

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
КРЕМЕНЧУЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ІМЕНІ МИХАЙЛА ОСТРОГРАДСЬКОГО



МЕТОДИЧНІ ВКАЗІВКИ  
ЩОДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ  
З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ  
**«ПРОЕКТУВАННЯ ТА АДМІНІСТРУВАННЯ  
КОМП'ЮТЕРНИХ МЕРЕЖ»**  
ДЛЯ СТУДЕНТІВ ДЕННОЇ ФОРМИ НАВЧАННЯ  
ЗІ СПЕЦІАЛЬНОСТІ 123 – "КОМП'ЮТЕРНА ІНЖЕНЕРІЯ"  
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»  
ЧАСТИНА II

КРЕМЕНЧУК 2017

Методичні вказівки щодо виконання лабораторних робіт з навчальної дисципліни «Проектування та адміністрування комп'ютерних мереж» для студентів денної форми навчання зі спеціальності 123 – «Комп'ютерна інженерія» освітнього ступеня «Бакалавр». Частина II

Укладач к. т. н., доц. О. Г. Славко

Рецензент к. т. н., доц. В. М. Сидоренко

Кафедра комп'ютерних та інформаційних систем

Затверджено методичною радою Кременчуцького національного університету імені Михайла Остроградського

Протокол № \_\_\_\_\_ від \_\_\_\_\_ 2017 р.

Голова методичної ради \_\_\_\_\_ проф. В. В. Костін

## ЗМІСТ

Вступ .....	4
1 Перелік лабораторних робіт .....	6
Лабораторна робота № 6 Створення домену Windows Server 2012.....	6
Лабораторна робота № 7 Створення й адміністрування облікових записів користувачів і груп.....	9
Лабораторна робота № 8 Приєднання комп'ютерів до домену. Публікація ресурсів у Active Directory.....	14
Лабораторна робота № 9 Групові політики.....	19
Лабораторна робота № 10 Мережевий аналізатор Network Monitor і мережі VPN.....	24
2 Критерії оцінювання знань студентів.....	30
Список літератури.....	31

## ВСТУП

Цей навчальний курс є логічним продовженням курсу «Комп'ютерні мережі». Його мета – набуття студентами необхідних знань і навичок організації та налаштування найважливіших інфраструктурних елементів корпоративних локальних обчислювальних мереж на базі серверів Microsoft. У рамках навчального курсу також розглядаються питання IP-адресації, загальні принципи розміщення імен комп'ютерів у мережах і т. ін.

На сьогодні системне адміністрування – це не стільки адміністративна, скільки інженерно-технічна робота, що стосується апаратного і програмного забезпечення, підтримки користувачів, ремонту та профілактики. Системний адміністратор має володіти навичками як в технічній стороні справи, так і в адміністративних функціях, а також у психології користувачів.

Практикум побудований на принципах задачного підходу, тобто навчання відбувається під час розв'язання вирішення конкретних практичних завдань. Усі пропонувані завдання об'єднані в контексті великого проекту, присвяченого розробці та адміністрування мережі кафедри (факультету).

Такий підхід стимулює зацікавленість студентів навчальною дисципліною, дозволяє їм легше засвоювати нові знання і вміння під час практичної діяльності.

Основний середовищем для виконання лабораторних робіт є віртуальна машина Microsoft Virtual PC 2007, на якій встановлена операційна система Microsoft Windows Server 2012. Це середовище дозволяє виконувати складні експерименти з операційною системою і мережними настройками незалежно від реальних машин і мереж. Окрім того, студенти мають на віртуальній машині правами адміністратора, що в аудиторних умовах на університетських комп'ютерах забезпечити вкрай складно.

**Мета та завдання навчальної дисципліни:** набуття студентами необхідних знань і навичок організації та налаштування найважливіших інфраструктурних елементів комп'ютерних мереж на базі серверів Microsoft,

оволодіння практичними навичками налаштування IP-адресації, а також знаннями про загальні принципи розміщення імен комп'ютерів у мережах, загальні відомості про TCP/IP і т. і.

**Місце навчальної дисципліни у навчальному процесі:** навчальна дисципліна базується на знаннях з навчальних дисциплін «Обчислювальна техніка», «Комп'ютерні мережі», «Комп'ютерні системи».

У результаті вивчення дисципліни студент повинен

**знати:**

- принципи розпізнавання імен комп'ютерів у LAN;
  - способи призначення адрес комп'ютерів;
  - механізм маршрутизації, побудови запитів і відповідей серверів у LAN;
- основні можливості Windows Server 2012 з Active Directory для організації корпоративної мережі;
- синтаксис основних інструментів командного рядка для керування серверними об'єктами;

**уміти:**

- налаштовувати DNS і DHCP-сервери;
- користуватися статичною, автоматичною й альтернативною системами адресації клієнтських комп'ютерів;
- створювати підмережі, надмережі, статичні та динамічні маршрути;
- користуватися командним рядком і спеціальними адміністративними інструментами для аналізу мережевого трафіку й усунення несправностей на основних серверних об'єктах, а також з віддаленим доступом до мережі.

# 1 ПЕРЕЛІК ЛАБОРАТОРНИХ РОБІТ

## Лабораторна робота № 6

### Тема. Створення домену Windows Server 2012

**Мета:** навчитися створювати домен Windows Server 2012, навчитися встановлювати службу каталогу Active Directory, вивчити структуру служби каталогу Active Directory.

### Короткі теоретичні відомості

Для централізованого управління факультетської мережею необхідно створити домен на основі Microsoft Windows Server 2012.

У процесі установки може знадобитися вкласти в дисковод інсталяційний компакт-диск Windows Server 2012. Можна використовувати фізичний компакт-диск або iso-образ інсталяційного диска операційної системи.

Продивитись створений домен можна декількома способами.

*1-й спосіб.*

Відкрити My Network Places – Entire Network – Microsoft Windows Network (Моє мережне оточення – Вся мережа – мережа Microsoft Windows). Переконавшись, що з'явився запис про домен mydomain, у якому міститься один комп'ютер – Server.

*2-й спосіб.*

1. У меню Start – Programs – Administrative Tools (Пуск – Програми – Адміністрування) вибрати Active Directory Users And Computers (Користувачі і комп'ютери Active Directory). Відкриється однойменне оснащення.

2. У дереві оснащення двічі клацнути на mydomain.ua (або на імені вашого домену), щоб побачити вміст сайту mydomain.ua.

3. У розділі Domain Controllers (Контролери домену) дерева оснащення переглянути назву контролера домену та його повне ім'я DNS (наприклад, якщо ім'я ізольованого сервера було server, то після установки домену має стати server.mydomain.ua).

4. У розділі Users (Користувачі) переглянути список вбудованих облікових записів користувачів і груп користувачів домену.

5. Активізувати вбудований обліковий запис Guest (Гість) і спробувати увійти в систему. Чи вдалася спроба зробити це? На контролери домену дозволено вхід лише адміністраторам домену.

6. Закрити консоль Active Directory Users And Computers.

