**Nazwa przedmiotu:**

Cyberbezpieczeństwo

**Koordynator przedmiotu:**

mgr inż. Pięta Sylwester

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Zarządzanie Bezpieczeństwem Infrastruktury Krytycznej

**Grupa przedmiotów:**

Kierunkowe

**Kod przedmiotu:**

CyberBezp

**Semestr nominalny:**

4 / rok ak. 2022/2023

**Liczba punktów ECTS:**

1

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

1 ECTS
15h ćwiczenia + 2h konsultacje + 5h studia literaturowe + 5h przygotowanie do ćwiczeń + 3h projekt = 30h

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

0,57 ECTS:
15h ćwiczenia + 2h konsultacje = 17h

**Język prowadzenia zajęć:**

polski

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

1 ECTS
15h ćwiczenia + 2h konsultacje + 5h studia literaturowe + 5h przygotowanie do ćwiczeń + 3h projekt = 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 teleinformatycznym przedsiębiorstwa pełnym zagrożeń, nowych zjawisk i trendów w obszarze cyberbezpieczeństwa. Wskazanie metod pozyskania wiedzy i praktyki w podejściu do bezpieczeństwem systemów teleinformatycznych szczególnie w kontekście zagrożeń w komunikacji sieciowej.

**Treści kształcenia:**

B. Ćwiczenia:
1-2. Wprowadzenie do zagadnień cyberzagrożeń i cyberbezpieczeństwa. Odniesienie do bezpieczeństwa systemów teleinformatycznych (powiązanie z atrybutami bezpieczeństwa: Poufność, Integralność, Dostępność, Rozliczalność, Autentyczność, Niezaprzeczalność, Niezawodność). Otoczenie teleinformatyczne przedsiębiorstw, aktualne zjawiska i trendy w informatyce w odniesieniu do cyberbezpieczeństwa. Statystyki.
3-4. Najważniejsze aktualne trendy w dziedzinie bezpieczeństwa: cele ataków i technologie, wymagające regulacje prawne, ochrona prywatności, „rozproszenie danych”, wielkie zbiory danych, dane w „chmurze obliczeniowej, BYOD, krypowaluty, IoT, IIoT, zabezpieczenia szyte na miarę, blockchain w bezpieczeństwie, zagrożenia mobilne…
5-6 Typologia aktualnych zagrożeń. Analiza rzeczywistego incydentu w zakresie cyberbezpieczeństwa (Na podstawie informacji prasowych, opisu branżowego itp.) Wyjaśnienie od strony technicznej i organizacyjnej incydentu. Dyskusja.
7-8. Zapobieganie i zabezpieczenia – typologia nowoczesnej ochro-ny. Rozwinięcie wybranych tematów i analiza przypadków: Analiza koncepcji rozwiązań zabezpieczających przed wybranymi incydentami bezpieczeństwa. Wyjaśnienie od strony technicznej i organizacyjnej. Dyskusja.
9-10. Zagadnienia z obszaru zapewnienia bezpieczeństwa w środo-wisku automatyki przemysłowej (OT).
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 ataku/ochrony/metod kryptograficznych: Wykorzystanie gotowych narzędzi i przykładowe technologie.
15 Zaliczenie. 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. 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. ISO/IEC 27000 - przegląd i terminologia - System Zarządzania Bezpieczeństwem Informacji.
3. ISO/IEC 27001 – wymagania związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.
4. ISO/IEC 27002 – wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.
5. ISO/IEC 27003 – porady i wskazówki dotyczące implementacji Systemu Zarządzania Bezpieczeństwem Informacji
6. 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, technicz-nego, 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:**