Nazwa zajęć: Bezpieczeństwo teleinformatyczne			ICT Security		
Kierunek: Zarządzanie					***Obowiązuje od roku ak.*** 2022/2023
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	***Ćwiczenia***		***Suma godzin:***
15 / 8	15 / 8		30 / 16

Specjalność:
Zarządzanie bezpieczeństwem w organizacji

Nazwiska osób odpowiedzialnych za zajęcia:
mgr Marek Bońkowski

Opis zajęć:
Przedmiot skierowany jest do studentów pragnących zdobyć wiedzę z zakresu projektowania i zarządzania systemami bezpieczeństwa wewnętrznego w podmiotach różnego typu. Zakres tematyczny przedmiotu obejmuje szerokie spektrum zagadnień związanych z bezpieczeństwem teleinformatycznym. Aby dobrze zrozumieć istotę zagrożeń oraz metody ich zapobiegania słuchacze najpierw zapoznają się ze strukturami oraz mechanizmami działania telefonii stacjonarnej, GSM, VoIP oraz sieci komputerowych, aby następnie poznać obszary zagrożeń i metody ochrony przed nimi dla każdej z technologii. Słuchacze zapoznają się z podstawami kryptografii oraz technikami jej stosowania w celu zapewnienia poufności danych zarówno przy ich przechowywaniu jak i przesyłaniu oraz weryfikacji ich integralności. W procesie nauczania przedstawione zostaną także zagadnienia dotyczące przetwarzania danych osobowych w systemach teleinformatycznych, ochrony informacji niejawnych a także zostanie omówienie bezpieczeństwo teleinformatyczne w ujęciu normy ISO 27001.

Cele dydaktyczne:

Kształcenie znajomości funkcjonowania systemów teleinformatycznych oraz technik zapewnienia im bezpieczeństwa

Przekazanie wiedzy dotyczącej struktur oraz zasad funkcjonowania telefonii stacjonarnej, GSM oraz VoIP a także sieci komputerowych. Poznanie obszarów zagrożeń w każdej z tych technologii oraz technik ich eliminacji. Przekazanie wiedzy z zakresu kryptografii oraz możliwości jej praktycznych zastosowań, a także prawidłowego przetwarzania danych osobowych w systemach teleinformatycznych.

Kształtowanie umiejętności oceny zagrożeń w systemach teleinformatycznych oraz skutecznego im przeciwdziałaniu. Sprawnej oceny procesu przetwarzania danych osobowych w systemach teleinformatycznych oraz ich zgodności z obowiązującymi przepisami prawa. Kształtowanie umiejętności doboru metod kryptograficznych w celu zapewnienia poufności danych w procesie ich przechowywania, przesyłania oraz udostępniania.

Kształtowanie samodzielności w zakresie analizy i oceny bezpieczeństwa teleinformatycznego w organizacji a także kompetencji w zakresie doboru odpowiednich rozwiązań i procedur.

Metody dydaktyczne:				***Metody oceniania:***	
MP1	wykład informacyjny			MO1	praca projektowa

MP2	studium przypadku				
MC1	projekt				
MC2	ćwiczenie praktyczne				
MS1	wykład problemowy				
MS2	dyskusja dydaktyczna				

Wykład

W1	Stacjonarna sieć telekomunikacyjna
W2	Sieć telekomunikacyjna GSM
W3	Sieć telekomunikacyjna VoIP
W4	Sieci komputerowe
W5	Podstawy kryptografii
W6	Zabezpieczanie informacji na cyfrowych nośnikach informacji (komputery, dyski, telefony komórkowe)
W7	Norma ISO 27001 - Bezpieczeństwo teleinformatyczne
W8	Audyty bezpieczeństwa teleinformatycznego

