



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo analiz Big Data [S2Inf1E-CYB>BDA]

Przedmiot

Kierunek studiów

Informatyka/Computing

Rok/Semestr

1/2

Studia w zakresie (specjalność)

Cyberbezpieczeństwo

Profil studiów

ogólnoakademicki

Poziom studiów

drugiego stopnia

Język oferowanego przedmiotu

angielski

Forma studiów

stacjonarne

Wymagalność

obligatoryjny

Liczba godzin

Wykład

15

Laboratorium

30

Inne

0

Ćwiczenia

0

Projekty/seminaria

0

Liczba punktów ECTS

2,00

Koordynatorzy

dr inż. Michał Weissenberg

michal.weissenberg@put.poznan.pl

dr hab. inż. Sławomir Hanczewski

slawomir.hanczewski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student powinien posiadać wiedzę z zakresu budowy i działania systemów komputerowych obejmujących zarówno urządzenia jak i protokoły. Powinien także rozumieć potrzebę poszerzania swoich kompetencji oraz posiadać umiejętność pozyskiwania informacji z określonych źródeł.

Cel przedmiotu

Przedstawienie teoretycznych i praktycznych zagadnień związanych z bezpieczeństwem analizy Big Data.

Przedmiotowe efekty uczenia się

Wiedza:

student posiada zaawansowaną i szczegółową wiedzę z zakresu szeroko rozumianego bezpieczeństwa analizy big data. student posiada wiedzę na temat trendów rozwojowych w zakresie big data, ai oraz bezpieczeństwa big data

Umiejętności:

student potrafi pozyskiwać informacje o bezpieczeństwie dużych zbiorów danych z literatury, baz danych oraz innych źródeł (zarówno w języku polskim jak i angielskim). student potrafi również integrować wiedzę na temat analizy big data i jej bezpieczeństwa oraz potrafi ocenić przydatność metod i narzędzi dla zapewnienia bezpieczeństwa big data. potrafi też współdziałać w zespole, przyjmując w nim różne role i wyznaczać kierunki dalszej nauki

Kompetencje społeczne:

student rozumie, że w zakresie bezpieczeństwa big data wiedza i umiejętności szybko się dezaktualizują. rozumie również, jak ważne jest korzystanie z najnowszej wiedzy.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza zdobyta na wykładach weryfikowana jest na zaliczeniu, które w zależności od wielkości grupy ma formę pisemną lub ustną. Zaliczenie pisemne składa się z 30 pytań testowych, na które proponuje się 4 odpowiedzi, ale tylko jedna odpowiedź jest prawidłowa. Próg zaliczenia egzaminu to 50%. Zagadnienia końcowe, na podstawie których przygotowywane są pytania, zostaną rozesłane do studentów pocztą elektroniczną z wykorzystaniem uczelnianego systemu poczty elektronicznej. W przypadku zaliczenia ustnego każdy student odpowiada na trzy pytania z zestawu 40 (są one znane studentom). Pytania zadaje prowadzący zaliczenie. Oceniana jest poprawność odpowiedzi oraz stopień zrozumienia problemu przez studenta.

Wiedza i umiejętności nabyte podczas ćwiczeń laboratoryjnych są weryfikowane poprzez sprawdzenie poprawności ćwiczenia. Brak zaliczenia ćwiczenia powoduje konieczność powtórzenia go w wyznaczonym przez prowadzącego terminie.

Treści programowe

Wykłady i ćwiczenia laboratoryjne poświęcone są problematyce bezpieczeństwa przetwarzania dużych zbiorów danych.

Tematyka zajęć

Wykłady:

1. Wprowadzenie do Big Data
(Big Data - co to jest?, charakterystyka danych, przechowywanie danych, przetwarzanie danych, wartość danych w zastosowaniach biznesowych, społecznych i środowiskowych)
2. Podstawy analizy Big Data
3. Sztuczna inteligencja wykorzystywana do analizy Big Data
4. Wykorzystanie Pythona w przetwarzaniu dużych zbiorów danych
(wprowadzenie do Pythona, biblioteki)
5. Bezpieczeństwo w nowoczesnych systemach teleinformatycznych
6. Wprowadzenie do bezpieczeństwa Big Data
7. Bezpieczeństwo Internetu Rzeczy
8. Dobre praktyki w zakresie bezpieczeństwa systemów Big Data
9. Problemy z zestawami Big Data
10. Problemy z algorytmami analizy Big Data
11. Monitorowanie procesu analizy Big Data

Ćwiczenia laboratoryjne

Tematyka ćwiczeń laboratoryjnych obejmuje pięć bloków:

1. Przygotowanie środowiska analitycznego Big Data
2. Głębokie uczenie w Big Data
3. Problemy z analizą Big Data
4. Bezpieczeństwo algorytmów analizy Big Data
5. Monitorowanie procesu analizy Big Data

Metody dydaktyczne

Wykład: prezentacja multimedialna uzupełniona przykładami i dodatkowymi objaśnieniami na tablicy. Wykłady prowadzone są zgodnie z zasadami wykładu tradycyjnego, w uzasadnionych przypadkach w formie wykładu konwersacyjnego.

Ćwiczenia laboratoryjne: prezentacja multimedialna, prezentacja ilustrowana przykładami podanymi na tablicy oraz wykonanie zadań podanych przez prowadzącego - ćwiczenia praktyczne.

Literatura

Podstawowa

1. Onur Savas, Julia Deng, "Big Data Analytics in Cybersecurity", Taylor & Francis Limited, 2021

2. Mostapha Zbakh, Mohamed Essaaidi, Pierre Manneback, Chunming Rong, "Cloud Computing and Big Data: Technologies, Applications and Security", Springer 2019

Uzupełniająca

Serwisy poświęcone Big Data, serwisy dostawców rozwiązań Big Data

Bilans nakładu pracy przeciętnego studenta

| | Godzin | ECTS |
|---|--------|------|
| Łączny nakład pracy | 50 | 2,00 |
| Zajęcia wymagające bezpośredniego kontaktu z nauczycielem | 45 | 1,50 |
| Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwii/egzaminu, wykonanie projektu) | 5 | 0,50 |