



ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра комп'ютерних наук та інформаційних систем

СИЛАБУС (SYLLABUS)

Дисципліна «Raid-масиви даних та розподілені серверні системи»

ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА

Викладач	Пурський Олег Іванович
Науковий ступінь	Доктор фізико-математичних. наук
Вчене звання	Професор
Посада	Завідувач кафедри комп'ютерних наук та інформаційних систем
Адреса кафедри	м. Київ, вул. Кіото 19, каб. Б-507, Б-526
E-mail	compdep@knute.edu.ua
Консультації	Відповідно до графіку індивідуальних консультацій на сайті кафедри

ПОЛІТИКА АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

<https://knute.edu.ua/file/MzEyMQ==/c12a9f74e87d9154696ca0f761da2e5c.pdf>

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання не авторських ідей, розробок, тверджень, відомостей і т.п.;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної наукової діяльності, використанні методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

- академічний плагіат – оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;
- самоплагіат – оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;
- фабрикація – вигадкування даних чи фактів, що використовуються в наукових дослідженнях;
- фальсифікація – свідомо зміна чи модифікація вже наявних даних, що стосуються наукових досліджень.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до академічної відповідальності:

- повторне проходження оцінювання (модульний контроль, іспит, залік тощо);
- повторне проходження відповідного освітнього компонента освітньо-професійної програми;

- відрахування з Університету;
- позбавлення наданих університетом пільг;
- відмова у присудженні відповідного ступеня вищої освіти;

ПОЛІТИКА ЩОДО ВІДВІДУВАННЯ ЗАНЯТЬ

- відвідування занять є обов'язковим;
- Студент, який пропустив практичне заняття, самостійно вивчає матеріал (при виникненні питань може звертатися за консультацією згідно розкладу консультацій викладачів оприлюдненого на сайті кафедри) за наведеними джерелами, виконує завдання і дає його викладачу.
- за об'єктивних причин (наприклад, хвороба, міжнародне стажування та ін.) навчання може відбуватись в он-лайн формі за погодженням із викладачем дисципліни.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назва дисципліни	Raid-масиви даних та розподілені серверні системи
Навчальний рік	2023-2024
Факультет	Факультет інформаційних технологій
Курс	4
Семестр	7
Група	
Освітній ступінь	бакалавр
Галузь знань	12 «Інформаційні технології»
Спеціальність	126 «Інформаційні системи і технології»
Загальна характеристика	Кількість годин –180 Кількість кредитів – 6 Співвідношення аудиторних годин і годин самостійної роботи - 70/110 Мова викладання – українська Форма викладання – очна
Підсумковий контроль	Екзамен
Програмне забезпечення	CrystalDiskInfo, SpeedFan, Victoria, Badblocks, HDDlife, R-Studio, Oracle VM VirtualBox, VMware Workstation, Wireshark.
Обладнання	Проектор, комп'ютерна техніка із встановленим програмним забезпеченням та доступом до мережі Інтернет.
Необхідні попередні дисципліни	«Інформаційні системи та технології», «Технології прикладного програмування».
Методика вивчення	Методика вивчення дисципліни полягає у набутті бакалаврами знань теоретичного і практично-прикладного характеру під час лекцій, лабораторних занять, самостійної роботи та вивчення першоджерел і навчально-методичної літератури.
Мета і завдання	Метою вивчення дисципліни «Raid-масиви даних та розподілені серверні системи» є надання необхідного обсягу теоретичних і практичних знань для роботи з різного роду масивами даних на основі розподілених серверних систем та з управління корпоративною ІТ-інфраструктурою, підготовка до самостійного вирішення задач в процесі практичної діяльності. Завданням вивчення дисципліни «Raid-масиви даних та розподілені серверні системи» є оволодіння теоретичними і практичними методами побудови Raid-масивів даних з використанням розподілених серверних систем та методи управління корпоративною ІТ-інфраструктурою

ТЕМАТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основні поняття дискових масивів даних. Технологія оцінки стану жорсткого диска з допомогою SMART.

Класи дискових масивів. Entry-level - початковий рівень. Mid-Range – середній рівень. Hi-End або Enterprise - рівень підприємства. Додаткові функції дискових масивів. Локальна реплікація. Віддалена реплікація. Dynamic Provisioning, Thin provisioning. Віртуалізація. Tiering. Дедуплікація. Застосування дискових масивів. DAS. NAS. SAN. CAS. Основні поняття про SMART. Атрибути SMART. Види тестів SMART (короткий (Short), довгий / розширений (Long / extended), транспортування (Conveyance), вибіркового (Selective)). Програмне забезпечення для проведення оцінки стану жорсткого диску (TRIM, Hdparm, E2fsprogs, Comparison of SMART tools, smartctl, Badblocks, SpeedFan, CrystalDiskInfo, HDDScan, HD Tune, HDDlife, Hard Drive, Inspector, OpenMediaVault, Victoria).

Тема 2. Технологія віртуалізації даних RAID.

Основні поняття про RAID. Рівні RAID. RAID рівня 0. RAID рівня 1. RAID рівнів 2 і 3. RAID рівнів 4 і 5. RAID рівня 6. Порівняння рівнів RAID. Комбіновані і додаткові рівні RAID. Нестандартні рівні RAID. RAID 7. RAID 7.3. RAID-DP. Hybrid RAID. Відновлення з RAID.

Тема 3. Поняття про розподілені серверні системи.

Вступ в розподілені серверні системи (PCC). Проміжне програмне забезпечення. Термінологія PCC. Класифікація PCC. Зв'язок в PCC. Історія розвитку розподілених обчислень. Перше покоління PCC. Друге покоління PCC. Сучасні PCC. Архітектури інформаційних систем. Файл-серверна архітектура. Клієнт-серверна архітектура.

Тема 4. Огляд та основні можливості ОС Windows Server. Планування просторів імен AD.

Системні вимоги. Загальна характеристика Windows Server. Апаратні ресурси. Основні сервіси. Служба DHCP. Особливості служби DHCP в системах сімейства Windows Server. Установка контролерів доменів. Призначення служби каталогів AD. Моделі управління безпекою: робоча група; доменна модель безпеки.

Тема 5. Адміністрування серверних інформаційних систем та мереж.

Основні поняття, основні етапи та процеси адміністрування серверних інформаційних систем та мереж. Планування і виконання функцій адміністратора інформаційних систем та мереж. Інформаційні мережі. Обліковий запис користувача. Реєстрація користувача в системі. Ресурси ІС. спільне використання ресурсу. Права доступу до ресурсу. Аудит / контроль використання ресурсів. Основні функції адміністратора. Основні методи і засоби адміністрування інформаційних систем та мереж. Структура стеку протоколів TCP/IP та типи адрес (локальні – апаратні, мережеві – IP-адреси, символічні – доменні). Формат IP-адрес. Класи IP-адрес. Особливі IP-адреси. Використання масок при IP-адресації. Адресація і технологія CIDR. Відображення IP-адрес на локальні адреси. Протокол розв'язування адрес ARP. Протокол Proху-ARP. Служба імен DNS. Ієрархічна організація служби DNS. Розподілення простору між серверами. Рекурсивна та не рекурсивна процедури. Кореневі сервери. Обернена зона. Протокол та режими DHCP. Алгоритм динамічного призначення адрес. Об'єднання мереж

протоколами мережевого рівня. Основні характеристики повторювачів, мостів, комутаторів, маршрутизаторів і концентраторів.

Тема 6. Технології передачі даних в корпоративних серверних мережах.

Основні технології передачі даних в серверних мережах. Фізичне середовище передачі даних. Технології комутації в корпоративних комп'ютерних мережах. Комутація каналів. Неefективність передачі пульсуючого трафіку. Комутація пакетів. Буферизація пакетів. Дейтаграмна передача. Передача з встановленням логічного зв'язку. Передача з встановленням віртуального каналу. Методи доступу в корпоративних комп'ютерних мережах. Детерміновані методи доступу: метод опитування; естафетний метод; метод вставки регістра; маркерний метод; метод доступу за пріоритетом запиту. Випадкові методи доступу: 1. Множинний доступ з виявленням конфліктів (МДОК): чиста АЛОНА; слотована АЛОНА. 2. Множинний доступ з контролем несучої (МДПН): а) з виявленням колізій CSMA/CD; б) з попередженням колізій CSMA/CA.

Тема 7. Сучасні програмні продукти для проектування корпоративних мереж.

Рішення при побудові корпоративних мереж . Векторний 2D-редактор CADE для Windows, інструмент для складання діаграм Concept Draw Pro, відкрите ПЗ для складання діаграм DIA, блокнот для складання мережевих діаграм Network Notepad, фактичний стандарт для складання діаграм в Windows- Microsoft Visio. 10-Страйк: Схема мережі.

