



Karta przedmiotu

Nazwa i kod przedmiotu	Zarządzanie bezpieczeństwem sieci, PG_00053895						
Kierunek studiów	Informatyka						
Data rozpoczęcia studiów	październik 2021 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	3	Język wykładowy			polski		
Semestr studiów	6	Liczba punktów ECTS			3.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			egzamin		
Jednostka prowadząca	Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Teleinformatyki						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Krzysztof Gierłowski					
	Prowadzący zajęcia z przedmiotu	dr inż. Krzysztof Gierłowski					
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	30.0	0.0	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		1.0		29.0	75
Cel przedmiotu	Celem przedmiotu jest zapoznanie studentów od strony teoretycznej i praktycznej z mechanizmami bezpieczeństwa, zagrożeniami, jakie są z nimi związane, rozwiązaniami jakie można zastosować w celu podniesienia bezpieczeństwa, a także wytworzenie podejścia do bezpieczeństwa rozumianego jako proces ciągle - zarządzania bezpieczeństwem.						

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 posiada znajomość aktualnych rozwiązań bezpieczeństwa systemów IT, potrafi dobierać je zależnie od identyfikowanych zagrożeń.	[SW1] Ocena wiedzy faktograficznej
	[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 potrafi skonfigurować poznane mechanizmy bezpieczeństwa stosowane w sieciach komputerowych.	[SU1] Ocena realizacji zadania
	[K6_W03] zna i rozumie w zaawansowanym stopniu budowę i zasady działania komponentów i systemów związanych z kierunkiem studiów, w tym teorii, metody i złożone zależności między nimi oraz wybrane zagadnienia szczegółowe – właściwe dla programu kształcenia	Student zna ograniczenia popularnych mechanizmów sieciowych pod względem bezpieczeństwa, potrafi zaproponować sposoby zmniejszenia zagrożenia.	[SW1] Ocena wiedzy faktograficznej
[K6_U42] potrafi wykorzystywać narzędzia i metody projektowania, optymalizacji, monitorowania, zarządzania, zwiększania niezawodności i ochrony przed zagrożeniami bezpieczeństwa w lokalnych i rozproszonych systemach i aplikacjach informacyjnych	Student posiada znajomość aktualnych rozwiązań bezpieczeństwa systemów IT, potrafi dobierać je zależnie od identyfikowanych zagrożeń.	[SU2] Ocena umiejętności analizy informacji	
Treści przedmiotu	Podstawowe mechanizmy bezpieczeństwa, w szczególności CIA. Klasy zagrożeń bezpieczeństwa systemów sieciowych. Kategorie i techniki ataków. Wymagania dotyczące zarządzania bezpieczeństwem sieci. Systemy kontroli dostępu. Biometria. Metody kryptograficzne, PKI. Rola polityki bezpieczeństwa. Utrzymanie poziomu bezpieczeństwa. Zarządzanie bezpieczeństwem systemów informacyjnych.		
Wymagania wstępne i dodatkowe	Znajomość podstaw funkcjonowania sieci komputerowych		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa ocena końcowej
	laboratorium	50.0%	50.0%
	egzamin pisemny	50.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	<p>Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2007 r.</p> <p>Liderman K. : Podręcznik administratora bezpieczeństwa sieciowego, Mikom, Warszawa 2003 r.</p> <p>Liderman K. : Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa 2008 r.</p> <p>Stokłosa J., Bilski T., Pankowski T.: Bezpieczeństwo danych w systemach informatycznych, PWN, Warszawa 2001 r.</p>	
	Uzupełniająca lista lektur	<p>Denning E.: Wojna informatyczna i bezpieczeństwo informacji, WNT, Warszawa 2002 r.</p> <p>Benjamin H. : Cisco CCIE Security, Mikom, Warszawa 2004 r.</p>	

	Adresy eZasobów	Adresy na platformie eNauczenie: Zarządzanie bezpieczeństwem sieci (2024L) - Moodle ID: 37073 https://enauczenie.pg.edu.pl/moodle/course/view.php?id=37073
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	