POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Cybersecurity of Enterprise Infrastructure, PG_00053095		
Kierunek studiów	Inżynieria danych		
Data rozpoczęcia studiów	październik 2020 r.	Rok akademicki realizacji przedmiotu	2022/2023
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	mieszane (blended-learning)
Rok studiów	3	Język wykładowy	angielski
Semestr studiów	6	Liczba punktów ECTS	3.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	egzamin
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 inż. Sławomir Ostrowski 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: 16.0

Cybersecurity of Enterprise Infrastructure 2023 - Moodle ID: 20658
https://enauczanie.pg.edu.pl/moodle/course/view.php?id=20658

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

Celem przedmiotu jest nabycie przez studenta wiedzy z zakresu zarządzania cyberbezpieczeństwem w infrastrukturach IT przedsiębiorstw.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K6_W04] zna architektury komputerów, procesy systemu operacyjnego, systemy plików, programy do przetwarzania tekstu, zasady zarządzania dyskami i pamięcią ram. zna problemy współdzielenia stanu, prezentacji i transformacji informacji w systemie rozproszonym, technologie hipermediów i związanych z nimi usług, architektury interaktywnej symulacji rozproszonej oraz metody interakcji agentów	Student: - opisuje infrastrukturę IT przedsiębiorstwa, - identyfikuje zasoby infrastruktury IT przedsiębiorstwa, - rozpoznaje problemy bezpieczeństwa IT przedsiębiorstw, - definiuje zabezpieczenia.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW1] Ocena wiedzy faktograficznej
[K6_U02] projektuje, analizuje poprawność i tworzy specyfikację funkcjonalną systemów informatycznych, dobierając odpowiednie środki, tworzy modele jakości, przygotowuje i ocenia ich dokumentację projektową	Student: - analizuje infrastrukturę IT przedsiębiorstwa, - szacuje koszt związany z bezpieczeństwem infrastruktury IT, - dobiera zabezpieczenia.	[SU2] Ocena umiejętności analizy informacji [SU1] Ocena realizacji zadania

<table>
<tr><td>Treści przedmiotu</td><td>• Podstawowe zagadnienia cyberbezpieczeństwa
• Użyteczne cyberbezpieczeństwo
• System zarządzania cyberbezpieczeństwem
• Standardy i wytyczne dotyczące cyberbezpieczeństwa
• Proces zarządzania cyberbezpieczeństwem
• Polityka cyberbezpieczeństwa
• Zagrożenia cyberbezpieczeństwa
• Zarządzanie ryzykiem
• Zabezpieczenia
• Koszt zarządzania cyberbezpieczeństwem</td></tr>
<tr><td>Wymagania wstępne i dodatkowe</td><td>Znajomość j. angielskiego w stopniu komunikatywnym</td></tr>
<tr><td>Sposoby i kryteria oceniania osiąganych efektów uczenia się</td><td>
<table>
<tr><th>Sposób oceniania (składowe)</th><th>Próg zaliczeniowy</th><th>Składowa oceny końcowej</th></tr>
<tr><td>Aktywność podczas wykładu</td><td>0.0%</td><td>5.0%</td></tr>
<tr><td>Egzamin</td><td>60.0%</td><td>45.0%</td></tr>
<tr><td>Ćwiczenia laboratoryjne</td><td>60.0%</td><td>50.0%</td></tr>
</table>
</td></tr>
<tr><td>Zalecana lista lektur</td><td>
<table>
<tr><td>Podstawowa lista lektur</td><td>1. ISO/IEC 27001:2013
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 Second 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.</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>1. Bruce Schneier, Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, WNT 2002
2. Zarządzanie w gospodarce elektronicznej: zarządzanie infrastrukturą informatyczną, red. Elżbiety Miłosz i Jana Smołki, PTI 2011
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
9. Jerzy Kisielnicki, Informatyczna infrastruktura zarządzania, PWN 1993</td></tr>
<tr><td>Adresy eZasobów</td><td>Uzupełniające
https://cyberdefence24.pl/cyberbezpieczenstwo - Portal cyberdefence24.pl
https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber - Baza wiedzy www.gov.pl
https://niebezpiecznik.pl/ - Portal niebezpiecznik.pl
https://www.nist.gov/topics/cybersecurity - Baza wiedzy o cyberbezpieczeństwie NIST
https://www.schneier.com/ - Blog Bruce'a Schneier'a
https://www.cert.pl/ - CERT NASK
https://www.enisa.europa.eu/ - Portal ENISA</td></tr>
</table>
</td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td>1. Przeanalizuj przedsiębiorstwo i jego infrastrukturę IT a następnie przygotuj powiązaną dokumentację.
2. Przeprowadź analizę ryzyka dla analizowanej infrastruktury IT.
3. Zaproponuj środki bezpieczeństwa dla analizowanej infrastruktury IT.
4. Podaj przykłady infrastruktur krytycznych.
5. Przedstaw i omów podstawowe funkcje zapory sieciowej.</td></tr>
<tr><td>Praktyki zawodowe w ramach przedmiotu</td><td>Nie dotyczy</td></tr>
</table>