



Kierunek studiów	Informatyczne Techniki Zarządzania
Profil	Praktyczny
Stopień studiów	1-go stopnia
Forma studiów	niestacjonarne

Sylabus przedmiotu

Bezpieczeństwo w systemach informatycznych

1. Dane podstawowe

Status programowy przedmiotu	Blok A: Technologie informatyczne w zarządzaniu
Rodzaj przedmiotu	Obligatoryjny
Kod przedmiotu	TZI-BSI-ZG
Rok studiów	3
Semestr	5
Osoba odpowiedzialna za przedmiot	prof. Mirosław Siergiejczyk
Język wykładowy	polski

2. Wymiar godzin i forma zajęć

Rodzaj	Liczba godzin
Wykład	16
Laboratorium	16
Razem godzin	32

3. Cele przedmiotu

Kod	Cel
CP1	Przekazanie studentom podstaw wiedzy o problemach związanych z bezpieczeństwem systemów informatycznych wykorzystywanych w zarządzaniu. Przedstawienie wzajemnej zależności pomiędzy danymi, informacją i wiedzą oraz omówienie własności i cech informacji. Studenci uczą się identyfikować i rozumieć problemy bezpieczeństwa informacji, takie jak zagrożenia w systemach informatycznych, polityka bezpieczeństwa informatycznego w organizacjach. Studenci zdobywają wiedzę o tym, jak skutecznie i efektywnie wykorzystywać podstawowe instrumenty i mechanizmy ochrony w systemach informatycznych.
CP2	Studenci zdobywają umiejętności analizy skutków zagrożenia bezpieczeństwa w systemach informatycznych. Studenci zdobywają umiejętności związane z zarządzaniem bezpieczeństwem w systemach teleinformatycznych i monitorowaniem bezpieczeństwa systemów informatycznych. Zdobывают umiejętności wykorzystywania narzędzi analizy zabezpieczeń, opracowania procedur reagowania i dokumentowanie incydentów.
CP3	Studenci zdobywają odpowiednie kompetencje społeczne, przygotowujące do uczestniczenia w realizacji projektów społeczno-gospodarczych, wnosząc wiedzę techniczną, a w szczególności w zakresie bezpieczeństwa systemów informatycznych.

4. Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

Brak wstępnych wymagań.

5. Efekty uczenia się

Wiedza

Kod	Student zna i rozumie:	Realizuje cel	Efekty kierunkowe
EU-W1	Zna i rozumie istotę systemów informacyjnych i informatycznych i ich rolę w obszarze zarządzania. Zna zależności pomiędzy danymi, informacją i wiedzą oraz identyfikuje własności i cechy informacji w zarządzaniu.	CP1	K1P_W01, K1P_W06, K1P_W07

Kod	Student zna i rozumie:	Realizuje cel	Efekty kierunkowe
EU-W2	Posiada wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i organizacyjnych aspektów dotyczących problemów bezpieczeństwa informacji, takich jak zagrożenia w systemach informatycznych, polityka bezpieczeństwa informatycznego w organizacjach, narzędzia analizy zabezpieczeń, opracowania procedur reagowania i dokumentowanie incydentów.	CP1	K1P_W01, K1P_W06, K1P_W07
EU-W3	Zna i rozumie typowe technologie teleinformatyczne w zakresie bezpieczeństwa systemów informatycznych, znajdujące zastosowanie w ochronie informacji w zarządzaniu i biznesie.	CP1	K1P_W07

Umiejętności

Kod	Student potrafi:	Realizuje cel	Efekty kierunkowe
EU-U1	Posiada umiejętności wykorzystania metod analitycznych, ilościowych i symulacyjnych do identyfikacji zagrożeń w systemach informatycznych oraz doboru środków i mechanizmów ochrony w systemach informatycznych w obszarze zarządzania i biznesu.	CP2	K1P_U01, K1P_U06
EU-U2	Potrafi, przy formułowaniu i rozwiązywaniu zadań w zakresie bezpieczeństwa uwzględniać ich aspekty systemowe i techniczne.	CP2	K1P_U01, K1P_U03, K1P_U06
EU-U3	Potrafi dokonać analizy ekonomicznej, prawnej i organizacyjnej podejmowanych działań w zakresie bezpieczeństwa.	CP2	K1P_U06
EU-U4	Potrafi dokonać identyfikacji zagrożeń systemów informatycznych, przede wszystkim informatycznych w obszarze zarządzania oraz dokonać analizy i ocenić stan bezpieczeństwa istniejących rozwiązań.	CP2	K1P_U06, K1P_U08

Kompetencje

Kod	Student jest gotów do:	Realizuje cel	Efekty kierunkowe
EU-K1	Zdobywa odpowiednie kompetencje społeczne, przygotowujące do uczestniczenia w realizacji projektów informatycznych, wnosząc wiedzę dotyczącą aspektów bezpieczeństwa informacji i przewidując konsekwencje podjętych w ramach tych projektów działań.	CP3	K1P_K05

