**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**МИКОЛАЇВСЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ**

Факультет менеджменту
Кафедра економічної кібернетики, комп'ютерних наук та інформаційних технологій

# АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

методичні рекомендації для практичних занять та самостійної роботи здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп'ютерні науки» спеціальності 122 «Комп'ютерні науки» денної форми здобуття вищої освіти

МИКОЛАЇВ
2024

**УДК 004.723**

**А28**

Друкується за рішенням науково-методичної комісії факультету менеджменту Миколаївського національного аграрного університету від 18 квітня 2024 року, протокол № 9.

**Укладачі:**

С. І. Тищенко – канд. пед. наук, доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет;

О.Ю. Пархоменко - канд. фіз.-мат. наук, доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет;

Р.С.Мірошник -асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет;

І. І. Хилько – старший викладач доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет

**Рецензенти:**

П.М.Полянський – канд. екон. наук, доцент, доцент кафедри загально-технічних дисциплін, Миколаївський національний аграрний університет;

Є.О.Давиденко – канд. техн. наук, доцент, завідувач кафедри інженерії програмного забезпечення, Чорноморський національний університет ім. Петра Могили.

**ЗМІСТ**

## Передмова

*Курс дисципліни:* «Адміністрування комп'ютерних систем та мереж» має важливе значення в теоретичній підготовці майбутніх фахівців і є обов’язковою компонентою підготовки здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп’ютерні науки» спеціальності 122 «Комп’ютерні науки».

*Мета дисципліни:* сформувати у здобувачів необхідний обсяг теоретичних і практичних знань про термінологічний апарат та теоретичні концепції адміністрування комп'ютерних систем та мереж, принципи організації і побудови комп'ютерних мереж, систем адміністрування комп'ютерних систем, методи проектування і засоби використання комп'ютерних мереж як складових елементів комп’ютерних систем.

Основними завданнями, що мають бути вирішені у процесі викладання дисципліни, є надання здобувачам вищої освіти:

- навичок проектування комп'ютерних мереж, визначення вимог, створення схем, розробки моделей мереж та забезпечення відповідності цілям і вимогам бізнесу;
- здатності оптимізації роботи мереж, забезпечення цілісності та безпеки даних, а також ведення адміністрування комп'ютерних систем і мереж;
- вмінь інтегрувати різноманітні програмні застосунки в мережі, розробляючи зв'язки між застосунками та комп'ютерними системами, створюючи API та інтерфейси для взаємодії з даними;
- знань про сучасні тенденції в галузі адміністрування комп'ютерних систем та мереж, такі як віртуалізація, кібербезпека, хмарні обчислення тощо.

Предмет дисципліни: основи сучасної теорії адміністрування комп'ютерних систем та мереж, введення в архітектуру комп'ютерних мереж, управління мережами, безпека комп'ютерних систем і мереж.

Структура навчального курсу дозволяє здобувачам застосовувати теоретичні знання до практичного адміністрування комп'ютерних систем і

мереж, проектувати логічні та фізичні моделі мереж, створювати та оптимізувати мережеві структури, забезпечувати їх безпеку та ефективність функціонування.

## Практична робота 1. TCP/IP утиліти та сервіси

Мета роботи: Ознайомити студентів з утилітами та сервісами мережевих під'єднань до інших комп'ютерів, а також діагностичні та інформаційні функції мережевих під'єднань.

Теоретичні відомості

TCP/IP утиліти та сервіси забезпечують мережеві під'єднання до інших комп'ютерів, а також діагностичні та інформаційні функції мережевих під'єднань. Для їх використання мережевий протокол TCP/IP повинен бути встановлений. У міру подачі матеріалу ми розширюватимемо перелік утиліт командного рядка платформи Windows. Повний перелік усіх утиліт командного рядка можна знайти на сторінці http://technet.microsoft.com/enus/library/bb490921.aspx

Утиліта ipconfig

Ця програма конфігурування відображає усі поточні налаштування протоколу TCP/IP на цьому вузлі.

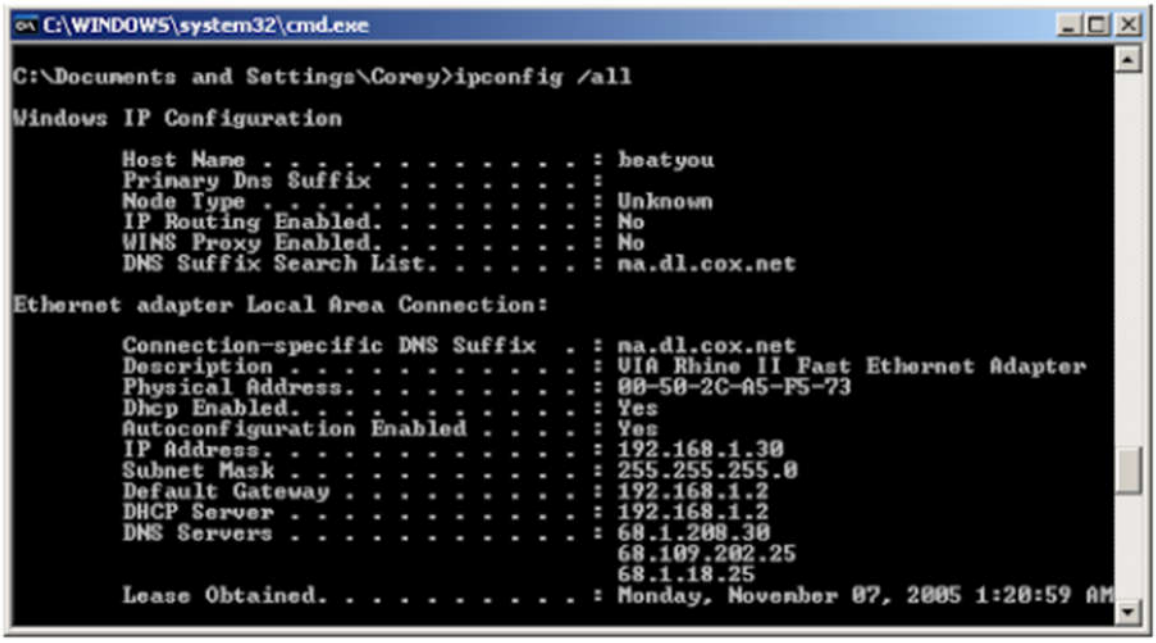
Формат команди:

ipconfig [/all\/renew [adapter] \/release [adapter] ]

Параметри утиліти наведені у табл. 1.1, а екранну форму виконання команди ipconfig.exe показано на рис. 1.1.

Таблиця 1.1 – Параметри утиліти ipconfig

| Ключі | Функції |
|---|---|
| *all* | Виводить всі дані. Без цього ключа відображається тільки IP-адреса, маска, шлюз за замовчуванням для кожного мережевого інтерфейсу |
| */renew [adapter]* | Команда оновлює параметри налаштування, отримані з DHCP. Ключ працює тільки на системах, які є клієнтом DHCP |
| */release [adapter]* | Скасовує поточну конфігурацію DHCP. Ключ працює тільки на системах, які є клієнтом DHCP |




Ключі Функції

all Виводить всі дані. Без цього ключа відображається тільки IP-

адреса, маска, шлюз за замовчуванням для кожного мережевого інтерфейсу

/renew

[adapter] Команда оновлює параметри налаштування, отримані з DHCP. Ключ працює тільки на системах, які є клієнтом DHCP

/release

[adapter] Скасовує поточну конфігурацію DHCP. Ключ працює тільки на системах, які є клієнтом DHCP

Рисунок 1.1 – Приклад виконання ipconfig

Утиліта ping

Утиліта ping (Packet Internet Groper) є одним з основних засобів, що використовуються для відлагодження мереж, і слугує для примусового виклику відповіді конкретної машини.

Запити утиліти ping передаються протоколом ICMP (Internet Control Message Protocol). Отримавши такий запит, програмне забезпечення, що реалізує протокол IP у адресата, негайно посилає exo-відповідь. Exo-запити посилаються задану кількість разів (ключ -n) або за замовчанням до того часу, поки користувач не введе команду переривання (Ctrl+C або Del) (ключ -i). У

результаті користувачеві виводяться статистичні дані про втрачені exo-відповіді і середній час реакції мережі на запити.

Під час виконання процедури ping exo-запит (ICMP-повідомлення тип=8, код=0) з часовою позначкою в полі дані посилаються адресатові. Якщо адресат активний, він приймає IP-пакет, міняє місцями адресу відправника й одержувача, і посилає його назад (ICMP-повідомлення тип=0, код=0). Вузол відправник, отримавши цю відповідь, може порівняти часову позначку, записану ним у пакет, з поточним показанням внутрішнього годинника і визначити час обороту пакета RTT (round trip time).

Час передачі ICMP-запиту загалом не дорівнює часу передачі відповіді. Це пов'язано з можливими змінами у каналі, а також з тим, що шляхи їх передачі можуть бути різними.

Успішний результат виконання команди ping означає, що живлення тесованої машини включене, машина не відмовила («не висить») і мережа знаходиться у робочому стані.

Утиліта ping є в операційній системі UNIX, а також у більшості реалізацій стека TCP/IP для інших операційних систем. У Windows утиліта ping є в комплекті постачання, але є програмою, що виконується у сеансі DOS з командного рядка (виконати утиліту cmd.exe).

Формат команди:

ping [-t][-a][-n число][-1 розмір] [-J][-i TTL]f-v TOS] f-r 4ucno][-s число] [[-j] список вузлів] \ [-k список вузлів]] [-w таймаут] ім'я вузла.

Параметри утиліти наведені у табл. 1.2.

Таблиця 1.2 – Параметри утиліти ping

| Ключі | Функції |
|---|---|
| *-t* | Відправка пакетів на вказаний вузол до команди переривання. Для виведення статистики і продовження натисніть |
| *-a* | Визначення адрес за іменами вузлів |
| *-n* | Кількість запитів, що відправляються |
| *-l* | Розмір буфера відправки |
| **-f** | Установка прапора, що забороняє фрагментацію пакета |
| *-i TTL* | Встановлення часу життя пакета (поле *Time To Live)* |
| *-vTOS* | Встановлення типу служби (поле *Type Of Service)* |
| *-r* | Запис маршруту для вказаної кількості переходів |
| *-s* | Штамп часу для вказаної кількості переходів |
| *-j список* | Вільний вибір маршруту за списком вузлів |
| *-k список* | Жорсткий вибір маршруту за списком вузлів |
| *-w інтервал* | Інтервал очікування кожної відповіді у мілісекундах |

## Порядок виконання роботи

1. Познайомитись з основними можливостями утиліт, що використовуються у роботі адміністратором, викликати їх у командному рядку (cmd) та вивчити їхні назви.
2. Вибрати 20 утиліт та представити їх у звіті.
3. Для трьох утиліт показати скриншоти виклику.
4. Оформити звіт про виконану роботу.

Зміст звіту

1. Теоретичні відомості 20 вибраних утиліт.
2. Скріншоти виклику трьох утиліт.
3. Зробити висновки.

**Практична робота 2.** Розробка плану приміщень та плану комп’ютерної мережі

**Мета роботи:** отримати навички проектування плану приміщень комерційних установ і плану комп’ютерної мережі з використанням інструментального засобу, наприклад, Microsoft Office Visio.

## Теоретичні відомості

Пасивне мережеве обладнання. При проектуванні комп'ютерних мереж в офісних приміщеннях використовують кабельні лотки та пластикові короби. Кабельний лоток – це відкрита конструкція, призначена для монтажу дротів і кабелів. Короб кабельний – конструкція із пластмаси для монтажу кабельних мереж усередині приміщення. Пластикові короби поділяються на кілька основних видів:

– кабельний канал (кабель-канал) – має просту конструкцію, він досить дешевий, деякі моделі дозволяють встановлювати розетки всередину кабель- каналу;

– парапетні короби – встановлюються на рівні робочого місця, внутрішній простір такого короба розділений на секції, він має подвійну стінку, і практично всі види парапетного короба підтримують монтаж розеток;

– короб на підлогу – короб для монтажу на підлогу, має посилену конструкцію та стійку до стирання поверхню.

Вимоги до серверної кімнати. Серверна кімната – приміщення для великого телекомунікаційного або серверного обладнання. Розміри серверної повинні відповідати вимогам до розташовуваного в ній обладнання. Якщо такі дані на момент вибору приміщення відсутні, розрахунки ведуться виходячи із площі робочих місць, що обслуговуються: на кожні її 10 м2 приймаються 0,07 м2 для серверної. Мінімальна площа апаратної приймається 14 м2.

Серверна кімната повинна розташовуватися в приміщенні, яке не має

зовнішніх стін будинку. Для забезпечення катастрофостійкості приміщень критичного електронного, електричного або механічного обладнання та комп’ютерів дані приміщення не допускається розміщати у підвальних поверхах або нижче очікуваного рівня повідкових вод, і на верхніх поверхах будинку, оскільки вони сильніше інших страждають у випадку пожежі.

Конструкція стін приміщення повинна бути герметичною, при цьому стіни та двері повинні мати вогнестійкість не менш 45 хвилин, а міжповерхові перекриття, окрім цього, повинні мати гідроізоляцію. Ширина дверей у серверну повинна бути не менш 910 мм, висота – 2000 мм. Конструкція дверей має певні обмеження: полотно повинне відкриватися назовні на 180 градусів, а дверна коробка не повинна мати поріг. При використанні в серверній великогабаритного обладнання передбачається встановлення двостулкових дверей. Для забезпечення герметичності в конструкції дверей повинна бути ущільнювальна прокладка, а для підвищення рівня захисту від злому необхідно передбачити протиз’ємне пристосування.

У серверній не повинно бути вікон. Обов'язковою умовою в цьому приміщенні є наявність фальшпідлоги, що витримує навантаження від обладнання, що встановлюється, і працюючих з ним людей. Рекомендована відстань між плитою на підлозі та фальшпідлогою – 400 мм, при цьому просвіт між фальшпідлогою і фальшстелею повинен бути не менш 2440 мм. Фальшпідлогу рекомендується робити з легко знімних модулів. Матеріал, із якого вона виготовлена, повинен бути міцним, зносостійким, мати погану займистість і мати електричний опір відносно землі від 1 до 20 Ом. Використання килимових покриттів у таких приміщеннях суворо заборонене. Перекриття під фальшпідлогою повинне бути герметизованим або пофарбованим.

Нумерація (маркування) розеток. Усі розетки в комп'ютерній мережі повинні бути пронумеровані. Причому, номер розетки повинен бути зазначений (приклеєний, підписаний) безпосередньо поруч із розеткою. Для кожного користувача комп'ютерної мережі повинні бути зарезервовані 2 розетки:

комп'ютерна для підключення комп'ютера користувача до комп'ютерної мережі та телефонна для підключення телефону. Правила нумерації розеток не регламентуються, але слід підкреслити, що кожна розетка повинна мати свій унікальний номер, а також пошук фізичного розташування розетки повинен бути не складним. Пропонується наступна складена нумерація розеток – 01-01- К01:

– перша і друга цифри – номер поверху;
– третя та четверта цифри – номер кімнати;
– п’ятий символ – тип розетки (К – комп’ютерна, Т – телефонна);
– шоста і сьома цифри – порядковий номер розетки.

