**Nazwa przedmiotu:**

Bezpieczeństwo informacji i systemów teleinformatycznych organizacji

**Koordynator przedmiotu:**

wykład: Prof. nzw. dr hab. inż. Marian Kowalewski, ćwiczenia: mgr inż. Jakub Kowalewski

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Administracja

**Grupa przedmiotów:**

Obowiązkowe

**Kod przedmiotu:**

A22\_BISTO

**Semestr nominalny:**

3 / rok ak. 2016/2017

**Liczba punktów ECTS:**

1

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

Nakład pracy studenta
Forma nakładu pracy studenta (udział w zajęciach, aktywność, przygotowanie sprawozdania, itp.) Obciążenie studenta [h] studia stacjonarne:
Udział w wykładach 15h
Udział w ćwiczeniach 15h
Praca własna:
Studiowanie wskazanej literatury 20h
Sumaryczne obciążenie pracą studenta 50h

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

1

**Język prowadzenia zajęć:**

polski

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

1

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

|  |  |
| --- | --- |
| Wykład: | 225h |
| Ćwiczenia: | 225h |
| Laboratorium: | 0h |
| Projekt: | 0h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Związki korelacyjne: przedmiot bazuje na zrealizowanej uprzednio, w ramach studiów I stopnia informatyce; pogłębia wiedzę w zakresie zagrożeń informacji i systemów teleinformatycznych oraz umiejętności stosowania metod organizacyjno – prawnych i programowo – technicznych przeciwdziałania tym zagrożeniom.

**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 oraz problemami zarządzania bezpieczeństwem informacji i systemów teleinformatycznych organizacji.
Wykłady dotyczą najistotniejszych problemów bezpieczeństwa informacji i systemów teleinformatycznych organizacji. W swej istocie dotyczą podstawowych pojęć związanych z bezpieczeństwem informacji, zagrożeń bezpieczeństwa informacji oraz metod przeciwdziałania tym zagrożeniom. Ponadto, organizowania procesu bezpieczeństwa informacji w organizacji i bezpiecznego wykorzystywania usług teleinformatycznych w działalności codziennej instytucji oraz w sytuacjach kryzysowych.
Ćwiczenia rozwijają umiejętności studentów w zakresie treści przedmiotu oraz opracowania modelu polityk bezpieczeństwa informacji organizacji w układzie minimalnym.

