przedmiotu w języku angielskim	Communication security mechanisms
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	3
Semestry	II
Język wykładowy	Polski

Wymagania wstępne: bez wymagań

Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowych umiejętności z zakresu działania sieci oraz bezpiecznej transmisji danych.

Efekty uczenia się:
EU1: posiada wiedzę z zakresu działania infrastruktury sieciowej (CYB_W05).
EU2: zna zabezpieczenia na poziomie komunikacji (CYB_W02, CYB_W03, CYB_W04).
EU3: potrafi konfigurować bezpieczne kanały komunikacyjne (CYB_U01, CYB_U03, CYB_U04).
EU4: potrafi zwiększać bezpieczeństwo usług sieciowych (CYB_U04).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
II	Z	8			10		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Sieci lokalne (LAN). Topologie sieciowe, 2. Protokół IP - budowa pakietu, metody przekazywania danych, adresowanie, podział adresów. 3. Protokoły routingu. 4. Protokoły warstwy transportowej (TCP/UDP). 5. Podstawowe i zaawansowane koncepcje kryptografii (szyfrowanie/deszyfrowanie, integralność danych, klasyfikacja ataków na szyfry, kryptografia symetryczna i asymetryczna, zaawansowane protokoły kryptograficzne, podpisy cyfrowe, protokoły ustalania klucza). 6. Szyfrowanie ruchu - L2 (MACSec), L3 (IPSec) i L4 (TLS). 7. Sieci VPN (site-to-site, remote-access) w systemie Linux. 8. Zapory ogniowe – typy, sposób działania, zapory sprzętowe i programowe. 9. System DNS. 10. Systemy wykrywania intruzów (IDS/IPS) oraz honeypot. 11. Bezpieczeństwo przechowywania informacji (szyfrowanie dysków i plików, kasowanie danych, maskowanie danych, bezpieczeństwo baz danych). 12. Uwierzytelnienie i integralność danych (siła protokołów	8

	uwierzytelniania, techniki ataków na hasła, techniki przechowywania haseł, kody uwierzytelniania wiadomości). 13. Kontrola dostępu (fizyczne zabezpieczenie danych, logiczna kontrola dostępu do danych, projektowanie bezpiecznej architektury, techniki zapobiegania wyciekowi informacji).	
K	1. Konfiguracja zapory ogniowej. 2. Konfiguracja serwera VPN. 3. Konfiguracja systemu IDS/IPS.	10

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 60% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 60% zadań praktycznych.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:
Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja do platformy CDeX.

Zatwierdzenie karty przedmiotu:

…….	……	……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek: Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Narzędzia typu SIEM
Nazwa przedmiotu w języku angielskim	SIEM tools
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	3
Semestry	II
Język wykładowy	Polski

Wymagania wstępne: bez wymagań

Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowych umiejętności wykorzystania narzędzi typu SIEM.

Efekty uczenia się:
EU1: zna elementy składowe tworzące środowisko systemów SIEM (CYB_W01, CYB_W08, CYB_W10).
EU2: potrafi konfigurować środowisko systemów SIEM (CYB_U04, CYB_U09).
EU3: potrafi wykrywać ataki z wykorzystaniem narzędzi SIEM (CYB_U08).
EU4: potrafi zarządzać oraz klasyfikować zdarzenia (logi) pod kątem funkcjonowania bezpieczeństwa usług i danych w infrastrukturze IT (CYB_U03, CYB_U04, CYB_U09).
EU5: jest gotów do wykonywania w sposób staranny i profesjonalny analizy bezpieczeństwa środowiska infrastruktury IT (CYB_K01).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
II	Z	8			16		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Charakterystyka sieci IT i OT. 2. Log Management (LMS). 3. Security Information Management (SIM). 4. Security Event Management (SEM). a) Intrusion Detection Systems (IDS) - analiza ruchu sieciowego, analiza heurystyczna, analiza anomalii, analiza sygnaturowa, analiza pakietów w oparciu o zdefiniowane reguły, śledzenie pakietów w dłuższym okresie, dekodowanie protokołów warstw wyższych, analiza konfiguracji i aktywności aplikacji/ - Network Based - Intrusion Detection System (NIDS). - Host Based - Intrusion Detection System (HIDS). - Network Node - Intrusion Detection System (NNIDS). b) IPS (Intrusion Prevention Systems). 5. Firewall NGFW. 6. SIEM (Security Information and Event Management) - monitoring bezpieczeństwa sieci, analiza zachowań, zapobieganie utracie danych, bezpieczeństwo w chmurze, audyt katalogów, analiza	8

