POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM , PG_00056981		
Kierunek studiów	Zarządzanie inżynierskie		
Data rozpoczęcia studiów	październik 2019 r.	Rok akademicki realizacji przedmiotu	2022/2023
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	4	Język wykładowy	polski
Semestr studiów	8	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	8.0	0.0	8.0	0.0	0.0	16

W tym liczba godzin zajęć na odległość: 0.0

Zarządzanie cyberbezpieczeństwem - niestacjonarne 2023 - Moodle ID: 27732
https://enauczanie.pg.edu.pl/moodle/course/view.php?id=27732

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	16	0.0	0.0	16

Cel przedmiotu

Zdobycie przez studenta wiedzy dotyczącej zarządzania cyberbezpieczeństwem w przedsiębiorstwie

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K6_W13] ma podstawową wiedzę z zakresu projektowania, modelowania i optymalizacji procesów i systemów technicznych	Student: - identyfikuje i opisuje cyberzasoby przedsiębiorstwa, - rozpoznaje i opisuje problemy cyberbezpieczeństwa przedsiębiorstw, - definiuje zabezpieczenia.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW1] Ocena wiedzy faktograficznej
[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 zabezpieczenia.	[SU2] Ocena umiejętności analizy informacji [SU1] Ocena realizacji zadania

Treści przedmiotu

- Podstawowe pojęcia związane z zarządzaniem cyberbezpieczeństwem
- System Zarządzania Bezpieczeństwem Informacji
- Zarządzanie ryzykiem
- Zabezpieczenia
- Standard ISO/IEC 27001
- Proces zarządzania bezpieczeństwem wg ISO/IEC 27001
- Polityka bezpieczeństwa
- Zagrożenia bezpieczeństwa

Wymagania wstępne i dodatkowe

Znajomość języka angielskiego

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
ćwiczenia laboratoryjne	60.0%	50.0%
aktywność podczas wykładu	60.0%	5.0%
sprawdzian wiedzy	60.0%	45.0%

<table>
<tr><td rowspan="3">Zalecana lista lektur</td><td>Podstawowa lista lektur</td><td>1. PN-ISO/IEC 27001
2. Ross Anderson, Inżynieria zabezpieczeń, WNT 2005; Wydanie trzecie dostępne w języku angielskim: https://www.cl.cam.ac.uk/~rja14/book.html
3. Andrzej Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT 2000
4. Adam Gałach, Instrukcja zarządzania bezpieczeństwem systemu Informatycznego, ODDK 2004
5. Krzysztof Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN 2009
6. Tadeusz Kifner, Polityka bezpieczeństwa i ochrony informacji, Helion 1999
7. Marcin Szeliga, Włamanie do komputera: jak się przed nim obronić?, PWN 2011
8. John Viega, Mity bezpieczeństwa IT: czy na pewno nie masz się czego bać?, Helion 2010</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>1. NIST SP 800-53
2. Edward Amoroso, Wykrywanie intruzów, RM 1999.
3. Bruce Schneier, Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, WNT 2002
4. Stuart McClure, Joel Scambray, George Kurtz, Hacking zdemaskowany. Bezpieczeństwo sieci - sekrety i rozwiązania, PWN 2006
5. Matt Bishop, Introduction to Computer Security, Prentice Hall PTR 2004
6. Micki Krause, Harold F. Tipton, Information Security Management Handbook, Auerbach 2007
7. Steve Purser, A Practical Guide to Managing Information Security, Artech 2004
8. Matt Bishop, Computer Security: Art and Science, Addison Wesley 2002
9. ISO/IEC 15408 (Common Criteria)</td></tr>
<tr><td>Adresy eZasobów</td><td>Uzupełniające
https://cyberdefence24.pl/cyberbezpieczenstwo - Portal cyberdefence24.pl
https://www.gov.pl/web/baza-wiedzy - Baza wiedzy gov.pl
https://www.nist.gov/topics/cybersecurity - Zasoby dot. cyberbezpieczeństwa NIST
https://www.schneier.com/ - Blog Bruce'a Schneiera
https://www.cert.pl/ - Portal CERT NASK
https://www.enisa.europa.eu/ - ENISA
https://niebezpiecznik.pl/ - Portal https://niebezpiecznik.pl/</td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td colspan="2">1. Przeanalizuj przedsiębiorstwo. Zidentyfikuj i opisz jego cyberzasoby.
2. Zidentyfikuj niezależne listy zagrożeń cyberbezpieczeństwa i opracuj własną listę cyberzagrożeń.
3. Oblicz ryzyko związane z cyberbezpieczeństwem.
4. Podaj przykład naruszenia integralności cyberzasobu.
5. Podaj przykład zabezpieczenia mającego na celu zmniejszenie ryzyka kopiowania danych księgowych przez osoby nieupoważnione.
6. Podaj i wyjaśnij formułę ryzyka cyberbezpieczeństwa.
7. Wymień i wyjaśnij najczęstsze strategie postępowania z zagrożeniami cybernetycznymi.</td></tr>
<tr><td>Praktyki zawodowe w ramach przedmiotu</td><td colspan="2">Nie dotyczy</td></tr>
</table>