6. Treści programowe

Kod	Tematyka	wykład	laboratorium	Realizuje efekt
TP1	Wprowadzenie. Informacja i dane. Charakterystyka informacji. Fazy procesu informacji i ich teleinformatyczna realizacja. Cele przedmiotu i treści merytoryczne/literatura. Pojęcia bezpieczeństwa systemu informatycznego. Bezpieczeństwo teleinformatyczne. Bezpieczeństwo informacji. Struktura i podstawowe elementy systemu informatycznego. Podstawowe funkcje systemu informatycznego. Podstawowe podsystemy struktury technicznej systemu informatycznego.	2	2	EU-K1, EU-U1, EU-U3, EU-W1, EU-W2
TP2	Analiza zagrożeń w systemach informatycznych. Typy najczęściej spotykanych zagrożeń w systemach informatycznych. Kategorie i rodzaje przestępstw oraz zagrożeń w cyberprzestrzeni.	2	2	EU-K1, EU-U1, EU-U2, EU-W1, EU-W2, EU-W3
TP3	Metodyki analizy i oceny ryzyka zagrożeń w systemach informatycznych zarządzania w organizacjach. Metody jakościowe i metody ilościowe.	2	2	EU-K1, EU-U1, EU-U2, EU-U3, EU-U4, EU-W2

Kod	Tematyka	wykład	laboratorium	Realizuje efekt
TP4	Podstawowe środki i mechanizmy ochrony w systemach informatycznych. Mechanizmy uwierzytelniania, strategie autoryzacji i kontroli dostępu, mechanizmy dostępności informacji. . Metody biometryczne. Podstawowe informacje dotyczące kryptografii. Szyfry symetryczne, szyfry asymetryczne. Użycie klucza prywatnego i publicznego. Zarządzanie kluczami (PKI).	2	2	EU-K1, EU-U1, EU-U2, EU-U4, EU-W3
TP5	Bezpieczeństwo systemów operacyjnych. Typowe naruszenia bezpieczeństwa systemów operacyjnych. Problemy uwierzytelniania i kontroli dostępu współczesnych systemów operacyjnych. Bezpieczeństwo infrastruktury sieciowej systemów informatycznych. Bezpieczeństwo podstawowych protokołów i urządzeń. Narzędzia podnoszące poziom bezpieczeństwa sieci.	2	2	EU-K1, EU-U2, EU-U4
TP6	Środki i mechanizmy ochrony fizycznej w systemach informatycznych. Zabezpieczenia sprzętowe. Zabezpieczenia lokalizacyjne. Środki bezpieczeństwa fizycznego, strefy ochronne. Systemy zasilania awaryjnego. Systemy kontroli dostępu. Systemy monitoringu wizyjnego.	2	2	EU-K1, EU-U2, EU-U4
TP7	Organizacyjne środki bezpieczeństwa. Obowiązki pracowników w zakresie bezpieczeństwa użytkowania systemów informatycznych. Zgłaszanie incydentów i podatności. Szkolenia dla pracowników. Procedury reagowania, dokumentowanie incydentów. Plan odzyskiwania po awarii (DRP).	2	2	EU-K1, EU-U1, EU-U2, EU-U4, EU-W1, EU-W3
TP8	Polityka bezpieczeństwa. Zakres Polityki Bezpieczeństwa. Model realizacji polityki bezpieczeństwa. Typowe elementy polityki bezpieczeństwa. Konceptcje strategii ochrony. Zarządzanie bezpieczeństwem w systemach teleinformatycznych. System zarządzania bezpieczeństwem informacji (ISMS - Information Security Management System).	2	2	EU-K1, EU-U1, EU-U2, EU-U3, EU-W1, EU-W2

Razem godzin: 32

7. Metody kształcenia

Kod	Metoda
MK1	Wykład z wykorzystaniem prezentacji komputerowej.
MK2	Zachęcanie studentów do zadawania pytań na wykładzie i dyskusji na ćwiczeniach.
MK3	Podawanie przykładów i opracowanie przez studentów zadań projektowych na ćwiczeniach pod kierunkiem prowadzącego.
MK4	Samodzielne wykonanie przez studentów dokumentacji projektowej.
MK5	Podręczniki, strony internetowe, normy i materiały dydaktyczne zamieszczane w systemie informatycznym UBI.

