POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Kryptografia w cyberbezpieczeństwie, PG_00048039		
Kierunek studiów	Informatyka		
Data rozpoczęcia studiów	luty 2023 r.	Rok akademicki realizacji przedmiotu	2022/2023
Poziom kształcenia	II stopnia	Grupa zajęć	Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	1	Język wykładowy	polski
Semestr studiów	1	Liczba punktów ECTS	3.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Teleinformatyki		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr hab. inż. Jerzy Konorski	
	Prowadzący zajęcia z przedmiotu	dr hab. inż. Jerzy Konorski	

Formy zajęć i metody nauczania

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	30.0	0.0	0.0	15.0	0.0	45
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	45	6.0	24.0	75

Cel przedmiotu

Celem przedmiotu jest przekazanie wiedzy i umiejętności związanych z podstawowymi mechanizmami kryptograficznymi. W ramach przedmiotu Studenci poznają podstawy zagrożeń i zabezpieczeń, kryptografii, protokoły kryptograficzne, implementacje i zastosowania kryptografii asymetrycznej - m. in. podpis cyfrowy, znakowanie czasem, PKI. Poruszana jest również tematyka powiązana bezpośrednio z kryptografią, m. in. prywatność i anonimowość, ochrona baz danych, czy elementy kryptografii kwantowej i postkwantowej. Wybrane zagadnienia Studenci mają możliwość poznać praktycznie w ramach zajęć projektowych.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K7_U06] potrafi analizować działanie elementów, układów i systemów związanych z kierunkiem studiów oraz mierzyć ich parametry i badać charakterystyki techniczne, interpretować uzyskane wyniki i wyciągać wnioski	Student w ramach prac projektowych integruje/ implementuje i prezentuje zastosowanie rozwiązania bezpieczeństwa w określonym scenariuszu użycia.	[SU1] Ocena realizacji zadania
[K7_U42] potrafi rozwiązywać problemy inżynierskie i badawcze w zakresie projektowania, oceny i utrzymania systemów i aplikacji informacyjnych z wykorzystaniem metod eksperymentalnych i technik zarządzania	Student potrafi praktycznie wykorzystać poznane rozwiązania bezpieczeństwa.	[SU4] Ocena umiejętności korzystania z metod i narzędzi
[K7_W03] zna i rozumie w pogłębionym stopniu budowę i zasady działania komponentów i systemów związanych z kierunkiem studiów, w tym teorie, metody i złożone zależności między nimi oraz wybrane zagadnienia szczegółowe – właściwe dla programu kształcenia	Student zna praktyczne rozwiązania pozwalające osiągnąć określone funkcje bezpieczeństwa.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym

<table>
<tr><td>Treści przedmiotu</td><td colspan="3">Podstawowe pojęcia związane z bezpieczeństwem systemów IT. Metody uwierzytelniania. Wprowadzenie do kryptografii. Kryptografia klucza publicznego i PKI. Usługi kryptograficzne. Protokoły kryptograficzne. Prywatność i anonimowość. Kryptograficzna ochrona baz danych. Elementy protokołów kryptografii kwantowej i postkwantowej.</td></tr>
<tr><td>Wymagania wstępne i dodatkowe</td><td colspan="3">Znajomość podstaw programowania w języku wysokiego poziomu</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>Projekt</td><td>50.0%</td><td>40.0%</td></tr>
<tr><td>Egzamin</td><td>50.0%</td><td>30.0%</td></tr>
<tr><td>Kolokwium</td><td>50.0%</td><td>30.0%</td></tr>
</table></td></tr>
<tr><td rowspan="3">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>Adresy eZasobów</td><td colspan="2">Adresy na platformie eNauczanie:</td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td colspan="3"></td></tr>
<tr><td>Praktyki zawodowe w ramach przedmiotu</td><td colspan="3">Nie dotyczy</td></tr>
</table>