KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo sieci

Przedmiot

Kierunek studiów
Informatyka

Rok/semestr
1/2

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
15	45	
Ćwiczenia	Projekty/seminaria	

Liczba punktów ECTS

5

Wykładowcy

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

Odpowiedzialny za przedmiot/wykładowca:
dr inż. Maciej Sobieraj
maciej.sobieraj@put.poznan.pl
tel: 61 665 3909
Wydział Informatyki i Telekomunikacji

Wymagania wstępne

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

Cel przedmiotu

Przekazanie studentom szczegółowej wiedzy teoretycznej z zakresu bezpieczeństwa sieci; przekazanie studentom wiedzy i umiejętności niezbędnych do projektowania i zapewniania bezpieczeństwa sieci; zapoznanie studentów z przemysłowymi standardami wdrażania rozwiązań w zakresie bezpieczeństwa sieci oraz stworzenie możliwości do nabycia umiejętności wymaganych do dalszego rozwoju kariery zawodowej (przygotowanie do egzaminów certyfikujących).

Przedmiotowe efekty uczenia się

Wiedza

Ma zaawansowaną wiedzę szczegółową dotyczącą wybranych zagadnień z zakresu zagrożeń

bezpieczeństwa sieci i usług chmurowych, metod i narzędzi wykorzystywanych do zapobiegania atakom, technik testowania bezpieczeństwa sieci.

Ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w zakresie bezpieczeństwa urządzeń sieciowych i bezpiecznych technik przesyłania danych; ma wiedzę na temat bieżących zagrożeń bezpieczeństwa systemów sieciowych.

Zna zaawansowane metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich z zakresu bezpieczeństwa sieci i systemów teleinformatycznych.

Umiejętności

Potrafi pozyskiwać z różnych źródeł informacje na temat zagrożeń bezpieczeństwa teleinformatycznego oraz technik skutecznego ich wykrywania i zapobiegania ich wykorzystania w systemach sieciowych. Pozyskane informacje (w języku polskim i angielskim) potrafi integrować i poddawać krytycznej ocenie.

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

Potrafi dokonać krytycznej analizy istniejących rozwiązań technicznych w obszarze bezpieczeństwa rozwiązań sieciowych oraz zaproponować ich ulepszenia.

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

Potrafi zaprojektować system zapewniający bezpieczeństwo przesyłanych danych.

Potrafi współdziałać w zespole przy formułowaniu i rozwiązywaniu zadań inżynierskich związanych z projektowaniem i implementacją systemów sieciowych odpowiedzialnych za bezpieczeństwo przesyłanych danych.

Potrafi określić kierunki dalszego uczenia się, niezbędne do efektywnej pracy w obszarze bezpieczeństwa sieci.

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 egzaminie pisemnym.

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

Egzamin pisemny 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.

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.

Treści programowe

Tematyka wykładów:

- Zagrożenia i ataki sieciowe, aktualny stan rozwiązań zapewniających bezpieczeństwa sieci.

- Przeciwdziałanie zagrożeniom: polityki bezpieczeństwa, narzędzia, usługi; zabezpieczenie dostępu do urządzenia; role administracyjne.

- Wprowadzenie do sieci definiowanych programowo i programowalności sieci.

- Uwierzytelnianie, autoryzacja, kontrola dostępu i zarządzanie tożsamością.

- Widoczność sieci (np. NetFlow, IPFIX itp.).

- Zabezpieczenie warstwy 2 (sieci VLAN; zagrożenia; IEEE 802.1AE/MACsec+).

- Zabezpieczanie płaszczyzny zarządzania, płaszczyzny sterowania i płaszczyzny danych urządzeń sieciowych.

- Technologie zapór sieciowych (przegląd list kontroli dostępu; rola zapór sieciowych w projektowaniu sieci; zapory sieciowe oparte na regułach strefowych).

- Zabezpieczanie sieci z użyciem ASA.

- Systemy wykrywania włamań i systemy zapobiegania włamaniom (implementacje różnych dostawców; obsługa i konfiguracja IPS).

- Wirtualne sieci prywatne (topologie; protokoły; implementacje: IPSec, DMVPN, FlexVPN, GETVPN, zdalny dostęp VPN oparty na kliencie, zdalny VPN bez klienta).

- Zabezpieczanie chmury.

- Testowanie bezpieczeństwa sieci.

Tematyka laboratoriów:

Zgodna z treścią wykładów

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.

2. Omar Santos, CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021

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	125	5,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	2,5
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, przygotowanie do egzaminu)[1]	65	2,5

[1] niepotrzebne skreślić lub dopisać inne czynności