**Nazwa przedmiotu:**

Podstawy bezpieczeństwa informacji i systemów teleinformatycznych

**Koordynator przedmiotu:**

dr hab. inż. Marian Kowalewski, prof PW

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Administracja

**Grupa przedmiotów:**

Obowiązkowe

**Kod przedmiotu:**

A13\_PBIST

**Semestr nominalny:**

5 / rok ak. 2016/2017

**Liczba punktów ECTS:**

1

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

Student uczestniczy w wykładach objętych programem przedmiotu (30h). Na potrzeby ugruntowania wymaganej wiedzy, studiowania wskazanej literatury przedmiotu, przygotowania się do egzaminu przeznacza 30h. Sumaryczne obciążenie pracą studenta kształtuje się na poziomie 30h. Ilość punktów ECTS - 1.

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

1 ECTS

**Język prowadzenia zajęć:**

polski

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

0

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

|  |  |
| --- | --- |
| Wykład: | 30h |
| Ćwiczenia: | 0h |
| Laboratorium: | 0h |
| Projekt: | 0h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Związki korelacyjne: przedmiot bazuje na zrealizowanych uprzednio przedmiotach informatycznych; pogłębia wiedzę w zakresie zagrożeń informacji i systemów teleinformatycznych oraz umiejętności stosowania metod organizacyjno – prawnych i programowo – technicznych przeciwdziałania tym zagrożeniom.

**Limit liczby studentów:**

wszyscy

**Cel przedmiotu:**

Celem przedmiotu jest nauczenie studentów stosowania zasad zapewnienia bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Ponadto, zapoznanie studentów z: podstawami prawnymi bezpieczeństwa informacji, zagrożeniami i metodami zapewnienia bezpieczeństwa informacji, modelami i strategiami oraz problemami zarządzania bezpieczeństwem informacji i systemów teleinformatycznych w instytucjach (organizacjach).

**Treści kształcenia:**

1. POJECIE BEZPIECZEŃSTWA INFORMACJI, PODSTAWOWE OKREŚLENIA. PRAWNO – ORGANIZACYJNE ASPEKTY BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Bezpieczeństwo informacji i systemów teleinformatycznych organizacji, podstawowe określenia. Podstawy prawno – organizacyjne bezpieczeństwa informacji i systemów teleinformatycznych w organizacji.
2. SYSTEMATYKA I CHARAKTERYSTYKA ZAGROŻEŃ INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Zagrożenia informacji i systemów teleinformatycznych – podstawowe określenia. Systematyka zagrożeń informacji oraz systemów teleinformatycznych organizacji. Charakterystyka i skutki zagrożeń informacji oraz systemów teleinformatycznych organizacji.
3. CYBERTERRORYZM SZCZEGÓLNYM ZAGROŻENIEM BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Pojecie cyberprzestrzeni i cyberterroryzmu . Formy i metody ataków w cyberprzestrzeni. Podstawy prawne ochrony cyberprzestrzeni. Metody przeciwdziałania zagrożeniom cyberprzestrzeni i cyberterroryzmu.
4. ZAGROŻENIA KRYTYCZNEJ INFRASTRUKTURY TELEINFORMATYCZNEJ - Infrastruktura krytyczna – podstawowe określenia i definicje. Zagrożenia krytycznej infrastruktury teleinformatycznej. Ochrona krytycznej infrastruktury teleinformatycznej. Podstawy prawne ochrony krytycznej infrastruktury teleinformatycznej w kraju.
5. BEZPIECZEŃSTWO INFORMACJI NIEJAWNYCH I DANYCH WRAŻLIWYCH - Informacja niejawna i dane wrażliwe – podstawowe określenia. Uwarunkowania organizacyjne oraz podstawy prawne bezpieczeństwa informacji niejawnej. Ochrona danych wrażliwych i osobowych.
6. METODY FIZYCZNE PRZECIWDZIAŁANIA ZAGROŻENIOM INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Klasyfikacja metod przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych. Fizyczne metody przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych. Techniczne środki przeciwdziałania zagrożeniom – aplikacje metod fizycznych.
7. METODY TECHNICZNE PRZECIWDZIAŁANIA ZAGROŻENIOM INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Metody kryptograficzne ochrony informacji i danych. Metody programowo – sprzętowe zapewnienia bezpieczeństwa informacji i systemów teleinformatycznych . Metody ochrony elektromagnetycznej. Elektroniczne systemy ochrony obiektów i zasobów systemów teleinformatycznych.
8. MODELE I STRATEGIE BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Modele i strategie bezpieczeństwa informacji – identyfikacja i charakterystyka. Aplikacje modeli polityk bezpieczeństwa informacji. Modele bezpieczeństwa systemu teleinformatycznego w rozwiązaniach praktycznych i dokumentach ETSI.
9. METODY ADMINISTRACYJNO – ORGANIZACYJNE PRZECIWDZIAŁANIA ZAGROŻENIOM INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Analiza systemowa w procesie organizacji bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Podstawy prawne bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Polityka bezpieczeństwa informacji i systemów teleinformatycznych organizacji – aplikacje.
10. METODYKI OPRACOWANIA POLITYK BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Charakterystyka metodyk opracowania polityk bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Metodyka TISM. Kryteria wyboru i wybór metodyki opracowania polityki bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Opracowanie polityki bezpieczeństwa informacji/systemu teleinformatycznego organizacji w układzie minimalnym.
11. RYZYKO, ANALIZA RYZYKA BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Istota analizy ryzyka bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Metody szacowania i oceny ryzyka bezpieczeństwa informacji i systemów teleinformatycznych organizacji.
12. ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Zarządzanie ryzykiem wg ISO/IEC. Analiza aplikacji zarządzania ryzykiem bezpieczeństwa informacji i systemów teleinformatycznych organizacji.
13. AUDYT BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI - Audyt bezpieczeństwa informacji i systemów teleinformatycznych organizacji – podstawowe określenia. Proces audytu bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Metodyki prowadzenia audytu. Standardy, wytyczne i procedury audytowania systemów teleinformatycznych organizacji.
14. ZARZĄDZENIE BEZPIECZEŃSTWEM INFORMACJI I SIECI TELEINFORMATYCZNYCH ORGANIZACJI - Podstawowe uwarunkowania zarządzania bezpieczeństwem informacji i systemów teleinformatycznych organizacji. Proces zarządzania bezpieczeństwem informacji. Podstawy prawne i normalizacyjne oraz praktyka w zarządzaniu bezpieczeństwem informacji. Zarządzanie sieciami teleinformatycznymi organizacji.

