KARTA PRZEDMIOTU

I. Dane podstawowe

Nazwa przedmiotu	Ochrona informacji w sieciach komputerowych
Nazwa przedmiotu w języku angielskim	Information protection in computer networks
Kierunek studiów	Informatyka
Poziom studiów (I, II, jednolite magisterskie)	II
Forma studiów (stacjonarne, niestacjonarne)	stacjonarne
Dyscyplina	Informatyka
Język wykładowy	polski

Koordynator przedmiotu/osoba odpowiedzialna	Br. Jakub Lasyk

Forma zajęć *(katalog zamknięty ze słownika)*	Liczba godzin	semestr	Punkty ECTS
wykład	30	4	Wykład – 6 Ćwiczenia - 0
konwersatorium			
ćwiczenia	30	4	
laboratorium			
warsztaty			
seminarium			
proseminarium			
lektorat			
praktyki			
zajęcia terenowe			
pracownia dyplomowa			
translatorium			
wizyta studyjna			

Wymagania wstępne	W1- Algorytmy i struktury danych, W2 - Podstawy programowania. W3 - Podstawowa wiedza z zakresu arytmetyki modułowej i algebry dużych liczb W4 - Podstawy projektowania i działanie sieci komputerowych

II. Cele kształcenia dla przedmiotu

C1 - Zapoznanie studentów z podstawowymi pojęciami z teorii informacji
C2 - Analiza bezpieczeństwa systemów operacyjnych i sieciowych
C3 - Nabycie przez studenta teoretycznych i praktycznych umiejętności ochrony informacji w sieciach komputerowych
C4 - Zrozumienie przez studenta teoretycznych i praktycznych aspektów nadmiarowego kodowania, kompresji danych i kryptografii
C5 - Nabycie przez studenta teoretycznej i praktycznej umiejętności analizy bezpieczeństwa systemów operacyjnych i sieci

C6 - Nabycie przez studenta teoretycznych i praktycznych umiejętności walki z wirusami komputerowymi

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

Symbol	Opis efektu przedmiotowego	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Student zna podstawowe pojęcia teorii informacji	MAT: K_W01, K_W02, K_W09, K_W11; INF: K_W01, K_W02
W_02	Student zna algorytmy kodowania korekcyjnego oraz kompresji danych	MAT: K_W01, K_W02, K_W11; INF: K_W01, K_W02
W_03	Student zna najważniejsze aspekty współczesnej kryptografii	MAT: K_W01, K_W02, K_W08, K_W10, K_W11, K_W12; INF: K_W05, K_W07
UMIEJĘTNOŚCI		
U_01	Student umie policzyć i zinterpretować entropię języka polskiego	MAT: K_U12; INF: K_U02, K_U03, K_U04
U_02	Student potrafi zaimplementować podstawowe algorytmy kodowania korekcyjnego oraz podstawowe algorytmy kryptografii symetrycznej i asymetrycznej	MAT: K_U19, K_U20, K_U21, K_U22; INF: K_U05, K_U17
U_03	Student potrafi zapewnić podstawowe bezpieczeństwo w systemach operacyjnych i sieciach komputerowych	MAT: K_U12, K_U20; INF: K_U05, K_U17
KOMPETENCJE SPOŁECZNE		
K_01	Student zna ograniczenia własnej wiedzy algorytmicznej i rozumie potrzebę ciągłego dokształcania się i podnoszenia kompetencji zawodowych i osobistych	MAT: K_K01; INF: K_K01
K_02	Student rozumie potrzebę systematycznej pracy i dotrzymywania terminów wykonywanych zadań	MAT: K_K02, K_K05; INF: K_K02, K_K05
K_03	Student rozumie i docenia znaczenie uczciwości intelektualnej w zakresie korzystania z cudzego oprogramowania. Zachowuje się etycznie podczas realizacji projektów algorytmicznych	MAT: K_K03; INF: K_K03
K_04	Student samodzielnie potrafi odnaleźć i wykorzystać różnego rodzaju informacje dotyczące algorytmiki, także w językach obcych	MAT: K_K04; INF: K_K04

IV. Opis przedmiotu/ treści programowe

1. Problem bezpieczeństwa SI.
2. Klasyfikacja i podstawowe parametry SI. Rodzaje kanałów danych. Kanały binarne.
3. Obliczanie ilości informacji w powiadomieniu. Utrata informacji w sieciach komputerowych i ich ocena w oparciu o entropię warunkową.
4. Niezawodność kanałów transmisyjnych z wykorzystaniem kodów nadmiarowych.
5. Teoretyczne podstawy i klasyfikacja kompresji danych.
6. Teoretyczne podstawy kryptografii.
7. Kryptografia symetryczna i asymetryczna.

