**Nazwa przedmiotu:**

Bezpieczeństwo informacji i systemów teleinformatycznych organizacji

**Koordynator przedmiotu:**

dr hab. Marian Kowalewski - prof. uczelni

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Administracja

**Grupa przedmiotów:**

Obowiązkowe

**Kod przedmiotu:**

A22\_BISTO

**Semestr nominalny:**

3 / rok ak. 2021/2022

**Liczba punktów ECTS:**

2

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

Student uczestniczy w wykładach oraz ćwiczeniach objętych programem przedmiotu (20h). Ponadto na potrzeby pozyskania i ugruntowania wymaganej wiedzy, studiowania wskazanej literatury, przygotowania się do ćwiczeń i ich realizacji przeznacza 30h. Sumaryczne obciążenie pracą studenta kształtuje się na poziomie 50h. Ilość punktów ECTS za przedmiot - 2.

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

0,6 p ECTS

**Język prowadzenia zajęć:**

polski

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

0,5 p. ECTS

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

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

**Wymagania wstępne:**

Brak

**Limit liczby studentów:**

cały rok

**Cel przedmiotu:**

Celem przedmiotu jest nauczenie studentów stosowania zasad zapewnienia bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Ponadto, zapoznanie z: podstawami prawnymi bezpieczeństwa informacji; zagrożeniami i metodami zapewnienia bezpieczeństwa informacji, modelami i strategiami w zakresie bezpieczeństwa informacji; problemami zarządzania bezpieczeństwem informacji i systemów teleinformatycznych organizacji oraz modelowania - budowania na ich potrzeby modelu polityk bezpieczeństwa informacji.

**Treści kształcenia:**

1. Pojęcie bezpieczeństwa informacji i systemów teleinformatycznych organizacji, charakterystyka zagrożeń informacji i systemów teleinformatycznych organizacji.
2. Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa informacji i systemów teleinformatycznych organizacji.
3. Metody fizyczne przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych organizacji.
4. Metody techniczne przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych organizacji.
5. Metody organizacyjno-administracyjne przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych organizacji.
6. Analiza ryzyka bezpieczeństwa informacji organizacji.
7. Audyt bezpieczeństwa informacji organizacji.
8. Zarządzanie bezpieczeństwem informacji i sieci teleinformatycznych organizacji.
9. Metodyka opracowania modelu - polityki bezpieczeństwa informacji organizacji.
10. Opracowanie modelu - polityki bezpieczeństwa informacji organizacji.

**Metody oceny:**

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (ocena uprzednio przygotowanych i wygłoszonych prezentacji wykładanych zagadnień zlecanych przez prowadzącego) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Egzamin:**

nie

**Literatura:**

1. Kowalewski J., Kowalewski M., Polityka bezpieczeństwa informacji w praktyce, Presccom, Wrocław 2014
2. Kowalewski J., Kowalewski M., Zagrożenia informacji w cyberprzestrzeni. Cyberterroryzm, Oficyna Wydawnicza PW, Warszawa 2017
3. Kowalewski J., Kowalewski M., Ochrona informacji w cyberprzestrzeni, Oficyna Wydawnicza PW, Warszawa 2017
4. Kowalewski M., Usługi teleinformatyczne administracji publicznej, Oficyna Wydawnicza PW, Warszawa 2019
5. Kowalewski M., Uwarunkowania prawne organizacji bezpieczeństwa informacji Rzeczypospolitej Polskiej, Oficyna Wydawnicza PW, Warszawa 2020
6. Kowalewski Jakub, Kowalewski Marian, Zarządzanie ryzykiem w bezpieczeństwie informacji organizacji, Oficyna Wydawnicza PW, Warszawa 2021
7. Kowalewski J., Kowalewski M,. Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa informacji, Telekomunikacja i Techniki Informacyjne nr 1-2/2014, Warszawa
8. Kowalewski M. i inni, Praca zbiorowa, Modele zagrożeń aglomeracji miejskiej wraz z systemem zarządzania kryzysowego na przykładzie m. st. Warszawy, rozdziały dotyczące zagrożeń i architektury systemu łączności, WAT, Warszawa, 2009
9. Liderman K.: Analiza ryzyka informacji w systemach komputerowych, PWN, Warszawa, 2008
10. Molski M., Łacheta M.: Przewodnik audytora systemów informatycznych, Helion, Gliwice, 2006
11. Programy, dyrektywy, ustawy, rozporządzenia i normy wskazane w toku wykładu

**Witryna www przedmiotu:**

-

**Uwagi:**

W ramach przedmiotu 50% czasu przeznaczona jest na wykłady związane z bezpieczeństwem informacji i systemów teleinformatycznych organizacji oraz 50% czasu na ćwiczenia, w wyniku których powstaje model polityki bezpieczeństwa informacji organizacji dotyczących ochrony danych osobowych.

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka W\_01:**

Zna i rozumie podstawowe uwarunkowania prawne oraz pojęcia, terminologię stosowaną w obszarze bezpieczeństwa informacji i systemów teleinformatycznych organizacji (P).

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_W03, K\_W04

**Powiązane charakterystyki obszarowe:** II.S.P7S\_WG.2, II.H.P7S\_WG.1.o, II.H.P7S\_WG.2, I.P7S\_WG, II.X.P7S\_WG.1.o, II.S.P7S\_WG.1, I.P7S\_WK

**Charakterystyka W\_02:**

Zna podstawy prawne bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Zna metody przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych organizacji.

