UNIWERSYTET
Andrzeja Frycza Modrzewskiego
w Krakowie

KARTA PRZEDMIOTU

1. Informacje wstępne

Nazwa przedmiotu	**Bezpieczeństwo systemów informatycznych i sieci teleinformatycznych**
Wydział	Wydział Zarządzania, Mediów i Technologii
Kierunek	Informatyka i ekonometria
Specjalność/Ścieżka specjalizacyjna	bezpieczeństwo informacji
Poziom PRK	6 PRK
Poziom kształcenia	studia pierwszego stopnia
Forma studiów	studia stacjonarne
Grupa zajęć	—
Liczba punktów ECTS	5
Rodzaj przedmiotu	specjalizacyjny
Liczba godzin ogółem	45 godz.
Cykl dydaktyczny	2024/2025 zimowy
Semestr studiów	5
Rok studiów	3
Profil kształcenia	praktyczny
Rok realizacji	2026/2027
Język wykładowy	polski
Osoba odpowiedzialna za przedmiot	mgr inż. Dominik Rosek (e-mail: drosek@uafm.edu.pl)

Semestr, liczba punktów ECTS, rodzaj zajęć, liczba godzin w planie studiów

Semestr	Laboratorium	Konwersatoria	ECTS
5	30 godz.	15 godz.	5

2. Cele przedmiotu

C1	Zapoznanie studentów aspektami bezpieczeństwa sieci i systemów komputerowych oraz zagadnieniami bezpieczeństwa elektronicznego i związanych z nimi fragmentów polityki bezpieczeństwa firmy.

3. Wymagania wstępne

Posiadanie wiedzy dotyczącej sieci komputerowych, podstawowa umiejętność obsługi pakietu biurowego.

4. Opis efektów uczenia się

W1	Wiedza: Student posiada uporządkowaną wiedzę ogólną z zakresu bezpieczeństwa systemów informatycznych i sieci, posiada wiedzę pozwalającą na samodzielne implementowanie polityk bezpieczeństwa oraz rozwiązywania problemów związanych bezpieczeństwem w aspekcie administrowania systemami komputerowymi.	
U1	Umiejętności: Potrafi zastosować podstawowe techniki zabezpieczania systemów komputerowych na poziomie systemu operacyjnego, urządzeń sieciowych. Samodzielnie potrafi dobrać środki ochrony adekwatne do problemu.	
K1	Kompetencje społeczne: Student zna znaczenie i wagę problemów zapewniania bezpieczeństwa systemom informatycznym, jest świadomy potrzeby ciągłego doskonalenia umiejętności i poszerzania wiedzy.	

5. Treści programowe

Laboratorium (30 godz.)

Kod	Tematyka zajęć (nr semestru: 5)
Lab1	Protokoły i standardy bezpieczeństwa internetu
Lab2	Aplikacje do uwierzytelniania w internecie
Lab3	Bezpieczeństwo sieci bezprzewodowych
Lab4	Bezpieczeństwo Linuksa
Lab5	Bezpieczeństwo systemu Windows
Lab6	Środowiska zaufane i zabezpieczenia wielopoziomowe

Konwersatoria (15 godz.)

