POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI, PG_00016968		
Kierunek studiów	Automatyka, robotyka i systemy sterowania		
Data rozpoczęcia studiów	luty 2022 r.	Rok akademicki realizacji przedmiotu	2022/2023
Poziom kształcenia	II stopnia	Grupa zajęć	
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	zaliczenie
Jednostka prowadząca	Wydział Elektrotechniki i Automatyki -> Katedra Automatyki		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Paweł Kowalski	
	Prowadzący zajęcia z przedmiotu	dr inż. Paweł Kowalski	

Formy zajęć i metody nauczania

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	15.0	0.0	0.0	0.0	15.0	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	4.0	16.0	50

Cel przedmiotu

Zapoznanie studentów z zasadami zarządzania bezpieczeństwem informacji i rozwiązaniami ochrony informacji w przemysłowych systemach sterowania i sieciach komputerowych. Powiązania IT (information technology) / OT (operational technology).

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K7_W07] ma wiedzę z zakresu systemów zarządzania bezpieczeństwem informacji, zna metody opracowania zintegrowanych systemów zarządzania	Student ma wiedzę z zakresu systemów zarządzania bezpieczeństwem informacji.	[SW1] Ocena wiedzy faktograficznej
[K7_K05] potrafi myśleć i działać w sposób przedsiębiorczy	Student pracuje w grupie, potrafi myśleć i działać w sposób przedsiębiorczy.	[SK3] Ocena umiejętności organizacji pracy [SK4] Ocena umiejętności komunikacji, w tym poprawności językowej [SK1] Ocena umiejętności pracy w grupie
[K7_U09] potrafi dokonać wstępnej analizy ekonomicznej planowanych zadań z zakresu automatyki i robotyki	Student potrafi dokonać wstępnej analizy ekonomicznej planowanych zadań z zakresu automatyki i robotyki	[SU1] Ocena realizacji zadania [SU2] Ocena umiejętności analizy informacji
[K7_W09] ma wiedzę z zakresu typowych systemów zabezpieczeń w warunkach przemysłowych, zna metody identyfikacji zagrożeń i projektowania systemów zabezpieczeń zgodnie z metodyką bezpieczeństwa funkcjonalnego, ma wiedzę z zakresu bezpieczeństwa informacji	Student potrafi przetestować system informatyczny pod względem bezpieczeństwa.	[SW1] Ocena wiedzy faktograficznej [SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym
[K7_U08] ma przygotowanie niezbędne do pracy w środowisku przemysłowym, prowadzenia badań, stosuje zasady bezpieczeństwa i higieny pracy	Student ma przygotowanie niezbędne do pracy w środowisku przemysłowym, prowadzenia badań, stosuje zasady bezpieczeństwa i higieny pracy.	[SU1] Ocena realizacji zadania [SU4] Ocena umiejętności korzystania z metod i narzędzi

Treści przedmiotu	**WYKŁAD** Podstawowe aspekty bezpieczeństwa informacji: identyfikacja, uwierzytelnienie i autoryzacja, poufność, integralność i dostępność. Zagrożenia: użytkownicy, ataki, złośliwe oprogramowanie, wojna informatyczna. Rodzaje i metody naruszeń bezpieczeństwa systemów komputerowych. Metody i środki ochrony informacji. Metody i systemy kontroli dostępu. Zapory przeciwogniowe. Wykrywanie intruzów. Zjawisko spamu i metody przeciwdziałania. Wirtualne sieci prywatne, architektury i protokoły. Metody i algorytmy kryptograficzne. Podstawowe zasady zarządzania bezpieczeństwem informacji. Identyfikacja zagrożeń oraz analiza i ocena ryzyka. Podstawowe strategie zarządzania bezpieczeństwem informacji. System bezpieczeństwa informacji w firmie i instytucji. Wymagania dotyczące ochrony informacji i zabezpieczeń w nawiązaniu do norm PN-ISO/ISO 17799, ISO/IEC TR 13335 oraz PN-ISO/IEC 27001 i innych norm tej serii. Norma ISO/IEC 15408 i znaczenie wspólnych kryteriów CC. Cykl życia i zarządzanie bezpieczeństwem informacji. Podstawy projektowania systemu zabezpieczeń z uwzględnieniem aspektów technicznych i organizacyjnych. Przykłady rozwiązań. Rola najwyższego kierownictwa. Audyt systemu zarządzania bezpieczeństwem informacji, narzędzia i prezentowanie wniosków. Metody i narzędzia do oceny bezpieczeństwa i ochrony. Zarządzanie jakością i niezawodnością oprogramowania. Bezpieczeństwo i ochrona sieci przewodowych i bezprzewodowych. Bezpieczeństwo przykładowych protokołów, zagrożenia i sposoby przeciwdziałania. Mechanizmy szyfrowania danych oraz uwierzytelnianie. Podpis elektroniczny. Standardy stosowane w sieciach bezprzewodowych oraz mechanizmy bezpieczeństwa. Zintegrowane zarządzanie bezpieczeństwem funkcjonalnym i ochroną informacji w programowalnych przemysłowych systemach sterowania i zabezpieczeń. Bezpieczeństwo i ochrona rozproszonych przemysłowych sieci komputerowych w nawiązaniu do normy IEC 62443.
Wymagania wstępne i dodatkowe	Wiedza dotycząca zastosowania systemów i sieci komputerowych oraz technologii programowalnych w przemyśle. Podstawowa wiedza o identyfikacji zagrożeń, analizy niezawodności i bezpieczeństwa oraz analizy i oceny ryzyka w obiektach i systemach technicznych, w tym infrastruktury krytycznej. Podstawowa wiedza w dziedzinie kryptografii.

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
Referat techniczny	50.0%	30.0%
Kolokwium	50.0%	40.0%
Prezentacja	50.0%	30.0%

Zalecana lista lektur

Podstawowa lista lektur	1. Anderson R.: Inżynieria zabezpieczeń. Wydawnictwo Naukowo Techniczne, Warszawa: 2005. 2. Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. Wydawnictwa Naukowo-Techniczne, Warszawa 2006. 3. Karpiński M. (red.): Bezpieczeństwo informacji. Wydawnictwo PAK, Warszawa 2012. 4. Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych. Wydawnictwo Naukowe PWN, Warszawa 2008. 5. Liderman K.: Bezpieczeństwo informacyjne. Wydawnictwo Naukowe PWN, Warszawa 2012. 6. Schneier B.: Kryptografia dla praktyków. Wiley, PWN, 2002. 7. Wesołowski J., Namieśnik J.: Bezpieczeństwo i ochrona informacji. Politechnika Gdańska, Wydział Chemiczny, Gdańsk 2007.
Uzupełniająca lista lektur	1. Dostalek L.: Bezpieczeństwo protokołu TCP/IP. Wydawnictwo Naukowe PWN, Warszawa, 2003. 2. Kosmowski K.T.: Functional safety management in critical systems, Gdańsk, 2008. 3. Sankar K. i inni: CISCO. Bezpieczeństwo sieci bezprzewodowych. Wyd. Mikom, Warszawa, 2005. 4. PN-ISO/IEC 27001: Technika informatyczna - Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania .
Adresy eZasobów	

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Zagrożenia związane z ochroną informacji. System zarządzania bezpieczeństwem funkcjonalnym i ochroną informacji w przedsiębiorstwie. Prawne i normalizacyjne aspekty zarządzania ochroną informacji.
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy