WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ I ZARZĄDZANIA WIT
POD AUSPICJAMI POLSKIEJ AKADEMII NAUK
01-447 Warszawa \ ul. Newelska 6 \ www.WIT.edu.pl

WYDZIAŁ INFORMATYCZNYCH TECHNIK ZARZĄDZANIA

Kierunek studiów	Informatyczne Techniki Zarządzania
Profil	Praktyczny
Stopień studiów	2-go stopnia
Forma studiów	niestacjonarne

Sylabus przedmiotu

Technologie kryptograficzne

1. Dane podstawowe

Status programowy przedmiotu	Blok A: Technologie i systemy informatyczne
Rodzaj przedmiotu	Obligatoryjny
Kod przedmiotu	TZM-TKR-ZC
Rok studiów	1
Semestr	1
Osoba odpowiedzialna za przedmiot	dr inż. Piotr Mroczkowski
Język wykładowy	polski

2. Wymiar godzin i forma zajęć

Rodzaj	Liczba godzin
Wykład	16
Laboratorium	16
Projekt	8
Razem godzin	40

3. Cele przedmiotu

Kod	Cel
CP1	Zapoznanie z zagadnieniami bezpieczeństwa informacji.
CP2	Zapoznanie z zagadnieniami kryptologii (kryptografii i kryptoanalizy).
CP3	Zapoznanie ze współczesnymi algorytmami kryptograficznymi.
CP4	Zapoznanie ze współczesnymi protokołami kryptograficznymi.
CP5	Zapoznanie z technologiami kryptograficznej ochrony informacji.

4. Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

Brak wymagań wstępnych.

5. Efekty uczenia się

Wiedza

Kod	Student zna i rozumie:	Realizuje cel	Efekty kierunkowe
EU-W1	Student zna i rozumie zagrożenia dla bezpieczeństwa informacji.	CP1	K1P_W11
EU-W2	Student zna i rozumie cele i zadania kryptologii.	CP1, CP2	K1P_W11
EU-W3	Student zna i rozumie współczesne algorytmy kryptograficzne.	CP1, CP2, CP3	K1P_W11
EU-W4	Student zna i rozumie wybrane protokoły kryptograficzne.	CP3, CP4	K1P_W11
EU-W5	Student zna i rozumie współczesne technologie kryptograficzne.	CP3, CP4, CP5	K1P_W11

Umiejętności

Kod	Student potrafi:	Realizuje cel	Efekty kierunkowe
EU-U1	Student potrafi definiować zagrożenia dla bezpieczeństwa informacji i im zapobiegać.	CP1	K1P_U11, K2P_U01
EU-U2	Student potrafi zdefiniować cele i zadania kryptologii.	CP1, CP2	K1P_U11, K2P_U01
EU-U3	Student potrafi wykorzystać współczesne algorytmy kryptograficzne do zapewnienia kryptograficznej ochrony informacji.	CP2, CP3	K1P_U11, K2P_U01
EU-U4	Student potrafi wykorzystać współczesne protokoły kryptograficzne do zapewnienia kryptograficznej ochrony informacji.	CP2	K1P_U11, K2P_U01
EU-U5	Student potrafi wykorzystać współczesne technologie kryptograficzne do zapewnienia kryptograficznej ochrony informacji.	CP3, CP4, CP5	K1P_U11, K2P_U01

Kompetencje

Kod	Student jest gotów do:	Realizuje cel	Efekty kierunkowe
EU-K1	Student jest gotów do zapobiegania zagrożeniom dla bezpieczeństwa informacji.	CP1, CP2, CP3, CP4, CP5	K1P_K07, K2P_K06
EU-K2	Student jest gotów do zapewnienia kryptograficznej ochrony informacji przy wykorzystaniu współczesnych technologii kryptograficznych.	CP1, CP2, CP3, CP4, CP5	K1P_K07, K2P_K06

