

KARTA PRZEDMIOTU

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

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

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

Kierunek studiów: **Informatyka**

Poziom studiów: **Studia I stopnia**

Forma studiów: **Niestacjonarne**

Profil: **Praktyczny**

Specjalność: **Systemy i sieci komputerowe**

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	8		18		
Liczba godzin całkowitego nakładu pracy studenta	50		75		
Forma zaliczenia	Zaliczenie z oceną		Zaliczenie z oceną		
Liczba punktów ECTS	2		3		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

Wiedza i kompetencje z zakresu sieci komputerowych.

Wiedza i kompetencje z zakresu baz danych.

Praktyczne umiejętności z zakresu utrzymania i administrowania systemów operacyjnych Windows i Linux.

CELE PRZEDMIOTU

C1	Zdobycie podstawowej wiedzy o polityce bezpieczeństwa oraz obowiązujących w tym zakresie norm, standardów, schemacie audytu bezpieczeństwa.
C2	Zdobycie umiejętności instalacji, uruchamiania oraz oceny możliwości funkcjonalnych i wydajności narzędzi programowych do podwyższania bezpieczeństwa w typowych organizacjach.
C3	Zdobycie wiedzy na temat aktualnych zagrożeń, występujących trendów i sposobów obrony.

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 ma wiedzę 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.
PEU_W03	Student ma wiedzę z zakresu podstaw kryptografii, szyfrowania symetrycznego i asymetrycznego oraz o infrastrukturze klucza publicznego PKI.
Z zakresu umiejętności:	
PEU_U01	Student potrafi instalować i uruchamiać narzędzia programowe do podwyższania bezpieczeństwa.
PEU_U02	Student potrafi wykorzystywać funkcjonalności mechanizmów i narzędzi do obrony przed atakami i podwyższania bezpieczeństwa oraz do audytu bezpieczeństwa systemów i sieci.
Z zakresu kompetencji społecznych:	
PEU_K01	Student rozumie cel mechanizmów i narzędzi do obrony przed atakami i podwyższania bezpieczeństwa i gotów jest je dobierać w zależności od potrzeb organizacji.

TREŚCI PROGRAMOWE		
Forma zajęć – wykład		Liczba godzin
W1	Wprowadzenie, omówienie zasad zaliczenia przedmiotu. Zagadnienia podstawowe dot. bezpieczeństwa. Polityka bezpieczeństwa, normy, audyt bezpieczeństwa.	2
W2	Koncepcja bezpieczeństwa systemów i sieci. Klasyfikacja ataków.	1
W3	Bezpieczeństwo fizyczne.	1
W4	Poufność informacji, uwierzytelnianie, autoryzacja, integralność, ataki na system operacyjny – wirusy, robaki, ukryte kanały komunikacyjne.	1
W5	Bezpieczeństwo sieci i stosu protokołów TCP/IP, ataki na komunikację i protokół IP, Bezpieczeństwo sieci bezprzewodowych.	1
W6	Podstawy kryptografii, szyfrowanie symetryczne i asymetryczne, infrastruktura PKI. Bezpieczeństwo wyszukiwarek internetowych, aplikacji i usług sieciowych, WWW, poczty elektronicznej, komunikatorów, bezpieczeństwo bankowości elektronicznej.	1
W7	Podsumowanie, zaliczenie.	1
Razem		8

TREŚCI PROGRAMOWE		
Forma zajęć – laboratorium		Liczba godzin
L1	Wprowadzenie, laboratorium i projektu, uszczegółowienie warunków zaliczeń zajęć, omówienie platformy sprzętowej, programowej i sieciowej laboratorium i do projektu.	2
L2	Wykonywanie w środowisku Linux kopii zapasowych wybranych plików. Obsługa crontab.	2
L3	Bezpieczeństwo sieci. Filtrowanie pakietów (firewall).	2
L4	Konfigurowanie łącza VPN, generowanie kluczy i certyfikatów potrzebnych do tego połączenia.	4
L5	Bezpieczeństwo obrona baz danych przed XSS i SQL Injection, zabezpieczenia przed XSS i SQL Injection w przeglądarkach internetowych.	3
L6	Instalacja narzędzi zwiększających poziom bezpieczeństwa, konfiguracja audytu dla zasobu sieciowego, wprowadzenie polis dostępu w systemie Windows.	3
L7	Podsumowanie, zaliczenie.	2
Razem		18

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
1.	Prezentacja treści z wykorzystaniem multimediiów.
2.	Laboratorium z wykorzystaniem stanowiska laboratoryjnego i oprogramowania komputerowego.
3.	Realizacja ćwiczeń podczas zajęć.
4.	Praca własna – studiowanie aktualnej literatury przedmiotu, źródeł internetowych.
5.	Dyskusja dydaktyczna.

