**Nazwa przedmiotu:**

Bezpieczeństwo informacji niejawnych i danych osobowych

**Koordynator przedmiotu:**

dr inż. Krzysztof Urbaniak

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Administracja

**Grupa przedmiotów:**

Bezpieczeństwo Narodowe Polski

**Kod przedmiotu:**

A2\_BIN

**Semestr nominalny:**

4 / rok ak. 2014/2015

**Liczba punktów ECTS:**

3

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

1) Liczba godzin kontaktowych - 35 godz., w tym:
a) udział w wykładach - 15 godz.,
b) udział w ćwiczeniach - 15 godz.,
c) udział w konsultacjach poza zajęciami - 5 godz.
2) Liczba godzin pracy własnej studenta - 40 w tym:
a) bieżące przygotowanie do uczestnictwa w wykładach - 5 godz.,
b) studia nad literaturą przedmiotu - 5 godz.,
c) zapoznanie się z literaturą prawniczą w tym z aktami prawnymi - 5 godz.,
d) realizacja zadania projektowego (ćwiczeniowego) - 20 godz.,
e) przygotowanie do zaliczenia projektu + zaliczenie ćwiczeń – 5 godz.
Razem 75 godz. ↔ 3 pkt. ECTS

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

1) Liczba godzin kontaktowych - 50 godz., w tym:
a) prowadzenie wykładu - 15 godz.
b) prowadzenie ćwiczeń - 15 godz.
c) przygotowanie oraz zaliczenie zadania projektowego - 15 godz.
d) konsultacje (poza wykładem) - 5 godz.
Razem 50 godz. ↔ 2 pkt. ECTS

**Język prowadzenia zajęć:**

polski

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

1) Liczba godzin kontaktowych - 15 godz., w tym:
a) udział w ćwiczeniach - 15 godz.,
2) Liczba godzin pracy własnej studenta - 25 w tym:
a) realizacja zadania projektowego (ćwiczeniowego) - 20 godz.,
b) przygotowanie do zaliczenia projektu + zaliczenie ćwiczeń – 5 godz.
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:**

Przedmiot wymaga podstawowej znajomości zasad bezpieczeństwa w zakresie przetwarzania informacji.

**Limit liczby studentów:**

grupa specjalizacyjna

**Cel przedmiotu:**

Celem przedmiotu jest zapoznanie studentów z podstawowymi pojęciami i zasadami bezpiecznego przetwarzania danych ze szczególnym uwzględnieniem danych osobowych i informacji niejawnych. Studenci zostaną zapoznani z zasadami wykorzystywania mechanizmów przetwarzania danych ze szczególnym uwzględnieniem zasad bezpieczeństwa i ochrony danych. Zostaną omówione ustawy regulujące te zasady tj. o ochronie danych osobowych, o ochronie informacji niejawnych oraz wybrane rozporządzenia w tym zakresie. Omówiona zostanie instytucja Generalnego Inspektora Ochrony Danych Osobowych i jego kompetencje. Prawa osoby, której dane dotyczą. Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych (karna i służbowa).
Dodatkowo studenci zostaną zapoznani z Metodyką zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych. Celem ćwiczeń praktycznych jest zapoznanie studentów z wybraną metodyką zarządzania ryzykiem w urzędach administracji rządowej w zakresie zagrożeń pochodzących z sieci teleinformatycznych. Kolejnym zadaniem będzie zapoznanie studentów z zagrożeniami i podatnościami występującymi w sieciach teleinformatycznych oraz metody zabezpieczania i ochrony danych.

**Treści kształcenia:**

Wykłady:
1. Podstawowe pojęcia związane z zasadami bezpiecznego przetwarzania informacji.
2. Ustawa o ochronie danych osobowych. Podstawowe pojęcia z zakresu ochrony danych osobowych. Instytucja Generalnego Inspektora Ochrony Danych Osobowych i jego kompetencje. Prawa osoby, której dane dotyczą. Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych.
3. Wybrane akty wykonawcze do ustawy o ochronie danych osobowych. Zabezpieczanie zbiorów danych osobowych.
4. Ustawa o ochronie informacji niejawnych. Organizacja ochrony informacji niejawnych. Dostęp do informacji niejawnych. Zasady sporządzania
i oznaczania materiałów niejawnych.
5. Metodyka zarządzania ryzykiem w instytucji przetwarzającej informacje.

Ćwiczenia:
1. Analiza zagrożeń i podatności oraz ich wpływ na bezpieczeństwo informacji.
2. Typy incydentów i metody zabezpieczeń.
3. Metodyka zarządzania ryzykiem. Szacowaniu ryzyka, postępowaniu z ryzykiem, akceptowaniu ryzyka, monitorowaniu ryzyka, informowaniu o ryzyku.

