Міністерство освіти і науки України

Національний університет водного господарства та природокористування
Кафедра автоматизації, комп'ютерно-інтегрованих технологій та робототехніки

02/05-3М

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт
з навчальної дисципліни
«Інформаційні системи і технології в електроенергетиці»
для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Електроенергетика, електротехніка та електромеханіка» спеціальності 141 «Електроенергетика, електротехніка та електромеханіка» денної і заочної форм навчання

Рекомендовано науково-методичною радою з якості ННІЕАВГ
Протокол № 9 від 21.04.2026 р.

Рівне – 2026

Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни «Інформаційні системи і технології в електроенергетиці» для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Електроенергетика, електротехніка та електромеханіка» спеціальності 141 «Електроенергетика, електротехніка та електромеханіка» денної і заочної форм навчання [Електронне видання] / Наумчук О. М. – Рівне : НУВГП, 2026. – 114 с.

Укладач: Наумчук О. М., доцент кафедри автоматизації, електротехнічних та комп'ютерно-інтегрованих технологій

Відповідальний за випуск: Христюк А. О., к.т.н., доцент, в.о. завідувача кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки

Керівник освітньої програми «Електроенергетика, електротехніка та електромеханіка»: Літковець С. П., к.т.н., доцент кафедри енергетики/

Попередня версія методичних вказівок 04-03-361М

Зміст

Вступ

Сучасні електроенергетичні системи характеризуються високим рівнем автоматизації, інтеграції інформаційних технологій та використання цифрових засобів керування і моніторингу. Функціонування таких систем забезпечується за рахунок застосування інформаційно-комунікаційних технологій, які охоплюють передачу даних, обробку інформації, візуалізацію процесів та забезпечення кібербезпеки. Важливу роль у цьому відіграють мережеві технології, засоби дистанційного керування, а також серверна інфраструктура, що забезпечує обмін даними між різними рівнями енергосистеми.

У сучасних умовах розвитку Smart Grid та цифрових підстанцій значно зростають вимоги до надійності, безпеки та ефективності інформаційних систем. Передача технологічних даних здійснюється як по дротових, так і по бездротових каналах зв'язку з використанням стандартів Ethernet, TCP/IP та спеціалізованих промислових протоколів. При цьому особлива увага приділяється питанням сегментації мереж, забезпечення захисту інформації, а також обмеженню доступу до критичних елементів системи, таких як ПЛК, РЗА та RTU.

Методичні вказівки спрямовані на формування у студентів практичних навичок роботи з сучасними інформаційними технологіями, що застосовуються в електроенергетиці. У ході виконання лабораторних робіт студенти ознайомлюються з принципами побудови комп'ютерних мереж, налаштуванням мережевого обладнання, розгортанням серверних сервісів, використанням мережевих протоколів, а також базовими засобами діагностики та кіберзахисту.

Особливу увагу приділено практичним аспектам: налаштуванню мережевих сервісів, використанню інструментів аналізу мережі, розгортанню web-серверів та оцінці їх безпеки, а також аналізу можливостей застосування безпроводових технологій у енергетичних системах. При цьому, враховуються реальні обмеження, пов'язані з вимогами до надійності, завадостійкості та кібербезпеки. Виконання лабораторних робіт дозволяє студентам отримати системне уявлення про архітектуру інформаційних систем електроенергетики, взаємодію їх компонентів та принципи побудови захищених мереж.

Лабораторна робота 1
Розробка web-сторінки інформаційного призначення

Мета роботи

Ознайомитися з базовими технологіями створення web-інтерфейсів та набути початкових навичок розробки простої web-сторінки для представлення інформації про електроенергетичний об’єкт з елементами інтерактивної взаємодії.

Теоретичні відомості

Веб-сторінка (англ. Web-page) — інформаційний ресурс, доступний у мережі Internet, який можна переглянути у веб-браузері. Зазвичай ця інформація записана у форматі HTML або XHTML і може містити гіпертекст з гіперпосиланнями на інші веб-сторінки.

Веб-сайт (англ, website, місце, майданчик в Інтернеті), також сайт (англ. site, місце, майданчик) — сукупність веб-сторінок, доступних в Інтернеті, які об'єднані, як за змістом, так і навігаційно. Фізично сайт може розміщуватися, як на одному, так і на кількох серверах.

Веб-сервер — це підключений до Інтернету комп'ютер, який приймає запити на отримання певних даних, обробляє їх та видає результати, використовуючи протокол HTTP (Hyper Text Transfer Protocol —протокол передавання гіпертексту).

HTML (англ. HyperText Markup Language - мова розмітки гіпертекстових документів) — стандартна мова розмітки web-сторінок в Інтернеті. Більшість web-сторінок створюються за допомогою мови HTML (або XHTML). Документ HTML обробляється браузером та відтворюється на екрані у зрозумілому для користувача вигляді. HTML разом із каскадними таблицями стилів та вбудованими скриптами — це три основні технології побудови web-сторінок.

HTML надає розробнику засоби для:

- створення структурованого документу шляхом позначення структурного складу тексту: заголовки, абзаци, списки, таблиці, цитати, смислові блоки, меню та інше;
- отримання інформації з Інтернету через гіперпосилання;
- створення інтерактивних форм;

- включення зображень, звуку, відео, та інших об'єктів до тексту.

HTML-документ – це файл, який має розширенням *.htm (або *.html). Найпростіший HTML-документ матиме наступний вміст:

```
<!DOCTYPE html>        <!-- Тип документу -->
<html lang="uk">              <!-- Мова вмісту -->
 <head>   <!-- Початок заголовку документа -->
  <meta charset="utf-8"> <!--Кодування символів-->
     <title>Назва сторінки</title>
     <!--Тегом title задається назва сторінки-->
 </head>
 <body>   <!--Початок тіла документу-->
  <h1>Заголовок</h1>
  <p>
     Абзац тексту.
  </p>
 </body>
</html>
```

Для зручності читання введені додаткові відступи, однак у HTML-документі це не обов'язково, крім того більшість web-браузерів ігнорують символи кінця рядка і множинні пробіли. Тому такі відступи можна не використовувати.

Як видно з прикладу, вся інформація про форматування документа зосереджена у фрагментах розташованих між знаками "<" і ">". Такий фрагмент, наприклад, <html> називається міткою (англ. - tag).

Більшість HTML-міток є парними, тобто на кожну відкриваючу мітку виду *<tag>* є закриваюча мітка виду *</tag>* з тією ж назвою, але з додаванням символу "/". Мітки можна вводити, як великими так і малими літерами. Наприклад, мітки *<body>*, <BODY> і <Body> будуть сприйняті браузером однаково.

Багато міток, крім назви можуть мати *атрибути* - елементи, що дають додаткову інформацію про те, як web-браузер повинен обробити поточну мітку. Коментарі в HTML-документі виділяються наступним чином: <!-- коментар -->

При розробці web-сторінок зазвичай розділяється дизайн та вміст (контент) web-сторінки. Дизайн елементів описується за

допомогою CSS (Cascading Style Sheets – каскадні таблиці стилів), де задаються шрифти, розміри, кольори блоків тексту, посилань, властивості фону тощо. CSS дозволяє визначати зовнішній вигляд контенту на веб-сторінці, а також створювати стильні та привабливі веб-сторінки. CSS можуть бути включені безпосередньо в HTML-документ або підключатись до нього з файлу **.css* в заголовку (між тегами <head> та </head>) наступним чином:

```
<style type="text/css">
@import "example.css";
</style>
```

або

```
<link rel="stylesheet" href="example.css" type="text/css">
```

Винесення CSS у окремі файли дозволяє не включати в кожну сторінку опис спільних стилів, а лише посилання на css-файл. Якщо властивість елементу описана одразу декількома способами, то найбільший пріоритет має задання її безпосередньо у тезі елементу, меншим пріоритетом – стиль, що застосовується за ідентифікатором, заданим в тезі, ще меншим – стиль, що застосовується до класу, псевдоелементу, всіх тегів заданого типу, а найнижчий пріоритет – стиль, заданий у зовнішньому CSS-файлі.

Розробкою стандартів HTML та CSS займається Консорціум WWW (англ. World Wide Web Consortium, W3C, http://www.w3.org/).

Особливість використання CSS у HTML-документі полягає в тому, що CSS відокремлює оформлення (дизайн) від структури документа (HTML-код). Це дозволяє легко змінювати вигляд сайту без зміни самої розмітки. У приведеному нижче прикладі можна побачити способи використання внутрішнього та зовнішнього стилів.

```
<html>
<head>
 <meta charset="UTF-8">
 <title>Приклад CSS</title>
 <!-- Зовнішній стиль -->
 <link rel="stylesheet" href="styles.css">
 <!-- Внутрішній стиль -->
```

```
  <style>
    h1 { color: darkblue; }
  </style>
 </head>
 <body>
  <h1>Заголовок</h1>
  <p style="color: gray;">Це абзац із вбудованим стилем.</p>
 </body>
 </html>
```

Для динамізації web-сторінок у них вставляються різноманітні скрипти, які, як правило, реалізовуються мовою JavaScript. JavaScript - це мова програмування, яка використовується для створення інтерактивних та динамічних веб-сторінок та додатків. Вона дозволяє розробникам створювати складні функції та взаємодію з користувачем. Особливість використання JavaScript у HTML-документі полягає в тому, що він додає динаміку та інтерактивність до веб-сторінки, яка за своєю природою є статичною. Використаний скрипт виділяється тегами *<script></script>*, наприклад:

```
<script type="text/javascript">
  if (confirm("Текст вікна підтвердження!")) {
        alert("Натиснуто ОК");
      } else {
        alert("Натиснуто Cancel");
      }
</script>
```

JavaScript у HTML використовується для надання веб-сторінкам динамічності та інтерактивності. Він дозволяє реагувати на дії користувача (кліки, введення даних, наведення), змінювати вміст і стилі елементів у реальному часі, взаємодіяти з DOM, а також обмінюватися даними із сервером без перезавантаження сторінки. Підключати JavaScript можна як у вигляді зовнішнього файлу, так і безпосередньо в коді HTML за допомогою тегу *<script>*.

Приведений нижче приклад показує можливість інтеграції JavaScript в HTML-код.

```
<html>
<head>
```

```
  <meta charset="UTF-8">
  <title>Приклад JavaScript</title>
</head>
<body>
  <h1 id="demo">Привіт!</h1>
  <button onclick="changeText()">Змінити текст</button>
  <script>
    function changeText() {
      document.getElementById("demo").innerHTML = "Текст змінено JavaScript!";
    }
  </script>
</body>
</html>
```

Застосовуючи описані вище технології розробки web-сторінок можна розробляти та редагувати інформаційні матеріали. Вказані технології є основними, що застосовуються при розробці web-ресурсів, що дасть змогу набути основні поняття для подальшого застосовування у розробці складних інформаційних систем.

Програма роботи

1. Ознайомитися з особливостями застосування технологій розробки web-сторінок: HTML, CSS, JavaScript, що розглянуто у теоретичних відомостях

2. Відкрити існуючі web-сторінки та переглянути їх код. Знайти в коді основні HTML-теги, JavaScript та посилання на CSS. Розробити просту web-сторінку на енергетичну тематику.

Порядок виконання роботи

1. Аналіз прикладу web-ресурсу.

1.1. Відкрити у браузері будь-який web-сайт технічної або енергетичної тематики.

1.2. Відкрити початковий код сторінки (View Page Source / Inspect).

1.3. Знайти та зафіксувати у звіті: структуру документа: <!DOCTYPE html>, <html>, <head>, <body>; приклади заголовків, абзаців, списків, таблиць; підключення CSS (<link>); підключення або використання JavaScript (<script>); наявність

тегу <noscript> (за наявності).

2. Вибір тематики web-сторінки.

2.1. Обрати тему сторінки в межах електроенергетики, наприклад: електроустановка (підстанція, щит, двигун); система електропостачання; об'єкт автоматизації; енергетичне обладнання. Узгодити тему з викладачем.

2.2. Сформувати структуру майбутньої сторінки: назва сторінки; 2–3 інформаційні розділи (опис, характеристики, застосування тощо).

3. Розробка структури HTML-документу.

3.1. Створити HTML-файл (.html).

3.2. Реалізувати базову структуру документа:

<html lang="...">

<head> (кодування, назва сторінки)

<body>

3.3. Додати обов'язкові елементи:

– заголовок сторінки (<h1>);

– підзаголовки (<h2>);

– абзаци тексту (<p>);

– список або таблицю (наприклад, характеристики обладнання);

– гіперпосилання.

4. Оформлення сторінки за допомогою CSS.

4.1. Створити окремий файл стилів (.css).

4.2. Підключити CSS до HTML через <link>.

4.3. Реалізувати базове оформлення: шрифт і розмір тексту; кольори елементів; відступи та вирівнювання.

5. Додавання інтерактивності (JavaScript).

5.1. Додати на сторінку елемент взаємодії: кнопка або інший керуючий елемент.

5.2. Реалізувати просту функцію JavaScript, наприклад: зміна тексту; виведення повідомлення; реакція на дію користувача.

5.3. Підключити JavaScript: у вигляді окремого файлу або в HTML через <script>.

6. Перевірка роботи сторінки.

6.1. Відкрити сторінку у браузері.

6.2. Перевірити: коректність відображення структури; роботу стилів; виконання JavaScript.

6.3. Усунути помилки (за наявності).

7. Формування результатів для звіту.

7.1. Підготувати HTML-код сторінки.

7.2. Зробити скріншоти: відображення сторінки у браузері; прикладу роботи JavaScript.

7.3. Оформити короткий висновок: що було реалізовано, які технології використано

8. Виконати оформлення результатів лабораторної роботи.

***Вимоги до оформлення звіту*:**

Звіт повинен містити:

- титульну сторінку;
- тему, мету та програму роботи;
- короткий опис проаналізованого web-ресурсу та фрагмент HTML-коду з виділеними основними тегами;
- опис розробленої web-сторінки (тематика та структура);
- HTML-код розробленої сторінки;
- CSS-код або фрагмент стилів, що використовуються на сторінці;
- фрагмент коду JavaScript та опис його роботи;
- скріншот web-сторінки у браузері;
- скріншот роботи інтерактивного елементу;
- висновок.

Контрольні запитання

1. Що таке HTML-документ і яку роль він виконує у web-сторінці?
2. Яка структура HTML-документу та призначення основних тегів (<html>, <head>, <body>)?
3. У чому полягає призначення CSS і як він впливає на відображення web-сторінки?
4. Які способи підключення CSS до HTML-документу існують?
5. Яку роль виконує JavaScript у web-сторінці та які задачі він дозволяє реалізувати?
6. Які обов’язкові елементи повинна містити web-сторінка для представлення технічного об’єкта (наприклад, електроустановки)?

7. Як організувати структуру web-сторінки для відображення технічної інформації (опис, характеристики, функції)?

8. Який елемент взаємодії з користувачем доцільно реалізувати за допомогою JavaScript у даній роботі та чому?

9. Як перевірити коректність відображення web-сторінки та виявити помилки у коді?

10. Яким чином web-технології можуть застосовуватись у сучасних інформаційних системах електроенергетики (наприклад, SCADA, моніторинг)?

Лабораторна робота 2
Розробка політики інформаційної безпеки підприємства

Мета роботи

Ознайомитися з принципами побудови системи управління інформаційною безпекою відповідно до стандартів ISO/IEC 27001 та ISO/IEC 27002 і набути практичних навичок розробки політики інформаційної безпеки підприємства з урахуванням структури мережі, загроз та заходів захисту.

Теоретичні відомості

Стандарт ISO/IEC 27001 (Information Security Management Systems) - міжнародний стандарт управління інформаційною безпекою, який визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, відповідальність співробітників, використання оцінки ризиків і т.д. в контексті інформаційної безпеки. В процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої – скорочення матеріальних втрат, пов'язаних з порушенням інформаційної безпеки. Стандарт покликаний заощадити підприємству фінансові та матеріальні засоби.

ISO/IEC 27002 — це стандарт інформаційної безпеки. Він містить практичні правила організації інформаційної безпеки. Розроблений у ньому підхід ґрунтується на заходах, які направлені на організацію управління діяльністю підприємства. Він розроблений на основі досвіду різних організацій та дозволяє реалізувати та оцінити ефективність процедур управління безпекою, а також дає можливість встановити довірчі відносини між різними організаціями.

Даний документ можна використовувати як загальноприйнятий стандарт при встановленні ділових відносин між організаціями і при підписанні контрактів з субпідрядниками або впровадженні інформаційних систем та продуктів.

Метою інформаційної безпеки є — забезпечити безперебійну роботу організації і зведення до мінімуму збитків від подій, що загрожують безпеці. Управління інформаційною безпекою дає можливість колективно використовувати інформацію, забезпечуючи при цьому її захист та захист обчислювальних

ресурсів. Інформаційна безпека складається з трьох основних компонентів:

а) конфіденційність: захист конфіденційної інформації від несанкціонованого розкриття або перехоплення;

б) цілісність: забезпечення точності і повноти інформації і комп'ютерних програм;

в) доступність: забезпечення доступності інформації і життєво важливих сервісів для користувачів, коли це потрібно.

Інформація існує в різних формах. Її можна зберігати на носіях, передавати по мережах, роздруковувати або записувати на папері, а також озвучувати в розмовах. З погляду безпеки всі види інформації, включаючи: паперову документацію, бази даних, диски, флеш-носії, хмарне середовище, розмови та все інше, що використовується для передачі даних, знань та ідей, потребує належного захисту.

Інформація, яку використовують різні інформаційні системи і технології є цінним виробничим ресурсом організації. Її доступність, цілісність і конфіденційність може мати особливе значення для забезпечення: конкурентоспроможності, руху грошових коштів, рентабельності, відповідності правовим нормам і іміджу організації. Сучасні організації стикаються зі зростаючою загрозою порушення інформаційної безпеки, що походить від багатьох джерел. Інформаційним системам і мережам можуть загрожувати: комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, відмови у роботі та аварії. З'являються все нові загрози, здатні завдати значних збитків, наприклад сучасні комп'ютерні віруси або хакерські атаки.

Передбачається, що такі загрози інформаційній безпеці з часом стануть все більш поширенішими, небезпечнішими і витонченішими. Разом з тим, через зростаючу залежність організацій від інформаційних систем і сервісів, вони можуть стати вразливішими по відношенню до загроз порушення захисту. Розповсюдження комп'ютерних мереж надає нові можливості для несанкціонованого доступу до комп'ютерних систем, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості їх централізованого контролю.

Захисні заходи будуть значно дешевшими і ефективнішими, якщо вони будуть розроблятися ще на стадіях розробки та

проектування. Чим швидше організація почне застосовувати заходи по захисту своїх інформаційних систем, ресурсів, мереж та даних тим дешевими і ефективними буде їх використання.

У відповідності до стандартів ISO/IEC 27001 та ISO/IEC 27002 на підприємствах пропонується застосовувати заходи управління інформаційною безпекою, які доцільно описати у таких розділах:

1. Політика інформаційної безпеки.
2. Організація інформаційної безпеки.
3. Управління активами (інформаційними ресурсами).
4. Безпека персоналу.
5. Фізична та екологічна безпека.
6. Управління доступом.
7. Криптографічний захист інформації.
8. Експлуатаційна безпека (адміністрування систем і мереж).
9. Безпека комунікацій та мереж.
10. Розробка, супровід і захист інформаційних систем.
11. Управління інцидентами інформаційної безпеки.
12. Забезпечення безперервності діяльності.
13. Відповідність правовим та нормативним вимогам.

У цих розділах представлений набір заходів управління безпекою, які засновані на практичних аспектах по захисту інформації у відповідності до досвіду сучасних міжнародних організацій.

Застосування засобів управління безпекою. Предстаавлені заходи інформаційної безпеки потрібно застосовувати з урахуванням місцевих умов. Проте більшість заходів, представлені у даній послідовності широко застосовують багато організацій, а їх використання рекомендується для всіх ситуацій з врахуванням обмежень. Ці заходи є базовими щодо управління безпекою, оскільки всі вони в сукупності визначають базовий промисловий стандарт на підтримку режимів безпеки. При використанні деяких із заходів контролю, наприклад, шифрування даних, можуть використовуватися сучасні системи шифрування, але перед їх застосуванням необхідно оцінки ризики, щоб визначити, чи потрібні вони і яким чином їх реалізувати. Для забезпечення вищого рівня захисту особливо цінних ресурсів або забезпечення протидії високим рівням загроз порушення режиму безпеки, можуть бути використані інші

заходи контролю, які виходять за рамки передбачених правил.

Основні заходи захисту інформації підприємства:

- розробка документу про політику інформаційної безпеки;
- розподіл обов'язків по забезпеченню інформаційної безпеки;
- навчання і підготовка персоналу для підтримки режиму інформаційної безпеки;
- повідомлення про випадки порушення захисту;
- засоби захисту від вірусів;
- планування безперебійної роботи організації;
- контроль за копіюванням програмного забезпечення, захищеного законом про авторське право;
- захист документації організації;
- захист даних;
- відповідність політиці безпеки.

Сучасні підприємства вирішують цю проблему, розробляючи принципи інформаційної безпеки для відповідних відділів та груп співробітників, щоб забезпечити ефективніше функціонування технологій захисту інформації.

Політика інформаційної безпеки. Метою політики інформаційної безпеки є визначення особливостей і забезпечення у актуальному стані інформаційної безпеки організації і/або системи. Положення про політику безпеки повинне бути доведене до відома всіх співробітників організації та користувачів системи.

