



Karta przedmiotu

Nazwa i kod przedmiotu	Wprowadzenie do cyberbezpieczeństwa, PG_00053947						
Kierunek studiów	Informatyka						
Data rozpoczęcia studiów	październik 2021 r.	Rok akademicki realizacji przedmiotu			2022/2023		
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 ogólnokademicki		
Forma studiów	stacjonarne	Sposób realizacji			na uczelni		
Rok studiów	2	Język wykładowy			polski		
Semestr studiów	4	Liczba punktów ECTS			2.0		
Profil kształcenia	ogólnokademicki	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. Krzysztof Gierłowski dr inż. Wojciech Gumiński dr inż. Michał Hoeff 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 nauczanie 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_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.			[SU1] Ocena realizacji zadania [SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania	
[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		

Treści przedmiotu	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.		
Wymagania wstępne i dodatkowe	Znajomość konfiguracji i obsługi popularnych systemów operacyjnych		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Ocena z części wykładowej	50.0%	50.0%
	Ocena z projektu	50.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	Materiały i prezentacje do zajęć	
	Uzupełniająca lista lektur	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	
	Adresy eZasobów	Adresy na platformie eNauczanie:	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	<ol style="list-style-type: none"> 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 		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		