**Metody oceny:**

Warunkiem zaliczenia wykładu jest uzyskanie pozytywnej oceny z zaliczenia ćwiczeń. Zaliczenie ćwiczeń odbywa się w formie pisemnej. Warunkiem zaliczenia ćwiczeń jest wykonanie i zaliczenie w grupach (max. 5 osób) „projektu”. Student jest zobowiązany dostarczyć projekt w ustalonym terminie. W przypadku istotnych błędów w wykonanym projekcie student (grupa) po omówieniu z prowadzącym ćwiczenia ma prawo do poprawy projektu i oddanie poprawionego projektu w ustalonym terminie.
Praca zaliczeniowa w postaci opracowania projektu na temat związany z przedmiotem, np. analizy ryzyka (postać elektroniczna, plik Excel lub Word). Opracowanie podstawowej analizy ryzyka wybraną metodyką zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w zaproponowanym podmiocie.
Określenie: rodzajów zagrożeń, zdefiniowanie ryzyk, określenie prawdopodobieństwa, określenie wpływu na dostępność, na integralność oraz poufność informacji. Określenie pierwotnego poziomu ryzyka, zabezpieczeń, skuteczności sterowania. Określenie końcowego poziomu ryzyka oraz decyzji o postępowaniu z ryzykiem.
Praca w grupie (do 5 osób).

**Egzamin:**

nie

**Literatura:**

1. S. Hoc, T. Szewc, Ochrona danych osobowych i informacji niejawnych, Warszawa : Wydawnictwo C. H. Beck, 2014
2. POLITYKA OCHRONY CYBERPRZESTRZENI RZECZYPOSPOLITEJ POLSKIEJ, RZECZPOSPOLITA POLSKA Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, 2013.
3. Banyś T.A.J., Łuczak J., Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych, PRESSCOM, Wrocław 2014, Wyd. II uzupełnione i rozszerzone.
4. J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych : komentarz, Warszawa Wolters Kluwer Polska, 2011
5. M. Witkowski, D. Jęda, Ochrona informacji niejawnych : nowe rozwiązania, Warszawa 2007
6. Ustawy i rozporządzenia regulujące problematykę ochrony danych osobowych i informacji.
7. Jerzy Stanik. MAiC. Wybrane aspekty w procesie projektowania, budowy i wdrażania systemu zarządzania ryzykiem.
8. PN ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji. Wymagania.
9. PN ISO/IEC 27005 Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji.
10. Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych. Warszawa 2015.

**Witryna www przedmiotu:**

nie dotyczy

**Uwagi:**

nie dotyczy

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt W\_01:**

Zna podstawowoe pojęcia z zakresu ochrony danych osobowych i informacji
niejawnych

Weryfikacja:

Praca zaliczeniowa w postaci opracowania analizy ryzyka (postać elektroniczna, plik Excel lub Word). Opracowanie podstawowej analizy ryzyka wybraną metodyką zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w zaproponowanym podmiocie.
Określenie: rodzajów zagrożeń, zdefiniowanie ryzyk, określenie prawdopodobieństwa, określenie wpływu na dostępność, na integralność oraz poufność informacji. Określenie pierwotnego poziomu ryzyka, zabezpieczeń, skuteczności sterowania itd.

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

**Powiązane efekty obszarowe:** S2A\_W06, S2A\_W09, S2A\_W01, S2A\_W02, S2A\_W03, S2A\_W07, S2A\_W11

**Efekt W\_02:**

Wie na czym polega zarządzanie bezpieczeństwem informacji w instytucji.

Weryfikacja:

Praca zaliczeniowa w postaci opracowania analizy ryzyka (postać elektroniczna, plik Excel lub Word). Opracowanie podstawowej analizy ryzyka wybraną metodyką zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w zaproponowanym podmiocie.
Określenie: rodzajów zagrożeń, zdefiniowanie ryzyk, określenie prawdopodobieństwa, określenie wpływu na dostępność, na integralność oraz poufność informacji. Określenie pierwotnego poziomu ryzyka, zabezpieczeń, skuteczności sterowania itd.

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

**Powiązane efekty obszarowe:** S2A\_W06, S2A\_W09, S2A\_W01, S2A\_W02, S2A\_W03, S2A\_W07, S2A\_W11

**Efekt W\_03:**

Ma wiedzę na temat wybranej metodyki zarządzania ryzykiem w instytucji w której przetwarzane są informacje.

Weryfikacja:

Praca zaliczeniowa w postaci opracowania analizy ryzyka (postać elektroniczna, plik Excel lub Word). Opracowanie podstawowej analizy ryzyka wybraną metodyką zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w zaproponowanym podmiocie.
Określenie: rodzajów zagrożeń, zdefiniowanie ryzyk, określenie prawdopodobieństwa, określenie wpływu na dostępność, na integralność oraz poufność informacji. Określenie pierwotnego poziomu ryzyka, zabezpieczeń, skuteczności sterowania itd.

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

**Powiązane efekty obszarowe:** S2A\_W06, S2A\_W09, S2A\_W01, S2A\_W02, S2A\_W03, S2A\_W07, S2A\_W11

### Profil ogólnoakademicki - umiejętności

**Efekt U\_01:**

Potrafi analizować proponowane rozwiązania w zakresie ochrony danych osobowych i informacji niejawnych

Weryfikacja:

Praca zaliczeniowa w postaci opracowania analizy ryzyka (postać elektroniczna, plik Excel lub Word). Opracowanie podstawowej analizy ryzyka wybraną metodyką zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w zaproponowanym podmiocie.
Określenie: rodzajów zagrożeń, zdefiniowanie ryzyk, określenie prawdopodobieństwa, określenie wpływu na dostępność, na integralność oraz poufność informacji. Określenie pierwotnego poziomu ryzyka, zabezpieczeń, skuteczności sterowania itd.

**Powiązane efekty kierunkowe:** K\_U06, K\_U12, K\_U13 BNP, K\_U14 BNP

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

**Efekt U\_02:**

Potrafi zaproponować i wdrożyć konkretne rozwiązania w zakresie zapewnienia
bezpieczeństwa informacji

Weryfikacja:

Praca zaliczeniowa w postaci opracowania analizy ryzyka (postać elektroniczna, plik Excel lub Word). Opracowanie podstawowej analizy ryzyka wybraną metodyką zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w zaproponowanym podmiocie.
Określenie: rodzajów zagrożeń, zdefiniowanie ryzyk, określenie prawdopodobieństwa, określenie wpływu na dostępność, na integralność oraz poufność informacji. Określenie pierwotnego poziomu ryzyka, zabezpieczeń, skuteczności sterowania itd.

**Powiązane efekty kierunkowe:** K\_U06, K\_U12, K\_U13 BNP, K\_U14 BNP

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

**Efekt U\_03:**

Potrafi opracować analizę ryzyka w zakresie bezpieczeństwa informacji (podatności, zagrożenia, ryzyko). Zakres podstawowy analizy.

Weryfikacja:

Praca zaliczeniowa w postaci opracowania analizy ryzyka (postać elektroniczna, plik Excel lub Word). Opracowanie podstawowej analizy ryzyka wybraną metodyką zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w zaproponowanym podmiocie.
Określenie: rodzajów zagrożeń, zdefiniowanie ryzyk, określenie prawdopodobieństwa, określenie wpływu na dostępność, na integralność oraz poufność informacji. Określenie pierwotnego poziomu ryzyka, zabezpieczeń, skuteczności sterowania itd.

**Powiązane efekty kierunkowe:** K\_U06, K\_U12, K\_U13 BNP, K\_U14 BNP

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

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt K\_01:**

Ma świadomość odpowiedzialności w zakresie przetwarzania danych osobowych i informacji niejawnych. Zna skutki zaniedbań w tym zakresie.

Weryfikacja:

Praca zaliczeniowa w postaci opracowania analizy ryzyka (postać elektroniczna, plik Excel lub Word). Opracowanie podstawowej analizy ryzyka wybraną metodyką zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w zaproponowanym podmiocie.
Określenie: rodzajów zagrożeń, zdefiniowanie ryzyk, określenie prawdopodobieństwa, określenie wpływu na dostępność, na integralność oraz poufność informacji. Określenie pierwotnego poziomu ryzyka, zabezpieczeń, skuteczności sterowania itd.

**Powiązane efekty kierunkowe:** K\_K03, K\_K04, K\_K08 BNP, K\_K09 BNP, K\_K10 BNP

**Powiązane efekty obszarowe:** S2A\_K02, S2A\_K03, S2A\_K01, S2A\_K03, S2A\_K06, S2A\_K07, S2A\_K01, S2A\_K03, S2A\_K01, S2A\_K03, S2A\_K01, S2A\_K03, S2A\_K05, S2A\_K07

**Efekt K\_02:**

Potrafi pracować w grupie i skutecznie analizować zdobyte informacje.

Weryfikacja:

Praca zaliczeniowa w postaci opracowania analizy ryzyka (postać elektroniczna, plik Excel lub Word). Opracowanie podstawowej analizy ryzyka wybraną metodyką zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w zaproponowanym podmiocie.
Określenie: rodzajów zagrożeń, zdefiniowanie ryzyk, określenie prawdopodobieństwa, określenie wpływu na dostępność, na integralność oraz poufność informacji. Określenie pierwotnego poziomu ryzyka, zabezpieczeń, skuteczności sterowania itd.

**Powiązane efekty kierunkowe:** K\_K03, K\_K04, K\_K08 BNP, K\_K09 BNP, K\_K10 BNP

**Powiązane efekty obszarowe:** S2A\_K02, S2A\_K03, S2A\_K01, S2A\_K03, S2A\_K06, S2A\_K07, S2A\_K01, S2A\_K03, S2A\_K01, S2A\_K03, S2A\_K01, S2A\_K03, S2A\_K05, S2A\_K07