KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Cyberbezpieczeństwo

Przedmiot

Kierunek studiów
Informatyka

Rok/semestr
2/3

Studia w zakresie (specjalność)
Sztuczna inteligencja

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
16	16	
Ćwiczenia	Projekty/seminaria	

Liczba punktów ECTS

2

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
prof. dr hab. inż. Mariusz Głąbowski
email: mariusz.glabowski@put.poznan.pl
tel: 61 665 3904
Wydział Informatyki i Telekomunikacji
Instytut Sieci Teleinformatycznych

Odpowiedzialny za przedmiot/wykładowca:
dr hab. inż. Paweł Śniatała
email: pawel.sniatala@put.poznan.pl
tel: 61 665 23 99
Wydział Informatyki i Telekomunikacji

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien mieć podstawową wiedzę z zakresu sieci komputerowych oraz algorytmów kryptograficznych. Powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł oraz mieć gotowość do podjęcia współpracy w ramach zespołu.

Cel przedmiotu

Przekazanie studentom wiedzy z zakresu szeroko rozumianego bezpieczeństwa teleinfomatycznego oraz metod i narzędzi wykorzystywanych do szacowania i kontroli ryzyka naruszenia poufności, integralności i dostępności danych. Zapoznanie studentów z zaawansowanymi metodami, technikami i narzędziami stosowanymi przy rozwiązywaniu złożonych zadań inżynierskich w obszarze projektowania i utrzymania systemów sieciowych odpowiedzialnych za bezpieczeństwo przesyłanych danych.

Przedmiotowe efekty uczenia się

Wiedza

Ma uporządkowaną i podbudowaną teoretycznie wiedzę ogólną związaną z kluczowymi zagadnieniami z zakresu bezpieczeństwa teleinformatycznego.

Ma zaawansowaną wiedzę szczegółową dotyczącą wybranych zagadnień z zakresu szeroko rozumianego bezpieczeństwa teleinfomatycznego oraz metod i narzędzi wykorzystywanych do szacowania i kontroli ryzyka naruszenia poufności, integralności i dostępności danych

Ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach informatyki i telekomunikacji w zakresie projektowania i utrzymania systemów sieciowych odpowiedzialnych za bezpieczeństwo przesyłanych danych.

Ma zaawansowaną i szczegółową wiedzę o procesach zachodzących systemach wykorzystywanych do szacowania i kontroli ryzyka naruszenia poufności, integralności i dostępności danych.

Umiejętności

Potrafi pozyskiwać informacje na temat zagrożeń bezpieczeństwa teleinformatycznego oraz technik ich szacowania i kontroli. Pozyskane informacje (w języku polskim i angielskim) potrafi integrować i poddawać krytycznej ocenie.

Potrafi planować i przeprowadzać testy w zakresie bezpieczeństwa teleinformatycznego oraz interpretować uzyskane wyniki i wyciągać wnioski.

Potrafi wykorzystać metody eksperymentalne do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych w obszarze bezpieczeństwa teleinformatycznego.

Potrafi integrować wiedzę z różnych obszarów informatyki i telekomunikacji przy przy formułowaniu i rozwiązywaniu zadań inżynierskich związanych z projektowaniem i implementacją systemów sieciowych odpowiedzialnych za bezpieczeństwo przesyłanych danych.

Potrafi ocenić przydatność i możliwość wykorzystania nowych rozwiązań sprzętowych i programowych służących do rozwiązywania zadań inżynierskich, polegających na budowie bezpiecznych systemów przesyłania danych.

Kompetencje społeczne

Rozumie, że w zakresie bezpieczeństwa teleinformatycznego wiedza i umiejętności bardzo szybko stają się przestarzałe.

Rozumie znaczenie wykorzystywania najnowszej wiedzy z zakresu bezpieczeństwa teleinformatycznego w rozwiązywaniu problemów badawczych i praktycznych. Ma świadomość konieczności profesjonalnego podejścia do rozwiązywanych problemów bezpieczeństwa teleinformatycznego i podejmowania odpowiedzialności za proponowane przez siebie projekty.

