Załącznik nr 5

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	prof. dr hab. Pavel Urbanovich

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

Wymagania wstępne	1.Umiejętność pracy indywidualnej i pracy w zespole. 2. Umiejętność korzystania z aktów prawnych i publikacji. 3. Umiejętność programowania. 4. Podstawowa wiedza z zakresu arytmetyki modułowej i algebry dużych liczb. 5. Umiejętności projektowania sieci komputerowych.

II. Cele kształcenia dla przedmiotu

1. Zapoznanie studentów z podstawami teorii informacji.
2. Nabycie przez studenta teoretycznej i praktycznej umiejętności analizy bezpieczeństwa systemów operacyjnych i sieci.
3. Zrozumienie przez studenta teoretycznych i praktycznych aspektów kodowania nadmiarowego, kompresji danych, kryptografii i steganografii.
4. Nabycie przez studenta teoretycznej i praktycznej umiejętności rozpracowania i wdrażania polityki bezpieczeństwa firmy, instytucji; ochrony praw autorskich oraz danych osobowych.

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

Symbol	Opis efektu przedmiotowego	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Student posiada rozszerzoną wiedzę informatyczną w zakresie podstawowych działów informatyki	**K_W01**
W_02	Student zna matematyczne podstawy teorii informacji, teorii algorytmów, kodowania nadmiarowego, kryptografii i steganografii oraz ich praktyczne zastosowania w programowaniu i szeroko rozumianej informatyce	**K_W03**
W_03	Student ma ogólną wiedzę o aktualnych kierunkach rozwoju i najnowszych osiągnięciach w zakresie informatyki	**K_W04**
UMIEJĘTNOŚCI		
U_01	Student potrafi zastosować zdobytą wiedzę w zakresie informatyki do pokrewnych dziedzin nauki i dyscyplin naukowych	**K_U02**
U_02	Student umie policzyć i zinterpretować entropię języka polskiego, angielskiego lub innego	**K_U02, K_U03, K_U04**
U_03	Student potrafi przedstawiać w mowie i na piśmie wyniki badań z wybranej gałęzi bezpieczeństwa sieci komputeorwych zawierające opis i uzasadnienie celu, przyjętą metodologię oraz znaczenie tych wyników na tle innych , podobnych badań argumentując swoje stanowisko oraz formułując wnioski	**K_U04, K_U15**
U_04	Student potrafi zaimplementować podstawowe algorytmy kodowania nadmiarowego, podstawowe algorytmy kryptografii symetrycznej i asymetrycznej, komresji danych oraz steganografii	**K_U02, K_U03, K_U04, K_U05, K_U15**
U_05	Student potrafi zapewnić podstawowe bezpieczeństwo w systemach operacyjnych i sieciach komputerowych	**K_U05, K_U15**
KOMPETENCJE SPOŁECZNE		
K_01	Student zna ograniczenia własnej wiedzy algorytmicznej i rozumie potrzebę ciągłego dokształcania	**K_K01**
K_02	Student rozumie potrzebę systematycznej pracy i dotrzymywania terminów wykonywanych zadań	**K_K02**
K_03	Student rozumie i docenia znaczenie uczciwości intelektualnej w zakresie korzystania z cudzego oprogramowania. Zachowuje się etycznie podczas realizacji projektów algorytmicznych.	**K_K03**
K_04	Student samodzielnie potrafi odnaleźć i wykorzystać różnego rodzaju informacje dotyczące algorytmiki, także w językach obcych.	**K_K04, K_K06**

IV. Opis przedmiotu/ treści programowe

Problem bezpieczeństwa sieci komputerowych i systemów informatycznych (SI). Cyberprzestrzeń i cyberbezpieczeństwo. Ochrona własności intelektualnej i danych osobowych.
Klasyfikacja i podstawowe parametry SI. Rodzaje kanałów transmisji danych. Kanały binarne. Badanie własności entropii Shannona, Hartley'a oraz entropii binarnej i warunkowej. Obliczanie ilości informacji w powiadomieniu.
Obliczanie ilości informacji w powiadomieniu. Utrata informacji w sieciach komputerowych i ich ocena w oparciu o entropię warunkową. Tworzenie aplikacji do badania i analizy ilości informacji w

powiadomieni. Niezawodność sieci komputerowych i kanałów transmisyjnych z wykorzystaniem kodów nadmiarowych. Kody Hamminga i kody cykliczne. Tworzenie aplikacji do badania i analizy niezawodności SI z zastosowaniem kodu cyklicznego. Teoretyczne podstawy i klasyfikacja metod kompresji danych. Tworzenie aplikacji mających na celu kompresję danych metodami: interwałów, Shannona-Fano, Huffmana. Teoretyczne podstawy kryptografii. Kryptografia symetryczna i asymetryczna. Szyfrowanie i deszyfrowanie informacji. Omówienie i implementacja algorytmu RSA (El-Gamala). Maszyna Enigma. Funkcja skrótu. Algorytmy klas MD i SHA. Podpis cyfrowy. Podpis cyfrowy oparty na algorytmie RSA i algorytmie El-Gamala. Standard i wykorzystanie podpisów cyfrowych w Polsce. Protokoły Kerberos i SSL/TLS. Wirusy komputerowe i metody ochrony przed nimi w sieciach komputerowych. Projektowanie bezpieczeństwa SI i badanie bezpieczeństwa systemów operacyjnych i sieci. Zapoznanie studentów z mechanizmami zabezpieczeń w systemach operacyjnych i sieciach komputerowych. Polityka bezpieczeństwa firm i instytucji.