## Хід роботи

**Завдання 1.** Установити на сервері службу каталогу Active Directory, створити домен mydomain.ua:

1. Запустити майстер установки Active Directory Start – Run – dcpromo.

2. Дотримуючись кроків майстра установки, вибрати наступні параметри установки:

– у вікні Domain Controller Type (Тип контролера домену) – перемикач Domain controller for a new domain (Контроллер домену в новому домені);

– у вікні Create New Domain (Створити новий домен) – перемикач Domain in a new forest (Домен в новому лісі);

– у вікні Install or Configure DNS (Установка або настройка DNS) – перемикач No, just install and configure DNS on this computer (Ні, DNS уже встановлена та налаштована на цьому комп'ютері), якщо служба DNS уже встановлена на сервері, або Yes, I will configure the DNS client (Так, я буду конфігурувати клієнта DNS);

– у вікні New Domain Name (Нове доменне ім'я) наберіть mydomain.ua в рядку Full DNS Name For New Domain (Повні DNS-ім'я нового домену);

– у вікні NetBIOS Domain Name (Доменне ім'я NetBIOS) має з'явитися запис MYDOMAIN;

– переконатися, що для розміщення бази даних і протоколу вибраний шлях C:\WINDOWS\NTDS, а для розміщення каталогу SYSVOL вказано шлях C:\WINDOWS\SYSVOL;

– у вікні Permissions (Дозволи) вибрати Permissions compatible only with

Windows Server 2012 OS (Дозволи, сумісні тільки з ОС Windows Server 2012);

– у вікні Directory Services Restore Mode Administrator Password (Пароль адміністратора для режиму відновлення) введіть пароль, який хочете присвоїти цьому обліковому запису сервера Administrator у разі, якщо комп'ютер завантажиться в режимі Directory Services Restore (Режим відновлення);

– у вікні Summary (Підсумки) вивчіть список вибраних вами параметрів установки і дочекайтеся завершення процесу установки Active Directory.

3. У вікні Completing The Active Directory Installation Wizard (Завершення роботи майстра інсталяції Active Directory), кнопку Finish (Готово), а потім кнопку Restart Now (Перезавантажити комп'ютер зараз).

**Завдання 2.** Продивитись створений домен одним зі способів, зазначених у коротких теоретичних відомостях вище. *Зберегти до звіту скріншоти за результатами обох способів.*

**Завдання 3.** Перевірити роботу служби DNS за допомогою оснащення DNS:

1. Відкрити консоль DNS командою Start – Programs – Administrative Tools – DNS (Пуск – Програми – Адміністрування – DNS).

2. У дереві консолі DNS натиснути правою кнопкою на ім'я сервера та вибрати команду Properties (Властивості). Відкриється вікно властивостей SERVER (якщо у сервера інше ім'я, то воно буде зазначене в заголовку вікна).

3. Перейти на вкладку Monitoring (Спостереження).

4. У списку Select A Test Type (Вибрати тип тесту) позначити прапорці A Simple Query Against This DNS Server (Простий запит до цього DNS-сервера) і A Recursive Query To Other DNS Servers (Рекурсивний запит до інших DNS-серверів) і клацнути Test Now (Протестувати). У вікні властивостей Server у списку результатів тестування має з'явитися напис PASS (Пройдено успішно) або FAIL (Не пройдено) – у стовпцях Simple Query (Простий запит) і Recursive Query (Рекурсивний запит). *Пояснити отримані результати.*

**Завдання 4.** Видалити службу Active Directory. Запустити майстер установки і видалення Active Directory Start – Run – dcprmo.



## Зміст звіту

1. Назва та мета роботи.
2. Методика проведення роботи з графічними результатами.
3. Письмові відповіді на контрольні запитання.

## Контрольні питання

1. Опишіть відмінності між робочою групою і доменом.
2. Яка основна відмінність між ОС Windows і Windows Server 2012?
3. Чи можливо створити домен у мережі, де всі комп'ютери мережі працюють під управлінням ОС Windows?
4. Дайте визначення контролера домену.
5. Перелічіть відомі вам вбудовані облікові записи користувачів і груп користувачів домену й опишіть їх призначення.
6. Що означає термін «ізолюваний» сервер?
7. Опишіть відмінності між робочою групою і доменом.
8. Чому вбудований обліковий запис Guest (Гість), як правило, буває відключений?

**Література:** [18, 20–22].

## Лабораторна робота № 7

**Тема.** Створення й адміністрування облікових записів користувачів і груп

**Мета:** навчитися створювати, змінювати, видаляти облікові записи і групи, задавати і змінювати паролі, додавати облікові записи в групи.

## Короткі теоретичні відомості

Обліковий запис у комп'ютерній системі – це сукупність наданої інформації про користувача, засобів і прав користувача щодо

багатокористувацької системи.

Обліковий запис, як правило, містить відомості, необхідні для ідентифікації користувача під час підключення до системи, інформацію для авторизації й обліку. Це ім'я користувача та пароль (або інше аналогічний засіб аутентифікації – наприклад, біометричні характеристики). Пароль або його аналог, як правило, зберігається в зашифрованому або хешованому вигляді (із міркувань безпеки).

В ОС Windows використовуються три типи облікових записів користувачів:

- *локальний обліковий запис користувача (local user account)* – дозволяє почати сеанс на комп'ютері та скористатися його ресурсами;
- *обліковий запис користувача домену (domain user account)* – дозволяє увійти в домен і скористатися мережевими ресурсами;
- *вбудований обліковий запис користувача (built-in user account)* – дозволяє виконати адміністративні завдання та скористатися локальними або мережевими ресурсами.

Під час створення доменного облікового запису, на відміну від локального, після імені користувача відображається ім'я домену, відокремлене від останнього знаком @.

Відповідно до вимог політики безпеки мережі, до групи адміністраторів не рекомендується включати інших користувачів домену, окрім осіб, які безпосередньо виконують функції адміністрування.

## **Хід роботи**

**Завдання 1.** Створити доменний обліковий запис декана, який має доступ до всіх ресурсів мережі, може здійснювати вхід на будь-який комп'ютер:

1. Виконати команду Start – All Programs – Administrative Tools – Active Directory Users and Computers (Пуск – Програми – Адміністрування – Користувачі та комп'ютери Active Directory).

2. Розкрити папку faculty.ua у лівій панелі вікна. У вкладених папках

вибрати Users (Користувачі).

3. У меню Action (Дія) вибрати команду New – User (Новий – Користувач).

4. Ввести необхідні відомості про користувача. У розділі User logon name (Ім'я користувача під час входу в систему) ввести dean (декан). Повне ім'я користувача (User logon name) – dean@faculty.ua.

5. Під час визначення пароля користувача обов'язково встановити прапорець User must change password at next logon (Користувач повинен змінити пароль під час наступного входу в систему).

6. Завершити створення облікового запису.

7. У правій панелі знайти обліковий запис. Двічі клацнути по ньому, щоб внести додаткові відомості (адреса, організація і т. д.).

