

KARTA KURSU
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 W02: zna elementarne algorytmy steganograficzne, języki i techniki programowania | SC_W01 SC_W02 |
| Umiejętności | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |

| | | |
|--|---|----------------------|
| | Po zakończeniu kursu student: U01: bada, opracowuje, wdraża i stosuje metody i środki steganograficzne ochrony informacji. U02: potrafi konstruować algorytmy steganograficzne i pisać pojedyncze aplikacje oraz większe projekty programistyczne, w oparciu o języki programowania niskiego i wysokiego poziomu z uwzględnieniem zasad bezpieczeństwa. | SC_U01 SC_U02 |
|--|---|----------------------|

| Kompetencje społeczne | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
|-----------------------|---|-------------------------------------|
| | Po zakończeniu kursu student: K01: potrafi formułować opinie na tematy związane z nauką o steganografii. | SC_K02 |

Studia stacjonarne

| Organizacja | | | | | | | | | | | |
|---------------|------------|---------------------|--|---|--|----|--|---|--|---|---|
| Forma zajęć | Wykład (W) | Ćwiczenia w grupach | | | | | | | | | |
| | | A | | K | | L | | S | | P | E |
| Liczba godzin | 20 | | | | | 30 | | | | | |

Studia niestacjonarne

| Organizacja | | | | | | | | | | | |
|---------------|------------|---------------------|--|---|--|----|--|---|--|---|---|
| Forma zajęć | Wykład (W) | Ćwiczenia w grupach | | | | | | | | | |
| | | A | | K | | L | | S | | P | E |
| Liczba godzin | 10 | | | | | 20 | | | | | |

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 w celu oceny ich poziomu wiedzy i osiągnięć.

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 | | | X | | | | | |
| W02 | | | | | X | | | X | | | | | |
| U01 | | | | | X | | | X | | | | | |
| U02 | | | | | X | | | X | | | | | |
| K02 | | | | | X | | | X | | | | | |

| | | | | | | | | | | | | | | | |
|-------------------------|---|-------------------------|-------------------|------------|--------------------|-----------|------------------|-----------|-------------|-----------|------------------------|-----------|-------------------|----------|----------------------|
| Kryteria oceny | <p>Ocena końcowa z kursu <i>Steganografia</i> opiera się na systemie punktowym. Maksymalna liczba punktów do zdobycia: 100, w tym:</p> <ul style="list-style-type: none"> 60 punktów – zadania laboratoryjne: <ul style="list-style-type: none"> - implementacja (do 30 pkt), - ocena odporności (do 15 pkt), - dokumentacja i prezentacja (do 10 pkt), - aktywność i samodzielność (do 5 pkt); 40 punktów – test zaliczeniowy: <ul style="list-style-type: none"> - wiedza teoretyczna, - znajomość metod, - umiejętność analizy i oceny odporności. <p>Warunki zaliczenia kursu:</p> <ul style="list-style-type: none"> minimum 51 punktów łącznie, minimum 30 punktów z laboratoriów oraz 15 punktów z testu. <p>Przeliczenie punktów na ocenę końcową:</p> <table> <tr> <td>Liczba punktów (ze 100)</td><td>Ocena w skali 2–5</td></tr> <tr> <td>91–100 pkt</td><td>bardzo dobra (5,0)</td></tr> <tr> <td>81–90 pkt</td><td>dobra plus (4,5)</td></tr> <tr> <td>71–80 pkt</td><td>dobra (4,0)</td></tr> <tr> <td>61–70 pkt</td><td>dostateczna plus (3,5)</td></tr> <tr> <td>51–60 pkt</td><td>dostateczna (3,0)</td></tr> <tr> <td>0–50 pkt</td><td>niedostateczna (2,0)</td></tr> </table> | Liczba punktów (ze 100) | Ocena w skali 2–5 | 91–100 pkt | bardzo dobra (5,0) | 81–90 pkt | dobra plus (4,5) | 71–80 pkt | dobra (4,0) | 61–70 pkt | dostateczna plus (3,5) | 51–60 pkt | dostateczna (3,0) | 0–50 pkt | niedostateczna (2,0) |
| Liczba punktów (ze 100) | Ocena w skali 2–5 | | | | | | | | | | | | | | |
| 91–100 pkt | bardzo dobra (5,0) | | | | | | | | | | | | | | |
| 81–90 pkt | dobra plus (4,5) | | | | | | | | | | | | | | |
| 71–80 pkt | dobra (4,0) | | | | | | | | | | | | | | |
| 61–70 pkt | dostateczna plus (3,5) | | | | | | | | | | | | | | |
| 51–60 pkt | dostateczna (3,0) | | | | | | | | | | | | | | |
| 0–50 pkt | niedostateczna (2,0) | | | | | | | | | | | | | | |

