Bezpieczeństwo systemów informatycznych i ochrona danych - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Bezpieczeństwo systemów informatycznych i ochrona danych
Kod przedmiotu	11.3-WK-IDP-BSIOD-P-S14_pNadGenSAUUV
Wydział	Wydział Matematyki, Informatyki i Ekonometrii
Kierunek	Inżynieria danych
Profil	ogólnoakademicki
Rodzaj studiów	pierwszego stopnia z tyt. inżyniera
Semestr rozpoczęcia	semestr zimowy 2017/2018

Informacje o przedmiocie

Semestr	5
Liczba punktów ECTS do zdobycia	6
Typ przedmiotu	obowiązkowy
Język nauczania	polski
Sylabus opracował	• dr inż. Janusz Jabłoński

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Projekt	15	1	-	-	Zaliczenie na ocenę
Laboratorium	30	2	-	-	Zaliczenie na ocenę
Wykład	30	2	-	-	Egzamin

Cel przedmiotu

Celem kursu jest zapoznanie studentów z podstawowymi definicjami oraz zagrożeniami bezpieczeństwa danych i systemów informatycznych. Zapoznanie studentów z metodami technikami i narzędziami zapobiegania przełamywaniu atrybutów bezpieczeństwa danych i systemów. Przygotowanie studentów do samodzielnego rozpoznania zagrożeń i zaproponowania efektywnego i bezpiecznego rozwiązania.

Wymagania wstępne

Student powinien zaliczyć kurs: Podstawy programowania.

Zakres tematyczny

Wykład/laboratorium/projekt:

- Zagrożenia systemów informatycznych: poufność, integralność dostępność
- Prawne i normalizacyjne uwarunkowania ochrony danych.
- Prawne uwarunkowania ochrona własności intelektualnej
- Praktyczne aspekty wykorzystania kryptografii i krypto-analiza.
- Modele i klasy bezpieczeństwa systemów informatycznych.
- Najczęstsze zagrożenia bezpieczeństwa protokołów i systemów teleinformatycznych
- Prawo telekomunikacyjne i ustawa o podpisie cyfrowym.
- Definiowanie polityki bezpieczeństwa.
- Podpis elektroniczny i infrastruktura klucza publicznego.
- Praktyczne metody zabezpieczania danych i systemów informatycznych.

Metody kształcenia

Wykład dostępny w formie elektronicznej; laboratoria komputerowe na których studenci realizują i analizują (na praktycznych przykładach) zagadnienia pokazujące mechanizmy i metody najczęściej występujących zagrożeń oraz metod eliminowania niebezpieczeństwa. Projekt będący opracowaniem i przedstawieniem rozwiązania jednego z możliwych zagrożeń bezpieczeństwa danych, aplikacji lub usług WEB z uwzględnieniem Cloud Computing.

