KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Cyberbezpieczeństwo [S2IBiJ1-BiZK>CYB]

Przedmiot

Kierunek studiów
Inżynieria bezpieczeństwa i jakości

Rok/Semestr
1/2

Studia w zakresie (specjalność)
Bezpieczeństwo i zarządzanie kryzysowe

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
0

Laboratorium
0

Inne (np. online)
0

Ćwiczenia
30

Projekty/seminaria
0

Liczba punktów ECTS

2,00

Koordynatorzy

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

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z podstaw programowania, systemów operacyjnych i sieci komputerowych. 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. Zapoznanie studentów z zaawansowanymi metodami, technikami i narzędziami stosowanymi przy rozwiązywaniu złożonych zadań w obszarze projektowania i utrzymania systemów sieciowych odpowiedzialnych za bezpieczeństwo przesyłanych danych. Rozwijanie u studentów umiejętności rozwiązywania problemów z cyberbezpieczeństwem pojawiających się we współczesnych sieciach teleinformatycznych.

Przedmiotowe efekty uczenia się

Wiedza:
1. Student zna w pogłębionym stopniu tendencje rozwojowe oraz dobre praktyki dotyczące zarządzania bezpieczeństwem w szczególności bezpieczeństwem danych w ogranizacjach w ujęciu lokalnym i

globalnym [K2_W04].
2. Student zna w pogłębionym stopniu zasady przepływu informacji, komunikacji, ochrony danych, uwarunkowań prawnych i regulacyjnych wpływających na cyberbezpieczeństwo charakterystyczne dla obszaru zarządzania bezpieczeństwem organizacji [K2_W14].

Umiejętności:
1. Student potrafi stosować metody i narzędzia rozwiązywania złożonych i nietypowych problemów oraz zaawansowane techniki informacyno-komunikacyjne charakterystyczne dla środowiska zawodowego związanego z zarządzaniem cyberbezpieczeństwem w organizacjach [K2_U02].
2. Student potrafi dobrać i zastosować narzędzia komputerowego wspomagania rozwiązywania problemów charakterystycznych dla zarządzania sferą cyberbezpieczeństwa w ogranizacjach [K2_U08].

Kompetencje społeczne:
1. Student jest krytyczny wobec swojej wiedzy, jest gotów do zasięgania opinii ekspertów podczas rozwiązywania problemów poznawczych i praktycznych, ciągłego dokształcania z branży IT, w szczególności związanej z cyberbezpieczeństwem w obszarze zarządzania bezpieczeństwem w organizacjach [K2_K01].
2. Student prawidłowo identyfikuje i rozstrzyga dylematy związane z szeroko pojętym bezpieczeństwem, szczególnie w obszarze danych, rozumie konieczność uświadamiania społeczeństwa w zakresie potrzeby kształtowania bezpieczeństwa w różnych obszarach funkcjonowania organizacji [K2_K02].

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Umiejętności nabyte w ramach zajęć ćwiczeniowych weryfikowane są na bieżąco. Na każdych zajęciach ćwiczeniowych oceniana jest poprawność wykonania ćwiczeń w skali od 0 do 100% (ocena formująca). Ocena końcowa określana jest na podstawie średniej punktów uzyskanych z poszczególnych zajęć, wymagane jest uzyskanie 51% punktów do zaliczenia (ocena podsumowująca). Skala ocen jest zgodna z zasadmi opisanymi w Regulamienie Studiów.

Treści programowe

Podstawowe zagadnienia dotyczące Cyberbezpieczeństwa.

Tematyka zajęć

Przegląd protokołów TCP/IP. Podstawy cyberbezpieczeństwa (NIST; zagrożenia, podatności, luki w zabezpieczeniach; IDS, IPS). Rodzaje ataków i podatności. Przygotowanie testów penetracyjnych. Podstawy bezpieczeństwa IoT. Podstawy kontroli dostępu (AAA, uwierzytelnienie użytkowników, listy kontroli dostępu). IPSec, wirtualne sieci prywatne. Zabezpieczanie warstwy 2 (sieci VLAN; zagrożenia; IEEE 802.1AE/MACsec+). Technologie zapór sieciowych. Rozwiązania i procedury stosowane w przedsiębiorstwach w ochronie przed cyberatakiem.

Metody dydaktyczne

Ćwiczenia: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy, ćwiczenia praktyczne w grupach, z wykorzystaniem urządzeń sieciowych.

Literatura

Podstawowa:
1. Santos, O., Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021
2. Migga Kizza, J., : 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. Woland A., Santuka, V., Harris, M., Sanbower J.,: 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. Barker, E., 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. Stewart J.M.,: Network Security, Firewalls And VPNs; Jones & Bartlett Learning Information Systems Security & Ass, 2nd Edition, 2013.
5. Blokdyk, G.,: IPsec VPN A Complete Guide; 5STARCooks; 2019.
6. Majchrzak J., Goliński M., Matura W., The concept of the qualitology and grey system theory application in marketing information quality cognition and assessment, Central European Journal of Operations Research, 2020, Vol. 28, No. 2.
7. Głąbowski M., Sobieraj M., Simulation Studies of Link Group in Elastic Optical Networks Used in Internet of Things Solutions, Transport and Telecommunication - 2023, vol. 24, no. 3, p. 278-287.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	60	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	30	1,00