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 kolokwium ustnym i/lub pisemnym.

Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania, przesyłane są studentom drogą mailową z wykorzystaniem systemu uczelnianej poczty elektronicznej.

Kolokwium ustne i/lub pisemne obejmuje od 3 do 5 pytań, na które oczekuje się odpowiedzi opisowej. Każda odpowiedź na pytanie jest oceniana w skali od 0 do 5 punktów. Każde pytanie jest równo punktowane. Próg zaliczeniowy: 50% punktów.

W przypadku kolokwium ustnego studenci losują pytania ze zbioru 30 pytań. W przypadku kolokwium pisemnego pytania są zadawane przez prowadzącego.

Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są na bieżąco. Na każdych zajęciach laboratoryjnych oceniana jest poprawność wykonania ćwiczeń w skali od 2 do 5. Ocena końcowa jest średnią ocen uzyskanych z poszczególnych zajęć laboratoryjnych.Ocena końcowa jest średnią ocen uzyskanych z poszczególnych zajęć laboratoryjnych.

Treści programowe

Tematyka wykładów:

- Zapewnienie wysokiej niezawodności i dostępności urządzeń sieciowych odpowiedzialnych za bezpieczne przeyłanie danych.

- Projektowanie i utrzymanie sieci IPSec VPN oraz SSL VPN.

- Wirtualizacja zapór sieciowych.

- Zapewnienie bezpieczeństwa aplikacjom sieciowym (webowym).

- Techniki wykrywania i zapobiegania zagrożeniom w warstwie sieci.

- Bezpieczeństwo sieci bezprzewodowych.

- Bezpieczeństwo usług chmurowych i platform chmurowych.

- Bezpieczeństwo Internetu Rzeczy.

Tematyka laboratoriów:

- Podstawy konfiguracji zapór sieciowych (np. Cisco/Huawei/CheckPoint).

- Zabepiecznie dostępu do urządzeń sieciowych z wykorzystaniem serwera Radius (AAA).

- Projekt i implementacja systemu zapór sieciowych o zwiększonej niezawodności.

- Projekt i implementacja sieci IPSec VPN.

- Projekt i implementacja sieci SSL VPN.

- Konfiguracja systemu zapobiegania włamaniom (IPS).

- Filtrowanie i ochrona treści z wykorzystaniem zapór sieciowych.

Metody dydaktyczne

Wykład informacyjny: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy.

Ćwiczenia laboratoryjne: ćwiczenia praktyczne w grupach, z wykorzystaniem urządzeń sieciowych.

Literatura

Podstawowa

1. Joseph Migga Kizza: Guide to Computer Network Security; Springer International Publishing, 2020, 10.1007/978-3-030-38141-7

Uzupełniająca

1. Khondoker, Rahamatullah (Ed.): SDN and NFV Security - Security Analysis of Software-Defined Networking and Network Function Virtualization; Springer International Publishing 2018.

2. Aaron Woland, Vivek Santuka, Mason Harris, Jamie Sanbower: Integrated Security Technologies and Solutions - Volume I: Cisco Security Solutions for Advanced Threat Protection with Next Generation Firewall, Intrusion Prevention, AMP, and Content Security, May 14, 2018, Cisco Press.

3. Elaine Barker, Quynh Dang, Sheila Frankel, Karen Scarfone, Paul Wouters: Guide to IPsec VPNs (NIST Special Publication 800-77); National Institute of Standards and Technology; 2020; This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-77r1

4. J. Michael Stewart: Network Security, Firewalls And VPNs; Jones & Bartlett Learning Information Systems Security & Ass, 2nd Edition, 2013.

5. Gerardus Blokdyk: IPsec VPN A Complete Guide; 5STARCooks; 2019.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	50	2,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	32	1,0
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, przygotowanie do kolokwium, wykonanie projektów)[1]	18	1,0

[1] niepotrzebne skreślić lub dopisać inne czynności