POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Wprowadzenie do cyberbezpieczeństwa, PG_00053947		
Kierunek studiów	Informatyka		
Data rozpoczęcia studiów	październik 2022 r.	Rok akademicki realizacji przedmiotu	2023/2024
Poziom kształcenia	I stopnia - inżynierskie	Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	2	Język wykładowy	polski
Semestr studiów	4	Liczba punktów ECTS	2.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Teleinformatyki		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Wojciech Gumiński	
	Prowadzący zajęcia z przedmiotu	dr inż. Wojciech Gumiński dr inż. Michał Hoeft dr inż. Krzysztof Gierłowski Zenon Werbowy	

Formy zajęć i metody nauczania

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	15.0	0.0	0.0	15.0	0.0	30

W tym liczba godzin zajęć na odległość: 0.0

Aktywność studenta i liczba godzin pracy

Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów	Udział w konsultacjach	Praca własna studenta	RAZEM
Liczba godzin pracy studenta	30	2.0	18.0	50

Cel przedmiotu

Celem przedmiotu jest nauczenie studenta podstaw związanych z cyberbezpieczeństwem. W ramach przedmiotu studenci poznają wybrane zagrożenia dla bezpieczeństwa. Prezentowany jest zbiór funkcji bezpieczeństwa, m. in.: poufność, integralność i dostępność wraz z mechanizmami pozwalającymi na ich realizację. W ramach zajęć praktycznych studenci nabywają umiejętności operowania materiałem kryptograficznym w podstawowych, popularnych scenariuszach użycia.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K6_W43] zna i rozumie w zaawansowanym stopniu standardy i metody administrowania systemami informatycznymi, monitorowania zachodzących w nich procesów oraz uodporniania ich na niepożądane zjawiska i działania	Student zna praktyczne rozwiązania pozwalające osiągnąć określone funkcje bezpieczeństwa.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym
[K6_U03] potrafi zaprojektować, zgodnie z zadaną specyfikacją, oraz wykonać typowe dla kierunku studiów proste urządzenie, obiekt, system lub zrealizować proces, używając odpowiednio dobranych metod, technik, narzędzi i materiałów, korzystając ze standardów i norm inżynierskich, stosując właściwe dla kierunków studiów technologie i wykorzystując doświadczenie zdobyte w środowisku zajmującym się zawodowo działalnością inżynierską	Student potrafi praktycznie wykorzystać poznane rozwiązania bezpieczeństwa. W ramach prac projektowych integruje/ implementuje i prezentuje ich zastosowanie w określonym scenariuszu użycia.	[SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania [SU1] Ocena realizacji zadania

<table>
<tr><td>Treści przedmiotu</td><td colspan="3">Podstawowe pojęcia związane z bezpieczeństwem systemów IT, funkcje bezpieczeństwa: integralność, poufność, uwierzytelnianie. Rodzaje zagrożeń i ataków: poznanie treści, modyfikacja treści, podszywanie, ataki celowane i niecelowane, malware, sieci botnet. Wprowadzenie do kryptografii: k. symetryczna i asymetryczna, klucze jednorazowe, szyfry blokowe i strumieniowe, integralność danych. Kryptografia klucza publicznego i PKI. Bezpieczeństwo w zastosowaniach: zastosowania PKI, obsługa rozwiązań wykorzystujących certyfikaty. Podstawy zarządzania bezpieczeństwem: polityka bezpieczeństwa, dobre praktyki bezpieczeństwa, dobre praktyki rozwijania bezpiecznego kodu.</td></tr>
<tr><td>Wymagania wstępne i dodatkowe</td><td colspan="3">Znajomość konfiguracji i obsługi popularnych systemów operacyjnych</td></tr>
<tr><td>Sposoby i kryteria oceniania osiąganych efektów uczenia się</td><td colspan="3"><table>
<tr><th>Sposób oceniania (składowe)</th><th>Próg zaliczeniowy</th><th>Składowa oceny końcowej</th></tr>
<tr><td>Ocena z projektu</td><td>50.0%</td><td>50.0%</td></tr>
<tr><td>Ocena z części wykładowej</td><td>50.0%</td><td>50.0%</td></tr>
</table></td></tr>
<tr><td rowspan="2">Zalecana lista lektur</td><td>Podstawowa lista lektur</td><td colspan="2">Materiały i prezentacje do zajęć</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td colspan="2">Schneier B.: Kryptografia dla praktyków

Bilski T., Pankowski T., Stokłosa J.: Bezpieczeństwo danych w systemach informatycznych

Stallings W.: Cryptography and Network Security

Gollmann D.: Computer security</td></tr>
<tr><td></td><td>Adresy eZasobów</td><td colspan="2">Adresy na platformie eNauczanie:
Wprowadzenie do cyberbezpieczeństwa 2024 - Moodle ID: 33397
https://enauczanie.pg.edu.pl/moodle/course/view.php?id=33397</td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td colspan="3">1. Implementacja wybranych algorytmów szyfrowania symetrycznego przy użyciu dostępnych bibliotek
2. Wykorzystanie infrastruktury klucza publicznego na potrzeby wzajemnego uwierzytelniania klient-serwer WWW
3. Wykorzystanie infrastruktury klucza publicznego na potrzeby podpisywania i szyfrowania poczty e-mail</td></tr>
<tr><td>Praktyki zawodowe w ramach przedmiotu</td><td colspan="3">Nie dotyczy</td></tr>
</table>