



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Podstawy usług i aplikacji chmurowych [S1Cybez1>PUiAC]

Przedmiot

Kierunek studiów

Cyberbezpieczeństwo

Rok/Semestr

2/4

Studia w zakresie (specjalność)

–

Profil studiów

ogólnoakademicki

Poziom studiów

pierwszego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

stacjonarne

Wymagalność

obligatoryjny

Liczba godzin

Wykład

16

Laboratorium

16

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. Mariusz Żal

mariusz.zal@put.poznan.pl

Wykładowcy

Wymagania wstępne

• Podstawowa znajomość zagadnień sieci komputerowych (protokoły, model OSI/TCP-IP). • Umiejętność korzystania z systemów operacyjnych (Windows, Linux) w zakresie instalacji oprogramowania i podstawowych poleceń sieciowych. • Podstawowa wiedza z zakresu wirtualizacji i/lub rozwiązań serwerowych. • Podstawowe umiejętności programowania w dowolnym języku (Python, C, Java).

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z fundamentalnymi zasadami działania chmur obliczeniowych, technikami wirtualizacji oraz projektowaniem aplikacji i usług w rozproszonym środowisku chmurowym. Studenci nauczą się korzystać z platform chmurowych (AWS, Azure, Google Cloud), konfigurować usługi obliczeniowe i sieciowe oraz wdrażać aplikacje o wysokiej dostępności i skalowalności. Szczególny nacisk zostanie położony na zagadnienia bezpieczeństwa w chmurze oraz automatyzacji wdrożeń i monitorowania aplikacji. Kurs przygotuje studentów do efektywnej pracy z nowoczesnymi technologiami chmurowymi oraz projektowania aplikacji IoT w środowiskach chmurowych.

Przedmiotowe efekty uczenia się

Wiedza:

- Rozumie podstawowe pojęcia i modele przetwarzania w chmurze (IaaS, PaaS, SaaS) oraz modele wdrożeń (chmura publiczna, prywatna, hybrydowa). [K1_W14]
- Zna podstawowe usługi obliczeniowe, sieciowe i bazodanowe oferowane przez wiodące platformy chmurowe (AWS, Azure, Google Cloud). [K1_W14]
- Rozumie architekturę chmur obliczeniowych, w tym koncepcje konteneryzacji oraz mikroserwisów. [K1_W07]
- Zna techniki zapewniania bezpieczeństwa w środowiskach chmurowych, w tym mechanizmy autentykacji, szyfrowania i kontroli dostępu. [K1_W14]
- Rozumie zasady skalowania aplikacji w chmurze oraz zapewniania wysokiej dostępności i niezawodności. [K1_W14]

Umiejętności:

- Potrafi skonfigurować środowisko chmurowe oraz uruchomić i zarządzać maszynami wirtualnymi i kontenerami. [K1_U02]
- Umie wdrażać aplikacje webowe w modelu IaaS i PaaS, konfigurować usługi sieciowe oraz zarządzać bazami danych w chmurze. [K1_U10]
- Potrafi zaprojektować i wdrożyć aplikację IoT w środowisku chmurowym, wykorzystując narzędzia do zarządzania cyklem życia aplikacji. [K1_U06]
- Umie stosować narzędzia do automatyzacji wdrożeń i monitorowania aplikacji, takie jak CI/CD, Docker Swarm i Kubernetes. [K1_U04]
- Potrafi optymalizować koszty korzystania z chmury oraz monitorować wydajność aplikacji. [K1_U08]

Kompetencje społeczne:

- Rozumie znaczenie chmur obliczeniowych we współczesnym IT oraz potrafi świadomie korzystać z technologii chmurowych, dbając o bezpieczeństwo i zgodność z regulacjami. [K1_K05]
- Potrafi pracować w zespołach projektowych, komunikując efektywnie wyniki swojej pracy oraz problemy i rozwiązania. [K1_K05]
- Jest świadomy konieczności stałego rozwoju i śledzenia trendów w dziedzinie chmur obliczeniowych. [K1_K01]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

1. Wiedza: test pisemny z pytaniami dotyczącymi usług i aplikacji chmurowych. Minimalny próg zaliczeniowy 50% sumy wszystkich możliwych punktów.
2. Umiejętności: bieżąca ocena realizacji zadań laboratoryjnych. Minimalny próg zaliczeniowy 50% sumy wszystkich możliwych punktów.

Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

W ramach przedmiotu studenci zdobędą wiedzę na temat architektury chmur obliczeniowych, modeli usług (IaaS, PaaS, SaaS) oraz podstawowych technik wirtualizacji i konteneryzacji. Poznają również zasady działania i konfiguracji platform chmurowych, takich jak AWS, Azure i Google Cloud, w tym usługi obliczeniowe, bazodanowe oraz sieciowe. Kurs obejmuje również zagadnienia związane z bezpieczeństwem w chmurze, w tym mechanizmy autentykacji, szyfrowania i zarządzania tożsamością. Szczególny nacisk zostanie położony na systemy zarządzania i orkiestracji usług w chmurze, takie jak Docker Swarm, Kubernetes oraz OpenStack, w tym monitorowanie stanu usług, obsługę awarii oraz zarządzanie cyklem życia aplikacji. Studenci nauczą się wdrażać aplikacje webowe oraz IoT w środowiskach chmurowych, z wykorzystaniem automatyzacji wdrożeń (CI/CD) oraz narzędzi do monitorowania wydajności i kosztów. Podczas laboratoriów uczestnicy będą mieli okazję praktycznie skonfigurować środowisko chmurowe, uruchomić maszyny wirtualne i kontenery oraz wdrożyć aplikacje w modelu PaaS. Zajęcia zakończą się projektem zespołowym, w którym studenci zaprojektują i wdrożą kompletną aplikację działającą w chmurze, uwzględniając jej skalowalność, bezpieczeństwo oraz

niezawodność.

Tematyka zajęć

Wykład:

1. Wprowadzenie do chmury obliczeniowej
 - Definicja chmury obliczeniowej, ewolucja modeli obliczeniowych.
 - Modele usług: IaaS, PaaS, SaaS.
 - Modele wdrożeń: chmura publiczna, prywatna, hybrydowa.
2. Architektura chmur obliczeniowych
 - Wirtualizacja jako fundament chmur obliczeniowych.
 - Konteneryzacja: Docker, Kubernetes - podstawy i zastosowania.
3. Techniki wirtualizacji:
 - Wirtualizacja jako narzędzie umożliwiające efektywne wykorzystanie zasobów fizycznych.
 - Porównanie rodzajów wirtualizacji: hipernadzorca typu 1 i 2, zagadnienia izolacji, architektura i przypadki użycia.
 - Narzędzia do wirtualizacji: pełna (KVM, XEN, VMWare, VBox), kontenerowa (LXC, Docker), hybrydowa (Kata Containers).
 - Techniki realizacji połączeń sieciowych dla maszyn wirtualnych i kontenerów zapewniające wysoką wydajność: DPDK, SR-IOV w architekturach x86 oraz ARM.
 - Mechanizmy przydziału i zarządzania zasobami (CPU/GPU, pamięć operacyjna, sieć, energia) oraz mechanizmy zapewnienia izolacji.
 - Zarządzanie cyklem życia maszyn wirtualnych i kontenerów, szczególne właściwości kontenerów (efemeryczność) i dobre praktyki tworzenia obrazów kontenerów.
4. Platformy chmurowe
 - AWS, Azure, Google Cloud - przegląd dostępnych usług obliczeniowych, bazodanowych i sieciowych.
 - Edge computing i fog computing - koncepcje oraz zastosowania.
5. Bezpieczeństwo w chmurze
 - Shared Responsibility Model.
 - Mechanizmy autentykacji, autoryzacji i szyfrowania danych.
 - Zarządzanie tożsamością i kontrola dostępu (IAM).
6. Systemy zarządzania i orkiestracji usług w chmurze:
 - Porównanie systemów: Docker Swarm, Cloudify, Kubernetes, OpenStack.
 - Realizowane funkcje podstawowe: umieszczenie/usunięcie obrazu, uruchomienie/zatrzymanie instancji, przydział zasobów, migracja maszyn wirtualnych/kontenerów, skalowanie usług (scale out & br/>in), równoważenie obciążenia.
 - Usługi wspomagające działanie chmury: monitorowanie stanu usług, obsługa mobilności aplikacji, zapewnienie niezawodności (obsługa awarii i anomalii).
 - Zarządzanie cyklem życia aplikacji: aktualizacja oprogramowania, repozytoria obrazów i kontenerów (OSBoxes, Docker Hub).
7. Zarządzanie i monitorowanie zasobów chmurowych
 - Automatyzacja wdrożeń: CI/CD.
 - Monitorowanie wydajności i kosztów.
8. Projektowanie aplikacji IoT w chmurze
 - Wykorzystanie platform chmurowych do tworzenia aplikacji IoT.
 - Przykłady zastosowań: inteligentne domy, zastosowania przemysłowe.

