



ДЕЦЕНТРАЛІЗОВАНІ ЗАСТОСУНКИ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	третій (PhD)
Галузь знань	12 Інформаційні технології
Спеціальність	121-інженерія програмного забезпечення, 123 – комп'ютерна інженерія, 126-інформаційні системи і технології
Освітньо-наукова програма	ОНП Інженерія програмного забезпечення, ОНП Комп'ютерна інженерія, ОНП Інформаційні системи і технології
Статус дисципліни	Вибіркова
Форма навчання	Очна (денна і вечірня)
Рік підготовки, семестр	2 курс, весняний семестр
Обсяг дисципліни	5 кредити
Семестровий контроль/ контрольні заходи	Залік
Розклад занять	Науково-педагогічний працівник
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: д.т.н., професор Гаврилко Євген Володимирович, gev.1964@ukr.net , тел. 067-506-91-85 Практика: д.т.н., професор Гаврилко Євген Володимирович, gev.1964@ukr.net , тел. 067-506-91-85
Розміщення курсу	Google classroom, Кампус

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Великої кількості комп'ютерів поєднаних високошвидкісними системами дозволяє створювати комп'ютерні мережі, або у новій парадигмі комп'ютерних наук – децентралізованих або розподілених систем (ДС). ДС – це набір незалежних комп'ютерів, що представляється їх користувачам єдиної об'єднаної системою. Вивчення дисципліни «Децентралізовані застосунки» присвячене різним підходам щодо розроблення і застосування алгоритмів, комп'ютерних програм, і їх нових компонентів, архітектури, масштабуванню і розподіленню для досягнення максимальних технічних і комерційних можливостей.

Метою навчальної дисципліни є формування у студентів здатностей до використання законодавства України, організаційних, технічних, алгоритмічних та інших методів і засобів, програм і даних, законодавства і стандартів у цій області, сучасних ДС, криптосистем; хешування, здатність їх застосовувати у професійній діяльності.

Завдання. Основними завданнями вивчення дисципліни «Децентралізовані застосунки» є отримання аспірантами компетенцій для того, щоб приймати участь у проектуванні інформаційних децентралізованих систем. В результаті вивчення дисципліни у аспірантів повинні сформуватися наступні компетентності:

загальні:

- Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- Здатність розв'язувати комплексні проблеми з **інженерії програмного забезпечення, з комп'ютерної інженерії, з інформаційних систем і технологій** у сфері інженерії програмного забезпечення та з дотичних до неї міждисциплінарних напрямів на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності,
- Здатність переосмислювати наявне та створювати нове цілісне знання та/або професійну практику і розв'язувати значущі соціальні, наукові, культурні.

спеціальні компетенції:

- Здатність інтегрувати знання з різних галузей, застосовувати системний підхід та враховувати нетехнічні аспекти при розв'язанні комплексних проблем програмного забезпечення, комп'ютерної інженерії та інформаційних систем і технологій;
- Здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері інженерії програмного забезпечення, комп'ютерної інженерії, інформаційних систем і технологій оцінювати та забезпечувати якість виконуваних досліджень;
- Здатність до застосування сучасних методології, методів та інструментів досліджень в науково-педагогічній, науковій діяльності та інноваціях;
- Здатність розробляти якісне та надійне програмне забезпечення складних програмних комплексів та систем на основі новітніх технологій та стандартів розроблення програмного забезпечення;
- Здатність застосовувати формальні методи проектування, розроблення та дослідження програмних систем та технологій децентралізованих систем та застосунків у наукових дослідженнях.

Після засвоєння навчальної дисципліни аспіранти мають продемонструвати такі програмні результати навчання:

- Мати передові концептуальні та методологічні знання з інженерії програмного забезпечення, комп'ютерних технологій, інформаційних систем та технологій та дотичних до неї міждисциплінарних напрямів, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напрямку, отримання нових знань та/або здійснення інновацій;
- Пропонувати нові ефективні методи і моделі розроблення, впровадження, супроводу та забезпечення якості програмного забезпечення та управління відповідними процесами на всіх етапах життєвого циклу;
- Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного, імітаційного та/або комп'ютерного моделювання, наявні літературні дані;
- Розробляти та реалізовувати наукові та/або інноваційні ІТ-проекти, які дають змогу переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та прикладні проблеми програмування з дотриманням норм академічної етики врахуванням соціальних, економічних та правових аспектів.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Пререквізити: вища математика, алгоритми, проєктування і розроблення ІСТ, методи і засоби обробки великих, бази даних, адміністрування операційних систем, теорія інформації та кодування, захист програмного забезпечення, управління ризиками інформаційних систем, теоретичні основи криптографії, основи баз даних, теорія систем та системний аналіз та інші.

