



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Infrastruktura i usługi chmur obliczeniowych [S2Teleinf2-SzliUM>IU]

Przedmiot

Kierunek studiów
Teleinformatyka

Rok/Semestr
1/2

Studia w zakresie (specjalność)
Sztuczna inteligencja i uczenie maszynowe

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
14

Laboratorium
24

Inne
14

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

dr hab. inż. Remigiusz Rajewski
remigiusz.rajewski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student ma podstawową wiedzę o sieciach teleinformatycznych (topologie sieci, architektury węzłów teleinformatycznych) i o protokołach używanych w sieciach teleinformatycznych. Ponadto student zna język angielski na poziomie umożliwiającym pozyskiwanie informacji z literatury angielskojęzycznej (książki, dane katalogowe, instrukcje, rekomendacje, itp.). Student powinien posiadać umiejętność odczytywania z literatury angielskojęzycznej (książki, rekomendacje, instrukcje, dane katalogowe) danych technicznych i wytycznych potrzebnych do właściwej konfiguracji urządzeń w sieci teleinformatycznej. Dodatkowo student powinien posiadać umiejętność używania różnych metod optymalizacji do rozwiązywania problemów w sieciach teleinformatycznych. Student powinien znać ograniczenia swojej wiedzy i umiejętności, oraz powinien rozumieć potrzebę swojej przyszłej edukacji.

Cel przedmiotu

Celem nauczania przedmiotu jest zaznajomienie studentów z tematyką chmury obliczeniowej, sposobem jej konfiguracji, świadczeniem różnych usług, przechowywaniem i przetwarzaniem danych użytkowników oraz bezpieczeństwem chmury obliczeniowej.

Przedmiotowe efekty uczenia się

Wiedza:

1. Zna metody symulacyjne i sposoby symulacji ruchu w sieciach teleinformatycznych [K2_W01].
2. Zna protokoły oraz narzędzia wykorzystywane w chmurach obliczeniowych [K2_W05].
3. Zna sposoby przechowywania informacji w chmurze z uwzględnieniem aspektów bezpieczeństwa danych użytkowników.
4. Zna architektury chmur obliczeniowych oraz metody ich konfiguracji.

Umiejętności:

1. Potrafi odczytywać dane z książek, rekomendacji, katalogów producenckich, instrukcji, itp. celem ich analizy i wykorzystania w aplikacjach serwerowych i klienckich dla chmur obliczeniowych [K2_U01].
2. Potrafi pisać programy konsolowe i aplikacje obiektowe w środowiskach programistycznych do obsługi strony klienckiej i serwerowej dla chmur obliczeniowych [K2_U07].
3. Potrafi przewidywać jakie skutki niesie niewłaściwa ochrona wrażliwych danych użytkowników w chmurze obliczeniowej.
4. Potrafi samodzielnie pozyskiwać nową wiedzę, odczytywać rekomendacje i wytyczne konfiguracyjne [K2_U10].

Kompetencje społeczne:

1. Wie, że musi uaktualniać co jakiś czas swoją wiedzę aby być na bieżąco [K2_K01].

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Warunkiem zaliczenia przedmiotu jest zaliczenie poszczególnych jego części: kolokwium zaliczeniowe z części wykładowej oraz kolokwium końcowe z laboratoriów.

Przyjęto następującą skalę ocen:

- bardzo dobry (A) - 5.0;
- dobry plus (B) - 4.5;
- dobry (C) - 4.0;
- dostateczny plus (D) - 3.5;
- dostateczny (E) - 3.0;
- niedostateczny (F) - 2.0.

Ocena formująca:

- Ocena formująca na wykładach: odpowiedź ustna albo test wielokrotnego wyboru zaliczony po uzyskaniu powyżej 50% wszystkich możliwych punktów.
- Ocena formująca na laboratoriach: bazuje w 5% na aktywności studenta na zajęciach, 15% oddanych sprawozdaniach oraz w 80% na kolokwium końcowym. Kolokwium końcowe może mieć formę ustną lub pisemną.