Тема 8. Технології глобальних мереж та їх використання в корпоративних мережах.

Технології віртуальних каналів. Технологія X.25. Технологія FrameRelay. Технологія ATM. Технології двопунктових каналів. Технології доступу. ISDN — мережі з інтегральними послугами. Мета і історія створення технології ISDN. Користувацькі інтерфейси ISDN. Підключення користувальницького устаткування до мережі ISDN. Адресація в мережах ISDN. Стек протоколів і структура мережі. Технологія ADSL. Пасивні оптоволоконні мережі. Технологія багатопротокольної комутації за мітками - MPLS. Технологія Ethernet операторського класу.

Тема 9: Проектування IT-інфраструктури.

Загальні положення проектування IT-інфраструктури. П'ять етапів життєвого циклу планування забезпечення безперервності бізнес-процесів: визначення цілей; проведення аналізу; проектування і розробка; реалізація; навчання персоналу, тестування, оцінка та підтримка актуальності плану. Визначення структури команд, розподіл ролей та відповідальності. Визначення стратегій захисту даних та IT-інфраструктури. Проектування узагальненої схеми корпоративної IT-інфраструктури на основі серверних систем. Узагальнена схема корпоративної IT-інфраструктури з централізованим сервером обробки даних і залученням хмарних послуг. Декомпозиція корпоративної IT-інфраструктури на чотири рівня – сервісів; додатків; обчислювальних ресурсів; мережевої взаємодії. Узагальнена ієрархічна схема корпоративної IT-інфраструктури. Розподіл сервісів на основі виділених серверів.

Тема 10: Управління IT-інфраструктурою.

Основні процеси управління IT-інфраструктурою. Системи управління IT-інфраструктурою. П'ять загальних процесів при управлінні IT-інфраструктурою: моніторинг, аналіз, управління,

оптимізація та планування. Технології побудови ПЗ управління IT-інфраструктурою (IT Management Software 2.0). Критерій ефективності управління. Аналіз стану елементів IT-інфраструктури. Загальні принципи аналізу стану і відомості метрик. Тестування компонентів IT-інфраструктури. Управління ресурсами і навантаженням IT-інфраструктури. Процесно-ресурсний підхід до управління розподілом ресурсів. Сучасні інформаційні технології управління IT-інфраструктурою.

Тема 11: Проектування мереж для IT-інфраструктури корпоративного рівня.

Проектування сховищ даних у корпоративній IT-інфраструктурі. Динамічне балансування навантаження. Розробка топології клієнт-серверної мережі для корпоративної IT-інфраструктури. Особливості проектування IT-інфраструктур нижніх рівнів ієрархії інформаційних систем. Проектування системи з двома паралельними каналами задля підвищення пропускної здатності або надійності. Проектування систем автоматичного управління на основі мультиплексних каналів. Характеристики мережевих компонентів, які впливають на довжину мережі. Декомпозиція каналів передачі даних. Багаторівнева топологія. Організація процесів управління передаванням інформації.

Тема 12. Мережеві інформаційні системи підприємства.

SOHO-мережі. Однорангові мережі. Мережа підприємства з централізованим управлінням. Управління локальними ресурсами. Методи управління локальною системою. Служба каталогів. Служба каталогів Windows (Active Directory). Домени Windows. Управління структурою домену підприємства. Створення нового домену. LDAP і Active Director. Делегування прав. Кошик Active Directory. Перегляд і відновлення вилучених об'єктів каталогу. Облікові записи та права. Поняття облікового запису. Локальні і доменні облікові записи. Групи користувачів. Інвентаризація фізичних каналів зв'язку. Облік комп'ютерів та програм. Моніторинг функціонування ПЗ. Управління за допомогою групових політик. Утиліти групового управління. Засоби автоматизації – сценарії. Окремі утиліти адміністрування третіх фірм. Автоматизація установки програмного забезпечення.

Тема 13. Моніторинг інформаційної системи. Відмовостійкість. Виявлення несправностей і їх усунення. Тестування.