6. Treści programowe

Kod	Tematyka	wykład	projekt	laboratorium	Realizuje efekt
TP1	Wprowadzenie do przedmiotu. Omówienie podstawowych zagrożeń dla bezpieczeństwa informacji oraz metod im zapobiegania. Przedstawienie podstawowych pojęć i definicji z dziedziny kryptologii.	2	1	2	EU-K1, EU-U1, EU-U2, EU-W1, EU-W2
TP2	Symetryczne techniki kryptograficzne zapewnienia poufności oparte na szyfrach blokowych. Omówienie idei szyfrowania blokowego oraz zapoznanie studentów ze współczesnymi szyframi blokowymi.	2	1	2	EU-K1, EU-K2, EU-U3, EU-W3
TP3	Symetryczne techniki kryptograficzne zapewnienia poufności oparte na szyfrach strumieniowych. Omówienie idei szyfrowania strumieniowego oraz zapoznanie studentów ze współczesnymi szyframi strumieniowymi.	2	1	2	EU-K1, EU-K2, EU-U3, EU-W3
TP4	Techniki kryptograficzne zapewnienia integralności i uwierzytelnienia: funkcje skrótu jako techniki kryptograficzne realizujące integralność danych, kody uwierzytelniania wiadomości MAC jako techniki kryptograficzne realizujące integralność i uwierzytelnienie danych.	2	1	2	EU-K1, EU-K2, EU-U3, EU-W3
TP5	Asymetryczne techniki kryptograficzne zapewnienia poufności, intergralności i uwierzytelnienia oparte na kryptosystemie RSA. Omówienie generacji kluczy asymetrycznych RSA, idei szyfrowania i deszyfrowania RSA oraz generacji i weryfikacji podpisów cyfrowych RSA. Przedstawienie podstawowych własności i parametrów bezpieczeństwa algorytmu RSA.	2	1	2	EU-K1, EU-K2, EU-U3, EU-U4, EU-W3, EU-W4

Kod	Tematyka	wykład	projekt	laboratorium	Realizuje efekt
TP6	Techniki zarządzania kryptograficznymi danymi kluczowymi. Omówienie problemu dystrybucji kluczy kryptograficznych. Omówienie algorytmu Diffiego-Hellmana jako przykład protokołu uzgadniania klucza.	2	1	2	EU-K1, EU-K2, EU-U3, EU-U4, EU-U5, EU-W3, EU-W4, EU-W5
TP7	Techniki kryptograficzne zapewniające bezpieczeństwo transportu danych: protokół TLS i SSH, HTTPS.	2	1	2	EU-K1, EU-K2, EU-U3, EU-U4, EU-U5, EU-W3, EU-W4, EU-W5
TP8	Techniki kryptograficzne zapewniające bezpieczeństwo transportu danych: protokół TLS i SSH, HTTPS.	2	1	2	EU-K1, EU-K2, EU-U3, EU-U4, EU-U5, EU-W3, EU-W4, EU-W5

Razem godzin: 40

7. Metody kształcenia

Kod	Metoda
MK1	wykład wsparty prezentacją komputerową
MK2	prezentacje studentów prezentowane za zajęciach
MK3	ćwiczenia laboratoryjne
MK4	sprawozdanie z ćwiczeń laboratoryjnych
MK5	(mini)projekt

8. Nakład pracy studenta

Aktywność studenta	Obciążenie
Przygotowanie do laboratorium	12
Przygotowanie do projektu	8
Przygotowanie do wykładu	8
Przygotowanie do zaliczenia	32
Praca związana z: laboratorium	16
Praca związana z: projekt	8
Praca związana z: wykład	16
Liczba punktów ECTS (1 punkt=25h)	4
Procentowy udział pracy własnej studenta w sumarycznym obciążeniu studenta	68,00%
Sumaryczne obciążenie pracą studenta	100

9. Status zaliczenia przedmiotu

Na ocenę końcową składają się: wyniki kolokwium zaliczeniowego (może być przeprowadzone w postaci ustnej), wyniki z laboratorium, wyniki z prowadzonych prezentacji, wyniki (mini)projektu.