	zagrożeń, kompleksowe zarządzanie incydentami. 7. Środowisko Splunk Enterprise. 8. Model bezpieczeństwa "Zero Trust Security".	
K	1. Konfiguracja środowiska Splunk Enterprise. 2. Zarządzanie oraz klasyfikacja logów/zdarzeń pod kątem bezpieczeństwa środowiska w warunkach codziennej pracy. 3. Łączenie w ciąg przyczynowo skutkowy logów/zdarzeń i wykrywanie dzięki niemu ataków cybernetycznych. 4. Analiza incydentów bezpieczeństwa przy pomocy systemu SIEM. 5. Rozpoznawanie schematów działania jednostek atakujących infrastrukturę. 6. Rozpoznanie i ocena infrastruktury IT pod kątem metod ochrony przed atakami cybernetycznymi. 7. Poznanie popularnych metod ataków na infrastrukturę oraz sposobu ich wykrywania. 8. Weryfikacja ruchu sieciowego za pomocą kolektora logów Splunk. 9. Szukanie anomalii oraz informacji związanych z infekcją złośliwym oprogramowaniem.	16

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 60% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 60% zadań praktycznych.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:

Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja do platformy CDeX.
3. D. Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter, 2019.
4. A.E. Thomas, Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence, 2018.

Zatwierdzenie karty przedmiotu:

…….	……	……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek:
Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Testy penetracyjne
Nazwa przedmiotu w języku angielskim	Penetration testing
Kategoria przedmiotu	specjalnościowy
Liczba punktów ECTS	3
Semestry	II
Język wykładowy	Polski

Wymagania wstępne: Bezpieczeństwo systemów Linux (CYB_BSL),
Bezpieczeństwo systemów Windows (CYB_BSW), Platforma analizy zagrożeń 1 (CYB_CTF1)

Cele przedmiotu: Celem przedmiotu jest zdobycie podstawowych umiejętności z zakresu oceny analizy ryzyka oraz metodologii przeprowadzania testów penetracyjnych.

Efekty uczenia się:
EU1: zna metodologie przeprowadzania testów penetracyjnych oraz podstawowe protokoły komunikacyjne (CYB_W05, CYB_W09).
EU2: potrafi przeprowadzać testy penetracyjne zgodnie z określoną metodyką (CYB_U03, CYB_U05, CYB_U07, CYB_U10).
EU3: przygotować raport (dokumentację techniczną) z wykonanych prac (CYB_U06).
EU4; jest gotów postępować etycznie, wykonywać swoją pracę zgodnie z przyjętymi standardami, uwzględniając w swoich działaniach aspekty ekonomiczne (CYB_K01, CYB_K02).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
II	Z	10			20		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
W	1. Rodzaje testów bezpieczeństwa i metodyki ich przeprowadzania. 2. Ataki na protokoły sieciowe. 3. Ataki na środowiska aplikacyjne. 4. Budowa i wykorzystanie protokołów komunikacyjnych. 5. Ataki na systemy sieci bezprzewodowych. 6. Wyprowadzanie informacji z zamkniętych środowisk. 7. Wybrane ataki na platformy Linux i Windows. 8. Eskalacja uprawnień w środowiskach systemów informatycznych. 9. Podstawy wykorzystania "exploitów".	10
K	1. Ataki na protokoły sieciowe. 2. Ataki na środowiska aplikacyjne. 3. Testy platform mobilnych oraz aplikacji dla nich przeznaczonych. 4. Analiza podatności protokołów komunikacyjnych. 5. Ataki na systemy sieci bezprzewodowych. 6. Wyprowadzanie informacji z zamkniętych środowisk. 7. Wybrane ataki na platformy Linux i Windows.	20

	8. Eskalacja uprawnień w środowiskach systemów informatycznych. 9. Podstawy wykorzystania "exploitów".	

Metody dydaktyczne: wykład problemowy, ćwiczenia laboratoryjne

Sposoby weryfikacji i oceny efektów uczenia się: Wykład: zaliczenie pisemne.
Laboratorium komputerowe: ocena wykonywanych zadań praktycznych.

Kryteria oceny: odpowiedzieć poprawnie na minimum 60% pytań na kolokwium z wiadomości przekazywanych na wykładach. Poprawne wykonanie minimum 60% zadań praktycznych.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:

Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja do platformy CDeX.
3. G. Khawaja, Kali Linux i testy penetracyjne. Biblia, Helion, 2022.
4. M. Hickey, J. Arcuri, Warsztat hakera. Testy penetracyjne i inne techniki wykrywania podatności, Helion, 2022.

