



Karta przedmiotu

Nazwa i kod przedmiotu	Podstawy cyberbezpieczeństwa, PG_00068775						
Kierunek studiów	Inżynieria biomedyczna, Inżynieria biomedyczna, Inżynieria biomedyczna						
Data rozpoczęcia studiów	luty 2027 r.	Rok akademicki realizacji przedmiotu			2027/2028		
Poziom kształcenia	II stopnia	Grupa zajęć			Grupa zajęć fakultatywnych Grupa zajęć specjalnościowych 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	2	Liczba punktów ECTS			2.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			egzamin		
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> 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					
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	15.0	0.0	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		3.0		17.0	50
Cel przedmiotu	Głównym celem przedmiotu Podstawy cyberbezpieczeństwa jest przekazanie wiedzy i umiejętności z zakresu ochrony systemów, sieci i danych przed zagrożeniami w cyberprzestrzeni. Przedmiot ma pomóc w zrozumieniu zagrożeń, zasad bezpieczeństwa oraz sposobów zapobiegania atakom cyfrowym.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K7_W04] zna i rozumie w pogłębionym stopniu zasady, metody i techniki programowania oraz zasady tworzenia oprogramowania komputerów albo programowania urządzeń lub sterowników wykorzystujących mikroprocesory albo inne elementy lub układy programowalne, specyficznych dla kierunku studiów, a także organizację pracy systemów wykorzystujących komputery lub te urządzenia	Student wymienia i opisuje atrybuty bezpieczeństwa. Student opisuje różnice między algorytmami kryptografii symetrycznej i asymetrycznej oraz podaje przykłady ich zastosowań.	[SW1] Ocena wiedzy faktograficznej
	[K7_U04] potrafi wykorzystywać posiadaną wiedzę z zakresu metod i technik programowania oraz dobrać i zastosować właściwe metody i narzędzia programistyczne w tworzeniu oprogramowania komputerów albo programowania urządzeń lub sterowników wykorzystujących mikroprocesory albo elementy lub układy programowalne, charakterystycznych dla danego kierunku studiów, dokonując oceny i krytycznej analizy wykonanego oprogramowania, a także syntezy i twórczej interpretacji prezentowanych za jego pomocą informacji	Student potrafi praktycznie wdrożyć poznane rozwiązania bezpieczeństwa w określonych scenariuszach użycia.	[SU1] Ocena realizacji zadania [SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania
Treści przedmiotu	<p>Treści przedmiotu - wykład</p> <p>Wykłady:</p> <ol style="list-style-type: none"> 1. Wprowadzenie do cyberbezpieczeństwa 2. Atrybuty bezpieczeństwa 3. Podstawowe typy zagrożeń 4. Aspekty prawne cyberbezpieczeństwa 5. Podstawy kryptografii 6. Algorytmy kryptograficzne symetryczne i asymetryczne 7. Praktyczne zastosowania metod kryptograficznych 8. Szyfrowanie dokumentów i podpisy cyfrowe 9. Infrastruktura klucza publicznego PKI i jej zastosowania 10. Bezpieczeństwo systemów informatycznych 11. Uwierzytelnianie i autoryzacja 12. Bezpieczeństwo dostępu zdalnego 13. Niezawodność i ciągłość działania 14. Monitorowanie systemów 15. Analiza przykładowych przypadków użycia <p>Laboratoria:</p> <ol style="list-style-type: none"> 1. Kucze, certyfikaty i PKI 2. Szyfrowanie, podpisy cyfrowe i PGP 3. Uwierzytelnianie i szyfrowanie w aplikacjach internetowych 4. Zapora sieciowa 5. Systemy IDS/IPS 6. Bezpieczny dostęp zdalny VPN 7. Monitorowanie systemów i analiza dzienników zdarzeń 		
Wymagania wstępne i dodatkowe			
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Ocena z realizacji laboratoriów	50.0%	50.0%
	Egzamin	50.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	<p>Cybersecurity Essentials: Practical Tools for Today's Digital Defenders; Cochran Kodi A; 2024; Berkeley, CA: Apress L. P.</p> <p>The Cyber Security Handbook Prepare for, respond to and recover from cyber attacks; Calder Alan, Perring Stephen; 2020; Ely: IT Governance Publishing</p> <p>Cybersecurity for Dummies; Steinberg Joseph; 2025; Newark: John Wiley & Sons, Incorporated</p> <p>Cyberbezpieczeństwo dla bystrzaków; Joseph Steinberg ; przekład: Grzegorz Werner; 2023; Gliwice : Helion</p> <p>Cyberbezpieczeństwo w Polsce i na świecie; Katarzyna Chałubińska-Jentkiewicz, Agnieszka Brzostek, Waldemar Kitler, Katarzyna Badźmirowska-Masłowska; 2024; Towarzystwo Wiedzy Obronnej</p>	

	Uzupełniająca lista lektur	Cybersecurity for eHealth: A Simplified Guide to Practical Cybersecurity for Non-Technical Healthcare Stakeholders & Practitioners; Ogu, Emmanuel C; 2021; United States: CRC Press Cyberbezpieczeństwo w placówce medycznej; Piotr Glen, Michał Grabiec, Piotr Janiszewski, Agnieszka Kręcisz-Sarna, Przemysław Kucharzewski, Maciej Lipka, Michał Nosowski, Marzena Pytlarz-Pietraszko, Marcin Sarna, Jowita Sobczak; 2022; Warszawa: Wiedza i Praktyka sp. z o.o. Boardroom Cybersecurity: A Director's Guide to Mastering Cybersecurity Fundamentals; Weis, Dan; 2024; Berkeley, CA: Apress L. P.
	Adresy eZasobów	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	generowanie i weryfikowanie certyfikatów; tworzenie i weryfikacja podpisów cyfrowych; konfiguracja zapory sieciowej oraz systemów IDS/IPS; szyfrowanie dokumentów; praktyczne wykorzystanie infrastruktury klucza publicznego PKI.	
Zajęcia praktyczne w ramach przedmiotu	Nie dotyczy	

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.