KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo sieci [S2TIIZM1E>BS]

Przedmiot

Kierunek studiów
Technologie informacyjne dla inteligentnej i zrównoważonej mobilności/Information Technology for Smart and Sustainable Mobility

Rok/Semestr
1/1

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
32

Laboratorium
16

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

4,00

Koordynatorzy

dr hab. inż. Maciej Sobieraj
maciej.sobieraj@put.poznan.pl

Wykładowcy

Wymagania wstępne

Wiedza: Podstawowa wiedza z zakresu sieci komputerowych, w tym znajomość modelu OSI, protokołów komunikacyjnych (np. TCP/IP), adresowania IP i podstaw działania urządzeń sieciowych (routery, przełączniki). Znajomość podstaw systemów operacyjnych, szczególnie w kontekście zarządzania siecią i bezpieczeństwem (np. użytkownicy, uprawnienia, konfiguracja sieci w systemach Linux/Windows). Podstawy kryptografii - ogólne zrozumienie pojęć takich jak szyfrowanie, klucze, podpisy cyfrowe czy funkcje skrótu. Umiejętności: Rozwiązywanie problemów - szczególnie w kontekście algorytmicznym i matematycznym. Podstawy programowania - analiza i tworzenie prostych skryptów np. w językach Python, C++ lub Java. Myślenie analityczne - umiejętność metodycznego podejścia do złożonych problemów.

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z kluczowymi pojęciami, protokołami i technikami zabezpieczania sieci komputerowych na różnych warstwach modelu komunikacji.

Przedmiotowe efekty uczenia się

Wiedza:
Student ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w zakresie bezpieczeństwa sieci informatycznych
Student ma zaawansowaną i szczegółową wiedzę o procesach zachodzących w cyklu życia systemów informatycznych
Student zna zaawansowane metody, techniki i narzędzia związane z bezpieczeństwem sieci, w szczególności metody ochrony sieci bezprzewodowych, sposoby zabezpieczania aplikacji i usług za pomocą protokołów, sposoby zabezpieczania sieci prywatnych, protokoły bezpieczeństwa warstwy transportowej i warstwy sieciowej oraz mechanizmy bezpieczeństwa między warstwami sieciowymi.
Student ma wiedzę dotyczącą ryzyka i zagrożeń związanych z bezpieczeństwem sieci

Umiejętności:
Student potrafi posługiwać się technikami informacyjno-komunikacyjnymi wykorzystywanymi przy realizacji przedsięwzięć z zakresu bezpieczeństwa systemów informatycznych
Student potrafi planować i przeprowadzać eksperymenty, interpretować uzyskane wyniki i wyciągać wnioski oraz formułować i weryfikować hipotezy związane ze złożonymi problemami inżynierskimi i prostymi problemami badawczymi
Student potrafi ocenić przydatność metod i narzędzi służących do zabezpieczenia systemów informatycznych, w tym dostrzec ograniczenia tych metod i narzędzi

Kompetencje społeczne:
Student jest gotów do krytycznej oceny posiadanej wiedzy i rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają przestarzałe
Student rozumie znaczenie wykorzystywania najnowszej wiedzy z zakresu bezpieczeństwa sieci w projektowaniu i eksploatacji systemów informatycznych

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Egzamin pisemny
Praca praktyczna - rozwiązywanie zadań

Treści programowe

Nowoczesna kryptografia, algorytmy AES i RSA, kryptografia na krzywych eliptycznych, arytmetyka modularna, funkcje skrótu, kryptografia kwantowa.

Tematyka zajęć

•Podstawowe pojęcia: podstawowe elementy bezpieczeństwa sieci, takie jak kanały komunikacyjne, zapory sieciowe (firewalle), sieci VPN i serwery proxy.
•Bezpieczeństwo międzywarstwowe: mechanizmy bezpieczeństwa między warstwami sieciowymi, w tym EAP i RADIUS, wspierające bezpieczne uwierzytelnianie na różnych poziomach sieci.
•Bezpieczeństwo na poziomie sieci: protokoły warstwy sieciowej, takie jak IPSec, wykorzystywane do zabezpieczania komunikacji IP poprzez uwierzytelnianie i szyfrowanie.
•Bezpieczeństwo na poziomie transportowym: protokoły bezpieczeństwa warstwy transportowej, takie jak SSL/TLS i QUIC, zapewniające bezpieczne przesyłanie danych w sieci.
•Bezpieczeństwo na poziomie aplikacji/usług: zabezpieczanie aplikacji i usług za pomocą protokołów takich jak HTTPS, umożliwiających szyfrowaną komunikację internetową.
•Bezpieczeństwo sieci bezprzewodowych: metody ochrony sieci bezprzewodowych, w tym standardy WEP i WPA.
•Sieci prywatne (VLAN, VPN): projektowanie i zabezpieczanie sieci prywatnych, ze szczególnym uwzględnieniem VLAN i VPN.

Metody dydaktyczne

Kurs prowadzony w formie zdalnej synchronicznie. Dopuszcza się prowadzenie zajęć w formie stacjonarnej.
Prezentacja multimodalna. Przykłady praktyczne, studium przypadku.

Literatura

Podstawowa:
Stallings, W. (2020), Cryptography and Network Security: Principles and Practices, 8th Edition, Pearson.

Uzupełniająca:
-

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	52	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	48	2,00