KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Wprowadzenie do cyberbezpieczeństwa [S2Inf1E-CYB>WdCYB]

Przedmiot

Kierunek studiów
Informatyka/Computing

Rok/Semestr
1/1

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
30

Laboratorium
30

Inne (np. online)
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

5,00

Koordynatorzy

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien mieć podstawową wiedzę z zakresu sieci komputerowych, algorytmów kryptograficznych, systemów operacyjnych Windows i Linux. 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. Kurs obejmuje wiedzę i umiejętności potrzebne do skutecznego wykonywania zadań i obowiązków analityka cyberbezpieczeństwa pracującego w centrum operacji bezpieczeństwa (Security Operations Center). W ramach realizacji przedmiotu zostaną omówione domeny cyberbezpieczeństwa jako elementy bazowe do zarządzania cyberbezpieczeństwem organizacji. Przedstawienie zasad działania zespołów reagowania na incydenty komputerowe (Computer Emergency Response Teams), oraz centrów operacji bezpieczeństwa (SOC). Zapoznanie się z założeniami systemów SIEM (Security Information and Event Management). W ramach ćwiczeń student opracuje własną koncepcję SOC z uwzględnieniem warunków rzeczywistych.

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.
ma wiedzę na temat zasad etycznych związanych z działaniami niezbędnymi do zapewniania bezpieczeństwa systemów teleinformatycznych.

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 wykorzystać metody eksperymentalne do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych w obszarze bezpieczeństwa teleinformatycznego.
potrafi ocenić przydatność i możliwość wykorzystania nowych rozwiązań sprzętowych i programowych służących do rozwiązywania zadań inżynierskich, polegających na budowie bezpiecznych systemów przesyłania danych.
potrafi współdziałać w zespole odpowiedzialnym za zapewnienie bezpieczeństwa systemom teleinformatycznym.
potrafi określić kierunki dalszego uczenia się w celu sprostania wyzwaniom stawianym osobom odpowiedzialnym za bezpieczństwo systemów teleinformatycznych.

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 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

- Podstawy cyberbezpieczeństwa.
- Rodzaje ataków i podatności.
- Podstawy przetwarzania w chmurze i bezpieczeństwa w chmurze;
zagrożenia bezpieczeństwa w chmurze).
- Podstawy bezpieczeństwa IoT.
- Podstawy kontroli dostępu.
- Przegląd PKI, certyfikatów głównych i tożsamości, IPSec, wirtualnych sieci prywatnych.
- Podstawy zarządzania operacjami bezpieczeństwa.
- Podstawy analizy włamań
- Wprowadzenie do kryminalistyki cyfrowej.
- Telemetria i analiza sieci i urządzeń końcowych.
- Analiza danych i zdarzeń.
- Zadania centrów operacji bezpieczeństwa.
- Modele cyberbezpieczeństwa i polowanie na zagrożenia.
- Podstawy bezpieczeństwa AI.
- Podstawy bezpieczeństwa i etyki.

Tematyka zajęć

Tematyka wykładów:
- Przegląd protokołów TCP/IP.
- Podstawy cyberbezpieczeństwa (NIST; zagrożenia, podatności, luki w zabezpieczeniach; IDS, IPS).
- Rodzaje ataków i podatności.
- Podstawy przetwarzania w chmurze i bezpieczeństwa w chmurze (modele chmury; DevOps, CI/CD;
zagrożenia bezpieczeństwa w chmurze).
- Podstawy bezpieczeństwa IoT.
- Podstawy kontroli dostępu (AAA, procesy, obowiązki, mechanizmy; implementacje kontroli tożsamości i kontroli dostępu).
- Przegląd PKI, certyfikatów głównych i tożsamości, IPSec, wirtualnych sieci prywatnych.
- Podstawy zarządzania operacjami bezpieczeństwa (zarządzanie tożsamością i dostępem; zarządzanie zdarzeniami i dziennikami; zarządzanie aktywami i zmianami; zarządzanie podatnościami; CSIRT, SOC, SIEM, SOAR).
- Podstawy analizy włamań (proces reagowania na incydenty; zespół reagowania na incydenty; artefakty).
- Wprowadzenie do kryminalistyki cyfrowej.
- Telemetria i analiza sieci i urządzeń końcowych (dzienniki, przechwytywanie pakietów, profilowanie sieci; profilowanie hostów).
- Analiza danych i zdarzeń (normalizacja danych; różne rodzaje analizy).
- Zadania centrów operacji bezpieczeństwa.
- Modele cyberbezpieczeństwa i polowanie na zagrożenia (modelowanie zagrożeń, np. STRIDE, PASTA, CVSS itp.;).
- Podstawy bezpieczeństwa AI.
- Podstawy bezpieczeństwa internetowego.
- Podstawy bezpieczeństwa i etyki.
Tematyka laboratoriów:
Zgodna z treściami 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. Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021
2. 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	125	5,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	2,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	65	2,50