**Nazwa przedmiotu:**

Warsztaty projektowe - Projekt polityki bezpieczeństwa

**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:**

-

**Semestr nominalny:**

6 / rok ak. 2018/2019

**Liczba punktów ECTS:**

4

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

4 ECTS:
10h wykład + 30h projekt + 70h przygotowanie studenta do zajęć, analiza literatury, przygotowanie projektu, prezentacji + 5h konsultacje + 5h przygotowanie do zaliczenia = 120h

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

1,5 ECTS:
10h wykład + 30h projekt + 5 h konsultacje = 45h

**Język prowadzenia zajęć:**

polski

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

3 ECTS:
30h projekt + 50h przygotowanie studenta do zajęć, przygotowanie projektu, prezentacji + 5h konsultacje + 5h przygotowanie do zaliczenia = 90h

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

|  |  |
| --- | --- |
| Wykład:  | 13h |
| Ćwiczenia:  | 0h |
| Laboratorium:  | 0h |
| Projekt:  | 27h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Pozytywne zaliczenie przedmiotów modułu Cyberbezpieczeństwo z zakresu IV, V i VI semestru oraz wybranych przedmiotów z modułu Za-rządzanie 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 25 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:**

A. Wykład:
1. Podsumowanie zagadnień dotyczących cyberbezpieczeństwa w zakresie środków technicznych, aspektów prawnych cyberprzestępczości, zarządzania bezpieczeństwem informacji, ochrony danych osobowych, zarządzania ryzykiem oraz zarządzania ciągłością działania zarówno w obszarze indywidualnym (obywatel) jak i przedsiębiorstwa (organizacji) czy państwa.
2. Typologia zagrożeń i ataków na systemy IT i OT. Statystyki z raportów wiodących firm i organizacji oraz tendencje i kierunki rozwoju w przyszłości. Systemy ochrony. Testy penetracyjne i reakcja na incydenty.
3. Podstawowe zagadnienia związane z procesami zarządzania ciągłością działania, aspekty prawne i normalizacyjne, ciągłość działania a zarządzanie ryzykiem, polityka i strategie zarządzania ciągłością działania, plan ciągłości działania, miejsce systemów IT obszarze zarządzania ciągłością działania
4. Przegląd najważniejszych standardów, regulacji prawnych i dobrych praktyk w odniesieniu do bezpieczeństwa IT. Ochrona informacji niejawnych. Obowiązek ochrony danych osobowych, aspekty prawne ochrony danych osobowych w kontekście prawa osób oraz odpowiedzialności za naruszenie ustawy. Organy ochrony danych osobowych. Anonimizacja danych. Certyfikacja i kodeks etyki zawodowej.
5. Przykłady dobrych praktyk. Kompozycja bezpieczeństwa IT w układzie: Cele i strategia organizacji; Polityka w zakresie bezpieczeństwa organizacji; Cele, strategia, polityka w zakresie bezpieczeństwa systemów informacyjnych w organizacji; System Zarządzania Bezpieczeństwem Informacji; Wytyczne zabezpieczeń dla syst. informatycznych.
6. Zaliczenie.
D. 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:**

A. Wykład:
1. Ocena formatywna: Test.
2. Ocena sumatywna: Wykład zostaje zaliczony na podstawie liczby zebranych punktów (>=51% max liczby punktów): ocena 3.0: 51%-60%pkt; 3.5: 61%-70%pkt; 4.0: 71%-80%pkt; 4,5: 81%-90%pkt; 5.0: 91%-100%pkt;
D. 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%.
E. Końcowa ocena z przedmiotu:
Ocena końcowa wystawiana jest z zachowaniem wagi ocen składowych:
20% oceny z wykładu; 80% oceny z projektu.
Warunkiem zaliczenia przedmiotu jest:
a. zaliczenie wykładu;
b. terminowość realizacji poszczególnych etapów projektu oraz obecność na warsztatach projektowych w terminach realizacji etapów;
c. obowiązkowa prezentacja projektu w wyznaczonym terminie;
d. czynny udział w dyskusji na temat pracy projektowej po prezentacji końcowej.

**Egzamin:**

nie

**Literatura:**

Obowiązkowa:
Literatura wskazana w poszczególnych przedmiotach modułu Cyber(bezpieczeństwo) ze szczególnym uwzględnieniem adekwatnej do celu realizowanego projektu, m.in.:
1. Tanenbaum A. S., Wetherall D. J., 2012, Sieci komputerowe, Gliwice: Helion
2. Tanenbaum A. S., Bos H., 2015, Systemy operacyjne, Gliwice: Helion
3. Stinson D. R., 2005, Kryptografia w teorii i w praktyce, Warszawa: WNT
4. J. Krawiec, G. Ożarek., 2014, System Zarządzania Bezpieczeństwem Informacji w praktyce. Zabezpieczenia., Warszawa: PKN
5. Liderman K., 2012, Bezpieczeństwo informacyjne, Warszawa: PWN
6. Wołowski F., Zawiła-Niedźwiecki J., 2012, Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, Warszawa: edu-Libri
7. Jatkiewicz P., 2015, Ochrona danych osobowych. Teoria i praktyka, Warszawa: Polskie Towarzystwo Informatyczne
Uzupełniająca:
1. Norma PN-ISO/IEC 27001:2014-12 - wersja polska, 2017, Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania, Warszawa: PKN
2. PN-I-13335-1:1999 - wersja polska, 1999, Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych, Warszawa: PKN
3. Norma PN-EN ISO 22301:2014-11 - wersja angielska, Bezpieczeństwo powszechne - Systemy zarządzania ciągłością działania – Wymagania, Warszawa: PKN

**Witryna www przedmiotu:**

www.olaf.wz.pw.edu.pl

**Uwagi:**

-

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt Z1\_W09:**

Absolwent zna i rozumie teorie oraz ogólną metodologię badań w zakresie zastosowań narzędzi informatycznych w zarządzaniu, ze szczególnym uwzględnieniem działań podejmowanych w środowisku internetowym

Weryfikacja:

Weryfikacja materiału przygotowanego przez studenta, rozmowy konsultacyjne.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt Z1\_W12:**

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

Weryfikacja:

Weryfikacja materiału przygotowanego przez studenta, rozmowy konsultacyjne.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Efekt Z1\_U01:**

Absolwent potrafi identyfikować i interpretować podstawowe zjawiska i procesy społeczne z wykorzystaniem wiedzy z zakresu zarządzania, ze szczególnym uwzględnieniem uwarunkowań zarządzania przedsiębiorstwem/organizacją oraz zarządzania projektami

Weryfikacja:

Realizacja projektu.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt Z1\_U13:**

Absolwent potrafi prawidłowo posługiwać się systemami normatywnymi w celu rozwiązywania zadań z zakresu nauk o zarządzaniu, ze szczególnym uwzględnieniem różnych systemów zarządzania.

Weryfikacja:

Realizacja projektu, rozmowy konsultacyjne.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt Z1\_K04:**

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

Weryfikacja:

Realizacja projektu, rozmowy konsultacyjne.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt Z1\_K01:**

Absolwent jest gotów do krytycznej oceny posiadanej wiedzy

Weryfikacja:

Realizacja projektu.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**