



## KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Mechanizmy i zasady bezpieczeństwa w chmurze [S2Teleinf2-SDP>BwC]

### Przedmiot

Kierunek studiów  
Teleinformatyka

Rok/Semestr  
2/3

Studia w zakresie (specjalność)  
Systemy definiowane programowo

Profil studiów  
ogólnoakademicki

Poziom studiów  
drugiego stopnia

Język oferowanego przedmiotu  
polski

Forma studiów  
stacjonarne

Wymagalność  
obligatoryjny

### Liczba godzin

Wykład  
14

Laboratorium  
24

Inne (np. online)  
0

Ćwiczenia  
0

Projekty/seminaria  
0

### Liczba punktów ECTS

4,00

### Koordynatorzy

mgr inż. Michał Weissenberg  
michal.weissenberg@put.poznan.pl

dr hab. inż. Sławomir Hanczewski  
slawomir.hanczewski@put.poznan.pl

### Wykładowcy

### Wymagania wstępne

Student rozpoczynający ten kurs powinien posiadać podstawową wiedzę z zakresu, sieci teleinformatycznych, systemów operacyjnych, systemów chmurowych oraz posiadać podstawowe umiejętności programowania. Powinien także posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł. Student powinien wykazywać takie cechy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla drugiego człowieka oraz gotowość do pracy w grupie.

## Cel przedmiotu

1. Zapewnienie studentom teoretycznych podstaw dotyczących systemów chmurowych. 2. Zapoznanie studentów z teoretycznymi informacjami na bezpieczeństwie infrastruktury systemów chmurowych. 3. Zapoznanie studentów z podstawowymi informacjami dotyczącymi zarządzania bezpieczeństwem systemów chmurowych oraz szacowaniem ryzyka. 4. Zapoznanie studentów z podstawowymi informacjami dotyczącymi bezpieczeństwa danych w systemach chmurowych. 5. Zapoznanie studentów z podstawowymi pojęciami dotyczącymi operacji bezpieczeństwa w chmurze oraz zarządzaniem tożsamością i dostępem

## Przedmiotowe efekty uczenia się

### Wiedza:

Student ma poszerzoną i pogłębioną wiedzę w zakresie urządzeń wchodzących w skład systemów teleinformatycznych, w szczególności systemów chmurowych [K2\_W02]

Student rozumie metodykę projektowania złożonych systemów teleinformatycznych; zna języki opisu sprzętu i komputerowe narzędzia do projektowania i symulacji systemów chmurowych [K2\_W04]

Student ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w zakresie teleinformatyki w obszarze systemów chmurowych [K2\_W07]

### Umiejętności:

Student potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie [K2\_U01]

Potrafi zaproponować ulepszenia lub rozwiązania alternatywne dla istniejących rozwiązań projektowych i systemów teleinformatycznych w obszarze systemów chmurowych [K2\_U9]

Potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć w zakresie technik, metod projektowania do projektowania i wytwarzania układów i systemów teleinformatycznych zawierających rozwiązania o charakterze innowacyjnym w obszarze systemów chmurowych [K2\_U10]

### Kompetencje społeczne:

Jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz do krytycznej oceny odbieranych treści [K2\_K01]

Jest gotów do myślenia i działania w sposób przedsiębiorczy [K2\_K05]

## 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: Wiedza jest weryfikowana poprzez test pisemny i/lub ustny składający się z 3-5 pytań. Ocena zaliczeniowa wynosi 51% punktów, a podczas testu nie wolno używać żadnych materiałów pomocniczych

Laboratorium: Wiedza jest weryfikowana na bieżąco podczas wykonywania zajęć laboratoryjnych na podstawie sprawozdań oraz poprzez kolokwium i/lub obronę projektu na końcu semestru. Ocena zaliczeniowa wynosi 51% punktów, a podczas zaliczenia nie wolno używać żadnych materiałów pomocniczych z wyjątkiem materiałów dostarczanych przez prowadzącego

## Treści programowe

### Tematyka wykładów:

- wprowadzenie do systemów chmurowych
- bezpieczeństwo infrastruktury w systemach chmurowych
- bezpieczeństwo komunikacji w systemach chmurowych
- bezpieczeństwo danych w systemach chmurowych
- zarządzanie bezpieczeństwem i ryzykiem w systemach chmurowych
- operacje bezpieczeństwa w systemach chmurowych
- testy penetracyjne, audyt i analityka bezpieczeństwa systemów chmurowych
- wirtualizacja i aplikacje w systemach chmurowych

### Tematyka laboratoriów:

zgodna z tematyką wykładów

## Tematyka zajęć

brak

## Metody dydaktyczne

Wykład: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy oraz pokazami praktycznymi.

Ćwiczenia laboratoryjne: ćwiczenia praktyczne wykonywane samodzielnie lub w grupach z wykorzystaniem komputera.

## Literatura

Podstawowa:

Chris Dotson, Bezpieczeństwo w chmurze, Wydawnictwo Naukowe PWN, 2020

Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021

Uzupełniająca

P. Mishra, E. S. Pilli, R. C. Joshi, "Cloud Security: Attacks, Techniques, Tools, and Challenges", CRC Press.,

2021 (<https://www.amazon.com/Cloud-Security-Attacks-Techniques-Challenges-ebook/dp/B09MTT5D3T>)

J. R. Vacca, "Cloud Computing Security: Foundations and Challenges". CRC Press, 2016

(<https://www.amazon.com/Cloud-Computing-Security-Foundations-Challenges/dp/1482260948>)

C. Dotson, "Practical Cloud Security: A Guide for Secure Design and Deployment", O'Reilly Media, 2019 (<https://www.amazon.com/Practical-Cloud-Security-Secure-Deployment/dp/1492037516>)

## Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	103	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	38	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	65	2,50