KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Moduł obieralny w zakresie: Techniki informatyczne i systemy komunikacyjne w energetyce – Teleinformatyczne systemy przetwarzania i wymiany danych

Przedmiot

Kierunek studiów
Energetyka

Rok/semestr
3/5

Studia w zakresie (specjalność)
-

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Number of hours

Wykład
30

Laboratoria
15

Inne (np. online)

Ćwiczenia

Projekty/seminaria

Liczba punktów ECTS

3

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr inż. Andrzej Kwapisz

Wydział Inżynierii Środowiska i Energetyki

email:andrzej.kwapisz@put.poznan.pl

tel. 616652282

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Wiedza z zakresu analizy matematycznej, teorii obwodów, podstaw przetwarzania sygnałów, programowania, baz danych.

Wiedza z zakresu infrastruktury sieci komputerowych, oprogramowania do komputerowego wspomagania projektowania.

Umiejętność pracy i współdziałania w grupie.

Cel przedmiotu

Poznanie nowoczesnych technologii informacyjnych stosowanych w elektroenergetyce. Zastosowanie metod numerycznych do przetwarzania danych w układach elektroenergetycznych i elektrycznych. Zapoznanie studentów z metodami gromadzenia, transmisji i przechowywania danych z sieci elektroenergetycznej. Zapoznanie z metodami szyfrowania i ochrony danych oraz regulacjami prawnymi dotyczącymi ochrony danych.

Przedmiotowe efekty uczenia się

Wiedza

1. Ma wiedzę na temat metod przetwarzania danych pochodzących z sieci elektroenergetycznej.

2. Ma wiedzę dotycząca bezpieczeństwa systemów transmisji i przetwarzania danych.

Umiejętności

1. Potrafi wykorzystywać dostępne tradycyjne i elektroniczne zasoby danych w celu zdobywania wiedzy

2. Potrafi przeprowadzić analizę danych w oparciu o informacje dostępne w systemach teleinformatycznych wykorzystywanych w elektroenergetyce. Potrafi stosować metody kryptograficzne i tworzyć bezpieczne magazyny i kanały transmisji danych.

Kompetencje społeczne

1. Posiada umiejętności do samodzielnego studiowania, pracy w grupie i pozyskiwania nowej wiedzy oraz rozumie wpływ technologi IT na pracę inżyniera.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład

Ocena aktywności na zajęciach, ocena za wykonane prace domowe, kolokwium zaliczeniowe w formie pisemnej na koniec semestru, kolokwium obejmuje pytania testowe lub zadania problemowe, egzamin w formie pisemnej obejmujący tematykę przedmiotu oceniany w skali punktowej od 0 do 100%, ocena końcowa dla wykładów prowadzonych przez więcej niż jednego wykładowcę na podstawie średniej ważonej, ocena końcowa dla więcej niż jednej oceny składowej na podstawie średniej ważonej

Laboratorium

Weryfikacja indywidualnego przygotowania do zajęć obejmująca materiał z pojedynczego ćwiczenia lub bloku ćwiczeń, ocena wykonanych samodzielnie przez studenta indywidualnych sprawozdań z ćwiczeń, kolokwium na koniec semestru, kolokwium obejmuje pytania testowe lub zadania problemowe, wszystkie oceny w skali punktowej od 0 do 100%, ocena końcowa na podstawie średniej ważonej z wszystkich ocen składowych.

Treści programowe

Wykład

Systemy sterowania i nadzoru jako narzędzie monitorowania pracy systemu elektroenergetycznego. Zastosowanie techniki mikroprocesorowej w układach automatyki i teleinformatyki, przetwarzanie zarejestrowanych sygnałów. Wybrane zagadnienia z zakresu kryptografii. Metody bezpiecznej transmisji danych, metody uwierzytelniania w systemach IT. Zasady sporządzania dokumentacji inżynierskiej dla systemów IT. Wybrane zagadnienia z zakresu praw ochrony danych (ochrona baz danych, ochrona danych osobowych). Wspomaganie nauczania poprzez szerokie wykorzystanie programów ogólnodostępnych (licencje otwarte). Prezentacja dostępnych alternatywnych źródeł pozwalających na samodzielne poszerzanie wiedzy i umiejętności przez studenta.

Laboratorium

Systemy sterowania i nadzoru, zastosowanie techniki mikroprocesorowej, konfiguracja oprogramowania w architekturze klient-serwer, tworzenie i weryfikacja kluczy szyfrujących, szyfrowanie danych w bazach danych, tworzenie bezpiecznych połączeń sieciowych.

Metody dydaktyczne

Wykład

Multimedialna i interaktywna prezentacja przedstawiająca istotne zagadnienia związane z przedmiotem, dyskusja dydaktyczna w oparciu o literaturę przedmiotu, wykład informacyjny, wykład problemowy, analiza przypadku, praca na materiałach źródłowych.

Laboratorium

Realizacja ćwiczeń, wykorzystanie ogólnodostępnej informacji oraz narzędzi programowych do wspomagania procesu dydaktycznego, zachęcanie studentów do samodzielnego poszukiwania optymalnych rozwiązań i rozwiązywania problemów.

Literatura

Podstawowa

1. Kacejko P., Inżynieria elektryczna i informatyczna w nowych technologiach elektroenergetycznych, 2010
2. Kasprzak, A., Projektowanie struktur rozległych sieci komputerowych, Oficyna Wydawnicza PWr, 2001.
3. Stallings, W., Brown, L., Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 2, Helion, 2019.
4. Aumasson, J-P., Nowoczesna kryptografia : praktyczne wprowadzenie do szyfrowania, PWN, 2018.
5. Michael Welschenbach, Kryptografia w językach C i C++, Mikom, 2002.
6. Mikołaj Karpiński et al., Bezpieczeństwo informacji : praca zbiorowa, Wydawnictwo PAK, 2012.

Uzupełniająca

1. Janusz Szmidt, Michał Misztal, Wstęp do kryptologii, Oficyna Wydawnicza WIT, 2002.
2. J. Izydorczyk, W. Sułek, P. Zawadzki, Kody i szyfry, Wydawnictwo PŚl, 2017.
3. Stokłosa, J., Kryptograficzna ochrona danych w systemach komputerowych, Nakom, 1994.
4. Niels Ferguson, Bruce Schneier, Kryptografia w praktyce, Helion, 2004.

Bilans nakładu pracy przeciętnego studenta

	Godziny	ECTS
Łączny nakład pracy	94	3
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	55	2
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, opracowanie sprawozdań, przygotowanie do kolokwiów)	39	1