Ćwiczenia

C1	Zabezpieczanie sieci PSTN
C2	Bezpieczeństwo w sieciach mobilnych
C3	Metody ataku na sieci komputerowe
C4	Zabezpieczenia sieci komputerowych
C5	Szyfrowanie symetryczne i asymetryczne
C6	Podpisy cyfrowe
C7	Zabezpieczanie cyfrowych nośników danych
C8	Tworzenie procedur bezpieczeństwa teleinformatycznego

Literatura podstawowa

1 A. Józefiok, CCNA 200-301. Zostań administratorem sieci komputerowych Cisco, Helion 2020.

2 J. Kurose, K. Ross, Sieci komputerowe. Ujęcie całościowe, Helion 2018

Literatura uzupełniająca

1 M. Bertaccini, Algorytmy kryptograficzne. Przewodnik po algorytmach w blockchain, kryptografii kwantowej, protokołach o wiedzy zerowej oraz szyfrowaniu omomorficznym, Helion 2023.

2 B. Galwas, Podstawy telekomunikacji optofalowej, Helion 2021.

3 D. R. Hayes, Informatyka w kryminalistyce. Praktyczny przewodnik, Helion 2021.

Warunki zaliczenia

Warunkiem zaliczenia jest przygotowanie pracy projektowej dotyczącej sieci komputerowych oraz telefonii stacjonarnych i mobilnych oraz kryptografii

Przykłady pytań zaliczeniowych

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	14 g	10 g	15 g			20 g	29 g
Przygotowanie się do zajęć								
Przygotowanie się do kolokwiów								
Realizacja zadanych ćwiczeń i zadań			10 g	10 g			10 g	10 g
Przygotowanie sprawozdania z ćwiczeń								
Przygotowanie projektu / pracy			15 g	20 g			15 g	20 g
Przygotowanie się i udział w egzaminie								
	25 g	22 g	50 g	53 g			75 g	75 g

Efekty uczenia się	KEK	Treści kształcenia	Metody dydaktyczne	M. oceniania
Ma pogłębioną wiedzę na temat wpływu zmian w organizacji na jej bezpieczeństwo teleinformatyczne oraz o możliwych zagrożeniach bezpieczeństwa teleinformatycznego	K_W02	W1-W8 C1-C8	MP1 MP2 MC1 MC2 MS1 MS2	MO1
Ma wiedzę o strukturach firm i organizacji oraz zachodzących między nimi relacjach niezbędną do prawidłowego oszacowania ryzyk i odpowiedniego doboru rozwiązań z zakresu bezpieczeństwa teleinformatycznego	K_W04	W7 W8 C8	MP1 MP2 MC1 MC2 MS1 MS2	MO1
Ma wiedzę możliwych metodach i drogach ataku teleinformatycznego wykorzystującego człowieka jako najsłabsze ogniwo oraz zna sposoby zapobiegania im.	K_W05	W1-W6 C1-C4 C7	MP1 MP2 MC1 MC2 MS1 MS2	MO1
Posiada umiejętność analizy i oceny dostępnych rozwiązań prawnych i technicznych w zakresie doboru metod ochrony w zależności od typu organizacji i wymagań bezpieczeństwa.	K_U02	C1-C8	MC1 MC2 MS2	MO1
Posiada umiejętność tworzenia i uzgadniania metod zabezpieczeń oraz tworzenia procedur bezpieczeństwa	K_U03	C1-C8	MC1 MC2 MS2	MO1

Ma świadomość ciągłych zmian przepisów oraz ciągłego rozwoju techniki teleinformatycznej i związanych z tym nowych niebezpieczeństw oraz metod ochrony. Jest skłonny do zasięgania opinii ekspertów w tym zakresie.	K_K02	W1-W8 C1-C8	MP1 MP2 MC1 MC2 MS1 MS2	MO1
Potrafi w sposób profesjonalny dobrać metody oraz zakres audytu teleinformatycznego oraz zachować poufność pozyskanych informacji	K_K07	W7 W8 C8	MP1 MP2 MC1 MC2 MS1 MS2	MO1