**Nazwa przedmiotu:**

Przeciwdziałanie zagrożeniom bezpieczeństwa informacji

**Koordynator przedmiotu:**

Prof. dr hab. Józef Janczak

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Administracja

**Grupa przedmiotów:**

Obieralne

**Kod przedmiotu:**

A13\_PZBI

**Semestr nominalny:**

6 / rok ak. 2015/2016

**Liczba punktów ECTS:**

3

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

Sumaryczne obciążenie pracą studenta 75 godz.
Udział w ćwiczeniach 30
Praca własna:
przygotowanie do zajęć 20
czytanie wskazanej literatury 15
napisanie referatu / eseju 10

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

3 ECTS

**Język prowadzenia zajęć:**

polski

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

2 ECTS

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

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

**Wymagania wstępne:**

Przedmiot pogłębia wiedzę kierunkową i rozwija umiejętności systemowego postrzegania bezpieczeństwa narodowego w sferze informacyjnej. Wykorzystuje wiedzę z przedmiotu: Inżynieria systemów bezpieczeństwa, Systemy i usługi informacyjne w administracji

**Limit liczby studentów:**

grupa obieralna

**Cel przedmiotu:**

Cele:
Zapoznać studentów z podstawami teoretycznymi bezpieczeństwa informacji w organizacji.
Uświadomić studentom istotę bezpieczeństwa informacji w organizacji.
Zapoznać studentów z rodzajami, źródłami zagrożeń oraz siłami i środkami i sposobami kształtującymi bezpieczeństwo informacji w organizacji.
Przygotować studentów do interpretowania zdobytej wiedzy różnych sytuacja życia społecznego i stosowania jej w praktycznym działaniu w funkcjonowaniu organizacji.

Przedmiot jest zorganizowany w układzie problemowym.
Ćwiczenia/seminaria rozwijają i kształtują umiejętności oraz ugruntowują i pogłębiają problematykę niektórych zagadnień z wykładów oraz nauczą oceny szans i zagrożeń funkcjonowania systemu bezpieczeństwa informacji oraz jego elementów ( instytucji i podmiotów) biorących udział w realizacji zadań w tym obszarze problemowym oraz dostrzegania słabych stron istniejących rozwiązań systemu bezpieczeństwa i formułowania własnych propozycji rozwiazywania problemów. Będą także asumptem do dyskusji między studentami a nauczycielem. Wystąpienia (referaty i prezentacje) mają dowieść faktu zapoznania się z zalecaną literaturą i aktami prawnymi oraz rozwijania umiejętności.