Типи кабельних сегментів. При проектуванні комп'ютерної мережі необхідно враховувати характеристики кабельних сегментів. Кабельний сегмент – відрізок кабелю або ланцюг відрізків кабелів, електрично (оптично) з'єднаних один з одним, що забезпечують з'єднання двох або більше вузлів мережі. Особливо важливо враховувати довжину кабельного сегмента. В таблиці 2.1. надані основні характеристики кабельних сегментів.

Таблиця 2.1 – Характеристики кабельних сегментів

| № | Стандарт | Швидкість передачі даних | Тип кабелю, що використовується | Максимальна довжина сегменту |
|---|---|---|---|---|
| 1 | Ethernet 100Base-FX | 100 Мбіт/с | волоконно-оптичний | 2000 м. |
| 2 | Ethernet 100Base-T | 100 Мбіт/с | вита пара | 100 м. |
| 3 | Ethernet 100Base-T2 | 100 Мбіт/с | UTP 3 | 100 м. |
| 4 | Ethernet 100Base-T4 | 100 Мбіт/с | UTP5, STP | 100 м. |
| 5 | Ethernet 1000Base-CX | 1000 Мбіт/с | STP | 25 м. |
| 6 | Ethernet 1000Base-LX | 1000 Мбіт/с | волоконно-оптичний | одномод. 5000 м. багатомод. 550 м. |
| 7 | Ethernet 1000Base-T | 1000 Мбіт/с | UTP 5 | 100 м. |

## Завдання

Необхідно спроектувати план поверху комерційної установи та план комп'ютерної мережі. Вихідними даними для цього є: кількість кімнат на поверсі, робочі місця користувачів комп'ютерної мережі та розподіл робочих місць (табл. 2.2).

На основі вихідних даних необхідно спроектувати план одного поверху, враховуючи, що одна з кімнат поверху повинна бути серверною кімнатою з одним робочим місцем для адміністратора мережі (серверна кімната входить у перелік кімнат з вихідних даних). Також необхідно врахувати всі вимоги щодо розташування серверної кімнати (двері, вікна тощо).

Таблиця 2.2 – Вихідні дані

| **Варіант №1** | | **Варіант №2** | | **Варіант №3** | | **Варіант №4** | |
|---|---|---|---|---|---|---|---|
| № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць |
| 1 | 7 | 1 | 1 | 1 | 4 | 1 | 4 |
| 2 | 6 | 2 | 6 | 2 | 8 | 2 | 8 |
| 3 | 9 | 3 | 7 | 3 | 10 | 3 | 8 |
| 4 | 5 | 4 | 10 | 4 | 3 | 4 | 3 |
| 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 2 | 6 | 7 | 6 | 4 | 6 | 8 |
| 7 | 1 | | | 7 | 1 | 7 | 1 |

| **Варіант №5** | | **Варіант №6** | | **Варіант №7** | | **Варіант №8** | |
|---|---|---|---|---|---|---|---|
| № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць |
| 1 | 5 | 1 | 5 | 1 | 25 | 1 | 30 |
| 2 | 8 | 2 | 7 | 2 | 5 | 2 | 3 |
| 3 | 10 | 3 | 12 | 3 | 1 | 3 | 2 |
| 4 | 5 | 4 | 1 | 4 | 7 | 4 | 1 |
| 5 | 5 | 5 | 9 | 5 | 15 | 5 | 1 |
| 6 | 3 | 6 | 5 | 6 | 3 | 6 | 4 |
| 7 | 1 | 7 | 1 | | | | |

| Варіант №9 | | Варіант №10 | | Варіант №11 | | Варіант №12 | |
|---|---|---|---|---|---|---|---|
| № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць |
| 1 | 1 | 1 | 3 | 1 | 1 | 1 | 10 |
| 2 | 7 | 2 | 1 | 2 | 3 | 2 | 5 |
| 3 | 10 | 3 | 5 | 3 | 10 | 3 | 1 |
| 4 | 12 | 4 | 7 | 4 | 7 | 4 | 8 |
| 5 | 3 | 5 | 9 | 5 | 14 | 5 | 9 |
| 6 | 4 | 6 | 5 | 6 | 5 | 6 | 4 |
| 7 | 6 | 7 | 8 | 7 | 6 | 7 | 4 |
| 8 | 2 | 8 | 1 | | | | |

| Варіант №13 | | Варіант №14 | | Варіант №15 | | Варіант №16 | |
|---|---|---|---|---|---|---|---|
| № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць |
| 1 | 6 | 1 | 5 | 1 | 25 | 1 | 18 |
| 2 | 8 | 2 | 7 | 2 | 5 | 2 | 3 |
| 3 | 9 | 3 | 3 | 3 | 1 | 3 | 2 |
| 4 | 5 | 4 | 1 | 4 | 4 | 4 | 5 |
| 5 | 5 | 5 | 9 | 5 | 12 | 5 | 1 |
| 6 | 1 | 6 | 5 | 6 | 3 | 6 | 4 |
| 7 | 3 | 7 | 3 | | | | |

| Варіант №17 | | Варіант №18 | | Варіант №19 | | Варіант №20 | |
|---|---|---|---|---|---|---|---|
| № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць | № кімнати | К-ть робочих місць |
| 1 | 15 | 1 | 1 | 1 | 14 | 1 | 10 |
| 2 | 8 | 2 | 4 | 2 | 5 | 2 | 3 |
| 3 | 5 | 3 | 10 | 3 | 3 | 3 | 2 |
| 4 | 5 | 4 | 2 | 4 | 7 | 4 | 6 |
| 5 | 5 | 5 | 3 | 5 | 13 | 5 | 1 |
| 6 | 3 | 6 | 5 | 6 | 1 | 6 | 4 |
| 7 | 1 | 7 | 3 | | | | |

При проектуванні поверху необхідно визначити робочі місця для персоналу, оснащені офісними меблями й персональними комп'ютерами. Також необхідно визначити можливе місце розташування для монтажу кабелю комп'ютерної мережі – місця для коробів, лотків і т.д.; визначити місце розташування для мережевого обладнання; визначити місце розташування телефонних і комп'ютерних розеток на робочих місцях користувачів і пронумерувати їх.

## Порядок виконання роботи

1. Визначити форму периметру зовнішніх несучих стін будівлі.

2. Спроектувати план поверху, тобто визначити розташування кімнат на поверсі. Необхідно також підписати номера кімнат. На поверсі повинні бути присутніми коридори для переміщень, серверна кімната, місця для комунікацій.

3. Показати розміри кімнат. Це необхідно для визначення порядку довжин кабельних сегментів від серверної до офісних кімнат.

4. Ґрунтуючись на вихідних даних визначити робочі місця користувачів комп'ютерної мережі. Для цього необхідно використовувати відповідні елементи Microsoft Office Visio: столи, стільці, комп'ютери і т.д.

5. Визначити місце розташування коробів, лотків, комп'ютерних мережевих розеток. Короба, лотки й розетки необхідно пронумерувати.

6. Заповнити кабельний журнал, у якому необхідно вказати відповідність мережевого обладнання, порту мережевого обладнання, мережевої комп'ютерної розетки, номера кімнати й ім'я комп'ютера. Приклад кабельного журналу представлено в табл. 2.3.

Таблиця 2.3 – Приклад кабельного журналу*

| № п/п | Назва пристрою | № порту | № розетки | Ім'я комп'ютера | № кімнати |
|---|---|---|---|---|---|
| 1. | КМ01 | 01 | 01-01-К01 | 01-01-01 | 01 |
| | | 02 | 01-01-К02 | 01-01-02 | |
| | | 03 | 01-01-К03 | 01-01-03 | |
| 2. | КМ02 | 01 | 01-01-Т01 | 01-01-01 | |
| | | 02 | 01-01-Т02 | 01-01-02 | |
| | | 03 | 01-01-Т03 | 01-01-03 | |
| 3. | КМ03 | 01 | 01-02-К04 | 01-02-04 | 02 |
| | | 02 | 01-02-К05 | 01-02-05 | |
| | | 03 | 01-02-К06 | 01-02-06 | |
| | | 04 | 01-02-К07 | 01-02-07 | |
| 4. | КМ04 | 01 | 01-02-Т04 | 01-02-04 | |
| | | 02 | 01-02-Т05 | 01-02-05 | |
| | | 03 | 01-02-Т06 | 01-02-06 | |
| | | 04 | 01-02-Т07 | 01-02-07 | |
| 5. | МР01 | 01 | 01-05-К36 | 01-05-36 | 03 |

* умовні позначення: КМ – комутатор, МР - маршрутизатор

## Зміст звіту

1. Розробити план приміщення згідно поданого до завдання і власного варіанту.
2. Заповнити кабельний журнал.
3. Зробити висновки.

**Практична робота 3.** Проектування комп’ютерної мережі: підбір мережевого обладнання та складання кошторису витрат

**Мета роботи:** отримати навички підбору активного та пасивного мережевого обладнання, а також складання кошторису витрат на побудову комп’ютерної мережі.

## Теоретичні відомості

Етап 1. Здійснити підбір активного та пасивного мережевого обладнання та вивчити його основні технічні характеристики.

Використовуючи проект комп’ютерної мережі, розроблений у попередній практичній роботі, підібрати необхідне мережеве обладнання для побудови комп’ютерної мережі. Результати оформити у вигляді таблиці (див. табл. 3.1.).

Обов’язковий перелік активного обладнання включає:

– сервер комп’ютерної мережі;
– робочі місця користувачів;
– VoIP-телефони;
– VoIP-шлюз;
– маршрутизатор;
– комутатори.

Для підбору обладнання ви можете скористатися будь-яким сайтом.

Таблиця 3.1 – Технічні характеристики мережевого обладнання

| № п/п | Тип обладнання | Найменування моделі | Основні технічні характеристики |
|---|---|---|---|
| 1 | Сервер | HP ProLiant DL120 G5 (470065-180) | Процесор: Intel Xeon E3110; 3,00 GHz; кількість процесорів встановлених/максимальна: 1/1; пам’ять: 1 GB; жорсткий диск: 250 GB; SATA; мережевий адаптер: 1xGigabit Ethernet |
| 2 | … | … | … |
| 3 | … | … | … |

Також необхідно провести розрахунок потреби у пасивному мережевому обладнанні:

– довжина кабелю (вита пара);

– кількість конекторів RJ-45;

– довжина коробів та лотків;

– кількість комп'ютерних та телефонних розеток. Результати розрахунків навести у звіті.

Етап 2. Скласти кошторис витрат. Результати оформити у вигляді таблиці.

Використовуючи перелік активного та пасивного мережевого обладнання, складений на першому етапі роботи, провести розрахунок витрат на придбання обладнання (див. табл. 3.2.).

Таблиця 3.2 – Кошторис витрат на обладнання комп'ютерної мережі

| № п/п | Найменування | Одиниці виміру | Кількість | Ціна за одиницю, грн. | Загальна вартість, грн. |
|---|---|---|---|---|---|
| 1 | Сервер HP ProLiant DL120 G5 (470065-180) | шт. | 1 | 6173,00 | 6173,00 |
| 2 | … | … | … | … | … |
| 3 | … | … | … | … | … |
| | ВСЬОГО | - | - | - | 6173,00 |

**Завдання студентам**

1. Здійснити підбір активного та пасивного мережевого обладнання на базі індивідуального завдання у практичній роботі №2.
2. Вивчити основні технічні характеристики активного та пасивного мережевого обладнання.
3. Скласти кошторис витрат.
4. Результати оформити у вигляді таблиці.
5. Оформити звіт.

## Зміст звіту

1. Таблиця активного та пасивного мережевого обладнання.
2. Таблиця кошторису витрат.
3. Зробити висновки.

**Практична робота 4.** Налаштування та адміністрування сервера на базі ОС Microsoft Windows Server

**Мета:** Ознайомитися з методами та засобами адміністрування операційної системи Windows Server

## Теоретичні відомості

Установка, налаштування і використання системи Windows Server залежить від тих завдань, які повинна виконувати конкретна інсталяція. Типові завдання системи корпорація Microsoft об'єднала у вигляді «ролей» сервера. До основни ролей належать:

- файловий сервер;
- сервер друку;
- сервер додатків (сервер, на якому виконуються веб-служби XML, веб- додатки і розподілені застосунки);
- поштовий сервер;
- сервер терміналів (сервер, що виконує завдання для клієнтських комп'ютерів, які працюють в режимі термінальної служби; вибір цієї ролі приводить до установки служб терміналів, що працюють в режимі сервера додатків);
- сервер відаленого доступу/сервер віртуальної приватної мережі;
- служба каталогів (контроллер домена Active Directory);
- система доменних імен (сервер, на якому запущена служба DNS);
- сервер протоколу динамічного налаштування вузлів (служба DHCP);
- сервер Windows Internet Naming Service (сервер, на якому запущена служба WINS);
- сервер потокового мультимедіа.

Віртуальна машина – це програмне забезпечення, що імітує поведінку фізичної машини і дозволяє виконувати програми, що призначені для цієї

машини, на інших комп’ютерах або операційних системах.

Віртуальна машина може бути реалізована на різних рівнях: апаратному, операційній системі або на рівні програми.

Віртуальні машини можуть використовуватися для:

- захисту інформації і обмеження можливостей програм;
- дослідження продуктивності ПО або нової комп’ютерної архітектури;
- емуляції різних архітектур;
- оптимізації використання ресурсів мейнфреймів та інших потужних комп’ютерів;
- моделювання інформаційних систем з клієнт-серверною архітектурою на одній ЕОМ (емуляція комп’ютерної мережі за допомогою декількох віртуальних машин);
- спрощення управління кластерами – віртуальні машини можуть просто мігрувати з однієї фізичної машини на іншу під час роботи;
- тестування і налагодження системного програмного забезпечення.

Найбільш відомими прикладами віртуальний машин є Oracle VirtualBox та VMware Workstation.

VirtualBox – це програма віртуалізації для операційних систем, розроблена німецькою фірмою Innotek, зараз вона належить Oracle Corporation. Вона встановлюється на наявну операційну систему, яка називається хостовою, всередину цієї програми встановлюється інша операційна система, яку називають гостьовою операційною системою.

VMware Workstation — гіпервізор компанії VMware для платформ x86 і x86-64, що дозволяє запустити на комп’ютері декілька операційних систем одночасно. Кожна віртуальна машина може виконувати свою власну операційну систему, включаючи Microsoft Windows, Linux, BSD і MS-DOS.

VMware Workstation підтримує з’єднання дійсних мережевих хостів та обміну фізичних дисків і USB пристрої з віртуальною машиною.

## Хід роботи

1. Ознайомитись з теоретичними відомостями.
2. Встановити і налаштувати віртуальну машину (Oracle VirtualBox або VMware Workstation).
3. Встановити операційну систему Microsoft Windows Server на віртуальну машину.
4. Налаштувати групову політику.
5. Налаштувати DHCP.
6. Налаштувати DNS-сервер.
7. Оформити звіт до практичної роботи, додавши до нього скріншоти основних етапів виконання та короткий опис до них.

**Практична робота 5.** Створення розподілених мережевих ресурсів засобами ОС Microsoft Windows Server

**Мета:** ознайомитись з можливостями Microsoft Windows по роботі з розподіленими ресурсами. Навчитись використовувати об'єкти групової політики з консолі керування груповою політикою для створення шаблонів управління та обслуговування ресурсів ОС

## Теоретичні відомості

Розподіленим мережним ресурсом є папка, до якої організовано доступ через мережу і яка має унікальне мережне ім’я. Створення загального доступу до папки вказує Службі доступу до файлів і принтерів Microsoft (File And Printer Sharing For Microsoft Networks)на можливість підключеннядо цієї папки та її підпайок клієнтам, на комп’ютерах яких виконуєтьсяслужба Клієнт для мереж Microsoft (Client For Microsoft Networks).

Розподілені ресурси можна створювати з контекстного меню папки або за допомогою консолі MMC. Відкривши оснащення Загальні папки (Shared Folders)у консолі MMC або в консолі Керування комп’ютером (Computer Management),спостерігаємо, що у Windows Server 2003 вже налаштовано декілька стандартних адміністративних загальних ресурсів: системний каталог (зазвичай C:\Windows) і корінь кожного жорсткого диска. Ім’я ресурсу для таких загальних папок закінчується знаком долара ($). Знак «долар» наприкінці мережного імені позначає приховані загальні папки системного призначення. їх не можна побачити у програмі переглядачі(провіднику), але до них можна звернутися, вказавши їх ім’я на зразок:

\\ ім’я_сервера\ім’я_загального_ресурсу$

До адміністративних загальних ресурсів (наприклад, логічних дисків c$, d$ тощо) можна звернутися тільки з використанням облікового запису адміністратора.

Загальні папки до консолі MMC. У контекстному меню пункту Загальні папки або в меню Дія (Action) необхідно вибрати Новий загальний ресурс (NewShare). Майстер створення загальних ресурсів містить такі сторінки:

– Шлях до папки (Folder Path) – вказує шлях до загальної папки на локальному диску;

– Ім’я, опис і параметри (Name, Description and Settings) – задає ім’я загального ресурсу. Ім’я ресурсу разом з іменем сервера утворюють мережний шлях доспільної папки–

\\ім’я_сервера\ім’я_загального_ресурсу;

– Дозволи (Permissions) – дає змогу вибрати користувачів, які матимуть доступ до ресурсу, та задати правила доступу (читання, запис).

Правила доступу до мережних ресурсів не такі детальні, як дозволи файлової системи NTFS, проте вони дають змогу налаштувати основні типи доступу до спільної папки (таблиця 5.1).

Таблиця 5.1 – Правила доступу до розподілених ресурсів

| Правило | Опис |
|---|---|
| Читання (Read) | Користувачі можуть переглядати назви папок, а також імена, вміст та атрибути файлів, запускати програми й звертатися до інших підпапок у середині папки із загальним доступом. |
| Зміна (Change) | Користувачі можуть створювати папки, додавати файли й редагувати їхній вміст, змінювати атрибути файлів, видаляти файли і папки та виконувати дії, визначені дозволом Читання (Read). |
| Повний доступ (Full Control) | Користувачі можуть змінювати локальні правила доступу, отримувати права власності на файли і виконувати всі дії, допустимі дозволом Зміна (Change). |

Іншим способом створення спільних ресурсів є використання вікна властивостей папки. Після виклику цього вікна потрібно перейти на вкладку Доступ (Sharring), у якій можна вказати:

– максимальну кількість одночасних з’єднань користувачів.

– правила доступу для окремих користувачів.

Параметри доступу до спільного ресурсу визначають максимальні діючі дозволи для всіх файлів і папок усередині нагальної папки. Призначаючи дозволи на рівні файлової системи NTFS для окремих файлів і папок, на рівні роботи через мережу, доступ можна посилити, але не розширити. Інакше кажучи, доступ користувача до файлу або папки визначається найбільш жорстким набором до. і поліп загального ресурсу й правил таблиці ACL. Це одна з причин, з якої, зазвичай, групі Всі (Everyone) надається дозвіл Повний доступ, (Full Control), а для захисту папок і файлів використовують тільки дозволи файлової системи NTFS.

Автентифікація при звертанні до розподіленого ресурсу будь-яким із запропонованих способів відбувається так:

– клієнт надсилає дані, які були введені користувачем у процесі реєстрації в системі;

– якщо логін і пароль збігаються із записом бази користувачів сервера, то сервер авторизує клієнта;

– якщо логін і пароль не збігаються з жодним записом бази користувачів сервера, то сервер надсилає запит клієнту на введення імені користувача та пароля.

Ще одним завданням, яке постає перед системним адміністратором, є конфігурування принтера для друку документів з віддаленого комп’ютера. Для цього потрібно встановити загальний доступ до принтера (за умови, що драйвер принтера вже встановлено на одному з комп’ютерів).

## Порядок виконання роботи

1. Відкрити оснащення ттс Групова політика. Перейти у гілку Політика паролів, задати мінімальну довжину пароля. Після цього спробувати змінити власний пароль на такий, довжина якого менша за вказану у політиці, переконатись у неможливості такої дії. Повторити ці дії з параметрами: Пароль повинен відповідати вимогам складності.

2. Перейти у гілку Політика блокування облікового запису, задати граничне значення блокування. Після цього спробувати кілька разів зайти у систему з неправильним вводом пароля - переконатись у спрацюванні блокування. Увійти у систему як адміністратор - зняти блокування через оснащення Локальні користувачі та групи у властивостях облікового запису.

3. Перейти у гілку Локальні політики\Призначення прав користувача, задати привілей на вимкнення комп'ютера тільки для групи адміністраторів. Увійти до системи як користувач без адміністративних привілеїв; переконатись, що пункт Виключити комп'ютер зник з меню Пуск, а також, що завершення роботи системи з командного рядка теж неможливе.

4. Оглянути вміст гілки Адміністративні шаблони для частин: Конфігурація комп'ютера та Конфігурація користувача. У гілці Панель керування\Екран увімкнути політику видалення значка Екран з панелі керування. Спробувати змінити параметри екрана. Переконатись, що політики діють на усіх користувачів локальної системи.

5. Перейти у гілку Політики обмеженого використання програм. Створити нову політику. Не змінюючи політики за замовчуванням, створити нове правило (правила), що забороняє виконання програм з будь-якого іншого тому, окрім тому C: (за потреби створити логічні диски або розділи). Спробувати виконати будь-який файл з цього тому. Створити нове правило для хешу програми, яке дасть змогу виконувати саме цей вказаний файл. Спробувати запустити на виконання цей файл. Для яких потреб можуть використовуватись правила такого типу?

6. Відкрити оснащення Аналіз та налаштування безпеки. Створити нову базу даних, яка відображатиме стан налаштування політик комп'ютера за певним шаблоном. Для порівняння обрати один із вбудованих шаблонів безпеки (власні шаблони можна створювати за допомогою оснастки Шаблони безпеки). Проаналізувати параметри безпеки комп'ютера. Результати аналізу відображаються як порівняння параметрів комп'ютера з параметрами шаблона (створеної бази даних). Базу даних можна редагувати у цьому самому вікні, а потім вибрати пункт контекстного меню Зберегти та за потреби, експортувати

відредагований шаблон безпеки.

7. Налаштувати комп'ютер за певним шаблоном безпеки (привести у відповідність параметри бази даних і поточні налаштування комп'ютера), виконавши необхідні дії.

8. У звіті до лабораторної роботи описати та пояснити отримані результати.

**Практична робота 6**. Налаштування та адміністрування сервера на базі ОС Linux

**Мета:** Розглянути основні методи та засоби адміністрування серверних платформ на базі операційної системи Linux.

## Теоретичні відомості

Механізм облікових записів

В ОС Linux Debian існує три типи користувачів: користувач root, звичайні користувачі та системні користувачі. Кожен користувач має в системі обліковий запис. Інформація про облікові записи зберігається в текстовому файлі /etc/ passwd. Зашифровані паролі зазвичай зберігаються /etc/shadow.

Системний користувач - це не людина, а процес, що виконується на комп'ютері. На відміну від звичайних користувачів, системні користувачі не мають початкових каталогів і паролів, тому в систему не можна увійти під ім'ям системного користувача.

Ідентіфікатори користувачів і груп

Комп'ютер - це машина, що працює з числами. Він ідентифікує користувачів по номерах, відомим, як ідентифікатор користувача (UID) і ідентифікатор групи (GID).

Користувач root має необмежені права в системі, його UID, GID рівні 0.

Ідентифікатори в діапазоні від 1 до 499 і 65 534 зарезервовані для системних користувачів.

Ідентифікатори для людей починаються з 500.

Права доступу

Права доступу бувають трьох видів: читання (read), запис (write), виконання (execute), а також кожен вид прав має цифровий аналог 4, 2, 1 відповідно. За наявності декількох видів прав одночасно цифри сумуються.

Команди зміни прав групи, користувача або доступу до файлу або каталогу:

– chgrp - зміна належності файлу або каталогу до певної групи

– chown - змінює власника файлу або каталогу

– chmod - змінює режим доступу до файлу або каталогу. За допомогою команди chmod g + s [ім'я каталогу].

Дізнатися поточні атрибути/права доступу Ви можете за допомогою команди ls-la.

Групи користувачів

Список груп міститься у файлі /etc/group.

Нижче представлені найбільш часто використовувані інструменти командного рядка для керування групами:

– groupadd - створення нової групи;

– groupdel - видалення існуючої групи;

– groupmod - модифікація параметрів групи (ключі:-g,-n)

– gpasswd - створення пароля групи (ключ:-A-створення адміністратора групи);

– useradd-G - використання команди з даними аргументом дозволяє додати користувача до певної групи при створенні облікового запису;

– usermod-G - додавання користувача до групи;

– grpck - перевірка файлу /etc/group на помилки.

Система Linux Debian надає адміністратору графічний інтерфейс system-config-users, але досвідчені адміністратори вважають, що краще використовувати консоль.

Управління користувачами

Насамперед, необхідно створити обліковий запис користувача з наданням UID, створити початковий каталог, помістити туди стандартний набір файлів. По-друге, користувача слід віднести до певної групи і визначити, який обсяг дискового простору він може використовувати.

В Debian є кілька інструментів командного рядка для керування

користувачами, такі як useradd, userdel, passwd, usermod. При створенні користувача в каталозі /etc/skel міститься набір файлів, які розташовані у початковому каталозі користувача.

– useradd - створення нового користувача;

– userdel - використовується для видалення облікового запису користувача, при цьому буде вилучений і початковий каталог користувача;

– passwd - задає пароль користувача (ключ:-l - заблокувати обліковий запис користувача);

– usermod - команда змінює атрибути користувача (ключі:-s,-u);

– useradd user-p password-u 1000.

Механізми отримання особливих привілеїв

Бувають випадки, коли звичайним користувачам потрібно запускати команди з правами інших користувачів. За допомогою команди su існує можливість замінити користувача на будь-якого іншого користувача системи. Використовуючи команду sudo можливо звичайному користувачеві виконувати команди, доступні лише суперкористувачеві. Список авторизованих користувачів міститься у файлі /ets/sudoers.

Дискові квоти

У великих системах, в яких працює багато користувачів, обов'язково виникає необхідність контролювати дисковий простір, який займають користувачі. Для управління дисковими квотами повинен бути проинсталлировать програмний пакет quota.

Хід роботи

В ході роботи необхідно вивчити теоретичні відомості, пов'язані з адмініструванням користувачів, а також виконати практичні завдання.

1. Ознайомитись із вмістом файлів:

– /etc/passwd,

– /etc/shadow,

– /etc/group.

2. Створити наступні групи:

– workers,

– teachers,

– students.

3. Створити користувача user_[номер варіанту]_N, де N =1, 2, .., 5, uid облікового запису повинен бути рівним 1000+N.

Користувачів з N рівним 1 і 2 додати до групи workers вручну, внісши зміни в конфігураційний файл. Після додавання користувачів здійснити перевірку файлу /etc/group на помилки.

Користувачів з N рівним 3, 4 та 5 додати до групи students за допомогою команд адміністрування *.

Якщо у Вас виникли питання з приводу використання тих чи інших ключів скористайтеся командою man для отримання довідки: man [ім'я команди].

Перевірте результат, виконавши дії п.1.

4. Створити користувача teacher_ [номер варіанта].

У коментарі до облікового запису повинні бути Ваше ім'я і прізвище. uid облікового запису повинен бути рівний 3000. Користувача додати до групи teachers.

4. Для всіх користувачів задайте паролі, використовуючи команду passwd.

5. Створити директорію labs в кореневому каталозі. У ньому створити каталоги library і tests.

6. Створити файли book_ [прізвище студента] _N і помістити їх в library.

7. Створити текстовий файл test_ [ім'я студента], і помістити в tests. файли повинні містити скрипт на створення користувача user [номер варіанта] і надання йому пароля pass [номер варіанту]. Зробіть ці файли виконуваними для користувачів групи students.

8. У директорії labs створити файл list, який повинен містити список файлів директорії / etc.

9. Дати право на зміну файлу лише користувачеві teacher_ [номер варіанту], а на читання користувачам групи workers.

10. Налаштувати права доступу до каталогу library і tests, таким чином, щоб користувачі групи teachers могли змінювати і створювати там файли, а користувачі групи students мали доступ на читання.

**Практична робота 7.** Створення розподілених мережевих ресурсів засобами мережевої файлової система

**Мета:** навчитися керувати розподіленими мережевими ресурсами.

## Теоретичні відомості

Файлові служби і служби друку надають технології, здатні допомогти в управлінні сховищем і загальними папками, виконанні реплікації і швидкого пошуку файлів, а також підтримки і забезпечення доступу клієнтських UNIX-комп'ютерів для вирішень завдань друку рівня підприємства. До складу файлових служб Windows Server входить:

– Управління загальними ресурсами і зберіганням.
– Розподілена файлова система (DFS).
– Диспетчер ресурсів файлового сервера.
– Служби для NFS.
– Служба пошуку Windows.
– Файлові служби Windows.
– Служба BranchCache для мережевих файлів.

**Управління загальними ресурсами і зберіганням**

Консоль управління загальними ресурсами і зберіганням надає інтегроване і спрощене управління загальними папками і ресурсами зберігання. Цю консоль можна використовувати для надання загального доступу до вмісту папок і управління використанням загальних папок.