METODY I FORMY OCENY
OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Formy oceny (F lub P)*	Numer efektu uczenia (przedmiotowego)	Metody oceny osiągnięcia efektu uczenia
F I	PEU_W01, PEU_U01, PEU_U02, PEU_K01	Ocena za aktywną realizację ćwiczeń laboratoryjnych.
P I	PEU_W01, PEU_U01, PEU_U02, PEU_K01	Ocena wykonania zadania na zajęciach zaliczeniowych.
F w	PEU_W01, PEU_W02, PEU_W03, PEU_K01	Dyskusja w trakcie zajęć.
P w (z uwzględnieniem PI)	PEU_W01, PEU_W02, PEU_W03, PEU_K01	Zaliczenie w formie pisemnej.

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

KRYTERIA OCENY
OŚIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Nr PEU	Ocena dostateczna	Ocena dobra	Ocena bardzo dobra
PEU_W01	Student posiada wiedzę z zakresu inżynierii bezpieczeństwa w sieciach komputerowych oraz kryptografii w systemach sieciowych i internetowych, oraz potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z zakresu bezpieczeństwa systemów i sieci.	Student nie tylko posiada wiedzę z zakresu inżynierii bezpieczeństwa w sieciach komputerowych oraz kryptografii w systemach sieciowych i internetowych, oraz potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z zakresu bezpieczeństwa systemów i sieci, ale i potrafi je zastosować.	Student nie tylko posiada wiedzę z zakresu inżynierii bezpieczeństwa w sieciach komputerowych oraz kryptografii w systemach sieciowych i internetowych, oraz potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z zakresu bezpieczeństwa systemów i sieci, ale i potrafi je zastosować do projektowania, wdrożenia i audytu bezpieczeństwa.
PEU_W02	Student ma wiedzę o atakach komputery, systemy i oprogramowanie sieci oraz na usługi komunikacyjne, informacyjne i biznesowe dostępne w Internecie, oraz posiada wiedzę o atakach za pomocą wirusów, robaków i ukrytych kanałów komunikacyjnych oraz potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy o takich atakach.	Student nie tylko ma wiedzę o atakach komputery, systemy i oprogramowanie sieci oraz na usługi komunikacyjne, informacyjne i biznesowe dostępne w Internecie, oraz posiada wiedzę o atakach za pomocą wirusów, robaków i ukrytych kanałów komunikacyjnych oraz potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy o takich atakach, ale i potrafi je wykrywać.	Student nie tylko ma wiedzę o atakach komputery, systemy i oprogramowanie sieci oraz na usługi komunikacyjne, informacyjne i biznesowe dostępne w Internecie, oraz posiada wiedzę o atakach za pomocą wirusów, robaków i ukrytych kanałów komunikacyjnych oraz potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy o takich atakach, potrafi je wykrywać, ale i potrafi im zapobiegać.
PEU_W03	Student ma wiedzę z zakresu podstaw kryptografii, szyfrowania symetrycznego i asymetrycznego oraz o infrastrukturze klucza publicznego PKI, potrafi wyszukiwać informacje i pozyskiwać wiedzę z tego zakresu.	Student ma nie tylko wiedzę z zakresu podstaw kryptografii, szyfrowania symetrycznego i asymetrycznego oraz o infrastrukturze klucza publicznego PKI, potrafi wyszukiwać informacje i pozyskiwać wiedzę z tego zakresu, ale i potrafi realizację infrastruktury PKI oceniać.	Student ma nie tylko wiedzę z zakresu podstaw kryptografii, szyfrowania symetrycznego i asymetrycznego oraz o infrastrukturze klucza publicznego PKI, potrafi wyszukiwać informacje i pozyskiwać wiedzę z tego zakresu, potrafi realizację infrastruktury PKI oceniać, ale i wie jak systemy PKI wdrażać.
PEU_U01	Student potrafi instalować i uruchamiać narzędzia programowe do podwyższania bezpieczeństwa, oraz potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z zakresu systemów wzmacniania bezpieczeństwa.	Student nie tylko umie instalować i uruchamiać narzędzia programowe do podwyższania bezpieczeństwa, potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z zakresu systemów wzmacniania bezpieczeństwa, ale i potrafi je zastosować.	Student nie tylko umie instalować i uruchamiać narzędzia programowe do podwyższania bezpieczeństwa, potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z zakresu systemów wzmacniania bezpieczeństwa, ale i potrafi je zastosować w procesie projektowania i wdrażania infrastruktury bezpieczeństwa.

