



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
Освітньо-наукова програма	Інженерія програмного забезпечення
Статус дисципліни	Вибіркова
Форма навчання	Очна (денна і вечірня)
Рік підготовки, семестр	2 курс
Обсяг дисципліни	5 кредити (150 год)
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 дотримуватись етики досліджень, а також правил академічної доброчесності в наукових дослідженнях та науково-педагогічній діяльності (ЗК1),
- здатність до наукового й абстрактного мислення, аналізу та синтезу (ЗК2),
- Здатність знаходити, обробляти й аналізувати необхідну інформацію для рішення проблем й прийняття рішень (ЗК10).

фахові:

- Здатність критично переосмислювати наявні технології програмної інженерії та відстежувати тенденції їх розвитку (ФК3);
- Здатність креативно (творчо) мислити, генерувати нові прогресивні ідеї в інженерії програмного забезпечення. (ФК7);
- Здатність застосовувати формальні методи проектування, розроблення та дослідження програмних систем та технологій у наукових дослідженнях (ФК6);
- механізми утворення архітектури в децентралізованих системах (ФК8);
- розробка застосувань в децентралізованих системах (ФК8).

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

- розробляти децентралізовані системи (ПРН3);
- працювати з децентралізованими системами (ПРН5);
- ролі і місця блокчейну при проектуванні і налагодженні інформаційних систем (ПРН7);
- принципів і методів побудови типових блокчейн рішень(ПРН7);
- основи функціонування консенсусу мережевого блокчейну(ПРН7);
- сучасних програмних технологій розгортання блокчейн-систем(ПРН7).
- **уміння:**
- проаналізувати відомі способи проектування блокчейну у відповідності з поставленим завданням і вибрати конкретний метод, виходячи із мети, завдань, реальних допущень та обмежень розробки блокчейну (ПРН17);
- - вибрати конкретні методи побудови блокчейну та побудувати прототип блокчейну(ПРН17).
- **досвід:**
- - раціонально використовувати сучасні технології, пакети прикладних програм та інтегровані середовища програмування блокчейну(ПРН19);
- - оволодіння сучасними програмними засобами програмування блокчейну в обраних середовищах(ПРН21).

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

Пререквізити: математика, інформатика, програмування, адміністрування операційних систем, теорія інформації та кодування, теоретичні основи криптографії, основи баз даних, теорія систем та системний аналіз.

Постреквізити: знання одержані при вивченні данної дисципліни використовуються в наступних дисциплінах: проектування розподілених баз даних, проектування інформаційних систем, проектування комп'ютеризованих інтелектуальних систем управління та інші.

3. Зміст навчальної дисципліни

Розділ 1. Базова модель децентралізованих систем.

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

Основна література

1. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен. — СПб.: Питер, 2003. — 877 с: ил. — (Серия «Классика computer science»)
1. Венбо М. Современная криптография: теория и практика : пер. с англ. / М. Венбо — М. : Издательский дом "Вильямс", 2005. — 768 с.
2. Артем Генкин, Алексей Михеев Блокчейн: как это работает и что ждет нас завтра. — М.:Д, 2018.
3. Дрешер Д. Основы блокчейна: вводный курс для начинающих в 25 небольших главах. — М.:АльпинаПабlishер, 2018.
4. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. — Львів : ВНТЛ, 2011. — 248 с.

Додаткова література

1. Гребенчук В. Г. Цифровая стеганография / В. Г. Гребенчук, И. Н. Оков, И. В. Туринцев. — М. : СОЛОН-Пресс, 2012. — 272 с.
2. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. — 2-е изд. — СПб. : БХВ-Петербург, 2013. — 368 с.
3. 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.

4. Поповский В. В. Защита информации в телекоммуникационных системах : учебник : в 2 т. / В. В. Поповский, А. В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 1. – 292 с.
5. Поповский В. В. Защита информации в телекоммуникационных системах : учебник : в 2 т. / В. В. Поповский, А. В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 2. – 252 с.
6. Столлингс В. Криптография и защита сетей: принципы и практика. – 2-е изд. / В. Столлингс; пер. с англ. – М. : Издательский дом "Вильямс", 2001. – 672 с.

Навчальний контент

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. World Wide Web.

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 (Digital Signature Algorithm). Стандарт ГОСТ Р34.10-94.4.2. 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 за стосунку 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. Нележна групова рассилка. 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 за стосунку на основі БЧ.

Огляд криптовалют. Застосування криптовалют

Огляд Токени. Застосування токенів.

Політика та контроль

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,
- пишуть модульну контрольну роботу,
- повинні позитивно закрити дві атестації (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 кредитного модуля дорівнює 100.

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

- виконання та захист лабораторних робіт,
- модульну контрольну роботу (МКР) тривалістю 1 акад. година.

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.

<i>Види завдань</i>	<i>Внесок до семестрового рейтингу балів</i>
Завдання №1. Симетричні криптосистеми. Алгоритм DES.	20
Завдання №2. Асиметричні криптосистеми. Алгоритм RSA.	20
Завдання №3. Електронно-цифровий підпис на основі алгоритму RSA	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 %.

2. Модульний контроль

Ваговий бал – 40.

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≤60	Незадовільно
RD < 40 або не виконані інші умови допуску до заліку	Не допущений

Робочу програму навчальної дисципліни (силабус):

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

Ухвалено кафедрою _____ (протокол № ____ від _____)

Погоджено Методичною комісією факультету¹ (протокол № __ від _____)

¹Методичною радою університету – для загальноуніверситетських дисциплін.