**Розподілена файлова система (DFS)**

Розподілена файлова система складається з двох технологій, які можуть бути використані разом або окремо для представлення відмовостійких і гнучких служб надання загального доступу до файлів і реплікації в мережах на основі операційних систем Windows.

Диспетчер ресурсів файлового сервера (FSRM)

Диспетчер ресурсів файлового сервера є комплектом інструментальних засобів, що дозволяють адміністраторам контролювати об'єми і типи даних, що зберігаються на серверах, а також управляти ними. За допомогою диспетчера ресурсів файл-сервера адміністратори можуть задавати квоти для папок і томів, активно відстежувати та автоматично класифікувати файли, застосовувати заснований на класифікації термін дії файлів і використовувати особливі завдання, а також генерувати докладні звіти сховища.

Служби для NFS

Служби для NFS надають вирішення сумісного доступу до файлів для підприємств, що працюють в змішаному середовищі Windows і UNIX. Служби для NFS дозволяють користувачам переміщати файли між операційною системою Windows Server і операційними системами UNIX за допомогою протоколу NFS.

Служба пошуку Windows

Служба пошуку Windows дозволяє виконувати швидкий пошук файлів на сервері з клієнтських комп'ютерів, сумісних з пошуком Windows.

Файлові служби Windows Server

Роль файлових служб в Windows Server включає служби індексування. Служба індексування розподіляє вміст по каталогу і властивості файлів на локальних і віддалених комп'ютерах. Також вона дозволяє швидко знайти файли за допомогою гнучкої мови запитів.

Примітка. На одному комп'ютері не можна встановити разом службу пошуку Windows і службу індексування. Обидва рішення індексування займають ресурси системи при активному індексуванні томів і папок, тому одночасна робота обох служб може істотно зменшити продуктивність системи.

Яке рішення індексування слід встановлювати?

Необхідно встановити службу пошуку Windows, якщо тільки не використовується додаток, що налаштовується, або додаток стороннього виробника, для якого потрібна наявність на сервері застарілої служби

індексування. У службі пошуку Windows надані деякі поліпшення в порівнянні із службою індексування, особливо це стосується розширення, поліпшення зручності роботи і збільшення продуктивності. Якщо є додатки, для роботи яких потрібна служба індексування, рекомендується відновити їх для сумісності із службою пошуку Windows.

Служба BranchCache для мережевих файлів

Служба BranchCache для мережевих файлів дозволяє комп'ютерам у філіях кешувати часто завантажувані файли із загальних папок з підтримкою BranchCache, а потім надавати ці файли іншим комп'ютерам в цій філії. Це знижує навантаження на мережу і прискорює доступ до файлів.

Завдання

Завдання 1. Встановлення ролі файлових служб.

Для того, щоб використовувати всі можливості файлових служб необхідно встановити роль Файлові служби у вікні Диспетчер сервера.

1. Відкрийте вікно Диспетчер сервера.
2. У лівій частині виберіть Ролі.
3. У правій частині вікна Диспетчер сервера (knR2) в розділі Зведення по ролях клацніть посилання Додати ролі.
4. У вікні Вибір ролей сервера в списку Ролі: встановіть прапорець Файлові служби і натисніть кнопку Далі.
5. У вікні Файлові служби ознайомтесь з довідкою по файлових службах і натисніть кнопку Далі.
6. У вікні Вибір служб ролей встановіть прапорці Файловий сервер, Диспетчер ресурсів файлового сервера і натисніть кнопку Далі.
7. У вікні Налаштувати спостереження за використанням сервера встановіть прапорець напроти тому, за яким здійснюватиметься спостереження (у нашому випадку диск C:) і натисніть кнопку Параметри.

8. У вікні Параметри спостереження за томом встановіть значення

порогу використання тому 85%, ознайомтесь з можливими звітами по використанню тому і натисніть кнопку ОК.

9. У вікні Налаштувати спостереження за використанням сервера натисніть кнопку Далі.

10. У вікні Налаштувати параметри звіту натисніть кнопку Далі.

11. У вікні Підтвердження вибраних елементів для встановлення ознайомтесь з інформаційним повідомленням і натисніть кнопку Встановити.

12. Дочекайтеся закінчення встановлення ролі сервера, ознайомтесь з інформаційним повідомленням про результати встановлення і натисніть кнопку Завершити.

Відобразіть у звіті скріншоти (2-3) з результатами виконання завдання.

Завдання 2. Створення загальних папок.

1. Для створення загальних папок необхідно увійти до Windows Server під обліковим записом Адміністратор і запустити оснащення Управління загальними ресурсами і сховищами. Для цього натисніть кнопку Пуск і виберіть послідовно Адміністрування і Управління загальними ресурсами і сховищами.

2. У вікні Управління загальними ресурсами і сховищами в меню Дія виконаєте команду Підготувати загальний ресурс.

Примітка. Підготовка загальних папок відбувається за допомогою майстра підготовки загальних папок. У вікні Розташування загальної папки вкажіть місце розташування створюваної загальної папки (для даного завдання C:\ Лабораторна робота) і натисніть кнопку Далі.

3. У вікні Дозволи NTFS встановіть перемикач Так, змінити дозвіл NTFS і натисніть кнопку Змінити дозволи.

4. У вікні Дозвіл для групи «Лабораторна робота» натисніть кнопку Додатково.

5. У вікні Додаткові параметри безпеки для «Лабораторна робота» зніміть прапорець Додати дозволи, успадковані від батьківських об'єктів.

6. У вікні Безпека Windows натисніть кнопку Додати.

Примітка. Таким чином, ми зможемо призначити нові дозволи для папки Лабораторна робота, відмінні від батьківської папки (в даному випадку диск C:).

7. У вікні Додаткові параметри безпеки для «Лабораторна робота» помітьте рядок Users (knclient\users) і натисніть кнопку Видалити.

8. Виконаєте попередню дію ще раз.

9. У вікні Додаткові параметри безпеки для «Лабораторна робота» натисніть кнопку OK.

10. У вікні Дозволи для групи «Лабораторна робота» натисніть кнопку Додати.

11. У вікні Вибір: «Користувач», «Група» або «Вбудований суб'єкт

безпеки» в полі Введіть імена вибираних об'єктів (приклади) введіть ім'я

облікового запису (у даному прикладі ваше ім’я), для якого необхідно додати дозволи, для перевірки правильності введеного імені користувача натисніть кнопку Перевірити імена. Зверніть увагу в полі Введіть імена вибираних об'єктів (приклади), повинно бути написано ваше Ім’я і Прізвище (ім'я@kn.local) і натисніть кнопку OK.

12. У вікні Дозвіл для групи «Лабораторна робота» зверніть увагу, що користувачеві, який названий вашим ім’ям наданий доступ на Читання і виконання та натисніть кнопку OK.

Примітка. Таким чином, доступ до папки Лабораторна роботамає тільки користувач названий вашим ім’ям (читання і виконання) і група Адміністратори, а також системний обліковий запис.

13. У вікні Дозволи NTFS натисніть кнопку Далі.

14. У вікні Протоколи загального доступу зверніть увагу на рядок Шлях до ресурсу (за допомогою даного шляху користувачі зможуть діставати доступ до мережевого ресурсу Лабораторна робота) і натисніть кнопку Далі.

15. У вікні Параметри SMB ознайомтесь із запропонованими

параметрами і натисніть кнопку Далі.

16. У вікні Дозволи SMB встановіть перемикач Користувачі і групи мають особливі дозволи для загального ресурсу і натисніть кнопку Дозволи… .

17. У вікні Дозволи для групи «Лабораторна робота» помітьте прапорець Повний доступ в стовпці Дозволити і натисніть кнопку ОК.

Примітки. При визначенні результуючого набору дозволів на доступ до загального ресурсу враховуються як дозволи NTFS, так і дозволи по протоколу загального доступу, після чого застосовуються суворіші дозволи. Таким чином, можна слідувати наступним рекомендаціям: дозволи загального доступу встановлювати в значення Повний доступ для групи Всі (Everyone), а права доступу визначати через дозволи NTFS.

18. У вікні Дозволи SMB натисніть кнопку Далі.

19. У вікні Політика квот натисніть кнопку Далі.

20. У вікні Політика блокування файлів натисніть кнопку Далі.

21. У вікні Публікація в просторі імен DFS натисніть кнопку Далі.

22. У вікні Перевірити параметри і створити загальний ресурс перевірте Параметри загальної папки і натисніть кнопку Створити.

23. У вікні Підтвердження переконайтесь, що завдання по створенню загальної папки виконане успішно і натисніть кнопку Закрити.

24. Для перевірки працездатності загальної папки необхідно увійти до системи під управлінням операційної системи Windows 7 під власним обліковим записом.

25. Після входу в систему натисніть кнопку Пуск, в рядку Знайти програми і файли введіть \\імя_сервера (у даному прикладі \\knR2).

26. У вікні Провідник двічі клацніть на ім'я теки Лабораторна робота.

27. Спробуйте створити нову теку в теці Лабораторна робота. Який буде результат? Чому?

Змінимо дозволи для папки Лабораторна робота так, щоб користувач названий вашим ім’ям зміг створювати папки і файли, копіювати файли і

папки в папку Лабораторна робота. Для цього:

1. Відкрийте оснащення Управління загальними ресурсами і сховищами, в списку Загальні ресурси виберіть папку Лабораторна робота і в меню Дії виконаєте команду Властивості.

2. У вікні Властивості: Лабораторна робота перейдіть на вкладку Дозволи і натисніть кнопку Дозволи NTFS.

3. У вікні Дозволи для групи «Лабораторна робота» виділіть рядок з власним обліковим записом, помітьте прапорець Змінити в стовпці Дозволити і натисніть кнопку ОК.

4. У вікні Властивості: Лабораторна робота натисніть кнопку ОК.

5. Перевірте внесені зміни, створивши в мережевій папці Лабораторна робота нову папку або файл.

@ Відобразіть у звіті скріншоти з результатами виконання завдання.

Завдання 3. Підключення мережевого диска.

Для того, щоб дістати доступ до мережевого диска користувач повинен пам'ятати шлях до цієї папки (\\ім'я_сервера\ім'я_загальної_папки). Щоб кожного разу не вводити цей шлях, користувач може підключити мережевий диск. Для цього:

1. Увійдіть до системи Windows під обліковим записом, який названий вашим ім’ям.

2. Відкрийте вікно Комп'ютер.

3. Натисніть клавішу ALT для відображення меню.

4. У меню Сервіс виконаєте команду Підключити мережевий диск.

5. У вікні Підключити мережевий диск вкажіть букву диска (наприклад, S:), що підключається, і теку (\\knR2\Лабораторна робота) і натисніть кнопку Готово.

6. Зверніть увагу, що у вікні Мій комп'ютер з'явився новий диск S:.

7. Виконайте перезавантаження і зверніть увагу, що мережевий диск

S: залишився підключеним.

У службі каталогів Active Directory створіть нового користувача: Іван Іванович Іваненко (ivanenkoii) надайте йому доступ на запис до мережевої папки. Таким чином, ми створили загальну папку і надали до неї доступ на запис всього для ДВОХ користувачів: власний обліковий запис і ivanenkoii. Що необхідно зробити, щоб надати доступ декільком користувачам? Додати всіх користувачів у вікні Дозволи для, вказавши відповідний рівень дозволу. Додавання декількох сотень користувачів може виявитися дуже трудомістким завданням. Зміна дозволів для всіх користувачів теж є витратним завданням.

Виходом з даної ситуації є об'єднанням користувачів в групи безпеки і наданням дозволу на папку для групи користувачів.

@ Відобразіть у звіті скріншоти з результатами виконання завдання.

**Практична робота 8.** Віддалене адміністрування сервера за допомогою сервера терміналів OpenSSH

**Мета:** вивчення протоколу SSH та способів його застосування.

## Теоретичні відомості

Протокол SSH (Secure SHell – «безпечна оболонка») – мережевий протокол сеансового рівня, що дозволяє здійснювати віддалене керування операційною системою та тунелювання TCP-з'єднань (наприклад, для передачі файлів). Схожий по функціональності з протоколами Telnet і rlogin, але, на відміну від них, шифрує весь трафік, включаючи паролі, що передаються. SSH припускає вибір різних алгоритмів шифрування. SSH-клієнти та SSH-сервери доступні для більшості мережевих операційних систем.

Перша версія протоколу, SSH-1, була розроблена 1995 р. дослідником Тату Улененом з Технологічного університету Гельсінкі, Фінляндія. SSH-1 був написаний для забезпечення більшої конфіденційності, ніж протоколи rlogin, telnet та rsh. У 1996 р. була розроблена безпечніша версія протоколу, SSH-2, несумісна з SSH-1. Протокол набув ще більшої популярності, і до 2000 р. він мав близько двох мільйонів користувачів. В даний час під терміном SSH зазвичай мається на увазі саме SSH-2, т.к. перша версія протоколу через істотні недоліки зараз практично не застосовується. У 2006 р. протокол був затверджений робочою групою IETF як Інтернет-стандарт. Перш ніж аналізувати протоколи ssh докладніше, слід визначити поняття ключ хоста.

Кожен хост, що працює з ssh, на якому може виконуватися як клієнт, так і сервер, може мати не менше одного ключа, причому для шифрування допускаються різні криптографічні алгоритми. Декілька хостів можуть мати загальний ключ хоста. Однак кожен хост повинен мати хоча б один ключ, з яким працює кожен із необхідних алгоритмів роботи з відкритими ключами. У проекті стандарту необхідний алгоритм лише один – DSS (Digital Signature Standard).

Протокол SSH розроблявся для надання безпеки даних, що передаються шляхом реалізації стійкого алгоритму шифрування даних, надійної системи аутентифікації користувача і сервера, наданням системи контролю цілісності переданих даних, а також інкапсуляцією додатків працюючих на основі протоколу TCP для встановлення безпечних тунелів.

Короткий опис та призначення кожного з трьох протоколів, що формують протокол SSH-2:

1. Протокол транспортного рівня – надає можливість шифрування та стиснення даних, що передаються, а також реалізує систему контролю цілісністю даних.

2. Протокол з'єднання – дозволяє клієнтам встановлювати багатопотокове з'єднання через оригінальний SSH тунель, таким чином знижуючи навантаження, яке створюють клієнтські процеси.

3. Протокол аутентифікації – протокол аутентифікації відокремлений від протоколу транспортного рівня, так як не завжди буває необхідним використання системи аутентифікації. Якщо потрібна аутентифікація, процес захищається оригінальним безпечним каналом, встановленим через протокол транспортного рівня.