**Treści kształcenia:**

Wykłady (tematy oraz zagadnienia)
1. PPOJECIE BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI. CHARAKTERYSTYKA ZAGROŻEŃ INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI
Bezpieczeństwo informacji i systemów teleinformatycznych (ST) organizacji – podstawowe określenia. Systematyka zagrożeń informacji oraz ST organizacji. Charakterystyka i skutki zagrożeń informacji oraz systemów teleinformatycznych organizacji
2. CYBERTERRORYZM SZCZEGÓLNYM ZAGROŻENIEM BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJ
Pojecie cyberprzestrzeni i cyberterroryzmu. Oprogramowanie złośliwe. Metody i ataki blokujące systemy informacyjne. Kategorie przestępstw komputerowych. Krytyczna infrastruktura telekomunikacyjna a cyberterroryzm. Podstawy prawne ochrony cyberprzestrzeni. Metody przeciwdziałania zagrożeniom cyberprzestrzeni i cyberterroryzmu
3. METODY FIZYCZNE PRZECIWDZIAŁANIA ZAGROŻENIOM INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI
Klasyfikacja metod przeciwdziałania zagrożeniom informacji i ST. Charakterystyka metod fizycznych przeciwdziałania zagrożeniom informacji i ST, techniczne środki przeciwdziałania zagrożeniom.
Podstawy prawne bezpieczeństwa informacji i ST organizacji.
4. METODY TECHNICZNE PRZECIWDZIAŁANIA ZAGROŻENIOM INFORMACJI I I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI
Metody kryptograficzne ochrony informacji. Metody programowo-sprzętowe zapewnienia bezpieczeństwa ST. Metody ochrony elektromagnetycznej. Elektroniczne systemy ochrony obiektów i zasobów ST
5. METODY ADMINISTRACYJNO-ORGANIZACYJNE PRZECIWDZIAŁANIA ZAGROŻENIOM INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH ORGANIZACJI
Analiza funkcjonalna w procesie organizacji bezpieczeństwa informacji organizacji. Podstawy prawne i normalizacyjne bezpieczeństwa informacji organizacji
6 ANALIZA RYZYKA BEZPIECZEŃSTWA INFORMACJI ORGANIZACJI
Proces zarządzania ryzykiem bezpieczeństwa informacji organizacji. Szacowanie ryzyka bezpieczeństwa informacji organizacji. Metody, standardy analiz i zarządzania ryzykiem bezpieczeństwa informacji organizacji
7 AUDYT BEZPIECZEŃSTWA INFORMACJI ORGANIZACJI
Określenie audytu bezpieczeństwa informacji i ST organizacji. Proces audytu bezpieczeństwa informacji i ST organizacji. Metodyki prowadzenia audytu. Standardy audytowania systemów teleinformatycznych
8 ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI I SIECI TELEINFORMATYCZNYCH ORGANIZACJ
Elementy proces zarządzania bezpieczeństwem informacji organizacji. Proces zarządzania bezpieczeństwem informacji organizacji. System Zarządzania Bezpieczeństwem Informacji organizacji. Zarządzanie sieciami (zasobami) teleinformatycznymi organizacji. Praktyczne uwagi w zarządzaniu bezpieczeństwem informacji organizacji
Ćwiczenia (tematy oraz zagadnienia)
1. METODYKA OPRACOWANIA POLITYKI BEZPIECZENSTWA INFORMACJI
Charakterystyka metodyki opracowania polityki bezpieczeństwa informacji. Wytyczne do opracowania modelu polityki bezpieczeństwa informacji w układzie minimalnym.
2. OPRACOWANIE MODELU POLITYKI BEZPIECZENSTWA INFORMACJI
Opracowanie projektu modelu polityki bezpieczeństwa informacji w układzie minimalnym.

**Metody oceny:**

Podstawą zaliczenia przedmiotu jest uzyskanie pozytywnej oceny z ćwiczeń i testu zaliczeniowego.
Na ocenę końcową przedmiotu składają się: ocena średnia z ćwiczeń i testu egzaminacyjnego.
Ocena za przedmiot
Ocena Student, który zaliczył przedmiot (moduł) wie / umie / potrafi:
3.0 Interpretować uzyskaną wiedzę w zakresie podstawowym. Nie wykazuje samodzielności w realizacji zadań. Posiada wiedzę i podstawowe umiejętności z przedmiotu na poziomie dostatecznym.
3.5 Opisać i interpretować treści programowe. Nie wykazuje w pełni inicjatywy. Posiada wiedzę i umiejętności z przedmiotu na poziomie dość dobrym objętych programem kształcenia.
4.0 Wyjaśnić i rozwiązać stawiane przed nim problemy, formułuje tezy i rozwiązuje zadania. Średnio zaangażowany w proces dydaktyczny. Prezentuje właściwą postawę etyczną. Opanował wiedzę i umiejętności z przedmiotu na średnim poziomie objętych program kształcenia.
4.5 Klasyfikować, porównać i analizować omawiane problemy, zjawiska i procesy. W sposób pełny i rzeczowy uzasadnia swoje stanowisko. Aktywnie uczestniczy w procesie dydaktycznym. Prezentuje nienaganną postawę etyczną. Prezentuje wysoki poziom wiedzy i umiejętności objętych programem kształcenia.
5.0 W sposób pełny i rzeczowy wyjaśnić i ocenić określone zjawisko, oraz uzasadnić swoje stanowisko. Stosuje prawidłową i skuteczną argumentację. Z zaangażowaniem realizuje proces dydaktyczny. Jest kreatywny i potrafi podejmować decyzje. Prezentuje nienaganną postawę etyczną. Prezentuje bardzo wysoki poziom wiedzy i umiejętności objętych programem kształcenia.

