

# 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             | <a href="#">Wydział Matematyki, Informatyki i Ekonometrii</a> |
| Kierunek            | Inżynieria danych                                             |
| Profil              | ogólnoakademicki                                              |
| Rodzaj studiów      | pierwszego stopnia z tyt. inżyniera                           |
| Semestr rozpoczęcia | semestr zimowy 2020/2021                                      |

| Informacje o przedmiocie        |                                                                          |
|---------------------------------|--------------------------------------------------------------------------|
| Semestr                         | 5                                                                        |
| Liczba punktów ECTS do zdobycia | 6                                                                        |
| Typ przedmiotu                  | obowiązkowy                                                              |
| Język nauczania                 | polski                                                                   |
| Sylabus opracował               | <ul style="list-style-type: none"><li>dr inż. Janusz Jabłoński</li></ul> |

| 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 przełamaniu 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 uczenia się i metody weryfikacji osiągnięcia efektów uczenia się

| Opis efektu | Symbole efektów | Metody weryfikacji | Forma zajęć |
|-------------|-----------------|--------------------|-------------|
|-------------|-----------------|--------------------|-------------|

| Opis efektu                                                                                                                                                                                                                                                                       | Symbole efektów                                                                                            | Metody weryfikacji                                                                                                                                                                                                                                                                                                                                                         | Forma zajęć                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 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   | <ul style="list-style-type: none"> <li>• <a href="#">K_K01</a></li> <li>• <a href="#">K_K04</a></li> </ul> | <ul style="list-style-type: none"> <li>• Egzamin pisemny.</li> <li>Kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym.</li> <li>Sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.</li> </ul>                                                      | <ul style="list-style-type: none"> <li>• Wykład</li> <li>• Laboratorium</li> </ul> |
| Student rozumie etyczne, prawne i społeczne aspekty informatyzacji i umie przestrzegać w swojej działalności zawodowej odnoszące się do nich zasady .                                                                                                                             | <ul style="list-style-type: none"> <li>• <a href="#">K_K05</a></li> </ul>                                  | <ul style="list-style-type: none"> <li>• Dyskusja w trakcie zajęć.</li> </ul>                                                                                                                                                                                                                                                                                              | <ul style="list-style-type: none"> <li>• Wykład</li> <li>• Laboratorium</li> </ul> |
| Student rozumie i ma świadomość ważności technicznych oraz pozatechnicznych aspektów i skutków działalności inżyniera i związanej z tym odpowiedzialności za podejmowane decyzje                                                                                                  | <ul style="list-style-type: none"> <li>• <a href="#">K_K07</a></li> </ul>                                  | <ul style="list-style-type: none"> <li>• Dyskusja w trakcie zajęć.</li> </ul>                                                                                                                                                                                                                                                                                              | <ul style="list-style-type: none"> <li>• Wykład</li> <li>• Laboratorium</li> </ul> |
| 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.                                               | <ul style="list-style-type: none"> <li>• <a href="#">K_W16</a></li> </ul>                                  | <ul style="list-style-type: none"> <li>• Egzamin pisemny.</li> <li>Kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym.</li> <li>Sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.</li> </ul>                                                      | <ul style="list-style-type: none"> <li>• Wykład</li> <li>• Laboratorium</li> </ul> |
| Student zna podstawowe pojęcia z zakresu bezpieczeństwa danych i systemów informatycznych oraz ma podstawową wiedzę na temat ich znaczenia w rozwoju społeczeństwa informacyjnego                                                                                                 | <ul style="list-style-type: none"> <li>• <a href="#">K_W01</a></li> </ul>                                  | <ul style="list-style-type: none"> <li>• Egzamin pisemny.</li> <li>Kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym.</li> <li>Sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.</li> </ul>                                                      | <ul style="list-style-type: none"> <li>• Wykład</li> <li>• Laboratorium</li> </ul> |
| 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. | <ul style="list-style-type: none"> <li>• <a href="#">K_W15</a></li> <li>• <a href="#">K_W17</a></li> </ul> | <ul style="list-style-type: none"> <li>• Egzamin pisemny.</li> <li>Kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym.</li> <li>Sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.</li> </ul>                                                      | <ul style="list-style-type: none"> <li>• Wykład</li> <li>• Laboratorium</li> </ul> |
| Student w podstawowym zakresie potrafi ocenić przydatność metod i narzędzi matematycznych i informatycznych jak również ocenić i zastosować właściwą metodę i narzędzia bezpieczeństwa.                                                                                           | <ul style="list-style-type: none"> <li>• <a href="#">K_U23</a></li> </ul>                                  | <ul style="list-style-type: none"> <li>• Praktyczne przykłady implementacyjne i obliczeniowe oraz kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym.</li> <li>Ocena sprawozdań oraz sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.</li> </ul> | <ul style="list-style-type: none"> <li>• Wykład</li> <li>• Laboratorium</li> </ul> |
| Student potrafi dbać o elementarne bezpieczeństwo danych i sieci komputerowych                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• <a href="#">K_U26</a></li> </ul>                                  | <ul style="list-style-type: none"> <li>• Praktyczne przykłady implementacyjne i obliczeniowe oraz kolokwia z zadaniami o zróżnicowanym stopniu trudności, pozwalającymi na ocenę, czy student osiągnął efekty kształcenia w stopniu minimalnym.</li> <li>Ocena sprawozdań oraz sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie zajęć.</li> </ul> | <ul style="list-style-type: none"> <li>• Wykład</li> <li>• Laboratorium</li> </ul> |

## 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.

## 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 Alina Szelecka (ostatnia modyfikacja: 08-06-2020 10:09)

Wygenerowano automatycznie z systemu SylabUZ