KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Ochrona informacji w systemach telekomunikacyjnych

Przedmiot

Kierunek studiów
Elektronika i Telekomunikacja

Rok/semestr
II/III

Studia w zakresie (specjalność)
Elektroniczne Systemy Programowalne i Optotelekomunikacja

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
30	0	
Ćwiczenia	Projekty/seminaria	
0	15	

Liczba punktów ECTS

4

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr hab. inż. Mieczysław Jessa

mieczyslaw.jessa@put.poznan.pl

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać uporządkowaną, podbudowaną matematycznie, szczegółową wiedzę z podstaw teorii telekomunikacji niezbędną do zrozumienia, analizy, oceny działania analogowych i cyfrowych systemów telekomunikacyjnych. Powinien również posiadać umiejętność pozyskiwania informacji z literatury, baz danych oraz innych źródeł w języku polskim lub angielskim.

Cel przedmiotu

Przekazanie studentom wiedzy na temat metod ochrony informacji w systemach telekomunikacyjnych.

Przedmiotowe efekty uczenia się

Wiedza

1. Ma praktyczną wiedzę na temat systemów bezpieczeństwa lub metod umożliwiających zapewnienie bezpieczeństwa informacji przesyłanych w systemach telekomunikacyjnych.

Umiejętności

1. Potrafi zastosować i/lub zaprojektować profesjonalne systemy nadzoru i bezpieczeństwa w różnego rodzaju sieciach bądź systemach telekomunikacyjnych.

2. Zna ograniczenia własnej wiedzy i umiejętności, rozumie konieczność dalszego dokształcania się.

Kompetencje społeczne

1. Ma poczucie odpowiedzialności za zaprojektowane systemy (elektroniczne i telekomunikacyjne) i zdaje sobie sprawę z zagrożeń dla ludzi i dla społeczeństwa w wypadku ich nieodpowiedniego zaprojektowania lub wykonania.

2. Posiada świadomość konieczności profesjonalnego podejścia do rozwiązywanych problemów technicznych i podejmowania odpowiedzialności za proponowane przez siebie rozwiązania techniczne.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu jest weryfikowana na podstawie pisemnego i/lub ustnego egzaminu, składającego się z 5 pytań otwartych, identycznie punktowanych. Próg zaliczeniowy wynosi 50%. Rozkład progów dla ocen od 2 do 5 jest równomierny. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania otwarte, przesyłane są studentom drogą mailową z wykorzytaniem uczelnianej poczty elektronicznej.

Wiedza i umiejętności nabyte w czasie realizacji zadań projektowych są weryfikowane na podstawie opracowanego projektu oraz prezentacji projektu przed grupą ćwiczeniową. Projekt i prezentacja są oceniane oddzielnie. Ocena końcowa jest średnią arytmetyczną obu ocen. Stosowana skala jest następująca: poniżej 3 - ocena 2,0, od 3 do 3,25 - ocena 3,0; od 3,26 do 3,75 - ocena 3,5; od 3,76 do 4,25 - ocena 4,0; od 4,26 do 4,75 - ocena 4,5; powyżej 4,75 - ocena 5,0.

Treści programowe

W ramach wykładu studenci poznają podstawowe metody ochrony informacji. Omawiane są takie pojęcia jak: podatność, zagrożenie, incydent, klasyfikacja zagrożeń, kategorie zagrożeń, przykłady zagrożeń dla przewodowych sieci telekomunikacyjnych, bezprzewodowych sieci telekomunikacyjnych, sieci komputerowych, zależności przyczynowo-skutkowe w procesie identyfikacji zagrożeń, statystyki awarii, podatności i zabezpieczeń, wnioski ze statystyk awarii oraz analiz podatności i zabezpieczeń, standardy i normy bezpieczeństwa informacyjnego (normy oficjalne-de jure, regionalne, krajowe, pozostałe tj. stosowane de facto), przykładowe modele ochrony informacji (Grahama-Denninga, Bella, Biby itp.), pojęcie ryzyka, metody analizy i szacowania ryzyka (dedukcyjne, indukcyjne, jakościowe, ilościowe), redukcja ryzyka, metody zarządzania ryzykiem wg norm BS, ISO/EIC, NIST oraz PN, metody zarządzania bezpieczeństwem wg BS, ISO/EIC, NIST oraz PN, trójpoziomowy model odniesienia, dokumenty ochrony informacji, ocena stanu ochrony informacji, audyt polityki bezpieczeństwa, wdrażanie zapisów dokumentu pt. "Polityka bezpieczeństwa" do praktyki telekomunikacyjnej.

Zajęcia projektowe polegają na opracowaniu oraz implementacji programowej/sprzętowej elementów zabezpieczeń systemów telekomunikacyjnych proponowanych przez prowadzącego lub przez

studentów, po uprzedniej akceptacji prowadzącego. Elementy proponowane przez prowadzącego to: szacowanie ryzyka przykładowego zdarzenia (kradzież karty dostępowj, kredytowej, hasła, PIN, uszkodzenie serwerta poczty itp.) za pomocą jednej z metod omawianych na wykładzie, implementacja metody uwierzytelnienia i/lub autoryzacji w układzie FPGA, programowa albo sprzętowa implementacja metody zapewnienia poufności transmisji email w sieci publicznej, opracowanie przykładowego dokumentu polityki bezpieczeństwa dla małej firmy, opracowanie na podstawie PN wytycznych do audytu bezpieczeństwa lokalnej sieci komputerowej.

Metody dydaktyczne

1. Wykład: prezentacja multimedialna.

2. Projekt: połączenie metody ćwiczeniowej i projektowej

Literatura

Podstawowa

1. A. Białas "Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie", WNT, Warszawa, 2007.

2. K. Liderman "Bezpieczeństwo informacyjne, nowe wyzwania", PWN, 2017.

Uzupełniająca

1. J. Stokłosa, T. Bilski, T. Pankowski "Bezpieczeństwo danych w systemach informacyjnych", PWN, 2001.

2. K. Liderman "Analiza ryzyka i ochrona informacji w systemach komputerowych", PWN, Warszawa, 2008.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	58	2,0
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)[1]	42	2,0

[1] niepotrzebne skreślić lub dopisać inne czynności