**Nazwa przedmiotu:**

Zarządzanie ryzykiem w systemach teleinformatycznych

**Koordynator przedmiotu:**

dr hab. inż. Anna Stelmach, prof. uczelni, Wydział Transportu Politechniki Warszawskiej, Zakład Inżynierii Transportu Lotniczego

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Transport

**Grupa przedmiotów:**

Specjalnościowe

**Kod przedmiotu:**

**Semestr nominalny:**

6 / rok ak. 2022/2023

**Liczba punktów ECTS:**

3

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

90 godz., w tym: praca na wykładach 9 godz., praca na ćwiczeniach projektowych 9 godz., studiowanie literatury przedmiotu 13 godz., przygotowanie się do egzaminu 10 godz., realizacja pracy projektowej poza godzinami zajęć 44 godz., konsultacje 2 godz. (w tym konsultacje w zakresie ćwiczeń projektowych 1 godz.), obrona pracy projektowej 1 godz., udział w egzaminie 2 godz.

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

1,0 pkt ECTS (23 godz., w tym: praca na wykładach 9 godz., praca na ćwiczeniach projektowych 9 godz., konsultacje 2 godz., obrona pracy projektowej 1 godz., udział w egzaminie 2 godz.).

**Język prowadzenia zajęć:**

polski

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

2,0 pkt. ECTS (55 godz., w tym: praca na ćwiczeniach projektowych 9 godz., realizacja pracy projektowej poza godzinami zajęć 44 godz., konsultacje w zakresie ćwiczeń projektowych 1 godz., obrona pracy projektowej 1 godz.).

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

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

**Wymagania wstępne:**

Brak.

**Limit liczby studentów:**

Wykład: 100 osób, ćwiczenia projektowe: 18 osób.

**Cel przedmiotu:**

 Poznanie metod i nabycie praktycznych umiejętności w zakresie zarządzania ryzykiem zagrożeń identyfikowanych w systemach teleinformatycznych.

**Treści kształcenia:**

Wykład:
1. Zapotrzebowanie na analizy bezpieczeństwa.
2. Pojęcie systemu zarządzania bezpieczeństwem w systemach teleinformatycznych.
3. Poziomy zarządzania ryzykiem w teleinformatyce i rodzaje ryzyka. Metoda zarządzania ryzykiem zagrożeń. Wskazywanie i prezentacja obszarów/domen analiz do zarządzania ryzykiem zagrożeń.
4. Proces identyfikacji zagrożeń, źródła zagrożeń, rozpoznawanie źródeł zagrożeń, atrybuty źródeł zagrożeń, grupowanie źródeł zagrożeń, formułowanie zagrożeń, poziomy możliwości i poziomy skutków aktywizacji zagrożeń, charakteryzowanie zagrożeń, aktywizacja zagrożeń.
5. Zdarzenia niepożądane i niebezpieczne. Scenariusze rozwoju zdarzeń niebezpiecznych.
6. Modele ryzyka, uogólniony model ryzyka, modele ryzyka w znanych metodach analizy ryzyka, szacowanie ryzyka. Wartościowanie/wycena ryzyka zagrożeń i kategorie ryzyka. Reagowanie na ryzyko zagrożeń, postępowania wobec ryzyka, środki redukcji ryzyka - elementy systemów bezpieczeństwa, monitorowanie ryzyka i komunikowanie o ryzyku.
7. Zasady zarządzania ryzykiem w ramach teleinformatyki bezpieczeństwa w systemach teleinformatycznych.
8. Zarządzanie eksploatacją sieci teleinformatycznych z uwzględnieniem wymagań dotyczących zarządzania ryzykiem w systemie bezpieczeństwa teleinformatycznego.
9. Źródła zagrożeń i zagrożenia dla bezpieczeństwa teleinformatyki. Praktyczne sposoby eliminowania lub zmniejszania ryzyka zagrożeń w syystemach teleinformatycznych.
10. Zasady prowadzenia dokumentacji sprawozdawczej z procesu szacowania ryzyka zagrożeń w teleinformatyce.

Ćwiczenia projektowe:
1. Określanie zdarzeń w systemach teleinformatycznych, identyfikacja zagrożeń oraz wskazania ich źródeł w oparciu o Model 5M.
2. Nadawanie kodów statystycznych zdarzeniom w systemach teleinformatycznych.
3. Tworzenie modelu ryzyka dla zagrożeń wynikających z określonego przedsięwzięcia teleinformatycznego.
4. Praktyczne metody oddziaływania na ryzyko zagrożeń w systemach teleinformatycznych.
5. Opracowywanie Arkusza Zarządzania Ryzykiem i Karty Szacowania Ryzyka z punktu widzenia projektanta systemów teleinformatycznych.