**Treści kształcenia:**

1. Współczesne zagrożenia bezpieczeństwa informacji:
1. Rodzaje zagrożeń BI.
2. Współczesne oblicza cyberterroryzmu.
3. Metody prowadzenia ataków cyberterrorystycznych.
4. Cyberterroryzm państwowy i niepaństwowy.
5. Koncepcje walki informacyjnej.
6. Odpowiedzialność karna za przestępstwa przeciwko ochronie informacji
2. Zagrożenia bezpieczeństwa informacji w organizacji:
1. Pojęcie i podział zagrożeń ze względu na ich lokalizację:
2. Zagrożenia zewnętrzne (sabotaż, infiltracja, ataki programistyczne; cyberataki, cyberterroryzm i in.).
3. Zagrożenia wewnętrzne (czynnik ludzki - błędy i pomyłki; naruszenie praw autorskich; szpiegostwo lub kradzież danych i in.).
4. Zagrożenia fizyczne (wypadki, awarie, katastrofy, klęki żywiołowe i in).
3. Prawne aspekty bezpieczeństwa i ochrony informacji niejawnych:
1. Podstawowe pojęcia ustawowe dotyczące ochrony informacji niejawnych.
2. Klasyfikowanie informacji niejawnych.
3. Organizacja ochrony informacji niejawnych.
4. Szkolenia w zakresie ochrony informacji niejawnych.
4. Bezpieczeństwo osobowe:
1. Rodzaje postępowań sprawdzających.
2. Ankiety bezpieczeństwa osobowego.
3. Udostępnianie informacji niejawnych.
4. Postępowanie odwoławcze i skargowe.
5. Odpowiedzialność karna za przestępstwa przeciwko ochronie informacji.
5. Bezpieczeństwo teleinformatyczne w organizacji:
1. Istota bezpieczeństwa teleinformatycznego.
2. Podstawowe wymagania bezpieczeństwa teleinformatycznego wg dokumentów normatywnych.
3. Bezpieczeństwo a prawo.
4. Poziomy i metody ochrony informacji w systemach i sieciach teleinformatycznych.
6. Podstawowe wymagania w zakresie bezpieczeństwa teleinformatycznego w organizacji:
1. Istota bezpieczeństwa teleinformatycznego.
2. Ujęcia bezpieczeństwa teleinformatycznego
3. Podstawowe wymagania bezpieczeństwa teleinformatycznego.
4. Realizacja wybranych przedsięwzięć bezpieczeństwa teleinformatycznego
5. Dokumentacja bezpieczeństwa teleinformatycznego.
7. Środki bezpieczeństwa fizycznego, tajne kancelarie:
1. Środki bezpieczeństwa fizycznego.
2. Sposoby i tryb przetwarzania informacji niejawnych.
3. Zasady organizacji i wymagania wobec KT.
4. Obowiązki kierownika kancelarii tajnej.
5. Dokumentacja kancelaryjna i organizacja pracy kancelarii tajnej.
8. Ochrona fizyczna zasobów informacji w organizacji:
1. Cele i zadania ochrony fizycznej zasobów informacji w instytucji.
2. Zabezpieczenia fizyczne typu budowlanego i mechanicznego.
3. Systemy alarmowe.
4. Przechowywanie i niszczenie nośników informacji.
9. Techniczne aspekty ochrony informacji:
1. Techniczne aspekty fizycznej ochrony informacji.
2. Zabezpieczenie dostępu do informacji.
3. Ochrona elektromagnetyczna.
4. Ochrona kryptograficzna.
5. Udział pracowników w zapewnieniu bezpieczeństwa i ochrony.
10. Kontrola dostępu do zasobów informacji, sprawowanie nadzoru w zakresie bezpieczeństwa informacji:
1. Cele i zadania kontroli dostępu do zasobów informacji.
2. Mechanizmy kontroli dostępu.
3. Przydzielanie uprawnień użytkownikom.
4. Zasada wiedzy niezbędnej.
5. Rozliczalność dostępu do danych.
11. Zarządzanie bezpieczeństwem informacyjnym w organizacji:
1. System Zarządzania Bezpieczeństwem Informacji - normy.
2. Wdrożenie SZBI zgodnego z wymaganiami normy ISO/IEC 27001 w organizacji.
3. Korzyści i problemy wynikające z wdrożenia SZBI.
4. Postulaty dla wdrażających SZBI.
12. Polityka państwa w zakresie bezpieczeństwa informacyjnego w organizacji:
1. Infrastruktura informacyjna państwa obywatelskiego.
2. Istota bezpieczeństwa informacyjnego.
3. Cele polityki państwa w zakresie bezpieczeństwa informacyjnego.
4. Założenia polityki bezpieczeństwa informacyjnego w instytucji.
13. Audyt bezpieczeństwa informacji w organizacji:
1. Wymagania i podstawowe informacje dotyczące audytu.
2. Cele i zadania audytu bezpieczeństwa informacyjnego w instytucji.
3. Prowadzenie audytu BI.
4. Sposoby realizacji audytów BI.
5. Specyfika audytu certyfikującego BI.
14. Zarządzanie ryzykiem w bezpieczeństwie informacji:
1. Proces zarządzania ryzykiem w bezpieczeństwie informacji.
2. Postępowanie z ryzykiem.
3. Informowanie o ryzyku.
4. Monitorowanie i przegląd ryzyka.
15. Kolokwium:
Test wielokrotnej odpowiedzi składający się z 20 pytań z podpowiedziami.

**Metody oceny:**

Podstawą zaliczenia przedmiotu jest aktywność na ćwiczeniach, uzyskanie pozytywnych ocen z testu i ćwiczeń. Ćwiczenia kończą się testem podsumowującym, który obejmuje wiedzę z zalecanej literatury. Ocena końcowa z ćwiczeń przedmiotowych będzie określona na podstawie efektów aktywności studenta w dyskusjach i efektów rozwiązania problemów oraz wykonanej pracy zaliczeniowej.
Warunki: aktywne uczestnictwo studenta we wszystkich zajęciach. Przygotowywanie się do zajęć na podstawie podanej literatury i materiałów źródłowych. W przypadku nieobecności, studiujący zobowiązani są do rozliczenia się z treściami merytorycznymi w godzinach konsultacji.
Na ocenę końcową z przedmiotu składają się: test (40%); wystąpienia (30%); pisemna praca zaliczeniowa (30%).