8. Переконаватися в тому, що декан може входити в систему в будь-який час (Вкладка Account – Logon Hours (Рахунок – Годинники входу)).

9. Спробувати увійти в домен під обліковим записом декана. Чому спроба не вдалася? *Запишіть у звіт причину відмови.*

10. Увійти у систему як адміністратор.

11. Подивитися властивість облікового запису декана, знову виконавши команду Start – All Programs – Administrative Tools – Active Directory Users and Computers. У вікні властивостей облікового запису вибрати вкладку Member of (Членство в групах) і додати обліковий запис декана в глобальну групу Адміністратори домену за допомогою команд Add ... – Advanced ... – Find now ... (Додати ... – Додатково ... – Знайти ...) з отриманого списку вибрати Domain Admins (Адміністратори домена).

12. Повторити спробу увійти у домен під обліковим записом декана.

13. Після входу в систему під обліковим записом адміністратора змінити пароль декана та знову задати необхідність зміни пароля під час наступного входу в систему. *Внести до звіту скріншоти вікон для пунктів 5, 8, 9, 13.*

**Завдання 2.** Виключити обліковий запис декана з групи адміністраторів:

1. Виконати команду Start – All Programs – Administrative Tools – Active

Directory Users and Computers.

2. Розкрити папку faculty.ua в лівій панелі вікна. У вкладених папках вибрати Users.

3. У правій панелі знайти обліковий запис. Двічі клацнути по ньому, перейти на вкладку Member of (Членство в групах). Серед списку груп вибрати Domain Admins і натиснути Remove. *Внести до звіту скриншот вікна, що забороняє вхід у домен.*

**Завдання 3.** Дозволити обліковому запису декана здійснювати вхід на контролер домену, не включаючи його в групу адміністраторів:

1. Додати обліковий запис декана до групи Print Operators, члени якої можуть здійснювати вхід на контролер домену.

2. Увійти у домен під обліковим записом декана.

3. Запропонувати інший спосіб, що дозволяє вхід на контролер домену.

*Внести до звіту скриншот вікна головного меню після входу декана на контролер домену. Опишіть інший спосіб вирішення входу на контролер домену декану.*

**Завдання 4.** Створити глобальну групу Teachers (Викладачі):

Тип групи – група безпеки; викладачі можуть здійснювати вхід на будь-який комп'ютер мережі, окрім сервера; для кожного з викладачів існує власний обліковий запис і настройки, що конфігурується особисто викладачем:

1. Виконати команду Start – All Programs – Administrative Tools – Active Directory Users and Computers.

2. Розкрити папку faculty.ua у лівій панелі вікна. У вкладених папках вибрати Users.

3. У меню Action вибрати команду New – Group (Нове – Група).

4. У полі Group Name (Назва групи) ввести Teachers.

5. В області Group Scope (Область дії групи) натиснути перемикач Global (Глобальна), а в області Group Type (Тип групи) – перемикач Security (Безпека).

6. Натиснути ОК.

**Завдання 5.** Додати до групи Teachers (Викладачі) члена групи обліковий

запис декана:

1. Переконайтеся, що відкрите оснащення Active Directory Users and Computers і вибрано контейнер Users.

2. У вікні властивостей групи Teachers вибрати вкладку Members (Члени групи), а потім послідовно кнопки Add... – Advanced... – Find now..., з отриманого списку вибрати обліковий запис декана.

3. У вікні властивостей облікового запису декана знайти інформацію про членство в групі Teachers. *Внести до звіту скриншот відповідного вікна.*

### **Зміст звіту**

1. Назва та мета роботи.
2. Методика проведення роботи з графічними результатами.
3. Письмові відповіді на контрольні запитання.

### **Контрольні питання**

1. Опишіть відмінності між локальним і доменним обліковими записами.
2. Із якою метою створюють групи користувачів?
3. Поясніть призначення локальних, глобальних і універсальних груп.
4. Пояснити значення груп безпеки груп розповсюдження.
5. Дайте визначення і наведіть приклади для наступних термінів: «Права користувачів», «привілеї користувачів», «дозвіл доступу користувачів».
6. Перерахуйте відомі вам вбудовані облікові записи користувачів і груп користувачів домену та опишіть їх призначення.
7. У яку вбудовану групу користувачів, відмінну від групи адміністраторів, потрібно включити обліковий запис, щоб користувач міг здійснювати вхід на робочу станцію? Чи існують інші способи зробити це?
8. Як заборонити вхід в систему у вихідні дні та неробочий час?
9. Як обмежити термін дії облікового запису?
10. Як відключити обліковий запис працівника, наприклад, під час його хвороби?

11. Назвіть довжину пароля мінімально рекомендовану і максимально можливу.

12. Як змінити пароль користувача?

13. Як заборонити зміну пароля користувачем?

14. Які наслідки видалення групи?

**Література:** [1, 6, 7, 9, 14, 18].

### **Лабораторна робота № 8**

**Тема. Приєднання комп'ютерів до домену. Публікація ресурсів у Active Directory**

**Мета:** навчитися приєднувати комп'ютери до домену, вивчити способи публікації ресурсів, навчитися задавати і змінювати права доступу, запускати програми від імені іншого користувача.

#### **Короткі теоретичні відомості**

Окрім користувачів членами домену є комп'ютери. Ви має забезпечити підключення всіх комп'ютерів факультету до домену faculty.ua. Основною метою створення комп'ютерної мережі є спільне використання ресурсів.

У факультетській мережі основним видом ресурсів є файли і папки. Їх слід надати у загальний доступ. Для запобігання конфліктних ситуацій адміністратору слід призначити всім користувачам домену права доступу до загальних ресурсів, що відповідають їх повноваженням.

Для **приєднання комп'ютера до домену** на робочій станції необхідно відкрити вікно System Properties (Властивості системи), виконавши одну з команд Settings (Налаштування) – Control Panel (Панель управління) – System (Система) або викликати із контекстного меню вікно властивостей папки My Computer (Мій комп'ютер).

Для того, щоб **відкрити загальний доступ до папки**, що розташована на

сервері та буде слугувати для тимчасового розміщення файлів усіх користувачів мережі (будь-який користувач мережі зможе зберігати в ній свої файли і папки, переглядати її вміст, але він не повинен мати прав на зміну доступу до неї), необхідно виконати наступні дії:

1. Створити на сервері папку UserDocs. Помістити в неї текстовий файл, що містить ваші особисті дані.

2. У контекстному меню папки вибрати Sharing & Security... (Загальний доступ і безпека).

3. На вкладці Sharing (Доступ) вибрати Share this folder... (Надати в загальний доступ). У пункті Share name... (Ім'я папки загального доступу) набрати ім'я «Студенти» – під таким ім'ям папка UserDocs буде доступна користувачам мережі.

4. На вкладці Security (Безпека) надати групам користувачів домену права читання та запису на цю папку (установити відповідні прапорці в стовпці Allow), але не дозволяти повний доступ.

