**Nazwa przedmiotu:**

Bezpieczeństwo danych, informacji i systemów teleinformatycznych

**Koordynator przedmiotu:**

mgr inż. Krzysztof Bartczak

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Zarządzanie Bezpieczeństwem Infrastruktury Krytycznej

**Grupa przedmiotów:**

Kierunkowe

**Kod przedmiotu:**

-

**Semestr nominalny:**

2 / rok ak. 2022/2023

**Liczba punktów ECTS:**

2

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

2 ECTS
10h wykład + 10h ćwiczenia + 15h praca indywidualna + 10h zapoznanie się z literaturą, przygotowanie się do zajęć +5h konsultacje = 50h

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

1 ECTS
10h wykład + 10h ćwiczenia +5h konsultacje = 25h

**Język prowadzenia zajęć:**

polski

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

1,6 ECTS
10h ćwiczenia + 15h praca indywidualna + 10h zapoznanie się z literaturą, przygotowanie się do zajęć +5h konsultacje = 40h

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

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

**Wymagania wstępne:**

-

**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:**

Celem przedmiotu jest zapoznanie studentów z problematyką bezpieczeństwo danych, informacji i systemów teleinformatycznych oraz zaznajomienie z zagrożeniami w kontekście poufności, integralności i dostępności informacji.

**Treści kształcenia:**

A. Wykład:
1. Regulamin przedmiotu oraz zasady jego zaliczenia. Założenia, definicje i klasyfikacja aspektów bezpieczeństwa danych i informacji. Definicja systemów krytycznych i niezawodności.
2. Atrybuty ochrony informacji. Tajność, integralność, dostępność, rozliczalność, autentyczność, niezaprzeczalność, niezawodność. Znaczenie podpisu elektronicznego oraz szyfrowania danych dla ochrony informacji.
3. Znaczenie bezpieczeństwa fizycznego i technicznego. Techniczne środki zapewnienia bezpieczeństwa fizycznego. Przykłady praktycznych rozwiązań.
4. Charakterystyka systemu teleinformatycznego. Zagrożenia i ochrona danych w sieciach teleinformatycznych. Poziomy komputerowego bezpieczeństwa systemów operacyjnych. Zasady projektowania zabezpieczeń. Ataki na system teleinformatyczny.
5. Przeciwdziałanie zagrożeniom dla bezpieczeństwa informacji. Metody ochrony danych i informacji w systemach teleinformatycznych. Bezpieczeństwo i zasady tworzenia kopii zapasowych.
6. Infrastruktura wysokiej dostępności. Klastry, wirtualizacja. Kwestie bezpieczeństwa danych i informacji.
7. Zagadnienie cyberbezpieczeństwa w świetle bezpieczeństwa teleinformatycznego. Typologia aktualnych zagrożeń. Zapobieganie i zabezpieczenia. Przykłady ataków cybernetycznych.
8. Podsumowanie. Egzamin ustny – termin „0”.
B. Ćwiczenia:
1. Organizacja i regulamin ćwiczeń. Podanie zasad zaliczenia.
2. Aspekty prawne, techniczne i fizyczne bezpieczeństwa danych i informacji. Prezentacje i dyskusja.
3. Charakterystyka i znaczenie podpisu elektronicznego oraz szyfrowania danych. Prezentacje i dyskusja.
4. Istota bezpieczeństwa teleinformatycznego. Przeciwdziałanie zagrożeniom dla bezpieczeństwa danych i informacji. Przegląd metod ochrony. Prezentacje i dyskusja.
5. Projekt i analiza bezpieczeństwa i niezawodności systemu teleinformatycznego. Prezentacje i dyskusja.
6. Projekt infrastruktury wysokiej dostępności. Określanie dostępności i procedury obsługi systemów. Prezentacje i dyskusja.
7. Przegląd aktualnych zagrożeń w zakresie cyberbezpieczeństwa. Atak cybernetyczny, a kwestie bezpieczeństwa danych i informacji. Prezentacje i dyskusja.
8. Podsumowanie i konsultacje. Rozliczenie ćwiczeń.

**Metody oceny:**

A. Wykład:
1. Ocena formatywna: aktywny udział w debacie na zajęciach
2. Ocena sumatywna : egzamin ustny, ocena w zakresie 2 – 5; zaliczenie: uzyskanie oceny ≥3
B. Ćwiczenia:
1. Ocena formatywna: ocena udziału w pracy zbiorowej, jednostkowej i grupowej.
2. Ocena sumatywna: terminowość wykonania projektów, zaliczenie wszystkich projektów oraz wynik rozmowy zaliczeniowej z prowadzącym.
E. Końcowa ocena z przedmiotu: od 2 do 5; do zaliczenia przedmiotu wymagane jest uzyskanie co najmniej oceny 3 zarówno z ćwiczeń, jak i z wykładu; waga: wykład: 0,5, ćwiczenia: 0,5.

**Egzamin:**

tak

**Literatura:**

Obowiązkowa:
1. Białas A., 2019, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Warszawa: WNT
2. Kowalewski J., Kowalewski M., 2017, Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni, Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej
Uzupełniająca:
1. Radziejewski R., 2019, Ochrona infrastruktury krytycznej. Teoria i praktyka, Warszawa: PWN

**Witryna www przedmiotu:**

www.olaf.wz.pw.edu.pl

**Uwagi:**

-

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka B2\_W05:**

Student zna i rozumie w pogłębionym stopniu wymagania prawne i regulacyjne w zakresie bezpieczeństwa funkcjonowania infrastruktury krytycznej.

Weryfikacja:

Egzamin ustny, Ocena projektów i prezentacji.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

**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:

Egzamin ustny, Ocena projektów i prezentacji.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

**Charakterystyka B2\_W09:**

Student zna i rozumie fundamentalne dylematy współ-czesnej cywilizacji związane z bezpieczeństwem organizacji.

Weryfikacja:

Egzamin ustny, Ocena projektów i prezentacji.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka B2\_U07:**

Student potrafi interpretować wymagania prawne i regulacyjne z zakresu bezpieczeństwa funkcjonowania organizacji i bezpieczeństwa infrastruktury krytycznej oraz przekładać je na procedury i wymagania wewnętrzne w zakresie działalności organizacji.

Weryfikacja:

Egzamin ustny, Ocena projektów i prezentacji.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

**Charakterystyka B2\_U08:**

Student potrafi prawidłowo posługiwać się normami prawnymi przy rozwiązywaniu wybranych problemów zapewniania bezpieczeństwa organizacji (w tym organizacji sektora publicznego).

Weryfikacja:

Egzamin ustny, Ocena projektów i prezentacji.

**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:

Egzamin ustny, Ocena projektów i prezentacji, aktywność podczas zajęć, praca w grupach, analiza zespołowa poszczególnych projektów.

**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 uwzględ-nieniem wsparcia technologicznego.

Weryfikacja:

Egzamin ustny, Ocena projektów i prezentacji, aktywność podczas zajęć, praca w grupach, analiza zespołowa poszczególnych projektów.

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**