Student, który zaliczył przedmiot (moduł) wie / umie / potrafi:
Poprawnie umie zdefiniować podstawowe pojęcia z zakresu systemów bezpieczeństwa państwa rozumie poruszane problemy na zajęciach, posiada podstawowa wiedze w obrębie poruszanych na zajęciach tematów.
Uzyskał co najmniej 40 % maksymalnej łącznej liczby punktów z testu i zaliczył ćwiczenia oraz pracę zaliczeniową z tematyki pracy własnej studenta na ocenę dostateczną.
Poprawie umie zdefiniować podstawowe pojęcia z zakresu systemów bezpieczeństwa państwa rozumie poruszane problemy na zajęciach, posiada podstawowa wiedzę w obrębie poruszanych na zajęciach tematów (0,5 za obecność i aktywność na zajęciach).
Uzyskał co najmniej 50 % maksymalnej łącznej liczby punktów z testu i zaliczył ćwiczenia oraz pracę zaliczeniową z tematyki pracy własnej studenta na ocenę dostateczną.
Potrafi wykorzystywać wiedzę posiadaną i nabytą podczas zajęć, umie argumentować i przedstawiać prawidłowo obszar zainteresowań systemów bezpieczeństwa państwa, zakres, cele i uwarunkowania stosunków politycznych, na poziomie dobrym określa problemy polityki zagranicznej państwa.
Uzyskał co najmniej 65 % maksymalnej łącznej liczby punktów z testu i zaliczył ćwiczenia oraz pracę zaliczeniową z tematyki pracy własnej studenta na ocenę dobrą.
Potrafi wykorzystywać wiedzę posiadaną i nabytą podczas zajęć, umie argumentować i przedstawiać prawidłowo obszar zainteresowań systemów bezpieczeństwa państwa, zakres, cele i uwarunkowania stosunków politycznych, na poziomie dobrym określa problemy polityki zagranicznej państwa (0,5 ) dopisywana za aktywność, obecność na zajęciach, inne.
Uzyskał co najmniej 70 % maksymalnej łącznej liczby punktów z testu i zaliczył ćwiczenia oraz pracę zaliczeniową z tematyki pracy własnej studenta na ocenę dobrą.
Umie wykazać się umiejętnością prawidłowych interpretacji zjawisk, prawidłowo wysuwa wnioski, planuje użycie nabytych umiejętności i potrafi przekazać swoją wiedzę innym z należytym zrozumieniem, samodzielnie poszukuje wiedzę oraz umiejętnie ją analizuje i interpretuje, posiada umiejętność uczenia się i postawę otwartą na wiedzę , sięga do literatury na dany temat i należycie ją wykorzystuje, potrafi uzasadniać i argumentować swoje poglądy.
Uzyskał co najmniej 80 % maksymalnej łącznej liczby punktów z testu i zaliczył ćwiczenia oraz pracę zaliczeniową z tematyki pracy własnej studenta na ocenę bardzo dobrą.

**Egzamin:**

nie

**Literatura:**

Literatura podstawowa:
1. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo WNT, Warszawa 2007.
2. Borowiecki R. i inni, System informacji strategicznej. Wywiad gospodarczy, Wyd. Difin, Warszawa 2001.
3. Cole E., Krutz R. L., Conley J., Bezpieczeństwo sieci Biblia, , Helion 2005.
4. Denning Dorothy E., Wojna informacyjna i bezpieczeństwo informacji, WNT, Warszawa 2002.
5. Janczak J., Nowak A., Bezpieczeństwo informacyjne. Wybrane problemy, AON, Warszawa 2013.
6. Nowak A., W. Scheffs, Zarządzanie bezpieczeństwem informacyjnym, AON, Warszawa 2010.
7. Kifner T., (1999) Polityka bezpieczeństwa i ochrony informacji, Wyd. Helion, Gliwice.
8. Kowalewski M., Kowalewski J., Polityka bezpieczeństwa informacji w praktyce, Wrocław 2014.
9. Liderman K., Bezpieczeństwo informacyjne, Warszawa, 2015.
10. Liderman K., Analiza ryzyka i ochrona informacji w systemach komputerowych, Warszawa, 2009 i PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.
11. Łuczak J., Tyburski M., Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC27001, WUE, Poznań 2010
12. Dokumenty normatywne (ustawy i rozporządzenia).
13. Sutton R. J., Bezpieczeństwo telekomunikacji, WKiŁ, Warszawa 2002.
Literatura uzupełniająca:
1. Gałach A., Instrukcja zarządzania bezpieczeństwem systemu informatycznego, Wydawnictwo ODDK, Gdańsk 2004.
2. Janczak J., Świdzikowski G., Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym, AON, Warszawa 2004.
3. Nowak A., Scheffs W., Zarządzanie bezpieczeństwem informacyjnym, AON, Warszawa 2009.
4. Pańkowska M., Zarządzanie zasobami informatycznymi, Wyd. Difin, Warszawa 2001.
5. Pipkin D. L., Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa, WNT, Warszawa 2002.
6. Polaczek T., Audyt bezpieczeństwa informacji w praktyce, Helion, Gliwice 2006.
7. Stokłosa J., Bilski T., Pankowski T., Bezpieczeństwo danych w systemach informatycznych, PWN, Warszawa-Poznań 2001.
8. Stallings W., Ochrona danych w sieci i intersieci, WNT, Warszawa 1997.
9. Rattray Gregory J., Wojna strategiczna w cyberprzestrzeni, Wydawnictwo Naukowo-Techniczne, Warszawa 2004.
10. Praca zbiorowa, Biała księga bezpieczeństwa narodowego RP, BBN, Warszawa 2013.