5. Якщо в розділі Group or user names (Імена груп або користувачів) присутні не всі облікові записи та групи, то їх можна додати допомогою команд Add... – Advanced... – Find now...(Додати – Додатково – Знайти). Із отриманого списку вибрати необхідні об'єкти доступу.

Для того, щоб **видалити робочу станцію з домену** необхідно виконати наступні дії:

1. На робочій станції зайти під обліковим записом адміністратора.

2. Викликати вікно властивостей папки My Computer (Мій комп'ютер).

3. На вкладці Computer Name (Ім'я комп'ютера) натисніть Network ID (Ідентифікація).

4. На вкладці Connecting to the Network (Підключення до мережі) виберіть This computer is for home use and not a part of business network (Комп'ютер призначений для домашнього використання і не входить до корпоративної мережі).

## Хід роботи

**Завдання 1.** Задати мережні параметри робочої станції: ім'я робочої станції – user1; IP-адресу надати з тієї ж підмережі, що і контролер домену (якщо не працює сервер DHCP).

**Завдання 2.** Переконатися в можливості встановлення зв'язку між контролером домену та робочою станцією. *Помістити у звіт скріншот, у якому відображено підтвердження встановлення зв'язку між комп'ютерами.*

**Завдання 3.** Включити робочу станцію до домену. Розглянути процес на прикладі включення робочої станції user1 у домен faculty.ua:

1. Для приєднання комп'ютера до домену на робочій станції відкрити вікно System Properties (Властивості системи), виконавши одну з команд Settings (Настройки) – Control Panel (Панель управління) – System (Система) або викликати з контекстного меню вікно властивостей папки My Computer (Мій комп'ютер).

2. Перейти на вкладку Computer Name (Ім'я комп'ютера).

3. Вибрати Network ID (Ідентифікація). Відкриється майстер мережевої ідентифікації Network Identification Wizard. Натиснути Next (Далі).

4. На вкладці Connecting to the Network (Підключення до мережі) вибрати This computer is part of a business network, and I use it to connect to other computers at work (Комп'ютер належить до корпоративної мережі, і під час роботи я використовую його для з'єднання з іншими комп'ютерами).

На цій вкладці існує другий варіант. Який? У яких випадках він застосовується?

5. Вибрати тип мережі – My company uses a network with domain (Моя організація використовує мережу з доменами).

6. У вікні Network Information (Мережева інформація) вивчити, які мережеві параметри знадобляться.

7. У вікні User Account and Domain Information (Відомості про облікову запису і домені) залишити все без змін. Натиснути Next.

8. У вікні Computer Domain (Домен комп'ютера) записати ім'я домену і



вузла – Computer name (Ім'я комп'ютера) – user1, а Computer domain (Домен комп'ютера) – faculty. Натисніть Next.

9. З'явиться вікно, у якому потрібно ввести ім'я та пароль запису, який має дозвіл на додавання користувачів до домену. Наприклад, у лабораторній роботі це будуть:

- User name – Administrator;
- Password – порожній (або поточний пароль адміністратора);
- Domain – faculty.ua;

10. У вікні User Account буде запропоновано додати нових користувачів. Вибрати перемикач Do not add user at this time (Не додавати учасників у цей час).

11. Натиснути Finish (Готово) і перезавантажити комп'ютер. *Внести до звіту скріншот вікна Computer Name (Ім'я комп'ютера) робочої станції.*

**Завдання 4.** На робочій станції увійти у систему під одним з доменних облікових записів.

*Внести до звіту скріншоти вікон Log on to Windows і головного системного меню після входу користувача на робочу станцію.*

**Завдання 5.** Відкрити загальний доступ до папки Users, розташованої на сервері.

*Внести до звіту скріншот вікна Security (Безпека) з відповідними установками для кожного користувача домену. Чому не рекомендується встановлювати повний доступ на папку Студенти для користувачів домену? Записати у звіт відповідь.*

**Завдання 6.** Отримати доступ до папки «Студенти» із робочої станції домену:

1. На робочій станції зайти під будь-яким доменним обліковим записом.
2. Отримати доступ до папки можна одним з таких способів:

– у мережевому оточенні знайти папку Users;

– виконати команду Start – Run (Пуск – Виконати) і ввести ім'я в форматі

\\ <ім'я сервера> \ <ім'я папки>. Наприклад: \\ server \ users.

3. Переконалися в тому, що тут ви зможете зберігати свої документи, змінювати наявні, але вам відмовлено змінювати права доступу на папку.

*Внести до звіту скриншот вікна повідомлення, що забороняє зміни прав доступу.*

**Завдання 7.** Підключити загальну папку Студенти як мережевий диск G:

1. Увійти під обліковим записом студента.
2. Відкрити контекстне меню папки Студенти.
3. Скористатися командою My Network Places (Моє мережне оточення) – Map Network Drive (Підключити мережевий диск).

**Завдання 8.** Вивчити використання команди Run As:

1. Увійти на сервер під обліковим записом адміністратора.
2. Помістити у папці Студенти з загальним доступом додаток, ярлик програми або програму з Control Panel.
3. Заборонити студенту доступ до об'єкта.
4. На робочій станції зайти під обліковим записом студента.
5. Відкрити папку Студенти і спробувати відкрити об'єкт. Скопіювати у буфер вікно, що забороняє доступ до об'єкта.
6. Виділити об'єкт і, утримуючи Shift, вибрати у контекстному меню команду Run As (Запустити як).
7. Установити перемикач Run The Program As The Following User (Запустити програму від імені наступного користувача).
8. У полі User name ввести mydomain \ Administrator, а в Password – пароль адміністратора. Натиснути ОК.
9. Запустити об'єкт.

*Внести до звіту скріншоти вікна, що забороняє доступ до об'єкта, вікна Run As, вікна програми або іншого об'єкта після отримання доступу до нього.*

**Завдання 9.** Видалити робочу станцію з домену.

*Внести до звіту скриншот, що забороняє зміни прав доступу. Запропонуйте інший спосіб виключення робочої станції з домену.*

## Зміст звіту

1. Назва та мета роботи.
2. Методика проведення роботи з графічними результатами.
3. Письмові відповіді на контрольні запитання.

## Контрольні питання

1. Як визначити, чи є комп'ютер членом домену або робочої групи?
2. Які дозволи існують для загальних папок?
3. Як скасувати успадкування властивостей об'єкта від батьківської папки?
4. Чи може користувач заборонити доступ адміністратору до своєї папки?  
Чи зможе адміністратор у цьому разі повернути права?
5. Опишіть права суб'єктів доступу – Власник і Адміністратор.
6. Яка утиліта, що не вимагає зміни користувача, дозволяє виконувати дії від імені іншого користувача?

**Література:** [2–5, 9, 19–21].

## Лабораторна робота № 9

### Тема. Групові політики

**Мета:** вивчити способи завдання групових політик, види параметрів групових політик, об'єкти групових політик, навчитися задавати групові політики для різних об'єктів.

### Короткі теоретичні відомості

Групові політики дозволяють реалізувати гнучке управління членами доменами – користувачами і комп'ютерами. У роботі потрібно навчитися використовувати групові політики і застосовувати їх для управління членами домену faculty.ua відповідно до вимог проекту.

