KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo informacji

Przedmiot

Kierunek studiów

Inżynieria Bezpieczeństwa

Rok/semestr

2/4

Studia w zakresie (specjalność)

Profil studiów

ogólnoakademicki

Poziom studiów

pierwszego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

stacjonarne

Wymagalność

obligatoryjny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
15	15	
Ćwiczenia	Projekty/seminaria	

Liczba punktów ECTS

2

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr inż. Krzysztof Hankiewicz

krzysztof.hankiewicz@put.poznan.pl

telefon 61 665 3408

Wydział Inżynierii Zarządzania

ul. Jacka Rychlewskiego 2

60-965 Poznań

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student ma wiedzę o informacji, technologii informacyjnej, informatyce, zarządzaniu.

Student potrafi posługiwać się na bieżąco Internetem; potrafi zdobywać informacje, także w językach obcych studiowanych przez siebie na uczelni.

Student jest zdolny do nawiązywania kontaktów w światowym społeczeństwie informacyjnym.

Cel przedmiotu

Celem przedmiotu jest ukształtowanie u studentów rozumienia podstawowej wiedzy z zakresu bezpieczeństwa informacji oraz umiejętności wyboru środków bezpieczeństwa i ochrony informacji, a w

sumie - wykorzystanie tego wszystkiego dla swego intensywnego uczestnictwa w światowym społeczeństwie informacyjnym

Przedmiotowe efekty uczenia się

Wiedza

1. Zna współczesne trendy i najlepsze praktyki w ramach technik informacyjnych i informatycznych, a także wspomagających proces modelowania zagrożeń.

2. Zna współczesne trendy i najlepsze praktyki stosowane w celu zapewnienia bezpieczeństwa informacji oraz systemów bankowych.

3. Zna podstawowe techniki i narzędzia stosowane przy rozwiązywaniu prostych zadań inżynierskich z zastosowaniem technologii informacyjnych, ochrony informacji i wspomagania komputerowego.

4. Zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony prawa autorskiego, bezpieczeństwa informacji i ochrony własności intelektualnej w gospodarce rynkowej

Umiejętności

1. Potrafi pozyskiwać, integrować, interpretować informacje z literatury, baz danych oraz innych właściwie dobranych źródeł, także w języku angielskim lub innym języku obcym uznawanym za język komunikacji międzynarodowej w zakresie Inżynierii Bezpieczeństwa; a także wyciągać wnioski oraz formułować i uzasadniać opinie.

2. Potrafi zastosować różne techniki w celu porozumiewania się w środowisku zawodowym oraz w innych środowiskach.

3. Potrafi korzystać z technik chroniących informacje.

4. Potrafi zastosować techniki informacyjno-komunikacyjne do realizacji zadań typowych dla działalności inżynierskiej.

Kompetencje społeczne

1. Rozumie potrzebę i zna możliwości ciągłego dokształcania się (studia pierwszego, drugiego i trzeciego stopnia, studia podyplomowe, kursy) - podnoszenia kompetencji zawodowych, osobistych i społecznych; potrafi argumentować potrzebę uczenia się przez całe życie.

2. Ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko i związanej z tym odpowiedzialności za podejmowane decyzje.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu jest weryfikowana przez ocenę aktywności studentów na wykładach oraz jednego 45-minutowego kolokwium realizowanego na ostatnim wykładzie. Kolokwium składa się z 5-6 pytań otwartych. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania zostaną podane studentom podczas wykładów.

Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są na podstawie wykonanych zadań.

Treści programowe

Terminologia i klasyfikacja tajemnic. Podstawy prawne w ochronie informacji, tajemnice prawnie chronione. Podstawowe moduły w zarządzaniu bezpieczeństwem informacji. Polityka bezpieczeństwa informacji. Wytwarzanie, przetwarzanie i przechowywanie dokumentów w systemach teleinformatycznych. Zasady udostępniania informacji - zagrożenia i mankamenty. Zabezpieczenia i wymagania w zakresie ochrony informacji. Administracyjne, techniczne i fizyczne bezpieczeństwo danych.

Metody dydaktyczne

1. Wykład: prezentacja multimedialna, ilustrowana przykładami.

2. Ćwiczenia laboratoryjne: zadania praktyczne wykonywane przez studentów w oparciu o podane instrukcje.

Literatura

Podstawowa

1. Stokłosa J. i innni, Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Wydawnictwo Politechniki Poznańskiej 2003

2. Anderson R., Inżynieria zabezpieczeń, Wydawnictwo Naukowo - Techniczne 2005

3. PN-EN ISO/IEC 27002:2017-06, Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji. PKN, 2018

4. PN-EN ISO/IEC 27001:2017-06, Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania, PKN, 2018

Uzupełniająca

1. Liderman K., Bezpieczeństwo informacyjne, Wydawnictwo Naukowe PWN, 2017

2. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. nr 133, poz. 883)

3. Ustawa z dnia 5 sierpni 2010 r. o ochronie informacji niejawnych (Dz. U. nr 182, poz. 1228)

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	60	2
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, przygotowanie do kolokwium)	30	1