Положення про політику безпеки має містити:

1) визначення інформаційної безпеки, її цілі, область застосування, її значення та механізми колективного використання інформації;

2) основні положення щодо реалізації мети та принципів інформаційної безпеки;

3) роз'яснення конкретних заходів політики безпеки, принципів, стандартів і вимог до її дотримання, включаючи:

- виконання правових і договірних вимог;
- навчання персоналу правилам безпеки;
- попередження і виявлення вірусів;
- забезпечення безперебійної роботи організації.

4) визначення загальних і конкретних обов'язків по забезпеченню режиму інформаційної безпеки;

5) роз'яснення процесу повідомлення про події, що несуть загрозу безпеці.

Особливості створення та використання паролів. Користувачі повинні вибирати нестандартні паролі. Це означає, що паролі не повинні бути пов'язані із заняттями або особистим життям користувачів.

Наприклад, не можна використовувати як пароль номер власного автомобіля, власне ім'я та ім'я дружини або дитини, дату та рік народження, частину адреси та ін. Це не означає, що пароль не повинен бути просто словом із словника. Також, не варто використовувати відомі імена, географічні назви, технічні терміни і сленг. Якщо є відповідні системні програмні засоби для здійснення контролю надійності що призначаються користувачам паролів, то необхідно використовувати ці засоби для того, щоб заборонити користувачам вибір легко вгадуваних паролів.

Паролі не повинні зберігатися в доступній для читання формі в командних файлах, сценаріях автоматичної реєстрації, програмних макросах, на комп'ютерах з неконтрольованим доступом, а також в інших місцях, де не уповноважені особи можуть отримати доступ до них. Користувачі не повинні вибирати таку опцію конфігурації, як автоматичне збереження пароля.

Не можна записувати паролі і залишати ці записи в місцях, де до них можуть отримати доступ не уповноважені особи. Пароль повинен бути негайно змінений, якщо є підстави вважати, що цей пароль став відомий будь кому крім користувача.

Для прикладу розробки політики інформаційної безпеки підприємства потрібно визначити структуру комп'ютерної мережі (мереж) підприємства. Такий підхід дасть змогу точно визначити її технічні та програмні можливості, а також оцінити конкретні вразливості даної структури. Розглянемо структуру комп'ютерної мережі підприємства, яка представлена на структурній схемі (рис. 1).

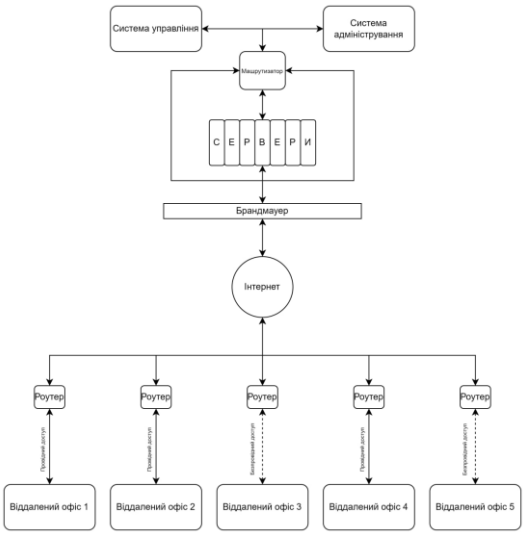


Рис. 1. Структурна схема комп'ютерної мережі підприємства

Представлена структура комп'ютерної мережі є змішаною локально-глобальною мережою з обмежувальним механізмом (апаратно-технічний) у вигляді брандмауера. Віддалені офіси, які можуть бути розташовані у різних частинах країни, мають можливість користуватись головними серверами за наявності спеціального токену доступу. Засоби адміністрування та система управління розташовані безпосередньо на головному сервері(ах) та мають можливість користуватися ними без токенів.

Серед вразливостей комп'ютерної мережі, які можуть виникнути в приведеній структурній схемі можуть бути такі:

- наявність помилок в програмному забезпеченні (ПЗ) та операційних системах (ОС);
- помилки адміністрування, конфігурації систем та методів захисту;
- невиконання рекомендацій спеціалістів по захисту мереж;
- економія на методах та системах безпеки чи ігнорування ними;
- недобросовістні працівники;
- несанкціонований доступ через недосконаліть локальних, безпроводових чи продових технологій зв'язку;

- обхід чи зламування головного захисту потоків даних до серверів у вигляді брандмауера;

- використання фейк-запитів до серверів з ціллю колекціонування обривків даних;

- DDoS-атаки з ціллю пошкодити комп'ютерну мережу;

- фізичні пошкодження (стихійні лиха, погодні катаклізми, неуважність працівників та ін.).

На відміну від структури комп'ютерної мережі інформаційна структура може суттєво відрізнятися і вона описує інформаційну взаємодію та обмін даними між окремими працівниками підприємства, або його відділами. Приклад інформаційної структури приведений на рис. 2.

Серед загроз інформаційної безпеки можуть виникати такі:

- використанні недосконалого ПЗ та неперевіреного обладнання;

- неповноцінні процеси роботи системи;

- складні експлуатаційних умови.

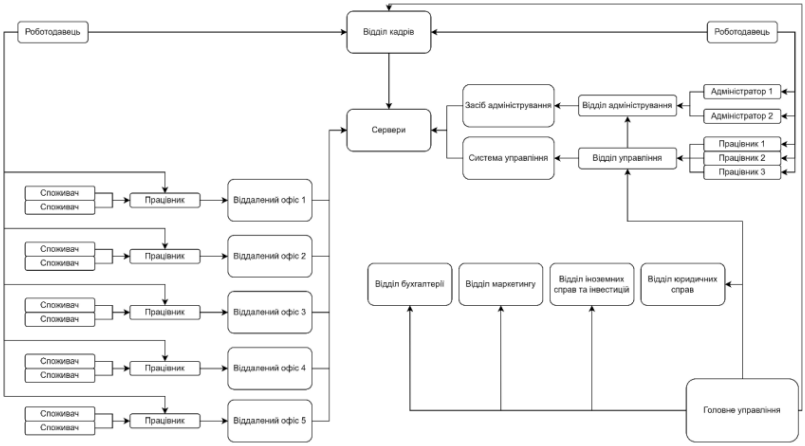


Рис. 2. Структурна схема інформаційної структури підприємства

Загрози інформаційної безпеки можуть мати організований та неорганізований (випадковий) характер. До ненавмисних загроз інформаційної безпеки відносяться:

- неполадки в роботі апаратури передачі даних;

- помилки та збої ПЗ;
- помилки в діях персонал або працівників, які працюють в системі;
- форс-мажори, викликані діями природних катаклізмів чи іншими непередбачуваними обставинами;
- проблеми через перебої електроенергії.

До навмисних загроз інформаційної безпеки відносяться:
- відсутність кібергігієни у працівників системи;
- використання публічних безпроводових точок доступу;
- надання токенів доступу для сторонніх користувачів;
- використання незареєстрованих у системі зовнішніх пристроїв;
- DdoS-атаки з ціллю пошкодити роботу системи;
- хакерські атаки з ціллю збору даних;
- порушення роботи брандмауера;
- підбір токенів доступу до системи;
- злиття даних працівником системи;
- імітація запитів до системи;
- обхід системи безпеки;
- ввід вірусів у систему.

Приведена технічна та інформаційна структура дозволить оцінити всі можливі вразливості та загрози і у майбутньому забезпечити мінімізацію наслідків від них.

Розглянемо приклад узагальненої політики інформаційної безпеки енергетичного підприємства на основі ISO/IEC 27001 та ISO/IEC 27002.

1. Мета і завдання. Метою цієї політики є забезпечення захисту інформаційних ресурсів, що підтримують діяльність підприємства, включаючи управління електромережами, обслуговування споживачів та фінансово-економічну діяльність. Основні завдання:
- гарантування конфіденційності, цілісності та доступності даних;
- захист критичної інфраструктури підприємства;
- мінімізація ризиків кібератак та несанкціонованого доступу.

2. Сфера дії. Політика поширюється на всі підрозділи підприємства, його співробітників, підрядників і партнерів, які мають доступ до інформаційних систем підприємства.

3. Основні принципи:

Конфіденційність – інформація споживачів, комерційні та технічні дані не підлягають розголошенню без законних підстав.

Цілісність – усі дані повинні бути захищені від несанкціонованих змін.

Доступність – критичні системи (АСДУ, SCADA, білінгові сервіси) мають бути доступні у відповідності до вимог безперервності бізнесу.

Відповідальність – кожен співробітник несе персональну відповідальність за дотримання правил безпеки.

4. Організація інформаційної безпеки:

Призначається відповідальний (офіцер) з інформаційної безпеки.

Впроваджується комітет з інформаційної безпеки для аналізу ризиків та інцидентів.

Проводиться навчання персоналу з питань кібергігієни.

5. Управління активами:

Всі сервери, мережеве обладнання та АСДУ підлягають інвентаризації.

Критичні активи класифікуються за рівнем важливості та захисту.

6. Контроль доступу:

Доступ надається за принципом мінімальних прав.

Використовується багатофакторна аутентифікація (MFA) для ключових систем.

Всі дії користувачів у SCADA та корпоративній мережі логуються.

7. Фізична безпека:

Дата-центри та диспетчерські пункти захищені системами відеонагляду та контролю доступу.

Обмежений доступ до серверних приміщень лише авторизованому персоналу.

8. Криптографічний захист:

Конфіденційні дані шифруються (AES-256, TLS 1.3).

Використовуються сертифікати електронного підпису для службових транзакцій.

9. Експлуатація та технічне обслуговування6

Регулярні оновлення ОС, SCADA-програмного забезпечення,

антивірусного ПЗ.

Ведення журналів безпеки з аналізом інцидентів.

10. Планування безперервності бізнесу:

Резервне копіювання критичних даних (мінімум щоденно).

План відновлення після аварії (Disaster Recovery Plan).

Випробування планів реагування на кібератаки.

11. Дотримання вимог:

Виконання національного законодавства України у сфері енергетики та захисту інформації.

Відповідність стандартам ISO/IEC 27001 та рекомендаціям НКРЕКП.

12. Моніторинг і вдосконалення:

Постійний аудит інформаційної безпеки.

Щорічний перегляд політики та оновлення відповідно до нових ризиків.

Програма роботи

1. Розглянути основні положення стандарту ISO/IEC 27001 та ISO/IEC 27002.
2. Навчитися розробляти політику безпеки організації.

Порядок виконання роботи

1. Виконати аналіз стандартів інформаційної безпеки.

1.1. Ознайомитися зі структурою стандартів ISO/IEC 27001 та ISO/IEC 27002.

1.2. Визначити основні групи заходів інформаційної безпеки.

2. Вибір та опис підприємства.

2.1. Обрати варіант підприємства та узгодити його з викладачем (наприклад енергопостачальне підприємство по типу районної, або обласної енергопостачальної компанії).

2.2. Описати структуру підприємства: основні підрозділи; інформаційні системи; використання комп'ютерної мережі.

3. Розробка структури комп'ютерної мережі.

3.1. Побудувати схему мережі підприємства (сервери, робочі станції, мережеве обладнання, доступ до Інтернету).

3.2. Виконати схему у вигляді структурної схеми.

3.3. Надати короткий опис роботи мережі.

4. Розробка інформаційної структури.

4.1. Побудувати схему інформаційних потоків між підрозділами.

4.2. Визначити: які дані передаються; хто має доступ до інформації.

5. Виконання ідентифікація загроз.

5.1. Визначити основні загрози інформаційній безпеці: технічні; організаційні; людський фактор.

5.2. Оформити результати у вигляді таблиці загроз.

6. Розробка заходів захисту.

6.1. Для кожної загрози визначити заходи захисту:

організаційні; технічні.

6.2. Оформити результати у вигляді таблиці заходів.

7. Розробка політики інформаційної безпеки

7.1. Сформувати документ політики ІБ відповідно до поданої у теоретичних відомостях структури (10–12 пунктів).

7.2. У кожному пункті: визначити вимоги; описати конкретні заходи безпеки.

8. Перевірка та узгодження результатів.

8.1. Перевірити відповідність політики: визначеним загрозам; структурі підприємства.

8.2. Переконатися у повноті усіх розділів та логічної узгодженості документа.

9. Виконати оформлення результатів лабораторної роботи.

9.1. Підготувати: схеми; таблиці; текст політики безпеки.

9.2. Оформити звіт.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- тему, мету та програму роботи;
- опис обраного підприємства та його структури;
- схему комп'ютерної мережі підприємства та її короткий опис;
- схему інформаційної структури (інформаційних потоків);
- таблицю загроз інформаційної безпеки;
- таблицю заходів захисту інформації;
- розроблену політику інформаційної безпеки (10–12 розділів);

- висновок.

Контрольні запитання

1. Яке призначення стандартів ISO/IEC 27001 та ISO/IEC 27002?
2. Що таке система управління інформаційною безпекою (ISMS)?
3. У чому полягають принципи конфіденційності, цілісності та доступності інформації?
4. Які основні групи заходів інформаційної безпеки визначає ISO/IEC 27002?
5. Яку роль відіграє політика інформаційної безпеки на підприємстві?
6. Які елементи повинна містити схема комп'ютерної мережі підприємства?
7. Як визначити основні загрози інформаційній безпеці для конкретного підприємства?
8. Яким чином пов'язані загрози та заходи захисту інформації?
9. Які розділи обов'язково повинна містити політика інформаційної безпеки?
10. Як забезпечити відповідність політики безпеки реальній структурі підприємства?

Лабораторна робота 3
Дослідження та побудова мереж передачі даних в електроенергетичних системах на базі Ethernet

Мета роботи

Ознайомитись з будовою і призначенням основних елементів для побудови локальних комп'ютерних мереж типу Ethernet. Навчитися створювати Ethernet мережу, налаштовувати TCP/IP параметри та тестувати з'єднання використовуючи стандартні утиліти ОС Windows

Теоретичні відомості

Передача даних у сучасних електроенергетичних системах базується на використанні стандартних мережевих технологій, зокрема Ethernet та стеку протоколів TCP/IP. Ці технології забезпечують обмін інформацією між пристроями автоматизації, системами диспетчеризації та серверним обладнанням, що дозволяє реалізувати функції моніторингу, керування та діагностики енергетичних об'єктів.

Технологія Ethernet є основою більшості локальних мереж і визначає принципи передачі даних на фізичному та канальному рівнях моделі OSI. У сучасних мережах використовується комутація пакетів і повнодуплексний режим передачі, що дозволяє уникнути колізій, характерних для ранніх реалізацій Ethernet (CSMA/CD). Передача даних здійснюється у вигляді кадрів, які містять MAC-адреси відправника та отримувача, що забезпечує адресацію пристроїв у межах локальної мережі. Як середовище передачі застосовуються кабелі типу скручена пара (UTP, STP) та волоконно-оптичні лінії, які забезпечують необхідну пропускну здатність і завадостійкість.

Для забезпечення міжмережевої взаємодії використовується стек протоколів TCP/IP. Основним елементом є IP-адресація, яка дозволяє ідентифікувати пристрої у мережі. Протокол IP відповідає за маршрутизацію пакетів, тоді як протокол TCP забезпечує надійну передачу даних із контролем доставки, а UDP — швидкий обмін без встановлення з'єднання. У мережах електроенергетики TCP/IP використовується як транспортна основа для передачі технологічної інформації між різними

рівнями систем автоматизації.

У сучасних електроенергетичних системах широко застосовуються автоматизовані системи керування технологічними процесами (АСУ ТП) та SCADA-системи. Типова структура такої системи включає програмовані логічні контролери (ПЛК), які здійснюють збір і первинну обробку даних з пристроїв, наприклад лічильників енергії, що встановлені на підстанціях, та SCADA-сервери, які виконують функції диспетчеризації, візуалізації та збереження даних. Обмін інформацією між ПЛК та SCADA здійснюється через мережу Ethernet з використанням стандартних протоколів на базі TCP/IP. При цьому мережа забезпечує передачу даних у режимі, наближеному до реального часу, що є критично важливим для керування енергетичними об'єктами.

Мережі передачі даних в електроенергетиці мають ряд особливостей у порівнянні зі звичайними офісними мережами. До них належать підвищені вимоги до надійності, безперервності роботи та захищеності від завад і відмов. Часто застосовуються резервування каналів зв'язку, сегментація мережі та використання промислового мережевого обладнання. Крім того, важливим є контроль затримок передачі даних і втрат пакетів, оскільки це безпосередньо впливає на якість роботи систем керування.

Для аналізу та діагностики мережі використовуються стандартні утиліти операційних систем, такі як *ipconfig*, *ping* та *tracert*. Вони дозволяють визначити параметри мережевого підключення, перевірити доступність вузлів та оцінити характеристики передачі даних. Зокрема, утиліта ping дає змогу оцінити час затримки (latency) та наявність втрат пакетів, що є важливими показниками ефективності роботи мережі. У контексті електроенергетичних систем ці параметри використовуються для оцінки якості зв'язку між елементами системи автоматизації.

Таким чином, технології Ethernet і TCP/IP є базою для побудови мереж передачі даних в електроенергетиці, забезпечуючи інтеграцію пристроїв автоматизації, систем моніторингу та керування. Розуміння принципів їх роботи є необхідною умовою для подальшого вивчення спеціалізованих

промислових протоколів і систем керування, що застосовуються в енергетичній галузі.

Розглянемо типові компоненти обладнання Ethernet-мереж. *Карта мережевого інтерфейсу* (Network Interface Card - NIC), яку також називають мережевим адаптером або мережевою картою - це пристрій, який здійснює фізичне під'єднання до мережі, тобто забезпечує фізичне сполучення з мережевим кабелем. У більшості випадків ця карта встановлюється безпосередньо в шину розширення комп'ютера (PCI, ISA, PCI Express та ін.). В окремих випадках карта може бути частиною окремого пристрою, до якого комп'ютер під'єднаний через паралельне або послідовне сполучення.

Повторювач (repeater) - це пристрій, який отримує електричний або оптичний сигнал з кабелю через відповідний інтерфейс, регенерує його і передає в кабель через інший інтерфейс. Завданням повторювача є пересилання будь-якого вхідного сигналу до всіх інших портів без модифікації і затримки. Також повторювач пересилає сигнали колізій, глушіння, шумів та ін. Повторювачі можуть мати два або більше порти. Прикладом багатопортового повторювача у мережі Ethernet є хаб.

Хаби Ethernet. Виготівники мережевого обладнання впровадили пристрої, які забезпечують можливість передавати дані через багато портів мережі Ethernet. Хаби можна об'єднувати або каскадувати (з використанням ієрархічної схеми), що збільшує кількість портів на окремому сегменті мережі.

Сучасні хаби - це значно складніші пристрої, які мають ряд властивостей, подібних до комутаторів або мостів, що значно покращує їх можливості при адмініструванні мережі. Зокрема, наявність внутрішніх комутаторів у хабі дозволяє розділити його порти на декілька груп. Передавання пакетів даних між цими групами портів може супроводжуватися буферизацією, фільтрацією, контролем правильності пакетів та відкиданням пошкоджених пакетів тощо.

Середовище передачі даних. Коаксіальний кабель донедавна був дуже популярний, що пов'язано з його високою перешкодозахищеністю (завдяки металевому обплетенню), а також більшими допустимими відстанями передачі (до

кілометра). До цього кабелю складніше під'єднатися з метою несанкціонованого прослуховування мережі, а також він менше продукує зовнішніх електромагнітних випромінювань.

Скручена пара. Існує декілька категорій цього типу кабелю, які позначаються CAT1...CAT7 та визначають ефективний пропускний частотний діапазон. Кабель вищої категорії зазвичай містить більше пар проводів і кожна пара має більше витків на одиницю довжини. Категорії неекранованої скрученої пари визначаються стандартами ANSI/EIA/TIA 568 та міжнародним стандартом ISO 11801.

Зараз найбільшого поширення здобули декілька типів структурованих кабельних систем, які відрізняються характеристиками та особливостями монтажу:

1. Кабельна система на основі неекранованого кабелю типу скручена пара UTP з опором 100 Ом (рис. 1):

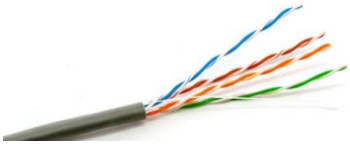


Рис. 1. Неекранований кабель скручена пара UTP- типу

Переваги кабелів UTP: багатоваріантність застосування, висока пропускна здатність при невеликій вартості; можуть передавати дані зі швидкістю до 100 Мб/с і підтримують сучасні технології передачі (Fast Ethernet, ATM та ін.); простота монтажу, невеликий діаметр та вага.

Недоліки кабелів UTP: невелика захищеність від механічних пошкоджень; чутливість до завад викликаних зовнішніми джерелами електромагнітних полів.

2. Кабельна система на основі екранованого кабелю типу скручена пара STP з опором 150 Ом (рис. 2).

Рис. 2. Екранований кабель скручена пара STP- типу

Переваги кабелів STP: забезпечують захист сигналів від впливу зовнішнього середовища та сигналів в інших кабелях; зменшують захист від впливу комунікаційних систем зосереджених в одному передавальному середовищі.

Недоліки кабелів STP: більша вартість у порівнянні з іншими типами кабелів типу скручена пара; необхідно забезпечення заземлення.

3. Кабельні системи на основі волоконно-оптичних кабелів (рис. 3).

Рис. 3. Волоконно-оптичний кабель

Переваги оптоволоконних кабелів: велика ширина смуги передавання; відносно невелика вартість; низьке енергоспоживання; нечутливість до електромагнітних завад.