Сам собою протокол транспортного рівня є достатнім для встановлення захищеного з'єднання, він є основою протоколу SSH-2 і протоколи з'єднання та аутентифікації базуються на ньому. Протокол аутентифікації відокремлений від протоколу транспортного рівня, так як іноді виникає ситуація, коли використання аутентифікації як не обов'язково, а й навіть небажано. Наприклад, якась організація надає на своєму FTP сервері анонімний доступ до патчів безпеки для будь-якої людини (або системи), яка захоче їх завантажити. У цьому випадку автентифікація не вимагатиметься, тоді як шифрування, стиснення та контроль цілісності даних забезпечуватиметься протоколом транспортного рівня. Більш того, за наявності каналу високої пропускної спроможності клієнти зможуть організувати багатопотокове з'єднання через оригінальне SSH з'єднання,

використовуючи протокол з'єднання. Розробники проекту протоколу

ssh особливо дбали про його довговічність. Протокол буде розширюваним; планується можливість доповнення криптографічних алгоритмів, які використовуються під час роботи ssh. З цією метою проектом передбачено, що між клієнтом та сервером відбуваються переговори, в результаті яких вибираються методи шифрування, формати відкритих ключів тощо, які будуть використані у даному сеансі. При цьому з метою забезпечення інтероперабельності має підтримуватись певний мінімальний набір національних криптографічних стандартів.

Окремої уваги заслуговують питання збільшення трафіку у зв'язку із застосуванням протоколів ssh. Зрозуміло, що при передачі в мережі великих пакетів додаткове навантаження, викликане передачею заголовків ssh, що управляють, невелика. Основну увагу слід звернути на програми, яким характерні короткі пакети, наприклад, telnet. Мінімальний розмір заголовка TCP/IP дорівнює 32 байти; мінімальний розмір пакета при використанні ssh збільшиться з 33 до (приблизно) 51 байту. Враховуючи, що в Ethernet мінімальна довжина поля даних пакета дорівнює 46 байт, додатковим навантаженням в 5 байт можна знехтувати. Найбільш істотним впливом ssh є, ймовірно, при використанні протоколу PPP на низькошвидкісних модемних з'єднаннях, оскільки PPP стискає заголовки TCP/IP. Однак суттєвий прогрес у швидкостях передачі дозволяє розраховувати, що додаткові затримки будуть вимірюватися кількома мілісекундами і залишаться непомітні людині.

Поради щодо безпеки використання SSH

1. Заборона віддаленого root-доступу.
2. Заборона підключення з порожнім паролем або вимкнення входу паролем.
3. Вибір нестандартного порту SSH-сервера.
4. Використання довгих SSH2 RSA-ключів (2048 біт і більше). Системи шифрування на основі RSA вважаються надійними, якщо довжина ключа щонайменше 1024 біт.

5. Обмеження списку IP-адрес, з яких дозволено доступ (наприклад, налаштування файлового блоку).

6. Заборона доступу з деяких потенційно небезпечних адрес.

7. Відмова від використання поширених або широко відомих системних логінів для доступу до SSH.

8. Регулярний перегляд повідомлень про помилки автентифікації.

9. Встановлення систем виявлення вторгнень (IDS-Intrusion Detection System).

10. Використання пасток, що підробляють SSH-сервіс (honeypots).

OpenSSH – це набір вільних програм, що надають шифрування сеансів зв'язку через комп'ютерні мережі з використанням протоколу SSH. Більшість користувачів telnet, rlogin, ftp та інших подібних програм не усвідомлюють, що їхні паролі пересилаються через інтернет у незашифрованому вигляді. OpenSSH шифрує весь трафік (включаючи паролі) для запобігання підслуховування, перехоплення з'єднань та інших видів мережевих атак. Крім того, OpenSSH надає різні способи створення тунелів, численні методи автентифікації, а також підтримує всі версії протоколу SSH.

Пакет OpenSSH містить програми ssh для заміни rlogin і telnet, scp для заміни rcp, і sftp як альтернативу для ftp. Пакет також включає демон sshd, та інші утиліти, такі як ssh-add, ssh-agent, ssh-keysign, ssh-keyscan, ssh-keygen і sftp- server.

Встановлення пакету OpenSSH

Коли відбувається підключення до інших комп'ютерів, OpenSSH запускає два процеси. Перший процес є привілейованим і керує видачею прав доступу у міру виникнення в них потреби. Другий процес взаємодіє із мережею. Для того, щоб мати правильно налаштоване середовище, необхідне додаткове налаштування, яке можна виконати в ролі користувача root за допомогою наступних команд:

install -v -m700 -d /var/lib/sshd && chown -v root:sys /var/lib/sshd &&

groupadd -g 50 sshd &&

useradd -c 'sshd PrivSep' -d /var/lib/sshd -g sshd \

-s /bin/false -u 50 sshd

Пакет OpenSSH дуже чутливий до змін у прикомпонованих бібліотеках OpenSSL. Після повторної компіляції пакет OpenSSH може не запуститись. В якості альтернативи використовуйте посилання на статичну бібліотеку OpenSSL. Щоб зробити посилання на статичну бібліотеку, потрібно виконати наступну команду:

sed -i 's@-lcrypto@/usr/lib/libcrypto.a -ldl@' configure

Встановлюється пакет OpenSSH за допомогою наступних команд:

sed -i.bak 's/ -ldes//' configure &&

./configure --prefix=/usr \

--sysconfdir=/etc/ssh \

--datadir=/usr/share/sshd \

--libexecdir=/usr/lib/openssh \

--with-md5-passwords \

--with-privsep-path=/var/lib/sshd && make

Якщо tcp_wrappers скомпоновано з використанням параметру --with-tcp-wrappers і якщо у є файл з обмеженнями /etc/hosts.deny, потрібно переконатися, що в рядок sshd файлу /etc/hosts.allow додано адресу 127.0.0.1. В іншому випадку набір тестів не пройде. Крім того, тестовий набір вимагає встановлення копії scp для того, щоб можна було завершити виконання тестів, які використовують мультиплексування. Щоб запустити набір тестів, спочатку в директорій /usr/bin потрібно скопіювати програму scp, попередньо переконавшись, що перед цим зроблено резервні копії всіх файлів, що містяться там.

Щоб запустити тестовий набір, потрібно виконати наступні команди:

make tests 2>&1 | tee check.log grep FATAL check.log

Якщо вказана вище команда не видасть фатальної помилки ("FATAL"), то в ролі користувача root можна перейти до встановлення:

make install &&

install -v -m755 -d /usr/share/doc/openssh-5.6p1 &&

install -v -m644 INSTALL LICENCE OVERVIEW README* WARNING.RNG \

/usr/share/doc/openssh-5.6p1 Конфігурація пакету OpenSSH Конфігураційні файли

~/.ssh/*, /etc/ssh/ssh_config та /etc/ssh/sshd_config

У ці файли вносити зміни не потрібно. Проте, можна вивчити файли

/etc/ssh/ і внести деякі зміни, що відповідають вимогам безпеки системи. Однією з рекомендованих змін є заборона користувачеві root входити до системи через ssh. Щоб вимкнути можливість користувача root входити в систему через ssh, потрібно виконати в ролі користувача root наступну команду:

echo "PermitRootLogin no" >> /etc/ssh/sshd_config

Додаткову інформацію про конфігурування можна знайти на сторінках man команд sshd, ssh та ssh-agent.

Завантажувальний скрипт

Щоб запускати сервер SSH під час завантаження системи, потрібно встановити завантажувальний скрипт /etc/rc.d/init.d/sshd, який знаходиться в blfs- bootscripts-20230101.

make install-sshd

Опис пакету

Встановлені програми: scp, sftp, sftp-server, slogin, ssh, sshd, ssh-add, ssh-agent, ssh-keygen, ssh-keyscan та ssh-keysign

Встановлені директорії: /etc/ssh, /var/lib/sshd, /usr/lib/openssh та /usr/share/doc/openssh-5.6p1

Короткий опис

scp – програма копіювання файлів, що діє як програма rcp, за винятком лише того, що вона використовує захищений протокол.

sftp – є програмою, схожою на FTP, яка працює поверх протоколів SSH1

та SSH2.

sftp-server – є підсистемою сервера SFTP. Ця програма зазвичай не викликається безпосередньо користувачем.

ssh – клієнтська програма, схожа на rlogin/rsh, за виключенням лише того, що вона використовує захищений протокол.

sshd – демон, який через ssh приймає запити на вхід до системи.

ssh-add – інструментальний засіб, за допомогою якого до ssh-agent додаються ключі.

ssh-agent – є агентом аутентифікації, який може зберігати закриті ключі. ssh-keygen – є інструментальним засобом генерації ключів.

ssh-keyscan – утиліта збору відкритих ключів із ряду хостів.

ssh-keysign – використовується програмою ssh для доступу до ключів локальних хостів та генерації цифрового підпису, необхідної для аутентифікації протоколу SSH версії 2 і при використанні окремого хоста. Ця програма зазвичай не викликається безпосередньо користувачем.

Завдання

1. Створити дві віртуальні машини (клієнт та сервер), налаштувати з’єднання між цими комп’ютерами, встановити на них ОС Linux та встановити OpenSSH.

2. Перевірити чи працюють на комп'ютерах ssh-сервери (ps ax|grep ssh). Якщо не працюють, то запустити їх відповідною командою.

3. Спробувати підключитися з клієнта до сервера за допомогою протоколу SSH. Вивчити передані пакети за допомогою tcpdump. Переглянути які події були відмічені у файлі журналу /var/log/auth.log

4. Перезавантажити віддалений сервер, не підключаючись до нього.

5. Віддалено перезапустити демон ssh без підключення.

6. Підключитися до віддаленого сервера та перезапустити демон ssh. Звернути увагу на те, що сеанс не завершився.

7. Запустіть FTP-сервіс на сервері.

8. Виконати передачу файлу через FTP за допомогою утиліти wget. Проаналізувати пакети, що проходять, за допомогою утиліти tcpdump(-XX). Запам'ятати швидкість передачі.

9. Виконати передачу через ssh. Проаналізувати пакети, що проходять, за допомогою утиліти tcpdump(-XX). Запам'ятати швидкість передачі. Порівняти пакети, що передаються, і швидкості передачі даних.

10. Увімкнути стиснення ssh і повторити вимірювання швидкості. У кожному тесті аналізувати результати для файлу, що складається з нулів, і для файлу, що складається з випадкових послідовностей (ddif=

/dev/urandomor=fileds=1Mcount=10), для текстового конфігураційного файлу або бінарного файлу.

Відобразіть у звіті скріншоти з результатами виконання завдання.

**Практична робота 9.** Адміністрування домену Active Directory

**Мета:** Освоїти методи та засоби адміністрування доменів Active Directory.

## Теоретичні відомості

Мережі Microsoft Windows підтримують дві моделі служб каталогів: робочу групу (workgroup) і домен (domain).

- Робочі групи - це вільні об'єднання комп'ютерів, в яких кожен комп'ютер управляється незалежно.
- Домени - це об'єднання комп'ютерів, колективно керованих за допомогою контролерів домену, тобто систем Windows Server 2003, що регулюють доступ до мережі, бази даних каталогу та загальних ресурсів.

Для організацій, які впроваджують Windows Server 2003, модель домену найбільш краща. Модель домену характеризується єдиним каталогом ресурсів підприємства - Active Directory, - якому довіряють всі системи безпеки, що належать домену. Тому такі системи здатні працювати з суб'єктами безпеки (обліковими записами користувачів, груп і комп'ютерів) в каталозі, щоб забезпечити захист ресурсів. Служба Active Directory, таким чином, відіграє роль ідентифікаційного сховища і повідомляє «хто є хто» в цьому домені.

Домени, дерева і ліси

Active Directory не може існувати без домену і навпаки. Домен - це основна адміністративна одиниця служби каталогів. Проте підприємство може включити в свій каталог Active Directory більше одного домену. Коли кілька моделей доменів спільно використовують безперервне простір імен DNS, вони утворюють логічні структури, звані деревами (tree). Наприклад, домени contoso.com, us.contoso.com і europe.contoso.com спільно використовують безперервне простір імен DNS і, отже, становлять дерево.

Домени Active Directory з різними кореневими доменами утворюють

кілька дерев. Вони об'єднуються в найбільшу структуру Active Directory - ліс

(forest). Ліс Active Directory містить всі домени в рамках служби каталогів. Ліс може складатися з декількох доменів в декількох деревах або тільки з одного домену. Коли доменів кілька, набуває важливості компонент Active Directory, званий глобальним каталогом (global catalog): він надає інформацію про об'єкти, розташовані в інших доменах лісу.

Групова політика

Організаційні підрозділи (ОП) також використовуються для об'єднання однаково налаштованих об'єктів - комп'ютерів і користувачів. Групова політика Active Directory дозволяє централізовано керувати практично будь-якими конфігураційними змінами системи. З її допомогою можна вказати настройки безпеки, розгорнути ПО і налаштувати поведінку ОС і додатків, навіть не торкаючись до комп'ютерів користувачів. Ви просто реалізуєте свою конфігурацію в рамках одного об'єкта групової політики (ОГП).

ОГП складаються з сотень можливих конфігураційних параметрів: від прав і привілеїв користувача до ПЗ, яке дозволено запускати на системі. ОГП підключається до контейнера всередині Active Directory (зазвичай до ОП, але може і до доменів або навіть сайтам), і після цього його налаштування поширюються на всіх користувачів і комп'ютери усередині цього контейнера.

Будь сервер може підтримувати одну або більше наступних ролей.

- Контролер домену (Domain controller) - сервер, на якому працюють служби каталогів і розташовується сховище даних каталогу. Контролери домену також відповідають за вхід в мережу і пошук в каталозі. При виборі цієї ролі на сервері будуть встановлені DNS і Active Directory. Поштовий сервер (POPS, SMTP) [Mail server (POP3, SMTP)] - сервер, на якому працюють основні поштові служби POP3 (Post Office Protocol 3) і SMTP (Simple Mail Transfer Protocol), завдяки чому поштові POP3-клієнти домену можуть відправляти і отримувати електронну пошту. Вибравши цю роль, ви визначаєте домен за замовчуванням для обміну поштою і створюєте поштові скриньки. Ці служби зручні в невеликих компаніях або при віддаленому

з'єднанні, коли електронна пошта необхідна, але цілком може обійтися без функціональності Microsoft Exchange Server.

- Сервер друку (Print, server) - сервер, організуючий доступ до мережевих принтерів і керуючий чергами друку і драйверами принтерів. Вибір цієї ролі дозволить вам швидко налаштувати параметри принтерів і драйверів.
- Сервер потоків мультимедіа (Streaming media server) - сервер, що надає мультимедійні потоки іншим системам мережі або Інтернету. Вибір цієї ролі приводить до установки служб Windows Media. Ця роль підтримується тільки у версіях Standard Edition і Enterprise Edition.
- Сервер додатків (Application server) - сервер, на якому виконуються Web- служби XML, Web-додатки та розподілені додатки. При призначенні сервера цій ролі на ньому автоматично встановлюються IIS, COM + і Microsoft. NET Framework. При бажанні ви можете додати до них серверні розширення Microsoft FrontPage, а також включити або виключити ASP.NET.
- Сервер терміналів (Terminal Server) - сервер, що виконує завдання для клієнтських комп'ютерів, які працюють в режимі термінальної служби. Вибір цієї ролі приводить до установки Terminal Server. Для віддаленого управління сервером встановлювати Terminal Server не потрібно. Необхідний для цього віддалений робочий стіл (Remote Desktop) встановлюється автоматично разом з ОС.
- Сервер віддаленого доступу або VPN-сервер (Remote access / VPN server)
- сервер, що здійснює маршрутизацію мережевого трафіку і керуючий телефонними з'єднаннями і з'єднаннями через віртуальні приватні мережі (virtual private network, VPN). Вибравши цю роль, ви запустите Майстер настройки сервера маршрутизації та віддаленого доступу (Routing and Remote Access Server Setup Wizard). За допомогою параметрів маршрутизації та віддаленого доступу ви можете дозволити лише вихідні підключення, вхідні і витікаючі з'єднання або повністю заборонити доступ ззовні.