| | |
|-------|--|
| Uwagi | |
|-------|--|

Treści merytoryczne (wykaz tematów)

| | |
|---|--|
| <p>Moduł 1: Wprowadzenie do steganografii</p> <ol style="list-style-type: none"> Podstawy steganografii cyfrowej <ul style="list-style-type: none"> - Definicje, terminologia, struktura systemów steganograficznych. - Zastosowania i różnice między kryptografią a steganografią. - Klasyfikacja pojemników i kanałów komunikacyjnych. Modele matematyczne i protokoły steganograficzne <ul style="list-style-type: none"> - Model komunikacyjny stegosystemu. - Protokoły steganograficzne: otwarte, zamknięte, mieszane. - Wymagania i właściwości pojemników i kluczy. <p>Moduł 2: Ukrywanie danych w obrazach cyfrowych</p> <ol style="list-style-type: none"> System wzrokowy człowieka a ukrywanie informacji <ul style="list-style-type: none"> - Cechy percepcji wzrokowej i wykorzystanie ich w osadzaniu danych. Formaty graficzne i ich specyfika <ul style="list-style-type: none"> - BMP, GIF, TIFF, JPEG – struktura i wpływ formatu na możliwości steganograficzne. Metody ukrywania w domenie przestrzennej <ul style="list-style-type: none"> - Ukrywanie w najmniej znaczącym bicie (LSB). | |
|---|--|

| | |
|---|---|
| | <ul style="list-style-type: none"> - Ukrywanie pseudolosowe (permutacja bitów). - Ukrywanie blokowe, metoda kwantyzacji, metoda „krzyża”. - Metoda wymiany palety kolorów. - Metoda Kuttera-Jordana-Bossena. |
| 6. | Ukrywanie danych w domenie częstotliwości <ul style="list-style-type: none"> - Transformacja DCT i kompresja JPEG. - Metoda Kocho-Zhao, jej modyfikacje i odporność na kompresję. |
| Moduł 3: Ukrywanie danych w dźwięku i tekście | |
| 7. | Ukrywanie danych w sygnałach audio <ul style="list-style-type: none"> - System słuchowy człowieka i jego ograniczenia. - Format WAV, MP3, OGG Vorbis. - Ukrywanie metodą echa, kodowanie fazowe. - Metody rozszerzania widma. |
| 8. | Steganografia tekstowa <ul style="list-style-type: none"> - Metody: spacji, formatowania, synonimów, interpunkcji. - sadzanie w dokumentach PDF, RTF, XML, napisach filmowych. |
| Moduł 4: Ataki na systemy steganograficzne i przeciwdziałanie | |
| 9. | Stegoanaliza i klasyfikacja ataków <ul style="list-style-type: none"> - Ataki wizualne, statystyczne, geometryczne, kryptograficzne. - Ataki na znaki wodne i protokoły komunikacyjne. |
| 10. | Odporność systemów i metody ochrony <ul style="list-style-type: none"> - Teoretyczno-złożonościowe podejście do oceny odporności. - Praktyczna ocena skuteczności systemu. - Projektowanie systemów odpornych na wykrycie. |

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 | 20 |
| | Laboratorium | 30 |
| | Pozostałe godziny kontaktu studenta z prowadzącym | 10 |
| liczba godzin pracy studenta bez kontaktu z prowadzącymi | Lektura w ramach przygotowania do zajęć | 10 |
| | 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 zaliczenia | 10 |
| Ogółem bilans czasu pracy | | 100 |
| 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 |
| | Laboratorium | 20 |
| | Pozostałe godziny kontaktu studenta z prowadzącym | 15 |
| 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) | 15 |
| | Przygotowanie do zaliczenia | 15 |
| Ogółem bilans czasu pracy | | 100 |
| Liczba punktów ECTS w zależności od przyjętego przelicznika | | 4 |