*Групова політика* – це набір правил, відповідно до яких відбувається налаштування робочого середовища ОС Windows. Групові політики створюються в домені та реплікуються в межах домену. Об'єкт групової політики (Group Policy Object, GPO) складається з двох фізично розділених складових: контейнера групової політики (Group Policy Container, GPC) та шаблону групової політики (Group Policy Template, GPT). Ці два компоненти містять у собі всю інформацію про параметри робочого середовища, що входять до складу об'єкта групової політики. Політики застосовуються зверху вниз ієрархією каталогу Active Directory.

За замовчуванням в ієрархії каталогу Active Directory створюються дві групові політики з надзвичайно виразними іменами:

- 1) Default Domain Policy (політика домену за замовчанням),
- 2) Default Domain Controller's Policy (політика контролера домену за замовчуванням).

Перша з них призначається домену, а друга — контейнеру, до складу якого входить контролер домену. За замовчуванням правом створення нових GPO володіють групи Enterprise Administrators (Адміністратор підприємства) і Domain Administrators (Адміністратори домену). Щоб створити новий об'єкт групової політики, необхідно виконати такі дії:

1. Переконайтеся в тому, що ви підключилися до системи з використанням облікового запису, що належить до однієї з груп: Domain Administrators або Enterprise Administrators.

2. Переконайтеся в тому, що в системі, до якої ви підключилися, установлені засоби адміністрування, необхідні для роботи з груповими політиками. Зокрема, вам буде потрібна оснастка Active Directory Users and Computers (Active Directory – користувачі та комп'ютери). Цьому оснащенню відповідає файл dsa.msc.

3. Відкрийте консоль Active Directory Users and Computers (Active Directory – користувачі та комп'ютери) і перейдіть до контейнера OU, щодо якого ви маєте намір застосувати політику.

4. Правою кнопкою миші клацніть на контейнері OU, з'явиться меню для вибору пункт Properties і перейдіть на вкладку GPO.

5. Щоб створити новий об'єкт GPO і призначити його поточному контейнеру, клацніть на кнопці New.

6. У списку посилань на об'єкти GPO з'явиться нова позиція, рядок імені якої буде знаходитися в режимі редагування. Дайте новому об'єктові GPO змістовне ім'я.

Створена політика є лише заготовкою. Її вміст формується на основі адміністративних шаблонів, що містяться в папці SysVol контролера домену, на якому був створений GPO. Ці шаблони можна розширити і модифікувати відповідно до потреб вашої організації. До наявних компонентів об'єкта GPO можна додати створені вами розширення. Наприклад, за допомогою групової політики можна керувати налаштуваннями прикладних програм. Інформація про те, як створювати свої власні розширення GPO, міститься в SDK (Windows 2000) (Software Development Kit). Після створення GPO слід модифікувати значення параметрів цього об'єкта так, щоб налаштувати визначену груповою політикою конфігурацію робочого середовища. На вкладці Group Policy (Групова політика) клацніть на кнопці Edit. При цьому запуститься редактор групової політики, за допомогою якого можна модифікувати конфігурацію комп'ютерів і користувачів, що визначається політикою.

### **Хід роботи**

**Завдання 1.** Задати у домені політику, відповідно до якої на рівні всього домену під час установці пароля користувача потрібно було б таке: довжина пароля – не менше 8 символів; користувач не може встановити жоден з трьох попередніх паролів; пароль має відповідати вимогам складності; максимальний вік пароля – 60 днів:

1. Для запуску консолі управління MMC виконати Start – Run – mmc.
2. Для управління об'єктами групової політики на рівні домену в консолі MMC необхідно додати оснащення Group Policy Object Editor командою File

(Консоль) – Add (Додати) – Remove Snap-in... (Додати або видалити оснастку) – Add... (Додати) і вибрати зі списку відповідну оснастку.

3. Для визначення об'єкта дії політики натиснути Browse... (Огляд...).

4. Вивчити вікно і перерахувати об'єкти групових політик.

5. Вибрати Default Domain Policy. Натисніть Finish (Готово). У лівому вікні консолі повинно з'явитися оснащення Default Domain Policy <ім'я контролера домену> Policy.

6. Розгорнути оснащення та вибрати Computer Configuration – Windows Settings – Security Settings – Account Policies – Password Policy.

7. Вивчити політики паролів і встановити установки відповідно до завдання.

8. Створити нового користувача і перевірити правильність налаштувань.

*Записати у звіт об'єкти групових політик. Внести до звіту скріншот вікна, що відображає встановлені параметри політики.*

**Завдання 2.** Задати політику на рівні всього домену, що виконує блокування облікових записів на 5 хвилин у тому разі, якщо поспіль було зроблено не менше трьох помилок входу в систему.

1. Відповідна політика перебуває в наступному розділі: Computer Configuration (Конфігурація комп'ютера) – Windows Settings (Конфігурація Windows) – Security Settings (Налаштування безпеки) – Account Policies (Політики облікових записів) – Account Lockout Policy (Політика блокування облікового запису).

2. Переконайтеся, що установки політики шляхом декількох спроб ввести неправильний пароль користувача на робочій станції.

3. Зайти на контролер домену, щоб розблокувати обліковий запис користувача. *Внести до звіту скріншоти вікна, що повідомляє про блокування облікового запису на робочій станції, і вікно зняття блокування.*

**Завдання 3.** Створити організаційний підрозділ StudentSecurity.

1. Виконати команду Start – Programs – Administrative Tools – Active Directory Users and Computers (Пуск – Програми – Адміністрування –

Користувачі та комп'ютери Active Directory).

2. Розкрити папку faculty.ua в лівій панелі вікна.

3. У меню Action виберіть команду New – Organization Unit.

4. У вікні New Object – Organization Unit (Новий об'єкт – Підрозділ) у полі Name набрати StudentSecurity.

5. Помістити в організаційний підрозділ обліковий запис студента.

6. Правою кнопкою клацнути по новому об'єкту, вибрати Properties (Властивості) – Security (Безпека).

7. Переглянути список груп, що володіють правом доступу до підрозділу StudentSecurity.

**Завдання 4.** Задати політику на рівні організаційного підрозділу StudentSecurity, що забороняє змінювати картинку робочого столу і завантажує загальну для всіх картинку.

1. Відкрити вікно StudentSecurity.

2. Виконати команду User Configuration (Конфігурація користувача) – Administrative Templates (Адміністративні шаблони) – Desktop (Робочий стіл) – ActiveDesktop, вибрати параметр, що забороняє зміну картинки і задати загальну картинку робочого столу для всього підрозділу.

3. Переконаватися в правильності налаштування.

### **Зміст звіту**

1. Назва та мета роботи.

2. Методика проведення роботи з графічними результатами.

3. Письмові відповіді на контрольні запитання.

### **Контрольні питання**

1. Що таке групова політика.

2. До яких об'єктів можна застосувати групові політики?

3. Де розташований об'єкт локальної групової політики?

