**Nazwa przedmiotu:**

Cyberbezpieczeństwo

**Koordynator przedmiotu:**

mgr inż. Pięta Sylwester

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Inżynieria Zarządzania

**Grupa przedmiotów:**

Specjalność: Bezpieczeństwo i zarządzanie ciągłością działania

**Kod przedmiotu:**

-

**Semestr nominalny:**

3 / rok ak. 2019/2020

**Liczba punktów ECTS:**

2

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

2 ECTS:
15h wykład + 15h ćwiczenia + 5h konsultacje + 10h przygotowanie do ćwiczeń + 10h przygotowanie do projektu + 5h zapoznanie się z literaturą = 60h

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

1,1 ECTS:
15h wykład + 15h ćwiczenia + 5h konsultacje = 35h

**Język prowadzenia zajęć:**

polski

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

1,5 ECTS:
15h ćwiczenia + 5h konsultacje + 10h przygotowanie do ćwiczeń + 10h przygotowanie do projektu + 5h zapoznanie się z literaturą = 45h

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

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

**Wymagania wstępne:**

Bezpieczeństwo systemów teleinformatycznych, Metody zapewniania bezpieczeństwa, Technologiczne wspieranie bezpieczeństwa

**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 wiedzy i praktyki w podejściu do bezpieczeństwem systemów teleinformatycznych.

**Treści kształcenia:**

A. Wykład:
1-2. Wprowadzenie do zagadnień cyberzagrożeń i cyberbezpieczeństwa. Odniesienie do bezpieczeństwa systemów teleinformatycznych (powiązanie z atrybutami bezpieczeństwa: Poufność, Integralność, Dostępność, Rozliczalność, Autentyczność, Niezaprzeczalność, Niezawodność). Interesujące otoczenie teleinformatyczne przedsiębiorstw, aktualne zjawiska i trendy w informatyce w odniesieniu do cyberbezpieczeństwa. Statystyki.
3-4. Najważniejsze aktualne trendy w dziedzinie bezpieczeństwa np.: AI, Ransomware – nowe cele i technologie, wymagające regulacje prawne, ataki na bezserwerowe aplikacje, ochrona prywatności, wielkie zbiory danych, ataki na krypowaluty, zakłócenia w internecie rzeczy, zabezpieczenia szyte na miarę, blockchain w bezpieczeństwie, bezpieczeństwo chmury, zapobieganie zamiast wykrywania, 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).
5-6. Rozproszenie danych. Dane w „chmurze obliczeniowej. Dane na urządzeniach mobilnych. Dane na urządzaniach prywatnych-BYOD. Pamięci przenośne.
7-8. Uwarunkowania prawne, (w tym RODO). Wpływ zmian prawnych na zarządzanie bezpieczeństwem.
9-10. Typologia aktualnych zagrożeń. Malware, 0-day exploits, 0-day malware. Zagrożenia - zmiana kierunku zainteresowania grup hackerskich/ przestępczych: Wyłudzenia - CryptoLocker (ransomware); APT nowej generacji, Haktywizm, aparat administracyjny państwa, finansowane przez państwa szpiegostwo przemysłowe, obiekty przemysłowe „w ogniu ataków”. Zapobieganie i zabezpieczenia – typologia nowoczesnej ochrony.
13-14. Zagadnienia z obszaru zapewnienia bezpieczeństwa w środowisku automatyki przemysłowej (OT).
15. Zaliczenie
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 w zakresie cyberbezpieczeństwa. (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. Aktualne informacje z serwisów internetowych dot. Bezpieczeństwa systemów informatycznych. W tym organizacji typu CERT.
Uzupełniająca:
1. Raporty czołowych producentów rozwiązań w zakresie bezpieczeństwa IT.

**Witryna www przedmiotu:**

www.olaf.wz.pw.edu.pl

**Uwagi:**

-

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt I2\_W04:**

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

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt I2\_W07:**

absolwent zna i rozumie główne trendy rozwojowe w zakresie nauk o zarządzaniu

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Efekt I2\_U06:**

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

Weryfikacja:

Kolokwium, Ocena projektu grupowego

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt I2\_U17:**

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

Weryfikacja:

Kolokwium, Ocena projektu grupowego

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt I2\_K01:**

absolwent jest gotów do krytycznej oceny odbieranych treści

Weryfikacja:

Kolokwium, Ocena projektu grupowego.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt I2\_K02:**

absolwent jest gotów do 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:**