Laboratoria:

1. Podstawy konfiguracji środowiska chmurowego
 - Tworzenie konta, zapoznanie z interfejsem użytkownika platform chmurowych.
2. Uruchamianie maszyn wirtualnych i kontenerów
 - Konfiguracja maszyn wirtualnych na AWS/Azure.
 - Tworzenie kontenerów i zarządzanie nimi przy użyciu Dockera.
3. Wdrażanie aplikacji w modelu PaaS
 - Deploy aplikacji webowej na platformie PaaS.
4. Bezpieczeństwo w chmurze
 - Konfiguracja IAM, reguł zapory sieciowej oraz szyfrowania danych.
5. Monitorowanie i automatyzacja
 - Tworzenie pipeline CI/CD z użyciem GitHub Actions lub GitLab CI.
6. Projekt zespołowy
 - Kompleksowe wdrożenie aplikacji z uwzględnieniem skalowalności, bezpieczeństwa i monitorowania.

Metody dydaktyczne

Wykłady:

- a) Prezentacja multimedialna z dodatkowymi przykładami przedstawianymi i objaśnianymi na tablicy.
- b) Studium przypadku oparte na prezentacji wykorzystującej systemy chmurowe

Zajęcia laboratoryjne i projekty:

- a) Praktyczne ćwiczenia programistyczne z użyciem komputerów
- b) Krótkie prezentacje multimedialne.

Literatura

Podstawowa:

- 1. Erl, T., Mahmood, Z., Puttini, R. Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 2013.
- 2. White papers i dokumentacja techniczna dostawców chmur (AWS, Azure, Google Cloud).
- 3. Krutz, R. L., Vines, R. D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley, 2010.
- 4. Galkin, B., Chaudhary, A. Beginning Azure DevOps: Leveraging Pipelines, Repos, Boards and More, Apress, 2021.

Uzupełniająca:

- 1. Jamsa, K. Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Security, Jones & Bartlett Learning, 2013.
- 2. Dokumentacja i tutoriale platform chmurowych (AWS, Azure, GCP).
- 3. Blogi oraz portale branżowe (np. Medium, DevOps.com).
- 4. Materiały dodatkowe publikowane przez ENISA (European Union Agency for Cybersecurity) dotyczące bezpieczeństwa chmur obliczeniowych.
- 5. Dokumentacja systemów zarządzania kontenerami (Docker, Kubernetes, OpenStack).
- 6. Materiały wideo i kursy online (np. Udemy, Coursera) dotyczące automatyzacji i wdrażania aplikacji w chmurze.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	60	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	32	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	28	1,00