4. Навести приклади нелокальних об'єктів групової політики.

5. У чому полягає різниця між конфігураційними і користувацькими параметрами?

6. Які вимоги висуваються до складного паролю?

**Література:** [2–7, 14, 19].

## **Лабораторна робота № 10**

### **Тема. Мережевий аналізатор Network Monitor і мережі VPN**

**Мета:** навчитися працювати з мережевим аналізатором кадрів Network Monitor, встановлювати і налаштовувати мережі VPN.

### **Короткі теоретичні відомості**

Мережевий аналізатор Network Monitor, що належить до Microsoft Windows Server 2012, використовується для аналізу та виявлення проблем у локальній мережі. Network Monitor дозволяє вести журнал мережевої активності, копію якого можна відіслати професійним мережевим аналітикам або в службу підтримки. Розробники мережевого програмного забезпечення застосовують Network Monitor для моніторингу та налагодження своїх додатків.

Віртуальні приватні мережі (Virtual Private Networks, VPN) дозволяють забезпечити безпечний доступ до ресурсів мережі. Припустимо, декан факультету захотів мати захищене з'єднання з сервером, тобто таке з'єднання, повідомлення з якого не можуть бути прочитані навіть у разі перехопленні повідомлення. Рішенням цієї задачі є настройка VPN.

Вікно Network Monitor містить елементи, наведені на рис. 3.

Network Monitor відображає загальну статистику відслідковується трафіку, у тому числі: відомості про широкомовних кадрах (Broadcast); відомості про багатоадресні кадри (Multicast); статистику використання мережі; кількість отриманих байт у секунду; кількість отриманих кадрів у секунду і т. д.



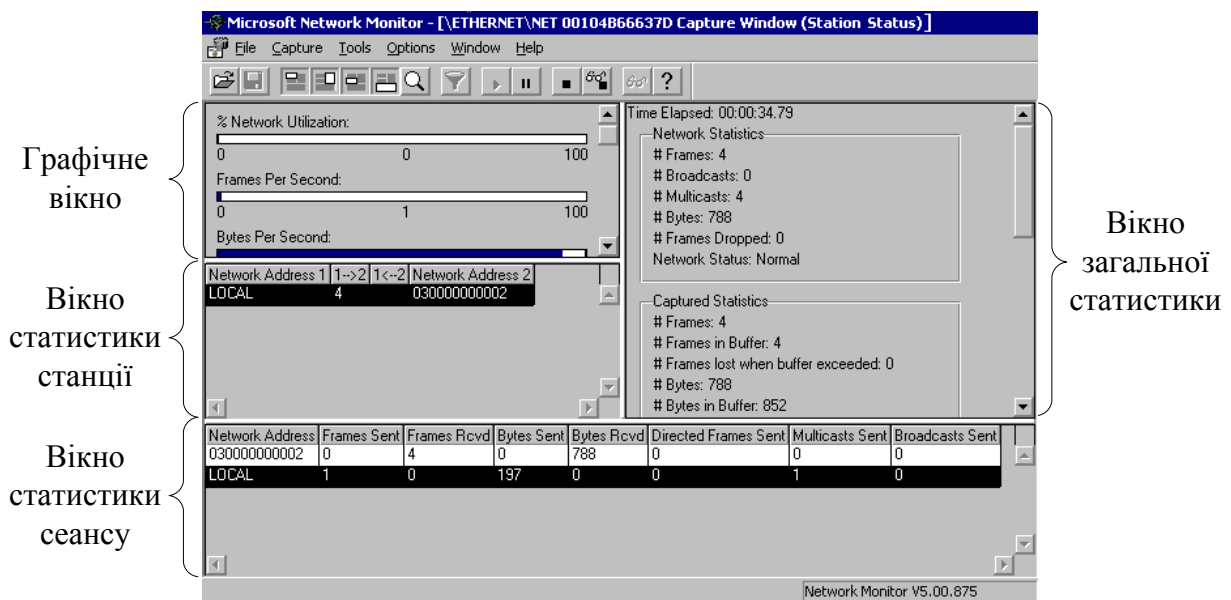


Рис. 3 – Елементи вікна Network Monitor

Зупинити моніторинг у Network Monitor можна за допомогою меню Capture – Stop або клавіші F11. Переглянути інформацію про отримані кадри: меню Capture – Display Captured Data (Захоплення – Перегляд зібраних даних) або клавіша F12. У вікні Summary (Загальна інформація) відобразиться докладна інформація про всі зібрані кадри. Подвійне клацання на будь-якому кадрі відкриє докладну статистику з цього кадру (рис. 4).

