**Nazwa przedmiotu:**

Bezpieczeństwo informacji niejawnych i danych osobowych

**Koordynator przedmiotu:**

dr inż. K. Urbaniak

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Administracja

**Grupa przedmiotów:**

Obowiązkowe

**Kod przedmiotu:**

A22\_BINDO

**Semestr nominalny:**

4 / rok ak. 2018/2019

**Liczba punktów ECTS:**

3

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

1. Liczba godzin kontaktowych – 40 godzin, w tym:
a) obecność na wykładach - 15 godzin
b) obecność na ćwiczeniach - 15 godzin
c) udział w konsultacjach związanych z realizacją i zaliczeniem projektu - 10 godzin
2. Praca własna studenta – 35 godzin, w tym:
a) przygotowanie do ćwiczeń - 20 godzin
b) przygotowanie projektu - 15 godzin
Łączny nakład pracy studenta wynosi 75 godzin, co odpowiada 3 punktom ECTS.

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

1. Liczba godzin kontaktowych – 40 godzin, w tym:
a) obecność na wykładach - 15 godzin
b) obecność na ćwiczeniach - 15 godzin
c) udział w konsultacjach związanych z realizacją i zaliczeniem projektu - 10 godzin
Razem 40 godz. ↔ 1,6 pkt. ECTS

**Język prowadzenia zajęć:**

polski

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

1. Liczba godzin o charakterze praktycznym – 40 godzin, w tym:
a) obecność na ćwiczeniach - 15 godzin
b) udział w konsultacjach związanych z realizacją i zaliczeniem projektu - 10 godzin
c) przygotowanie projektu - 15 godzin
Razem 40 godz. ↔ 1,6 pkt. ECTS

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

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

**Wymagania wstępne:**

Znajomość zagadnień związanych z ochroną danych osobowych. Podstawowa wiedza w zakresie bezpiecznego przetwarzania informacji.

**Limit liczby studentów:**

grupa specjalizacyjna

**Cel przedmiotu:**

Przekazanie studentom wiedzy i umiejętności w zakresie:
- znajomości terminologii z zakresu bezpieczeństwa i ochrony informacji,
- poznania źródeł prawa i norm w zakresie ochrony danych osobowych i informacji niejawnych,
- poznania i rozumienia praktycznych metod ochrony danych osobowych,
- znajomości terminologii związanych z ochroną informacji niejawnych,
- poznania roli organów państwowych w ochronie danych osobowych,
- znajomości zasad bezpiecznego przetwarzania danych osobowych i informacji niejawnych,
- poznania sprzętowych i programowych metod ochrony danych,
- poznania procesu zarządzania ryzykiem,
- praktycznego opracowania analizy ryzyka przy wykorzystaniu wybranej metodyki,
- znajomości narzędzi informatycznych do wspomagania procesu zarządzania ryzykiem.

**Treści kształcenia:**

1. Podstawowe pojęcia i definicje z zakresu bezpieczeństwa i ochrony informacji.
2. Organizacja ochrony danych osobowych. Prawne aspekty ochrony danych osobowych w świetle prawa europejskiego i prawa krajowego. Zasady ochrony danych osobowych.
3. Podstawy ochrony informacji niejawnych. Ochrona IN w prawie polskim.
4. Metody organizacyjne i techniczne ochrony informacji.
5. Pojęcia i definicje związane z atrybutami bezpieczeństwa.
6. Pojęcia i definicje związane z zarządzaniem ryzykiem.
7. Metodyka zarządzania ryzykiem.
8. Analiza ryzyka - studium przypadku.
9. Narzędzia informatyczne w ochronie danych i informacji.
10. Narzędzia informatyczne wspomagające zarządzanie ryzykiem.

**Metody oceny:**

Zajęcia praktyczne związane są z wykonaniem projektu polegającego na wykonaniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Egzamin:**

nie

**Literatura:**

Stankowska I. - o ochronie informacji niejawnych. Komentarz, LexisNexis, Warszawa, 2010,
Hoc S., Szewc T., Ochrona danych osobowych i informacji niejawnych, Warszawa: Wydawnictwo C. H. Beck, 2014
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
Krasuski A., Ochrona danych osobowych na podstawie RODO, Wolters Kluwer Polska, 2018.
Prusak R., Kardas E. Zarządzanie ryzykiem bezpieczeństwa informacji w świetle wymagań normatywnych. 2017.
PN-I-13335-1:1999 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych. Warszawa: PKN, 1999.
PN-ISO/IEC 27001:2014 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania. Warszawa: PKN, 2013.
PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji. Warszawa: PKN, 2013.
Polaczek T. Audyt bezpieczeństwa informacji w praktyce. Gliwice: Helion, 2006.
https://www.zut.edu.pl/fileadmin/pliki/audytor/kontrolazarzadcza/podr%C4%99cznik\_zarzadzanie\_ryzykiem\_w\_sektorze\_publicznym.pdf
Pieleszek M. Bądź bezpieczny w cyfrowym świecie. Poradnik bezpieczeństwa IT dla każdego, Helion, 2018

**Witryna www przedmiotu:**

do uzupełnienia

**Uwagi:**

W trakcie zajęć wykonana zostanie analiza ryzyka przy wykorzystaniu metodyki stosowanej w administracji publicznej.

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka W\_01:**

Posiada wiedzę w zakresie ochrony informacji niejawnych oraz danych osobowych i znaczenie tej problematyki w obowiązującym stanie prawnym. Wie jak otoczenie prawne determinuje działania w zakresie ochrony informacji (P).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_W02, K\_W04, K\_W10, K\_W12 BNP

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

**Charakterystyka W\_02:**

Zna uwarunkowania i źródła zagrożeń bezpieczeństwa informacji (B).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_W12 BNP, K\_W10

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

**Charakterystyka W\_03:**

Wie jak skutecznie stosować zabezpieczenia informatyczne w celu minimalizacji ryzyka oddziaływania zagrożenia (I).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_W10, K\_W12 BNP

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

**Charakterystyka W\_04:**

Zna programowe i sprzętowe metody ochrony informacji (I).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_W10, K\_W12 BNP

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

### Profil ogólnoakademicki - umiejętności

**Charakterystyka U\_01:**

Potrafi dostosować warunki przetwarzania informacji do wymagań prawnych (P).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_U04, K\_U12, K\_U13 BNP, K\_U14 BNP

**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, II.T.P7S\_UW.2, II.T.P7S\_UW.1, I.P7S\_UK, I.P7S\_UO

**Charakterystyka U\_02:**

Potrafi analizować źródła zagrożeń i proponować metody zabezpieczeń, wpływające na minimalizację ryzyka wystąpienia negatywnych skutków zagrożeń (B).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_U14 BNP, K\_U13 BNP

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

**Charakterystyka U\_03:**

Potrafi zaproponować metody informatyczne w celu zabezpieczenia organizacji i minimalizacji ryzyka oddziaływania zagrożenia (I).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_U12, K\_U13 BNP

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

**Charakterystyka U\_04:**

Potrafi wykorzystywać narzędzia informatyczne w procesie zarządzania ryzykiem bezpieczeństwa informacji (I).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_U13 BNP, K\_U12

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

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka K\_01:**

Ma zdolność samodzielnego, skutecznego pozyskiwania informacji z dostępnych w ramach administracji publicznej systemów informacji prawnej i prawidłowej interpretacji tych informacji, w szczególności w zakresie ochrony danych osobowych i informacji niejawnych (P).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_K04, K\_K08 BNP, K\_K09 BNP, K\_K10 BNP

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

**Charakterystyka K\_02:**

Ma świadomość konsekwencji zaniedbań w zakresie zapewnienia bezpieczeństwa i ochrony informacji (B).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_K08 BNP, K\_K10 BNP

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

**Charakterystyka K\_03:**

Ma świadomość odpowiedzialności związanej z przetwarzaniem informacji w systemach teleinformatycznych (I).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_K08 BNP, K\_K09 BNP

**Powiązane charakterystyki obszarowe:** I.P7S\_KK

**Charakterystyka K\_04:**

Jest świadom znaczenia właściwych zabezpieczeń w systemach teleinformatycznych instytucji (I).

Weryfikacja:

Wykonanie projektu polegającego na przeprowadzeniu analizy ryzyka bezpieczeństwa informacji - studium przypadku. Praca zespołowa.

**Powiązane charakterystyki kierunkowe:** K\_K08 BNP, K\_K09 BNP

**Powiązane charakterystyki obszarowe:** I.P7S\_KK