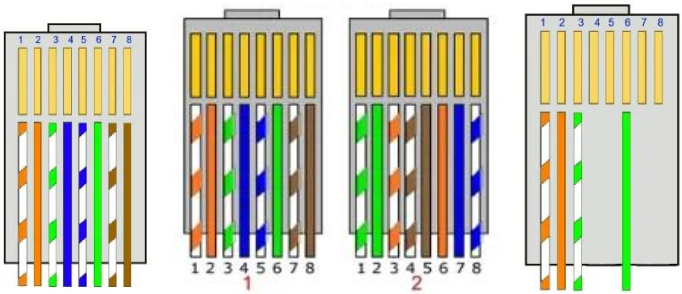
Недоліки оптоволоконних кабелів: складність монтажу та необхідність використання спеціальних пристроїв; вища вартість кабелю та монтажу у порівнянні з іншими типами.

З розглянутих вище кабельних систем найбільшого поширення здобули кабельні системи на основі скрученої пари у яких використовуються роз'єми типу RJ-9, RJ-11, RJ-12, RJ-14, RJ-21, RJ-45, RJ-45S, RJ-50. Серед них найбільше поширеними типами роз'ємів є: RJ-11, RJ-12 та RJ-45. Корпус RJ - конектора, як правило, складається з прозорого пластика, усередині якого кілька ножів-контактів. У комп'ютерних мережах (4-жильна скручена пара) за технологіями 10BASE-T, 100BASE-T та 1000BASE-TX зазвичай використовується стандартний конектор RJ-45, що має з'єднання 8P8C. Восьмиконтактні модульні з'єднувачі RJ-45 (рис. 4) мають вісім контактів та поділяються на: екрановані і неекрановані, зі вставкою і без, для круглого і плоского, для одножильного і багатожильного кабелю. У новій невикористаній вилці контакти виходять за межі корпуса. У процесі обтискання вони будуть втоплені всередину корпуса, проріжуть ізоляцію проводу і встромляться в жили провідників.

Рис. 4. Зовнішній вигляд восьмиконтактного конектора RJ-45

Для виконання монтажу кабелів типу скручена пара використовується спеціальний обтискний інструмент (рис. 5). Спочатку знімають верхню ізоляцію з кабелю, потім розплітають та вирівнюють провідники за певною схемою (пряма або перехресна). Пряма схема (рис. 6, а) використовується для підключення пристроїв різних типів, наприклад: ПК - Switch, Switch – Router, або Router - ПК. Перехресна схема (рис. 6, б) використовується для підключення однотипних пристроїв, наприклад: ПК - ПК, Switch - Switch, Router - Router і т. д. Деколи при побудові локальної мережі для швидкості передачі даних до 100 Мб/с та для економії використовують 4-х провідний кабель. Монтаж такого кабелю здійснюється подібно, як і 8-и жильного за виключенням того, що у конекторі задіяні тільки 1, 2, 3 і 6 жили, як показано на рис. 6, в. Далі провідники за відповідно обраною схемою вставляють у конектор так, щоб всі жили розташувалися у своїх напрямних каналах, а зовнішня ізоляція кабелю потрапила під планку затискання конектора. Після цього проводиться обтискання кабелю.

Рис. 5. Обтисний інструмент для кабелю скручена пара



а) б) в)

Рис. 6. Способи розташування провідників у восьмиконтактному з'єднувачі RJ-45: а) пряма схема, б) перехресна схема, в) пряма схема для 4-х жильного кабелю

Діагностика мережі в операційних системах Windows. До складу операційної системи Windows включено ряд комунікаційних утиліт, які дають можливість перевірити працездатність з'єднання з віддаленим вузлом (*ping*), прослідкувати маршрут проходження пакетів до віддаленого вузла (*tracert*) та ін. Для їх запуску достатньо перейти в режим командного рядка *(Пуск → Програми → Система Windows → Командний рядок)* і ввести з клавіатури у відповідь на запрошення назву утиліти з відповідними параметрами. Для зупинки виконання якоїсь команди/утиліти в командному рядку необхідно натиснути комбінацію клавіш Ctrl+C.

Розглянемо особливість використання системних утиліти мережної діагностики**.** Утиліта *ipconfig* призначена для перевірки правильності конфігурації TCP/IP для операційної системи Windows. Вона виводить значення для поточної конфігурації стека TCP/IP: MAC- і IP- адресу, маску підмережі, адресу шлюзу за замовчуванням, адреси серверів WINS (Windows Internet Naming Service) і DNS, використання DHCP. При усуненні несправностей в мережі TCP/IP слід спочатку перевірити правильність конфігурації за допомогою утиліти *ipconfig*.

Синтаксис утиліти: *ipconfig [/ all] [/ renew [adapter]] [/ release] [adapter]* (тут і далі в квадратних дужках вказані необов'язкові параметри):

• *all* видає весь список параметрів, без цього ключа

відображається тільки IP-адреса, маска і шлюз за умовчанням;

• *renew* [*adapter*] оновлює параметри конфігурації DHCP для зазначеного мережного адаптера з ім'ям adapter;

• *release* [*adapter*] звільняє виділену DHCP IP -адресу.

Таким чином, утиліта *ipconfig* (рис. 7) дозволяє з'ясувати, чи ініціалізована конфігурація і чи не дублюються IP- адреси:

• якщо конфігурація ініціалізована, то з'являються IP-адреса, маска, шлюз;

• якщо IP- адреси дублюються, то маска мережі буде 0.0.0.0;

• якщо при використанні DHCP комп'ютер не зміг отримати IP- адресу, то значення буде 0.0.0.0.

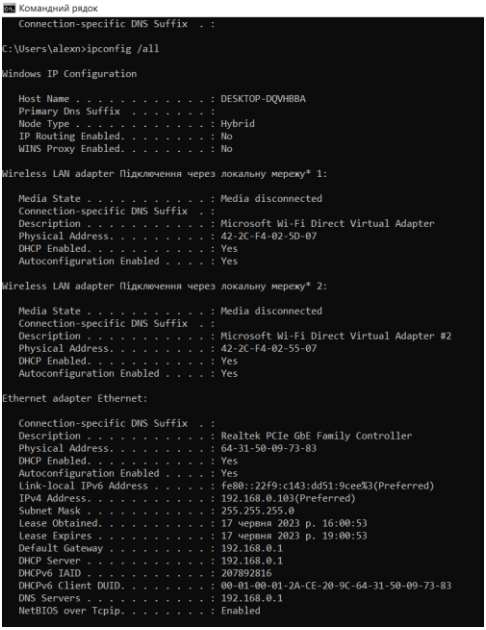


Рис. 7. Відображення встановлених мережних конфігурацій утилітою *ipconfig*

Утиліта *ping* (Packet Internet Grouper) використовується для перевірки конфігурування TCP/IP та діагностики помилок з'єднання. Вона визначає доступність і функціонування конкретного хоста (вузла) будь якого мережного пристрою, що

обмінюється інформацією з іншими мережними пристроями. Команда *ping* перевіряє з'єднання з віддаленим хостом шляхом відправлення до нього *ехо-пакетів* протоколу ICMP (Internet Control Message Protocol) і прослуховування *ехо-відповідей*. Ping виводить кількість переданих і прийнятих пакетів. Кожен прийнятий пакет перевіряється відповідно з переданим повідомленням. Якщо зв'язок між хостами поганий, то з цих повідомлень визначають скільки пакетів втрачено.

За замовчуванням передаються чотири ехо-пакета довжиною 32 байта, що представляють собою послідовність спеціальних символів. Атрибути утиліти *ping* дозволяють змінити розмір і кількість пакетів, вказати чи слід записувати маршрут, яку тривалість часу встановлювати, чи можна фрагментувати пакети і т.д. При отриманні відповіді визначається, за який час (у мілісекундах) відправлений пакет доходить до віддаленого хоста і повертається назад. Оскільки, значення за замовчуванням для очікування відгуку складає 1 с, то всі значення даного поля будуть менше 1000 мс.

При використанні утиліти *ping* необхідно врахувати те, що затримка, визначена утилітою, викликана не тільки пропускною здатністю каналу передачі даних, а й завантаженістю ПК. Деякі сервери в цілях безпеки можуть не відправляти ехо-відповіді, так як з утиліти *ping* може починатися хакерська атака.

Утиліта *ping* можна використовувати для тестування як з доменним іменем хоста, так і з IP -адресою. Якщо *ping* з IP-адресою виконалася успішно, а з доменним іменем - невдало, це означає, що проблема полягає в розпізнаванні відповідності адреси та імені, а не в мережному з'єднанні.

Синтаксис команди: *ping [-t], [-a], [-n count], [-llength], [-f], [-i ttl], [-v tos], [-r count], [-s count], [-j host-list], [-k host-list], [-w timeout], [destination-list]*

Параметри команди:

-t виконує команду ping до переривання (Ctrl-Break - переглянути статистику і продовжити, Ctrl-C - перервати виконання команди);

-a дозволяє визначити доменне ім'я віддаленого комп'ютера за його IP-адресою;

-n count посилає кількість пакетів Echo, вказане параметром

count (за замовчуванням передається чотири запиту);

-l length посилає пакети довжиною *length* байт (максимальна довжина 8192 байти);

-f посилає пакет з встановленим прапорцем «Не фрагментувати», що забороняє фрагментованість пакета на транзитних маршрутизаторах;

-i ttl встановлює час існування пакета на величину *ttl* (кожен маршрутизатор зменшує *ttl* на одиницю, тобто час існування є лічильником пройдених маршрутизаторів (хопів));

-v tos встановлює значення поля «сервіс», що задає пріоритет обробки пакета;

-r count записує шлях вихідного пакету і пакету, що повертається в полі запису шляху, *count* - від 1 до 9 хостів;

-s count задає максимально можливу кількість переходів з однієї підмережі в іншу (хопів);

-j host-list направляє пакети за допомогою списку хостів, визначеного параметром *host -list*). Максимальна кількість хостів дорівнює 9;

-k host-list направляє пакети через список хостів, визначений у *host-list*, причому зазначені хости не можуть бути розділені проміжними маршрутизаторами (жорстка статична маршрутизація);

-w timeout вказує час очікування timeout відповіді від віддаленого хоста в мілісекундах (за замовчуванням - 1с);

-destination-list вказує віддалений вузол, до якого треба направити пакети ping , може бути ім'ям хоста або IP -адресою ПК.

Найчастіше у форматі команди *ping* використовуються опції *-t* та *-n*. Приклад виконання утиліти *ping* наведено на рис. 8.

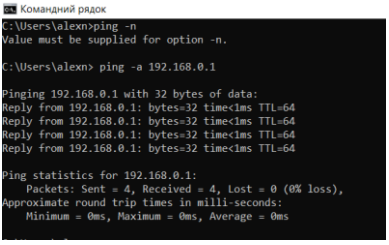


Рис. 8. Приклад використання утиліти *ping -a*

Підсумовуючи, слід зазначити, що мережеві технології Ethernet та TCP/IP є основою побудови сучасних систем передачі даних в електроенергетиці, забезпечуючи взаємодію між пристроями автоматизації, системами диспетчеризації та обчислювальними ресурсами. Вони дозволяють організувати надійний обмін технологічною інформацією між окремими елементами. Розуміння принципів функціонування мереж, особливостей їх побудови та методів діагностики є необхідною передумовою для ефективного налаштування, аналізу та експлуатації мережевої інфраструктури енергетичних об'єктів.

Програма роботи.

1. Ознайомитись з будовою і призначенням основних елементів для побудови локальних мереж типу Ethernet.

2. Навчитися створювати Ethernet мережу, налаштовувати TCP/IP параметри та тестувати з'єднання використовуючи утиліти ОС Windows.

Порядок виконання роботи.

1. Аналіз мережевих технологій.

1.1. Ознайомитися з принципами роботи Ethernet та TCP/IP.

1.2. Визначити роль цих технологій у системах електроенергетики.

2. Дослідження фізичного рівня мережі.

2.1. Розглянути типи кабелів (UTP, STP, оптоволокно) та їх застосування в енергетиці.

2.2. Ознайомитися зі схемами обтискання RJ-45 (пряма, перехресна).

2.3. Виконати обтискання кабелю скручена пара (один варіант — прямий або перехресний).

2.4. Перевірити правильність обтискання (візуально або тестером).

3. Формування моделі мережі енергетичного об'єкта.

3.1. Сформувати спрощену модель мережі:

- ПК (робоча станція оператора);
- комутатор;
- умовний ПЛК (як мережевий вузол, можна використати інший пристрій, наприклад інший ПК, або ноутбук).

3.2. Визначити взаємозв'язки між елементами передачі даних.

4. Налаштування TCP/IP параметрів.

4.1. Визначити IP-адреси для вузлів мережі.

4.2. Виконати налаштування TCP/IP у ОС Windows:

- IP-адреса;
- маска підмережі;
- шлюз (за потреби).

4.3. Перевірити правильність конфігурації за допомогою утилвти *ipconfig*.

5. Тестування мережевого з'єднання.

5.1. Перевірити з'єднання між вузлами за допомогою утиліти *ping*.

5.2. Визначити:

- доступність вузлів;
- час затримки;
- наявність втрат пакетів.

5.3. Використати утиліту *tracert* для аналізу маршруту.

6. Аналіз роботи мережі.

6.1. Проаналізувати результати тестування на: стабільність з'єднання та затримку передачі.

6.2. Оцінити придатність мережі для використання в електроенергетиці, визначити: чи забезпечується надійність та чи можливі затримки.

7. Узагальнення результатів.

7.1. Зробити висновок про:

- роботу Ethernet мережі;
- роль TCP/IP у передачі технологічних даних;
- застосування мереж у системах енергетики.

8. Оформлення звіту лабораторної роботи.

8.1. Оформити: результати налаштувань; результати тестування; короткий аналіз роботи мережі.

***Вимоги до оформлення звіту*:**

Звіт повинен містити:

- титульну сторінку;
- мету та програму роботи;
- короткий опис виконаних етапів роботи;
- фотографії або ілюстрації виконання фізичного підключення

мережі (кабель, підключення вузлів);

- скріншоти налаштування TCP/IP параметрів;
- скріншоти результатів виконання команд ipconfig, ping, tracert;
- короткий аналіз результатів тестування мережі (затримки, доступність, стабільність);
- висновок.

Контрольні запитання

1. Що таке технологія Ethernet та де вона застосовується в електроенергетиці?
2. Які функції виконує стек протоколів TCP/IP?
3. Що таке IP-адреса і для чого вона використовується?
4. Яка роль MAC-адреси в мережі Ethernet?
5. Які типи кабелів застосовуються в мережах передачі даних і в чому їх відмінності?
6. Яке призначення комутатора в мережі?
7. Як організовується передача даних між ПЛК та SCADA-системою?
8. Які параметри можна визначити за допомогою утиліти ping?
9. Для чого використовується команда ipconfig?
10. Які особливості мереж передачі даних в електроенергетичних системах?

Лабораторна робота 4
Розробка та налаштування безпроводових мереж у системах електроенергетики

Мета: Ознайомитися з принципами побудови та налаштування безпроводових мереж у електроенергетичних системах та набути практичних навичок конфігурації Wi-Fi мереж з урахуванням вимог безпеки та надійності.

Теоретичні відомості

Технологія Wi-Fi (IEEE 802.11) - це сімейство технологій безпроводового передавання у радіодіапазоні. Сімейство стандартів IEEE 802.11 визначає фізичний та канальний рівень протоколів передавання, вони відрізняються фізичною реалізацією та швидкістю. На основі IEEE 802.11 будують безпроводові локальні мережі Wireless LAN (WLAN). Мережа Wi-Fi може працювати в двопунктових сполученнях, однак найчастіше використовують один або декілька пунктів доступу.

Ранні стандарти, такі як 802.11a, 802.11b та 802.11g, заклали основу розвитку Wi-Fi мереж. Зокрема, стандарт 802.11b працює у діапазоні 2,4 ГГц та забезпечує швидкість до 11 Мбіт/с, тоді як 802.11a (5 ГГц) і 802.11g (2,4 ГГц) підтримують швидкість до 54 Мбіт/с. На сьогодні ці стандарти вважаються застарілими та використовуються переважно у старому обладнанні.

У сучасних мережах застосовуються більш ефективні стандарти. Стандарт 802.11n (Wi-Fi 4) підтримує роботу у діапазонах 2,4 і 5 ГГц та забезпечує швидкість до 600 Мбіт/с. Стандарт 802.11ac (Wi-Fi 5) працює у діапазоні 5 ГГц і забезпечує значно вищу пропускну здатність (понад 1 Гбіт/с). Найсучасніший стандарт 802.11ax (Wi-Fi 6) підвищує не лише швидкість, а й ефективність роботи мережі при великій кількості пристроїв.

Принцип дії мережі Wi-Fi. Кожен Wi-Fi-адаптер (станція) постійно сканує ефір у пошуку сигналів від пунктів (точок) доступу. Сканування буває пасивним та активним. При пасивному скануванні Wi-Fi-адаптер переглядає окремі канали в пошуку найсильнішого сигналу з пунктів доступу. А кожен пункт доступу періодично передає сигнал (кадр) присутності. В цьому

кадрі є ідентифікатор пункту та доступні швидкості передавання. При активному скануванні Wi-Fi-адаптер сам ініціює сканування, передаючи кадр вимоги на передавання, а пункти доступу відповідають кадрами присутності і надалі процес відбувається так, як при пасивному скануванні.

Після сканування відбувається процес автентифікації, який ініціює Wi-Fi-адаптер, що передає запит до пункту доступу. Цей пункт перевіряє запит і підтверджує або відхиляє його. Wi-Fi-адаптер після успішної автентифікації обирає пункт доступу, з яким буде працювати та узгоджує швидкість передавання. Пункт доступу відповідає кадром підтвердження у якому наводиться додаткову інформацію про себе. Після цього, починається сеанс передавання.

Режими аутентифікації у Wi-Fi-мережах:

1. *Відкрита аутентифікація*. Підключення відбувається без пароля, шифрування не використовується, всі дані передаються у відкритому вигляді тому вони можуть бути перехоплені.

2. *Personal (персональна аутентифікація)*. Використовується єдиний пароль для всіх пристроїв у мережі, при цьому кількість пристроїв обмежена (невелика).

3. *Enterprise (відокремлена аутентифікація)*. Використовуються визначені паролі для різних користувачів з використанням сервера аутентифікації (застосування протоколів Radius, LDAP), захищеність користувачів найвища, але необхідно використовувати спеціальне обладнання.

Для розгортання Wi-Fi-мережі використовують безпроводові точки доступу і безпроводові адаптери. Однак у найпростішому випадку для передачі даних через Wi-Fi-з'єднання навіть не потрібно використання точки доступу. Серед режимів функціонування Wi-Fi-мереж широкого застосування отримали: *Infrastructure* і *Ad Hoc*.

У режимі *Ad Hoc*, що також називають *Independent Basic Service Set (IBSS)*, або *Peer to Peer* (точка-точка), вузли мережі безпосередньо взаємодіють один з одним без участі точки доступу. Цей режим потребує мінімального устаткування: кожен Wi-Fi-клієнт такої мережі повинен бути оснащений тільки Wi-Fi-адаптером. При такій конфігурації не потрібно створення мережної інфраструктури. Основними недоліками режиму Ad

Нос є: обмежений діапазон дії мережі і неможливість підключення до зовнішніх мереж. Якщо обидва Wi-Fi-клієнти перебувають у безпосередній близькості, або в межах прямої видимості, то режим Ad Hoc дозволяє об'єднати їх у одну мережу. Такий режим може бути ефективним при передачі даних з одного пристрою на інший. Але, якщо необхідно об'єднати в таку Wi-Fi-мережу пристрої розташовані на більших відстанях, або в різних приміщеннях, то режим Ad Hoc не ефективний, оскільки потужності передавачів і чутливості приймачів для забезпечення стійкого з'єднання буде недостатньо. У такому випадку для організації ефективної Wi-Fi-мережі потрібно застосовувати стаціонарну точку доступу. Перевагою цього підходу є те, що це дає змогу розширити зону покриття (радіус дії) Wi-Fi-мережі.

Точка доступу в безпроводовій мережі виконує функцію, яка аналогічна до функції комутатора традиційної кабельної мережі і дозволяє поєднувати всіх клієнтів у єдину мережу. Завдання точки доступу - координувати обмін даними між всіма клієнтами мережі і забезпечити всім клієнтам рівноправний доступ до середовища передачі даних.

Режим функціонування безпроводової мережі на базі точки доступу називається - *Infrastructure Mode*. Розрізняють два різновиди режиму Infrastructure Mode: основний *BSS (Basic Service Set)* і розширений *ESS (Extended Service Set)*. У режимі BSS всі вузли мережі зв'язуються між собою тільки через одну точку доступу, що може виконувати також роль моста до зовнішньої мережі. А у розширеному режимі, тобто ESS, використовується інфраструктура з декількох мереж BSS, причому самі точки доступу взаємодіють одна з одною, що дозволяє передавати дані від однієї BSS до іншої. Між собою точки доступу з'єднуються за допомогою кабельної мережі, або радіомостами.

У сучасних електроенергетичних системах безпроводові мережі стандарту IEEE 802.11 застосовуються переважно як допоміжний засіб доступу до інформаційних ресурсів, а не як основний канал передачі технологічних даних. Їх використання регламентується вимогами до надійності, електромагнітної

сумісності та інформаційної безпеки, що характерні для об'єктів електроенергетики, зокрема підстанцій та систем автоматизації.

