**Nazwa przedmiotu:**

Cyberbezpieczeństwo w gospodarce cyfrowej

**Koordynator przedmiotu:**

mgr inż. Pięta Sylwester

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Zarządzanie

**Grupa przedmiotów:**

Specjalność: Zarządzanie ekosystemem przedsiębiorczości

**Kod przedmiotu:**

-

**Semestr nominalny:**

2 / rok ak. 2020/2021

**Liczba punktów ECTS:**

2

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

2 ECTS:
8h wykład + 18h ćwiczenia + 5h konsultacje + 5h studia literaturowe + 14h przygotowanie do ćwiczeń i projektu = 50h

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

1,24 ECTS:
8h wykład + 18h ćwiczenia + 5h konsultacje = 31h

**Język prowadzenia zajęć:**

polski

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

1,68 ECTS:
18h ćwiczenia + 5h konsultacje + 5h studia literaturowe + 14h przygotowanie do ćwiczeń i projektu = 42h

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

|  |  |
| --- | --- |
| Wykład:  | 8h |
| Ćwiczenia:  | 18h |
| Laboratorium:  | 0h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Podstawy programowania, Sieci komputerowe, Bezpieczeństwo systemów operacyjnych

**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:**

Zapoznanie studentów z aktualnym otoczeniem teleinformatycznym przedsiębiorstwa pełnym zagrożeń, nowych zjawisk i trendów w obszarze cyberbezpieczeństwa. Wskazanie metod pozyskania wie-dzy i praktyki w podejściu do bezpieczeństwem systemów telein-formatycznych.

**Treści kształcenia:**

A. Wykład:
1-2. Wprowadzenie do zagadnień cyberzagrożeń i cyberbezpieczeństwa. Bezpieczeństwo systemów IT w odniesieniu do celów, strategii oraz polityki bezpieczeństwa organizacji. Techniczne wytyczne zabezpieczeń dla systemów informatycznych na podstawie: norm, dobrych praktyk, zaleceń organów regulacyjnych państwa lub branży.
3-4. Najważniejsze aktualne trendy w dziedzinie bezpieczeństwa: AI, Ransomware, wymagające regulacje prawne, ataki na bezserwerowe aplikacje, ochrona prywatności, wielkie zbiory danych, ataki na krypowaluty, zakłócenia w internecie rzeczy, blockchain w bezpieczeństwie, bezpieczeństwo chmury, bezpieczeństwo devops, zagrożenia mobilne…
5-6 Rozwinięcie wybranych tematów: Sieci bezprzewodowe. Internet rzeczy – IoT. Przemysłowy Internet Rzeczy (IIoT). Przemysł 4.0. Bezprzewodowa sieć sensorowa (WSN). Rozproszenie danych: w „chmurze obliczeniowej”, urządzeniach mobilnych, na urządzaniach prywatnych (BYOD). Zagadnienia z obszaru zapewnienia bezpieczeństwa w środowisku automatyki przemysłowej (OT).
7-8. Wytyczne zabezpieczeń wg norm: PN-ISO/IEC 27002: Organizacja bezpieczeństwa informacji. Urządzenia mobilne i telepraca. Bezpieczeństwo zasobów ludzkich. Relacje z dostawcami. Sprzęt i oprogramowanie. Postępowanie z nośnikami. Kontrola dostępu. Zabezpieczenia kryptograficzne. Bezpieczeństwo sieci.
9-10. Bezpieczna eksploatacja: Dokumentowanie procedur eksploatacyjnych. Zarządzanie zmianami. Ochrona przed szkodliwym oprogramowaniem. Kopie zapasowe. Zarządzanie podatnościami technicznymi. Pozyskiwanie, rozwój i utrzymanie aplikacji i systemów. Wybrane aspekty zarządzania ciągłością działania. Zarządzanie incydentami dot. bezpieczeństwa. Rejestrowanie zdarzeń. Systemy SIEM i organizacja SOC. Audyt systemów informacyjnych.
B. Ćwiczenia:
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 rzeczywistego incydentu. (jw.)
5-6. Analiza przypadku 3. Analiza koncepcji rozwiązań zabezpieczających przed wybranymi incydentami bezpieczeństwa. Wyjaśnienie od strony technicznej i organizacyjnej. Dyskusja.
7-8. Laboratorium obrazujące wybrany aspekt techniczny ataku: Wykorzystanie gotowych narzędzi i przykładowe techniki ataku.
9-12. Projekt zespołowy - analiza wybranego przypadku/ przegląd wybranego incydentu – analiza w podejściu technicznym i organizacyjnym. Opracowanie koncepcji ochrony 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 (max 50pkt) 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 (max 50pkt) 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 sys-temów 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 informa-tycznego, Katedra Inżynierii Systemów Informatycznych Za-rządzania, Uniwersytet Ekonomiczny we Wrocławiu.
Uzupełniająca:
1. Normy ISO/IEC 27001:2013, System Zarządzania bezpieczeń-stwem informacji
2. Raporty czołowych producentów rozwiązań w zakresie bezpie-czeństwa IT.

**Witryna www przedmiotu:**

www.olaf.wz.pw.edu.pl

**Uwagi:**

-

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt Z2\_W12:**

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

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt Z2\_W13:**

absolwent zna i rozumie fundamentalne dylematy współczesnej cywilizacji w zakresie społecznej odpowiedzialności biznesu oraz zrównoważonego rozwoju

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Efekt Z2\_U08:**

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

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt Z2\_U16:**

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

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt Z2\_K01:**

krytycznej oceny odbieranych treści

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt Z2\_K02:**

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:**