



## KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Ochrona dostępu w rozproszonych systemach multimedialnych [S1Cybez1>ODwRSM]

### Przedmiot

Kierunek studiów

Cyberbezpieczeństwo

Rok/Semestr

3/5

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

16

Inne

0

Ćwiczenia

0

Projekty/seminaria

16

### Liczba punktów ECTS

4,00

### Koordynatorzy

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

### Wykładowcy

### Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z zakresu podstaw telekomunikacji, cyfrowego przetwarzania sygnałów i wprowadzenia do multimedii. Powinien posiadać umiejętność wykonywania obliczeń za pomocą aparatu matematycznego z zakresu analizy matematycznej i rachunku prawdopodobieństwa oraz pozyskiwania informacji ze wskazanych źródeł. Powinien również rozumieć konieczność poszerzania swoich kompetencji. Ponadto w zakresie kompetencji społecznych student musi prezentować takie postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawczą, kreatywność, kulturę osobistą, szacunek dla innych ludzi.

## Cel przedmiotu

Celem przedmiotu "Ochrona dostępu w rozproszonych systemach multimedialnych" jest zapoznanie studentów z metodami przesyłania multimediów, różnorodnymi zagrożeniami i atakami, którym podlegają rozproszone systemy multimedialne, oraz z technikami i narzędziami służącymi do ich zabezpieczenia. W ramach tego przedmiotu studenci zdobywają wiedzę na temat architektury typowych systemów służących do strumieniowania i zapisywania wizji. Dzięki temu kształtują umiejętności analizy i identyfikacji potencjalnych zagrożeń oraz podejmowania odpowiednich działań zapobiegawczych, mających na celu zabezpieczenie rozproszonych systemów przesyłania wizji oraz dozoru wizyjnego przed nieautoryzowanymi dostęпами i manipulacjami.

## Przedmiotowe efekty uczenia się

### Wiedza

K1\_W05 Ma zaawansowaną wiedzę w zakresie złożonych struktur danych; zna podstawy teorii, zna zasady administrowania danymi i związanymi z nimi standardami; zna zasady cyberbezpieczeństwa i prywatności wykorzystywane do zarządzania ryzykiem związanym z wykorzystywaniem, przetwarzaniem, przechowywaniem i przesyłaniem informacji lub danych.

K1\_W07 Ma pogłębioną i wiedzę o typach i architekturach oraz o projektowaniu, konfigurowaniu i utrzymaniu sieci komputerowych; zna i rozumie wykorzystywane w nich protokoły, algorytmy oraz mechanizmy.

K1\_W11 Ma pogłębioną wiedzę o projektowaniu, konfigurowaniu oraz utrzymaniu systemów komputerowych, w tym systemów rozproszonych; zna i rozumie wykorzystywane w nich mechanizmy.

K1\_W14 Ma wiedzę ogólną związaną z kluczowymi zagadnieniami z zakresu przetwarzania rozproszonego; ma zaawansowaną wiedzę szczegółową dotyczącą zagadnień przetwarzania chmurowego oferowanego na rynku; zna modele usług chmurowych oraz koncepcji związanych z bezpieczeństwem, zarządzaniem, zamówieniami i administracją; zna ekonomiczne, prawne i inne uwarunkowania działalności firm oferujących usługi chmurowe.

### Umiejętności:

1\_U02 Potrafi posłużyć się właściwie dobranymi metodami i narzędziami, w tym zaawansowanymi technikami informacyjno-komunikacyjnymi, a także opracować proste aplikacje lub skonfigurować proste systemy, w celu przeprowadzenia symulacji, analizy i projektowania systemów lub aplikacji właściwych dla kierunku studiów

K1\_U10 Na podstawie dostępnej dokumentacji i specyfikacji oraz standardów potrafi zaprojektować i zaimplementować w językach wysokiego poziomu bezpieczną aplikację internetową lub mobilną

K1\_U14 Ma umiejętności w zakresie języka obcego na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego, a także umie czytać ze zrozumieniem karty katalogowe, normy, dokumentacje techniczne oraz instrukcje obsługi układów i urządzeń właściwych dla kierunku studiów

### Kompetencje społeczne:

K1\_K01 Rozumie znaczenie podnoszenia kompetencji zawodowych, osobistych i społecznych; ma świadomość, że wiedza i umiejętności w obszarze cyberbezpieczeństwa szybko ewoluują

