POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Zabezpieczenie systemów i usług sieciowych, PG_00049302		
Kierunek studiów	Inżynieria biomedyczna, Inżynieria biomedyczna, Inżynieria biomedyczna		
Data rozpoczęcia studiów	październik 2020 r.	Rok akademicki realizacji przedmiotu	2023/2024
Poziom kształcenia	I stopnia - inżynierskie	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	4	Język wykładowy	polski
Semestr studiów	7	Liczba punktów ECTS	3.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	egzamin
Jednostka prowadząca	Wydział Elektroniki, Telekomunikacji i Informatyki		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Adam Bujnowski	
	Prowadzący zajęcia z przedmiotu	dr inż. Adam Bujnowski mgr inż. Michał Gryko	

Formy zajęć i metody nauczania	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	42.0	75

Cel przedmiotu	Celem przedmiotu jest zapoznanie studentów z typowymi problemami i zagadnieniami związanymi z zabezpieczeniami systemów informacyjnych. Omówione zostaną przyczyny problemów z bezpieczeństwem, podstawowe techniki zapobiegania tym problemom oraz metody analizy problemów.

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K6_U02] potrafi innowacyjnie wykonywać zadania związane z kierunkiem studiów oraz rozwiązywać złożone i nietypowe problemy, wykorzystując wiedzę z fizyki, w zmiennych i nie w pełni przewidywalnych warunkach	Student dokonuje analizy zabezpieczeń powierzonego systemu	[SU1] Ocena realizacji zadania
	[K6_U09] potrafi dokonać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych związanych z kierunkiem studiów i ocenić te rozwiązania, a także wykorzystać zdobyte w środowisku zajmującym się zawodowo działalnością inżynierską doświadczenie związane z utrzymaniem urządzeń, obiektów i systemów technicznych typowych dla kierunku studiów	Student zna podstawowe źródła aktualnych informacji z zakresu polityki bezpieczeństwa i umie z nich korzystać	[SU2] Ocena umiejętności analizy informacji
	[K6_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	Student potrafi dokonać automatyzacji analizy systemu na poziomie logów systemowych	[SU4] Ocena umiejętności korzystania z metod i narzędzi
	[K6_W08] zna i rozumie fundamentalne dylematy współczesnej cywilizacji oraz podstawowe ekonomiczne, prawne i inne uwarunkowania różnych rodzajów działań związanych z kierunkiem studiów, w tym podstawowe pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego	Student potrafi oszacować koszt prowadzonej polityki bezpieczeństwa	[SU2] Ocena umiejętności analizy informacji
	[K6_U07] potrafi wykorzystać metody wspomagania procesów i funkcji, specyficzne dla kierunków studiów	Student potrafi stworzyć reguły dostępu do wybranych usług systemowych i je zaaplikować	[SU4] Ocena umiejętności korzystania z metod i narzędzi

Treści przedmiotu	Pojęcia podstawowe, niezawodność sprzętu komputerowego, miary, metody zapewniania, redundancja, skalowalnosć Zabezpieczenia fizycznego dostępu do serwera Zapewnienie warunków klimatycznych i mediów konsumpcyjnych dla serwera - pojęcie serwerowni i infrastruktura Podstawy kryptografii i kryptoanalizy Przegląd technologii kryptograficznych wykorzystywanych w technologiach teleinformatycznych Zabezpieczanie systemu operacyjnego Administracja i zabezpieczenia ferm komputerowych Metody analizy bezpieczeństwa systemu - logi zdarzeń i analiza powłamaniowa Wirusy komputerowe - zasada działania i techniki dezaktywacji Zapory sieciowe i kontrola ruchu zabezpieczenia serwerów bazodanowych Zabezpieczenia usług informacyjnych Zabezpieczenia serwisów plikowych Przegląd podstawowych technika hackerskich - metody przeciwdziałania Audyt bezpieczeństwa systemu - podsumowanie
Wymagania wstępne i dodatkowe	

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
laboratorium	50.0%	50.0%
Kolokwium końcowe	50.0%	50.0%

Zalecana lista lektur

Podstawowa lista lektur	Praca zbiorowa, Vademecum teleinformatyka T1 , 2 i ch , IDG Wainwright , Apache 2.0 dla zaawansowanych, Helion/Wrox 2003/06 Polaczek, Audyt bezpieczeństwa w praktyce, Helion 2006 Kifner, Polityka bezpieczeństwa i ochrony informacji, Helion
Uzupełniająca lista lektur	Greg Hoglund, Jamie Butler, Rootkity . sabotowanie jądra systemu Windows, Helion 2006
Adresy eZasobów	Adresy na platformie eNauczanie:

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy