



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Cyberbezpieczeństwo i telekomunikacja w elektroenergetyce

Przedmiot

Kierunek studiów

Elektrotechnika

Studia w zakresie (specjalność)

Poziom studiów

studia II stopnia

Forma studiów

studia stacjonarne

Rok/semestr

1/2

Profil studiów

ogólnoakademicki

Język oferowanego przedmiotu

polski

Wymagalność

przedmiot obligatoryjny

Number of hours

Wykład

15

Laboratoria

Inne (np. online)

Ćwiczenia

Projekty/seminaria

Liczba punktów ECTS

1

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr inż. Andrzej Kwapisz

Odpowiedzialny za przedmiot/wykładowca:

Wydział Inżynierii Środowiska i Energetyki

email: andrzej.kwapisz@put.poznan.pl

tel. +48 61 665 2282

Wymagania wstępne

Student rozpoczynający przedmiot powinien posiadać podstawową wiedzę z zakresu informatyki obejmującą systemy operacyjne i sieci komputerowe, urządzenia sieciowe, podstawowe protokoły komunikacyjne oraz podstawową wiedzę dotyczącą systemów telekomunikacyjnych.

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z podstawowymi zagadnieniami dotyczącymi bezpieczeństwa systemów teleinformatycznych, zaznajomienie z zagrożeniami cyberbezpieczeństwa i przeciwdziałania zagrożeniom wynikającym ze stosowania nowoczesnych technologii IT.

Przedmiotowe efekty uczenia się

Wiedza

1. Zna i rozumie problemy związane z cyberbezpieczeństwem.

2. Ma uporządkowaną wiedzę z zakresu architektury i bezpieczeństwa systemów komputerowych i teleinformatycznych.

Umiejętności



1. Umie dokonać oceny zagrożeń cyberbezpieczeństwa dla systemów teleinformatycznych i opracować strategie przeciwdziałania tym zagrożeniom.

Kompetencje społeczne

1. Ma świadomość szybkiego postępu w zakresie technologii IT oraz wynikających z tego zagrożeń dla bezpieczeństwa infrastruktury fizycznej, bezpieczeństwa ekonomicznego i osobistego.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład

Ocena aktywności na zajęciach, 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, próg zaliczeniowy 60%. Liczba pytań na kolokwium 10-20, punktacja zależna od trudności pytania.

Treści programowe

Wykład

Wprowadzenie do zagadnień cyberbezpieczeństwa, zagrożenia, luki bezpieczeństwa, ataki w cyberprzestrzeni, złośliwe oprogramowanie, wyciek danych. Rodzaje ataków na sieć komputerową, ataki na systemy łączności bezprzewodowej. Szyfrowanie danych i kryptografia, metody kryptografii z zastosowaniem kluczy symetrycznych i asymetrycznych. Analiza przebiegu cyberataku, testy penetracyjne infrastruktury sieciowej. Uprawnienia bezpieczeństwa w systemach komputerowych. Zapobieganie zagrożeniom cyberbezpieczeństwa, monitorowanie i filtrowanie ruchu sieciowego, zapory sieciowe, wirtualne sieci prywatne (VPN). Podatność na cyberataki systemów telekomunikacyjnych i teletransmisyjnych stosowanych w elektroenergetyce.

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, pokaz multimedialny, demonstracja.

Literatura

Podstawowa

1. Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, PWN, Warszawa, 2017
2. Kowalewski J., Kowalewski M., Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni, Oficyna Wydawnicza PW, Warszawa, 2017
3. Krawiec J., Cyberbezpieczeństwo: podejście systemowe, Oficyna Wydawnicza PW, Warszawa, 2019
4. Liderman K. [red] i inni, Bezpieczeństwo teleinformatyczne: problemy formalne i techniczne, Wojskowa Akademia Techniczna, Warszawa, 2006
5. PN-EN 60950, Bezpieczeństwo urządzeń techniki informatycznej, PKN, Warszawa, 2002



6. PN-ISO/IEC 14888-3, Technika informatyczna - Techniki zabezpieczeń - Podpisy cyfrowe z załącznikiem - Część 3: Mechanizmy oparte na certyfikatach, PKN, Warszawa, 2002
7. PN-ISO/IEC 2382-8, Technika informatyczna - Terminologia - Bezpieczeństwo, PKN, Warszawa, 2001
8. Stallings W., Brown L., Bezpieczeństwo systemów informatycznych: zasady i praktyka. T. 1, Helion, Gliwice, 2019
9. Stallings W., Brown L., Bezpieczeństwo systemów informatycznych: zasady i praktyka. T. 2, Helion, Gliwice, 2019

Uzupełniająca

1. Białas A. [red.] i inni, Podstawy bezpieczeństwa systemów teleinformatycznych: podręcznik do szkoleń autoryzowanych przez Departament Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego: , Wydaw. Pracowni Komputerowej Jacka Skalmierskiego, Gliwice, 2002
2. Engebretson P., Hacking i testy penetracyjne: podstawy, Helion, Gliwice, 2013
3. Kennedy D. [red.] i inni, Metasploit: przewodnik po testach penetracyjnych, Helion, Gliwice, 2013
4. Kowalewski J., Kowalewski M., Zagrożenia informacji w cyberprzestrzeni, cyberterrorizm, Oficyna Wydawnicza PW, Warszawa, 2017
5. Luttgens J., Pepe M., Mandia K., Incydenty bezpieczeństwa: metody reagowania w informatyce śledczej, Helion, Gliwice, 2016
6. Parker C., Firewall nie powstrzyma prawdziwego smoka, czyli Jak zadbać o cyberbezpieczeństwo: przewodnik dla niefachowców, Helion, Gliwice, 2019
7. Scambray J., Shema M., Hakerzy - aplikacje webowe: [sekrety zabezpieczeń aplikacji webowych], Translator, 2002
8. Szychowiak. M., Bezpieczeństwo systemów informatycznych: zaawansowane ćwiczenia w systemach Windows i Linux, WPP, Poznań, 2017
9. Wołowski F., Zawila-Niedźwiecki J., Bezpieczeństwo systemów informacyjnych: praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, edu-Libri, Kraków-Warszawa, 2012
10. Odnośnik: https://pp-hip.pfsl.poznan.pl/ipac20/ipac.jsp?session=1662630L8QA66.63770&profile=bpp&page=1&group=0&term=Sieci+komputerowe+--+%3Frodki+zabezpieczaj3Fce.&index=SUBJECT&uindex=&aspect=basic_search&menu=search&ri=6&source=~!bpptest&1662632865190, Biblioteka PP, aktualizacja: 1.10.2022

Bilans nakładu pracy przeciętnego studenta

	Godziny	ECTS
Łączny nakład pracy	30	1
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	15	0,5
Praca własna studenta (studia literaturowe, analiza przedstawionych przypadków , przygotowanie do kolokwium)	15	0,5