



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Techniki ochrony multimediów [S1Cybez1>TOMm]

Przedmiot

Kierunek studiów

Cyberbezpieczeństwo

Rok/Semestr

3/6

Studia w zakresie (specjalność)

–

Profil studiów

ogólnoakademicki

Poziom studiów

pierwszego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

stacjonarne

Wymagalność

obieralny

Liczba godzin

Wykład

24

Laboratorium

24

Inne

0

Ćwiczenia

0

Projekty/seminaria

0

Liczba punktów ECTS

3,00

Koordynatorzy

dr hab. inż. Dawid Mieloch prof. PP
dawid.mieloch@put.poznan.pl

mgr inż. Jakub Stankowski
jakub.stankowski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Podstawowa wiedza z podstaw programowania, techniki cyfrowej, przetwarzania sygnałów multimedialnych oraz umiejętność pozyskiwania informacji ze wskazanych źródeł, w tym źródeł w języku angielskim.

Cel przedmiotu

Przekazanie podstawowej wiedzy dotyczącej steganografii, znakowania wodnego, szyfrowania multimediów, kontroli dostępu do multimediów, kryptografii kwantowej i zastosowań szyfrowania kwantowego.

Przedmiotowe efekty uczenia się

Wiedza:

K1_W12 - Ma pogłębioną wiedzę w zakresie uwierzytelniania, autoryzacji i zasad sterowania dostępem do systemów komputerowych; jest świadom konieczności stosowania polityk sterowania dostępem oraz

ich adaptacji do poziomu ryzyka; zna zasady uwierzytelniania biometrycznego;
K1_W13 - Zna zasady ukrywania danych, tj. kryptografię i steganografię; ma zaawansowaną wiedzę z zakresu kryptografii, algorytmów kryptograficznych i ich ograniczeń oraz ich znaczenia dla cyberbezpieczeństwa; ma poszerzoną wiedzę w zakresie kompresji danych

Umiejętności:

K1_U01 - Potrafi korzystać ze źródeł literaturowych, integrować pozyskane informacje, oceniać je oraz dokonywać ich interpretacji i wyciągać wnioski, w celu rozwiązania złożonych i nietypowych problemów w obszarze cyberbezpieczeństwa

K1_U08 - Potrafi dokonać porównania różnych rozwiązań technicznych, ocenić je ze względu na wybrane kryteria użytkowe, ekonomiczne, ekologiczne, prawne oraz etyczne

Kompetencje społeczne:

K1_K05 - Ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, jest gotowy do podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania, a także dbałości o dorobek i tradycje zawodu

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład - egzamin pisemny, pytanie zamknięte (test)/otwarte,

Laboratoria - na końcową ocenę składają się: ocena merytoryczna wykonywania zadań laboratoryjnych, ocenianie ciągłe, na każdych zajęciach (odpowiedzi ustne), bierząca aktywność na zajęciach, oceny uzyskane na sprawdzianach pisemnych, uzyskiwanie punktów dodatkowych za aktywność podczas zajęć oraz wyniki zadań do samodzielnej realizacji.

Skala ocen: p<50% : 2.0; p <50%, 60%) : 3.0; p <60%, 70%) : 3.5; p <70%, 80%) : 4.0; p <80%, 90%) :

4.5; p >= 90% : 5.0

Zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Treści programowe obejmują zagadnienia związane z ochroną, analizą i kontrolą dostępu do multimediów w kontekście ich bezpieczeństwa. Obejmują one metody ukrywania informacji w plikach audiowizualnych, techniki znakowania pozwalające na identyfikację źródła treści oraz mechanizmy szyfrowania stosowane w ochronie plików przed nieautoryzowanym dostępem. Szczególny nacisk położony jest na metody wykrywania manipulacji i analizy integralności multimediów, co ma kluczowe znaczenie w wykrywaniu fałszerstw i zabezpieczaniu danych przed ingerencją.

Dodatkowo w treściach programowych uwzględniono zagadnienia dotyczące kontroli dostępu do treści cyfrowych, obejmujące systemy ograniczające kopiowanie i rozpowszechnianie multimediów.

Omówione są także nowoczesne technologie zabezpieczeń, w tym metody kryptograficzne oraz ich wpływ na jakość i efektywność transmisji danych. Podjęta zostaje również tematyka zależności między kompresją a bezpieczeństwem treści, a także wykorzystania nowoczesnych technik w celu zapewnienia integralności i poufności multimediów w środowiskach cyfrowych.

Tematyka zajęć

1. Ukrywanie informacji w multimediach

- Podstawowe pojęcia i cele.
- Metody osadzania ukrytych danych w plikach dźwiękowych, graficznych i wideo.
- Zastosowania ukrywania danych w kontekście ochrony prywatności i zabezpieczeń.
- Techniki wykrywania ukrytych danych w multimediach, analiza statystyczna i wizualna.

2. Techniki znakowania multimediów

- Rodzaje znakowania i ich zastosowania.
- Sposoby osadzania znaków w różnych formatach multimedialnych.
- Metody usuwania i modyfikowania znaków.
- Przykłady ataków i zabezpieczeń znakowanych treści.

3. Szyfrowanie treści multimedialnych

- Sposoby zabezpieczania danych audiowizualnych.
- Algorytmy szyfrowania i ich wpływ na jakość treści.
- Mechanizmy ochrony multimediiów podczas przechowywania i transmisji.
- Wydajność szyfrowania w systemach dystrybucji treści.
- Wpływ metod kompresji na bezpieczeństwo zaszyfrowanych plików.

4. Ochrona dostępu do multimediiów

- Mechanizmy kontroli dostępu i ich rola w zabezpieczaniu treści.
- Metody ograniczania kopiowania i odtwarzania.
- Przykłady stosowania systemów zabezpieczających multimedia.
- Problematyka prywatności i ograniczeń związanych z ochroną treści.

5. Nowoczesne metody ochrony danych multimedialnych

- Wykorzystanie nowych technologii do zabezpieczania informacji.
- Metody dystrybucji kluczy i ochrona przed przechwyceniem danych.
- Przykłady zastosowań w komunikacji, chmurze i systemach inteligentnych.

Metody dydaktyczne

Wykład hybrydowy: wykład tradycyjny z dodatkiem multimedialnych materiałów edukacyjnych, wykłady problemowe - analiza przypadków, dopuszcza się możliwość zapraszania prelegentów z branży lub nauki
Laboratorium - zajęcia komputerowe.

Literatura

Podstawowa:

Deb, S., & Sahu, A. K. (2023). Securing the Digital World: A Comprehensive Guide to Multimedia Security. Routledge.

Puech, W. (2023). Multimedia Security 1: Authentication and Data Hiding. Wiley-ISTE.

Anderson, R. (2020). Inżynieria zabezpieczeń. Tom II. Helion.

Pieprzyk, J. (2011). Teoria bezpieczeństwa systemów komputerowych. Helion.

Uzupełniająca:

Wong, D. (2023). Prawdziwy świat kryptografii. Helion.

Aumasson, J.-P. (2017). Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press.

Baker, R. L. (2024). Prawdziwa głębia OSINT. Odkryj wartość danych Open Source Intelligence. Helion.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	78	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	48	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	30	1,00