Nazwa zajęć: Bezpieczeństwo informacyjne w organizacji			Information Security in Organization		
Kierunek: Zarządzanie					***Obowiązuje od roku ak.*** 2023/2024
Poziom: II st. magisterski		***Profil:*** Praktyczny		***Grupa zajęć:*** Specjalnościowe	
Semestr: 2	***Forma zaliczenia:*** Z - zaliczenie na ocenę	***Punkty ECTS:*** 3		***Zajęcia do wyboru:*** Tak	***Język zajęć:*** polski

Forma zajęć i liczba godzin na studiach stacjonarnych i niestacjonarnych:

Wykład 15 / 8	***Ćwiczenia*** 15 / 8		***Suma godzin:*** 30 / 16

Specjalność:
Zarządzanie bezpieczeństwem w organizacji

Nazwiska osób odpowiedzialnych za zajęcia:
mgr Dariusz Mikołajczyk

Opis zajęć:
Celem przedmiotu rozwinięcie umiejętności poruszania się w materii ochrony informacji prawnie chronionych, ze szczególnym uwzględnieniem najczęściej spotykanych grup informacji chronionych w organizacjach: danych osobowych, informacji niejawnych, tajemnicy przedsiębiorstwa. Wskazane zostaną techniki konstruowania dokumentacji w zakresie ochrony informacji, aspektów ochrony informacji w obszarach personalnym, teleinformatycznym, papierowym. Dokonany zostanie opis budowy struktur organizacyjnych odpowiedzialnych za ochronę informacji w jednostkach organizacyjnych. Zarysowane zostaną techniki prowadzenia projektów wdrażania systemów ochrony informacji w poszczególnych grupach informacji chronionych oraz certyfikacji systemów zarządzania w tym zakresie w oparciu o normy ISO. Omówione zostaną najbardziej typowe zagrożenia w dziedzinie ochrony informacji i sposoby im zapobiegania.

Cele dydaktyczne:

Przekazanie wiedzy i umiejętności dotyczących samodzielnego zarządzania bezpieczeństwem informacyjnym oraz konstruowania jego struktur, procedur i klasyfikowania poszczególnych informacji pod kątem systemów ich ochrony.

Zapoznanie studentów ze złożonością i wielopłaszczyznowością w zakresie zapewnienia bezpieczeństwa informacyjnego w jednostce lub w organizacji.

Kształtowanie umiejętności samodzielnego konstruowania struktur i prowadzenia projektów w dziedzinie bezpieczeństwa informacyjnego w jego szerokim pojęciu tematycznym.

Rozwinięcie kompetencji w zakresie samodzielnego organizowania struktur i kierowania nimi, umiejętności współpracy w dziedzinie bezpieczeństwa informacyjnego wewnątrz organizacji jak i poza jej strukturami, zdolności analitycznego i organizacyjnego myślenia.

Metody dydaktyczne:				***Metody oceniania:***	
MP1	wykład informacyjny			MO1	kolokwium pisemne
MP2	opis			MO2	aktywność w trakcie zajęć
MP3	objaśnienie				
MP4	studium przypadku				

MC1	ćwiczenie praktyczne				
MS1	dyskusja dydaktyczna				

Wykład

W1	Współczesne zagrożenia w zakresie ochrony informacji.
W2	Zarządzanie ochroną informacji w organizacji - budowa i integracja systemu.
W3	Ochrona informacji niejawnych w organizacji.
W4	Ochrona danych osobowych.
W5	Ochrona tajemnicy przedsiębiorstwa - podstawowy system ochrony informacji.
W6	Norma ISO 27001 i 27002 - Zintegrowany System Bezpieczeństwa Informacji.

Ćwiczenia

C1	Przygotowanie struktury dokumentacji bezpieczeństwa informacji w przykładowej organizacji.
C2	Opracowanie zasad bezpieczeństwa niezbędnych dla funkcjonowania tajemnicy przedsiębiorstwa.
C3	Opracowanie jednej z wybranych procedur dotyczących ochrony danych osobowych.
C4	Dobór zabezpieczeń wynikających z ISO 27002 dla konktretnego aktywa informacyjnego.
C5	Opracowanie szkolenia dla pracowników z zakresu ochrony informacji w przykładowej organizacji.