Efekty kształcenia i metody weryfikacji osiągania efektów kształcenia

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Student rozumie i ma świadomość ważności technicznych oraz pozatechnicznych aspektów i skutków działalności inżyniera i związanej z tym odpowiedzialności za podejmowane decyzje	• K_K07	• Dyskusja w trakcie zajęć.	• Wykład • Laboratorium
Student zna podstawowe pojęcia z zakresu ochrony własności intelektualnej oraz prawa patentowego, rozumie społeczne aspekty informatyki oraz uwarunkowania etyczno prawne i ekonomiczne związane z zawodem analityka i informatyka.	• K_W16	• Egzamin pisemny. Kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym. Sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.	• Wykład • Laboratorium
Student zna podstawowe pojęcia z zakresu bezpieczeństwa danych i systemów informatycznych oraz ma podstawową wiedzę na temat ich znaczenia w rozwoju społeczeństwa informacyjnego	• K_W01	• Egzamin pisemny. Kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym. Sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.	• Wykład • Laboratorium
Student zna podstawowe pojęcia z zakresu technologii sieciowych, w tym architektury sieci komputerowych, protokołów komunikacyjnych, bezpieczeństwa i budowy aplikacji sieciowych oraz zna podstawowe zasady bezpieczeństwa i higieny pracy przy komputerze w sieci komputerowej.	• K_W15 • K_W17	• Egzamin pisemny. Kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym. Sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.	• Wykład • Laboratorium
Student w podstawowym zakresie potrafi ocenić przydatność metod i narzędzi matematycznych i informatycznych jak również ocenić i zastosować właściwą metodę i narzędzia bezpieczeństwa.	• K_U23	• Praktyczne przykłady implementacyjne i obliczeniowe oraz kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym. Ocena sprawozdań oraz sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.	• Wykład • Laboratorium
Student potrafi dbać o elementarne bezpieczeństwo danych i sieci komputerowych	• K_U26	• Praktyczne przykłady implementacyjne i obliczeniowe oraz kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym. Ocena sprawozdań oraz sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.	• Wykład • Laboratorium
Rozumie potrzebę ciągłego podnoszenia swoich kwalifikacji poprzez poszerzanie swojej wiedzy i umiejętności w zakresie ochrony danych i systemów informatycznych; rozumie i docenia znaczenie uczciwości intelektualnej w działaniach własnych i innych osób; postępuje etycznie	• K_K01 • K_K04	• Egzamin pisemny. Kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym. Sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.	• Wykład • Laboratorium
Student rozumie etyczne, prawne i społeczne aspekty informatyzacji i umie przestrzegać w swojej działalności zawodowej odnoszące się do nich zasady .	• K_K05	• Dyskusja w trakcie zajęć.	• Wykład • Laboratorium

Warunki zaliczenia

Egzamin z wykładu. Zaliczenie laboratorium na podstawie sprawdzianów (20%) oraz sprawozdań ze zrealizowanych przykładowych zadań (80%).

Projekt zaliczany na podstawie opracowania wybranego zagadnienia z zakresu bezpieczeństwa systemów informatycznych (40%) z przykładem prezentującym możliwe zabezpieczenie (60%).

Na ocenę z przedmiotu składa się ocena z wykładu (35%) laboratorium (35%) oraz projektu (30%). Warunkiem zaliczenia przedmiotu jest uzyskanie zaliczenia z wykładu laboratorium oraz projektu.

Obciążenie pracą

Obciążenie pracą	Studia stacjonarne (w godz.)	Studia niestacjonarne (w godz.)

Godziny kontaktowe (udział w zajęciach; konsultacjach; egzaminie, itp.)	85	-
Samodzielna praca studenta (przygotowanie do: zajęć, kolokwium, egzaminu; studiowanie literatury przygotowanie: pracy pisemnej, projektu, prezentacji, raportu, wystąpienia; itp.)	75	-
Łącznie	**160**	**-**

Punkty ECTS	**Studia stacjonarne**	**Studia niestacjonarne**
Zajęcia z udziałem nauczyciela akademickiego	3	-
Zajęcia bez udziału nauczyciela akademickiego	3	-
Łącznie	**6**	**-**

Literatura podstawowa

1. N. Ferguson, B. Schneier, Kryptografia w praktyce., Helion, 2004
2. J. Stokłosa, T. Bliski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych.* PWN, Warszawa, 2001;
3. W. Stallings, Cryptography and network security, Prentice Hall, USA 2011;
4. W. R. Cheswick. *Firewalle i bezpieczeństwo w sieci*. Helion, Gliwice, 2003;

Literatura uzupełniająca

1. B. Hoffman, B. Sullivan, Bezpieczeństwo aplikacji tworzonych w technologii Ajax, Helion, Gliwice, 2009;
2. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Helion, Gliwice, 2012;
3. L. Kępa, P. Tomasik, S. Dobrzyński, Bezpieczeństwo systemu e-commerce, czyli jak bez ryzyka prowadzić biznes w internecie, Helion, Gliwice, 2012.

Uwagi

Zmodyfikowane przez dr Robert Dylewski (ostatnia modyfikacja: 09-04-2017 16:27)