



Karta przedmiotu

Nazwa i kod przedmiotu	POZYTYWNE ZARZĄDZANIE ORGANIZACJA, PG_00053113						
Kierunek studiów	Zarządzanie (4 semestralne), Zarządzanie (3 semestralne)						
Data rozpoczęcia studiów	październik 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	niestacjonarne	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	8.0	0.0	16.0	0.0	0.0	24
	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	24		6.0		45.0	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_U13] analizuje i ocenia zjawiska społeczne zachodzące w organizacjach oraz potrafi tworzyć zespoły zadaniowe w oparciu o zasady pracy grupowej		
	[K7_W06] posiada pogłębioną wiedzę o różnych rodzajach więzi społecznych i występujących między nimi prawidłowościach w organizacji, wśród interesariuszy oraz w jej otoczeniu		
	[K7_K71] potrafi wyjaśnić potrzebę korzystania z wiedzy z zakresu nauk humanistycznych lub społecznych lub ekonomicznych lub prawnych w funkcjonowaniu w środowisku społecznym	Student: - organizuje zespół w ramach, którego będzie prowadził prace związane z zapewnianiem bezpieczeństwa informacji w przedsiębiorstwie, - analizuje działalność i organizację przedsiębiorstwa tego, identyfikuje misję i cele.	[SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce
	[K7_U71] potrafi zastosować wiedzę z zakresu nauk humanistycznych lub społecznych lub ekonomicznych lub prawnych do rozwiązywania problemów	Student: - dobiera środki kontrolne służące zapewnieniu bezpieczeństwa informacji w przedsiębiorstwie, - rozróżnia metody związane z zapewnianiem bezpieczeństwa informacji, w tym metody szacowania kosztu zarządzania bezpieczeństwem informacji, czy metody analizy ryzyka	[SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu [SU1] Ocena realizacji zadania
[K7_W02] ma pogłębioną wiedzę z zakresu klasycznych i nowoczesnych koncepcji zarządzania oraz możliwości ich zastosowania w zarządzaniu współczesnymi organizacjami różnego typu	Student: - rozpoznaje zmieniające się zagrożenia wobec zasobów informacyjnych w przedsiębiorstwie - określa skutki i znaczenie zagrożeń bezpieczeństwa zasobów informacyjnych w kontekście zmieniającego się otoczenia przedsiębiorstwa.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW1] Ocena wiedzy faktograficznej	
Treści przedmiotu	<p>WYKŁAD</p> <ul style="list-style-type: none"> • Podstawowe pojęcia związane z zarządzaniem bezpieczeństwem informacji • Koszt zarządzania bezpieczeństwem informacji w przedsiębiorstwie • System Zarządzania Bezpieczeństwem Informacji • Standard ISO/IEC 27001 i publikacja specjalna NIST SP 800-53 • Proces zarządzania bezpieczeństwem wg ISO/IEC 27001 i NIST SP 800-53 • Polityka bezpieczeństwa • Zagrożenia bezpieczeństwa • Zarządzanie ryzykiem • Mechanizmy ochrony • Zagadnienia związane z kadrami przedsiębiorstwa <p>LABORATORIUM</p> <ul style="list-style-type: none"> • Analiza przedsiębiorstwa i jego systemu informatycznego • Szacowanie ryzyka • Oszacowanie kosztu zarządzania bezpieczeństwem • Formułowanie polityki bezpieczeństwa • Dobór środków bezpieczeństwa zgodnie z ISO/IEC 27001 lub NIST SP 800-53 (do wyboru) 		
Wymagania wstępne i dodatkowe	Język angielski		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa ocena końcowej
	Sprawdzian wiedzy	60.0%	40.0%
	Raporty z pracy w laboratorium	60.0%	60.0%
Zalecana lista lektur	Podstawowa lista lektur	<ol style="list-style-type: none"> 1. Ross Anderson, Inżynieria zabezpieczeń, WNT 2005 2. Andrzej Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT 2000 3. PN-ISO/IEC 27001:2007 4. Adam Gałach, Instrukcja zarządzania bezpieczeństwem systemu Informatycznego, ODDK 200 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 	

	Uzupełniająca lista lektur	<ol style="list-style-type: none"> 1. Edward Amoroso, Wykrywanie intruzów, RM 1999. 2. Bruce Schneier, Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, WNT 2002 3. Stuart McClure, Joel Scambray, George Kurtz, Hacking zdemaskowany. Bezpieczeństwo sieci - sekrety i rozwiązania, PWN 2006 4. Matt Bishop, Introduction to Computer Security, Prentice Hall PTR 2004 5. Micki Krause, Harold F. Tipton, Information Security Management Handbook, Auerbach 2007 6. Steve Purser, A Practical Guide to Managing Information Security, Artech 2004 7. Matt Bishop, Computer Security: Art and Science, Addison Wesley 2002 8. ISO/IEC 15408 (Common Criteria), NIST SP 800-53
	Adresy eZasobów	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	<ol style="list-style-type: none"> 1. Student dokonuje charakterystyki przedsiębiorstwa poprzez podanie jego misji i celów, opisu działalności oraz schematu organizacyjnego. Następnie przeprowadza identyfikację zasobów informacyjnych w przedsiębiorstwie oraz z nimi powiązanych. Efekty powyższych działań umieszcza w raporcie. 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. 	
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy	