POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Cybersecurity of Enterprise Infrastructure, PG_00053095		
Kierunek studiów	Inżynieria danych		
Data rozpoczęcia studiów	październik 2025 r.	Rok akademicki realizacji przedmiotu	2027/2028
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	angielski
Semestr studiów	6	Liczba punktów ECTS	3.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	egzamin
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Zarządzania i Ekonomii -> Katedra Informatyki W Zarządzaniu		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr hab. inż. Rafał Leszczyna	
	Prowadzący zajęcia z przedmiotu	dr hab. inż. Rafał Leszczyna	

Formy zajęć i metody nauczania

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	30.0	0.0	30.0	0.0	0.0	60

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	60	6.0	9.0	75

Cel przedmiotu

Nabycie wiedzy i umiejętności zarządzania infrastrukturą i bezpieczeństwem IT w przedsiębiorstwie

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K6_W04] wykazuje się kreatywnym i przedsiębiorczym działaniem w formułowaniu i realizowaniu innowacyjnych pomysłów	Student wykazuje się kreatywnym i przedsiębiorczym działaniem w analizie oraz szacowaniu ryzyka i kosztów związanych z bezpieczeństwem IT, formułując innowacyjne rozwiązania w zakresie ochrony infrastruktury IT oraz tworzenia dokumentacji bezpieczeństwa, dostosowanych do specyfiki przedsiębiorstwa.	[SW2] Ocena wiedzy zawartej w prezentacji
[K6_U02] przygotowuje i przedstawia w sposób przekonujący profesjonalne prezentacje wyników swoich działań, z ich zaawansowaną interpretacją	Student przygotowuje i przedstawia profesjonalne prezentacje wyników analiz związanych z bezpieczeństwem IT, w tym szacowania ryzyka i kosztów	[SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu [SU2] Ocena umiejętności analizy informacji
[K6_U04] formułuje logiczne rozwiązania złożonych lub nieustrukturyzowanych problemów	Student formułuje logiczne rozwiązania złożonych problemów związanych z bezpieczeństwem IT	[SU4] Ocena umiejętności korzystania z metod i narzędzi [SU2] Ocena umiejętności analizy informacji

Treści przedmiotu	WYKŁAD Wprowadzenie do przedmiotu Infrastruktura IT przedsiębiorstwa Koszt związany z bezpieczeństwem IT Zarządzanie ryzykiem Szacowanie ryzyka Standardy bezpieczeństwa IT Zagrożenia bezpieczeństwa IT Dokumentacja bezpieczeństwa IT w przedsiębiorstwie (m.in. opis infrastruktury IT, opis procedur bezpieczeństwa) Środki ochrony bezpieczeństwa infrastruktury IT LABORATORIUM Analiza infrastruktury IT przedsiębiorstwa Szacowanie ryzyka Szacowanie kosztu związanego z bezpieczeństwem IT Stworzenie dokumentacji bezpieczeństwa infrastruktury IT w przedsiębiorstwie Dobór środków ochrony bezpieczeństwa infrastruktury IT
Wymagania wstępne i dodatkowe	Brak wymagań
Sposoby i kryteria oceniania osiąganych efektów uczenia się	

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
Raporty z pracy w laboratorium	60.0%	60.0%
Egzamin	60.0%	40.0%

Zalecana lista lektur	Podstawowa lista lektur	Ross Anderson, Inżynieria zabezpieczeń, WNT 2005. Adam Gałach, Instrukcja zarządzania bezpieczeństwem systemu Informatycznego, ODDK 2004. Janusz Zawiła-Niedźwiecki, Franciszek Wołowski, Bezpieczeństwo systemów informacyjnych: Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, Edu-Libri, Kraków - Warszawa, 1, 2012. Krzysztof Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN 2009. Tadeusz Kifner, Polityka bezpieczeństwa i ochrony informacji, Helion 1999.
	Uzupełniająca lista lektur	John Viega, Mity bezpieczeństwa IT: czy na pewno nie masz się czego bać?, Helion 2010. Edward Amoroso, Wykrywanie intruzów, RM 1999. Bruce Schneier, Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, WNT 2002. Stuart McClure, Joel Scambray, George Kurtz, Hacking zdemaskowany. Bezpieczeństwo sieci - sekrety i rozwiązania, PWN 2006.
	Adresy eZasobów	Adresy na platformie eNauczanie:
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Przeanalizuj infrastrukturę IT przedsiębiorstwa a następnie przygotuj jej dokumentację. Przeprowadź analizę ryzyka dla analizowanej infrastruktury IT. Zaproponuj środki bezpieczeństwa dla analizowanej infrastruktury IT. Podaj przykłady infrastruktur krytycznych. Przedstaw i omów podstawowe funkcje zapory sieciowej.	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.