Постреквізити: знання одержані при вивченні даної дисципліни використовуються в ході наукових досліджень та розробки програмних застосунків для дисертації.

3. Зміст навчальної дисципліни

Розділ 1. Базова модель децентралізованих системах.

Тема 1.1. Парадигма, принципи, концепції розвитку децентралізованих (розподілених) систем.

Тема 1.2. Зв'язок в комп'ютерних і децентралізованих системах.

Розділ 2. Процеси в децентралізованих системах.

Тема 2.1. Процеси в децентралізованих системах.

Тема 2.2. Процеси іменування сутностей в децентралізованих системах.

Тема 2.3. Процеси синхронізації в децентралізованих системах.

Тема 2.4. Процеси утворення несуперечливості і реплікація в децентралізованих системах.

Тема 2.5. Процеси забезпечення відмовостійкості в децентралізованих системах.

Тема 2.6. Процеси забезпечення захисту процесів, комп'ютерних систем і мереж в децентралізованих системах.

Розділ 3. Підходи утворення архітектури у децентралізованих систем.

Тема 3.1. Підходи щодо розподілу системи об'єктів в децентралізованих системах.

Тема 3.2. Підходи до розподілу файлових систем в децентралізованих системах.

Тема 3.3. Підходи до розподілу файлових систем в децентралізованих системах.

Тема 3.4. Підходи до розподілу систем узгодження в децентралізованих системах.

Розділ 4. Застосунки у децентралізованих систем.

4.1. Шифрування в децентралізованих застосунках.

4.2. Хешування інформації для файлових систем в децентралізованих застосунках.

4.4. Застосунки на основі Блокчейну.

4.5. Криптосистеми та криптовалюти.

4.6. Токен.

4. Навчальні матеріали та ресурси

Література

1. Таненбаум Е. Розподілені системи. Принципи / Е. Таненбаум, М. ван Стеен. К, 2003. 877 с.
2. М. Венбо Сучасна криптографія: теорія и практика : пер. с англ. / М. Венбо – К. 2005. 768 с.
3. Артем Генкін, Алексей Михеев. Блокчейн: як це працює. – Днепр.: 2015. 129
4. Равал С. Децентралізовані програми. Технологія Blockchain в дії... 2017. 193 с.
<https://balka-book.com/search/filter=1:raval-s-213038/>
5. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів : ВНТЛ, 2011. 248 с.
6. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.

5. Методика опанування навчальної дисципліни(освітнього компонента)

Розділ 1. Базова модель децентралізованих системах.

Тема 1.1. Парадигма, принципи розвитку децентралізованих (розподілених) систем.

Лекція 1.1. Парадигма, принципи, концепції розвитку децентралізованих (розподілених) систем.

Визначення ДС. Порядок з'єднання користувача з ресурсами. Задачі ДС. Концепція апаратних рішень. Концепції програмних рішень. Модель клієнт-сервер.

Тема 1.2. Зв'язок в комп'ютерних і децентралізованих системах.

Лекція 1.2. Зв'язок в комп'ютерних і децентралізованих системах.

Рівні протоколів. Віддалений виклик процедур. Звернення до віддалених об'єктів. Зв'язок по повідомленням. Зв'язок на основі потоків даних.

Розділ 2. Процеси в децентралізованих системах.

Тема 2.1. Процеси в децентралізованих системах.

Лекція 2.1. Процеси в децентралізованих системах.

Потоки виконання. Клієнти. Сервера. Перенесення коду. Програмні агрегати.

Тема 2.2. Процеси іменування сутностей в децентралізованих системах.

Лекція 2.2. Процеси іменування сутностей в децентралізованих системах.

Сутності і їх найменування. Розміщення мобільних сутностей. Видалення сутностей.

Тема 2.3. Процеси синхронізації в децентралізованих системах.

Лекція 2.3. Процеси синхронізації в децентралізованих системах.

Синхронізація годинника. Логічний годинник. Глобальні стани. Алгоритми голосування. Взаємні виключення. Розподіл транзакцій.

Тема 2.4. Процеси утворення несуперечливості і реплікація в децентралізованих системах.

Лекція 2.4. Процеси утворення несуперечливості і реплікація в децентралізованих системах.