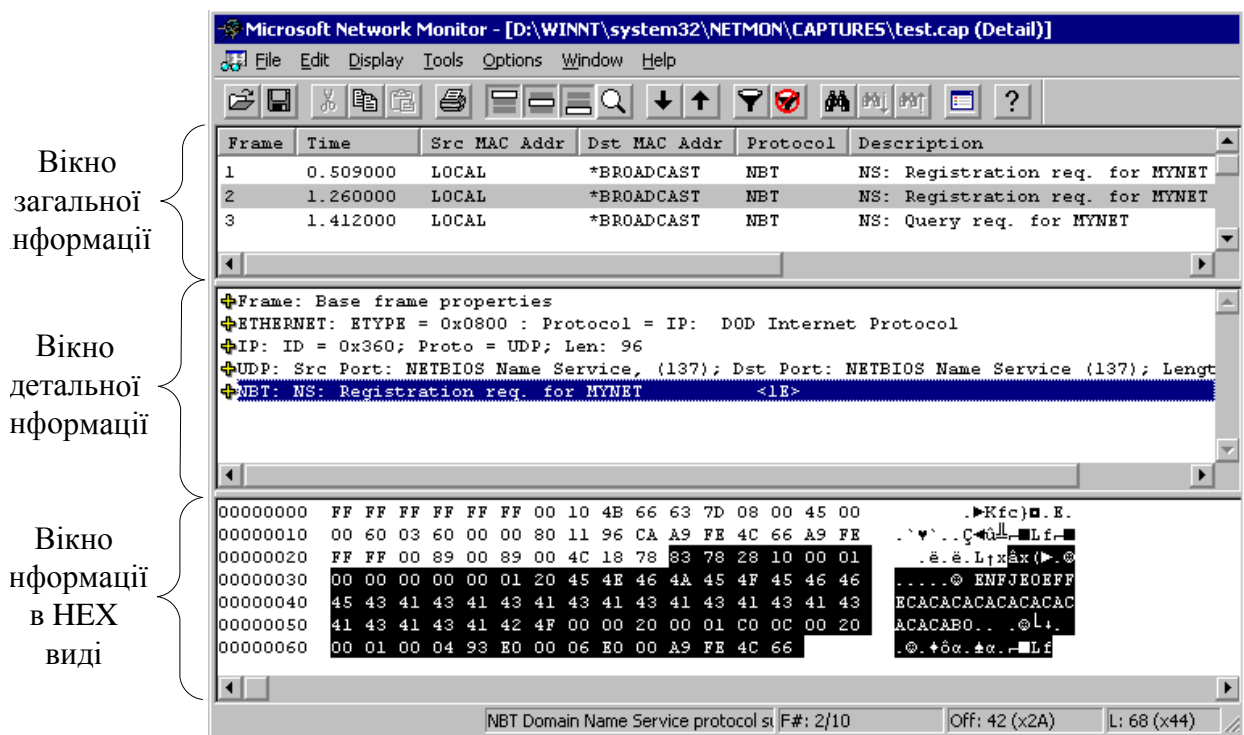


Рис. 4 – Елементи вікна Summary

У вікні Summary Pane (Вікно загальної інформації) відображається: Frame – номер кадру; Time – час захоплення кадру; Src MAC Addr – MAC-адресу джерела; Dst MAC Addr – MAC-адресу приймача; Protocol – протокол, що передав кадр; Description – опис кадру; Src Other Addr – ім'я джерела; Dst Other Addr – ім'я приймача; Type Other Addr – тип протоколу нижнього рівня.

За допомогою Network Monitor можна переглядати інформацію, передану по мережі, якщо вона незашифрована.

Для перегляду зібраних кадрів необхідно відкрити вікно Summary, де в одному з кадрів можна прочитати надіслане повідомлення. Якщо повідомлення не вдалося відправити, це свідчить, швидше за все, про те, що на сервері за замовчуванням відключена служба Messenger.

Щоб увімкнути службу, необхідно відкрити оснащення Services: Start – All Programs – Administrative Tools – Services. Далі необхідно знайти службу Messenger, клацнути по ній два рази, вибрати у списку Startup type тип Manual, натиснути кнопку Apply. Потім натиснути кнопку Start і кнопку OK.

Передача текстової інформації в незашифрованому вигляді по відкритих мережах небезпечна. Розв'язання проблеми – організація віртуальних приватних мереж VPN.

Для того, щоб встановити VPN-сервер необхідно відкрити оснащення Routing and Remote Access (Маршрутизація та віддалений доступ): Start – All Programs – Administrative Tools – Routing and Remote Access.

Якщо VPN-сервер встановлений і запущений необхідно встановити діапазон IP-адрес, які VPN-сервер може призначати VPN-клієнтам. Для цього необхідно в контекстному меню сервера вибрати пункт Properties (Властивості). Перейдіть на вкладку IP, вибрати Static address pool (Діапазон статичних адрес), натиснути кнопку Add (Додати), ввести початковий і кінцевий адреси діапазону, наприклад 192.168.2.1–192.168.2.10 і натиснути OK.

Для активізації можливості віддаленого підключення в однієї з облікових записів необхідно відкрити оснащення Active Directory Users and Computers (Користувачі і комп'ютери Active Directory), вибрати будь-який обліковий запис,

наприклад, Administrator (Адміністратор). У контекстному меню облікового запису вибрати пункт Properties (Властивості), перейти на вкладку Dial-in (Комутований доступ), у розділі Remote Access Permission (Dial-in or VPN) вибрати пункт Allow access (Дозволити доступ), натиснути ОК. Для перевірки параметрів підключення в контекстному меню з'єднання необхідно вибрати пункт «Стан», перейти на вкладку «Відомості» і вписати параметри «Тип сервера», «Перевірка справжності», «IP-адреса сервера» і «IP-адреса» клієнта.

### **Хід роботи**

**Завдання 1.** Установити мережевий аналізатор Network Monitor:

1. Запустити віртуальну машину з Windows Server 2012. У панелі управління (Start – Control Panel) виберіть пункт Add or Remove Programs. Клацнути кнопку Add / Remove Windows Components.

2. У вікні Windows Component Wizard (Майстер компонентів Windows) вибрати Management And Monitoring Tools і клацнути кнопку Details.

3. У вікні Management And Monitoring Tools позначити прапорець Network Monitor Tools (Інструменти Мережевого монітора) і натиснути ОК.

4. У вікні Майстра компонентів Windows клацнути Next.

**Завдання 2.** Виконати моніторинг мережевих кадрів за допомогою Network Monitor:

1. Запустити Network Monitor: Start – All Programs – Administrative Tools – Network Monitor (Пуск – Програми – Адміністрування – Мережевий монітор).

2. Запустити моніторинг кадрів: меню Capture – Start або клавіша F10.

3. Запустити з командного рядка утиліту ping і перевірити доступність фізичного комп'ютера: ping 192.168.1.10

4. Зупинити моніторинг у Network Monitor (див. теоретичні відомості).

**Завдання 3.** Перехоплення текстових повідомлень.

1. Запустити моніторинг кадрів у Network Monitor.

2. З командного рядка на сервері відправити текстове повідомлення на клієнтський комп'ютер за допомогою команди net send:

net send 192.168.1.10 Hello!

3. Після передачі повідомлення зупинити моніторинг кадрів. Відкрити вікно Summary для перегляду зібраних кадрів (рис. 5). Увімкнути службу (див. короткі теоретичні відомості). Спробувати надіслати повідомлення ще раз.

**Завдання 4.** Установка сервера віртуальної приватної мережі (VPN).

1. Установити VPN-сервер (див. короткі теоретичні відомості).

2. У контекстному меню сервера вибрати пункт Configure and Enable Routing and Remote Access (конфігурувати і активувати маршрутизацію та віддалений доступ). У вікні майстра Routing and Remote Access Server Setup Wizard вибрати пункт Custom configuration. Установити прапорець VPN access (Доступ VPN). На пропозицію запустити службу потрібно відповісти Yes (Так).

3. Установити діапазон IP-адрес, які VPN-сервер може призначати VPN-клієнтам (див. короткі теоретичні відомості).

4. Активізувати можливості віддаленого підключення в однієї з облікових записів (див. короткі теоретичні відомості).

**Завдання 5.** Налаштувати VPN-клієнт для отримання доступу до ресурсів видаленого комп'ютера.

1. Запустити віртуальну машину з Windows XP (ті самі дії за наявності дозволів можна виконувати на фізичному комп'ютері).

2. Відкрити вікно мережних підключень (Пуск – Панель управління – Мережеві підключення). Зліва в розділі Мережеві завдання вибрати «Створення нового підключення». У «Майстрі нових підключень» вибрати «Підключити до мережі на робочому місці», потім – «Підключення до віртуальної приватної мережі». У наступному вікні ввести назву для підключень (наприклад, «VPN»).

Потім необхідно вибрати "Не набирати номер для попереднього підключення". У наступному вікні слід ввести IP-адресу VPN-сервера (192.168.1.1). Натиснути кнопку «ОК».

3. Для підключення до VPN-серверу необхідно відкрити створене підключення та ввести у поле імені користувача ім'я того облікового запису,

якому дозволено доступ до VPN-сервера. Якщо встановлено пароль, ввести його. Натиснути кнопку «Підключення». Якщо все правильно, має встановитися VPN- підключення, а в правому нижньому кутку екрана має з'явитися значок підключення.

