



Karta przedmiotu

Nazwa i kod przedmiotu	POZYTYWNE ZARZĄDZANIE ORGANIZACJA, PG_00053107						
Kierunek studiów	Zarządzanie (4 semestralne), Zarządzanie (3 semestralne)						
Data rozpoczęcia studiów	luty 2023 r.	Rok akademicki realizacji przedmiotu			2023/2024		
Poziom kształcenia	II stopnia	Grupa zajęć			Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	stacjonarne	Sposób realizacji			na uczelni		
Rok studiów	1	Język wykładowy			polski		
Semestr studiów	2	Liczba punktów ECTS			3.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			zaliczenie		
Jednostka prowadząca	Wydział Zarządzania i Ekonomii -> Katedra Zarządzania						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot						
	Prowadzący zajęcia z przedmiotu						
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	30.0	0.0	0.0	45
	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	45		6.0		24.0	75
Cel przedmiotu	Celem przedmiotu jest zdobycie przez studenta wiedzy dotyczącej zarządzania bezpieczeństwem informacji w przedsiębiorstwie.						
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu		Sposób weryfikacji i oceny efektu		
	[K7_W06] posiada pogłębioną wiedzę o różnych rodzajach więzi społecznych i występujących między nimi prawidłowościach w organizacji, wśród interesariuszy oraz w jej otoczeniu						
	[K7_U13] analizuje i ocenia zjawiska społeczne zachodzące w organizacjach oraz potrafi tworzyć zespoły zadaniowe w oparciu o zasady pracy grupowej						
	[K7_W02] ma pogłębioną wiedzę z zakresu klasycznych i nowoczesnych koncepcji zarządzania oraz możliwości ich zastosowania w zarządzaniu współczesnymi organizacjami różnego typu						
	[K7_K71] potrafi wyjaśnić potrzebę korzystania z wiedzy z zakresu nauk humanistycznych lub społecznych lub ekonomicznych lub prawnych w funkcjonowaniu w środowisku społecznym						
	[K7_U71] potrafi zastosować wiedzę z zakresu nauk humanistycznych lub społecznych lub ekonomicznych lub prawnych do rozwiązywania problemów						

Treści przedmiotu	<p>WYKŁAD</p> <ul style="list-style-type: none"> <li>• Wstęp do przedmiotu</li> <li>• System Zarządzania Bezpieczeństwem Informacji</li> <li>• Standard ISO/IEC 27001 i publikacja specjalna NIST SP 800-53</li> <li>• Proces zarządzania bezpieczeństwem wg ISO/IEC 27001 i NIST SP 800-53</li> <li>• Polityka bezpieczeństwa</li> <li>• Zagrożenia bezpieczeństwa; Identyfikacja i ocena zagrożeń</li> <li>• Zarządzanie ryzykiem</li> <li>• Mechanizmy ochrony: Kontrola dostępu; Identyfikacja i uwierzytelnianie; Kryptografia; Zapory sieciowe; Ochrona przed złośliwym oprogramowaniem; Systemy detekcji intruzów; Ochrona fizyczna;</li> <li>• Zagadnienia związane z kadrą przedsiębiorstwa</li> <li>• Koszt zarządzania bezpieczeństwem informacji w przedsiębiorstwie</li> </ul> <p>LABORATORIUM</p> <ul style="list-style-type: none"> <li>• Analiza przedsiębiorstwa i jego systemu informatycznego</li> <li>• Szacowanie ryzyka</li> <li>• Oszacowanie kosztu zarządzania bezpieczeństwem</li> <li>• Sformułowanie polityki bezpieczeństwa</li> <li>• Dobór środków bezpieczeństwa zgodnie z ISO/IEC 27001 lub NIST SP 800-53 (do wyboru)</li> </ul>		
Wymagania wstępne i dodatkowe	Język angielski		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Raporty z pracy w laboratorium	60.0%	60.0%
	Sprawdzian wiedzy	60.0%	40.0%
Zalecana lista lektur	Podstawowa lista lektur	<ol style="list-style-type: none"> <li>1. Standardy NIST SP 800-53 i ISO/IEC 27001</li> <li>2. R. Anderson, Inżynieria zabezpieczeń, WNT</li> <li>3. A. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT</li> <li>4. Materiały opracowane w formie pisemnej</li> </ol>	
	Uzupełniająca lista lektur	<ol style="list-style-type: none"> <li>1. Edward Amoroso, Wykrywanie intruzów. Wydawnictwo RM, Warszawa 1999</li> <li>2. Bruce Schneier, Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C. WNT</li> <li>3. Stuart McClure, Joel Scambray, George Kurtz. Hacking zdemaskowany. Bezpieczeństwo sieci - sekrety i rozwiązania. PWN 2006</li> </ol>	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	<ol style="list-style-type: none"> <li>1. W pierwszym etapie student wybiera rzeczywiste bądź proponuje fikcyjne przedsiębiorstwo, dla którego będzie przeprowadzał dalsze analizy podczas zajęć laboratoryjnych. Dokonuje jego charakterystyki poprzez podanie misji, celu, opisu działalności oraz schematu organizacyjnego. Następnie przeprowadza identyfikację zasobów informacyjnych w przedsiębiorstwie oraz z nimi powiązanych. Tworzy diagram (w MS Visio) i opis systemu informatycznego. Efekty powyższych działań umieszcza w raporcie.</li> <li>2. Student dokonuje oszacowania kosztu zarządzania bezpieczeństwem w przedsiębiorstwie. W tym celu określa wartość kilku wskaźników charakteryzujących przedsiębiorstwo, takich jak liczba użytkowników, liczba pracowników bezpieczeństwa, czy wskaźnik przyjęć. Następnie wprowadza te dane do arkusza kalkulacyjnego, aby otrzymać wyniki oszacowań. Wyniki te poddaje analizie, a wnioski oraz powiązane dane przedstawia w raporcie.</li> </ol>		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		