На електричних підстанціях Wi-Fi використовується для забезпечення сервісного доступу інженерно-технічного персоналу до обладнання. Наприклад, під час налагодження або технічного обслуговування пристроїв релейного захисту та автоматики (РЗА), контролерів або серверів автоматизованих систем керування технологічними процесами (АСУ ТП), спеціалісти підключаються до локальної мережі підстанції за допомогою ноутбуків або планшетів. У таких випадках Wi-Fi функціонує як точка доступу до внутрішньої мережі Ethernet, яка об'єднує обладнання підстанції. Типові параметри таких мереж відповідають стандартам IEEE 802.11n або 802.11ac, що працюють у діапазонах 2,4 ГГц або 5 ГГц і забезпечують швидкість передачі даних від десятків до сотень Мбіт/с. При цьому передача критичних сигналів керування та захисту, наприклад сигналів протиаварійної автоматики, здійснюється виключно по дротових каналах зв'язку.

У системах автоматизованого комерційного обліку електроенергії (АСКОЕ) безпроводові технології можуть застосовуватись для локального доступу до вузлів збору даних. Зокрема, у практиці експлуатації використовується підключення до концентраторів або лічильників через вбудовані або зовнішні комунікаційні модулі. Інженер, перебуваючи безпосередньо на об'єкті, може встановити з'єднання з пристроєм через Wi-Fi для зчитування архівів споживання, перевірки параметрів або конфігурації обладнання. Такі підключення зазвичай здійснюються в межах локальної мережі з приватною IP-адресацією (наприклад, 192.168.x.x), що відповідає стандартній практиці налаштування мережевих пристроїв.

У задачах моніторингу технічного стану обладнання Wi-Fi використовується для організації допоміжних каналів збору даних від датчиків або діагностичних систем. Це може включати передачу інформації про температуру, вібрацію або інші параметри стану трансформаторів, розподільчих пристроїв або допоміжного обладнання. Такі рішення зазвичай застосовуються у вигляді локальних безпроводових сегментів, які інтегруються з основною мережею через маршрутизатори або шлюзи. При

цьому вимоги до часу затримки та гарантованості доставки даних у таких системах є менш жорсткими, ніж у системах релейного захисту.

Разом з тим, використання Wi-Fi в електроенергетиці обмежується рядом факторів, перш за все електромагнітними завадами. На підстанціях, особливо високої напруги, виникають значні електромагнітні поля внаслідок комутаційних процесів, роботи силового обладнання та імпульсних перенапруг. Ці фактори можуть негативно впливати на стабільність радіоканалу, що проявляється у вигляді зниження рівня сигналу, зростання кількості повторних передач і втрат пакетів. Особливо чутливим до завад є діапазон 2,4 ГГц, який також використовується іншими пристроями, що може призводити до додаткового навантаження на канал.

Ще одним суттєвим обмеженням є відсутність гарантованих параметрів затримки передачі даних. У безпроводових мережах застосовується метод доступу CSMA/CA, який не забезпечує детермінованого часу доставки пакетів. У результаті затримки можуть змінюватися в залежності від завантаження мережі та кількості підключених пристроїв. Це робить Wi-Fi непридатним для передачі критичних сигналів керування в реальному часі, які потребують гарантованої доставки з мінімальними затримками.

З точки зору інформаційної безпеки, безпроводові мережі є більш вразливими порівняно з провідними. Для забезпечення захисту даних використовуються сучасні механізми шифрування, такі як WPA2 (з алгоритмом AES) або WPA3, а також додаткові засоби контролю доступу, включаючи фільтрацію за MAC-адресами та сегментацію мережі. У практиці експлуатації енергетичних об’єктів доступ до критичних систем через Wi-Fi, як правило, обмежується і може додатково захищатися за допомогою VPN-з’єднань.

Таким чином, безпроводові мережі Wi-Fi в електроенергетичних системах використовуються як допоміжний інструмент для обслуговування, налаштування та моніторингу обладнання. Їх застосування доцільне у задачах, де не вимагається жорстка детермінованість передачі даних, однак для реалізації критичних функцій керування та захисту

використовуються виключно провідні або спеціалізовані комунікаційні технології.

Розглянемо особливість функціонування безпроводових мереж. Устаткування безпроводових мереж включає *точки доступу* (Access Point) і *безпроводові адаптери*. Точки доступу виконують роль концентраторів, що забезпечують зв'язок між абонентами та між собою, а також функцію мостів, що здійснюють зв'язок з кабельною локальною мережею та з Інтернетом. Декілька близько розташованих точок доступу утворюють зону доступу Wi-Fi, в межах якої всі абоненти, які мають безпроводові адаптерами отримують доступ до мережі. Такі зони доступу (*Hotspot*) створюються в місцях масового скупчення людей: в аеропортах, студентських кампусах, бібліотеках, офісах, бізнес-центрах і т. п.

Найкращий способом налаштування точки доступу за допомогою комп'ютера (зі встановленим мережним адаптером Ethernet), який підключений до мережевого комутатора. Розглянемо приклад налаштування точки доступу TP-Link TL-WR814N. Для цієї точки доступу за замовчуванням встановлена IP адреса 192.168.0.1 з маскою підмережі 255.255.255.0. Для того, щоб приступити до налаштування точки доступу необхідно призначити комп'ютеру статичну IP адресу з тієї ж підмережі, що і для TP-Link TL-WR814N. Для налаштувань параметрів TCP/IP протоколів потрібно перейти в меню: «*Панель керування → Мережа й Інтернет → Мережеві підключення*» і виконати налаштування в спеціальному мережевому інтерфейсі.

Для налаштування підключення точки доступу до мережі потрібно перейти у браузері за адресою 192.168.0.1 ввівши її в полі адресації. Також для даного типу роутера можна ввійти ввівши в полі адреси браузера http://tplinklogin.net. *Зауваження*. IP-адреса повинна бути в межах локальної мережі, тобто 192.168.0.X. У вікні авторизації необхідно ввести логін і пароль. За замовчуванням у багатьох точках доступу використовується логін: *admin* та пароль: *admin*, або порожнє поле. Для точного визначення цих параметрів необхідно звернутися до технічної документації на точку доступу. Після успішної авторизації відкривається сторінка з налаштуваннями точки доступу (рис. 1). Основні налаштування безпроводової мережі за допомогою меню

виконують за допомогою меню *Мережа* (*Сеть*) приведено на рис. 2.

Технології захисту бездротових мереж. *WEP* (Wired Equivalent Privacy) — стандарт захисту, який ґрунтується на методі потокового кодування з використанням алгоритму RC4 (загальний секретний ключ). *WPA* (Wi-Fi Protected Access) - технологія захисту, яка грунтується на протоколі TKIP (Temporal Key Integrity Protocol), що використовує стійкий механізм шифрування. TKIP змінює ключ шифрування для кожного переданого пакета, що ускладнює можливість його підбору. *WPA PSK* (WPA Pre-Shared Key) – це спрощена версія технології WPA, яка може застосовуватися для невеликих безпроводових мереж. У ній, як і в WEP, використовується статичний ключ, але він автоматично змінюється в певних часових інтервалах. *WPA2* є покращеною версією WPA та більш захищеною завдяки заміні TKIP на CCMP (блочне шифрування з кодом автентичності повідомлень). На даний час застосування WPA2 є обов'язковою для всіх сертифікованих Wi-Fi пристроїв. *WPA2 PSK* – це спрощена версія WPA2, яка аналогічна до WPA PSK, але з використанням AES-шифрування.

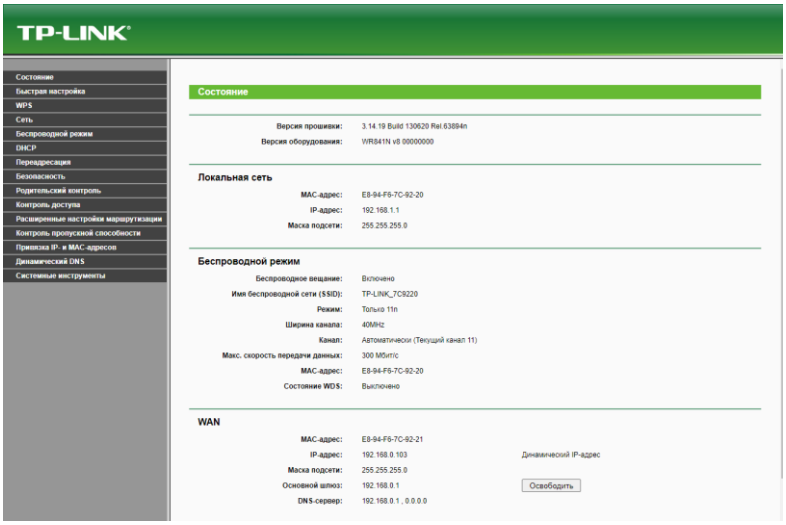


Рис. 1. Основне меню налаштуваннями TP-Link TL-WR814N

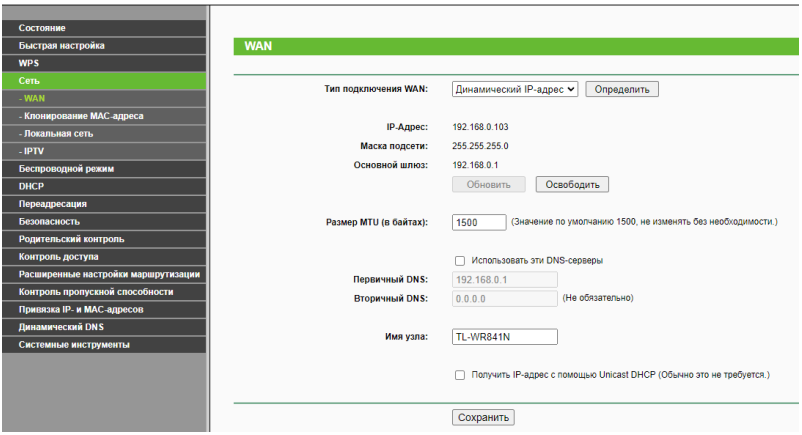


Рис. 2. Основні налаштування безпроводової мережі

Налаштування сервісу DHCP. DHCP – це протокол динамічної конфігурації, який дає змогу отримувати динамічні IP-адреси. На рис. 3 показано варіанти настроювання конфігурації DHCP. При ввімкнені DHCP пристрої можуть отримувати IP адресу автоматично з вказаного діапазону (*Начальный IP-адрес*). Така IP адреса буде змінюватися через певні проміжки вказаного часу (*Срок действия адреса*). Більшість сучасних мобільних пристроїв (смартфони, планшети) не мають налаштувань статичної IP-адреси, тому для їх нормального функціонування у цій мережі потрібно ввімкнення служби DHCP.

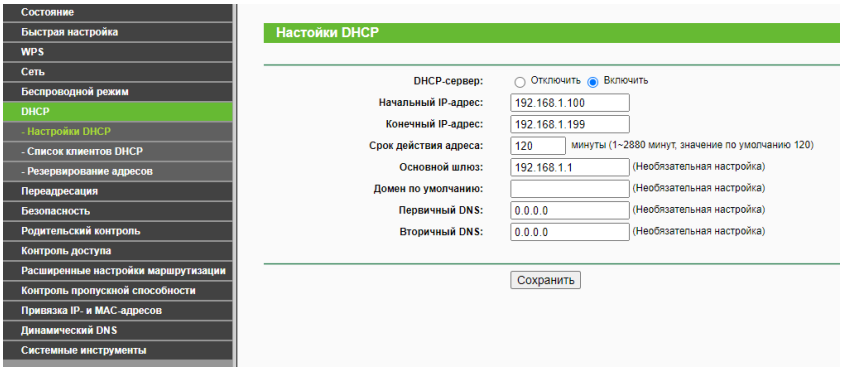


Рис. 3. Настроювання протокола динамічної конфігурації DHCP

Для перегляду різної статистичної інформації: списку підключених вузлів, помилок та інших параметрів використовується меню *Состояние* (рис. 4).

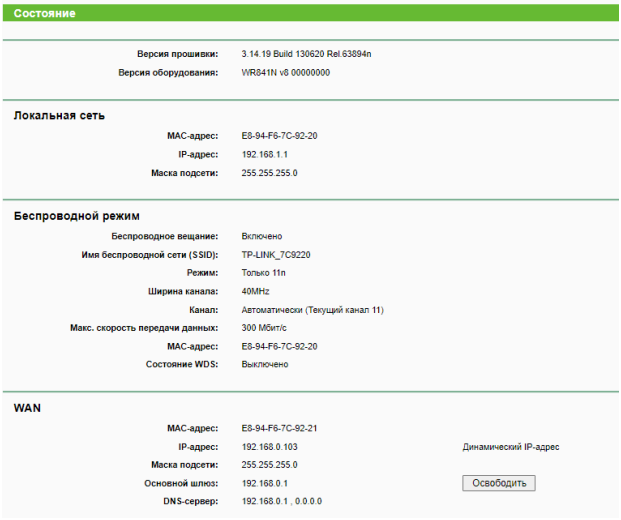


Рис. 4. Вигляд меню *Состояние*

Налаштування списку дозволених пристроїв за MAC-адресами можна виконати у додаткових налаштуваннях (рис. 5).

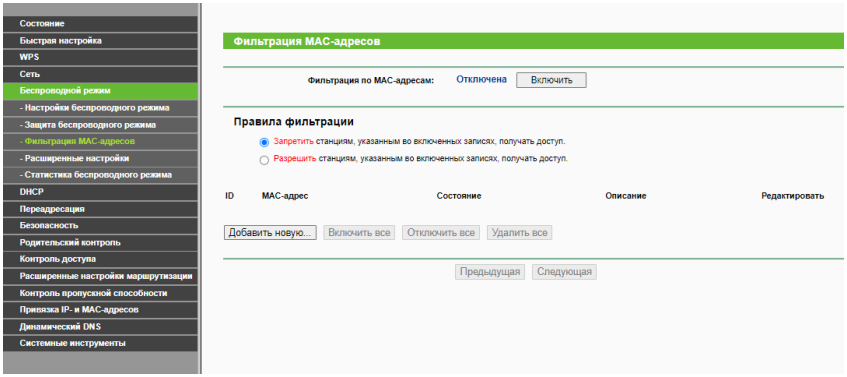


Рис. 5. Меню налаштувань параметрів MAC-адрес

Використовуючи *Tools*–меню для налаштувань прав доступу (рис. 6) можна обмежити доступу приховавши назву точки доступу. Це дасть змогу, приховати її видимість для інших, а при необхідності підключення до неї потрібно ввести її ім'я.

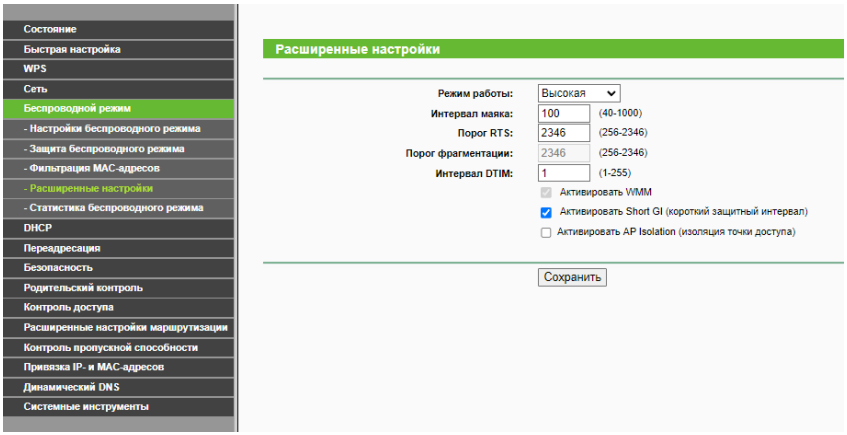


Рис. 6. Меню для додаткових налаштувань безпеки

Налаштування безпроводового Wi-Fi з'єднання на комп'ютері з ОС Windows. Для того щоб переглянути доступні безпроводові мережі і під'єднатися до Wi-Fi-мережі на локальному комп'ютері з операційною системою Windows 10 (подібно і на Windows 11) необхідно натиснути на відповідне зображення мережевого підключення у правому нижньому куті рядку стану. Після цього з'явиться перелік доступних безпроводових мереж. Для того щоб переглянути властивості безпроводової мережі можна у цьому ж вікні поряд з кнопкою доступних мереж натиснути на вкладку «*Налаштування мережі та інтернету*», або перейти в меню: «*Панель керування → Мережа й Інтернет → Мережеві підключення → Стан Wi-Fi → Властивості безпроводової мережі*» (рис. 7).

Підключення до невидимої мережі. Щоб налаштувати підключення до невидимої мережі (тієї яка не надсилає повідомлення з SSID ідентифікатором) потрібно перейти в пункт «*Стан Wi-Fi → Властивості безпроводової мережі*» та на відповідній вкладці вибрати необхідну мережу і зазначити

галочку «*Підключатися,навіть якщо мережа не передає своє ім'я (SSID)*» (рис. 7).

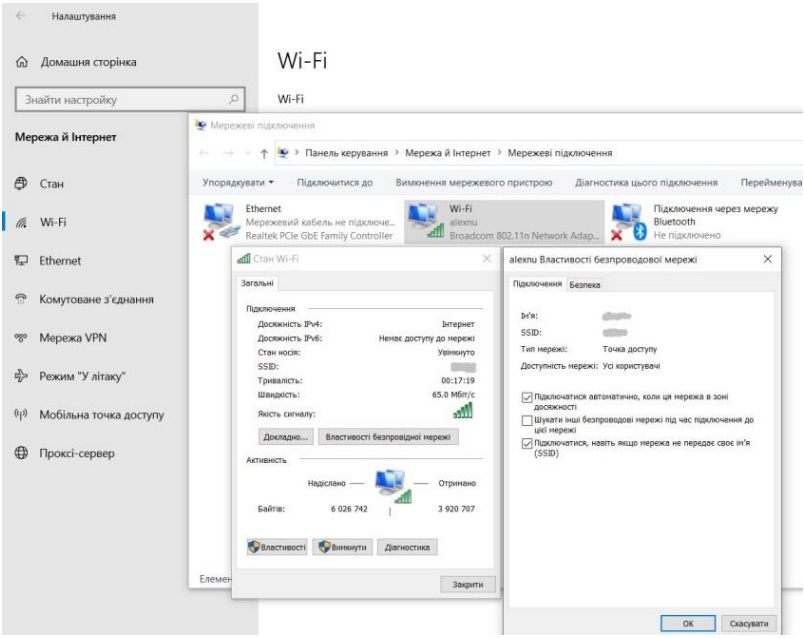


Рис. 7. Настроювання безпроводової мережі

Також можемо здійснити інші налаштування мережі та методи її аутентифікації.

Програма роботи

1. Ознайомитися з принципами побудови та функціонування безпроводових мереж стандарту IEEE 802.11.
2. Виконати базове налаштування Wi-Fi точки доступу та параметрів мережі.
3. Налаштувати параметри безпеки (шифрування, автентифікація, фільтрація доступу).
4. Провести тестування роботи мережі та аналіз її параметрів.

Порядок виконання роботи

1. Під'єднати точку доступу (Wi-Fi маршрутизатор) до

локального комп'ютера за допомогою патч-корда RJ45. *Зауваження*. У якості прикладу використано Wi-Fi маршрутизатор TP-Link TL-WR841N. У випадку використання іншого маршрутизатора опис меню з налаштуваннями можуть відрізнятися.

2. Налаштувати TCP/IP властивості для під'єднання до точки доступу та записати попередні налаштування. Для цього необхідно перейти: *Панель керування > Мережа й Інтернет > Мережеві підключення > Ethernet > Властивості Протокол інтернету версії 4 (TCP/IPv4) - властивості.*

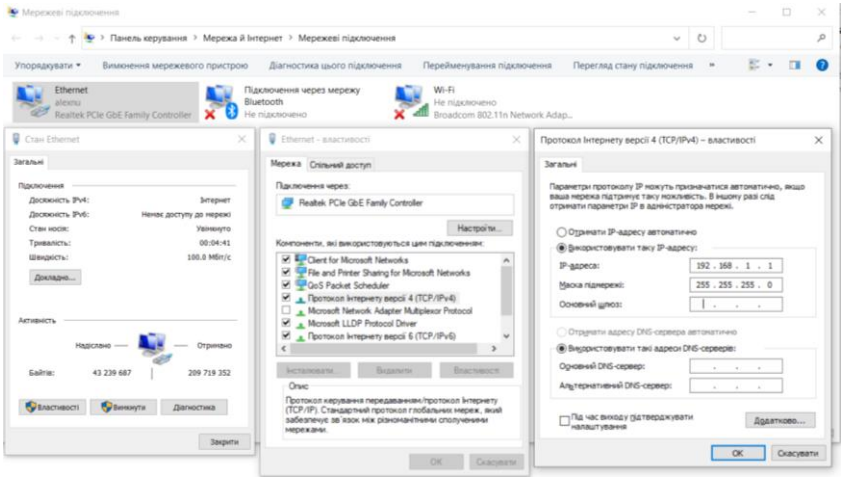


Рис. 8. Налаштування TCP/IP властивості для під'єднання до точки доступу

3. Перевірити зв'язок з точкою доступу за допомогою утиліти *ping* ввівши вказану IP-адресу (рис. 9).

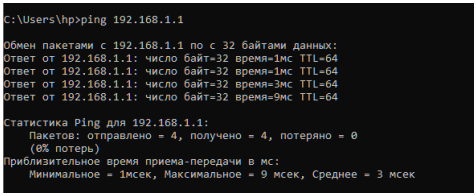


Рис. 9. Перевірити зв'язок з точкою доступу

4. Ознайомитись з наявними налаштуваннями маршрутизатора (меню *Status*): DHCP-сервера; MAC-адреси підключених пристроїв; алгоритм шифрування даних у безпровідній мережі; швидкість з'єднання; потужність сигналу та ін.