4. Перевірити параметри підключення. Переконайтеся, що обидві адреси належать тому діапазону, який ви призначили на VPN-сервер.

**Завдання 6.** Спробувати перехопити повідомлення в VPN-підключення.

1. На віртуальній машині з Windows Server 2012 запустити моніторинг кадрів у Network Monitor.

2. Передати текстове повідомлення на VPN-клієнт за допомогою команди net send. Використовувати IP-адресу клієнта, вписаний з вкладки Відомості VPN-підключення, наприклад: net send 192.168.2.2 Hello!

3. Після передачі повідомлення зупинити моніторинг у NetworkMonitor. Перейти у вікно Summary і спробувати знайти текстове повідомлення. За результатами зробити висновки.

### **Зміст звіту**

1. Назва та мета роботи.
2. Методика проведення роботи з графічними результатами.
3. Письмові відповіді на контрольні запитання.

### **Контрольні питання**

1. Для чого використовується мережевий аналізатор Network Monitor?
2. Які види фільтрів дозволяє застосовувати Network Monitor?
3. Для чого слугує VPN?
4. Назвіть протоколи аутентифікації, що застосовуються в VPN.
5. Як у з'єднанні VPN можна вибрати протокол PPTP або L2TP?
6. Як захищаються пакети, передані по VPN?

**Література:** [12, 14, 15, 18, 22].

## 2 КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ

У 8-му семестрі студенти виконують 10 лабораторних робіт. Загальна кількість балів, яку отримують студенти за виконання лабораторних робіт, становить 25 балів – сума за захист виконаних лабораторних робіт (максимально по 2,5 бала на кожную лабораторну роботу).

### Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		Для іспиту, курсового проекту (роботи), практики	Для заліку
90–100	A	Ввідмінно	Зараховано
82–89	B	Добре	
74–81	C		
64–73	D	Задовільно	
60–63	E		
35–59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання
0–34	F	Незадовільно з обов'язковим повторним вивченням навчальної дисципліни	Не зараховано з обов'язковим повторним вивченням навчальної дисципліни

## СПИСОК ЛИТЕРАТУРИ

1. Вишнеvский А. Служба каталога Windows 2008 : учебный курс / А. Вишнеvский. – СПб.: Питер, 2009. – 464 с.
2. Джост М. Безопасность IIS, 2-е изд. / М. Джост, М. Кобб. – М. : НОУ «Интуит», 2016. – 192 с.
3. Tulloch M. Introducing Windows Server 2012. RTM Edition / M. Tulloch, etc. – Redmond : Microsoft Press, 2012. – 239 p.
4. Моримото Р. Microsoft Windows Server 2012. Полное руководство / Р. Моримото и др. – М. : «Вильямс», 2013. – 1456 с.
5. Реймер С. Windows Server 2008 Active Directory Resource Kit / С. Реймер, К. Кезема, М. Малкер, Б. Райт. – СПб. : Питер, 2009. – 816 с.
6. Минаси М. Windows Server 2012 R2. Полное руководство. Том 2. Дистанционное администрирование, установка среды с несколькими доменами, виртуализация, мониторинг и обслуживание сервера / М. Минаси и др. – М. : Вильямс, 2015. – 864 с.
7. Минаси М. Windows Server 2012 R2. Полное руководство. Том 1. Установка и конфигурирование сервера, сети, DNS / М. Минаси и др. – М. : Вильямс, 2014. – 960 с.
8. Линн С. Администрирование Microsoft Windows Server 2012 / С. Линн. – СПб. : Питер, 2014. – 304 с.
9. Разработка инфраструктуры сетевых служб Microsoft Windows Server 2008. Учебный курс MCSE. – М. : Изд-во Русская редакция, 2009. – 520 с.
10. Marshall N. Mastering VMware vSphere / N. Marshall, S. Lowe, G. Orchard, J. Atwell. – Indianapolis : Wiley Publishing, Inc., 2015. – 840 p.
11. Minasi M. Mastering Windows Server 2008 R2 / M. Minasi, D. Gibson, A. Finn, W. Henry, B. Hynes. – Indianapolis : Wiley Publishing, Inc., 2010. – 1454 p.
12. Stallings W. Operating Systems: Internals and Design Principles : 8<sup>th</sup> edition / W. Stallings. – Prentice Hall, 2014. – 800 p.
13. Бозуэлл У. Внутренний мир Windows Server 2003, SP1 и R2: Inside

Windows Server 2003 / У. Бозуэлл. – М. : «Вильямс», 2006. – 1264 с.

14. Рассел Ч. Microsoft Windows Server 2008 : справочник администратора / Ч. Рассел, Ш. Кроуфорд. – М. : ЭКОМ Паблишерз, 2009. – 1360 с.

15. Михеев М. Администрирование VMware vSphere 4.1. Администрирование и защита / М. Михеев. – М. : ДМК Пресс, 2012. – 236 с.

16. Ли К. DNS и BIND, 5-е издание / К. Ли, П. Альбитц; пер. с англ. – СПб. : Символ Плюс, 2008. – 712 с.

17. Трич Б. Microsoft Windows Server 2003. Службы терминала / Б. Трич. – СПб. : Эком, 2006. – 688 с.

18. Моримото Р. Microsoft Windows Server 2012 : полное руководство / Р. Моримото, М. Ноэл, О. Драуби, Р. Мистри, К. Амарис. – М. : Вильямс, 2011. – 1456 с.

19. Торчинский Ф. UNIX. Практическое пособие администратора / Ф. Торчинский. – М. : Символ-Плюс, 2005. – 400 с.

20. Лимончелли Т. Системное и сетевое администрирование. Практическое руководство / Т. Лимончелли, К. Хоган, С. Чейлап. – М. : Символ-Плюс, 2009. – 944 с.

21. Windows Server 2008 и Windows Server 2012: устранение неполадок и поддержка [Электронный ресурс]. – Режим доступа: <http://technet.microsoft.com/ru-ru/windowsserver/bb512923.aspx>.

22. Выполняем миграцию файловых серверов из Windows Server 2003 в Windows Server 2012 R2 [Электронный ресурс]. – Режим доступа: <https://habrahabr.ru/company/microsoft/blog/243485/>.



Методичні вказівки щодо виконання лабораторних робіт з навчальної дисципліни «Проектування та адміністрування комп'ютерних мереж» для студентів денної форми навчання зі спеціальності 123 – «Комп'ютерна інженерія» освітнього ступеня «Бакалавр». Частина II

Укладач к. т. н., доц. Славко О. Г.

Відповідальний за випуск зав. кафедри КІС проф. А. В. Луговой

Підп. до др. \_\_\_\_\_. Формат 60×84 1/16. Папір тип. Друк ризографія.

Ум. друк. арк. \_\_\_\_\_. Наклад \_\_\_\_\_ прим. Зам. № \_\_\_\_\_. Безкоштовно.

Видавничий відділ  
Кременчуцького національного університету  
імені Михайла Остроградського  
вул. Першотравнева, 20, м. Кременчук, 39600