PEU_U02	Student potrafi wykorzystywać funkcjonalności mechanizmów i narzędzi do obrony przed atakami i podwyższania bezpieczeństwa oraz do audytu bezpieczeństwa systemów i sieci, potrafi również poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z tego zakresu.	Student nie tylko potrafi wykorzystywać funkcjonalności mechanizmów i narzędzi do obrony przed atakami i podwyższania bezpieczeństwa oraz do audytu bezpieczeństwa systemów i sieci, potrafi również poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z tego zakresu, ale i potrafi je zastosować.	Student nie tylko potrafi wykorzystywać funkcjonalności mechanizmów i narzędzi do obrony przed atakami i podwyższania bezpieczeństwa oraz do audytu bezpieczeństwa systemów i sieci, potrafi również poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z tego zakresu, potrafi je zastosować, ale i zastosować w procesie projektowania, wdrażania i utrzymania infrastruktury bezpieczeństwa.
PEU_K01	Student jest gotów do stosowania mechanizmów i narzędzi ochronnych oraz narzędzi audytowych bezpieczeństwa systemów i sieci oraz potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z zakresu obrony przed atakami i podwyższania bezpieczeństwa systemów i sieci.	Student nie tylko jest gotów do stosowania mechanizmów i narzędzi ochronnych oraz narzędzi audytowych bezpieczeństwa systemów i sieci oraz potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z zakresu obrony przed atakami i podwyższania bezpieczeństwa systemów i sieci, ale i potrafi je zastosować.	Student nie tylko jest gotów do stosowania mechanizmów i narzędzi ochronnych oraz narzędzi audytowych bezpieczeństwa systemów i sieci oraz potrafi poszukiwać literatury, dokumentacji i innych źródeł i wiedzy z zakresu obrony przed atakami i podwyższania bezpieczeństwa systemów i sieci, ale i potrafi je zastosować do projektowania, wdrożenia infrastruktury bezpieczeństwa sieci i systemów informatycznych.

LITERATURA PODSTAWOWA
Cole E., Krutz R., Conley J., Bezpieczeństwo sieci. Biblia. Helion, Gliwice, 2005. Krawiec J. Cyberbezpieczeństwo. Podejście systemowe, Oficyna Wydawnicza Politechniki Warszawskiej, 2019.
LITERATURA UZUPEŁNIAJĄCA
Polaczek T., Audyt bezpieczeństwa informacji w praktyce. Helion, Gliwice, 2006.
ŹRÓDŁA CYFROWE
https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa https://niebezpiecznik.pl https://sekurak.pl https://zaufanatrzeciastrona.pl

**MACIERZ POWIĄZANIA EFEKTÓW UCZENIA DLA PRZEDMIOTU
BEZPIECZEŃSTWO SYSTEMÓW I 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_W03	C1	W1, W2	1, 2, 5
PEU_W02	K_W05	C3	W2, W5, W7	1, 2, 5

PEU_W03	K_W03, K_W05	C1, C3	W3, W4, W5, W6	1, 2, 4, 5
PEU_U01	K_U01, K_U07	C2	L1-L6	3, 4, 5
PEU_U02	K_U08	C2	L1-L6	2, 3, 4, 5
PEU_K01	K_K02	C1	L6, W1	1, 2, 3, 5