Forma studiów	Egzamin	Praca egzaminacyjna	Zaliczenie	Praca zaliczeniowa
niestacjonarne			×	

10. Metody weryfikacji efektów uczenia się

Składowe oceny końcowej

Forma sprawdzenia	Wybrana forma	Punktacja	Realizuje efekt
Egzamin pisemny	×	50	EU-U4, EU-U3, EU-U5, EU-U2, EU-K2, EU-K1, EU-U1, EU-W5, EU-W4, EU-W3, EU-W2, EU-W1
Egzamin ustny			
Sprawdzian pisemny			
Zaliczeniowy przegląd prac			
Referat pisemny			
Referat ustny			
Kolokwium			
Praca domowa			
Miniprojekt			
Praca na zajęciach			
Projekt z dokumentacją	×	30	EU-U4, EU-U3, EU-U5, EU-U2, EU-K2, EU-K1, EU-U1, EU-W5, EU-W4, EU-W3, EU-W2, EU-W1
Ustna prezentacja projektu			
Obecność na zajęciach			
Sprawdzian ustny			
Kartkówka			
Aktywność na zajęciach			
Egzaminacyjny przegląd prac			
Sprawozdanie z praktyki zawodowej			
Prezentacja indywidualna	×	20	EU-U4, EU-U3, EU-U5, EU-W5, EU-W4, EU-W3
Prezentacja zespołowa			

Zasady wyliczania oceny z przedmiotu

Zakres punktów	Ocena
0 – 50	2,0
51 – 60	3,0
61 – 70	3,5
71 – 80	4,0
81 – 90	4,5
91 – 100	5,0

11. Macierz realizacji przedmiotu

Efekt uczenia się	Cel przedmiotu	Treści programowe	Metody kształcenia
EU-W1	CP1	TP1	MK1, MK2, MK3, MK4, MK5
EU-W2	CP1, CP2	TP1	MK1, MK2, MK3, MK4, MK5
EU-W3	CP1, CP2, CP3	TP2, TP3, TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4, MK5
EU-W4	CP3, CP4	TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4, MK5
EU-W5	CP3, CP4, CP5	TP6, TP7, TP8	MK1, MK2, MK3, MK4, MK5
EU-U1	CP1	TP1	MK1, MK2, MK3, MK4, MK5
EU-U2	CP1, CP2	TP1	MK1, MK2, MK3, MK4, MK5
EU-U3	CP2, CP3	TP2, TP3, TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4, MK5
EU-U4	CP2	TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4, MK5

Efekt uczenia się	Cel przedmiotu	Treści programowe	Metody kształcenia
EU-U5	CP3, CP4, CP5	TP6, TP7, TP8	MK1, MK2, MK3, MK4, MK5
EU-K1	CP1, CP2, CP3, CP4, CP5	TP1, TP2, TP3, TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4, MK5
EU-K2	CP1, CP2, CP3, CP4, CP5	TP2, TP3, TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4, MK5

12. Odniesienie efektów uczenia się

Efekt uczenia się	Efekty kształcenia dla kierunku studiów	Charakterystyki drugiego stopnia w obszarze kształcenia
EU-W1	K1P_W11	P6S_WG
EU-W2	K1P_W11	P6S_WG
EU-W3	K1P_W11	P6S_WG
EU-W4	K1P_W11	P6S_WG
EU-W5	K1P_W11	P6S_WG
EU-U1	K2P_U01, K1P_U11	P6S_UW, P7S_UW
EU-U2	K2P_U01, K1P_U11	P6S_UW, P7S_UW
EU-U3	K2P_U01, K1P_U11	P6S_UW, P7S_UW
EU-U4	K2P_U01, K1P_U11	P6S_UW, P7S_UW
EU-U5	K2P_U01, K1P_U11	P6S_UW, P7S_UW
EU-K1	K2P_K06, K1P_K07	P6S_KO, P7S_KO
EU-K2	K2P_K06, K1P_K07	P6S_KO, P7S_KO

13. Literatura

Literatura podstawowa

1. Marcin Karbowski, Podstawy kryptografii, Helion, 2014
2. William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii., Helion, 2012
3. William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji., Helion, 2012

Literatura uzupełniająca

1. Jean-Philippe Aumasson, Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfowania., PWN, 2018

14. Informacje o nauczycielach akademickich

Osoby odpowiedzialne za przedmiot

1. dr inż. Piotr Mroczkowski

Osoby prowądzace przedmiot

1. dr inż. Piotr Mroczkowski