8. Nakład pracy studenta

Aktywność studenta	Obciążenie
Przygotowanie do egzaminu	45
Samodzielne wykonanie projektów domowych	48
Praca z nauczycielem związana z: laboratorium	16
Praca z nauczycielem związana z: wykład	16
Liczba punktów ECTS (1 punkt=25h)	5
Procentowy udział pracy własnej studenta w sumarycznym obciążeniu studenta	74,40%
Sumaryczne obciążenie pracą studenta	125

9. Status zaliczenia przedmiotu

Forma studiów	Egzamin	Praca egzaminacyjna	Zaliczenie	Praca zaliczeniowa
niestacjonarne	×			

10. Metody weryfikacji efektów uczenia się

Składowe oceny końcowej

Forma sprawdzenia	Wybrana forma	Punktacja	Realizuje efekt
Egzamin pisemny	×	60	EU-W3, EU-W2, EU-W1, EU-U4, EU-U3, EU-U2, EU-U1
Egzamin ustny			
Sprawdzian pisemny			
Zaliczeniowy przegląd prac			
Referat pisemny			
Referat ustny			
Kolokwium			
Praca domowa			
Miniprojekt	×	30	EU-U4, EU-U3, EU-U2, EU-U1
Praca na zajęciach			
Projekt z dokumentacją			
Ustna prezentacja projektu			
Obecność na zajęciach			
Sprawdzian ustny			
Kartkówka			
Aktywność na zajęciach	×	10	EU-K1
Egzaminacyjny przegląd prac			
Sprawozdanie z praktyki zawodowej			
Prezentacja indywidualna			
Prezentacja zespołowa			

Zasady wyliczania oceny z przedmiotu

Zakres punktów	Ocena
0 – 50	2,0
51 – 60	3,0
61 – 70	3,5
71 – 80	4,0
81 – 90	4,5
91 – 100	5,0

11. Macierz realizacji przedmiotu

Efekt uczenia się	Cel przedmiotu	Treści programowe	Metody kształcenia
EU-W1	CP1	TP1, TP2, TP7, TP8	MK1, MK2, MK3, MK4, MK5
EU-W2	CP1	TP1, TP2, TP3, TP8	MK1, MK2, MK3, MK4, MK5
EU-W3	CP1	TP2, TP4, TP7	MK1, MK2, MK3, MK4, MK5
EU-U1	CP2	TP1, TP2, TP3, TP4, TP7, TP8	MK1, MK2, MK3, MK4, MK5
EU-U2	CP2	TP2, TP3, TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4, MK5
EU-U3	CP2	TP1, TP3, TP8	MK1, MK2, MK3, MK4, MK5
EU-U4	CP2	TP3, TP4, TP5, TP6, TP7	MK1, MK2, MK3, MK4, MK5
EU-K1	CP3	TP1, TP2, TP3, TP4, TP5, TP6, TP7, TP8	MK1, MK2, MK3, MK4, MK5

12. Odniesienie efektów uczenia się

Efekt uczenia się	Efekty kształcenia dla kierunku studiów	Charakterystyki drugiego stopnia w obszarze kształcenia
EU-W1	K1P_W01, K1P_W07, K1P_W06	P6S_WG
EU-W2	K1P_W01, K1P_W07, K1P_W06	P6S_WG
EU-W3	K1P_W07	P6S_WG
EU-U1	K1P_U06, K1P_U01	P6S_UW

Efekt uczenia się	Efekty kształcenia dla kierunku studiów	Charakterystyki drugiego stopnia w obszarze kształcenia
EU-U2	K1P_U06, K1P_U03, K1P_U01	P6S_UW
EU-U3	K1P_U06	P6S_UW
EU-U4	K1P_U08, K1P_U06	P6S_UW
EU-K1	K1P_K05	P6S_KO

13. Literatura

Literatura podstawowa

1. Andress J., Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie (ebook). , Helion, Gliwice 2022
2. Kowalewski M., Kowalewski J. , Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni. , Oficyna Wydawnicza PW, Warszawa 2017
3. Liderman K., Bezpieczeństwo informacyjne. Nowe wyzwania (ebook). , PWN, Warszawa 2018
4. Nelson S., Profesjonalne tworzenie kopii zapasowych i odzyskiwanie danych, Helion, Gliwice 2012
5. Stallings W., Brown L, Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 1. i Tom.2, Helion, Gliwice 2019

Literatura uzupełniająca

1. Cheswick W. R., Firewalle i bezpieczeństwo w sieci, Helion, Gliwice 2003
2. Ferguson N., Schneier B. , Kryptografia w praktyce, Helion, Gliwice 2004
3. Liderman K., Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa 2009
4. Liderman K., Bezpieczeństwo teleinformatyczne, WSISiZ, Warszawa 2003
5. Polaczek T., Audyt informacji bezpieczeństwa informacji w praktyce, Helion, Gliwice 2006
6. Serafin M., Sieci VPN. Zdalna praca i bezpieczeństwo danych, Helion, Gliwice 2008
7. Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Helion, Gliwice 2012

Pozostałe

1. Normy
2. Strony internetowe

14. Informacje o nauczycielach akademickich

Osoby odpowiedzialne za przedmiot

1. prof. Mirosław Siergiejczyk

Osoby prowadzące przedmiot

1. dr Artur Jagnieža
2. prof. Mirosław Siergiejczyk