K1\_K02 Rozumie znaczenie wiedzy w rozwiązywaniu problemów z zakresu cyberbezpieczeństwa; jest świadomy konieczności wykorzystania wiedzy ekspertów podczas rozwiązywania zadań inżynierskich w zakresie wykraczającym poza własne kompetencje

## 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:

a) w zakresie wykładów weryfikowanie założonych efektów kształcenia realizowane jest przez: • ocenę wiedzy wykazanej na egzaminie. Egzamin polega na udzielaniu odpowiedzi na pytania i na rozwiązywaniu problemów. Do otrzymania oceny 3.0 niezbędne jest zdobycie minimum 50% punktów; 3,5 - 60% punktów; 4,0 - 70% punktów; 4,5 - 80% punktów; 5,0 - 90% punktów. b) w zakresie ćwiczeń laboratoryjnych weryfikowanie założonych efektów kształcenia realizowane jest przez: • ocenę merytoryczną wykonywania zadań laboratoryjnych, • uzyskiwanie punktów dodatkowych za aktywność podczas zajęć.

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

1. Wprowadzenie do rozproszonych systemów multimedialnych (DMMS)
2. Zagrożenia bezpieczeństwa w DMMS
3. Mechanizmy ochrony dostępu w DMMS
4. Studia przypadków i przykłady
5. Trendy i wyzwania przyszłości

## Tematyka zajęć

- Definicja DMMS i ich komponenty (bazy danych multimedialnych, serwery informacyjne, klienci)
- Ewolucja DMMS: od małych sieci LAN do obsługi urządzeń mobilnych i aplikacji o dużej przepustowości
- Nowe wyzwania w projektowaniu DMMS: łączność bezprzewodowa, skalowalność, obsługa dużej liczby klientów, różnorodność urządzeń i aplikacji
- Kluczowe technologie i rozwiązania: streaming mediów, buforowanie, QoS
- Przegląd metod przesyłania danych multimedialnych
- o Rozsiewcze usługi telewizyjne: Telewizja kablowa, naziemna, satelitarna, tworzenie strumienia transportowego, metody szyfrowania i dostępu warunkowego (DRM), synchronizacja nadajnika i odbiornika.
- o Usługi internetowe: IPTV, architektura nowoczesnych mediów strumieniowych, porównanie metod strumieniowania, przykłady metod wydajnego strumieniowania wizji.
- Nieautoryzowany dostęp do treści multimedialnych
- Ataki typu Denial-of-Service (DoS)
- Kradzież danych
- Dystrybucja złośliwego oprogramowania
- Podszycanie się pod użytkowników lub serwery
- Autentykacja i autoryzacja: Metody uwierzytelniania użytkowników i urządzeń. Kontrola dostępu. Zarządzanie prawami dostępu do treści. Szyfrowanie treści multimedialnych.
- Ochrona przed atakami DoS: Mechanizmy wykrywania i zapobiegania atakom DoS. Redundacja i równoważenie obciążenia. Ograniczanie przepustowości i filtrowanie ruchu
- Bezpieczeństwo danych: Ochrona przed utratą i uszkodzeniem danych. Kopie zapasowe i odzyskiwanie danych
- Analiza istniejących systemów DMMS i ich mechanizmów bezpieczeństwa
- Najlepsze praktyki w zakresie ochrony dostępu w DMMS
- Nowe technologie i ich wpływ na bezpieczeństwo DMMS (np. chmura obliczeniowa, Internet of Things)
- Rozwój sztucznej inteligencji i uczenia maszynowego w kontekście bezpieczeństwa DMMS
- Kwe

## Metody dydaktyczne

Wykład: wspomagany prezentacją oraz przykładami fonii, obrazów i wizji. Laboratoria: realizacja projektów na komputerach (samodzielna lub w kilkuosobowych grupach).

## Literatura

Podstawowa:

-D. Bull – Communicating Pictures, Elsevier, 2014

B. Bing – Next-Generation Video Coding and Streaming, Wiley, 2015

Uzupełniająca:

-M. Domański – Obraz cyfrowy, Wydawnictwa Komunikacji i Łączności WKŁ, 2011

D. Karwowski – Zrozumieć kompresję obrazu, [www.zrozumieckompresje.pl](http://www.zrozumieckompresje.pl), 2019

L. Chariglione – The MPEG Representation of Digital Media, Springer, 2012

## Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	116	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	56	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiiw/egzaminu, wykonanie projektu)	60	2,00