

KARTA KURSU
(realizowanego w specjalności)

CYBERBEZPIECZEŃSTWO
(nazwa specjalności)

Nazwa	Steganografia
Nazwa w j. ang.	Steganography

Koordynator	dr hab. prof. UKEN Serhii Semenov	Zespół dydaktyczny
		dr hab. prof. UKEN Serhii Semenov
Punktacja ECTS*	4	

Opis kursu (cele kształcenia)

Celem kursu jest opanowanie przez studentów metod i zasad budowy, implementacji i stosowania systemów i protokołów steganograficznych oraz umiejętność stosowania metod, algorytmów i narzędzi oceny odporności na steganografię i innych jakościowych wskaźników systemów steganograficznych i protokołów. Podczas nauki protokołów steganograficznych studenci powinni umieć uzasadniać wymagania, rozwiązywać zadania analizy i syntezy protokołów steganograficznych, tworzyć modele programowe i przeprowadzać modelowanie systemów steganograficznych, praktycznie implementować algorytmy obliczeniowe ochrony steganograficznej informacji. Kurs jest realizowany w języku polskim.

Warunki wstępne

Wiedza	Podstawowe definicje i pojęcia z teorii sygnałów. Rozumie pojęcie transmitancji i jej zastosowania. Orientuje się w analizie częstotliwościowej sygnałów z wykorzystaniem transformacji Fouriera.
Umiejętności	Podstawowe umiejętności w zakresie analizy stacjonarnych liniowych systemów dyskretnych. Umiejętność programowania i samodzielnego korzystania z literatury przedmiotu. Znajomość pakietów matematycznych.
Kursy	Przetwarzanie sygnałów

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Po zakończeniu kursu student:	
	W01: ma wiedzę na temat zasad działania podstawowych narzędzi steganograficznych w kontekście zapewnienia zabezpieczenia struktur lokalnych i sieciowych	SC_W01
	W02: zna elementarne algorytmy, języki i techniki programowania	SC_W02
	W03: zna zagadnienia dotyczące systemów informatycznych i sieci komputerowych	SC_W03

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	Po zakończeniu kursu student:	
	U01: bada, opracowuje, wdraża i stosuje metody i środki steganograficzne ochrony informacji	SC_U01
	U02: potrafi używać dedykowanych środowisk programistycznych wraz z wybranymi bibliotekami w celu efektywnego i bezpiecznego tworzenia aplikacji.	SC_U03
	U03: potrafi analizować i projektować sieci i systemy teleinformatyczne, stosując metody steganograficzne.	SC_U04

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	Po zakończeniu kursu student:	
	K01: potrafi formułować opinie na temat metody steganograficzne.	SC_K02

Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	15					30					

Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	10					15					

Opis metod prowadzenia zajęć

1 Wykłady: Podczas wykładów wykładowcy wprowadzają materiał teoretyczny, wyjaśniają kluczowe pojęcia i metody oraz przedstawiają przykłady i ilustracje. Wykłady mogą być prowadzone w klasie lub online, a nagrania wykładów mogą być udostępniane do późniejszego przeglądania.

2. Sesje laboratoryjne: sesje laboratoryjne umożliwiają studentom przeprowadzanie praktycznych eksperymentów z rzeczywistymi danymi. Mogą one obejmować badanie istniejących produktów oprogramowania do steganograficznej ochrony danych, wdrażanie własnych rozwiązań w tej dziedzinie i wiele innych zadań, które pomagają studentom utrwalić wiedzę teoretyczną.

3. Dyskusje grupowe i zadania: dyskusje grupowe i zadania ułatwiają dzielenie się wiedzą między studentami i zachęcają do wspólnego uczenia się. Metody te mogą obejmować fora dyskusyjne, projekty grupowe i wspólne rozwiązywanie problemów.

4 Samodzielna nauka: Studenci mogą również mieć dostęp do materiałów do samodzielnej nauki, takich jak podręczniki, artykuły i kursy online. Pozwala to uczniom na pogłębienie wiedzy i zbadanie tematów, które ich szczególnie interesują.

5 Testy i ocena: w trakcie kursu uczniowie mogą brać udział w testach i quizach w celu oceny ich poziomu wiedzy i osiągnięć. Oceny te mogą obejmować zarówno egzaminy pisemne, jak i oceny projektów i laboratoriów.

Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01					X								
W02					X								
W03					X								
U01					X			X					
U02					X			X					
U03					X			X					
K01					X			X					

Kryteria oceny

Ocena końcowa zależy od ocen częściowych, regularności wykonywania zadań oraz oceny otrzymanej za projekt zespołowy (indywidualny). W szczególności ocenę dobrą i bardzo dobrą z zadań może uzyskać student, który: - samodzielnie tworzy oprogramowanie wykorzystujące rozważane metody steganograficznej ochrony danych, - potrafi analizować uwarunkowania i obszary stosowalności badanych algorytmów

Uwagi

Treści merytoryczne (wykaz tematów)