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	Wykłady z prezentacjami multimedyalnymi, a także zajęcia, realizowane z wykorzystaniem metod i technik kształcenia na odległość, konsultacje, praca samodzielna studenta	Kolokwium pisemny, Egzamin	Oceniony wynik kolokwium, Ocena egzaminacyjna
W_02	Wykłady z prezentacjami multimedyalnymi, a także zajęcia, realizowane z wykorzystaniem metod i technik kształcenia na odległość, ćwiczenia laboratoryjne, konsultacje, praca samodzielna studenta	Kolokwium pisemny, Aplikacja programowa studenta, Egzamin	Oceniony wynik kolokwium, Oceniona aplikacja, Ocena egzaminacyjna
W_03	Wykłady z prezentacjami multimedyalnymi, a także zajęcia, realizowane z wykorzystaniem metod i technik kształcenia na odległość, konsultacje,	Kolokwium pisemny, Egzamin	Oceniony wynik kolokwium, Ocena egzaminacyjna

	praca samodzielna studenta		
UMIEJĘTNOŚCI			
U_01	Wykłady z prezentacjami multimedyalnymi, a także zajęcia, realizowane z wykorzystaniem metod i technik kształcenia na odległość, konsultacje, praca samodzielna studenta	Kolokwium pisemny, Egzamin	Oceniony wynik kolokwium, Ocena egzaminacyjna
U_02	Wykłady z prezentacjami multimedyalnymi, a także zajęcia, realizowane z wykorzystaniem metod i technik kształcenia na odległość, ćwiczenia laboratoryjne, konsultacje, praca samodzielna studenta	Kolokwium pisemny, Aplikacja programowa studenta, Egzamin	Oceniony wynik kolokwium, Oceniona aplikacja, Ocena egzaminacyjna
U_03	Wykłady z prezentacjami multimedyalnymi, a także zajęcia, realizowane z wykorzystaniem metod i technik kształcenia na odległość, konsultacje, praca samodzielna studenta	Kolokwium pisemny, Egzamin	Oceniony wynik kolokwium, Ocena egzaminacyjna
U_04	Wykłady z prezentacjami multimedyalnymi, a także zajęcia, realizowane z wykorzystaniem metod i technik kształcenia na odległość, ćwiczenia laboratoryjne, konsultacje, praca samodzielna studenta	Kolokwium pisemny, Aplikacja programowa studenta, Egzamin	Oceniony wynik kolokwium, Oceniona aplikacja, Ocena egzaminacyjna
U_05	Wykłady z prezentacjami multimedyalnymi, a także zajęcia, realizowane z wykorzystaniem metod i technik kształcenia na odległość, ćwiczenia laboratoryjne, konsultacje, praca samodzielna studenta	Kolokwium pisemny, Egzamin	Oceniony wynik kolokwium, Ocena egzaminacyjna

KOMPETENCJE SPOŁECZNE			
K_01, K_02, K_03, K_04	Wykłady z prezentacjami multimedyalnymi, a także zajęcia, realizowane z wykorzystaniem metod i technik kształcenia na odległość, ćwiczenia laboratoryjne, konsultacje, indywidualne rozmowy ze studentami, dyskusje, praca samodzielna studenta	Egzamin	Ocena egzaminacyjna

VI. Kryteria oceny, wagi…

Przedmiot kończy się egzaminem. Warunkiem przystąpienia do egzaminu jest pozytywna ocena z ćwiczeń, uzyskanie pozytywnych ocen z co najmniej dwóch kolokwiów odbywających się w formie testu pisemnego. Próg zdawalności 60%.

Warunkiem zaliczenia ćwiczeń jest przygotowanie autorskich aplikacji (co najmniej 4) z opisem ich fukcjonalności i wyników przeprowadzonych badań (pliki tekstowe), umieszczonych w dostępnej dla egzaminatora chmurze; zaliczenie 2 kolokwiów.

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: obecność studenta na wykładach (min – 60%), obecność studenta na ćwiczeniach (100%), aktywności studenta na ćwiczeniach.	Liczba godzin
Liczba godzin kontaktowych z nauczycielem	**Wykady – 30** **Ćwiczenia - 30**
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