KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Wstęp do cyberbezpieczeństwa [S1Cybez1>WdC]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
1/1

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
30

Laboratorium
0

Inne
0

Ćwiczenia
0

Projekty/seminaria
30

Liczba punktów ECTS

4,00

Koordynatorzy

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

dr Renata Dąbrowska
renata.dabrowska@put.poznan.pl

Wykładowcy

Wymagania wstępne

brak

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z podstawami cyberbezpieczeństwa i ochrony danych, obejmując zagadnienia bezpieczeństwa teleinformatycznego, szacowania ryzyka oraz zarządzania bezpieczeństwem. Zajęcia łączą teorię z praktyką poprzez grupowe projekty (analiza ryzyka, tworzenie i wdrażanie systemów ochrony). Przedmiot przedstawia studentom międzynarodowy kontekst cyberbezpieczeństwa (UE, NATO), skupiając się na działaniach SOC, CSIRT, SIEM i reakcjach na incydenty.

Przedmiotowe efekty uczenia się

Wiedza:
• Student zna kluczowe zagadnienia i standardy z zakresu cyberbezpieczeństwa.

• Ma wiedzę o metodach szacowania ryzyka i ochrony danych w systemach IT.
• Rozumie zasady działania SOC, CSIRT i systemów SIEM.

Umiejętności:
• Potrafi analizować zagrożenia i podatności oraz zaproponować środki zaradcze.
• Umie pozyskiwać informacje o podatnościach i zagrożeniach.
• Efektywnie współpracuje w zespole projektowym.

Kompetencje społeczne:
• Rozumie znaczenie ciągłego doskonalenia wiedzy w dynamicznie zmieniającym się środowisku.
• Jest świadomy odpowiedzialności za decyzje w projektach dotyczących bezpieczeństwa IT.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

1. Wiedza: egzamin pisemny z pytaniami otwartymi.
2. Umiejętności: bieżąca ocena realizacji projektów grupowych oraz końcowa prezentacja wyników.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 50% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Przedmiot „Wstęp do cyberbezpieczeństwa” zapoznaje studentów z kluczowymi - dla bezpieczeństwa teleinformatycznego - pojęciami, zagrożeniami i technikami ochrony danych oraz systemami w cyberprzestrzeni. Obejmuje podstawowe aspekty bezpieczeństwa teleinformatycznego, metody szacowania ryzyka oraz zarządzanie bezpieczeństwem organizacji. Kurs uwzględnia także międzynarodowy kontekst cyberbezpieczeństwa, w tym działania UE, NATO i innych organizacji międzynarodowych. Przedmiot rozwija zarówno umiejętności analityczne, jak i praktyczne poprzez realizację projektów grupowych. Jest to pierwszy kurs z zakresu cyberbezpieczeństwa na studiach inżynierskich i nie wymaga wcześniejszej wiedzy w tej dziedzinie.

Tematyka zajęć

I. Wprowadzenie do cyberbezpieczeństwa (12x45 min)
1. Podstawowe pojęcia i definicje
o Cyberprzestrzeń i jej znaczenie w nowoczesnym społeczeństwie.
o Terminologia: podatność, zagrożenie, atak, ryzyko.
o Sześcian bezpieczeństwa: kluczowe cele cyberbezpieczeństwa, stany danych, obszary działań obronnych.
o Modele, standardy, zalecenia (np. NIST, ISO 27000).
o Bazy podatności i ich rola (np. CVE).
2. Rodzaje podatności i ataków
o Typy podatności i złośliwego oprogramowania.
o Klasyfikacja ataków (np. DDoS, phishing, ransomware).
o Specyfika bezpieczeństwa w systemach chmurowych i IoT.
3. Podstawowe strategie ochrony
o Zarządzanie ryzykiem i polityki bezpieczeństwa.
o Modele i mechanizmy sterowania dostępem (IAAA).
II. Cyberbezpieczeństwo w wymiarze międzynarodowym (6x45 min)
1. Inicjatywy międzynarodowe
o Działania UE: ENISA, EUROPOL, jednolity rynek cyfrowy.
o Rola NATO i współpraca z UE w zakresie cyberobrony.
o Organizacje międzynarodowe: ONZ, OECD, G7, G20.
2. Zespoły reagowania na incydenty komputerowe
o Zadania i struktura zespołów reagowania.
o Przykłady realnych incydentów i metod reagowania.

III. Cyberhigiena i narzędzia ochrony (12x45 min)
1. Podstawy działania sieci teleinformatycznych w kontekście bezpieczeństwa
2. Zasady bezpiecznego korzystania z urządzeń i sieci
o Zarządzanie hasłami, uwierzytelnianie dwuskładnikowe (2FA).
o Certyfikaty cyfrowe i infrastruktura klucza publicznego (PKI).
IV. Aspekty praktyczne cyberbezpieczeństwa
1. Analiza przypadków
o Studium przypadków ataków cybernetycznych i ich skutków.
o Analiza reakcji organizacji na incydenty bezpieczeństwa.
2. Projekt grupowy
o Opracowanie i wdrożenie systemu ochrony danych w środowisku testowym.
o Analiza ryzyka, polityka bezpieczeństwa, prezentacja wyników.

Metody dydaktyczne

• Wykłady online z wykorzystaniem prezentacji multimedialnych i analizy przypadków.
• Projekty grupowe realizowane w laboratorium.

Literatura

Podstawowa:
1. "Cybersecurity Essentials" by Charles J. Brooks, Christopher Grow, Philip A. Craig, Jr., and Donald Short. Published by John Wiley & Sons in 2018. ISBN: 978-1-119-36239-5.
2. "Network Security Essentials: Applications and Standards" by William Stallings. Published by Pearson in 2017. ISBN: 978-0-134-52733-8.

Uzupełniająca:
1. Dokumenty ENISA, NIST i NATO dotyczące cyberbezpieczeństwa.
2. Materiały własne przygotowane przez prowadzących.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	120	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	60	2,00