Opis przedmiotu

1. Nazwa przedmiotu: Zarządzanie bezpieczeństwem informacji

2. **Kod przedmiotu: 11.3 BSS.ZBI.07**

3. **Język wykładowy**: polski

4. **Kierunek**: Informatyka

5. **Specjalność: Bezpieczeństwo sieci i systemów informatycznych**

6. **Rok**: IV Semestr: 7

7. **Tytuł/stopień oraz imię i nazwisko prowadzącego przedmiot**:

Dr inż. Mariusz Gola

8. **Tytuły/stopnie oraz imiona i nazwiska pozostałych członków zespołu**:

……..

9. **Formy zajęć wchodzące w skład przedmiotu, wymiar godzinowy, forma zaliczenia**:

Forma zajęć	Wykład	Ćwiczenia/ Ćwiczenia tablicowe	Laboratorium/ Ćwiczenia praktyczne	Projekt	Seminarium
Liczba godzin w semestrze	30		15		
Forma zaliczenia	Kolokwium		Zaliczenie		

10. **Liczba punktów ECTS**: 2

11. **Poziom** : zaawansowany

12. **Wymagania wstępne**:

Ogólna znajomość systemów operacyjnych i sieci komputerowych i zagadnień związanych z ochrona informacji w systemach i sieciach komputerowych.

13. **Cele kształcenia**:

Celem przedmiotu jest zapoznanie studentów z technicznymi i organizacyjnymi aspektami związanymi z zarządzaniem bezpieczeństwem informacji. Po ukończeniu przedmiotu student będzie posiadał wiedzę niezbędną do opracowania a także weryfikacji polityki bezpieczeństwa firmy. Jednym z celów jest także zapoznanie studentów z aspektami przeprowadzania audytów teleinformatycznych..

14. **Opis treści kształcenia w ramach poszczególnych form zajęć**:

14.1. **Wykład**:

W ramach wykładu poruszane będą treści związane z następującymi zagadnieniami:
- Informacja w działalności organizacji - zagrożenia dla ciągłości działalności.
- Klasyfikacja zagrożeń i ich źródło.
- Normy zarządzania bezpieczeństwem informacji.
- Podstawowe pojęcia i definicje zawarte w normie ISO/IEC 27001:2005.
- System zarządzania bezpieczeństwem informacji, model zarządzania i wymagania
- Polityka bezpieczeństwa, organizacja i zarządzanie bezpieczeństwem informacji, zarządzanie

aktywami bezpieczeństwo osobowe, fizyczne i środowiskowe, bezpieczeństwo aplikacji i systemów, zarządzanie systemami i sieciami, kontrola dostępu do systemów, rozwój i utrzymanie systemów, zarządzanie incydentami i ciągłością działania, zgodność z regulacjami prawnymi, niezależne przeglądy i kontrola wewnętrzna.

- Analiza ryzyka i definiowanie potrzeb dla systemów przetwarzających informacje.
- Nadzór i odpowiedzialność.
- Dokumentacja systemu zarządzania bezpieczeństwem informacji.
- Przeprowadzanie audytu teleinformatycznego. Cele i powody przeprowadzania audytów, skład zespołu audytowego, poszczególne etapy audytu, najlepsze praktyki audytowi, przedstawienie norm, metodologia audytu, obszary prac audytowych , prace wykonywane na poszczególnych etapach audytu

14.4.Ćwiczenia teoretyczne:

14.5.Laboratorium/ Ćwiczenia praktyczne

W ramach laboratorium studenci powinni w sposób praktyczny utrwalać i weryfikować swoją widzę nabyta podczas wykładów. Ćwiczenia laboratoryjne będą prowadzone w następujących formach.,

Analiza przypadku: Na podstawie opracowań przygotowanych przez prowadzącego studenci będą analizować bezpieczeństwo wybranej firmy, zgodność zastosowanych rozwiązań z istniejącymi normami. Będą proponować własne rozwiązania. Studenci będą także przygotowywać dokumentacje niezbędną do przeprowadzania audytu teleinformatycznego.

***Projekt*:** Na podstawie wytycznych podanych przez prowadzącego (potrzeby klienta) studenci będą opracowywać politykę bezpieczeństwa dla firmy. Rozwiązania te będą dyskutowane podczas zajęć z prowadzącym i pozostałymi studentami.

Ćwiczeni praktyczne: Studenci będą wykonywać ćwiczenia praktyczne związane wykorzystaniem testów penetracyjnych, analizą ruchu sieciowego, badaniem bezpieczeństwa systemów.

15. **Literatura podstawowa**:

1. Polityka bezpieczeństwa i ochrony informacji, Tadeusz Kifner, Helion 1999
2. Przewodnik audytora systemów informatycznych, Marian Molski, Małgorzata Łacheta Helion 2006
3. Audyt bezpieczeństwa informacji w praktyce, Tomasz Polaczek Helion 2006

16. **Literatura towarzysząca**:

1. Hacking. Sztuka penetracji. Wydanie II, Jon Erickson Helion 2008
2. 125 sposobów na bezpieczeństwo sieci. Wydanie II, Autor: Andrew Lockhart, Helion 2007
3. PKI. Podstawy i zasady działania, Carlisle Adams, PWN 2007