**Metody oceny:**

Ocena z egzaminu. Forma egzaminu - test z wykładanej tematyki przedmiotu.

**Egzamin:**

tak

**Literatura:**

1. Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa, 2008
2. Cole E., Krutz R. L., Conley J.: Bezpieczeństwo sieci. Biblia. Helion, Warszawa 2005
3. Dudek A. Nie tylko wirusy. Wydawnictwo Helion, Warszawa 2005
4. Kowalewski J., Kowalewski M., Zagrożenia informacji w cyberprzestrzeni. Cyberterroryzm. Oficyna Wydawnicza PW, Warszawa 2017
5. Kowalewski J., Kowalewski M., Ochrona informacji w cyberprzestrzeni, Oficyna Wydawnicza PW, Warszawa 2017
6. Kowalewski J., Kowalewski M., Polityka bezpieczeństwa informacji w praktyce, Presscom sp. z o.o., Wrocław 2014
7. Kowalewski M., Ołtarzewska A., Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności, Telekomunikacja i Techniki Informacyjne nr 3-4, IŁ-PIB, Warszawa 2007
8. Liderman K.: Analiza ryzyka informacji w systemach komputerowych, PWN, Warszawa 2008
9. Strebe M: Podstawy bezpieczeństwa sieci. Mikom, Warszawa 2005

**Witryna www przedmiotu:**

**Uwagi:**

Brak

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt W\_01:**

Zna i rozumie podstawowe pojęcia, terminologię stosowaną w obszarze bezpieczeństwa informacji i systemów teleinformatycznych organizacji

Weryfikacja:

Test egzaminacyjny z bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_W10, K\_W12

**Powiązane efekty obszarowe:** S1A\_W05, S1A\_W06, S1A\_W01, S1A\_W02, S1A\_W04, S1A\_W07

**Efekt W\_02:**

Zna źródła i zagrożenia informacji oraz systemów teleinformatycznych organizacji

Weryfikacja:

Test egzaminacyjny z bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Wystąpienia w toku wykładów