Основні способи моніторингу. Журнали системи і програм . Протокол SNMP. Опитування служб. Моніторинг з використанням агентів. Моніторинг на основі протоколу SNMP. Найпростіші варіанти моніторингу. Контроль журналів Windows. Система моніторингу Nagios. Необхідність моніторингу мережі. Сервер протоколів. Системи моніторингу трафіку. Територіальна розподіленість. Центри обробки даних (дата-центри). Мережева інфраструктура. Вибір правильної топології мережі передачі даних. Ферми серверів. Відмовостійкі рішення для додатків. Дублювання даних. Віддзеркалення серверів баз даних. Розподілена файлова система. Створення DFS. Реплікація DFS. Підтримка DFS в Linux-системах. Кластери. Розподілені каталоги. Реплікація даних каталогів. Відмовостійкі рішення і віртуальні системи. Збір інформації про збій. Особливості збоїв в різних компонентах. Моніторинг відмовостійкої структури. Несправності підсистеми передачі даних. Несправності апаратної частини. Помилки програмного забезпечення. Відновлення інформаційних систем. Відновлення з резервної копії. Відновлення завантажувача системи. Завантаження в спеціальних режимах. Відкат до попередніх станів системи. Відновлення шляхом

перевстановлення. Відновлення видалених даних. Основні теоретичні положення тестування програмного забезпечення. Тестування в моделі життєвого циклу розробки програмного забезпечення. Цикли тестування програмного забезпечення. Загальні критерії вибору тестів. Специфіка модульного та інтеграційного тестування програмного забезпечення. Індустріальне тестування. Використання метрик Маккейб, Пратта, Джілбі і Ченіна для оцінки якості програм. Визначення якості програми по Метриці Холстеда. Специфіка автоматизованого тестування програмного забезпечення. Основи тестування інформаційних систем. Поняття «тестування інформаційних систем». Критерії тестування. Принципи тестування. Методи тестування. Тестування «білого ящика». Тестування «чорного ящика».

Тема 14. Технології кібербезпеки інформаційних систем та мереж.

Основні поняття, концепції і принципи інформаційної кібербезпеки. Необхідність захисту інформаційних систем і телекомунікацій. Типи та приклади атак. Пасивні та активні атаки. Відмова в обслуговуванні. Впровадження шкідливих програм. Викрадення особистості, фішинг. Ієрархія засобів захисту від інформаційних загроз. Засоби безпеки технічного рівня. Захист мережі з використанням брандмауерів та серверів-посередників. Рівні захисту інформаційних систем. Технології аутентифікації, авторизації і управління доступом. Технології безпеки на основі фільтрації і моніторингу трафіка. Стандартні і додаткові правила фільтрації маршрутизаторів Cisco. Файерволи. Проксі-сервери. Файерволи з функцією NAT. Технологія NAT. Програмні файерволи хоста. Типові архітектури мереж, які захищаються файерволами. Моніторинг трафіка. Аналізатори протоколів. Система моніторингу netFlow. Системи виявлення вторгнень. Архітектура мережі з захистом периметру і розподілом внутрішніх зон. Аудит подій безпеки. Атаки на транспортну інфраструктуру мереж. TCP-атаки. Затоплення SYN-пакетами. Підробка TCP-сегмента. Розірвання TCP-з'єднання. ICMP-атаки. Перенаправлення трафіку. ICMP-атака Smart. Ping-атаки. UDP-атаки. IP-атаки. Мережева розвідка. Сканування мережі, портів. Атаки на DNS. DDOS-атаки відображенням від DNS-серверів. Методи захисту служби DNS. Безпека маршрутизації на основі BGP. Технології захищеного каналу. Технології IPSec. Бази даних SAD і SPD. Безпека програмного коду і мережевих служб. Безпека передачі даних в мережах Wi-Fi. WEP (Wired Equivalent Privacy) – алгоритм забезпечення конфіденційності і цілісності даних. Технологія WPA (Wi-Fi Protected Access). Технологія WPA2. Технологія VPN 1.1. Персональні дані. Корпоративні дані. Зловмисники та експерти з кібербезпеки. Кібервійни. Правові та етичні проблеми кібербезпеки. Розуміння етики роботи у сфері кібербезпеки.

Перелік навчальних робіт студентів та оцінки їх у балах з дисципліни «Raid-масиви даних та розподілені серверні системи»

Види робіт	К-сть балів
Лабораторне заняття №1. Тема: «Дискові масиви, як основа побудови будь-якої серверної системи. Оцінювання стану жорсткого диску з допомогою SMART».	2
Лабораторне заняття №2. Тема: «Оцінювання стану жорсткого диску з допомогою SMART».	2

Лабораторне заняття №3. Тема: «RAID – масив, як основа для налаштування серверної системи».	4
Лабораторне заняття №4. Тема: «Організація розподілених серверних систем».	4
Лабораторне заняття №5. Тема: «Створення домену Windows Server. Групові політики».	2
Лабораторне заняття №6. Тема: «Особливості технологій адміністрування систем та мереж».	4
Лабораторне заняття №7. Тема: «Моделювання локальної мережі. Адресація вузлів мережі».	4
Лабораторне заняття №8. Тема: «Налаштування маршрутизації даних. Побудова мережі передачі даних підприємства».	4
Лабораторне заняття №9. Тема: «Проектування мережі та налаштування мережевих пристроїв».	4
Лабораторне заняття №10. Тема: «Створення моделей в Packet Tracer».	4
Лабораторне заняття №11. Тема: «Інфраструктура, як код. Terraform. Pulumi».	4
Лабораторне заняття №12. Тема: «Оркестратори. Nomad. Kubernetes. Шаблонізатори конфігурацій Kubernetes».	4
Лабораторне заняття №13. Тема: «Централізовані системи логування. ЕФК. Системи моніторингу. Prometheus».	4
Лабораторне заняття №14. Тема: «Побудова мережі підприємства».	4
Лабораторне заняття №15. Тема: «Розгортання та адміністрування системи моніторингу Nagios у середовищі віртуальних машин. Використання SNMP протоколу для керування та моніторингу мережі».	4
Лабораторне заняття №16. Тема: «Прийоми і технології тестування. Розробка тестових планів і тестових прикладів та тестування».	4
Лабораторне заняття №17. Тема: «Проектний підхід в тестуванні. Управління тестуванням. Виявлення помилок. Тестова документація ».	4
Лабораторне заняття №18. Тема: «Функціональне тестування. Модульне тестування. Методи побудови моделей тестування ».	4
Лабораторне заняття №19. Тема: «Створення списків доступу».	2
Лабораторне заняття №20. Тема: «Налаштування облікового запису».	2
Лабораторне заняття №21. Тема: «Програмне забезпечення захисту інформаційної системи».	4
Модульний контроль	6
Виконання індивідуального завдання (СР)	20
Разом: Аудиторна робота	80
Самостійна робота (СР)	20
Всього:	100

КОНТРОЛЬ ТА КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ

При вивченні дисципліни використовуються наступні форми контролю знань студентів: поточний; модульний; підсумковий.

Поточний контроль передбачає перевірку теоретичних питань, самостійної роботи, практичних робіт та усне опитування по кожній практичній роботі. По даному виду контролю оцінювання знань здійснюється у відповідності до бального розподілу наведеного в попередній таблиці.

Модульний контроль передбачає виконання модульної контрольної роботи. Всі завдання оцінюються в 6 балів. Перше завдання (теоретичне) – 2 бали, друге завдання (практичне) – 2 бали, третє завдання (практичне) – 2 бали.

Формою підсумкового контролю є екзамен. Екзаменаційна оцінка (100 балів) є результатом виконання двох теоретичних питань (2 x 20 балів = 40 балів) та практичного завдання (60 балів).

Результуюча оцінка з дисципліни визначається як середня від балів набраних протягом семестру та отриманих на іспиті.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний:

1. Тарнавський Ю. А., Кузьменко І. М. Організація комп'ютерних мереж [Електронний ресурс]. Підручник / Ю. А. Тарнавський, І. М. Кузьменко. К.: КПІ ім. Ігоря Сікорського, 2018. - 259 с.
2. Пупена О. М., Ельперін І. В., Луцька Н. М., Ладанюк А. П. Промислові мережі та інтеграційні технології в автоматизованих системах : навч. посіб. для студ. вищ. навч. закл. / О. М. Пупена, І. В. Ельперін, Н. М. Луцька, А. П. Ладанюк. – Київ : Ліра -К, 2019. – 550 с.
3. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настралін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с.
4. Ролік А.І. Управління корпоративною IT-інфраструктурою / А.І. Ролік, С.Ф. Теленик, М.В. Ясочка. - К.: Наукова думка, 2019. – 576 с.
5. Рудніченко М.Д. Навчальний посібник з дисципліни "Тестування програмного забезпечення інформаційних систем" для студентів спеціальності - 126 Інформаційні системи і технології / Упоряд.: Н.Д. Рудніченко, Н. В. Бут. - Одеса: ОНПУ, 2020. - 56 с