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_W03, K\_W04

**Powiązane charakterystyki obszarowe:** I.P7S\_WK, II.X.P7S\_WG.1.o, II.S.P7S\_WG.1, II.S.P7S\_WG.2, II.H.P7S\_WG.1.o, II.H.P7S\_WG.2, I.P7S\_WG

**Charakterystyka W\_03:**

Zna modele, strategie, polityki bezpieczeństwa oraz zasady zarządzania bezpieczeństwem informacji organizacji

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_W04, K\_W03

**Powiązane charakterystyki obszarowe:** II.H.P7S\_WG.2, I.P7S\_WK, II.X.P7S\_WG.1.o, II.S.P7S\_WG.1, II.S.P7S\_WG.2, II.H.P7S\_WG.1.o, I.P7S\_WG

**Charakterystyka W\_04:**

Zna źródła i zagrożenia informacji oraz systemów teleinformatycznych organizacji

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_W01, K\_W03, K\_W06, K\_W09, K\_W10

**Powiązane charakterystyki obszarowe:** I.P7S\_WG, II.S.P7S\_WG.1, II.S.P7S\_WG.2, II.H.P7S\_WG.1.o, I.P7S\_WK, II.X.P7S\_WG.1.o, II.H.P7S\_WG.2, II.T.P7S\_WG

**Charakterystyka W\_05:**

Ma podstawową wiedzę dotyczącą zasad bezpiecznego wykorzystywania usług teleinformatycznych w codziennej działalności organizacji oraz sytuacjach kryzysowych

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_W06, K\_W09, K\_W10, K\_W01, K\_W03

**Powiązane charakterystyki obszarowe:** I.P7S\_WG, II.S.P7S\_WG.1, I.P7S\_WK, II.T.P7S\_WG, II.S.P7S\_WG.2, II.H.P7S\_WG.1.o, II.X.P7S\_WG.1.o, II.H.P7S\_WG.2

### Profil ogólnoakademicki - umiejętności

**Charakterystyka U\_01:**

Potrafi prowadzić analizy zagrożeń informacji i systemów teleinformatycznych organizacji w oparciu o wiedze i podstawy prano-normalizacyjne

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_U06, K\_U08, K\_U09, K\_U10, K\_U12

**Powiązane charakterystyki obszarowe:** I.P7S\_UW, I.P7S\_UK, II.X.P7S\_UW.3.o, II.S.P7S\_UW.1, II.S.P7S\_UW.2.o, II.S.P7S\_UW.3.o, II.H.P7S\_UW.1, I.P7S\_UU, I.P7S\_UO, II.T.P7S\_UW.2, II.X.P7S\_UW.2

**Charakterystyka U\_02:**

Potrafi stosować metody przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych organizacji

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji)

**Powiązane charakterystyki kierunkowe:** K\_U04, K\_U06, K\_U09, K\_U10, K\_U12

**Powiązane charakterystyki obszarowe:** II.S.P7S\_UW.2.o, II.S.P7S\_UW.3.o, II.H.P7S\_UW.1, II.H.P7S\_UW.2.o, I.P7S\_UW, I.P7S\_UK, II.X.P7S\_UW.3.o, II.S.P7S\_UW.1, I.P7S\_UO, II.T.P7S\_UW.2, II.X.P7S\_UW.2

**Charakterystyka U\_03:**

Potrafi bezpiecznie stosować usługi teleinformatyczne w codziennej działalności organizacji oraz w sytuacjach kryzysowych

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_U08, K\_U09, K\_U10, K\_U12, K\_U06

**Powiązane charakterystyki obszarowe:** II.S.P7S\_UW.3.o, I.P7S\_UK, I.P7S\_UO, I.P7S\_UW, II.T.P7S\_UW.2, II.X.P7S\_UW.2, II.S.P7S\_UW.2.o, II.X.P7S\_UW.3.o, II.S.P7S\_UW.1, II.H.P7S\_UW.1, I.P7S\_UU

**Charakterystyka U\_04:**

Potrafi opracować politykę bezpieczeństwa informacji lub systemu teleinformatycznego organizacji

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_U05, K\_U08, K\_U09, K\_U10, K\_U12

**Powiązane charakterystyki obszarowe:** I.P7S\_UW, II.X.P7S\_UW.2, II.S.P7S\_UW.1, II.S.P7S\_UW.2.o, II.S.P7S\_UW.3.o, II.H.P7S\_UW.1, II.H.P7S\_UW.2.o, I.P7S\_UK, I.P7S\_UU, I.P7S\_UO, II.T.P7S\_UW.2

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka K\_01:**

Rozumie potrzebę uczenia się ustawicznego w swoim życiu i inspirowania tej potrzeby w swoim środowisku

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_K04, K\_K07, K\_K01, K\_K02, K\_K03

**Powiązane charakterystyki obszarowe:** I.P7S\_KK, I.P7S\_KR, I.P7S\_KO

**Charakterystyka K\_02:**

Ma świadomość dynamicznego rozwoju systemów informatycznych i informatycznych i rosnącego zagrożenia bezpieczeństwa przesyłanej, przetwarzanej i przechowywanej w nich organizacji

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02, K\_K03, K\_K04, K\_K07

**Powiązane charakterystyki obszarowe:** I.P7S\_KK, I.P7S\_KR, I.P7S\_KO

**Charakterystyka K\_03:**

Potrafi współpracować w grupie i współdziałać z różnymi podmiotami w zakresie zapewnienia bezpieczeństwa informacji organizacji

Weryfikacja:

Przedmiot zaliczany na ocenę. Ocenę przedmiotu stanowi średnia z sumy ocen z części teoretycznej (test z wykładów) oraz części praktycznej - ćwiczeniowej (ocena opracowanego modelu - polityki bezpieczeństwa informacji organizacji).

**Powiązane charakterystyki kierunkowe:** K\_K01, K\_K02, K\_K03, K\_K04, K\_K07

**Powiązane charakterystyki obszarowe:** I.P7S\_KK, I.P7S\_KR, I.P7S\_KO