Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2023/2024

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo w sieciach telekomunikacyjnych
Nazwa przedmiotu w języku angielskim	Security in telecommunication networks
Kod przedmiotu	WIiT I oIIS D4 23/24
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	4.00
Semestry	2

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
2	30	0	0	30	0	0

3 Cele przedmiotu

Cel 1 Wprowadzenie do bezpieczeństwa sieci telekomunikacyjnych

Cel 2 Zapoznanie studentów z metodami bezpiecznej transmisji przez sieć komputerową

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 znajomość podstaw sieci komputerowych (protokoły, techniki transmisji)

5 Efekty kształcenia

EK1 Umiejętności Student potrafi konfigurować sprzęt i oprogramowanie związane z bezpieczeństwem sieci.

EK2 Wiedza Student potrafi prezentować zagrożenia bezpieczeństwa w warstwach modeli OSI i TCP/IP.

EK3 Wiedza Student potrafi przedstawić metody bezpiecznej transmisji.

EK4 Wiedza Student potrafi przedstawić techniki ataków w sieciach komputerowych.

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	transmisja w sieci komputerowej i techniki ataków	4
W2	Bezpieczeństwo w warstwie alpikacji	4
W3	Bezpieczeństwo w warstwie transportowej	2
W4	Bezpieczeństwo w warstwie sieci	2
W5	Bezpieczeństwo w warstwie łącza danych	2
W6	Bezpieczeństwo w warstwie fizycznej	2
W7	transmisja bezprzewodowa i zagrożenia	2
W8	VPN	2
W9	Firewall	2
W10	Testy penetracyjne	3
W11	ACL	2
W12	AAA	2
W13	Certyfikaty	1

Laboratorium komputerowe		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
K1	Wykorzystanie sieci komputerowych	2

Laboratorium komputerowe		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
K2	Sniffing	2
K3	Wykrywanie sniffingu	2
K4	Scanning	2
K5	DoS/DDoS	2
K6	Man in the middle	2
K7	Bezpieczeństwo poczty elektronicznej	2
K8	VyOS	4
K9	Firewall programowe	2
K10	Firewall sprzętowe	4
K11	Kali Linux	4
K12	Hasła i funkcje skrótu	2

7 Narzędzia dydaktyczne

N1 Wykłady (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N2 Ćwiczenia laboratoryjne (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N3 Dyskusja (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N4 Konsultacje (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	60
Konsultacje przedmiotowe	10
Egzaminy i zaliczenia w sesji	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	15
Opracowanie wyników	20
Przygotowanie raportu, projektu, prezentacji, dyskusji	11
kolokwium zaliczeniowe	4
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**120**
Sumaryczna liczba punktów ECTS dla przedmiotu	4.00

9 Sposoby oceny

Ocena formująca

F1 Kolokwium

F2 Test

F3 Sprawozdania z ćwiczeń laboratoryjnych

Ocena podsumowująca

P1 Kolokwium pisemne

P2 Średnia ważona ocen formujących

Warunki zaliczenia przedmiotu

W1 Pełna obecność na obowiązkowych formach zajęć

W2 Konieczność zaliczenia wszystkich testów i ćwiczeń praktycznych przed przystąpieniem do egzaminu.

Ocena aktywności bez udziału nauczyciela

B1 Ocena ze sprawozdania laboratoryjnego przygotowanego przez studenta

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie spełnia kryteriów na ocenę 3.0.
Na ocenę 3.0	To co na ocenę niższą oraz student potrafi wykonać częściową konfigurację, często popełniając błędy.
Na ocenę 3.5	To co na ocenę niższą oraz student potrafi konfigurować podstawowe usługi, błędy popełnia rzadko.
Na ocenę 4.0	To co na ocenę niższą oraz student potrafi konfigurować zaawansowane metody bezpieczeństwa, ma odpowiednią wiedzę, zaawansowana konfiguracja nie zawsze działa poprawnie.
Na ocenę 4.5	To co na ocenę niższą oraz student radzi sobie z konfiguracją zaawansowanych metod bezpieczeństwa, ma szeroki zakres wiedzy pozwalający mu zrozumieć konfigurowane metody.
Na ocenę 5.0	To co na ocenę niższą oraz student radzi sobie z konfiguracją każdej podstawowej i zaawansowanej usługi bezpieczeństwa.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie spełnia kryteriów na ocenę 3.0.
Na ocenę 3.0	To co na ocenę niższą oraz student potrafi opisać podstawowe metody bezpiecznej transmisji danych. Student zna model OSI.
Na ocenę 3.5	To co na ocenę niższą oraz student zna model OSI i TCP/IP. Student potrafi w prosty sposób przypisywać techniki ataku do warstw modelu.
Na ocenę 4.0	To co na ocenę niższą oraz student potrafi szczegółowo opisać techniki ataków i podstawowo techniki obrony.
Na ocenę 4.5	To co na ocenę niższą oraz student potrafi szczegółowo opisać techniki obrony przed atakami w sieci.
Na ocenę 5.0	To co na ocenę niższą oraz student zna wszystkie techniki ataku i metody obrony przed nimi przy użyciu zaawansowanych narzędzi.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie spełnia kryteriów na ocenę 3.0.
Na ocenę 3.0	To co na ocenę niższą oraz student potrafi opisać podstawowe metody zabezpieczania sieci komputerowych.
Na ocenę 3.5	To co na ocenę niższą oraz student potrafi szczegółowo opisać metody bezpiecznej transmisji danych.
Na ocenę 4.0	To co na ocenę niższą oraz student potrafi opisać zasady VPN, ACL, AAA i sposoby ich konfiguracji.
Na ocenę 4.5	To co na ocenę niższą oraz student zna wszystkie techniki bezpiecznej transmisji danych i potrafi je skonfigurować.

Na ocenę 5.0	To co na ocenę niższą oraz student potrafi konfigurować zaawansowane narzędzia bezpieczeństwa i ma szeroką wiedzę na temat bezpiecznej transmisji danych.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie spełnia kryteriów na ocenę 3.0.
Na ocenę 3.0	To co na ocenę niższą oraz student potrafi opisać podstawowe metody bezpiecznej transmisji danych.
Na ocenę 3.5	To co na ocenę niższą oraz student potrafi wymienić i opisać techniki ataków pasywnych.
Na ocenę 4.0	To co na ocenę niższą oraz student potrafi wymienić i opisać techniki aktywnych ataków.
Na ocenę 4.5	To co na ocenę niższą oraz student zna metody obrony przed atakami pasywnymi i aktywnymi.
Na ocenę 5.0	To co na ocenę niższą oraz student ma szeroką wiedzę i potrafi konfigurować zaawansowane narzędzia bezpieczeństwa.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I2_W02 I2_W03 I2_U03b	Cel 1	W9 W10 W11 W12	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK2	I2_W06 I2_U06 I2_K04	Cel 2	W2 W3 W4 W5 W6 W7	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK3	I2_W02 I2_K04	Cel 1	W1 W8 W13	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK4	I2_W02 I2_W06 I2_U07	Cel 2	W2 W3 W4 W5 W6 W7	N1 N2 N3 N4	F1 F2 F3 P1 P2

11 Wykaz literatury

Literatura podstawowa

[1] **William Stallings, Lawrie Brown** — *Bezpieczeństwo systemów informatycznych. Zasady i praktyka.*, , 2016, Helion

[2] **Chris McNab** — *Network Security Assessment*, , 2016, O'Reilly Media

[3] **WatchGuard** — *WatchGuardhttp://www.watchguard.com/help/docs/webui/XTM_ 11/en-US/v11_ 9_ Web_ UI_ User_ Gui US).pdf*, , 2014,

[4] **Michal Zalewski** — *Cisza w sieci*, , 2005, Helion

[6] — *Źródła internetowe (Sekurak, Haking)*, , 0,

Literatura uzupełniająca

[1] **Adam Józefiok** — *Security CCNA 210-260. Zostań administratorem sieci komputerowych Cisco*, , 2016, Helion

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr inż. Dariusz Żelasko (kontakt: `dariusz.zelasko@pk.edu.pl`)

Osoby prowadzące przedmiot

1 dr inż. Dariusz Żelasko (kontakt: `dariusz.zelasko@pk.edu.pl`)

2 mgr inż. Andrzej Mycek (kontakt: `andrzej.mycek@pk.edu.pl`)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .

. . . . . .