**Nazwa przedmiotu:**

Bezpieczeństwo systemów teleinformatycznych

**Koordynator przedmiotu:**

mgr inż. Pięta Sylwester

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Inżynieria Zarządzania

**Grupa przedmiotów:**

Specjalność: Bezpieczeństwo i zarządzanie ciągłością działania

**Kod przedmiotu:**

-

**Semestr nominalny:**

3 / rok ak. 2018/2019

**Liczba punktów ECTS:**

2

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

2 ECTS:
10h wykład + 15h ćwiczenia + 5h konsultacje+ 10h przygotowanie do ćwiczeń + 10h przygotowanie do projektu = 50h

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

1,1 ECTS:
10h wykład + 15h ćwiczenia + 5h konsultacje =30h

**Język prowadzenia zajęć:**

polski

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

1,6 ECTS:
15h ćwiczenia + 5h konsultacje + 10h przygotowanie do ćwiczeń + 10h przygotowanie do projektu = 40h

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

|  |  |
| --- | --- |
| Wykład:  | 12h |
| Ćwiczenia:  | 12h |
| Laboratorium:  | 0h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Wiedza z zakresu: sieci komputerowe, systemy operacyjne

**Limit liczby studentów:**

- od 25 osób do limitu miejsc w sali audytoryjnej (wykład) - od 25 osób do limitu miejsc w sali laboratoryjnej (ćwiczenia)

**Cel przedmiotu:**

Opanowanie przez studentów wiedzy z zakresu teorii i praktyki w zarządzaniu bezpieczeństwem systemów teleinformatycznych.

**Treści kształcenia:**

A. Wykład:
1-2. Wprowadzenie do zagadnień bezpieczeństwa systemu informatycznego. Bezpieczeństwo systemów IT w odniesieniu do celów, strategii oraz polityki bezpieczeństwa organizacji. Techniczne wytyczne zabezpieczeń dla systemów informatycznych na podstawie: norm, dobrych praktyk, zaleceń odpowiednich organów regulacyjnych państwa lub branży.
3-4. Wytyczne wg norm: PN-ISO/IEC 27002: Organizacja bezpieczeństwa informacji. Organizacja wewnętrzna. Urządzenia mobilne i telepraca. Bezpieczeństwo zasobów ludzkich. Bezpieczeństwo informacji w relacjach z dostawcami.
5-6. Zarządzanie aktywami (sprzęt i oprogramowanie). Postępowanie z nośnikami. Kontrola dostępu. Zabezpieczenia kryptograficzne. Zarządzanie bezpieczeństwem sieci.
7-8. Bezpieczna eksploatacja: Dokumentowanie procedur eksploatacyjnych. Zarządzanie zmianami. Ochrona przed szkodliwym oprogramowaniem. Kopie zapasowe. Nadzór nad oprogramowaniem produkcyjnym. Zarządzanie podatnościami technicznymi. Pozyskiwanie, rozwój i utrzymanie systemów. Wybrane aspekty zarządzania ciągłością działania.
9-10. Zarządzanie incydentami związanymi z bezpieczeństwem informacji. Rejestrowanie zdarzeń. Systemy SIEM (ang. Security Information and Event Management) i organizacja SOC (ang. Security Operations Center). Audyt systemów informacyjnych.
B. Ćwiczenia:
1-2. Przegląd norm i dobrych praktyk. Przegląd przykładowej dokumentacji dot. bezpiecznej eksploatacji, ciągłości działania. Dyskusja.
3-4. Analiza przypadku 1. Analiza zdarzeń/przypadków z zakresu incydentu naruszenia bezp. teleinformatycznego w hipotetycznych organizacjach. (Na podstawie opisu/dokumentacji przedsiębiorstwa)
5-6. Analiza przypadku 2. Wskazanie słabych punktów, potencjalnych zagrożeń, propozycji naruszenia bezpieczeństwa w przykładowych hipotetycznych organizacjach. (Na podstawie opisu/dokumentacji przedsiębiorstwa)
7-8. Laboratorium: Testowanie wybranej technologii zabezpieczającej.
9-12. Projekt zespołowy - Opracowanie dokumentacji systemu zarządzania bezpieczeństwem IT dla hipotetycznej organizacji we wskazanej branży.
13-14 Prezentacja projektów, dyskusja.
15 Zaliczenie

**Metody oceny:**

A. Wykład:
1. Ocena formatywna: zadanie projektowe (wykonywane w zespołach) oraz test wielokrotnego wyboru (perforowana forma elektroniczna).
2. Ocena sumatywna : ocena punktowa za zadane i test (max 40pkt) oraz ocena liczbowa; skala ocen (2,0; 3,0; 3,5; 4,0; 4,5; 5,0).
B. Ćwiczenia:
1. Ocena formatywna: kolokwium, 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).
E. Końcowa ocena z przedmiotu: Wynik punktowy – suma punktów z wykładu i ćwiczeń, wynikowa ocena liczbowa wg skali ocen
(0-50pkt-2,0; 51-60pkt-3,0; 61-70pkt-3,5; 71-80pkt-4,0; 81-90pkt-4,5; 91-100pkt-5,0)

**Egzamin:**

nie

**Literatura:**

Obowiązkowa:
1. Wołowski F., Zawiła-Niedźwiecki J., 2012 , Bezpieczeństwo systemów informacyjnych, Warszawa: Edu-Libri,
2. Górka M. (red.), 2014, Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Warszawa: Difin
3. Rot A., 2008, Zarządzanie ryzykiem jako element ładu informatyczne-go, Katedra Inżynierii Systemów Informatycznych Zarządzania, Uniwersytet Ekonomiczny we Wrocławiu.
Uzupełniająca:
1. Normy ISO/IEC 27001:2013, System Zarządzania bezpieczeństwem informacji

**Witryna www przedmiotu:**

www.olaf.wz.pw.edu.pl

**Uwagi:**

-

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt I2\_W04:**

absolwent zna i rozumie podstawowe procesy zachodzące w cyklu życia systemów i procesów zarządzania

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt I2\_W07:**

absolwent zna i rozumie główne trendy rozwojowe w zakresie nauk o zarządzaniu

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Efekt I2\_U06:**

absolwent potrafi analizować, prognozować i modelować złożone procesy społeczne z wykorzystaniem zaawansowanych metod i narzędzi z zakresu zarządzania, w tym narzędzi IT

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt I2\_U17:**

absolwent potrafi dokonywać krytycznej analizy stanu obecnego oraz jego niewystarczalności w stosunku do stanu oczekiwanego

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt I2\_K01:**

absolwent jest gotów do krytycznej oceny odbieranych treści

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt I2\_K02:**

absolwent jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz konieczności samokształcenia się przez całe życie

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**