**Egzamin:**

nie

**Literatura:**

Zalecana literatura i pomoce naukowe
Literatura podstawowa:
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., Polityka bezpieczeństwa informacji w praktyce, Presscom sp. z o.o., Wrocław 2014
5. Kowalewski M., Ołtarzewska A., Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności, Telekomunikacja i Techniki Informacyjne nr 3-4, IŁ-PIB, Warszawa 2007
6. Kowalewski M. i inni, Sieci i usługi w zarządzaniu kryzysowym, TiTI, Warszawa 2011
7. Kowalewski M. i inni, Perspektywiczne sieci i usługi komunikacji elektronicznej na potrzeby bezpieczeństwa i zarządzania kryzysowego, IŁ-PIB, Warszawa 2010
8. Liderman K.: Analiza ryzyka informacji w systemach komputerowych, PWN, Warszawa 2008
9. Liderman K., Bezpieczeństwo informacyjne, Wydawnictwo naukowe PWN, Warszawa 2012
10. Sosinsky B., Sieci komputerowe, Biblia, Helion, Gliwice 2011
11. Strebe M: Podstawy bezpieczeństwa sieci. Mikom, Warszawa 2005
Literatura uzupełniająca:
1. Bral W.: Obieg i ochrona dokumentów w zarządzaniu jakością, środowiskiem i bezpieczeństwem informacji, Difin, Warszawa 2008
2. Kowalewski M. i inni, Ostrzeganie i alarmowanie ludności w niebezpieczeństwie, TiTI, Warszawa 2011
3. 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
4. Molski M., Łacheta M.: Przewodnik audytora systemów informatycznych, Helion, Gliwice 2006
5. Sikorski W., ECDL Podstawy technik informatycznych i komunikacyjnych, PWN, Warszawa 2009
6. Sutton Roger J.: Bezpieczeństwo telekomunikacji, WKŁ, Warszawa 2004

**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 zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_W10

**Powiązane efekty obszarowe:** S2A\_W06, S2A\_W09

**Efekt W\_02:**

Zna źródła i zagrożenia informacji oraz systemów teleinformatycznych organizacji

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_W10

**Powiązane efekty obszarowe:** S2A\_W06, S2A\_W09

**Efekt W\_03:**

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

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_W10

**Powiązane efekty obszarowe:** S2A\_W06, S2A\_W09

**Efekt W\_04:**

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

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_W10

**Powiązane efekty obszarowe:** S2A\_W06, S2A\_W09

**Efekt W\_05:**

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

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_W10

**Powiązane efekty obszarowe:** S2A\_W06, S2A\_W09

### Profil ogólnoakademicki - umiejętności

**Efekt U\_01:**

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

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_U06, K\_U10

**Powiązane efekty obszarowe:** S2A\_U01, S2A\_U02, S2A\_U03, S2A\_U06, S2A\_U08, S2A\_U03, S2A\_U04, S2A\_U05

**Efekt U\_02:**

Potrafi stosować metody przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych organizacji

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_U06, K\_U12

**Powiązane efekty obszarowe:** S2A\_U01, S2A\_U02, S2A\_U03, S2A\_U06, S2A\_U08, S2A\_U02, S2A\_U04, S2A\_U06

**Efekt U\_03:**

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

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_U12

**Powiązane efekty obszarowe:** S2A\_U02, S2A\_U04, S2A\_U06

**Efekt U\_04:**

Potrafi opracować politykę bezpieczeństwa informacji lub systemu teleinformatycznego organizacji

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_U06, K\_U07, K\_U08, K\_U12

**Powiązane efekty obszarowe:** S2A\_U01, S2A\_U02, S2A\_U03, S2A\_U06, S2A\_U08, S2A\_U06, S2A\_U02, S2A\_U03, S2A\_U04, S2A\_U06, S2A\_U08, S2A\_U02, S2A\_U04, S2A\_U06

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt K\_01:**

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

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_K04

**Powiązane efekty obszarowe:** S2A\_K01, S2A\_K03, S2A\_K06, S2A\_K07

**Efekt K\_02:**

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

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń.

**Powiązane efekty kierunkowe:** K\_K07

**Powiązane efekty obszarowe:** S2A\_K03, S2A\_K04, S2A\_K06, S2A\_K07

**Efekt K\_03:**

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

Weryfikacja:

Test zaliczeniowy, wystąpienia w toku ćwiczeń

**Powiązane efekty kierunkowe:** K\_K03

**Powiązane efekty obszarowe:** S2A\_K02, S2A\_K03