- Вузол кластера серверів (Server cluster node) - сервер, який діє у складі групи серверів, об'єднаних у кластер. Вибір цієї ролі призводить до запуску Майстра створення кластера (New Server Cluster Wizard), що дозволяє створити нову кластерну групу, або Майстра додавання вузлів (Add Nodes Wizard), який

допоможе додати сервер до існуючого кластеру. Ця роль підтримується тільки у версіях Enterprise Edition і Datacenter Edition.

- Файл-сервер (File server) - сервер, що надає доступ до файлів і керуючий ним. Вибір цієї ролі дозволить вам швидко налаштувати параметри квотування та індексування. Ви також можете встановити Web-прикладений і для адміністрування файлів. У цьому випадку буде встановлений IIS і включені сторінки ASP (Active Server Pages).

- DHCP-сервер (DHCP Server) - сервер, на якому запущений DHCP (Dynamic Hose Configuration Protocol), що дозволяє автоматизувати призначення IP-адрес клієнтам мережі. При виборі цієї ролі на сервері буде встановлений DHCP і запущений Майстер створення області (New Scope Wizard).

- DNS-сервер (DNS Server) - сервер, на якому запущена служба DNS, роздільна імена комп'ютерів в IP-адреси і навпаки. При виборі цієї ролі на сервері буде встановлена DNS і запущений Майстер налаштування DNS-сервера (Configure DNS Server Wizard).

- WINS-сервер (WINS server) - сервер, на якому запущена служба WINS (Windows Internet Name Service), роздільна імена NetBIOS у IP-адреси і навпаки. Вибір цієї ролі призводить до установкеWINS.

Управління обраними ролями сервера здійснюється за допомогою програми Керування даним сервером (Manage Your Server), у вікні якої зосереджені всі основні інструменти для управління Windows Server 2003. Зокрема, тут перераховані поточні ролі сервера (рис.1). Щоб відкрити це вікно, скористайтеся меню Адміністрування (Administrative Tools).

Хід роботи

1. У середовищі програмного емулятора створити проект комп'ютерної мережі.

2. Провести встановлення операційноїсистеми ОС Windows 2003 ServerEnterpriseEdition/ОС Microsoft Windows Server 2019 Datacenter.

3. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 3.1. Під час розрахунку враховувати, що комутатору та інтерфейсу маршрутизатора мережі також виділяється по одній IP-адресі. Результати навести у вигляді таблиці.

Таблиця 3.1–Параметри для розрахунку:

| № варіанта | IP-адреса мережі | Префікс мережі | № варіанта | IP-адреса мережі | Префікс мережі |
|---|---|---|---|---|---|
| 1 | 191.G.N.0 | /24 | 16 | 206.G.N.0 | /24 |
| 2 | 192.G.N.0 | /25 | 17 | 207.G.N.0 | /25 |
| 3 | 193.G.N.0 | /26 | 18 | 208.G.N.0 | /26 |
| 4 | 194.G.N.0 | /27 | 19 | 209.G.N.0 | /27 |
| 5 | 195.G.N.0 | /28 | 20 | 210.G.N.0 | /28 |
| 6 | 196.G.N.0 | /24 | 21 | 211.G.N.0 | /24 |
| 7 | 197.G.N.0 | /25 | 22 | 212.G.N.0 | /25 |
| 8 | 198.G.N.0 | /26 | 23 | 213.G.N.0 | /26 |
| 9 | 199.G.N.0 | /27 | 24 | 214.G.N.0 | /27 |
| 10 | 200.G.N.0 | /28 | 25 | 215.G.N.0 | /28 |
| 11 | 201.G.N.0 | /24 | 26 | 216.G.N.0 | /24 |
| 12 | 202.G.N.0 | /25 | 27 | 217.G.N.0 | /25 |
| 13 | 203.G.N.0 | /26 | 28 | 218.G.N.0 | /26 |
| 14 | 204.G.N.0 | /27 | 29 | 219.G.N.0 | /27 |
| 15 | 205.G.N.0 | /28 | 30 | 220.G.N.0 | /28 |

4. Перевірити можливість інформаційного обміну між робочими станціями мережі. У разі виявлення проблем зв'язку знайти та усунути їх причини.

5. На сервері Serv_G_N_1 провести встановлення Active Directory, а сервер Serv_G_N_2 додати у домен та надати йому роль додатковий контролеру домену.

6. Додати в домен робочі станції(станцію).

7. На сервері Serv_G_N_1 в Active Directory створити групу користувачів GR_G_N. В цій групі створити нового користувача та, використовуючи цей обліковий запис, здійснити вхід у систему з робочої станції.

**Практична робота 10.** Організація доменів засобами сервера Samba та NIS

**Мета:** Отримати навики роботи по організації доменів засобами серверів Samba та NIS

## Теоретичні відомості

Продукт Samba призначений для надання послуг для Unix (та Linux) систем у мережах Windows. При цьому створюється можливість спільного використання файлів та прінтерів в обох типах мереж та послуги аутентифікації Windows.

Система Samba була розроблена в Австралії (Автор - Andrew Tridgell) на початку 90-х, програмістом, якому потрібно було організувати взаємний доступ між комп”ютерами з DOS та UNIX. Через те, що коди SMB протоколу були недоступні, автору довелося відбудовувати специфікацію SMB аналізуючи мережеві пакети. Система Samba є вільним продуктом з відкритим кодом. Через багато років, коли Samba була вже загальноприйнятим та широко використовуваним продуктом, Microsoft запропонувала свою відкриту специфікацію доступу до файлів Windows – CIFS (Common Internet File System), яка дозволила ліквідувати деякі недоліки Samba, пов”язані з недостатнім ступенем „розшифровки” окремих нюансів організації захисту доступу до файлів Windows у нових версіях цієї ОС.

Мережі Windows в значній мірі відрізняються від мереж UNIX і однією з головних відмінностей є використання протоколу NETBIOS та імен NETBIOS. Кожен комп”ютер у мережі Windows має NETBIOS- ім”я яке містить назву комп”ютера та байт типу ресурсу. Цей байт визначає які ролі відіграє комп”ютер у мережі. Окрема машина може мати декілька

різних ролей, наприклад „Робоча станція”, „Підтримка Win Popup сервісу»,

«Файловий сервер та сервер друку», «Броузер домена» (Domain master

browser) та інші.Броузер домена відовідає за періодичну перевірку які ресурси наявні у мережі та кешування цієї інформації. Інші робочі станції мережі у пошуках наявнийх ресурсів можуть звертатися напряму до Броузера домена. Крім ролей комп”ютера з імені NETBIOS можна отримати інформацію до яких доменів чи робочих груп він належить.

Кожна машина, що працює з протоколом SMB повідомляє інших про те, що вона надає певні послуги. Ці послуги не обмежуються сумісним використанням файлів чи прінтерів. Послугами може бу віддалене адміністрування, сервіс pop-up повідомлень та ін.

По мережі послуги доступні за UNC – іменами:

\\machine name\service name

Символ зворотної косої риски (\) має спеціальне значення для UNIX. Тому Samba замість нього сприймає пряму косу риску (/) та перетворює її у зворотну при необхідності.

Samba складається з таких головних утіліт та програм. Серверна частина:

- smbd –демон що керує сумісним використанням файлів та прінтерів
- nmbd – демон, що реалізує функції NETBIOS
- sambaconfig – утіліта налаштування
- smbpasswd – утіліта підтримки паролів Клієнтська частина:
- smbclient – подібна до FTP програма доступу до файлів
- smbspool – програма для передавання завдань на друг на прінтери
- smbmount, smbumount – утіліти для монтування/демонтування файлових систем

Графічні середовища KDE та GNOME пропонують зручні графічні оболонки для роботи з каталогами спільного використання на компютерах з ОС Windows. Наприклад, для KDE такою програмою є smb4K.

**Хід роботи**

1. Залогуватися у системі відповідно до заданих викладачем параметрів

2. Вивести на екран та занотувати у звіті основні секції файлу налаштувань smb.conf. Пояснити їх

3. За допомогою утіліти nmblookup визначити наявні у мережі комп”ютери та іхні ролі

4. За допомогою утіліти smbclient залогуватися на віддалений windows- комп»ютер і скачати вкавзаний файл на локальний Linux- компютер

5. Змонтувати Windows-каталог та переписати файл на віддалений windows-комп’ютер

6. Демонтувати Windows-каталог

**Практична робота 11.** Налаштування файлового сервера на базі FreeNAS

**Мета:** Освоїти роботу по налаштуванню файлового сервера з використанням FreeNAS

## Теоретичні відомості

FreeNAS — вільний NAS-сервер, який підтримує: Samba, FTP, NFS, Rsync та AFP протоколи; iSCSI і S.M.A.R.T.; можливість місцевої аутентифікації користувачів; та програмний RAID (рівнів 0,1,5); веб-інтерфейс для налаштовування. FreeNAS займає менше 64 МБ після установки на CompactFlash карти пам'яті, жорсткий диск або USB Флеш- накопичувач. Зараз FreeNAS поширюється у вигляді ISO-образу та у формі вихідного коду. Також є можливість використовувати FreeNAS із Live CD, коли файли конфігурацій зберігаються на дискеті або флеш-накопичувачі. Існує також образ диска готової системи для VMware.

Операційна система FreeNAS основана на мінімальній FreeBSD 7,2, забезпечена веб-інтерфейсом, PHP сценаріями, та документацією на основі m0n0wall. FreeNAS випущена відповідно до ліцензії BSD. У грудні 2009 року було повідомлено, що один з розробників (Фолькер Тейл) покине FreeNAS і почне роботу над аналогічним проектом OpenMediaVault, але основаним на Debian GNU/Linux на відміну від FreeBSD. В той же час iXsystems запропонувала фінансувати подальшу розробку FreeNAS.

Можливості

- Протоколи: CIFS (за допомогою Samba), TFTP, FTP, NFS, SSH, rsync, AFP, UPnP, протокол BitTorrent та сервіс iTunes.
- Розширення (плагіни) для: SlimServer, Xbox Media Stream Protocol.
- rsync сервер, клієнт та локальна синхронізації.

- Підтримка

Unison(https://alliance.seas.upenn.edu/~bcpierce/wiki/index.php?n=Main.UnisonFAQGeneral)

- ison.Можливість використання iSCSI для створення віртуальних дисків.
- iSCSI ініціювання.
- Файлові системи: ZFS, UFS і ext2/ext3 повністю підтримуються, а також підтримка читання/запису в файлові системи NTFS і FAT32.
- Жорсткі диски: P-ATA/S-ATA, SCSI, iSCSI, USB та FireWire.
- GPT/EFI розділи для жорстких дисків обсягом більше 2 Тб.
- Мережеві карти: всі дротові та бездротові карти, які підтримуються FreeBSD 7.2.
- Завантаження із жорсткого диску, USB флеш-накопичувача, CompactFlash карти пам'яті, CD-ROM + дискети, чи просто USB флеш-накопичувача.
- Апаратні RAID карти: всі, які підтримуються FreeBSD 7.2.
- Програмні рівні RAID: 0, 1, 5, JBOD, 5+0, 5+1, 0+1, 1+0, та інші. Також підтримуються RAID-Z та RAID-Z2 (як частина ZFS).
- Шифрування дисків за допомогою geli.
- Керування користувачами та групами (локальна аутентифікація користувачів, або в домені Microsoft).
- Підтримка технології S.M.A.R.T..
- Віддалене керування syslog.
- SNMP моніторинг (Netgraph та MibII).
- Звітування та відсилання звітів по електронній пошті.
- Підтримка VLAN
- Інтерфейси агрегації каналів та відмовостійких ліній
- Підтримка джерел безперебійного живлення

Хід роботи

1. Змініть рівень завантаження за замовчуванням в файлі /etc/inittab на 3й і перезавантажте віртуальний сервер. Після завантаження поверніть 5й рівень і знову перезавантажитеся.

2. Виставте рівень завантаження для файлового і веб сервісів, використовуючи команду chkconfig:

chkconfig - - list - список всіх процесів на всіх рівнях chkconfig - - list | grep smb - цікавлять нас процеси

3. Виконавши команду chkconfig - - level 3 smb onми включимо автоматичне завантаження сервісу smb на 3 рівні завантаження ОС.

4. Для виконання цього завдання попросіть Вашого сусіда виконати роль зловмисника, а саме змінити пароль root за допомогою команди passwd і перевантажити віртуальну машину за допомогою команди shutdown-r nowабо init 6.

Існує механізм дозволяє встановити новий пароль користувача root: Коли побачите екран завантажувача GRUB натисніть «пробіл».

Потім натисніть «e» (edit).3.

Виберіть рядок з kernel і потім знову натисніть «e» (edit).

Допишіть слово «single» (однокористувацький режим) в кінці рядка.

Натисніть «enter»

Натисніть «b» (boot).

Після завантаження в консольному режимі Змінюємо пароль за допомогою passwd.

І перевантажуємося shutdown-r now або init 6. Входимо з новим паролем в систему.

