**Nazwa przedmiotu:**

Warsztaty projektowe - Projekt polityki bezpieczeństwa

**Koordynator przedmiotu:**

Dr inż. Katarzyna Skroban

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Zarządzanie

**Grupa przedmiotów:**

Specjalność: Zarządzanie w gospodarce cyfrowej

**Kod przedmiotu:**

WP\_Cyber

**Semestr nominalny:**

6 / rok ak. 2022/2023

**Liczba punktów ECTS:**

2

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

2 ECTS:
30h projekt + 12h przygotowanie studenta do zajęć, analiza literatury, przygotowanie projektu, prezentacji + 3h konsultacje + 5h przygotowanie do zaliczenia = 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:  | 0h |
| Ćwiczenia:  | 0h |
| Laboratorium:  | 0h |
| Projekt:  | 30h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Pozytywne zaliczenie przedmiotów modułu Cyberbezpieczeństwo z zakresu IV, V i VI semestru oraz wybranych przedmiotów z modułu Zarządzanie oraz IT w Zarządzaniu: Podstawy zarządzania projektami;
Architektura korporacyjna; Zarządzanie usługami IT; Inżynieria wymagań; Sieci komputerowe; Podstawy programowania (opc.); Bezpieczeństwo systemów operacyjnych; Podstawy kryptografii; Zagadnienia prawne i normalizacyjne w IT; System zarządzania bezpieczeństwem informacji; Zarządzanie ryzykiem; Bezpieczeństwo cloud computing; Zarządzanie obecnością internetową.

**Limit liczby studentów:**

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

**Cel przedmiotu:**

Celem przedmiotu jest podsumowanie wiedzy z zakresu cyberbezpieczeństwa poprzez wykonanie indywidualnego zadania projektowego w obszarze polityki i zarządzania bezpieczeństwem IT. Student wykonuje pełny lub częściowy projekt polityki bezpieczeństwa dla wybranej, funkcjonującej lub hipotetycznej organizacji. Projekt zostaje wykonamy w oparciu o dostępne systemy norm lub biblioteki dobrych praktyk.

**Treści kształcenia:**

Projekt:
Praktyczna analiza przypadków i przykłady dobrych praktyk:
1. Analiza wybranego incydentu;
2. Przykłady zastosowania najważniejszych standardów, regulacji prawnych i dobrych praktyk w odniesieniu do bezpieczeństwa IT;
3. Przykłady dobrych praktyk wdrożenia systemów BCM;
4. Przykład Polityki Bezpieczeństwa Informacji;
5. Funkcja Administratora bezpieczeństwa informacji;
6. Audyt bezpieczeństwa;
7. Zabezpieczenia techniczne i organizacyjne systemów informatycznych.
Konsultacje merytoryczne dot. projektu:
8. Ustalenie tematu i omówienie szablonów projektów: Projekt polityki bezpieczeństwa…; Projekt system zarządzania bezpieczeństwem informacji…; Projekt planu ciągłości działania…; Projekt instrukcji typu: Wytyczne zabezpieczeń dla syst. informatycznych…
9. Przekazanie kolejnych fragmentów pracy (5 terminów) zawierających elementy takie jak: sformułowanie celu, przeprowadzenie analizy i diagnozy bieżącego stanu organizacji, identyfikacja i sformułowanie problemu w organizacji, dobór i sposób wykorzystania narzędzi (systemu zarządzania, praktyk…), sformułowanie założeń dla rozwiązania problemu, analiza ryzyka, rozwiązanie problemu (projekt, dokumentacja…) oraz wykazanie jego opłacalności i zasadności wdrożenia do praktyki, harmonogram wdrożenia.
10. Prezentacja projektów – dyskusja.

**Metody oceny:**

Projekt:
1. Ocena formatywna: Zaliczenie w formie pisemnej i prezentacji – projekt polityki bezpieczeństwa dla wybranej, funkcjonującej lub hipotetycznej organizacji (realizacja indywidualna). Weryfikacja zawartości i terminowości oddania fragmentów materiału przygotowywanego przez studenta, rozmowy konsultacyjne, prezentacja końcowa.
2. Ocena sumatywna: Ocena merytoryczna przygotowanego materiału stanowi podstawę do zaliczenia przedmiotu i wystawienia oceny.
W zakres oceny wchodzą:
a. realizacja i zawartość projektu (w tym sformułowanie celu, dobór i sposób wykorzystania narzędzi, analiza literaturowa, dobór i sposób wykorzystania źródeł) - 80%;
b. układ i redakcja pracy (struktura formalna, przejrzystość, staranność edytorska, poprawność języka, wykorzystanie materiału ilustracyjnego) - 10%;
c. prezentacja projektu końcowego - 10%.

**Egzamin:**

nie

**Literatura:**

Obowiązkowa:
1. Gałaj-Emiliańczyk K., 2020, Wdrożenie systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001:2019, ODDK Ośrodek Doradztwa i Doskonalenia Kadr
2. Vacca J., 2017, Cloud Computing Security, CRC Press Taylor & Francis Group
3. Abhishek C., MukundImplementing C., 2020. Implementing an Information Security Management System. Security Management Based on ISO 27001 Guidelines. Apress
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:**

moodle.usos.pw.edu.pl

**Uwagi:**

-

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka Z1\_WG4:**

Absolwent zna i rozumie w zaawansowanym stopniu teorie, metody i narzędzia z zakresu analizy potrzeb biznesowych, w tym zapewnienia bezpieczeństwa w obszarze zarządzania technologiami informacyjnymi (IT)

Weryfikacja:

Projekt - Zaliczenie pisemne projektu i prezentacji

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka Z1\_UW3:**

Absolwent analizując oraz krytycznie oceniając istniejące w organizacji rozwiązania potrafi zaproponować ich usprawnienie, wykorzystując poznane metody i narzędzia z zakresu bezpieczeństwa IT

Weryfikacja:

Projekt - Zaliczenie pisemne projektu i prezentacji

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

**Charakterystyka Z1\_UW4:**

Absolwent potrafi wykorzystać posiadaną wiedzę do zastosowania właściwie dobranych metodyk zarządzania projektami w odniesieniu do projektu polityki bezpieczeństwa IT w organizacji

Weryfikacja:

Projekt - Zaliczenie pisemne projektu i prezentacji

**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 polityki bezpieczeństwa IT 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 pisemne projektu i prezentacji

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**