Ocena podsumowująca:

- Warunkiem uzyskania pozytywnej oceny końcowej z wykładów jest uzyskanie powyżej 50% wszystkich możliwych punktów z kolokwium zaliczeniowego. Kolokwium może mieć formę ustną lub pisemną (w zależności od ilości studentów na roku). W przypadku przeprowadzania kolokwium zaliczeniowego w postaci pisemnej, będzie ono mieć w zdecydowanej większości formę testu wielokrotnego wyboru z opcjonalnie możliwymi pytaniami opisowymi. Ocena końcowa z wykładów zależy od całkowitej liczby zdobytych punktów z kolokwium zaliczeniowego albo z odpowiedzi ustnej. Procent uzyskanych punktów z zaliczenia końcowego przekłada się na ocenę końcową z wykładów w następujący sposób:
 - >93% - 100% 5.0 (bdb)
 - >85% - 93% 4.5 (db+)
 - >76% - 85% 4.0 (db)
 - >65% - 76% 3.5 (dst+)
 - >50% - 65% 3.0 (dst)
 - >0% - 50% 2.0 (ndst)
- Ocena końcowa z laboratoriów zależy w zdecydowanej większości od ilości zdobytych punktów z kolokwium końcowego oraz od ilości punktów zdobytych z oddanych terminowo sprawozdań. Sprawozdania oddane po wyznaczonym przez prowadzącego terminie mają automatycznie przypisane z pierwszego podejścia ujemne punkty równe połowie maksymalnej ilości możliwych punktów. Sprawozdania można poprawiać ale jedynie do wyznaczonego przez prowadzącego terminu. Pozytywna ocena końcowa z laboratoriów obowiązuje jedynie w przypadku, gdy student uzyska z każdej ze składowych częściowych (czyli z kolokwium końcowego oraz ze sprawozdań) niezależnie ponad 50%

możliwych punktów (czyli ponad 50% możliwych punktów ze sprawozdań oraz ponad 50% możliwych punktów z kolokwium końcowego). Kolokwium końcowe może mieć formę ustną albo pisemną (w zależności od ilości osób na roku). Informacja, jaka forma kolokwium obowiązuje w danym roku jest podawane do wiadomości studentów na zajęciach organizacyjnych (czyli pierwsze zajęcia w semestrze). Procentowo ocena końcowa z laboratorium kształtuje się następująco:

- >93% - 100% 5.0 (bdb)
- >85% - 93% 4.5 (db+)
- >76% - 85% 4.0 (db)
- >65% - 76% 3.5 (dst+)
- >50% - 65% 3.0 (dst)
- >0% - 50% 2.0 (ndst)

Treści programowe

1. Wprowadzenie (3 godz.)

Organizacja i plan zajęć. Warunki uzyskania zaliczenia. Podstawowe informacje na temat rodzaju sieci teleinformatycznych i umiejscowienia chmur obliczeniowych. Rys historyczny. Wpływ rozwoju cywilizacyjnego na sposób pracy z danymi, ich obróbką oraz ich przechowywanie. Tendencje i zmiany podejścia w pracowaniu z danymi użytkowników oraz ich przechowywanie.

2. Podstawowe pojęcia i modele (2 godz.)

Cechy charakterystyczne wspólne dla większości środowisk chmurowych. Przegląd różnych modeli dostarczania i wdrażania w chmurze obliczeniowej.

3. Technologie umożliwiające przetwarzanie w chmurze (4 godz.)

Sieci szerokopasmowe i architektura internetowa. Technologia wirtualizacji. Technologia sieci. Technologia wielodostępu. Technologia usług. Przykłady Data Center.

4. Mechanizmy infrastruktury chmury obliczeniowej (2 godz.)

Obwód sieci logicznej. Serwer wirtualny. Urządzenia pamięci masowej w chmurze. Monitor wykorzystania chmury. Replikacja zasobów. Gotowe środowiska chmurowe.