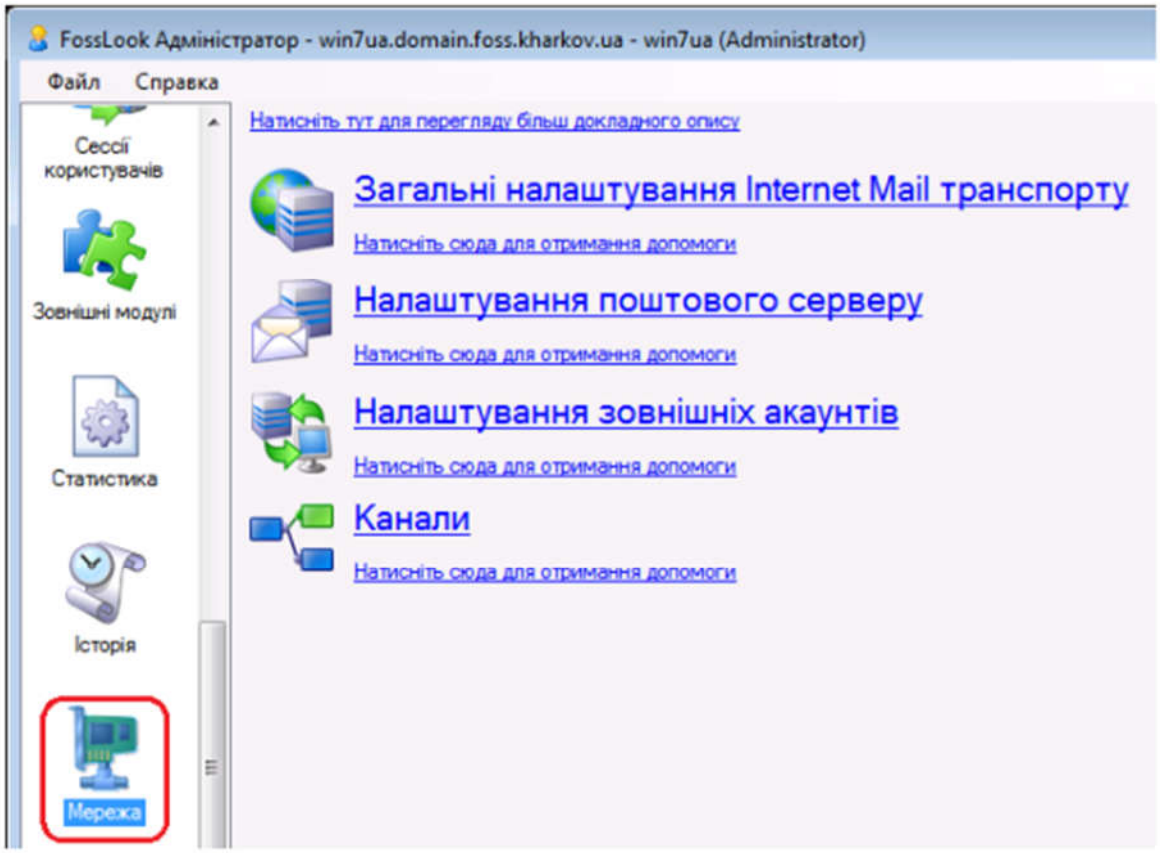
**Практична робота 12.** Налаштування поштового сервера

**Мета:** Отримати навики роботи по налаштуванню поштового сервера

## Теоретичні відомості

Поштовий сервер FossLook призначений для створення "внутрішніх" поштових скриньок користувачів (на вашому домені) і роботи з ними - прийому/відправки повідомлень. Сервер також ініціює прийом повідомлень з інших поштових серверів (mail.ru, gmail.com і т.п.), а також відправку ними повідомлень, якщо у користувачів, зареєстрованих на сервері FossLook, є зовнішні поштові скриньки.

Для налаштування сервера запустіть Майстер адміністрування і перейдіть на сторінку "Мережа":

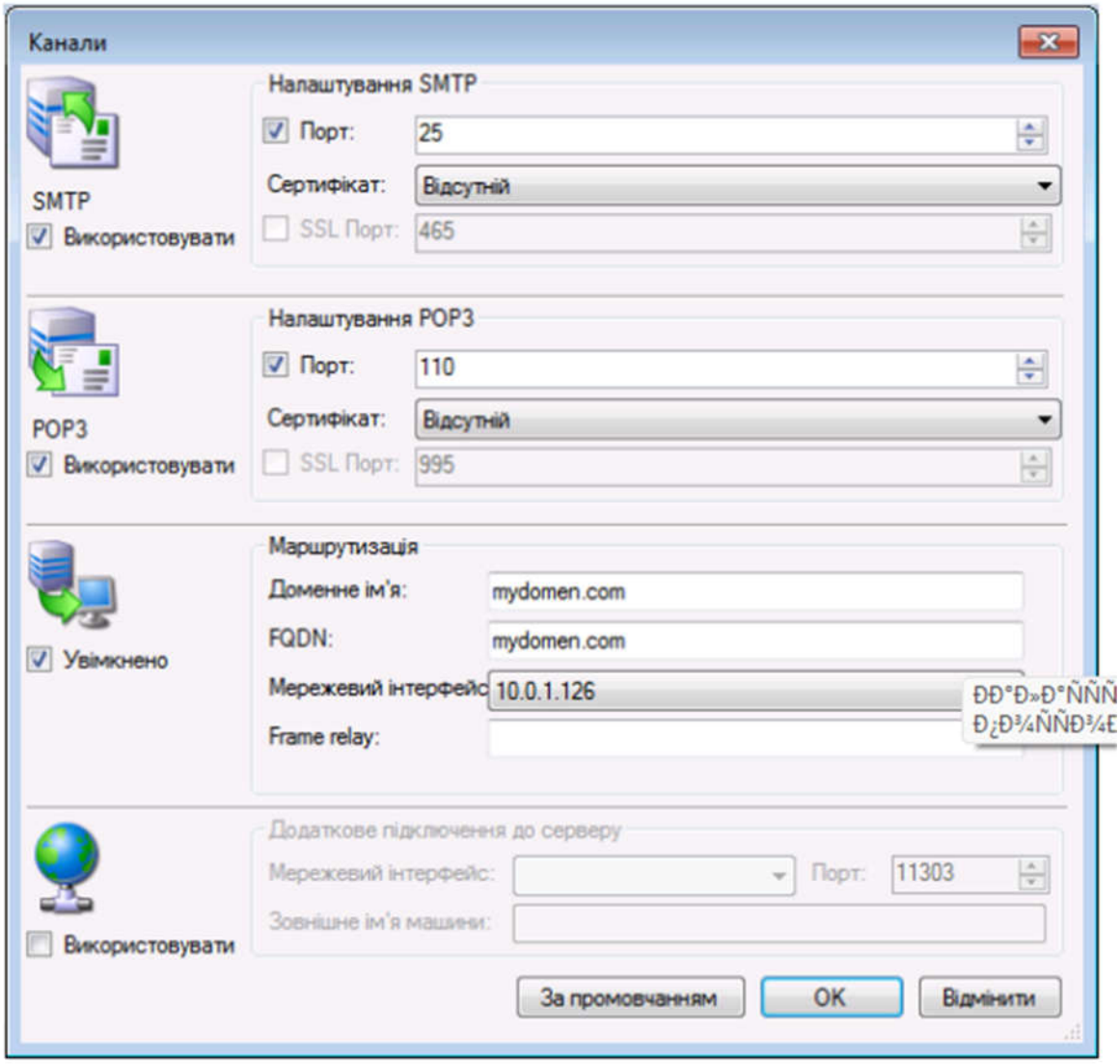



Це стартова сторінка налаштувань поштового серверу. Розглянемо всі діалоги налаштувань, які запускаються при натисканні відповідних посилань

на стартовій сторінці:

- Канали
- Загальні налаштування Internet Mail транспорту
- Налаштування поштового сервера
- Налаштування зовнішніх акаунтів

Канали - найважливіша сторінка. Заповнивши її, ви зможете створювати і працювати з "внутрішніми" поштовими скриньками, що використовують ваше власне доменне ім'я.




Призначення елементів даної сторінки наступне: Секція "Налаштування SMTP"

- Опція Використовувати - включає або відключає можливість

обміну між сервером FossLook і зовнішніми поштовими серверами.

- Порт - номер порта для обміну повідомленнями по SMTP- протоколу.
- Сертифікат - дані про сертифікат для шифрованого обміну.
- SSL Порт – номер порта для зашифрованого обміну. Секція "Налаштування POP3"
- Використовувати - включає або відключає можливість обміну між сервером FossLook і зовнішніми поштовими клієнтами, крім MS Outlook.
- Порт - номер порта для обміну повідомленнями по POP3-протоколу.
- Сертифікат - дані про сертифікат для шифрованого обміну.
- SSL Порт - номер порта для зашифрованого обміну. Секція "Маршрутизація"
- Доменне ім'я - доменне ім'я машини, на якій встановлено сервер FossLook.
- FQDN - повне доменне ім'я машини, на якій встановлено сервер FossLook.
- Мережевий інтерфейс - IP-адресу мережевої карти на сервері FossLook, через яку відбувається з'єднання з Internet.
- Відхилити більше ніж - максимальне обмеження на розмір вхідного повідомлення.
- Frame relay - доменне ім'я або IP-адресу проміжного сервера, через який вся кореспонденція буде відправлятися далі адресатам.

Секція "Outlook Конектор"

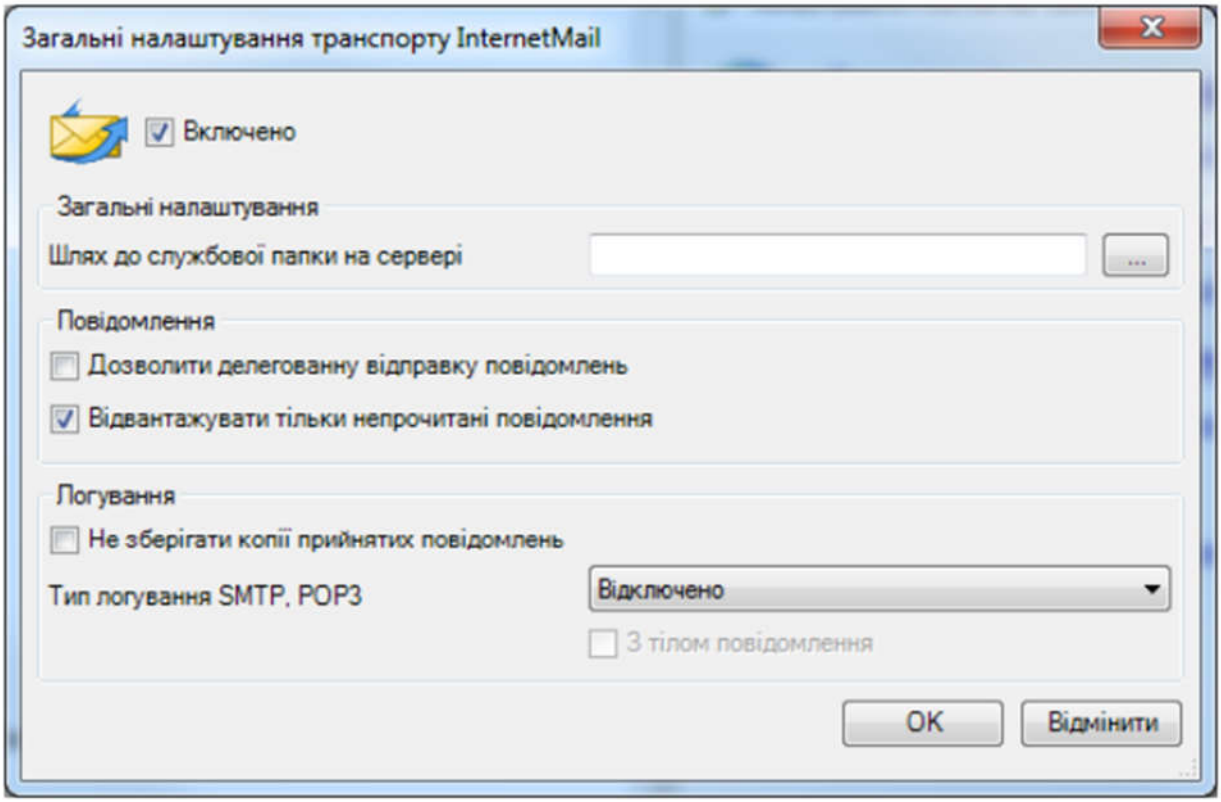
- Використовувати - включає або відключає можливість підключення до поштового сервера за допомогою поштового клієнта Microsoft Outlook.
- Мережевий інтерфейс - IP-адресу мережевої карти на сервері FossLook, через яку сервер з'єднується з локальною мережею (у разі якщо є окрема машина-шлюз з Internet) або IP-адресу мережевої карти на шлюзі, через

яку відбувається з'єднання з Internet (якщо сервер FossLook встановлений на даній машині-шлюзі).

- Порт - номер порта для з'єднання по сервера FossLook з Internet.
- Ім'я машини - доменне ім'я машини або IP-адреса машини-шлюзу з Internet (якщо сервер FossLook встановлений на інший машині, не на шлюзі, в локальній мережі).

Для роботи з внутрішніми поштовими скриньками достатньо заповнити обов'язкові поля секцій налаштувань POP3, SMTP і Маршрутизація.

Сторінка налаштувань модуля Internet Mail транспорт, обслуговуючого роботу поштового сервера:




Призначення елементів даної сторінки наступне:

- Опція Включено - включити / відключити роботу модуля (тобто вкл. / викл. поштовий сервер).
- Шлях до службової папці на сервері - альтернативний шлях для зберігання логів і ін. службових файлів поштового сервера. Якщо порожньо, використовується шлях по-замовчуванням.

- Опція Дозволити делеговану відправку повідомлень - дана опція діє в разі, коли користувачеві делеговані повноваження іншого користувача або відділу, і він відправляє повідомлення від імені іншого користувача (відділу). При включенні даної опції у одержувача в атрибутах повідомлень в колонці "відправник" вказується реальний відправник повідомлення, а в колонці "від імені" - користувач, від імені якого відправлено повідомлення. Якщо галочка знята, в обох колонках вказується тільки користувач (відділ), від імені якого відправлено повідомлення.
- Тип логування SMTP, POP3 - тип логування протоколу, можна вибрати: відключити, логування в один файл, логування в декілька файлів (кожна сесія логується в окремий файл), також можна включити додавання тіла повідомлень в логи.

Налаштування поштового сервера. Призначення елементів даної сторінки наступне:

- Список адрес заміни - списки заміни одержувачів повідомлень виду "адреса, на який відправляється лист"; "адреса, на який воно приходить".
- Список винятків локальних адрес - список локальних адрес, з яких можна відправляти листи без авторизації.
- Таймаут вихідного підключення - таймаут з'єднання з іншими SMTP серверами при відправці пошти.

- Максимальна кількість повідомлень за одну сесію - максимально можлива кількість повідомлень, які сервер може прийняти по SMTP за один раз. Повідомлення можуть бути отримані як від поштових клієнтів, так і інших поштових серверів.
- Максимальний розмір повідомлень, Мегабайт - максимально допустимий розмір повідомлення для відправки/прийому на сервері, Мб.
- ОпціяДозволяти видаляти повідомлення по POP3 - дозволяє видаляти повідомлення при заборі пошти по POP3 з поштового сервера (іншим клієнтом).
- Інтервал для повторного відправлення повідомлень з черги - задає,

через який час (год: хв: сек) буде ініційована повторна відправка повідомлення з черги (якщо попередня спроба не вдалася).

- Кількість повторних відправок повідомлень з черги - визначає кількість повторних відправок повідомлень з черги (у разі невдалих попередніх відправок). Якщо повідомлення так і не було відправлено після заданої кількості спроб, воно потрапляє в лог "Bad Messages".

Налаштування зовнішніх акаунтів. Призначення елементів даної сторінки наступне:

- Період повторення помилки, хвилини - якщо протягом заданого часу (в хв) помилка повторюється, користувачеві надсилається повідомлення.
- Період перевірки пошти - період перевірки зовнішніх акаунтів на наявність нових повідомлень.
- Опція Отримувати тільки непрочитані повідомлення - включає прийом тільки непрочитаних листів з зовнішніх серверів.