Моделі. Моделі несуперечності, орієнтовані на дані. Протоколи розподілу. Протоколи несуперечності.

Тема 2.5. Процеси забезпечення відмовостійкості в децентралізованих системах.

Лекція 2.5. Процеси забезпечення відмовостійкості в децентралізованих системах.

Розуміння відмовостійкості. Відмовостійкість процесів. НЕлежність зв'язку клієнт – сервер. Нележна групова рассилка. Розподілене підтвердження. Відновлення.

Тема 2.6. Процеси забезпечення захисту процесів, комп'ютерних систем і мереж в децентралізованих системах.

Лекція 2.6. Процеси забезпечення захисту процесів, комп'ютерних систем і мереж в децентралізованих системах.

Загрози. Криптографія в ДС. Захищеність каналів. Контроль доступів. Керування захистом.

Розділ 3. Підходи утворення архітектури у децентралізованих систем.

Тема 3.1. Підходи щодо розподілу системи об'єктів в децентралізованих системах.

Лекція 3.1. Підходи щодо розподілу системи об'єктів в децентралізованих системах.

CORBA.DCOM.Globe. Порівняння згаданих систем.

Тема 3.2. Підходи до розподілу файлових систем в децентралізованих системах.

Лекція 3.2. Підходи до розподілу файлових систем в децентралізованих системах.

Мережева файлова система Sun. Приклад файлової систем и без серверів. Масштабуєма система захисту.

Тема 3.3. Підходи до розподілу файлових систем в децентралізованих системах.

Лекція 3.3. WorldWideWeb.

Тема 3.4. Підходи до розподілу систем узгодження в децентралізованих системах.

Лекція 3.4. TIB/Rendezvous.

Розділ 4. Застосунки у децентралізованих систем.

Тема 4.1. Шифрування в децентралізованих застосунках.

Лекція 4.1. Цифрові підписи.

Схема застосування цифрового підпису. Цифровий підпис на основі шифру RSA. Цифровий підпис на основі шифру Ель-Гамала. Алгоритм цифрового підпису DSA (DigitalSignatureAlgorithm). Стандарт ГОСТ Р34.10-944.2. Хешування інформації для файлових систем в децентралізованих застосунках.

Тема 4.4. Застосунки на основі Блокчейну.

Лекція 4.4. Застосунки на основі Блокчейну (БЧ).

Схема БЧ. Принципи розроблення застосунку на основі БЧ.

Тема 4.5. Криптосистеми та криптовалюти.

Лекція 4.5. Криптовалюти.

Огляд криптовалют. Застосування криптовалют

Тема 4.6. Токени.

Лекція 4.5. Токени, як сутність сучасного обміну мистецтвом.

Огляд Токени. Застосування токенів.

6. Самостійна робота аспіранта

Розділ 1. Базова модель безпеки інформації.

Визначення ДС. Порядок з'єднання користувача з ресурсами. Задачі ДС. Концепція апаратних рішень. Концепції програмних рішень. Модель клієнт-сервер.

Рівні протоколів. Віддалений виклик процедур. Звернення до віддалених об'єктів. Зв'язок по повідомленням. Зв'язок на основі потоків даних.

Розділ 2. Процеси в децентралізованих системах.

Потоки виконання. Клієнти. Сервера. Перенесення коду. Програмні агрегати.

Сутності і їх найменування. Розміщення мобільних сутностей. Видалення сутностей.

Синхронізація годинника. Логічний годинник. Глобальні стани. Алгоритми голосування. Взаємні виключення. Розподіл транзакцій.

Моделі. Моделі несуперечності, орієнтовані на дані. Протоколи розподілу. Протоколи несуперечності.

Розуміння відмовостійкості. Відмовостійкість процесів. НЕлежність зв'язку клієнт – сервер. Належна групова розсилка. Розподілене підтвердження. Відновлення.

Загрози. Криптографія в ДС. Захищеність каналів. Контроль доступів. Керування захистом.

Розділ 3. Підходи утворення архітектури у децентралізованих систем.

CORBA.DCOM.Glode. Порівняння згаданих систем.

Мережева файлова система Sun. Приклад файлової систем и без серверів. Масштабуєма система захисту.

Розділ 4. Застосунки у децентралізованих систем.

Схема застосування цифрового підпису. Цифровий підпис на основі шифру RSA. Цифровий підпис на основі шифру Ель-Гамала. Алгоритм цифрового підпису DSA (Digital Signature Algorithm). Стандарт ГОСТ Р34.10-944.2. Хешування інформації для файлових систем в децентралізованих застосунках.