Kod	Tematyka zajęć (nr semestru: 5)
Kon1	Przegląd: Koncepcje bezpieczeństwa komputerowego, Zagrożenia, ataki i aktywa, Podstawowe zasady projektowania bezpieczeństwa, Powierzchnie ataków i drzewa ataków, Strategia bezpieczeństwa komputerowego, Standardy.
Kon2	Uwierzytelnianie użytkownika: Zasady cyfrowego uwierzytelniania użytkownika, Uwierzytelnianie oparte na hasłach, Uwierzytelnianie oparte na żetonach, Uwierzytelnianie biometryczne, Zdalne uwierzytelnianie użytkownika, Zagadnienia bezpieczeństwa uwierzytelniania użytkownika.
Kon3	Malware — szkodliwe oprogramowanie: Rodzaje szkodliwego oprogramowania, Zaawansowane trwałe zagrożenie, Rozsiewanie — socjotechnika — spam pocztowy, konie trojańskie, Ładunek — psucie systemu, Ładunek — działania ukradkowe — boczne drzwi, rootkity, Przeciwdziałania.
Kon4	Ataki polegające na odmowie świadczenia usług: Odmowa usług jako rodzaj ataku , Ataki zatapiające, Rozproszone ataki blokowania usług, Ataki na przepływność oparte na aplikacjach, Ataki odbijające i ataki ze wzmocnieniem, Obrona przed odmową świadczenia usług, Reagowanie na atak typu odmowa świadczenia usług.
Kon5	Wykrywanie włamań: Intruzi, Wykrywanie włamań, Podejścia analityczne, Wykrywanie włamań oparte na hoście, Wykrywanie włamań oparte na sieci, Rozproszone lub hybrydowe wykrywanie włamań, Miodownice (honeypoty).
Kon6	Zapory sieciowe i systemy zapobiegania włamaniom: Zapotrzebowanie na zapory sieciowe, Charakterystyka zapór sieciowych i polityka dostępu, Rodzaje zapór sieciowych, Posadowienie zapór sieciowych, Umiejscowienie i konfiguracja zapór sieciowych, Systemy zapobiegania włamaniom.
Kon7	Bezpieczeństwo systemów operacyjnych: Wprowadzenie do bezpieczeństwa systemów operacyjnych, Planowanie bezpieczeństwa systemu operacyjnego, Hartowanie systemów operacyjnych, Bezpieczeństwo aplikacji, Dbałość o bezpieczeństwo, Bezpieczeństwo w systemach Linux i UNIX, Bezpieczeństwo w systemie Windows, Bezpieczeństwo wirtualizacji.

6. Metody dydaktyczne

Laboratorium	
M4	Ćwiczenia komputerowe
M15	Praca nad projektami

M16	Praca w grupach
M19	Studium przypadku
M23	Zajęcia praktyczne
Konwersatoria	
	Wykład informacyjny
M1	Analiza przypadków
M3	Burza mózgów
M10	Konwersatorium
M13	Metody e-learningowe
M17	Prezentacja multimedialna
M20	Uczenie się w oparciu o problem

7. Nakład pracy studenta

Forma aktywności studenta	Obciążenie studenta
Laboratorium	**30 godz.**
W tym metodą e-learning:	**0 godz.**

Konwersatoria	**15 godz.**
W tym metodą e-learning:	**0 godz.**

Praca własna studenta
80 godz.

Całkowite obciążenia	
Sumaryczna liczba godzin dla przedmiotu wynikajaca z całego nakładu pracy studenta	**125 godz.**
Sumaryczna liczba punktów ECTS dla przedmiotu	**5 ECTS**

8. Kryteria oceny

Laboratorium	
Na ocenę 5:	zaliczenie praktyczne zadań w laboratorium oraz projektów na min. 90%
Na ocenę 4,5:	zaliczenie praktyczne zadań w laboratorium oraz projektów na min. 80%
Na ocenę 4:	zaliczenie praktyczne zadań w laboratorium oraz projektów na min. 70%
Na ocenę 3,5:	zaliczenie praktyczne zadań w laboratorium oraz projektów na min. 60%
Na ocenę 3:	zaliczenie praktyczne zadań w laboratorium oraz projektów na min. 50%

Konwersatoria	
Na ocenę 5:	zaliczenie egzaminu na min. 90%
Na ocenę 4,5:	zaliczenie egzaminu na min. 80%
Na ocenę 4:	zaliczenie egzaminu na min. 70%
Na ocenę 3,5:	zaliczenie egzaminu na min. 60%
Na ocenę 3:	zaliczenie egzaminu na min. 50%

9. Literatura

Literatura podstawowa

1. Liderman K — Bezpieczeństwo informacyjne, Warszawa, 2012, Wydawnictwo Naukowe PWN
Liderman — Podręcznik administratora bezpieczeństwa teleinformatycznego, Warszawa, 2009, Mikom
William Stallings, Lawrie Brown - Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 1 i 2

Literatura uzupełniająca

1. A. Białas — Bezpieczeństwo Informacji i Usług w Nowoczesnej Instytucji i Firmie, Warszawa, 2007, WNT
Lehtinen R., Russell D — Podstawy ochrony komputerów, Gliwice, 2007, Helion

10. Informacja o osobach prowadzących zajęcia

Osoby prowadzące zajęcia

mgr inż. Dominik Rosek (e-mail: drosek@uafm.edu.pl)