**Nazwa przedmiotu:**

Obszary bezpieczeństwa w organizacji

**Koordynator przedmiotu:**

mgr inż. Pięta Sylwester

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Zarządzanie Bezpieczeństwem Infrastruktury Krytycznej

**Grupa przedmiotów:**

Kierunkowe

**Kod przedmiotu:**

-

**Semestr nominalny:**

4 / rok ak. 2019/2020

**Liczba punktów ECTS:**

1

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

1 ECTS
10h ćwiczenia + 2h konsultacje + 5h studia literaturowe + 5h przygotowanie do ćwiczeń + 8h przygotowanie do projektu = 30h

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

0,40 ECTS
10h ćwiczenia + 2h konsultacje = 12h

**Język prowadzenia zajęć:**

polski

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

1 ECTS
10h ćwiczenia + 2h konsultacje + 5h studia literaturowe + 5h przygotowanie do ćwiczeń + 8h przygotowanie do projektu = 30h

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

|  |  |
| --- | --- |
| Wykład: | 0h |
| Ćwiczenia: | 15h |
| Laboratorium: | 0h |
| Projekt: | 0h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Podstawy bezpieczeństwo danych, informacji i systemów teleinformatycznych, Podstawy kryptografii, Technologiczne wspieranie bezpieczeństwa

**Limit liczby studentów:**

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

**Cel przedmiotu:**

Zapoznanie studentów z aktualnym otoczeniem wewnętrznym i zewnętrznym przedsiębiorstwa w kontekście obszarów bezpieczeństwa w organizacji. Wskazanie metod identyfikacji, klasyfikacji i charaktery-styki obszarów bezpieczeństwa w organizacji.

**Treści kształcenia:**

B. Ćwiczenia:
1-2. Wprowadzenie w tematykę obszarów bezpieczeństwa w organizacji. Całościowe, systemowe spojrzenie na procesy zarządzania w organizacji w kontekście utrzymania bezpieczeństwa na zamierzonym poziomie. Otoczenie informacyjne i teleinformatyczne przedsiębiorstw. Aktualne zjawiska i trendy w odniesieniu do bezpieczeństwa. Typologia aktualnych zagrożeń w różnych obszarach. Statystyki.
3-4. Mapa obszarów i określenia elementów składowych organizacji, uwzględniająca możliwie najszersze ujęcie w odniesieniu do zagrożeń i utrzymania bezpieczeństwa. Bezpieczeństwo fizyczne i środowiskowe, bezpieczeństwo techniczne, bezpieczeństwo systemów informatycznych, bezpieczeństwo finansowe, bezpieczeństwo osobowe i ochrona prywatności (systemy biometryczne) oraz bezpieczeństwo przeciwpożarowe i ochrona środowiska. Powiązanie zagadnień z procesami zarządzania ryzykiem.
3-4 Dokumenty i procedury w organizacji: Cele, strategia, polityka organizacji; Cele, strategia, polityka w zakresie bezpieczeństwa organizacji; Cele, strategia, polityka w zakresie bezpieczeństwa systemów informacyjnych w organizacji; System Zarządzania Bezpieczeństwem Informacji; Wytyczne zabezpieczeń dla systemów informatycznych. Procedury instrukcje stanowiskowe. Zagadnienia prawne: Monitoring, monitoring wizyjny a ochrona prywatności i danych osobowych.
5-6 Wzorce organizacyjne oparte na najlepszych praktykach sfery biznesowej umożliwiające sformułowanie metody skutecznego i efektywnego zarządzania bezpieczeństwem.
7-8. Zapobieganie i zabezpieczenia – typologia nowoczesnej ochrony. Integracja systemów zabezpieczeń, ochrony fizycznej, systemy kontroli dostępu, nowoczesne/inteligentne systemy zapewniające komfort bezpieczeństwa. Powiązanie zagadnień z procesami zarządzania ciągłością działania. Audyt bezpieczeństwa obszarowego.
9-10 Rozwinięcie wybranych tematów i analiza przypadków: Analiza koncepcji rozwiązań zabezpieczających przed wybranymi incydentami bezpieczeństwa. Wyjaśnienie od strony technicznej i organizacyjnej. Dyskusja.
11-12. 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 Ćwiczenia komputerowe obrazujące wybrany aspekt techniczny tematyki zajęć: Wykorzystanie gotowych narzędzi, przykładowe technologie.
15 Zaliczenie. Dyskusja.
Konsultacje merytoryczne dot. projektu:
1. 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…
2. Przekazanie kolejnych fragmentów pracy 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.
3. Prezentacja projektów – dyskusja.

**Metody oceny:**

B. Ćwiczenia:
1. Ocena formatywna: zadanie projektowe (wykonywane w zespołach), prezentacja oraz kolokwium.
2. Ocena sumatywna: ocena punktowa (max 100pkt) oraz ocena liczbowa: skala ocen (2,0; 3,0; 3,5; 4,0; 4,5; 5,0).

**Egzamin:**

nie

**Literatura:**

Obowiązkowa:
1. Wołowski F., Zawiła-Niedźwiecki J., 2012, Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, Kraków: edu-Libri
2. Praca zbiorowa, red. Szatkowski T., 2016 Bezpieczeństwo danych w sektorze publicznym, Polskie Towarzystwo Informatyczne,
3. Aktualne informacje z serwisów internetowych dot. Bezpieczeństwa systemów informatycznych. W tym organizacji typu CERT.
Uzupełniająca:
1. Normy ISO/IEC 27001:2013, System Zarządzania bezpieczeństwem informacji.
2. Raporty czołowych producentów rozwiązań w zakresie bezpieczeństwa IT.

**Witryna www przedmiotu:**

www.olaf.wz.pw.edu.pl

**Uwagi:**

Wykonywanie ćwiczeń i projektu zalecane w zespołach.

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka B2\_W07:**

Student zna i rozumie w pogłębionym stopniu miejsce bezpieczeństwa w zarządzaniu zasobowym, zna wybrane zagadnienia z zakresu zaawansowanej wiedzy w obrębie bezpieczeństwa osobowego, fizycznego, technicznego, a także bezpieczeństwa danych i informacji oraz systemów teleinformatycznych.

Weryfikacja:

Kolokwium. Projekt.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

**Charakterystyka B2\_W09:**

Student zna i rozumie i rozumie fundamentalne dylematy współczesnej cywilizacji związane z bezpieczeństwem organizacji.

Weryfikacja:

Kolokwium. Projekt. Dyskusja.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka B2\_U04:**

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

Weryfikacja:

Kolokwium. Projekt.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

**Charakterystyka B2\_U11:**

Student potrafi komunikować się z użyciem specjalistycznej terminologii.

Weryfikacja:

Kolokwium. Projekt.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka B2\_K02:**

Student jest gotów do oceny stanu wiedzy (własnej i zespołu) oraz rozumie potrzebę uzupełniania jej w trybie ustawicznym

Weryfikacja:

Kolokwium. Projekt. Dyskusja.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

**Charakterystyka B2\_K05:**

Student jest gotów do uznawania znaczenia wiedzy z zakresu bezpieczeństwa w organizacji w rozwiązywaniu problemów poznawczych i praktycznych, z uwzględnieniem wsparcia technologicznego.

Weryfikacja:

Kolokwium. Projekt. Dyskusja.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**