POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM, PG_00070750		
Kierunek studiów	Zarządzanie inżynierskie		
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu	2028/2029
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	niestacjonarne	Sposób realizacji	na uczelni
Rok studiów	3	Język wykładowy	polski
Semestr studiów	6	Liczba punktów ECTS	3.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
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		

Formy zajęć

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	9.0	0.0	18.0	0.0	0.0	27
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	27	3.0	70.0	100

Cel przedmiotu

Przygotowanie studentów do samodzielnej identyfikacji i analizy zagrożeń cyberbezpieczeństwa oraz projektowania odpowiednich środków ochrony, na podstawie wiedzy z zakresu zarządzania ryzykiem, głównych koncepcji, procesów i norm zarządzania cyberbezpieczeństwem, oraz kształtowanie postaw związanych z odpowiedzialnym wykorzystaniem technologii w kontekście cyberbezpieczeństwa organizacji.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K6_K01] jest gotów pełnić role zawodowe w sposób odpowiedzialny, uwzględniając w procesach decyzyjnych kwestie prawne, etyczne i kulturowe.	jest gotów podejmować odpowiedzialne decyzje w obszarze cyberbezpieczeństwa, uwzględniając ich konsekwencje prawne, etyczne i społeczne, zwłaszcza w zakresie ochrony danych i prywatności.	[SK3] Ocena umiejętności organizacji pracy [SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce
[K6_W03] zna wiarygodne źródła informacji i wykorzystuje zaawansowaną wiedzę do wyjaśniania współczesnych problemów zarządzania.	zna i rozumie wiarygodne źródła informacji, koncepcje i procesy zarządzania cyberbezpieczeństwem oraz standardy (np. ISO/IEC 27001, NIST), w kontekście analizy zagrożeń i doboru odpowiednich środków zabezpieczeń dla systemów informatycznych w przedsiębiorstwie.	[SW2] Ocena wiedzy zawartej w prezentacji
[K6_U06] potrafi zdobywać wiedzę specjalistyczną z zakresu zarządzania inżynierskiego, wykazując umiejętność efektywnego planowania pracy indywidualnej oraz uczenia się przez całe życie.	potrafi przeanalizować cyberzasoby przedsiębiorstwa, zidentyfikować potencjalne zagrożenia oraz zaproponować adekwatne działania minimalizujące ryzyko, z wykorzystaniem dostępnych narzędzi i metodyk zarządzania.	[SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu [SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania

Treści przedmiotu

Treści przedmiotu - wykład

1. Podstawowe pojęcia i koncepcje cyberbezpieczeństwa
2. Używalne cyberbezpieczeństwo
3. Proces zarządzania cyberbezpieczeństwem
4. Zarządzanie ryzykiem cyberbezpieczeństwa
5. Zagrożenia cyberbezpieczeństwa
6. Wybrane standardy i wytyczne dotyczące cyberbezpieczeństwa
7. Zabezpieczenia

Treści przedmiotu - laboratoria

1. Podstawowe pojęcia i koncepcje cyberbezpieczeństwa
2. Używalne cyberbezpieczeństwo
3. Proces zarządzania cyberbezpieczeństwem
4. Zarządzanie ryzykiem cyberbezpieczeństwa
5. Zagrożenia cyberbezpieczeństwa
6. Wybrane standardy i wytyczne dotyczące cyberbezpieczeństwa
7. Zabezpieczenia

Wymagania wstępne i dodatkowe

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
Studium przypadku	60.0%	50.0%
Pisemny sprawdzian wiedzy z pytaniami zamkniętymi i otwartymi	60.0%	45.0%
Aktywność merytoryczna w trakcie wykładu	60.0%	5.0%

Zalecana lista lektur

Podstawowa lista lektur

1. ISO/IEC 27001:2017
2. NIST SP 800-53 Revision 5
3. Computer security handbook, edited by Seymour Bosworth, M. E. Kabay and Eric Whyne. 6th ed. Wiley, 2014
4. Ross Anderson, Security Engineering Third Edition, https://www.cl.cam.ac.uk/~rja14/book.html
5. David Kennedy, Jim OGorman, Devon Kearns, and Mati Aharoni, Metasploit: The Penetration Testers Guide, No Starch Press, 2011

Uzupełniająca lista lektur

1. Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, Osborne/McGraw-Hill, 2001
2. Matt Bishop, Introduction to Computer Security, Prentice Hall PTR 2004
3. Micki Krause, Harold F. Tipton, Information Security Management Handbook, Auerbach 2007
4. Steve Purser, A Practical Guide to Managing Information Security, Artech 2004
5. Matt Bishop, Computer Security: Art and Science, Addison Wesley 2002
6. ISO/IEC 15408 (Common Criteria)
7. Sjaak Laan, IT Infrastructure Architecture Infrastructure Building Blocks and Concepts, Lulu Press Inc. 2017

Adresy eZasobów

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania

- Przeprowadź analizę przedsiębiorstwa. Zidentyfikuj i opisz jego cyberzasoby
- Zidentyfikuj niezależne listy zagrożeń cyberbezpieczeństwa i opracuj własną listę cyberzagrożeń
- Oszacuj ryzyko cyberbezpieczeństwa
- Wyjaśnij systematyczne podejście do zarządzania cyberbezpieczeństwem w przedsiębiorstwie
- Wybierz standard cyberbezpieczeństwa, uzasadnij swój wybór
- Podaj przykład naruszenia integralności cyberzasobu
- Podaj przykład zabezpieczenia służącego zmniejszeniu ryzyko skopiowania danych księgowych przez nieuprawnionych użytkowników
- Podaj i wyjaśnij wzór na ryzyko cyberbezpieczeństwa
- Wskaż i wyjaśnij najczęstsze strategie postępowania z zagrożeniami związanymi z cyberbezpieczeństwem
- Opisz podstawowe cechy kontroli dostępu

Zajęcia praktyczne w ramach przedmiotu

Nie dotyczy