

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Bezpieczeństwo sieci komputerowych**

Nazwa w języku angielskim: **Security of computer networks**

Karta przedmiotu ważna od roku akademickiego: **2022/2023**

Kierunek studiów: **Informatyka**

Poziom studiów: **Studia I stopnia**

Forma studiów: **Niestacjonarne**

Profil: **Praktyczny**

Specjalność: **Cyberbezpieczeństwo**

Język wykładowy: **Polski**

Jednostka prowadząca: **Wydział Nauk Społecznych i Technicznych**

Prowadzący: **dr Grzegorz Jastrzębski**

OBCIĄŻENIE STUDENTA

	Wykład	Konwersatorium	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć dydaktycznych organizowanych przez Uczelnię	16				
Liczba godzin całkowitego nakładu pracy studenta	50				
Forma zaliczenia	Zaliczenie z oceną				
Liczba punktów ECTS	2				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

Wiedza i kompetencje z zakresu sieci komputerowych.

CELE PRZEDMIOTU

C1	Nabycie wiedzy z zakresu inżynierii bezpieczeństwa w sieciach komputerowych i kryptografii w systemach sieciowych i internetowych.
C2	Zdobycie wiedzy o sposobach, mechanizmach i narzędziach do zapewniania poufności i integralności informacji, oraz do uwierzytelniania i autoryzacji dostępu do zasobów i usług w systemach informatycznych i serwisach internetowych.
C3	Zdobycie wiedzy o atakach komputery, systemy i oprogramowanie sieci oraz na usługi komunikacyjne, informacyjne i biznesowe dostępne w Internecie, nabycie wiedzy o atakach za pomocą wirusów, robaków i ukrytych kanałów komunikacyjnych oraz rozwijanie umiejętności wykorzystania zdobytej wiedzy.

PRZEDMIOTOWE EFEKTY UCZENIA – PEU	
Z zakresu wiedzy:	
PEU_W01	Student posiada wiedzę z zakresu inżynierii bezpieczeństwa w sieciach komputerowych i kryptografii w systemach sieciowych i internetowych.
PEU_W02	Student posiada wiedzę o sposobach, mechanizmach i narzędziach do zapewniania poufności i integralności informacji oraz do uwierzytelniania i autoryzacji dostępu do zasobów i usług w systemach informatycznych i serwisach internetowych.
Z zakresu umiejętności:	
PEU_U01	Student potrafi wykorzystywać narzędzia do zabezpieczania integralności danych i do ochrony sieci.
Z zakresu kompetencji społecznych:	
PEU_K01	Student dostrzega cel mechanizmów i narzędzi do obrony przed atakami i podwyższania bezpieczeństwa oraz audytu bezpieczeństwa systemów i sieci.

TREŚCI PROGRAMOWE		
Forma zajęć – wykład		Liczba godzin
W1	Wprowadzenie, omówienie zasad zaliczenia zajęć. Bezpieczeństwo podstawowych protokołów i urządzeń sieciowych w poszczególnych warstwach modelu OSI.	3
W2	Narzędzia podnoszące poziom bezpieczeństwa sieci.	3
W3	Tunele VPN i protokół IPsec.	3
W4	Zapory sieciowe (firewall).	3
W5	Bezpieczeństwo infrastruktury sieci bezprzewodowych i urządzeń mobilnych (WiFi, Bluetooth).	2
W6	Bezpieczeństwo usług VoIP. Podsumowanie, zaliczenie.	2
Razem		16

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
1.	Prezentacja treści z wykorzystaniem multimediiów.
2.	Dyskusja.
3.	Analiza przypadku.

METODY I FORMY OCENY
OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Formy oceny (F lub P)*	Numer efektu uczenia (przedmiotowego)	Metody oceny osiągnięcia efektu uczenia
F w	PEU_W01, PEU_W02, PEU_U01, PEU_K01	Dyskusja, analiza przypadku podczas wykładu.
P w	PEU_W01, PEU_W02, PEU_U01, PEU_K01	Zaliczenie w formie pisemnej.

*F – ocena formująca (w trakcie semestru), P – ocena podsumowująca (na koniec semestru)

KRYTERIA OCENY
OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Nr PEU	Ocena dostateczna	Ocena dobra	Ocena bardzo dobra
PEU_W01	Student posiada podstawową wiedzę o sposobach, mechanizmach i narzędziach do zapewniania poufności i integralności informacji oraz do uwierzytelniania i autoryzacji dostępu do zasobów i usług w systemach informatycznych i serwisach internetowych.	Student opanował wymaganą wiedzę o sposobach, mechanizmach i narzędziach do zapewniania poufności i integralności informacji oraz do uwierzytelniania i autoryzacji dostępu do zasobów i usług w systemach informatycznych i serwisach internetowych.	Student opanował wymaganą wiedzę o sposobach, mechanizmach i narzędziach do zapewniania poufności i integralności informacji oraz do uwierzytelniania i autoryzacji dostępu do zasobów i usług w systemach informatycznych i serwisach internetowych i potrafi ją odnieść do zastosowań praktycznych.
PEU_W02	Student ma podstawową wiedzę o atakach na komputery, systemy i oprogramowanie sieci oraz na usługi komunikacyjne, informacyjne i biznesowe dostępne w Internecie, oraz ma wiedzę o atakach za pomocą wirusów, robaków i ukrytych kanałów komunikacyjnych.	Student opanował wymaganą wiedzę o atakach na komputery, systemy i oprogramowanie sieci oraz na usługi komunikacyjne, informacyjne i biznesowe dostępne w Internecie oraz ma wiedzę o atakach za pomocą wirusów, robaków i ukrytych kanałów komunikacyjnych.	Student opanował wymaganą wiedzę o atakach na komputery, systemy i oprogramowanie sieci oraz na usługi komunikacyjne, informacyjne i biznesowe dostępne w Internecie, oraz ma wiedzę o atakach za pomocą wirusów, robaków i ukrytych kanałów komunikacyjnych i potrafi ją odnieść do zastosowań praktycznych.
PEU_U01	Student potrafi znaleźć odniesienia do praktycznego wykorzystania wiedzy zdobytej podczas wykładu.	Student potrafi wykorzystać w praktyce większość wiedzy zdobytej podczas wykładu.	Student sprawnie potrafi wykorzystać w praktyce wiedzę zdobytą podczas wykładu.
PEU_K01	Student dostrzega cel stosowania mechanizmów i narzędzi ochronnych oraz narzędzi audytowych bezpieczeństwa systemów i sieci.	Dodatkowo dostrzega, że ich celem jest obrona przed atakami i podwyższanie bezpieczeństwa.	Dodatkowo jest gotów podejmować działania z zakresu cyberbezpieczeństwa z własnej inicjatywy w środowisku pracy.

LITERATURA PODSTAWOWA

E. Cole, R. L. Krutz, J. Conley, Bezpieczeństwo sieci. Biblia, Helion 2005.
J. Stokłosa, Bezpieczeństwo danych w systemach informatycznych, PWN, 2001.

LITERATURA UZUPEŁNIAJĄCA

T. Polaczek, Audyt bezpieczeństwa informacji w praktyce. Helion, Gliwice, 2006.
A. Białas (red.), Podstawy bezpieczeństwa systemów teleinformatycznych.
Wyd. Prac. Komp. J. Skalmierskiego, Gliwice, 2002.

MACIERZ POWIĄZANIA

EFEKTÓW UCZENIA DLA PRZEDMIOTU BEZPIECZEŃSTWO SIECI KOMPUTEROWYCH Z EFEKTAMI UCZENIA NA KIERUNKU INFORMATYKA

Przedmiotowy efekt uczenia	Odniesienie przedmiotowego efektu do efektów uczenia zdefiniowanych dla kierunku studiów i specjalności	Cele przedmiotu	Treści programowe	Numer narzędzia dydaktycznego
PEU_W01	K_W02	C1-3	W1-6	1-3
PEU_W02	K_W03, K_W05	C1-3	W1-6	1-3
PEU-U01	K_U07, K_U08	C3	W1-6	1-3
PEU_K01	K_K03, K_K04	C1-3	W1-6	1-3