Зауваження. Щоб зайти в налаштування маршрутизатора необхідно в браузері відкрити сторінку за адресою основного шлюзу (див. п.2). У стандартних налаштуваннях часто використовують IP: 192.168.0.1. Також для входу на цю сторінку потрібно мати логін і пароль адміністратора точки доступу, він може бути вказаний в документації, або на зворотній стороні маршрутизатора.

4.1. Зафіксувати основні параметри мережі: IP-адресу точки доступу, діапазон DHCP, тип шифрування, канал, стандарт (802.11n/ac).

5. Виконати зміну назву точки доступу (SSID) використовуючи меню *Настройка беспроводного режима* (рис. 10).

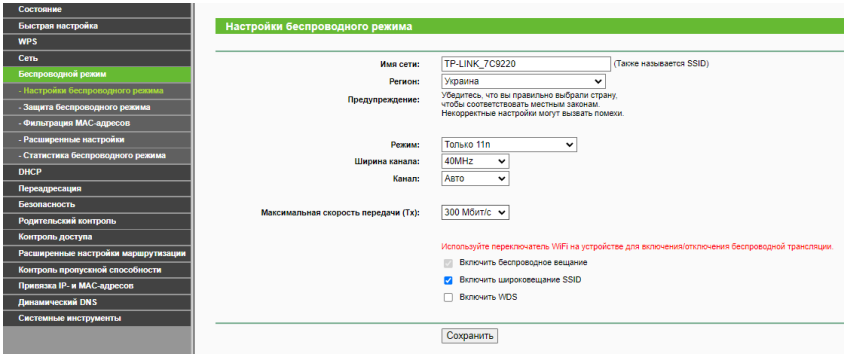


Рис. 10. Зовнішній вигляд меню маршрутизатора з вибором налаштування мережі

5.1. Ввести параметри налаштування мережі натиснувши (*редаг*.) ввівши назву мережі, у нашому прикладі це - ххх та режими роботи маршрутизатора, подібно як це показано на рис. 11.

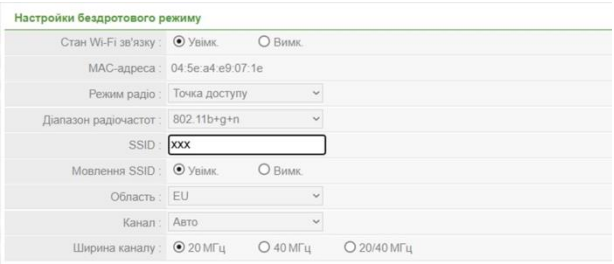


Рис. 11. Зміна назви точки доступу (SSID)

6. Виконати вибір типу шифрування даних та задання пароля доступу (рис. 12).

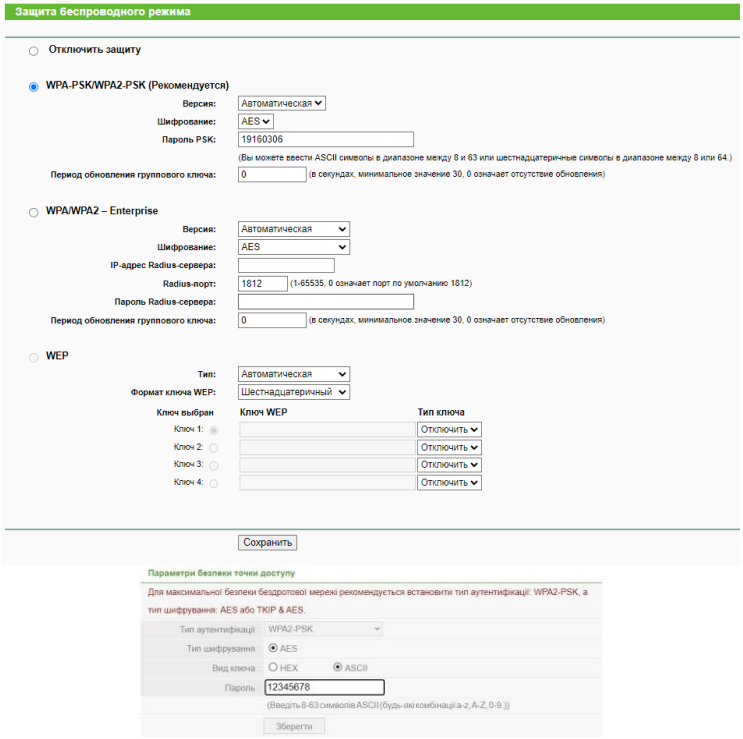


Рис. 12. Приклад зміни типу шифрування та пароля доступу

7. Виконати підключення до налаштованої точки доступу та

перевірити наявність з’єднання (рис. 13).

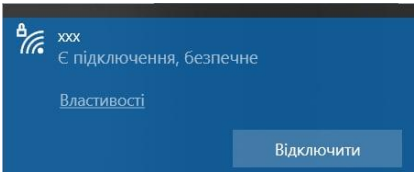


Рис. 13. Перевірка можливості з’єднання з маршрутизатором

8. Під’єднатися до точки доступу з довільного пристрою та провести тестування з’єднання за допомогою утиліт *ping*, *netstat* та ін. (рис. 14).

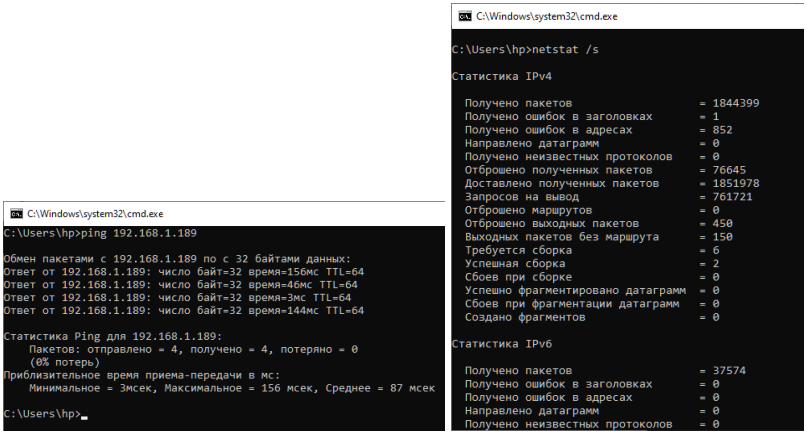


Рис. 14. Перевірка з’єднання з маршрутизатора за допомогою утиліт *ping*, *netstat*

8.1. Проаналізувати якість з’єднання: затримку (ping), стабільність, рівень сигналу. Зробити висновок щодо можливості використання даного з’єднання.

9. Порівняти роботу мережі при використанні WPA2-PSK та WPA3 (за наявності), оцінити вплив на підключення та безпеку.

9.1. Змінити параметри аутентифікації (WPA-PSK, WPA2-PSK та ін.) почергово перевіряючи та доналаштовуючи з’єднання на маршрутизаторі.

10.Знайти під’єднаний/ні пристрій/ої в меню статистики на

точці доступу та зафіксувати їх MAC-адреси (у нижчеподаному прикладі доступні тільки 3-и пристрої) (рис. 15).

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
Redmi7A-Redmi	192.168.1.189	c8:3d:dc:14:33:1d	11h 56m 13s
?	192.168.1.227	40:2c:f4:02:5d:07	11h 33m 1s
Aleks	192.168.1.221	64:31:50:09:73:83	11h 46m 21s

Рис. 15. MAC-адреси під'єднаних пристроїв

10.1. Виконати тестування роботи фільтру MAC-адрес. Для цього спочатку заблокуйте доступ до тестованого пристрою вказавши його MAC-адресу, а потім дозвольте підключення тільки цьому пристрою (рис. 16).

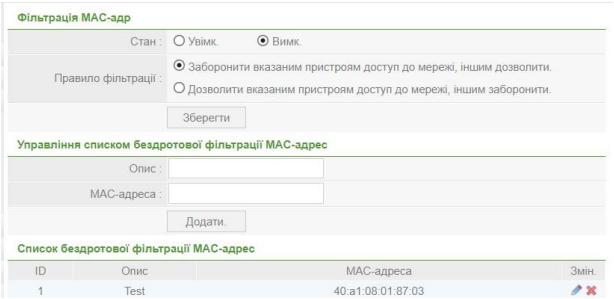


Рис. 16. Налаштування фільтрації за MAC-адресами

10.2. Виконати приховування точки доступу (SSID) за допомогою встановлення відповідної відмітки (рис. 17) та перевірити результат за допомогою стороннього пристрою.

Рис. 17. Виконання приховування маршрутизатора

10.3. Виконати під'єднання до прихованої (невидимої) мережі та протестувати це з'єднання (за допомогою послідовності, яка описана в теоретичних відомостях, рис. 7).

11. Зберегти резервну копію конфігурації після завершення

налаштування..

11.1. Від'єднати точку доступу від локального комп'ютера та повернути налаштування TCP/IP до початкових значень.

12. Результати виконання всіх пунктів оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму роботи;
- опис виконання роботи за пунктами із поясненням виконаних дій;
- скріншоти налаштувань точки доступу (SSID, шифрування, DHCP, MAC-фільтрація);
- результати тестування з'єднання (ping, підключення пристроїв);
- зафіксовані основні параметри мережі (IP-адреса, діапазон DHCP, тип шифрування, стандарт Wi-Fi);
- короткий аналіз якості з'єднання та можливості застосування Wi-Fi в електроенергетичних системах;
- висновок.

Контрольні запитання

1. Що таке Wi-Fi та які рівні моделі OSI він охоплює?
2. Які основні стандарти IEEE 802.11 використовуються у сучасних мережах?
3. У чому відмінність між діапазонами 2,4 ГГц та 5 ГГц?
4. Які режими роботи Wi-Fi мереж існують (Infrastructure, Ad Hoc)?
5. Яку функцію виконує точка доступу (Access Point)?
6. Що таке SSID та для чого він використовується?
7. Які методи автентифікації та шифрування застосовуються у Wi-Fi мережах?
8. Для чого використовується DHCP у безпроводових мережах?
9. Які основні обмеження використання Wi-Fi в електроенергетичних системах?

10.Чому безпроводові мережі не застосовуються для передачі критичних сигналів керування?

Лабораторна робота 5
Віртуалізація та використання мережевих операційних систем в інформаційних системах електроенергетики

Мета роботи

Ознайомитися з принципами віртуалізації та використання мережевих операційних систем для розгортання серверних і мережевих сервісів в інформаційних системах електроенергетичних об'єктів.

Теоретичні відомості

Віртуалізація – надання абстрагованих від апаратної реалізації обчислювальних ресурсів, що забезпечує логічну ізоляцію процесів, виконуваних на одному фізичному ресурсі. Віртуалізація дозволяє запустити декілька операційних систем (ОС) на одному комп'ютері. За допомогою цієї властивості можна убезпечити операційну системи та ПК від помилок та пошкоджень на етапі розробки і впровадження нових операційних систем, програм та функцій, а також для безпечного використання мережевих функцій та налаштувань.

Поширеним способом віртуалізації є бінарна трансляція, що полягає у перехопленні гіпервізором інструкцій віртуалізованої системи та їх заміні на "безпечні" інструкції, що далі виконуються процесором (напр., VMWare Workstation, VirtualBox, QEMU). Гіпервізор – це програма, яка керує фізичними ресурсами обчислювальної машини та розподіляє ці ресурси між декількома різними операційними системами, дозволяючи запускати їх одночасно.

Більшу продуктивність віртуалізовних систем забезпечує паравіртуалізація («спосіб свідомого співробітництва»), гостьові операційні системи підготовлюються для виконання в віртуалізованому середовищі, для чого програмне ядро цих операційних систем дещо модифікується. Операційна система взаємодіє із програмою гіпервізора, який надає їй гостьовий API, замість використання безпосередньо таких ресурсів, як таблиця сторінок пам'яті.

Апаратна віртуалізація – віртуалізація за допомогою спеціальної процесорної архітектури. На відміну від програмної

віртуалізації, можливе використання ізольованих гостьових систем, керованих гіпервізором безпосередньо. Апаратна віртуалізація забезпечує більшу продуктивність у порівнянні з продуктивністю невіртуалізованної машини, що дає віртуалізації можливість практичного використання і широкого застосування. Найбільш поширені технології віртуалізації Intel-VT і AMD-V (Xen, VMWare Workstation, VirtualBox).

Для виконання різноманітних операцій та команд з адміністрування та захисту комп'ютерних мереж широко використовуються Unix-подібні операційні системи. Одна з таких – операційних систем Linux. Linux є розробкою вільного програмного забезпечення. На відміну від комерційних операційних систем (Microsoft Windows та MacOS), початкові коди Linux доступні усім для використання, зміни та розповсюдження абсолютно вільно (в тому числі безкоштовно).

У сучасних електроенергетичних системах операційні системи сімейства Linux широко застосовуються як платформа для розгортання серверів SCADA та систем збору технологічних даних. Це обумовлено їх стабільністю, відкритістю, підтримкою мережевих протоколів та можливістю роботи в безперервному режимі (24/7). У промисловій практиці використовуються як універсальні дистрибутиви (Debian, Ubuntu Server, Red Hat Enterprise Linux), так і спеціалізовані рішення, оптимізовані для роботи в автоматизованих системах керування технологічними процесами (АСУ ТП).

Типовий дистрибутив Linux складається з:

– ядра Linux;
– інструментів та бібліотек проєкту GNU;
– додаткових програм;
– документації;
– графічної системи (графічного серверу);
– віконуваного менеджера;
– середовища робочого столу та ін.

SCADA-сервери, які функціонують під керуванням Linux, виконують обробку, візуалізацію та архівування технологічних даних, що надходять від програмованих логічних контролерів (ПЛК) та пристроїв релейного захисту. У таких конфігураціях

сервер Linux виконує роль центрального вузла, що забезпечує збір даних, їх обробку та надання доступу клієнтським робочим станціям через мережу Ethernet із використанням TCP/IP. Як правило, для підвищення надійності SCADA-сервери працюють у виділених сегментах мережі (наприклад, технологічна підмережа з адресацією типу 192.168.x.x або 10.x.x.x), із обмеженим доступом з боку зовнішніх мереж.

У задачах збору та зберігання технологічної інформації Linux використовується як платформа для серверів баз даних та архівів. Зокрема, на таких серверах розгортаються системи керування базами даних, наприклад PostgreSQL або MySQL/MariaDB, які забезпечують довготривале зберігання параметрів режимів роботи енергетичного обладнання (напруга, струм, потужність, стан вимикачів тощо). Дані надходять у реальному часі через мережеві протоколи та записуються у базу для подальшого аналізу. Linux-сервери в таких системах забезпечують виконання мережевих сервісів, керування доступом користувачів та інтеграцію з іншими компонентами інформаційної інфраструктури.

Однією з ключових переваг використання Linux у енергетичних системах є можливість гнучкого налаштування мережевих параметрів і сервісів. Засоби конфігурації мережі (ip, netplan, systemd-networkd) дозволяють реалізувати статичну IP-адресацію, сегментацію мережі, маршрутизацію та обмеження доступу. Крім того, системи безпеки, такі як iptables або nftables, забезпечують фільтрацію трафіку на рівні мережевого стека, що є важливим для захисту SCADA та серверів збору даних від несанкціонованого доступу. У практиці експлуатації також застосовується розмежування доступу до систем через ролі користувачів та використання захищених каналів зв’язку.

Сучасні системи Linux дозволяють виконувати практично все за допомогою програм з графічним інтерфейсом, починаючи від встановлення програмного забезпечення і закінчуючи налаштуванням системи. Але для роботи з серверами, адмініструванням мереж та для інших задач теж використовується термінал. Термінал - це програма Linux, яка має інтерфейс командного рядка і є інструментом, за допомогою якого здійснюється керування операційною системою та виконання

багатьох різноманітних операцій. За допомогою термінала можна: встановлювати і запускати програми; працювати з файлами; налаштовувати систему та багато іншого. Для роботи в терміналі необхідно використовувати команди. Команда - це ім'я програми, яке вводиться в терміналі для її запуску. Разом з ім'ям в команді можуть бути присутніми опції і параметри.

У нашому випадку ми використовуватимемо команди дистрибутива Debian. Варто зауважити, що ті ж команди використовуються та подібні для інших дистрибутивів Linux. Розглянемо деякі приклади команд терміналу:

lsb_release -a виводить інформацію про поточну версію ОС;

uname -a надає інформацію про поточне ядро системи;

su (англ. "substitute user" - замінити користувача) застосовується для перемикання з одного користувача на іншого, при цьому вона може запустити як оболонку входу в умовах поточного каталогу і оточення (su), так і повністю змінити налаштування, замінивши їх оточенням цільового користувача (su -). Синтаксис команди: *su [ім'я_користувача]*;

sudo (англ. "Substitute User and do" - підмінити користувача та виконати) використовується як префікс до команд Linux, дозволяючи користувачеві виконувати команди, що вимагають привілеїв *root*.

На відміну від *su*, команда *sudo* вимагає введення пароля поточного користувача. *root* або суперкористувач — це спеціальний обліковий запис та група користувачів у Unix-подібних системах з ідентифікатором, власник якого має право на виконання всіх без винятку операцій. Основні команди терміналу Debian показано в табл. 1.

Таблиця 1

Перелік основних команд терміналу Debian

Команда	Опис	Приклад використання
ls	Відображає список файлів і каталогів	ls -l
cd	Змінює поточний каталог	cd /home/user
pwd	Показує поточний шлях	pwd

mkdir	Створює новий каталог	mkdir new_folder
rmdir	Видаляє порожній каталог	rmdir old_folder
rm	Видаляє файл або каталог	rm -r temp
cp	Копіює файли або каталоги	cp file.txt /home/user/
mv	Переміщує або перейменовує файли	mv old.txt new.txt
cat	Виводить вміст файлу	cat info.txt
nano	Редагує текстовий файл у редакторі nano	nano config.txt
sudo	Виконує команду від імені адміністратора	sudo apt update
reboot	Перезавантажує систему	sudo reboot
shutdown	Вимикає систему	sudo shutdown -h now
top	Відображає активні процеси	top
ps	Показує список процесів	ps aux
kill	Завершує процес за PID	kill 1234
ping	Перевіряє доступність вузла в мережі	ping google.com
ip a	Показує налаштування мережевих інтерфейсів	ip a
ss	Відображає активні мережеві з’єднання	ss -tuln
wget	Завантажує файли з Інтернету	wget https://example.com/file.txt
scp	Копіює файли між комп’ютерами через SSH	scp file.txt user@192.168.1.2:/home/user/
apt update	Оновлює список доступних пакетів	sudo apt update
apt upgrade	Оновлює встановлені пакети	sudo apt upgrade
apt	Встановлює новий пакет	sudo apt install vim

install		
apt remove	Видаляє встановлений пакет	sudo apt remove nano
apt search	Шукає пакети в репозиторії	apt search firefox
whoami	Показує ім’я поточного користувача	whoami
adduser	Створює нового користувача	sudo adduser student
passwd	Змінює пароль користувача	passwd
chmod	Змінює права доступу до файлу	chmod 755 script.sh
chown	Змінює власника файлу або каталогу	sudo chown user:user file.txt

З іншими командами можна познайомитися у документації до дистрибутива, а також на різноманітних довідкових ресурсах наприклад: *https://linuxguide.rozh2sch.org.ua*

Таким чином, Linux виступає базовою платформою для реалізації серверної частини інформаційних систем електроенергетики, зокрема SCADA та систем збору даних. Його використання забезпечує надійне функціонування мережевих сервісів, підтримку стандартних промислових протоколів та можливість інтеграції з різними компонентами автоматизованих систем, що підтверджується широким застосуванням у сучасних енергетичних підприємствах.

Програма роботи

1. Створити віртуальну машину та ознайомитись з її інтерфейсом.
2. Запустити віртуальну машину та встановити операційну систему Debian.
3. Використати основні команди терміналу Debian.

Порядок виконання роботи

1. Розглянути особливості віртуалізації.

1.1. Визначити, яку інформаційну систему імітує створювана віртуальна машина.

1.2. Визначити основні функції цієї системи з обробки та зберігання даних, мережевого обміну даними та доступ користувачів.

1.3. Запустити віртуальну машину Oracle VM VirtualBox.

Зауваження. Для роботи Oracle VM VirtualBox необхідно, щоб в налаштуванні BIOS було увімкнено апартну віртуалізацію на ПК. Якщо процесор ПК не підтримує апаратну віртуалізацію AMD-V або Intel VT-x необхідно в налаштуваннях віртуальної машини зняти відмітку «*Увімкнути VT-x/AMD-V*» на вкладці *Система > Прискорення*.

2. Скопіювати файл віртуального диска на локальний комп'ютер.

3. Створити нову віртуальну машину (кнопка *Create/Створити* на панелі інструментів). Вибір операційної системи у вікні створення впливає лише на відображувану піктограму віртуальної машини та не обмежує використання у ній інших операційних систем, наприклад, Windows (у нашому випадку вказуємо тип Debian).

4. Вказати розмір RAM не менше ніж 512 Мб.

5. Створити новий віртуальний диск, прийнявши параметри за замовчуванням.

5.1. Підключити ISO-образ інсталяційного диску з якого буде встановлюватися операційна система та вказати шлях до папки з попередньо завантаженою інсталяцією операційної системи. У нашому випадку це ОС Debian.

5.2. Завантажити ISO-образ за посиланням *https://www.debian.org/download*. За вказаним посиланням знаходиться найновіший ISO-образ ОС Debian (на момент виходу даних методичних вказівок - Debian-12.7.0).

Зауваження. Для запуску інсталяції потрібно в *Налаштування* віртуальної машини у закладці *Пам'ять* додати *Оптичний привод* у який треба додати попередньо завантажений ISO-образ Debian. У процесі встановлення вказуємо логін і пароль для звичайного користувача та користувача з правами адміністратора (*root*), а також інші параметри операційної системи.

