KARTA PRZEDMIOTU

I. Dane podstawowe

Nazwa przedmiotu	Ochrona danych
Nazwa przedmiotu w języku angielskim	Data protection
Kierunek studiów	informatyka
Poziom studiów (I, II, jednolite magisterskie)	I stopnia
Forma studiów (stacjonarne, niestacjonarne)	stacjonarne
Dyscyplina	informatyka
Język wykładowy	polski

Koordynator przedmiotu	Prof. dr hab. Pavel Urbanovich

Forma zajęć *(katalog zamknięty ze słownika)*	Liczba godzin	semestr	Punkty ECTS
wykład	30	III	5
konwersatorium			
ćwiczenia			
laboratorium	30	III	
warsztaty			
seminarium			
proseminarium			
lektorat			
praktyki			
zajęcia terenowe			
pracownia dyplomowa			
translatorium			
wizyta studyjna			

Wymagania wstępne	1 - Algorytmy i struktury danych. 2 - Podstawy programowania. 3 - Znajomość podstaw matematyki oraz programowania.

II. Cele kształcenia dla przedmiotu

1 - Zapoznanie studentów z kopiami bezpieczeństwa oraz technologią RAID.
2 - Zrozumienie przez studenta teoretycznych i praktycznych aspektów kodowania nadmiarowego, kompresji danych oraz kryptografii.
3 - Analiza bezpieczeństwa systemów operacyjnych i sieciowych.

III. Efekty uczenia się dla przedmiotu wraz z odniesieniem do efektów kierunkowych

Symbol	Opis efektu przedmiotowego	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Student wie jakie są rodzaje kopii bezpieczeństwa	K_W03, K_W10
W_02	Student zna technologię RAID	K_W04, K_W10
W_03	Student zna algorytmy kodowania korekcyjnego	K_W03, K_W04, K_W06
W_04	Student zna najważniejsze aspekty współczesnej kryptografii	K_W03, K_W04, K_W06
UMIEJĘTNOŚCI		
U_01	Student potrafi utworzyć kopię zapasową	K_U02
U_02	Student umie wybrać odpowiednią technologię RAID	K_U02
U_03	Student potrafi zaimplementować podstawowe algorytmy kodowania korekcyjnego	K_U02
U_04	Student potrafi zaimplementować podstawowe algorytmy kryptografii symetrycznej i asymetrycznej	K_U02
KOMPETENCJE SPOŁECZNE		
K_01	Student ma świadomość zdobytej wiedzy i umiejętności	K_K01
K_02	Student rozumie potrzebę dokształcania się i podnoszenia kompetencji zawodowych	K_K01
K_03	Student wie jak identyfikować i rozwiązywać podstawowe problemy	K_K01
K_04	Student pracuje sprawnie, w zespole i indywidualnie, umiejętnie ocenia priorytety w realizacji projektu	K_K05

IV. Opis przedmiotu/ treści programowe

1. Metody ochrony danych przed ich zniszczeniem.
2. Rodzaje i nośniki kopii bezpieczeństwa. Metody tworzenia kopii danych.
3. Technologia RAID.
4. Badanie własności entropii Shannona i Hartley\'a.
5. Błędy w informacji.
6. Teoretyczne podstawy i klasyfikacja metod kodowania nadmiarowego.
7. Kodowanie nadmiarowe przy użyciu kodu prostej parzystości i kodu Hamminga.
8. Teoretyczne podstawy kryptografii.
9. Kryptografia symetryczna i asymetryczna.
10. Szyfrowanie i deszyfrowanie informacji. Praktyczne zastosowania kryptografii.
11. Omówienie algorytmów AES i RSA.
12. Podpis cyfrowy.

V. Metody realizacji i weryfikacji efektów uczenia się

Symbol efektu	Metody dydaktyczne *(lista wyboru)*	Metody weryfikacji *(lista wyboru)*	Sposoby dokumentacji *(lista wyboru)*
WIEDZA			
W_01, W_02,	- Analiza laboratoryjna, - dyskusja	- kolokwium, - sprawdzian pisemny,	- uzupełnione i ocenione kolokwium,