5. Zasady bezpieczeństwa (2 godz.)

Podstawowe nazewnictwo i koncepcje. Agenci zagrożeń. Zagrożenia dla bezpieczeństwa w chmurze.

6. Mechanizmy bezpieczeństwa w chmurze (2 godz.)

Szyfrowanie. Haszowanie. Podpis cyfrowy. Infrastruktura klucza publicznego. Zarządzanie tożsamością i dostępem. Logowanie jednokrotne. Grupy bezpieczeństwa oparte na chmurze. Wzmocnione obrazy wirtualnego serwera.

Tematyka zajęć

1. Wprowadzenie (3 godz.)

Organizacja i plan zajęć. Warunki uzyskania zaliczenia. Podstawowe informacje na temat rodzaju sieci teleinformatycznych i umiejscowienia chmur obliczeniowych. Rys historyczny. Wpływ rozwoju cywilizacyjnego na sposób pracy z danymi, ich obróbką oraz ich przechowywanie. Tendencje i zmiany podejścia w pracowaniu z danymi użytkowników oraz ich przechowywanie.

2. Podstawowe pojęcia i modele (2 godz.)

Cechy charakterystyczne wspólne dla większości środowisk chmurowych. Przegląd różnych modeli dostarczania i wdrażania w chmurze obliczeniowej.

3. Technologie umożliwiające przetwarzanie w chmurze (4 godz.)

Sieci szerokopasmowe i architektura internetowa. Technologia wirtualizacji. Technologia sieci. Technologia wielodostępu. Technologia usług. Przykłady Data Center.

4. Mechanizmy infrastruktury chmury obliczeniowej (2 godz.)

Obwód sieci logicznej. Serwer wirtualny. Urządzenia pamięci masowej w chmurze. Monitor wykorzystania chmury. Replikacja zasobów. Gotowe środowiska chmurowe.

5. Zasady bezpieczeństwa (2 godz.)

Podstawowe nazewnictwo i koncepcje. Agenci zagrożeń. Zagrożenia dla bezpieczeństwa w chmurze.

6. Mechanizmy bezpieczeństwa w chmurze (2 godz.)

Szyfrowanie. Haszowanie. Podpis cyfrowy. Infrastruktura klucza publicznego. Zarządzanie tożsamością i dostępem. Logowanie jednokrotne. Grupy bezpieczeństwa oparte na chmurze. Wzmocnione obrazy wirtualnego serwera.

Metody dydaktyczne

Wykład: prezentacja multimedialna, możliwe dodatkowe przykłady pokazywane w przeglądarce

internetowej.

Laboratorium: wprowadzenie do danych ćwiczeń, w zależności od tematu zajęć, może być poprzedzone prezentacją multimedialną i/lub przykładami podanymi przez prowadzącego w przeglądarce internetowej. Każde ćwiczenie laboratoryjne posiada instrukcję lub tutorial na stronie producenta oprogramowania lub dostawcy serwisów chmurowych. Niektóre instrukcje zawierają również dodatkowe pytania dotyczące studiowanych zagadnień.

Literatura

Podstawowa:

1. N. K. Sehgal, P. Ch. P. Bhatt: Cloud Computing: Concept and Practices, Springer, 2018.
2. K. L. Jackson: Architecting Cloud Computing Solutions, Packt Publishing, 2018.
3. N. B. Ruparelia: Cloud Computing, The MIT Press, 2016.
4. R. Rafaels: Cloud Computing: From Beginning to End, CreateSpace Independent Publishing Platform, 2015.
5. M. J. Kavis: Architecting the Cloud, Willey, 2014.

Uzupełniająca:

1. T. Erl, R. Cope, A. Naserpour: Cloud Computing Design Patterns, Prentice Hall, 2015.
2. A. Bahga, V. Madisetti: Cloud Computing: A Hands-On Approach, CreateSpace Independent Publishing Platform, 2013.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	78	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	38	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	40	1,50