**Nazwa przedmiotu:**

Bezpieczeństwo w cloud computing

**Koordynator przedmiotu:**

Dr hab. inż. Katarzyna Rostek, prof. PW

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Zarządzanie

**Grupa przedmiotów:**

Specjalność: Zarządzanie w gospodarce cyfrowej

**Kod przedmiotu:**

BezClo

**Semestr nominalny:**

6 / rok ak. 2022/2023

**Liczba punktów ECTS:**

2

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

2 ECTS
15h wykład + 15h projekt + 8h opracowanie projektu + 4h studiowanie literatury + 3h udział w konsultacjach + 5h przygotowanie do zaliczenia przedmiotu = 50h

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

1,3 ECTS

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

-

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład:  | 15h |
| Ćwiczenia:  | 0h |
| Laboratorium:  | 0h |
| Projekt:  | 15h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Podstawy programowania, baz danych, sieci komputerowych, systemów operacyjnych.

**Limit liczby studentów:**

- od 15 osób do limitu miejsc w sali audytoryjnej (wykład) - od 8 osób do limitu miejsc w sali laboratoryjnej (projekt)

**Cel przedmiotu:**

Zapoznanie studenta z wybranymi technologiami witalizacyjnymi i chmurowymi oraz z aktualnym otoczeniem teleinformatycznym przedsiębiorstwa pełnym zagrożeń, nowych zjawisk i trendów w obszarze cyberbezpieczeństwa w tym bezpieczeństwa wirtualizacji i infrastruktury chmurowej. Dobre praktyki w ochronie danych w chmurze obliczeniowej. Wskazanie metod pozyskania wiedzy i praktyki w podejściu do bezpieczeństwem systemów teleinformatycznych w rozwiązaniach chmurowych.

**Treści kształcenia:**

Wykład:
1. Cyberbezpieczeństwo
2. Zagrożenia i zabezpieczenia
3. Cloud Computing
Projekt:
1. Analiza przypadku 1. Analiza rzeczywistego incydentu w zakresie cyberbezpieczeństwa (Na podstawie informacji prasowych, opisu branżowego itp.) Wyjaśnienie od strony technicznej i organizacyjnej incydentu. Dyskusja.
2. Analiza przypadku 2. Analiza koncepcji rozwiązań zabezpieczających przed wybranymi incydentami bezpieczeństwa. Wyjaśnienie od strony technicznej i organizacyjnej. Dyskusja.
3. Laboratorium obrazujące wybrane rozwiązanie chmurowe w tym aspekt użytkowy oraz techniczny ataku i ochrony.
4. Projekt zespołowy / konsultacje merytoryczne na wybrany temat: „Analiza wybranego przypadku, wybranego incydentu, analiza w podejściu technicznym i organizacyjnym…”, „Opracowanie koncepcji rozwiązania technicznego dla organizacji … w oparciu o technologię Cloud Computing – uruchomienie prototypu.”
5. Przekazanie w ustalonych terminach kolejnych fragmentów pracy zawierających elementy takie jak: sformułowanie celu, przeprowadzenie analizy i diagnozy bieżącego stanu organizacji, identyfikacja oczekiwanej funkcjonalności, dobór i sposób wykorzystania narzędzi, sformułowanie założeń dla rozwiązania, kosztorys, harmonogram wdrożenia.
Prezentacja projektów, dyskusja.

**Metody oceny:**

Wykład:
1. Ocena formatywna: kolokwium zaliczeniowe;
2. Ocena sumatywna : Ocena kolokwium zaliczeniowego; ocena w zakresie 2-5; Do zaliczenia wymagane jest uzyskanie oceny >=3
Projekt:
1. Ocena formatywna: projekt, prezentacja.
2. Ocena sumatywna: ocena punktowa ustalana na podstawie sumarycznej liczby punktów uzyskanych z ćwiczeń i projektu (max 60pkt) oraz ocena liczbowa: skala ocen (2,0; 3,0; 3,5; 4,0; 4,5; 5,0).
Końcowa ocena z przedmiotu: Ocena końcowa w zakresie 2-5, wyliczania zgodnie z wagami (kolokwium zaliczeniowe - 0,5 oraz projekt - 0, 5); Do zaliczenia wymagane jest uzyskanie oceny >=3

**Egzamin:**

nie

**Literatura:**

Obowiązkowa:
1. Mather T., Kumaraswamy S.,Latif S., 2009, Cloud Security and Privacy, O’Railly
2. Vacca J., 2017, Cloud Computing Security, CRC Press Taylor & Francis Group
Uzupełniająca:
1. McNab, C., 2017, Ocena bezpieczeństwa sieci, Warszawa: Promise.
2. Stallings W., 2012, Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Gliwice: Helion
3. McNab, C., 2017. Network Security Assessment, O'Reilly

**Witryna www przedmiotu:**

moodle.usos.pw.edu.pl

**Uwagi:**

-

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka Z1\_WG9:**

Absolwent zna i rozumie w zaawansowanym stopniu współczesne technologie informacyjne, w tym narzędzia przetwarzania danych w chmurze (cloud computing), co pozwala mu być świadomym ich użytkownikiem i znaleźć ich zastosowania w organizacjach w cyfrowej gospodarce

Weryfikacja:

Wykład – pisemne zaliczenie
Projekt - Zaliczenie projektu

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka Z1\_UW1:**

Absolwent potrafi wykorzystywać posiadaną wiedzę do formułowania i rozwiązywania złożonych i nietypowych problemów z zakresu bezpieczeństwa w cloud computing, w szczególności w zakresie analizy i oceny problemu, syntezy informacji, formułowania wymagań oraz proponowania rozwiązań z zakresu bezpieczeństwa w cloud computing

Weryfikacja:

Projekt - Zaliczenie projekt

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

**Charakterystyka Z1\_UW5:**

Absolwent potrafi wykorzystywać posiadaną wiedzę do analizy potrzeb biznesowych, w tym oczekiwań i potrzeb klientów w warunkach ciągłej transformacji gospodarki. Do w/w analiz dobiera oraz stosuje poznane metody i narzędzia cloud computing, dbając o bezpieczeństwo danych

Weryfikacja:

Projekt - Zaliczenie projektu

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka Z1\_KK1, Z1\_KK2, Z1\_KO4:**

Absolwent rozumie jak istotna jest jego własna wiedza z zakresu zarządzania bezpieczeństwem w cloud computing dla funkcjonowania i pokonywania problemów w organizacji oraz dla działania w sposób przedsiębiorczy. Jest gotów do jej krytycznej oceny i zasięgania opinii ekspertów w tej dziedzinie

Weryfikacja:

Projekt - Zaliczenie projektu

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**