Literatura podstawowa

1 K. Liderman, Bezpieczeństwo informacyjne. Nowe wyzwania, PWN 2018

Literatura uzupełniająca

1 D. Mikołajczyk, Bezpieczeństwo informacyjne w firmie - budowa systemu i zagrożenia, Katowice 2011

2 R. i M.Taradejna, Ochrona informacji w działalności gospodarczej, społecznej i zawodowej oraz życiu prywatnym, PIKW 2004

3 D. Pipkin, Bezpieczeństwo informacji, WNT 2000

4 R. Borowiecki, M. Kwieciński, Informacja w zarządzaniu przedsiębiorstwem, Zakamycze 2003

5 B. Fiszer, W. Świerczyńska - Głowina, Dostęp do informacji ustawowo chronionych, zarządzanie informacją, Uniwersystet Jagielloński 2006

Źródła dodatkowe

1 Normy ISO/IEC 27001:2022 oraz ISO/IEC 27002:2022

2 Ustawa o ochronie informacji niejawnych i zwalczaniu nieuczciwej konkurencji

3 Rozporządzenie Parlamentu Europejskiego i Rady (EU) 2016/679 z 27.04.2016 r. - RODO

4 Materiały i opracowania własne prowadzącego przedmiot

Warunki zaliczenia

Warunkiem zaliczenia jest uzyskanie pozytywnej oceny z kolokwium pisemnego. Ocena ta może zostać podniesiona w wyniku aktywności na zajęciach.

Przykłady pytań zaliczeniowych

Klasyfikacja informacji w organizacji.

Elementy składowe bezpieczeństwa informacyjnego.

Ochrona danych osobowych - struktura zarządcza i dokumentacyjna.
Wymagania prawne z zakresu ochrony informacji niejawnych
Zagrożenia dla bezpieczeństwa informacji w organizacji
Norma ISO 27001 - zawartość, wdrożenie, certyfikacja
Budowa systemu tajemnicy przedsiębiorstwa - elementy składowe, wdrażanie systemu

Obciążenie pracą studenta

Studia stacjonarne/niestacjonarne

Forma pracy studenta	Wykład		Ćwiczenia				Suma	
Zajęcia z bezpośrednim udziałem nauczyciela	15 g	8 g	15 g	8 g			30 g	16 g
Zapozanie się z literaturą przedmiotu	10 g	15 g					10 g	15 g
Przygotowanie się do zajęć			10 g	15 g			10 g	15 g
Przygotowanie się do kolokwiów	15 g	15 g					15 g	15 g
Realizacja zadanych ćwiczeń i zadań			10 g	14 g			10 g	14 g
Przygotowanie sprawozdania z ćwiczeń								
Przygotowanie projektu / pracy								
Przygotowanie się i udział w egzaminie								
	40 g	38 g	35 g	37 g			75 g	75 g

Efekty uczenia się	KEK	Treści kształcenia	Metody dydaktyczne	M. oceniania
Zna złożoność pojęcia i szerokość aspektów bezpieczeństwa informacji w organizacji, wieloaspaktowość tematyki i jej znaczenia dla każdego podmiotu	K_W01	W1-W6 C1	MP1-MP4 MC1	MO1
Zna zasady projektowania systemu ochrony informacji w organizacji, uwzględniającego wymagania prawne jakie go dotyczą	K_W02	W2 W6 C1 C4	MP1-MP4 MC1 MS1	MO1 MO2
Rozumie zakres szerokiej odpowiedzialności osób zajmujących się bezpieczeństwem informacji w organizacji i ich obowiązków wobec instytucji zewnętrznych	K_W04	W3-W5 C2 C3 C5	MP1-MP4 MC1 MS1	MO1 MO2
Rozumie i potrafi w praktyce budować struktury organizacyjne konieczne do zarządzania bezpieczeństwem informacji w organizacjach	K_U01	W2 W6 C1-C3	MP1-MP4 MC1 MS1	MO1 MO2

Posiada umiejętność tworzenia dokumentacji związanej z bezpieczeństwem w zakresie ochrony informacji	K_U04	W3-W5 C1-C3	MP1-MP4 MC1 MS1	MO1 MO2
Posiada umiejętność analizy i oceny dostępnych rozwiązań prawnych w zakresie metod zarządzania bezpieczeństwem informacji i budowy odpowiednich struktur do realizacji celów istniejących w tej dziedzinie.	K_U07	W1-W6 C1-C3	MP1-MP4 MC1 MS1	MO1 MO2
Potrafi inicjować działania zmierzające do budowy procesów ochrony informacji w organizacji i wytrwale dąży do ich efektywnego zakończenia.	K_K05	W2 W6 C1	MP1-MP4 MC1	MO1
Ma świadomość ciągłych zmian przepisów i rozwiązań prawnych w zakresie szeroko rozumianych zagadnień bezpieczeństwa informacji. Jest skłonny do aktualizowania swojej wiedzy w tym zakresie.	U_K09	W3-W5	MP1-MP4	MO1