KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo analizy Big Data

Przedmiot

Kierunek studiów
Informatyka

Rok/semestr
1/2

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
15	30	0
Ćwiczenia	Projekty/seminaria	
0	0	

Liczba punktów ECTS

4

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr hab. inż. Sławomir Hanczewski,

slawomir.hanczewski@put.poznan.pl

tel. 61 665 3921

Wydział Informatyki i Telekomunikacji

ul. Piotrowo 3 60-965 Poznań

Odpowiedzialny za przedmiot/wykładowca:
mgr inż. Michał Weissenberg,

slawomir.hanczewski@put.poznan.pl

tel. 61 665 3946

Wydział Informatyki i Telekomunikacji

ul. Piotrowo 3 60-965 Poznań

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 egzaminie, który w zależności od wielkości grupy ma formę pisemną lub ustną. Egzamin pisemny 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 egzaminu ustnego każdy student odpowiada na trzy pytania z zestawu 40 (są one znane studentom). Pytania zadaje prowadzący egzamin. 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:

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

. 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	100	4,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2,0
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)[1]	55	2,0

[1] niepotrzebne skreślić lub dopisać inne czynności