**Nazwa przedmiotu:**

Bezpieczeństwo w cloud computing

**Koordynator przedmiotu:**

mgr inż. Pięta Sylwester

**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. 2020/2021

**Liczba punktów ECTS:**

2

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

2 ECTS
30h projekt + 6h opracowanie projektu + 4h studiowanie literatury + 5h udział w konsultacjach + 5h przygotowanie do zaliczenia przedmiotu = 50h

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

1,40ECTS
30h projekt + 5h konsultacje = 35h

**Język prowadzenia zajęć:**

polski

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

2 ECTS
30h projekt + 6h opracowanie projektu + 4h studiowanie literatury + 5h udział w konsultacjach + 5h przygotowanie do zaliczenia przedmiotu = 50h

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

|  |  |
| --- | --- |
| Wykład:  | 0h |
| Ćwiczenia:  | 0h |
| Laboratorium:  | 0h |
| Projekt:  | 30h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

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

**Limit liczby studentów:**

- od 25 osób do limitu miejsc w sali audytoryjnej (wykład) - od 25 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:**

D. Projekt:
1-2. Analiza przypadku 1. Analiza rzeczywistego incydentu w zakresie cyberbezpieczeństwa (Na podstawie informacji prasowych, opisu branżowego itp.) Wyjaśnienie od strony technicznej i organizacyjnej incydentu. Dyskusja.
3-4. Analiza przypadku 2. Analiza koncepcji rozwiązań zabezpieczających przed wybranymi incydentami bezpieczeństwa. Wyjaśnienie od strony technicznej i organizacyjnej. Dyskusja.
5-7. Laboratorium obrazujące wybrane rozwiązanie chmurowe w tym aspekt użytkowy oraz techniczny ataku i ochrony.
8-14. 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.”
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.
15. Prezentacja projektów, dyskusja.

**Metody oceny:**

D. Projekt:
1. Ocena formatywna: projekt, prezentacja.
2. Ocena sumatywna: ocena punktowa ustalana na podstawie suma-rycznej 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).

**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

**Witryna www przedmiotu:**

www.olaf.wz.pw.edu.pl

**Uwagi:**

-

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt Z1\_W07:**

Absolwent zna i rozumie teorie oraz ogólną metodologię badań w zakresie identyfikacji, tworzenia i optymalizacji procesów, ze szczególnym uwzględnieniem procesów zarządzania.

Weryfikacja:

Kolokwia, ocena projektu, egzamin.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt Z1\_W12:**

Absolwent zna i rozumie podstawowe procesy zachodzące w cyklu życia systemów zarządzania

Weryfikacja:

Kolokwia, ocena projektu.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Efekt Z1\_U06:**

Absolwent potrafi identyfikować i interpretować podstawowe zjawiska i procesy społeczne z wykorzystaniem wiedzy z zakresu identyfikacji, tworzenia i optymalizacji procesów, ze szczególnym uwzględnieniem procesów zarządzania

Weryfikacja:

Kolokwia, ocena projektu.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt Z1\_U17:**

Absolwent potrafi projektować nowe rozwiązania, jak również doskonalić istniejące, zgodnie z przyjętymi założeniami ich realizacji i wdrożenia.

Weryfikacja:

Kolokwia, ocena projektu.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt Z1\_K01:**

Absolwent jest gotów do krytycznej oceny posiadanej wiedzy.

Weryfikacja:

Kolokwia, ocena projektu.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt Z1\_K02:**

Absolwent jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych

Weryfikacja:

Kolokwia, ocena projektu.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**