**Powiązane efekty kierunkowe:** K\_W10, K\_W12

**Powiązane efekty obszarowe:** S1A\_W05, S1A\_W06, S1A\_W01, S1A\_W02, S1A\_W04, S1A\_W07

**Efekt W\_03:**

Zna metody przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych organizacji

Weryfikacja:

Test egzaminacyjny z bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_W10, K\_W12

**Powiązane efekty obszarowe:** S1A\_W05, S1A\_W06, S1A\_W01, S1A\_W02, S1A\_W04, S1A\_W07

**Efekt W\_04:**

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

Weryfikacja:

Test egzaminacyjny z bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_W10, K\_W12

**Powiązane efekty obszarowe:** S1A\_W05, S1A\_W06, S1A\_W01, S1A\_W02, S1A\_W04, S1A\_W07

**Efekt W\_05:**

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

Weryfikacja:

Test egzaminacyjny z bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_W10, K\_W12

**Powiązane efekty obszarowe:** S1A\_W05, S1A\_W06, S1A\_W01, S1A\_W02, S1A\_W04, S1A\_W07

### Profil ogólnoakademicki - umiejętności

**Efekt U\_01:**

Potrafi prowadzić analizy zagrożeń informacji i systemów teleinformatycznych organizacji

Weryfikacja:

Test egzaminacyjny z bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_U01, K\_U10

**Powiązane efekty obszarowe:** P1A\_U01, P1A\_U02, P1A\_U03, P1A\_U05, P1A\_U06, P1A\_U07, P1A\_U08, P1A\_U09, P1A\_U10, S1A\_U01, S1A\_U02, S1A\_U03, S1A\_U04, S1A\_U05, S1A\_U06, S1A\_U07, S1A\_U08

**Efekt U\_02:**

Potrafi stosować metody przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych organizacji

Weryfikacja:

Test egzaminacyjny z bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_U10

**Powiązane efekty obszarowe:** S1A\_U01, S1A\_U02, S1A\_U03, S1A\_U04, S1A\_U05, S1A\_U06, S1A\_U07, S1A\_U08

**Efekt U\_03:**

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

Weryfikacja:

Test egzaminacyjny z bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_U10

**Powiązane efekty obszarowe:** S1A\_U01, S1A\_U02, S1A\_U03, S1A\_U04, S1A\_U05, S1A\_U06, S1A\_U07, S1A\_U08

**Efekt U\_04:**

Potrafi opracować politykę bezpieczeństwa informacji lub systemu teleinformatycznego organizacji w układzie minimalnym

Weryfikacja:

Test egzaminacyjny z bezpieczeństwa informacji i systemów teleinformatycznych organizacji. Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_U10

**Powiązane efekty obszarowe:** S1A\_U01, S1A\_U02, S1A\_U03, S1A\_U04, S1A\_U05, S1A\_U06, S1A\_U07, S1A\_U08

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt K\_01:**

Jest świadomy odpowiedzialności w zakresie bezpieczeństwa informacji i systemów teleinformatycznych w środowisku funkcjonowania zawodowego

Weryfikacja:

Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_K02

**Powiązane efekty obszarowe:** S1A\_K01, S1A\_K02, S1A\_K04, S1A\_K06

**Efekt K\_02:**

Ma świadomość dynamicznego rozwoju systemów teleinformatycznych i ich rosnącego zagrożenia oraz stosowania metod ochrony i zasad bezpiecznego przetwarzania informacji zwłaszcza w obszarze funkcjonowania administracji publicznej

Weryfikacja:

Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_K06, K\_K09

**Powiązane efekty obszarowe:** S1A\_K02, S1A\_K03, S1A\_K04, S1A\_K03, S1A\_K04, S1A\_K06

**Efekt K\_03:**

Potrafi współdziałać z różnymi podmiotami, wykorzystywać nabytą wiedzę techniczną w zakresie zapewnienia bezpieczeństwa informacji i systemów teleinformatycznych organizacji

Weryfikacja:

Wystąpienia w toku wykładów.

**Powiązane efekty kierunkowe:** K\_K06, K\_K08, K\_K09

**Powiązane efekty obszarowe:** S1A\_K02, S1A\_K03, S1A\_K04, S1A\_K02, S1A\_K03, S1A\_K04, S1A\_K03, S1A\_K04, S1A\_K06