POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM , PG_00056590		
Kierunek studiów	Zarządzanie inżynierskie		
Data rozpoczęcia studiów	październik 2021 r.	Rok akademicki realizacji przedmiotu	2024/2025
Poziom kształcenia	I stopnia - inżynierskie	Grupa zajęć	
Forma studiów	stacjonarne	Sposób realizacji	na odległość (e-learning)
Rok studiów	4	Język wykładowy	angielski
Semestr studiów	7	Liczba punktów ECTS	3.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	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	15.0	0.0	15.0	0.0	0.0	30

W tym liczba godzin zajęć na odległość: 30.0

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	0.0	0.0	30

Cel przedmiotu

Zdobycie przez studenta podstawowej wiedzy o zarządzaniu cyberbezpieczeństwem w organizacjach.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K6_U08] analizuje rozwiązania inżynierskie i menedżerskie w procesach podejmowania decyzji z uwzględnieniem aspektów projakościowych i prośrodowiskowych oraz bezpieczeństwa procesów pracy	Student: - analizuje przedsiębiorstwo i jego zasoby informatyczne, - analizuje zagrożenia cyberbezpieczeństwa, - dobiera środki ochrony.	[SU2] Ocena umiejętności analizy informacji [SU1] Ocena realizacji zadania
[K6_W13] ma podstawową wiedzę z zakresu projektowania, modelowania i optymalizacji procesów i systemów technicznych	Student: - opisuje przedsiębiorstwo, - identyfikuje i opisuje zasoby informatyczne przedsiębiorstwa, - rozpoznaje i opisuje problemy cyberbezpieczeństwa przedsiębiorstw, - definiuje środki ochrony.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW1] Ocena wiedzy faktograficznej

Treści przedmiotu

- Podstawowe pojęcia i koncepcje cyberbezpieczeństwa
- Używalne cyberbezpieczeństwo
- Proces zarządzania cyberbezpieczeństwem
- Zarządzanie ryzykiem cyberbezpieczeństwa
- Zagrożenia cyberbezpieczeństwa
- Wybrane standardy i wytyczne dotyczące cyberbezpieczeństwa
- Zabezpieczenia

Wymagania wstępne i dodatkowe

Znajomość języka angielskiego w stopniu umożliwiającym płynną komunikację

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
aktywne uczestniczenie w spotkaniach zajęciowych	60.0%	5.0%
ćwiczenia laboratoryjne	60.0%	50.0%
sprawdzian wiedzy	60.0%	45.0%

<table>
<tr><td rowspan="3">Zalecana lista lektur</td><td>Podstawowa lista lektur</td><td colspan="2">ISO/IEC 27001:2017
NIST SP 800-53 Revision 5
Computer security handbook, edited by Seymour Bosworth, M. E. Kabay and Eric Whyne. 6th ed. Wiley, 2014.
Ross Anderson, Security Engineering Third Edition, https://www.cl.cam.ac.uk/~rja14/book.html
David Kennedy, Jim OGorman, Devon Kearns, and Mati Aharoni, Metasploit: The Penetration Testers Guide, No Starch Press, 2011.</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td colspan="2">Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, Osborne/McGraw-Hill, 2001
Matt Bishop, Introduction to Computer Security, Prentice Hall PTR 2004
Micki Krause, Harold F. Tipton, Information Security Management Handbook, Auerbach 2007
Steve Purser, A Practical Guide to Managing Information Security, Artech 2004
Matt Bishop, Computer Security: Art and Science, Addison Wesley 2002
ISO/IEC 15408 (Common Criteria)
Sjaak Laan, IT Infrastructure Architecture Infrastructure Building Blocks and Concepts, Lulu Press Inc. 2017</td></tr>
<tr><td>Adresy eZasobów</td><td colspan="2">Adresy na platformie eNauczanie:</td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td colspan="3">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.</td></tr>
<tr><td>Praktyki zawodowe w ramach przedmiotu</td><td colspan="3">Nie dotyczy</td></tr>
</table>