**Metody oceny:**

Wykład: egzamin pisemny z wykorzystaniem testu złożonego z 10 pytań otwartych. Wymagane jest udzielenie poprawnych odpowiedzi na co najmniej 6 pytań.
Projekt: poprawne rozwiązanie 15 zadań projektowych. Wszystkie zadania projektowe muszą być poprawnie rozwiązane.
Ocena zintegrowana: wyliczona na podstawie poprawnych odpowiedzi udzielonych przez studenta w teście przygotowanym przez wykładowcę oraz średnia z ocen wszystkich zadań projektowych.

**Egzamin:**

tak

**Literatura:**

Literatura podstawowa:
1. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. nr 159 poz. 948)
2. SP 800-30 Rev. 1: Guide for Conducting Risk Assessments, 2012.
3. Łydziński D.: Analiza ryzyka w środowisku informatycznym, IT Professional, 2014.
4. Skorupski J.: Ilościowe metody analizy incydentów w ruchu lotniczym. Oficyna Wyd. Politechniki Warszawskiej, Warszawa, 2018.
5. Trebiński B.: Bezpieczeństwo teleinformatyczne, Obronność 2018.
6. Kałuża Z.: Bezpieczeństwo sieci i systemów teleinformatycznych, Kultura Bezpieczeństwa nr 10, 2018.
7. Zawiła-Niedźwiecki J.: Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji, OWPW 2018.

**Witryna www przedmiotu:**

www.wt.pw.edu.pl

**Uwagi:**

O ile nie powoduje to zmian w zakresie powiązań danego przedmiotu z efektami uczenia się określonymi dla programu studiów w treściach kształcenia mogą być wprowadzane na bieżąco zmiany związane z uwzględnieniem najnowszych osiągnięć naukowych.

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka W01:**

Zna główne obszary zarządzania ryzykiem w systemach teleinformatycznych, podstawowe przyczyny i czynniki zagrożeń. Zna podstawowe metody, techniki, narzędzia analizy ryzyka w systemach teleinformatycznych.

Weryfikacja:

Egzamin pisemny z wykorzystaniem testu złożonego z 10 pytań otwartych, wymagane jest udzielenie poprawnych odpowiedzi na co najmniej 6 z tych pytań.

**Powiązane charakterystyki kierunkowe:** Tr1A\_W12, Tr1A\_W09, Tr1A\_W05

**Powiązane charakterystyki obszarowe:** P6U\_W, I.P6S\_WG.o, I.P6S\_WK, III.P6S\_WK

### Profil ogólnoakademicki - umiejętności

**Charakterystyka U01:**

Potrafi w sposób krytyczny korzystać z literatury i innych materiałów źródłowych w celu analizy zagrożeń wpisujących się merytorycznie w problematykę zarządzania ryzykiem w systemach teleinformatycznych.

Weryfikacja:

Rozwiązanie zagadnień projektowych, wymagane jest poprawne rozwiązanie dwóch zagadnień.

**Powiązane charakterystyki kierunkowe:** Tr1A\_U18, Tr1A\_U01

**Powiązane charakterystyki obszarowe:** P6U\_U, I.P6S\_UW.o, III.P6S\_UW.o

**Charakterystyka U02:**

Potrafi identyfikować, interpretować i wyjaśniać podstawowe zjawiska i procesy związane ściśle
z teorią i praktyką zarządzania ryzykiem w systemach teleinformatycznych.

Weryfikacja:

Prezentacja, analiza i dyskusja wybranego zagadnienia projektowego. Wymagane przedstawienie spójnego i logicznego omówienia zadania.

**Powiązane charakterystyki kierunkowe:** Tr1A\_U18, Tr1A\_U03

**Powiązane charakterystyki obszarowe:** P6U\_U, I.P6S\_UW.o, III.P6S\_UW.o, I.P6S\_UK

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka K01:**

Rozumie istotność problematyki zarządzania ryzykiem w systemach teleinformatycznych, rozumie konieczność identyfikacji zagrożeń oraz ich konsekwencji.

Weryfikacja:

Aktywny udział w dyskusji podczas prezentacji przygotowanych przez innych studentów. Wymagane co najmniej 2 pogłębione udziały w dyskusji.

**Powiązane charakterystyki kierunkowe:** Tr1A\_K01

**Powiązane charakterystyki obszarowe:** P6U\_K, I.P6S\_KK