Zatwierdzenie karty przedmiotu:

……..	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów

Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

Obowiązuje uczestników rozpoczynających studia podyplomowe w roku akademickim 2023/2024
Nazwa studiów podyplomowych Cyberbezpieczeństwo – praktyczna analiza zagrożeń
Nazwa jednostki/jednostek organizacyjnych prowadzących studia wraz z symbolem jednostki/jednostek:
Wydział Inżynierii Elektrycznej i Komputerowej E-0
Nazwa jednostki wiodącej Wydział Inżynierii Elektrycznej i Komputerowej E-0
Kod i nazwa studiów podyplomowych według klasyfikacji ISCED 0688 - Interdyscyplinarne programy i kwalifikacje obejmujące technologie informacyjno-komunikacyjne

Nazwa przedmiotu w języku polskim	Platforma analizy zagrożeń 2
Nazwa przedmiotu w języku angielskim	Threat Intelligence Platform 2
Kategoria przedmiotu	Specjalnościowy
Liczba punktów ECTS	2
Semestry	II
Język wykładowy	Polski

Wymagania wstępne: Platforma analizy zagrożeń 1 (CYB_CTF1)

Cele przedmiotu: Celem przedmiotu jest synteza i usystematyzowanie zdobytej wiedzy i umiejętności w zakresie cyberbezpieczeństwa, hardeningu systemów Linux oraz Windows w celu redukcji powierzchni ataku.

Efekty uczenia się:
EU1: potrafi zwiększać poziom bezpieczeństwa systemów komputerowych (CYB_U02, CYB_U09).
EU2: potrafi rozpoznawać incydenty oraz reagować na wybrane typy ataków, szczególnie w odniesieniu do aplikacji internetowych (CYB_U03, CYB_U08, CYB_U09).
EU3: potrafi analizować, identyfikować podatności systemów operacyjnych oraz aplikacji (CYB_U02, CYB_U03
CYB_U07, CYB_U08).
EU4: potrafi przeprowadzać podstawowe testy penetracyjne (CYB_U10).
EU5: jest gotów do działania zgodnie z zasadami etyki przeprowadzania testów penetracyjnych (CYB_K01).

Forma zajęć, semestralna liczba godzin

Semestr	Forma zaliczenia (E/Z)	Wykłady	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
II	E				10		

Treści programowe (oddzielnie dla każdej formy zajęć):

Forma zajęć	Tematyka zajęć	Liczba godzin
K	1. Utwardzanie systemów operacyjnych w celu redukcji powierzchni ataku. 2. Wykrywanie nieautoryzowanego dostępu do systemów informatycznych. 3. Elementy podstawowej analizy powłamaniowej. 4. Monitoring i identyfikacja zagrożeń w systemach operacyjnych i infrastrukturze sieciowej w celu ich zabezpieczania. 5. Rozpoznawanie incydentów oraz reagowania na wybrane ataki na aplikacje internetowe. 6. Kompleksowe zarządzanie incydentami. 7. Analiza, wykrywanie i wskazywanie podatności systemów operacyjnych oraz aplikacji. 8. Zabezpieczanie środowiska przed zaawansowanymi	10

	cyberzagrożeniami. 9. Wybrane techniki przeprowadzania testów penetracyjnych.	

Metody dydaktyczne: ćwiczenia laboratoryjne, testy sprawdzające.

Sposoby weryfikacji i oceny efektów uczenia się: Laboratorium komputerowe: ocena wykonywanych zadań praktycznych. Egzamin końcowy

Kryteria oceny: Poprawne wykonanie minimum 60% zadań praktycznych na zajęciach laboratorium komputerowego i egzaminie.

Dodatkowe informacje ustalane przez osobę odpowiedzialną za przedmiot:

Wykaz literatury:
1. Materiały dostarczone przez prowadzącego w formie elektronicznej.
2. Dokumentacja do platformy CDeX.
3. Dokumentacja Metasploit: https://docs.metasploit.com.
4. V. Costa-Gazcón, Aktywne wykrywanie zagrożeń w systemach IT w praktyce. Wykorzystywanie analizy danych, frameworku ATT&CK oraz narzędzi open source, Helion, 2022.

Zatwierdzenie karty przedmiotu:

…….	……	……..……
miejscowość, data	osoba odpowiedzialna za przedmiot	kierownik jednostki organizacyjnej PK/ przewodniczący rady programowej studiów