Rozdział 1. Wprowadzenie do steganografii

1.1. Przedmiot steganografii, podstawowe terminy i definicje. Historyczne przykłady systemów steganograficznych

1.2. Obszary zastosowań steganografii. Praktyczne aspekty budowy systemów steganograficznych

1.3. Model matematyczny i strukturalny schemat systemu steganograficznego. Klasyfikacja kontenerów

Rozdział 2. Ukrywanie danych w statycznych obrazach

2.1. Cechy systemu wzrokowego człowieka (SWC). Podstawowe właściwości SWC wykorzystywane przy ukrywaniu danych w obrazach

2.2. Cyfrowe formaty statycznych obrazów (formaty BMP, GIF, TIFF, JPEG). Cechy przetwarzania komputerowego obrazów

2.3. Podstawowe etapy algorytmu kompresji obrazów JPEG. Ataki na systemy steganograficzne z wykorzystaniem JPEG

2.4. Odporność systemu steganograficznego na aktywne ataki

2.5. Ukrywanie danych w dziedzinie przestrzennej obrazów. Metody ukrywania w najmniej znaczącym bicie danych

2.6. Ukrywanie danych w dziedzinie przestrzennej obrazów (ukrywanie blokowe, metoda kwantyzacji, metoda „krzyża”)

2.7. Ukrywanie danych w dziedzinie częstotliwości obrazów. Metoda Kocha-Zhao i jej modyfikacje

2.8. Ukrywanie danych w dziedzinie częstotliwości obrazów. Metoda Hsu-Wu i metoda Friedricha

2.9. Ukrywanie danych w statycznych obrazach za pomocą metod rozszerzania widma

Rozdział 3. Ukrywanie danych w sygnałach audio

3.1. Cechy systemu słuchowego człowieka (SSC). Podstawowe właściwości SSC wykorzystywane przy ukrywaniu danych w sygnałach audio

3.2. Cyfrowe formaty sygnałów audio (formaty WAV, WMA, MP3, AAC, OGG Vorbis). Cechy przetwarzania komputerowego sygnałów audio

3.3. Ukrywanie danych w dziedzinie przestrzennej sygnału audio (ukrywanie w najmniej znaczącym bicie danych oraz za pomocą echosygnałów)

3.4. Ukrywanie danych w dziedzinie częstotliwości sygnału audio (kodowanie fazowe)
3.5. Ukrywanie danych w sygnałach audio za pomocą metod rozszerzania widma
Rozdział 4. Ukrywanie danych w plikach tekstowych
4.1. Metody steganografii tekstowej
4.2. Analiza realizacji metod
Rozdział 5. Ataki na systemy steganograficzne i przeciwdziałanie im
5.1. Ataki na systemy ukrytego przesyłania wiadomości. Ataki na systemy cyfrowych znaków wodnych (CZW)
5.2. Klasyfikacja ataków na systemy cyfrowych znaków wideo (CZW)
5.3. Ataki mające na celu usuwanie CZW
5.4. Ataki geometryczne
5.5. Ataki kryptograficzne
5.6. Ataki na protokół używany
5.7. Metody przeciwdziałania atakom na systemy CZW. Statystyczna analiza stegoanalizy i przeciwdziałanie
5.8. Praktyczna ocena odporności systemów steganograficznych. Teoretyczno-łożonościowe podejście do oceny odporności systemów steganograficznych. Odporność na ataki imitacyjne systemów przesyłania ukrytych wiadomości
5.9. Ataki wizualne na systemy steganograficzne
5.10. Statystyczne ataki na systemy steganograficzne z obrazami jako kontenerami
5.11. Statystyczne ataki na systemy steganograficzne z sygnałami audio jako kontenerami
5.12. Kierunki zwiększania odporności systemów steganograficznych na statystyczne ataki
5.13. Teoretyczno-łożonościowe podejście do oceny odporności steganograficznych systemów
5.14. Odporność na ataki statystyczne systemów przesyłania ukrytych wiadomości

Wykaz literatury podstawowej

1. "Steganografia cyfrowa. Sztuka ukrywania informacji" Volodymyr Mosorov Wydawnictwo: Wydawnictwo Uniwersytetu Łódzkiego
2. "Codes, Ciphers, Steganography & Secret Messages" By Sunil Tanna 2021
3. "Steganography, The World of Secret Communications" By Michael T Hegarty 2018
4. "Steganography in Digital Media Principles, Algorithms, and Applications" By Jessica Fridrich 2009
5. Steganography The Art of Hiding Information" By Ms Karen Bailey 2014

Wykaz literatury uzupełniającej

1. "Hiding in Plain Sight Steganography and the Art of Covert Communication" By Eric Cole 2003
2. "Digital Watermarking and Steganography Fundamentals and Techniques" By Frank Y. Shih 2007
3. "Cryptography using Modified ASCII Conversion & Mathematical Function@ By Dr. Sheshang Degadwala 2019

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia stacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	30
	Pozostałe godziny kontaktu studenta z prowadzącym	2
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	5
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	8
	Przygotowanie do egzaminu/zaliczenia	10
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		4

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia niestacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	15
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	10
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	10
	Przygotowanie do egzaminu/zaliczenia	10
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		4