5.3. Після встановлення ОС Debian вимикаємо віртуальну

машину.

6. Для повторного запуску віртуальної машини, якщо ОС Debian не запуститься автоматично, потрібно в меню *Пам'ять* вибрати встановлену операційну систему та за допомогою опції налаштування (кнопка *Налаштувати*) задати тип підключення до мережі — *проміжний адаптер/мережевий міст*.

7. Виконати повторний запуск віртуальної машини та ввійти в систему з логіном та паролем вказаними при встановленні операційної системи.

Зауваження. Для виконання команд у ОС Debian необхідно серед доступних програм вибрати *Термінал,* що дає змогу виконувати всі необхідні процедури та команди.

8. Виконати команду *sudo ip a* (*sudo* – виконується від імені поточного користувача, за замовчуванням). За необхідності виконання команди від суперкористувача *root* – вводимо *ip a*.

8.1. Копіюємо отриманий результат та записуємо у звіт, після чого знову вимкаємо віртуальну машину.

Зауваження. Для переходу до користувача *root* потрібно виконати команду *su root* та після цього ввести пароль користувача *root*.

9. Змінити *налаштування мережі* у Oracle VM VirtualBox гостьової системи на NAT. Для цього необхідно перейти за вказаним шляхом (*Машина > Налаштувати > Мережа > Тип підключения > NAT*) та виконати зміни.

10. Порівняти отримані IP-адреси операційної системи Debian, яка запущена з віртуальної машини з адресою хост-системи, тобто з ОС Windows за допомогою команди *ipconfig -a*. Порівняти IP-адреси та визначити, чи належать вони до однієї підмережі залежно від типу підключення.

11. Перевірити час передачі пакетів до будь якого мережевого вузла в інтернеті програмою *ping* та оцінити затримку (RTT) і доступність вузла.

12. Порівняти отримані результати (час відгуку, втрати пакетів) між ОС Debian та ОС Windows. Для зупинки виконання команди *ping* використати комбінацію CTRL+C.

13. Виконати аналіз роботи мережевої операційної системи у віртуальному середовищі.

13.1. Проаналізувати отримані IP-адреси при використанні:

проміжний адаптер/мережевий міст (*Bridge*) та *NAT*.

13.2. Визначити доступність віртуальної машини в мережі та можливість її взаємодії з іншими вузлами.

13.3. Зробити висновок щодо: відмінностей режимів *NAT* і *Bridge*; доцільності їх використання в інформаційних системах електроенергетики.

14. Результати виконання оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

– титульну сторінку;

– мету роботи;

– програму та порядок виконання роботи;

– скріншоти створення та налаштування віртуальної машини;

– скріншоти результатів виконання команди *ip a*;

– скріншоти налаштувань мережі в режимах *Bridge* та *NAT*;

– результати виконання команди *ping* та їх порівняння (*Debian / Windows*);

– аналіз отриманих IP-адрес та режимів роботи мережі;

– висновок.

Контрольні запитання

1. Що таке віртуалізація та яке її призначення?
2. Які існують типи віртуалізації (апаратна, програмна, паравіртуалізація)?
3. Яке призначення гіпервізора?
4. Чому операційна система Linux широко використовується на серверах?
5. Які функції виконують сервери SCADA та збору даних в енергетичних системах?
6. У чому полягає різниця між режимами NAT та Bridge у VirtualBox?
7. Які IP-адреси використовуються у внутрішніх мережах (приватні діапазони)?
8. Яке призначення команди ip a в Linux?
9. Які параметри можна оцінити за допомогою команди ping?

10.У чому полягають особливості використання віртуалізації в електроенергетичних системах?

Лабораторна робота 6
Використання DHCP і DNS-серверів у мережах інформаційних систем електроенергетики

Мета роботи

Ознайомитися з принципами роботи та налаштування DHCP і DNS-серверів та набути практичних навичок їх використання у мережах інформаційних систем електроенергетичних об'єктів з урахуванням вимог до надійності та адресації вузлів.

Теоретичні відомості

DHCP (Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла) — це протокол прикладного рівня моделі OSI, що дозволяє комп'ютерам підключеним до мережі автоматично одержувати IP-адресу та інші параметри, необхідні для роботи в мережі. Для цього комп'ютер звертається до спеціального серверу DHCP. Під час запуску системи комп'ютер, який є DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає і відправляє повідомлення-відповідь, яка містить IP-адресу і деякі інші конфігураційні параметри. При цьому сервер DHCP може працювати в різних режимах:

Динамічний розподіл. Адміністратор присвоює IP-діапазон адрес на сервері DHCP. Кожен клієнтський комп'ютер в мережі повинен запитати IP-адресу від DHCP-сервера, коли мережа ініціалізується за концепцією "оренди". Коли закінчується термін оренди, якщо вона не буде продовжена, DHCP-сервер має право повернути адресу і призначити її на інші комп'ютери.

Автоматичне виділення. Сервер DHCP буде постійно призначати вільну IP-адресу з діапазону, встановленого адміністратором, запитуючому комп'ютеру. Основна відмінність з динамічним розподілом в тому, що сервер зберігає записи минулих оренд і намагається привласнити ту ж адресу тому ж комп'ютеру для майбутніх мережних підключень.

Статичний розподіл. Сервер DHCP здійснює призначення IP-адрес виключно на основі таблиці MAC-адрес, які зазвичай заповнені вручну адміністратором мережі. Якщо MAC-адреса комп'ютера не зазначена в таблиці, йому не буде призначена

мережева адреса.

NAT (від англ. Network Address Translation — «перетворення мережевих адрес») — це механізм у мережах TCP/IP, який дозволяє змінювати IP-адресу у заголовку пакету, що проходить через пристрій маршрутизації трафіку.

DNS (Domain Name System) використовується для перетворення символьних адрес, зрозумілих людині (наприклад, www.example.com), у числові IP-адреси, які використовуються у ПК. Це ієрархічна система, що складається з кореневих, доменних та авторитетних серверів. DNS працює на рівні додатків та забезпечує зручність користувачів у доступі до ресурсів мережі. Розрізняють декілька типів процедур перетворення DNS імен. Серед них найбільшого поширення здобули рекурсивна та нерекурсивна процедури.

Особливість нерекурсивної процедури запиту DNS імен:

1) DNS-клієнт звертається до кореневого DNS-сервера з вказівкою повного доменного імені;

2) DNS-сервер відповідає клієнту, вказуючи адресу наступного DNS-сервера, який виконує обслуговування домену верхнього рівня, заданого в наступній старшій частині імені;

3) DNS-клієнт виконує запит наступного DNS-сервера, який його надсилає до DNS-сервера потрібного піддомена і т.д., доти, доки не буде знайдено DNS-сервер, який повністю відповідає запитуваному імені IP-адреси. Сервер дає кінцеву відповідь клієнту.

Особливість рекурсивної процедура:

1) DNS-клієнт запитує локальний DNS-сервер, який обслуговує піддомен, якому належить клієнт;

2) якщо локальний DNS-сервер відповідь знає, то повертає її клієнту, в протилежному випадку виконує ітеративні запити до кореневого сервера до тих пір, поки не отримає відповідь;

3) після отримання відповіді сервер передає її клієнту.

Отже, при рекурсивній процедурі клієнт фактично передоручає роботу власному серверу. Для прискорення пошуку IP-адрес DNS-сервери часто застосовують кешування відповідей, які проходять через них.

У сучасних інформаційних системах електроенергетики протоколи DHCP та DNS використовуються як складові

мережевої інфраструктури, однак їх застосування має чітко визначені обмеження, зумовлені вимогами до надійності, детермінованості та безпеки функціонування технологічних процесів.

Протокол DHCP застосовується переважно для автоматичної конфігурації мережевих параметрів службових і допоміжних пристроїв, таких як робочі станції операторів, інженерні ноутбуки, а також допоміжні сервери. У таких випадках DHCP-сервер забезпечує видачу IP-адрес, шлюзу за замовчуванням та інших параметрів мережі в межах визначеного діапазону адрес (наприклад, 192.168.x.x або 10.x.x.x). Це дозволяє спростити адміністрування мережі та зменшити кількість помилок при налаштуванні клієнтських пристроїв.

Водночас у системах автоматизації електроенергетичних об’єктів важливі пристрої, такі як програмовані логічні контролери (ПЛК), пристрої релейного захисту та автоматики (РЗА), а також SCADA-сервери, як правило, використовують статичну IP-адресацію. Це обумовлено необхідністю забезпечення стабільної адресації, передбачуваності мережевих з’єднань та виключення залежності від роботи DHCP-сервера. Використання динамічної адресації для таких пристроїв може призвести до втрати зв’язку або некоректної роботи систем керування.

Протокол DNS у енергетичних системах використовується для забезпечення іменованого доступу до серверів та мережевих ресурсів. Зокрема, DNS-сервери застосовуються для перетворення доменних імен серверів SCADA, серверів баз даних або інших інформаційних ресурсів у відповідні IP-адреси. Це дозволяє спростити конфігурацію клієнтських систем і підвищити гнучкість адміністрування, оскільки зміна IP-адреси сервера не потребує переналаштування всіх клієнтів.

У практиці експлуатації SCADA-систем DNS використовується, зокрема, для забезпечення доступу клієнтських робочих станцій до серверів візуалізації та обробки даних, а також для організації взаємодії між серверними компонентами системи. При цьому DNS-сервери зазвичай розташовуються в межах внутрішньої мережі підприємства та не залежать від зовнішніх DNS-служб.

Таким чином, у мережах електроенергетичних систем застосовується комбінований підхід до адресації: критично важливі пристрої використовують статичні IP-адреси, тоді як DHCP застосовується для допоміжних вузлів мережі. DNS, у свою чергу, забезпечує зручний доступ до серверних ресурсів та підтримує структуровану організацію мережі, не впливаючи на детермінованість роботи технологічних систем.

Програма роботи

1. Навчитися налаштовувати мережі гостьової системи.
2. Навчитися налаштовувати та використовувати DNS та DHCP-сервери.

Порядок виконання роботи

1. Виконати аналіз використання DHCP та DNS у електроенергетичних системах.

1.1. Визначити, які пристрої у мережі електроенергетичного об'єкта можуть використовувати DHCP.

1.2. Визначити, які пристрої повинні використовувати статичні IP-адреси.

2. Запустити віртуальну машину Oracle VM VirtualBox.

2.1. Запустити ОС та ввійти з логіном та паролем вказаними при встановленні ОС Debian.

2.2. Запустити *Термінал,* після цього виконуємо всі необхідні процедури та команди.

3. Встановити *dnsmasq* та файловий менеджер *Midnight Commander* (MC) за допомогою команди *apt install dnsmasq mc*.

3.1. Відкрити файл налаштування DHCP та DNS-сервера *dnsmasq* (файл знаходиться в каталозі /*etc*, назва файлу: *dnsmasq.conf*). Змінити діапазон видаваних IP-адрес.

3.2. Виконати прив'язку MAC-адреси одного з вузлів локальної мережі до IP-адреси.

Зауваження. Оскільки редагування файлів налаштувань дозволено лише користувачу *root* (суперкористувачу), запуск файлового менеджера здійснюється командою *sudo mc* (відповідно без *sudo*, якщо ви з початку запустили ОС Debian під користувачем *root*). Переміщення по об'єктам у каталозі здійснюється клавішами керування курсором, перехід у

батьківський каталог (на рівень вище) – вибором .. *(дві крапки)*, перегляд текстового файлу – натисканням F3, редагування – F4.

3.3. Виконати редагування вказаного файлу за допомогою файлового менеджера *MC* та редактора *Nano*.

Зауваження. При першій спробі редагування з *MC* буде запропоновано обрати текстовий редактор за замовчуванням. Рекомендується обрати *Nano* вибором відповідної цифри та натисканням *Enter*.

4. Виконати завдання діапазон IP-адрес до видачі рядком *dhcp-range=*.

Зауваження. За замовчуванням рядки *dhcp-range=* закоментовані, тобто починаються з '#' - символу коментаря та ніяк не інтерпретуються при зчитуванні налаштувань.

4.1. Виконати задавання діапазону адрес, наприклад від 192.168.45.12 до 192.168.45.27 та час оренди 72 години, або інший діапазон. Для цього, знайдіть і розкоментуйте рядок (видаливши символ #).

4.2. Виконайте налаштування прив'язки IP-адреси до MAC-адреси, яке виконується подібним чином, знайшовши рядок виду: *#dhcp-host=MAC-адреса, IP-адреса* у файлі *dnsmasq.conf*.

4.3. Збережіть внесені зміни, натисніть *Ctrl+O* та підтвердіть ім'я файлу для збереження натисканням *Enter*.

4.4. Вийдіть з текстового редактора натисканням *Ctrl+X* та з файлового менеджера натисканням *F10*.

4.5. Виконайте застосування нових налаштувань шляхом перезапуску *Dnsmasq* командою *sudo service dnsmasq restart* (відповідно без sudo, якщо ви працюєте під користувачем *root*).

Зауваження. Виконавши пп. 3 і 4 ми налаштували можливість доступу до нашої локальної мережі тільки вказаними нами вузлами мережі IP-адрес, зокрема з прив'язкою MAC-адрес. Такий підхід обмежує доступ інших пристроїв, які не входять до вказаного нами діапазону MAC-адрес. Таким чином ми обмежили видачу IP-адрес лише визначеним вузлам мережі на основі MAC-адрес.

5. Виконати перевірку роботи DHCP-сервера. Це потрібно для того, щоб переконатися, що служба *dnsmasq* працює правильно.

5.1. Виконати перезапуск службу *dnsmasq* шляхом введення у терміналі команди: *sudo systemctl restart dnsmasq.* Ця команда

перезапускає DNS/DHCP сервер, щоб він зчитав нові налаштування.

5.2. Виконуємо перевірку запуску служби, для цього виконуємо команду терміналу: *sudo systemctl status dnsmasq.*

5.3. Визначаємо запуск служби. При появі повідомлення: *Active: active (running)* — сервер працює правильно. Якщо отримано повідомлення *failed* - значить є помилка у файлі налаштувань, потрібно переглянути журнал системи.

6. Виконати аналіз відповідності виданих IP-адрес заданому діапазону та прив'язці MAC-адрес.

Зауваження. Служба *dnsmasq* зберігає список усіх виданих IP-адрес у спеціальному файлі: *cat /var/lib/misc/dnsmasq.leases.*

6.1. Знаходимо файл *cat /var/lib/misc/dnsmasq.leases* (подібно до того, як це робили з файлом *dnsmasq.conf,* що описано у п. 3.

6.2. У файлі знаходимо рядок з переліком IP та MAC-адрес, наприклад: *1725345600 52:54:00:12:34:56 192.168.45.15 pc1 01:52:54:00:12:34:56* та перевіряємо наявність записів. Якщо записів немає — клієнти ще не отримали адресу. Така ситуація можлива, якщо інші пристрої ще не підключалися до мережі. Таким чином ми перевірили можливість налаштування та доступу DHCP-сервера.

7. Зробити висновок щодо доцільності використання DHCP для допоміжних вузлів та необхідності застосування статичної IP-адресації для критичних пристроїв електроенергетичних систем.

8. Результати виконання оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

– ·титульну сторінку;

– ·мету роботи;

– ·програму та порядок виконання роботи;

– ·короткий опис застосування DHCP та DNS у електроенергетичних системах;

– ·скріншот файлу налаштувань dnsmasq;

– ·скріншот результатів перевірки роботи служби (status dnsmasq);

– ·скріншот файлу dnsmasq.leases;

– ·аналіз отриманих IP-адрес та їх відповідності налаштуванням;

– ·висновок.

Контрольні запитання

1. Яке призначення протоколу DHCP у комп’ютерних мережах?
2. Які режими розподілу IP-адрес підтримує DHCP-сервер?
3. У чому полягає різниця між динамічним, автоматичним і статичним розподілом IP-адрес?
4. Яке призначення протоколу DNS у мережевій інфраструктурі?
5. У чому полягає відмінність між рекурсивною та нерекурсивною процедурами DNS-запиту?
6. Для чого використовується DNS-кешування?
7. Які пристрої в електроенергетичних системах доцільно налаштовувати через DHCP, а які — через статичні IP-адреси?
8. Чому для ПЛК, пристроїв РЗА та SCADA-серверів зазвичай використовують статичну IP-адресацію?
9. Яку роль виконує DNS у роботі SCADA-систем і серверів баз даних?
10. У чому полягають особливості використання DHCP та DNS у мережах інформаційних систем електроенергетики?

Лабораторна робота 7
Резервне копіювання та відновлення даних в інформаційних системах електроенергетичних об'єктів

Мета роботи

Ознайомитися з методами резервного копіювання та відновлення даних у системах автоматизації електроенергетичних об'єктів і навчитися реалізовувати процеси створення резервних копій та відновлення працездатності системи після аварійних збоїв.

Теоретичні відомості

У сучасних енергетичних підприємствах значна частина технологічних процесів — від вимірювання параметрів обладнання до управління генерацією та передачею електроенергії — здійснюється за допомогою інформаційно-керуючих систем. Надійність їхньої роботи безпосередньо залежить від збереженості даних і можливості відновлення систем після збоїв або аварій.

Одним із ключових елементів інформаційної безпеки є резервне копіювання — процес створення копій важливої інформації з метою її збереження і подальшого відновлення у випадку пошкодження, збою або втрати. Для енергетичних організацій ця процедура є обов'язковою, адже навіть короткочасна втрата даних може призвести до порушення технологічного процесу, помилок у системах керування або втрати важливих архівів вимірювань.

Резервне копіювання забезпечує безперервність роботи підприємства, дозволяє відновити дані після збоїв обладнання, кібератак, людських помилок чи пошкодження носіїв інформації. У сучасних енергетичних інформаційних системах воно реалізується як автоматизований і регулярний процес, який контролюється службами інформаційної безпеки або технічного обслуговування.

Резервне копіювання (backup) — це процес створення копій файлів, баз даних або цілої операційної системи з метою подальшого їх відновлення у випадку втрати. Його основні завдання:

- збереження критично важливої інформації — баз даних SCADA, журналів подій, звітів, технічної документації.

- швидке відновлення роботи після аварій — збою живлення, поломки жорсткого диска, вірусної атаки тощо.

- захист від людського фактору — випадкового видалення або зміни налаштувань.

- дотримання вимог стандартів і нормативів у сфері енергетики (зберігання архівів облікових даних протягом визначеного терміну).

Сучасні системи резервного копіювання інформації передбачають ефективну стратегію, організаційні рішення і політику збереження даних. Існують різні технології резервного копіювання, які відрізняються витратами коштів і часу:

- *повне резервне копіювання* - вибрані дані будуть скопійовані повністю. Найнадійніший спосіб, але потребує найбільшої кількості ресурсів, місця для зберігання даних і часу копіювання, тому в такому вигляді застосовується рідко, зазвичай комбінується з іншими видами. Дозволяє відновити втрачені дані з нуля швидше за всі інші види копіювання;

- *інкрементне копіювання* - записуються тільки ті дані, які були змінені з часу минулого копіювання. Для таких копій потрібно значно менше пам'яті, ніж при повному копіюванні і записуються вони значно швидше. При такому підході також необхідно періодично робити повну резервну копію, при будь-якій аварії систему відновлюють з такої копії, а потім накочуються на неї всі наступні інкрементні копії в хронологічному порядку. Важливим елементом інкрементного копіювання є відновлення видалених файлів і проміжних версій, які змінювалися;

- *диференціальне резервне копіювання* - схоже на інкрементне, тобто копіюються тільки зміни, зроблені з моменту останнього повного копіювання. Його відмінність полягає в тому, що в кожну наступну копію зберігаються зміни з попередньої і додаються нові. Для відновлення після аварії знадобиться тільки повна копія і остання з диференціальних, що значно скорочує час відновлення.

Створення резервної копії (*backup*) даних надає можливість виконати відновлення інформації при втраті оригіналу, з якого

було створено резервну копію. При цьому під втратою треба розуміти настання події, що призвела до зміни даних, після чого вони втратили цінність або були видалені з носія. Приклад: умисне завдання шкоди через видалення важливої для підприємства інформації.

Об'єкти резервного копіювання — це дані або сукупність даних, з яких можна створити резервну копію. Приклади об'єктів: файли або теки, дані прикладних програм, дані операційної системи чи сама ОС, образи віртуальних машин та дисків віртуальних машин, файлові системи тощо.

Рівні резервного копіювання. *Повне резервне копіювання* (Full Backup або L0) — повна копія даних. Рівень, який забезпечує створення повної копії об'єкту резервного копіювання. Цей рівень дозволяє забезпечити максимальну відповідність оригіналу даних його копії.

Диференційне резервне копіювання (Differential Backup або L1) — копіювання змін, що були зроблені після створення останньої повної копії. Створення такої копії потребує більше часу та займає більший об'єм, ніж додаткове копіювання, але дозволяє пришвидшити процес відновлення. Загалом є альтернативою між створенням повної або додаткової копії.

Додаткове резервне копіювання (Incremental Backup або L2) — копіювання змін, що відбулись із часу повного, диференційного або додаткового копіювання. Загалом на додаткове копіювання затрачається менше часу, бо копіюється менше файлів. Однак процес відновлення даних займає більше часу, оскільки повинні спочатку відновлюватися дані останньої повної копії і після цього - всі резервні копії, від яких залежить додаткова копія.

Під час роботи операційної системи деякі файли можуть використовуватись нею та бути недоступними для читання користувачем, тому резервна копія системного розділу ОС повинна виконуватись при неактивній ОС або використовувати технології ОС, що забезпечують актуальність вмісту файлів (Shadow Copy, Snapshot).