Хід роботи

1. Створити віртуальну машину.
2. Встановити та налаштувати ОС Windows Server.
3. Здійснити налаштування поштового сервера.

**Практична робота 13**. Налаштування хостинг-сервера

**Мета:** Навчитись налаштовувати та використовувати хостинг-сервер

## Теоретичні відомості

Програмним засобом для розміщення гіпертекстових навчальних систем та інформаційним центром навчального мережного комплексу повинен бути веб-вузол, який створюється на базі веб-сервера. У вузькому значенні веб-сервер — це набір програм, який забезпечує обмін даними засобами протоколу передачі гіпертексту (HTTP — Hyper Text Transfer Protocol). У широкому розумінні під веб-сервером розуміють набір апаратних і програмних засобів, що забезпечують функціонування веб- вузла. Серед веб-серверів найбільш поширеними є Apache та Microsoft Internet Information Server. Загальними вимогами до веб-серверів є: робота з мовами серверних скриптів (PHP, Perl, ASP), робота із серверами СУБД.

Враховуючи популярність Apache, PHP, MySQL, компанією Dklab (www.dklab.ru) розроблений програмний комплекс «Денвер». За допомогою цього комплексу можна організувати веб-сервер Apache з підтримкою мов PHP, Perl та сервер СУБД MySQL на комп'ютері, що працює під управлінням будь-якої ОС Windows. Як правило, при встановленні комплексу не потрібно проводити жодних додаткових налаштувань, і тому його можна використовувати навіть недостатньо підготовленим користувачем. Простота встановлення та налаштування комплексу дають змогу використовувати Денвер у процесі самостійного створення веб-сайтів учнями і вдома. Серед переваг комплексу слід відзначити його модульність, можливість розширення, кирилізований інтерфейс.

Окремо слід відзначити повну автономність комплексу Денвер, яка полягає у тому, що:

- комплекс встановлюється в одну папку і не записується жодних

даних в іншу папку або реєстр операційної системи;

- системі не потрібна спеціальна програма вилучення (деінсталяції) комплексу;
- для запуску комплексу не встановлюються додаткові сервіси.

У випадку встановлення комплексу існує можливість його запуску на іншому комп'ютері, виконавши лише копіювання його папки.

Базову конфігурацію можна завантажити із сайту компанії Dklab за адресою http://dklab.ru. У разі необхідності існує можливість завантаження додаткових складових, які містять інтерпретатор мови Perl з модулями, бібліотеки, використання яких розширюють можливості мови PHP і забезпечують роботу з архівами, графікою, базами даних, відмінними від MySQL.

Компоненти комплексу вже зконфігуровані для роботи за замовчуванням. Звичайно, для підвищення ефективності роботи та використання додаткових можливостей необхідно редагувати конфігураційні файли, проте основні, базові можливості є доступними відразу після встановлення.

До комплексу Денвер входять такі програмні складові:

- сервер Apache, до складу якого входять виконувані файли, дистрибутивні та адаптовані конфігураційні файли;
- інтерпретатор мови PHP, що містить виконувані файли, модуль для веб-сервера Apache, дистрибутивний і адаптований конфігураційний файл. Інтерпретатор, подібно до ОС Linux, працює як модуль веб-сервера Apache, що дає змогу відлагодження програм;
- сервер СУБД MySQL, до складу якого входять виконувані файли, файли повідомлень про помилки, база даних MySQL;

- phpmyadmin — веб-інтерфейс для управління базами даних;
- інтерпретатор мови Perl, що містить виконувані файли без додаткових модулів;
- програма для імітації роботи поштового сервера Sendmail, яка не

відправляє листи, а лише записує їх у файл;

- система пошуку віртуальних веб-вузлів.

Після запуску програми інсталяції здійснюється перевірка наявності необхідних для встановлення драйверів та утиліт операційної системи. Наступним кроком є задання папки, у якій будуть розміщені сервери.

Оскільки програми встановлення додаткових модулів комплексу здійснюють перегляд кореневих папок дисків, то не варто вказувати папки дуже глибокого вкладення. Програма встановлення створює віртуальний диск, який є необхідним для функціонування компонент системи. Окремий диск спрощує роботу з веб-інструментарієм, формуючи структуру папок, схожу до Unix-систем. Віртуальний диск — це диск, кореневий каталог якого збігається з однією з папок на фізичному диску. Після його створення всі дії з віртуальним диском насправді здійснюватимуться із вказаною папкою. Для уникнення конфліктів з назвами реальних дисків операційної системи віртуальному диску слід виділити одну з останніх літер латинського алфавіту, наприклад Z.

Після копіювання файлів необхідно вказати режим роботи віртуального диска:

- віртуальний диск створюється у процесі завантаження ОС Windows. У випадку завершення роботи комплексу віртуальний диск не від’єднується. Такий режим можна використовувати за необхідності роботи з віртуальним диском без запуску серверів;
- віртуальний диск створюється тільки після завантаження комплексу.

Найдоцільнішим є другий спосіб створення віртуального диска, оскільки це не сприятиме випадковому доступу до файлів комплексу.

Для зручності запуску та зупинки програм комплексу на робочому столі створюються ярлики.

Структура папок системи подібна до Unix-систем.

Open Server - це портативна серверна платформа і програмне

середовище, створене спеціально для веб-розробників з урахуванням їх рекомендацій та побажань.

До складу програмного комплексу входить великий набір серверного програмного забезпечення, багатофункціональний та зручний інтерфейс, системи адміністрування та налаштування компонентів. Програмний комплекс широко використовується для розробки, налагодження і тестування веб-проектів, а так само для надання веб-сервісів в локальній мережі.

Хоча спочатку програмні засоби, що входять до складу комплексу, не розроблялись спеціально для роботи один з одним, таке поєднання програмних засобів стало популярним серед користувачів операційної системи Windows, в першу чергу через те, що вони отримували безкоштовний комплекс програм з надійністю роботи на рівні Linux серверів.

Завдяки зручності і простоті управління програмний комплекс Open Server зарекомендував себе як першокласний і надійний інструмент необхідний кожному веб-майстру.

Ідея проекту Open Server полягає в тому, щоб користувач (розробник) не був залежним від робочого місця. Звичайний розробник часто залежить від роботи за конкретним комп'ютером, від операційної системи та програм встановлених на цьому комп'ютері. Використання програмного комплексу Open Server дозволить звільнити розробника від подібних незручностей.

Користувач отримує набір портативних (що не вимагають установки) програм для веброзробника. Якщо Open Server необхідний тільки як заміна таким програмам як Denwer, Vertrigo, Xampp і т.д., то можна скористатися версією «Mini», яка містить тільки серверну частину платформи.

Хід роботи

1. Встановити програмний комплекс (ПК) «Денвер». Встановлювати програмний засіб необхідно у каталог D:\WebServers\Прізвище, де Прізвище записуємо латинськими літерами.
2. Завантажити ПК «Денвер».

3. У вікні браузера завантажити сторінку за адресою http://localhost.

4. Ознайомитися та провести тестування функціонування віртуальних вузлів різних рівнів (для правильної роботи віртуальних вузлів потрібно відключити проксі-сервер в налаштуваннях браузера), інтерпретаторів мов веб-програмування (PHP, Perl та ін), web-інтерфейсу для роботи із сервером MySQL phpMyAdmin та інших компонентів програмного комплексу.

5. Створити віртуальний вузол: http://Прізвище.ii. Прізвище записуємо латинськими літерами.

6. Створити декілька текстових файлів з даними про себе, свої захоплення, друзів та ін. та розмістити їх у створеному вузлі.

7. Переглянути вміст створених файлів за допомогою браузера.

8. Створити віртуальний вузол (доменне ім’я третього рівня): http://Ім’я.Прізвище.ii. Ім’я і прізвище записати латинськими літерами.

9. Розмістити в каталозі, який відповідає за доменне ім’я третього рівня, файл test.php з наступним вмістом:

```
<h1>Перевірка PHP</h1>
<?
phpinfo();
?>
```

10. Переглянути вміст файла test.php у браузері та визначити версію веб-сервера Apache та інтерпретатора мови PHP, встановлених на сервері.

11. Відкрити та ознайомитися з web-інтерфейсом phpMyAdmin для роботи із сервером баз даних MySQL.

12. Переглянути вміст всіх баз даних та виписати назви таблиць бази даних phpmyadmin.

13. Закрити вікно браузера та зупинити роботу Web-сервера.

14. Виконати завдання 1-13 для програмного комплексу «Open Server».

## Перелік питань для підсумкового контролю знань

1. Мережеве адміністрування.
2. Стандарти мережевого адміністрування.
3. Стабільна працездатність мережі.
4. Аналітика функціонування мережі.
5. Робоче місце адміністратора.
6. Комутація кабелів та розміщення обладнання.
7. Обладнання серверної.
8. Програмне забезпечення.
9. Політика розподілу мережевих адрес.
10. Унікальність IP-адрес.
11. Діапазон використання адрес.
12. Налаштування DHCP-сервера.
13. Головний сервер.
14. Системні журнали.
15. Перегляд подій системного журналу.
16. Типи повідомлень.
17. Віддалене керування Active Directory.
18. Керування сервером з командного рядка.
19. Комплект PsTool.
20. Пакет Support Tools.
21. Якість роботи мережі.
22. Утиліта PING.
23. Команда ipconfig.
24. SuperScan.

25. Електронна пошта в мережі.

26. Майстер налаштування сервера.

27. POP3. SMTP.

28. Вирішення завдань адміністрування по email.

29. Інтернет для мережі.

30. Зовнішня адреса мережі.

31. Підключення до мережі Інтернет із застосуванням перетворення мережевих адрес (NAT).

32. Підключення через проксі-сервер.

33. Робота з файловою системою.

34. Пошук файлів.

35. Операції з файлами та каталогами.

36. Допоміжні засоби.

37. Керування обліковими записами.

38. Отримання списку користувачів.

39. Списки груп і користувачів.

40. Додавання облікових записів та їх розблокування.

41. Зміна прав користувачів.

42. Загальний доступ до папок і файлів.

43. Робота сценаріїв.

44. Групи рівня доступу.

45. Обмеження прав локального входу в систему на сервері.

46. Права помічника адміністратора.

47. Безправні користувачі пошти.

48. Ізолювання підмережі.

49. Автоматизоване керування політикою безпеки.

50. Керування доступом до об’єктів мережі.

51. Доступ до черг друку.

52. Доступ до інших мереж.

53. Захист мереж.

54. Віддалене керування.

55. Використання служби Telnet.

56. Дефрагментація.

57. Створення завдань.

58. Конфігурація IP-протоколу.

59. Загальний доступ до файлів.

60. Віддалений доступ до робочого столу.

61. Підключення до віддаленого робочого столу.

62. Remote Administrator.

63. Налаштування Radmin-сервера.

64. Мережевий профіль.

65. Підключення мережевого профілю.

66. Облік робочих станцій.

67. Віртуальний комп’ютер.

68. Емулятор віртуального комп’ютера.

69. Створення та налаштування віртуальних машин.

70. Керування декількома віртуальними машинами.

71. Під’єднання віртуальних комп’ютерів до мережі.

72. Віртуальна приватна мережа VPN.

73. Застосування VPN.

74. Під’єднання до робочих станцій мережі.

75. Можливі проблеми та перспективи.

76. Використання ресурсів комп’ютерів мережі.

77. Розширення можливостей робочих станцій.

78. Оточення робочих станцій.

**Список рекомендованих та використаних джерел**


1. Воробієнко П. П., Нікітюк Л. А., Резніченко П. І. Телекомунікаційні та інформаційні мережі : підручник [для вищих навчальних закладів]. Київ : Самміт-Книга, 2010. 708 с.
2. Демида Б. А., Обельовська К. М., Яковина В. С. Основи адміністрування LAN у середовищі MS Windows : навчальний посібник. Львів: Видавництво Львівської політехніки, 2014. 488 с.
3. Журавська І. М. Проектування та монтаж локальних комп’ютерних мереж : навчальний посібник. Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. 396 с.
4. Комп'ютерні мережі та телекомунікації : навч. посіб. / Ю. Г. Машкаров, І. В. Кобзев, О. В. Орлов, М. В. Мордвинцев. Харків : Вид-во ХарРІ НАДУ "Магістр", 2012. 212 с.
5. Микитишин А. Г., Митник М. М., Стухляк П. Д. Телекомунікаційні системи та мережі : нвчальний посібник. Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.
6. Рамський Ю. С., Олексюк В. П., Балик А. В. Адміністрування комп’ютерних мереж і систем : навч. посібник. Тернопіль : Навчальна книга – Богдан, 2015. 196 с.
7. Тарнавський Ю. А., Кузьменко І. М. Організація комп’ютерних мереж : підручник для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп’ютерні науки» / КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2018. 259 с.

8. Адміністрування комп’ютерних систем та мереж : конспект лекцій для студентів спеціальності 121 "Інженерія програмного забезпечення" / уклад. В. О. Ліщина. Луцьк : Луцький НТУ, 2016. 67 с.
9. Адміністрування комп’ютерних систем та мереж : конспект лекцій для студентів напряму підготовки 6.050101 «Комп’ютерні науки» / уклад. П. В. Саварин, А. А. Ящук. Луцьк : Луцький НТУ, 2016. 68 с.
10. Адміністрування комп’ютерних систем та мереж : методичні вказівки до виконання лабораторних робіт для студентів напряму підготовки 6.050101 «Комп’ютерні науки» / уклад. П.В. Саварин. Луцьк : Луцький НТУ, 2014. 91 с.
11. Адміністрування комп’ютерних мереж та операційних систем: методичні вказівки до лабораторних робіт для студентів за напрямом підготовки 6.050103 «Програмна інженерія» факультету інформаційних технологій УжНУ / Розробник: к.т.н. Поліщук В.В. Ужгород: 2017. 31 с.
12. Cisco – Україна. URL : https://www.cisco.com/c/uk_ua/index.html
13. EVE - The Emulated Virtual Environment for Network, Security and DevOps professionals. URL : http://www.eve-ng.net
14. Електронний посібник із дисципліни «Комп’ютерні системи та мережі». Укладач : к.п.н., доцент Саварин Павло Вікторович. URL : https://elib.lntu.edu.ua/sites/default/files/elib_upload/12/index.html

Навчальне видання

# АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Методичні рекомендації

**Укладачі:**

**Тищенко** Світлана Іванівна

**Пархоменко** Олександр Юрійович

**Мірошник Роман Сергійович**

**Хилько Іван Іванович**

Формат 60х84 1/16. Ум. друк. арк. 2.94.

Наклад 50 прим. Зам. № _____

Надруковано у видавничому відділі

Миколаївського національного аграрного університету

54020, м. Миколаїв, вул. Георгія Гонгадзе, 9

Свідоцтво суб'єкта видавничої справи ДК № 4490 від 20.02.2013