W_03, W_04	- praca pod kierunkiem, - wykład konwencjonalny, - wykład konwersatoryjny, - wykład problemowy	- przygotowanie/ wykonanie projektu	- oceniony tekst pracy pisemnej, - protokół, - wydruk,
UMIEJĘTNOŚCI			
U_01, U_02, U_03, U_04	- analiza tekstu, - ćwiczenia laboratoryjne, - ćwiczenia praktyczne, - dyskusja, - metoda problemowa, - metoda projektu, - design thinking	- kolokwium, - sprawdzian pisemny, - przygotowanie/ wykonanie projektu	- uzupełnione i ocenione kolokwium, - oceniony tekst pracy pisemnej, - protokół, - wydruk,
KOMPETENCJE SPOŁECZNE			
K_01, K_02, K_03, K_04	- ćwiczenia laboratoryjne, - dyskusja, - metoda obserwacji uczestniczącej, - metoda problemowa, - metoda projektu, - design thinking	- kolokwium, - sprawdzian pisemny, - przygotowanie/ wykonanie projektu	- uzupełnione i ocenione kolokwium, - oceniony tekst pracy pisemnej, - protokół, - wydruk,

VI. Kryteria oceny, wagi…

Ocena dostateczna
(W) - Student wie jakie są rodzaje kopii bezpieczeństwa
(W) - Student zna technologie RAID
(U) - Student potrafi utworzyć kopię zapasową
(U) - Student umie wybrać odpowiednią technologię RAID
(K) - Student ma świadomość zdobytej wiedzy i umiejętności

Ocena dobra
(W) - Student wie jakie są rodzaje kopii bezpieczeństwa
(W) - Student zna technologie RAID
(W) - Student zna algorytmy kodowania korekcyjnego
(U) - Student potrafi utworzyć kopię zapasową
(U) - Student umie wybrać odpowiednią technologię RAID
(U) - Student potrafi zaimplementować podstawowe algorytmy kodowania korekcyjnego
(K) - Student ma świadomość zdobytej wiedzy i umiejętności
(K) - Student rozumie potrzebę dokształcania się i podnoszenia kompetencji zawodowych

Ocena bardzo dobra
(W) - Student wie jakie są rodzaje kopii bezpieczeństwa
(W) - Student zna technologie RAID
(W) - Student zna algorytmy kodowania korekcyjnego
(W) - Student zna najważniejsze aspekty współczesnej kryptografii
(U) - Student potrafi utworzyć kopię zapasową
(U) - Student umie wybrać odpowiednią technologię RAID
(U) - Student potrafi zaimplementować podstawowe algorytmy kodowania korekcyjnego
(U) - Student potrafi zaimplementować podstawowe algorytmy kryptografii symetrycznej i asymetrycznej
(K) - Student ma świadomość zdobytej wiedzy i umiejętności

(K) - Student rozumie potrzebę dokształcania się i podnoszenia kompetencji zawodowych
(K) - Student wie jak identyfikować i rozwiązywać podstawowe problemy

Sposoby weryfikacji zakładanych efektów kształcenia:
Przygotowanie 6 krótkich sprawozdań wraz z programami z zakresu:
1. Technologia RAID
2. Entropia oraz rozkład prawdopodobieństw liter w danym języku
3. Kody korekcyjne - kod Hamminga
4. Algorytm Euklidesa oraz rozszerzony algorytm Euklidesa
5. Szyfrowanie i deszyfrowanie - metody symetryczne
6. Szyfrowanie i deszyfrowanie - metody asymetryczne

Ocena końcowa to średnia z zadanych sprawozdań (włącznie z programami). Aktywność na zajęciach wpływa na ocenę końcową, do 0,5 stopnia w górę w zależności od poziomu aktywności.

Obciążenie pracą studenta

Forma aktywności studenta	Liczba godzin
Liczba godzin kontaktowych z nauczycielem	Wykład 30 Ćwiczenia 30 Konsultacje 30
Liczba godzin indywidualnej pracy studenta	Przygotowanie do zajęć 15 Studiowanie literatury 15 Przygotowanie do kolokwiów i egzaminu 20

VII. Literatura

Literatura podstawowa
1. Douglas R. Stinson, Kryptografia, Wydawnictwo: WNT, 2005 2. Mirosław Kutyłowski, Willy-B. Strothman, Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, RM 1999. 3. Jean-Philippe Aumasson, Nowoczesna kryptografia : praktyczne wprowadzenie do szyfrowania, przekład Małgorzata Dąbkowska-Kowalik i Witold Sikorski, PWN 2018 4. Bruce Schneier, Kryptografia dla praktyków : protokoły, algorytmy i programy źródłowe w języku C, przekład Roman Rykaczewski, Ryszard Sobczak, Piotr Szpryngier, Wydawnictwo Naukowo-Techniczne 2002
Literatura uzupełniająca
5. Internet agresja i ochrona, Wydawnictwo Robomatic 1998. 6. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Kryptografia stosowana, Wydawnictwo: WNT 2005 7. Ochrona informacji w sieciach komputerowych. Pod red. P.Urbanowicza, wydawnictwo KUL 2004 8. William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii, przekład Andrzej Grażyński, HELION, 2012