Щоб забезпечити можливість відновлення системного розділу у випадку, коли операційна система не може завантажитись з нього, резервну копію створюють за допомогою технологій LiveCD/LiveUSB/PXE. Це дозволяє за критичної помилки

завантаження операційної системи завантажити «відновлювальний» LiveCD/LiveUSB/PXE та відновити вміст системного розділу. Оптичний диск, що дозволяє завантажити операційну систему з нього без необхідності встановлення, називають LiveCD. Якщо аналогічну функцію має USB-накопичувач, його називають LiveUSB. PXE (англ. Preboot Execution Environment) — середовище для завантаження комп'ютерів за допомогою мережевої карти без використання жорстких дисків, компакт-дисків чи інших пристроїв, що застосовуються при локальному завантаженні операційної системи. Для організації завантаження системи в PXE використовуються протоколи IP, UDP, DHCP та TFTP. PXE-код, який зазвичай знаходиться в ПЗП мережевої карти, отримує з мережі по протоколу TFTP (отримаючи для цього адресу TFTP-сервера за допомогою DHCP) виконуваний файл, після чого передає йому управління.

Як правило, резервну копію зберігають в файлі-образі диска. Образ диска — файл, що містить у собі повну копію вмісту та структури файлової системи та даних, що містяться на диску. Образ розділу диску бажано розміщувати на іншому фізичному носії, щоб у випадку виходу з ладу диску не був втрачений і образ диску.

Під час виконання резервного копіювання важливу роль відіграють спеціалізовані програми, які дозволяють створювати точні копії систем, дисків або окремих файлів, а також відновлювати їх у разі збою. Одними з найбільш зручних інструментів для цього в середовищі ОС Linux є Clonezilla Live та GParted, які прості, універсальні та мають безкоштовний доступ.

Clonezilla Live — це програма, призначена для створення повних копій (образів) жорстких дисків або розділів. Вона запускається не з самої операційної системи, а з окремого завантажувального носія — флешки або віртуального диска. Завдяки цьому можна створювати резервні копії навіть тих систем, які не завантажуються. Clonezilla створює точний образ усього системного диска разом із операційною системою, драйверами, налаштуваннями, програмами та користувацькими файлами. Це дозволяє, у разі збою, швидко відновити роботу комп'ютера без повторного встановлення Debian чи іншої

системи. У даній лабораторній роботі Clonezilla застосовується для копіювання системного диска в образ або безпосередньо на інший резервний диск, а також для подальшого відновлення системи з цієї копії. Інтерфейс програми побудований у вигляді текстового меню, що дозволяє виконати основні дії покроково: вибір джерела, вибір диска-приймача, підтвердження операції та перевірка результату. Clonezilla підтримує більшість файлових систем і може працювати з носіями будь-якого типу, що робить її універсальним засобом резервного копіювання як для навчальних цілей, так і для промислових систем.

GParted (GNOME Partition Editor) — це програма для створення, редагування та форматування розділів на жорстких дисках. У процесі виконання лабораторної роботи вона використовується на етапі підготовки резервного носія. Перед тим як створити копію системи, необхідно мати порожній диск, на якому буде розміщено резервну копію. За допомогою GParted можна відформатувати диск у потрібну файлову систему (наприклад, *ext4*), створити таблицю розділів типу *msdos* і надати розділу унікальну мітку, щоб програма Clonezilla могла легко його ідентифікувати.

На практиці обидві програми взаємодіють між собою послідовно. Спочатку за допомогою GParted створюється і готується резервний диск, після чого Clonezilla виконує копіювання основного системного диска Debian 13 на цей резервний. У випадку збою або пошкодження операційної системи користувач завантажується з Clonezilla Live і розгортає образ системи назад на робочий диск, фактично відновлюючи працездатність системи за кілька хвилин. Такий підхід забезпечує повний цикл резервного копіювання — від підготовки носія до відновлення після збоїв, що є особливо важливим для енергетичних інформаційних систем, де надійність та швидке відновлення роботи є критичними умовами функціонування.

Окрім згаданих програм, для резервного копіювання і відновлення системи використовуються інші, які можуть використовуватись як у професійних енергетичних середовищах, так і на звичайних персональних комп’ютерах. До них належать, Acronis True Image, Macrium Reflect, EaseUS Todo Backup, Redo Rescue, Timeshift (для Linux) і стандартні інструменти

операційної системи Windows. Усі ці програми мають спільне завдання — створити копію даних або всього системного диска для подальшого швидкого відновлення після збоїв.

У середовищі ОС Windows резервне копіювання реалізується за допомогою вбудованих засобів. Для цього можна скористатися функцією «*Резервне копіювання та відновлення*» або «*Історією файлів*». У першому випадку користувач створює повну копію системи, включно з налаштуваннями, драйверами та файлами, яка зберігається на іншому диску чи зовнішньому носії. Це так званий системний образ, що дозволяє повністю відновити комп'ютер у разі пошкодження операційної системи. У другому варіанті, копіюються лише користувацькі документи, зображення та робочі матеріали, які можуть бути відновлені окремо без впливу на саму систему.

Процес резервного копіювання у Windows зазвичай виконується через майстер, де користувач послідовно вибирає носій, тип даних і графік створення копій. Після налаштування система автоматично зберігає нові версії файлів або системних знімків за розкладом. У разі збою або втрати даних користувач може запустити майстер відновлення та вибрати, яку саме копію відновити. У промислових і офісних умовах Windows Backup часто використовується разом із хмарними сервісами, такими як OneDrive чи Google Drive, що дозволяє зберігати копії поза основним робочим комп'ютером і забезпечує додатковий рівень безпеки.

Таким чином, використання резервного копіювання дає змогу: створити точну копію системи або важливих файлів, яка зберігається на надійному носії та швидко повернути роботу комп'ютера або енергетичної інформаційної системи до нормального стану після будь-якого технічного збою.

Програма роботи

1. Ознайомитися з технологіями захисту даних за допомогою резервного копіювання з теоретичних відомостей.
2. Виконати резервне копіювання диска та відновити дані з резервної копії.

Порядок виконання роботи

1. Аналіз об’єкта резервного копіювання.

1.1. Визначити, яку інформаційну систему імітує віртуальна машина (наприклад: SCADA-сервер, робоча станція оператора, сервер обробки даних).

1.2. Визначити склад даних, що підлягають резервному копіюванню: операційна система; налаштування системи; прикладні програми; користувацькі дані.

1.3. Обґрунтувати важливість резервного копіювання для обраного типу енергетичної системи.

1.4. Виконати копіювання програми Clonezilla Live та GParted на локальний ПК відповідно з *https://clonezilla.org/downloads.php* та *https://gparted.org/download.php,* при цьому потрібно скопіювати образ у форматі *iso* з необхідними параметрами операційної системи та зберегти їх у папці, наприклад D:\Backup_Lab.

2. Створення у віртуальній машині OracleVM VirtualBox нового резервного жорсткого диску.

2.1. Для створення нового жорсткого диску у *OracleVM VirtualBox Manager* необхідно вибрати пункт: *Налаштування > Пам’ять > Контролер: SATA > Жорсткий диск* та натиснувши кнопку  (Add attachment), яка додає жорсткий диск. Часто кнопка знаходиться внизу вікна, або праворуч від меню *«Контролер: SATA».* Після виконання цих дій у списку жорстких дисків має з’явитися новий диск зі вказаною вами назвою, наприклад *BackupDisk*.

2.2. Виконуємо під’єднання до віртуальної машини OracleVM VirtualBox ISO-образ GParted (завантажений раніше), після приєднання перезапускаємо віртуальну машину та завантажуємося з нього. Додавання віртуального диску відбувається подібно до того, як ми додавали віртуальний диск для установки ОС Debian на попередніх лабораторних роботах, натиснувши відповідну кнопку  , (праворуч від меню *«Контролер: IDE»)* яка *додає привод оптичного диску*.

2.3. Перезапускаємо віртуальну машину OracleVM VirtualBox, при цьому має завантажитися програма GParted.

2.4. У процесі запуску GParted, вибираємо мову та виконуємо

вказівки системи.

2.6. Після завантаження GParted у списку доступних жорстких дисків (у правому верхньому куті менеджера GParted вибираємо порожній жорсткий диск (як правило цей диск буде відображатися, як «не розподілено»). Виконуємо форматування цього нового жорсткого диску у файловій системі *ext4*. Для цього вибираємо меню: *Пристрій* > *Створити таблицю розділів…* > *msdos* > *apply* (див. рис. 1).

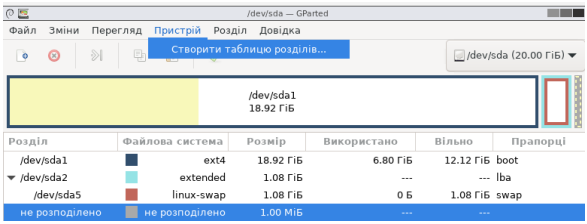


Рис. 1. Таблиця розділів диску

Зауваження. Під час створення розділу (резервний диск) необхідно задати йому *мітку розділу*, у відповідному вікні, за допомогою якої його можна буде відрізнити при створенні резервної копії (якщо цю опцію не виконати, то відрізнити новий диск від існуючого буде складно). Після цього створюємо новий розділ (клацнувши по диску правою клавішею) і застосовуємо зміни.

3. Створення резервної копії.

3.1. Перезавантажити віртуальну машину та завантажитись з *Live CD Clonezilla*. Для цього у меню віртуальної машини у пункті: *Налаштування* > *Пам'ять* > *Контролер:IDE* > *Оптичний привід* вказати шлях до завантаженого *iso*-образу *Clonezilla* (див. п. 1).

3.2. Запускаємо віртуальну машину і обираємо подальші налаштування *Live CD Clonezilla* за замовчуванням. Після виконання аналізу дискового простору ми отримаємо два диска, один з яких має встановлену операційну систему, а інший резервний. Обираємо другий диск на який буде виконуватися резервне копіювання.

3.3. Виконуємо резервне копіювання одного жорсткого диска

в образ диска на іншому, використовуючи вказівки Clonezilla. Для кращого розуміння інтерфейсу при встановленні вибираємо українську або російську мову. Після запуску вибираємо роботу з дисками або розділами використовуючи образи, так як показано на рис. 2.

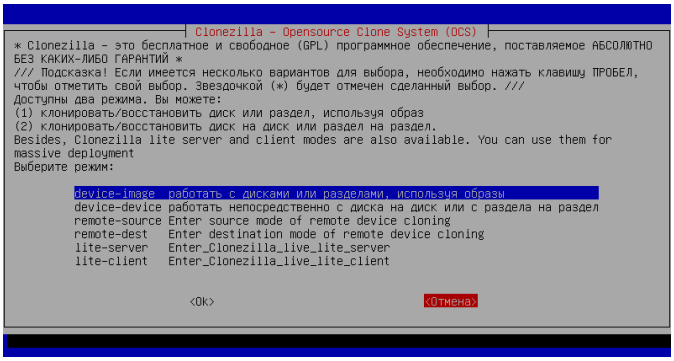


Рис. 2. Вибір у програмі *Clonezilla* режим роботи з дисками або розділами використовуючи образи

3.4. Вибираємо команду *rerun1* (рис. 3). Для вибору диску на який буде встановлена резервна копія необхідно зі запропонованого списку вибрати створений попередньо резервний диск.

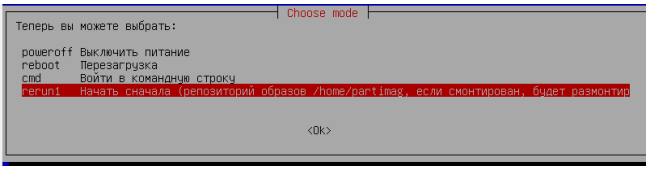


Рис. 3. Вибір команди *rerun1*

Зауваження. Щоб розрізняти новостворений розділ (резервний диск) необхідно задати йому мітку розділу, якщо цього не було зроблено раніше за допомогою програми GParted (п. 2). Для цього, перезапускаємо віртуальну машину і використовуючи програму GParted додаємо мітку розділу у новостворюваному диску. Також розрізнити ці диски (зі встановленою ОС Debian та новостворений резервний диск)

можна порівнявши їх розміри, попередньо визначивши розмір диску зі встановленою ОС.

3.5. Продовжуємо процес у Clonezilla з попереднього пункту. По завершенні створення резервної копії програма Clonezilla запропонує перевантажитися.

4. Імітація збою системи. Заванатажуємо (перезавантажуємо) віртуальну машину з ОС Debian. Після завантаження, виконуємо команду, що пошкоджує завантажувальний сектор (імітація збою): *sudo dd if=/dev/zero of=/dev/sda bs=1k count=1k* (якщо виконано вхід під користувачем *root*, то виконуємо команду без *sudo*).

Застереження. Команда *dd* знищує завантажувальний сектор і її не слід виконувати на реальних носіях, щоб уникнути втрати даних.

5. Переконатись в неможливості завантаження ОС Debian з даного жорсткого диска, перезапустивши ОС. Завантаження не повинно відбуватися у зв'язку з тим, що ми пошкодили завантажувальну область, при цьому повинно з'явитися повідомлення про фатальну помилку.

6. Відновлення операційної системи. Відновити встановлену ОС Debian з раніше створеної резервної копії за допомогою програми *Clonezilla*, повторно заватаживши з *Live CD Clonezilla* та обравши при розгортанні образу диска в якості цільового диска той, на якому був знищений завантажувальний запис. Переконатись в нормальному завантаженні відновленої ОС.

Для виконання цього процесу запускаємо знову Clonezilla так як в п. 3, проводимо ті ж самі налаштування, проте в кінці обираємо опцію *restoredisk*. Потрібно вказати *відновити образ з диску* вказавши шлях до папки в якій зберігається резервна копія та вибрати режим відновлення, як показано на рис. 4, при цьому має запуститися процес відновлення.

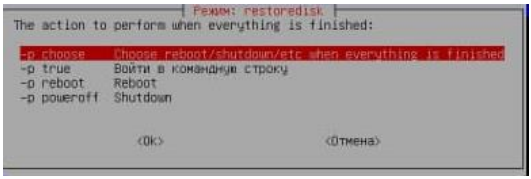


Рис. 4. Вибір режиму відновлення

7. Очікуємо результат копіювання резервної копії Після відновлення перезапускаємо віртуальну машину і переконуємося, що ОС Debian знову запускається у нормальному режимі.

8. Аналіз результатів резервного копіювання та відновлення.

8.1. Оцінити результати відновлення системи: коректність завантаження ОС; доступність даних; збереження налаштувань.

8.2. Визначити: час відновлення системи та повноту відновлення даних.

8.3. Зробити висновок щодо: ефективності використаного методу резервного копіювання та можливості його застосування в електроенергетичних системах.

9. Результати виконання оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму та порядок виконання роботи;
- опис обраного об’єкта резервного копіювання (тип системи та склад даних);
- скріншоти та короткий опис підготовки резервного носія (GParted);
- скріншоти та опис процесу створення резервної копії (Clonezilla);
- скріншоти та опис процесу імітації збою системи;
- скріншоти та опис процесу відновлення системи;
- аналіз результатів резервного копіювання та відновлення (час, повнота, коректність);
- висновок..

Контрольні запитання

1. Що таке резервне копіювання та яке його призначення в енергетичних системах?

2. Які дані є критичними для резервного копіювання в SCADA-системах?

3. Які існують типи резервного копіювання та в чому їх відмінність?

4. Що таке образ диска і де його доцільно зберігати?
5. У чому полягає різниця між інкрементним та диференціальним копіюванням?
6. Для чого використовуються LiveCD / LiveUSB при відновленні системи?
7. Яке призначення програм Clonezilla та GParted?
8. Які наслідки може мати відсутність резервного копіювання в енергетичних системах?
9. Які параметри характеризують ефективність відновлення системи (час, повнота)?
10. У чому полягають особливості організації резервного копіювання в електроенергетиці?

Лабораторна робота 8
Використання протоколів FTP, TFTP, Telnet, SSH у мережах інформаційних систем електроенергетики

Мета роботи

Ознайомитися з використанням протоколів FTP, TFTP, Telnet та SSH та набути практичних навичок їх застосування для передачі даних і віддаленого адміністрування обладнання в інформаційних системах електроенергетики.

Теоретичні відомості

Протокол передавання файлів *FTP* (File Transfer Protocol) — це протокол, який використовується для передавання файлів через Інтернет. Протокол FTP зазвичай застосовується для того, щоб зробити файли доступними для завантаження. З його допомогою можна завантажувати web-сторінки в процесі створення чи модернізації web-сайту, виконувати обмін зображеннями та ін.

Протокол передачі файлів *TFTP* (Trivial File Transfer Protocol) в основному використовується для первинного завантаження бездискових робочих станцій. На відміну від FTP протокол TFTP не містить можливостей аутентифікації (хоча можлива фільтрація за IP-адресою). Цей протокол заснований на транспортному протоколі UDP.

Telnet (англ. TErminaL NETwork) — мережевий протокол для реалізації текстового інтерфейсу через мережу. Часто вживається у вигляді програми-клієнта, тому Telnet — це програма з текстовим інтерфейсом, яка дає змогу підключитись до іншого комп'ютера через Інтернет за цим протоколом. Якщо власник або адміністратор надає право підключитися до ПК, то програма Telnet дає змогу вводити команди для доступу до програм і служб на віддаленому комп'ютері, ніби так, як би ви працювали безпосередньо за ним. Програму Telnet можна використовувати для доступу до електронної пошти, баз даних і файлів. Як правило, завдяки простоті програмної реалізації Telnet часто використовується для доступу до вбудовуваних систем, або мережевого обладнання.

Оскільки у протоколі Telnet не передбачено використання ні шифрування, ні перевірки достовірності даних, то він вразливий

для будь якого виду атак, до яких вразливий протокол TCP. Тому для доступу до UNIX-подібних операційних систем використовується інший протокол - SSH.

SSH-протокол (від англ. Secure Shell) - криптографічний мережевий протокол прикладного рівня, який забезпечує захищений віддалений доступ до комп'ютерів і серверів через незахищену мережу. SSH схожий за функціональністю з протоколом Telnet і rlogin, проте шифрує весь потік даних, в тому числі, передані паролі.

Криптографічний захист протоколу SSH не фіксований, він надає вибір різних алгоритмів шифрування. Крім того, цей протокол дозволяє не тільки використовувати безпечний віддалений *shell* (командний інтерпретатор, який використовується в Unix сумісних операційних системах) на ПК, тобто виконувати команди, які подає користувач, або які читаються з файлів, але і тунелювати графічний інтерфейс — X Tunnelling (тільки для Unix-подібних ОС або програм, що використовують графічний інтерфейс X Window System). SSH здатний передавати через безпечний канал будь-який інший мережевий протокол (Port Forwarding), забезпечуючи можливість безпечної передачі не тільки X-інтерфейсу, але і, наприклад, звуку та відео.

Для роботи за протоколом SSH потрібно використовувати SSH-сервер і SSH-клієнт. SSH-сервер перевіряє наявність з'єднання від клієнтських ПК і при встановленні зв'язку виконує аутентифікацію, після чого починає обслуговування клієнта. SSH-клієнт використовується для входу на віддалений ПК і виконання команд. Для з'єднання SSH-сервер і SSH-клієнт повинні створити пари відкритих і закритих ключів та обмінятися ними, при цьому також використовується пароль.

У сучасних інформаційних та автоматизованих системах електроенергетики протоколи передачі даних і віддаленого доступу відіграють важливу роль у забезпеченні обміну інформацією між серверами, робочими станціями та мережевим обладнанням. Їх використання визначається вимогами до надійності, безпеки та сумісності з промисловими стандартами.

Протоколи FTP та SFTP застосовуються для передачі файлів між серверами та клієнтськими системами. У практиці

експлуатації енергетичних підприємств вони використовуються для передавання звітів, журналів подій, а також архівів даних SCADA-систем. Зокрема, FTP може застосовуватись у внутрішніх мережах для передачі великих обсягів даних між серверами, тоді як SFTP (на базі SSH) використовується у випадках, коли необхідно забезпечити захищену передачу інформації. Такий підхід відповідає сучасним вимогам інформаційної безпеки, визначеним у галузевих стандартах.

Протокол TFTP широко застосовується у мережевому обладнанні, зокрема для завантаження конфігураційних файлів та оновлення прошивок комутаторів, маршрутизаторів і вбудованих пристроїв. Його використання обумовлене простотою реалізації та мінімальними вимогами до ресурсів пристрою. У промислових мережах, у тому числі на енергетичних об'єктах, TFTP використовується для початкового налаштування обладнання або резервного копіювання конфігурацій. Водночас через відсутність механізмів автентифікації та шифрування його застосування обмежується внутрішніми, ізольованими сегментами мережі.

Протокол Telnet історично використовувався для віддаленого доступу до мережевих пристроїв та серверів, зокрема для їх конфігурації. Однак через відсутність шифрування даних і передачу облікових даних у відкритому вигляді він є небезпечним і не відповідає сучасним вимогам кібербезпеки. У сучасних енергетичних системах його використання обмежується, його поступово витісняють більш захищені протоколи.

Протокол SSH (Secure Shell) є сучасним стандартом для віддаленого адміністрування серверів і мережевого обладнання в електроенергетиці. Він забезпечує захищений канал зв'язку з використанням криптографічних методів шифрування та підтримує механізми автентифікації користувачів (паролі, ключі). SSH використовується для конфігурації мережевих пристроїв, адміністрування серверів SCADA, виконання команд на віддалених вузлах, а також для організації захищеної передачі даних (зокрема через SFTP та SCP). Його широке застосування відповідає рекомендаціям міжнародних стандартів у сфері інформаційної безпеки та експлуатації критичної інфраструктури.