**Witryna www przedmiotu:**

do uzupełnienia

**Uwagi:**

Brak

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt W\_PZBI01:**

Posiada wiedzę ogólną o systemie bezpieczeństwa informacji w organizacji

Weryfikacja:

kolokwium (pytania problemowe lub testowe)

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt W\_PZBI02:**

Posiada wiedzę o zagrożeniach bezpieczeństwa informacji

Weryfikacja:

Kolokwium (pytania testowe)

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt W\_PZBI03:**

Posiada wiedzę o organizacjach działających w obszarze bezpieczeństwa informacji i o relacjach między nimi, w tym bezpieczeństwa informacji w skali organizacji, kraju a także międzynarodowej.

Weryfikacja:

Kolokwium (pytania testowe)

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Efekt U\_PZBI01:**

Posiada umiejętność przewidywania ludzkich zachowań w zakresie powstawania zagrożeń bezpieczeństwa informacyjnego, analizowania ich motywów oraz społecznych konsekwencji.

Weryfikacja:

Wypowiedź pisemna na wybrany przez studenta
temat związany z problematyką przedmiotu (10 –
20 stron A4).

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt U\_PZBI02:**

Posiada umiejętności opracowania projektu bezpieczeństwa informacji, w tym: wykorzystuje podstawową wiedzę teoretyczną do opisu i analizowania procesów i zjawisk zachodzących w obszarze bezpieczeństwa informacji; posiada umiejętność prognozowania procesów i zjawisk zachodzących w obszarze bezpieczeństwa informacji z wykorzystaniem standardowych metod i narzędzi; analizuje rozwiązania konkretnych problemów występujących w obszarze bezpieczeństwa informacji i uczestniczy w podejmowaniu rozstrzygnięć w tym zakresie; potrafi zaplanować siły i środki przeznaczone do zapewnienia bezpieczeństwa informacji w celu wykonania typowych zadań w tym obszarze.

Weryfikacja:

Wypowiedź pisemna na wybrany przez studenta
temat związany z problematyką przedmiotu (10 –
20 stron A4).

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt U\_ PZBI03:**

Posiada umiejętności opracowania projektu systemu bezpieczeństwa informacji na rzecz zapewnienia bezpieczeństwa w organizacji.

Weryfikacja:

Wypowiedź pisemna na wybrany przez studenta
temat związany z problematyką przedmiotu (10 –
20 stron A4).

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt K\_PZBI01:**

Inspiruje oraz organizuje proces uczenia się innych osób.

Weryfikacja:

Wypowiedzi ustne na zajęciach, prezentowanie własnych poglądów

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt K\_PZBI02:**

Jest przygotowany do aktywnego uczestniczenia w grupach (zespołach) i organizacjach, realizujących cele na rzecz zapewnienia bezpieczeństwa informacyjnego. Potrafi komunikować się z otoczeniem i przekazywać podstawową wiedzę na temat działalności różnych podmiotów w obszarze bezpieczeństwa informacyjnego. Umie uczestniczyć w budowaniu projektów na rzecz zapewnienia bezpieczeństwa informacyjnego, zna aspekty prawne, ekonomiczne i polityczne tej działalności oraz potrafi przewidywać w podstawowym zakresie jej skutki.

Weryfikacja:

Wypowiedzi ustne na zajęciach, prezentowanie własnych poglądów.

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

**Efekt K\_PZBI03:**

Ma świadomość skutków zaniedbań w zakresie organizacji poszczególnych komponentów nowoczesnego systemu bezpieczeństwa informacji w organizacji.

Weryfikacja:

Wypowiedzi ustne na zajęciach, prezentowanie
własnych poglądów

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**