8. Maszyna Enigma.
9. Funkcja skrótu.
10. Podpis cyfrowy. Podpis cyfrowy oparty na algorytmie RSA i algorytmie ElGamala.
11. Standard i wykorzystanie podpisów cyfrowych w Polsce.
12. Wirusy komputerowe i metody ochrony przed nim.
13. Protokoły Kerberos i SSL.
14. Projektowanie bezpieczeństwa SI i badanie bezpieczeństwa systemów operacyjnych i sieci.
15. Badanie własności entropii Shannona, Hartley\'a oraz entropii binarnej i warunkowej. Obliczanie ilości informacji w powiadomieniu.
16. Kodowanie nadmiarowe przy użyciu kodu parzystości oraz metody Hamminga. Tworzenie aplikacji mających na celu kompresję danych metodami: interwałów, Shannona-Fano, Huffmana.
17. Szyfrowanie i deszyfrowanie informacji. Omówienie i implementacja algorytmu RSA. Badanie bezpieczeństwa systemów operacyjnych i sieciowych.
18. Użycie podpisu cyfrowego, analiza długości hasła, analiza bezpiecznego czasu zastosowania hasła oraz prawdopodobieństwa złamania hasła.
19. Zapoznanie studentów z mechanizmami zabezpieczeń w systemach operacyjnych

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	wykład konwencjonalny wykład konwersatoryjny wykład problemowy praca pod kierunkiem	Kolokwium / Egzamin / Zaliczenie pisemne / Zaliczenie ustne	Uzupełnione i ocenione kolokwium / Protokół / Wydruk / Plik sprawozdania
W_02	wykład konwencjonalny wykład konwersatoryjny wykład problemowy praca pod kierunkiem	kolokwium	Uzupełnione i ocenione kolokwium
W_03	wykład konwencjonalny wykład konwersatoryjny wykład problemowy praca pod kierunkiem	kolokwium	Uzupełnione i ocenione kolokwium
W_04	praca pod kierunkiem	Kolokwium / Sprawdzian pisemny / Sprawdzenie umiejętności praktycznych	Uzupełnione i ocenione kolokwium / Oceniony tekst pracy pisemnej / Sprawdzian pisemny
UMIEJĘTNOŚCI			
U_01	Dyskusja Ćwiczenia laboratoryjne Ćwiczenia praktyczne	Kolokwium / Sprawdzian pisemny	Uzupełnione i ocenione kolokwium / Sprawdzian pisemny
U_02	Dyskusja Ćwiczenia laboratoryjne	Kolokwium / Sprawdzian pisemny / Sprawdzenie umiejętności praktycznych	Uzupełnione i ocenione kolokwium / Test / Sprawdzian pisemny
KOMPETENCJE SPOŁECZNE			
K_01	Dyskusja	Sprawdzian pisemny	Sprawdzian pisemny

VI. Kryteria oceny, wagi…

Ćwiczenia: Zaliczenie – 2 kolokwia (po 50%) na 6. i 12. ćwiczeniach, kolokwium może być przesunięte na inny termin po uzgodnieniu ze studentami.

Wykład: Egzamin (dla osób, które zaliczyły ćwiczenia) składa się z dwóch części: praktycznej (50%) – weryfikującej umiejętności zastosowania wiedzy podanej na wykładzie i ćwiczeniach, pisemnej (50%) – sprawdzającej wiedzę podaną na wykładzie

Ocena niedostateczna (poniżej 50% punktów)

(W) - Student nie potrafi omówić nawet podstawowych zagadnień związanych z ochroną informacji w sieciach komputerowych.

(U) - Student nie potrafi omówić i zaimplementować żadnego rozwiązana z zakresu ochrony informacji.

(K) - Student nie rozumie potrzeby dokształcania się.

Ocena dostateczna (50% - 75% punktów)

(W) - Student potrafi omówić podstawowe zagadnienia związane z ochroną informacji w sieciach k(U) - Student potrafi omówić i zaimplementować proste rozwiązana z zakresu ochrony informacji.

(K) - Student rozumie potrzebę dokształcania się.

Ocena dobra (76% - 90% punktów)

(W)- Student potrafi omówić zagadnienia związane z ochroną informacji w sieciach komputerowych oraz dokonać ich analizy porównawczej.

(U)- Student potrafi omówić i zaimplementować większość najważniejszych rozwiązań z zakresu ochrony informacji.

(K)- Student rozumie potrzebę dokształcania się i podnoszenia kompetencji zawodowych i osobistych.

Ocena bardzo dobra (powyżej 90% punktów)

(W)- Student potrafi omówić zagadnienia związane z ochroną informacji w sieciach komputerowych oraz dokonać ich analizy porównawczej a także umieć w sposób praktyczny dokonać niezbędnych obliczeń.

(U)- Student potrafi omówić i zaimplementować większość najważniejszych rozwiązań z zakresu ochrony informacji. Wskazać ich zalety, wady oraz ograniczenia.

(K)- Student potrafi zorganizować pracę własną oraz zespołu, do którego należy.

VII. Obciążenie pracą studenta

Forma aktywności studenta	Liczba godzin
Liczba godzin kontaktowych z nauczycielem	90
Liczba godzin indywidualnej pracy studenta	60

VIII. Literatura

Literatura podstawowa
1. William Stallings, Lawrie Brown, Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Tom I, wyd. IV, Wydawnictwo: Helion, 2019 2. William Stallings, Lawrie Brown, Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Tom II, wyd. IV, Wydawnictwo: Helion, 2019. 3. Jean-Philippe Aumasson, Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania, Wydawnictwo PWN, 2018. 4. Douglas R. Stinson, Kryptografia, Wydawnictwo: WNT, 2005. 5. Khalid Sayood,Kompresja danych - wprowadzenie, RM 2002. 6. Mirosław Kutyłowski, Willy-B. Strothman, Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, RM 1999
Literatura uzupełniająca
1. Internet agresja i ochrona, Wydawnictwo Robomatic 1998. 2. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Kryptografia stosowana, Wydawnictwo: WNT, 2005 3. Ochrona informacji w sieciach komputerowych. Pod red. P.Urbanowicza, wydawnictwo KUL, 2004