Схема БЧ. Принципи розроблення застосунку на основі БЧ.

Огляд криптовалют. Застосування криптовалют

Огляд Токени. Застосування токенів.

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування лекційних та практичних занять є обов'язковим за винятком поважних причин (хвороби, форс-мажорних обставин).

В разі пропущення занять з поважних причин викладач надає можливість студенту виконати усі або деякі лабораторні завдання (винятком є виконання деяких завдань у зв'язку із закінченням навчального процесу).

В разі пропущення занять без поважних причин, а також через порушення граничного терміну виконання завдання (deadline) студент може отримати зменшену кількість балів від максимальної оцінки за відповідне завдання.

Протягом семестру студенти:

- виконують та захищають лабораторні роботи у відповідні терміни,
- повинні позитивно закрити два календарні контролі (в кінці березня та в середині травня),
- по закінченні навчального процесу складають залік.

8. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

Система рейтингових (вагових) балів та критерії оцінювання

Максимальна кількість балів з навчальної дисципліни дорівнює 100.

Рейтинг студента з дисципліни складається з балів, що він отримує за:

- виконання та захист лабораторних робіт.

1. Виконання завдань лабораторних робіт

Завдання лабораторної роботи являє собою індивідуальне виконання робіт, що пов'язані з рішенням на ЕОМ заданої задачі комп'ютерного моделювання.

Вагові бали завдань наведено у таблиці.

Види завдань	Внесок до семестрового рейтингу балів
Завдання №1. Технології віддаленого виклику процедур – GRPC. Використовуючи технологію GRPC, розробити клієнт-серверну програму відповідно до індивідуального завдання.	20
Завдання №2. Робота з брокерами повідомлень. Розподілений веб-додаток розбити на 2 модулі: - перший модуль приймає запит від клієнта, наприклад REST або GRPC, валідує і відправляє через систему обміну повідомлення другої частини; - другий модуль - забирає повідомлення з черги та зберігає у БД. Система управління чергами, наприклад, RabbitMQ. Для швидкого встановлення та налаштування Rabbit рекомендується застосувати образ Docker. Для передачі даних використовувати JSON або XML згідно з варіантом індивідуальних завдань.	20
Завдання №3. Децентралізовані системи. За індивідуальними завданнями до лабораторної роботи №1 розробити децентралізовану систему. Дозволяється використовувати сервер лише як реєстр пір'їв. Для підтвердження цілісності даних або автентичності відправника використовувати хешування або ЕЦП.	20

Максимальна кількість балів за всі завдання дорівнює 60 балів.

Критерії оцінювання

Підготовка до роботи (у відсотках від максимальної кількості балів за відповідну роботу):

- протокол відповідає вимогам, охайний – 20 %;
- протокол відповідає вимогам, але є чисельні виправлення – 10 %;

Виконання завдання лабораторної роботи:

- робота виконана повністю і вірно протягом відведеного часу – 50 %;
- робота виконана пізніше зазначеного терміну – 20 %;

Якість захисту роботи:

- студент вірно і повністю відповів на запитання – 30 %;
- студент при відповіді допустив несуттєві неточності – 20 %;
- студент при відповіді на запитання допустив суттєві неточності, але самостійно виправив їх – 10 %.

Контрольна робота складається з 20 тестових завдань. За кожну вірну відповідь на запитання надається 2 бали.

Сума вагових балів контрольних заходів протягом семестру складає:

$$R = 60 + 40 = 100 \text{ балів.}$$

Необхідною умовою допуску до заліку є зарахування усіх лабораторних робіт, а також стартовий рейтинг (r_c) не менше 40% від R , тобто 40 балів.

Сума балів переводиться до залікової оцінки згідно з таблицею:

Бали (RD)	Традиційна оцінка
95..100	Відмінно
85...94	Дуже добре
75...84	Добре
65...74	Задовільно
60...64	Достатньо
$RD \leq 60$	Незадовільно
$RD < 40$ або не виконані інші умови допуску до заліку	Не допущений

Робочу програму навчальної дисципліни (силабус):

Складено професор, д.т.н., професор Гаврилко Є.В.

Ухвалено кафедрою інженерії програмного забезпечення в енергетиці НН ІАТЕ (протокол № 34 від 10.05.2024)

Погоджено Методичною комісією (протокол № 9 від 31.05.2024 р.)