Таким чином, у сучасних електроенергетичних системах

використовується комбінований підхід до застосування протоколів: FTP і TFTP застосовуються для передачі даних і конфігурацій у контрольованих мережах, тоді як SSH (і похідні від нього протоколи, такі як SFTP) використовується як основний засіб безпечного віддаленого доступу. Протокол Telnet використовується у обмежених випадках, або замінюється на більш сучасні.

Програма роботи

1. Ознайомитися з принципами роботи та особливостями застосування протоколів FTP, TFTP, Telnet та SSH у мережах електроенергетичних систем.

2. Виконати встановлення та базове налаштування серверів FTP, TFTP, Telnet та SSH.

3. Перевірити роботу протоколів шляхом передачі даних і встановлення віддаленого доступу між вузлами мережі.

4. Провести аналіз і зробити висновки щодо ефективності та безпеки використання протоколів у інформаційних системах електроенергетики.

Порядок виконання роботи

1. Виконати запуск віртуальної машину Oracle VM VirtualBox.

Зауваження. Переконайтеся, що при підключенні віртуальної машини встановлений тип підключення мережевого адаптера: *проміжний адаптер/мережевий міст*.

1.1. Запустити ОС з логіном та паролем вказаними при встановленні ОС Debian.

1.2. Запустити Термінал, після цього виконуємо всі необхідні процедури та команди.

1.3. Підготувати систему до виконання лабораторної роботи. Видалити службу *Dnsmasq* для уникнення конфлікту мережевих служб командою *sudo apt-get purge dnsmasq*. Перевірити виконання команди: має висвітлитися повідомлення про те, що команда виконана.

1.4. Виконати команду *sudo ip a* та занотувати IP-адресу віртуальної машини після виводу даних команди.

2. Виконати встановлення сервера *vsftpd* (Very Secure FTP Daemon)та FTP-клієнта.

2.1. Виконуємо команду *sudo apt-get install vsftpd* та команду *apt install ftp*.

Зауваження. Для виконання редагування *vsftpd*, подібно, як у попередній лабораторній роботі використовуємо файловий менеджер *MC* запуск якого здійснюється командою *sudo mc* (відповідно без *sudo*, якщо ви працюєте під користувачем *root*). Навігація по об'єктах у каталозі здійснюється клавішами керування курсором, перехід у батьківський каталог (на рівень вище) – вибором *.. (дві крапки)*, перегляд текстового файлу – натисканням *F3*, редагування – *F4* (рис. 1).

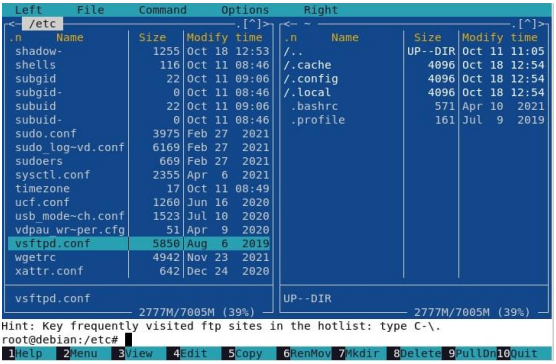


Рис. 1. Вигляд вмісту папки */etc/* з виділеним файлом *vsftpd.conf* у файловому менеджері *MC*

Для редагування файлу *vsftpd.conf* використовуємо текстовий редактор *Nano* (див. попередні лабораторні роботи) (рис. 2).

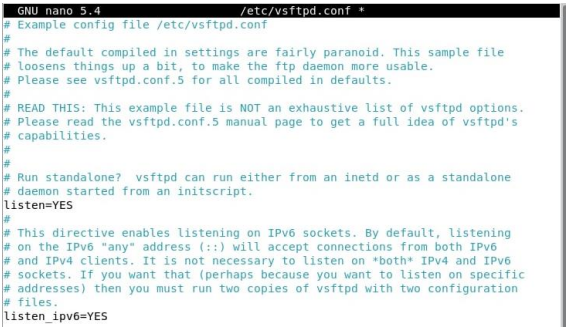


Рис. 2. Вміст файлу *vsftpd.conf* при редагуванні редактором *Nano*

2.2. Після внесення змін у файлі *vsftpd.conf* натискаємо на комбінацію *Ctrl+O→Enter* та перезапускаємо FTP-сервер командою *sudo service vsftpd restart* (відповідно без *sudo*, якщо ви працюєте під користувачем *root*). Після виконання вказаних команд система має виконати встановлення.

3. Виконання входу на сервер FTP.

3.1. Перевіряємо можливість логіну (входу) на сервер командою *ftp localhost*, ввівши логін та пароль користувача.

3.2. Перевірити можливість передачі файлів та доступу до сервера. При успішному підключенні буде виведено запрошення вводу команд: *ftp*> (рис. 3).

Зауваження. У випадку, якщо логін і пароль *ftp*-користувача співпадає з логіном і паролем локального користувача (ОС Debian) вхід буде виконано без запиту пароля, у іншому випадку необхідно буде ввести логін і пароль, який, як правило, відповідає локальному (той самий що при вході в Debian).

```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Рис. 3. Вигляд виконання команди при вході на *ftp*-сервер

4. Перевірка роботи служби FTP (у цьому пункті виконання команд відбувається у ОС Windows).

4.1. Під'єднатись з хост-системи до віртуальної машини як до віддаленого хосту за допомогою FTP-клієнта (використавши IP-адресу гостьової системи) та створити у будь-якій папці новий текстовий файл на сервері.

Зауваження. Для під'єднання використовуємо вбудований FTP-клієнт ОС Windows. Для цього у вікні *Провідника* потрібно перейти в меню «*Комп'ютер*», а потім обрати ярлик: «*Підключити мережевий диск > Підключитися до веб-сайту, де можна зберігати документи та зображень»*. Якщо використовується ОС Windows 11, то послідовність дій буде подібною, лише потрібно ПКМ клацнути на: *Цей ПК > Підключити мережевий диск.* При цьому, використати IP-адресу отриману у п. 1.4, та виконати всю послідовність дій по підключенню (рис. 4).

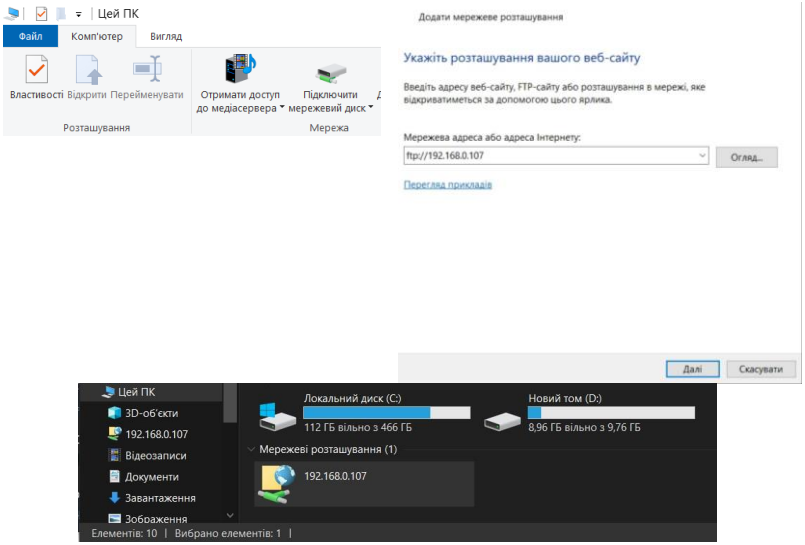


Рис. 4. Процес підключення хост-системи до віртуальної машини

4.2. Повернутися до Терміналу ОС Debian та вивести вміст зміненої теки командою: *ls -la ~*. При цьому, отримаємо результат, який подібний до того, що показано на рис. 5 та зберігаємо його у звіт.

```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la ~
output to local-file: /root?
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
local: /root: Is a directory
226 Directory send OK.
225 No transfer to ABOR.
ftp>
```

Рис. 5. Опис вмісту зміненої теки

5. Використання TFTP-протоколу.

5.1. Встановити TFTP-сервер TFTPD-HPA командою *sudo apt-get install tftpd-hpa*.

5.2. Змінити налаштування сервера у файлі */etc/default/tftpd-hpa*, вказавши в якості шляху до кореневого каталога файлової системи для клієнтів каталог */srv/tftp* (може бути вказаний за

замовченням) (рис. 6).

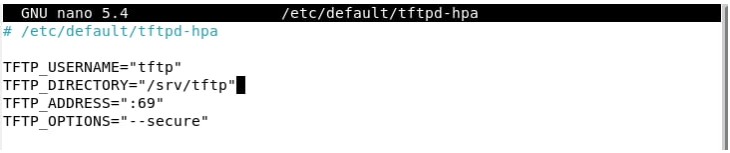


Рис. 6. Параметри налаштування сервера у файлі */etc/default/tftpd-hpa*

5.3. Скопіювати в каталог */srv/tftp* файл *timezone*. Це можна зробити використовуючи програму *MC*, тобто відкрити обидва каталоги у різних вікнах програми *MC* та виконати копіювання так, як показано на рис. 7.

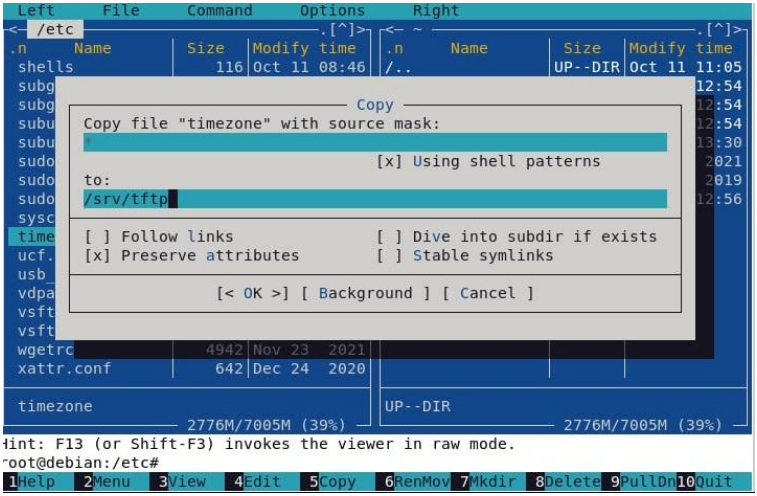


Рис. 7. Процес копіювання файлу *timezone* в *к*аталог */srv/tftp*

5.4. Перезапустити TFTP-сервер використовуючи команду service *tftpd-hpa restart*.

5.5. Під'єднатись до TFTP-сервера з ОС Debian за допомогою програми TFTPD32, яку можна завантажити з сайту *https://bitbucket.org/phjounin/tftpd64/downloads/* та скопіювати файл *timezone* на хост-систему так, як показано на рис. 8. Передача виконується між віртуальною машиною та хост-

системою.

Зауваження. Файл з вказаного сервера скопіюється на локальний комп'ютер у вказаний каталог. Так ми встановили TFTP-сервер та перевірили можливість підключення до нього та виконали передачу даних.

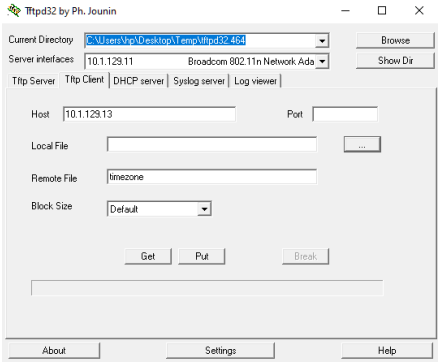


Рис. 8. Копіювання файлу *timezone* на хост-систему

6. Використання Telnet-протоколу.

6.1. Встановити *Telnet*-сервер виконавши команду: *sudo apt-get install telnetd*.

6.2. Під'єднатись до гостьової системи за протоколом *Telnet* за допомогою програми *PuTTY* (*putty.exe (the SSH and Telnet client itself)*), яку можна запустити з сайту *https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html*.

6.3. У вікні *PuTTY* виконати команду, наприклад *uname -a*. Зберегти результати та після виконання всіх дій відключитись від *Telnet*-сервера.

6.4. Оцінити ризики використання *Telnet* через відсутність шифрування переданих даних.

7. Використання SSH-протоколу.

7.1. Підключитись до гостьової системи за допомогою SSH. Це можна зробити використовуючи ту ж саму програму *PuTTY* вказавши відповідний тип SSH (рис. 9).

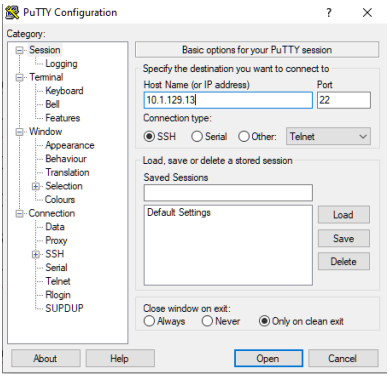


Рис. 9. Робота програми PuTTY в режимі SSH

7.2. Отримати ключ для підключення до сервера з повідомлення (рис. 10). Застосування ключа дасть змогу перевірити, що підключення здійснюється справді до потрібного вузла, а не вузла зловмисника з іншим ключем.

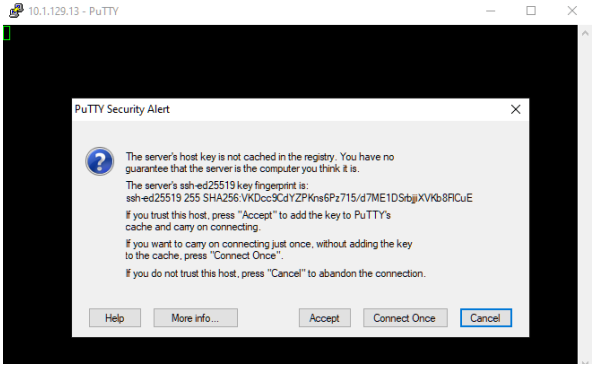


Рис. 10. Відображення ключа з програми PuTTY в режимі SSH

Зауваження. Якщо для входу буде використовуватися логін *root*, то потрібно дозволити його вхід з паролем змінивши у файлі */etc/sshd/sshd_config* рядок з налаштуванням *PermitRootLogin* на значення *yes* видаливши встановлений за замовчуванням параметр. Після цього перезавантажити SSH-сервер командою *service sshd restart*.

7.3. Видалити встановлені TFTP- та Telnet-сервери командою

sudo apt-get purge tftpd-hpa telnetd.

7.4. Порівняти використання SSH та Telnet з точки зору безпеки віддаленого доступу.

7.5. Результати виконання команди з використанням протоколу SSH скопіюйте в звіт. Після завершення вказаних дій виконайте команду *sudo poweroff*.

8. Виконати аналіз використання протоколів.

8.1. Порівняти використання: FTP та TFTP; Telnet та SSH.

8.2. Визначити, які протоколи є безпечними, а які мають обмеження використання.

8.3. Зробити висновок щодо доцільності використання протоколів FTP, TFTP, Telnet та SSH у мережах електроенергетичних систем з урахуванням вимог до безпеки.

9. Результати виконання оформити у вигляді звіту відповідно до встановлених вимог на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму роботи;
- результати виконання кожного етапу роботи (відповідно до пунктів порядку виконання);
- скріншоти встановлення та налаштування FTP, TFTP, Telnet та SSH;
- скріншоти перевірки роботи протоколів (передача файлів, віддалене підключення);
- результати виконання команд у терміналі;
- порівняльний аналіз протоколів FTP і TFTP, Telnet і SSH;
- оцінку безпеки використання протоколів;
- висновок щодо доцільності використання протоколів у мережах електроенергетичних систем.

Контрольні запитання

1. Яке призначення та принцип роботи протоколу FTP?
2. У чому полягають основні відмінності між FTP та TFTP?
3. Які особливості використання протоколу TFTP у мережевому обладнанні?

4. Яке призначення протоколу Telnet та в чому його основні недоліки?

5. Які переваги протоколу SSH порівняно з Telnet?

6. Які механізми безпеки реалізовані в протоколі SSH?

7. У яких випадках доцільно використовувати FTP або SFTP у мережах електроенергетики?

8. Для яких задач у електроенергетичних системах застосовується TFTP?

9. Чому Telnet не рекомендується використовувати у сучасних інформаційних системах?

10. Які протоколи є доцільними для використання у критичних системах електроенергетики та чому?

Лабораторна робота 9
Захист web-інтерфейсів інформаційних систем електроенергетики

Мета роботи

Навчитись розгортати web-сервери та реалізовувати базові механізми захисту web-інтерфейсів у інформаційних системах електроенергетики.

Теоретичні відомості

Сучасні енергетичні підприємства активно інтегрують web-технології у свої системи автоматизації, диспетчерського керування та обліку енергії. Web-компоненти є важливою частиною архітектури SCADA (Supervisory Control and Data Acquisition) і Smart Grid-систем, забезпечуючи доступ користувачів до оперативної інформації через звичайний веб-браузер.

У сучасних електроенергетичних системах web-сервери використовуються як засіб надання доступу до інформації та інтерфейсів керування на верхніх рівнях автоматизації. Вони застосовуються у складі SCADA-систем, систем комерційного обліку електроенергії (АСКОЕ), а також інших інформаційних підсистем для візуалізації даних, формування звітів та забезпечення віддаленого доступу користувачів через web-інтерфейс.

Важливо розрізняти функціональне призначення web-серверів у енергетичних системах: вони не використовуються для прямого керування польовими пристроями, такими як програмовані логічні контролери (ПЛК), пристрої релейного захисту та автоматики (РЗА) або RTU. Web-сервери працюють на рівні HMI/SCADA та забезпечують доступ до вже оброблених даних, що надходять із нижчих рівнів системи автоматизації.

Згідно з сучасними практиками побудови захищених мереж, зокрема вимогами стандарту IEC 62443 (Industrial Communication Networks – Network and System Security — «Промислові комунікаційні мережі. Безпека мереж і систем»), web-сервери повинні розміщуватись у демілітаризованій зоні (DMZ). Демілітаризована зона (DMZ) — це окремий сегмент мережі,

який розташовується між корпоративною (IT) мережею та технологічною (OT) мережею і призначений для розміщення сервісів, доступних зовнішнім користувачам. Такий підхід забезпечує ізоляцію критичних систем і дозволяє обмежити прямий доступ до них.

Ключовою вимогою безпеки є відсутність прямого мережевого доступу web-серверів до польових пристроїв. Взаємодія з ПЛК, RTU та іншими елементами нижнього рівня повинна здійснюватися виключно через SCADA-сервери або спеціалізовані шлюзи з контролем доступу. Це дозволяє мінімізувати ризики несанкціонованого впливу на технологічний процес.

Таким чином, web-сервер у енергосистемі виконує роль інтерфейсного та інформаційного рівня, забезпечуючи зручний доступ до даних, але не беручи участі у безпосередньому керуванні обладнанням. Його правильне розміщення та ізоляція є критично важливими умовами забезпечення кібербезпеки енергетичних об'єктів.

Розглянемо детальніше поняття web-сервер (англ. Web Server). Web-сервер — це сервер, що приймає HTTP-запити від клієнтів, зазвичай веб-браузерів, видає їм HTTP-відповіді, зазвичай разом з HTML-сторінкою, зображенням, файлом, медіа-потоком або іншими даними. Також web-сервером називають програмне забезпечення, що виконує функції web-сервера, так і комп'ютер, на якому це програмне забезпечення працює. У даній лабораторній роботі під терміном web-сервер ми розумітимемо саме програмне забезпечення. Серед найбільш поширеного програмного забезпечення, яке виконує функції web-сервера є Apache HTTP-сервер.

Apache HTTP-сервер — це відкритий web-сервер для UNIX-подібних, Microsoft Windows, Novell NetWare та інших операційних систем, який розробляється та підтримується спільнотою розробників відкритого програмного забезпечення під керівництвом Apache Software Foundation. Якщо користувач в рядку адреси браузера не вказав шлях до файлу, а лише адресу сайту, за замовчуванням web-сервер надсилає у відповідь файл *index.html*, *index.php* або інший, вказаний у налаштуваннях сервера. Каталог у файловій системі, у якому розміщений цей

файл та інші файли і каталоги сайту, повинен бути визначений, як кореневий каталог web-сервера. Браузер користувача не може отримати доступ до файлів, які знаходяться за межами кореневого каталогу сервера (якщо у кореневому каталозі або у підкаталогах немає посилань за його межі).

Для динамічного створення HTML-сторінок у відповідь на запити користувача часто використовується мова PHP – інтерпретована мова програмування, код якої можна вбудовувати безпосередньо в *html-код* web-сторінок. Код PHP в HTML повинен знаходитись між початковим тегом *<?php* та кінцевим *?>* (або між *<script language="php">* та *</script>*). Дані, необхідні для генерування web-сторінки-відповіді користувачеві, як правило, зберігаються в базах даних (БД). Однією з найпоширеніших систем управління базами даних (СУБД) є MySQL. *MySQL-сервер* виконує обробку SQL-запитів від інших програм, оновлення і керування реляційними БД, створення схеми бази даних і її модифікації, системи контролю за доступом до бази даних.

Система керування вмістом (англ. Content Management System, CMS) — це програмне забезпечення для організації web-сайтів чи інших інформаційних ресурсів в Інтернеті чи в окремих комп'ютерних мережах. Основні функції CMS: надання інструментів для створення вмісту web-сторінок, організація спільної роботи над вмістом, зберігання, контроль версій, дотримання режиму доступу, управління потоком документів, публікація вмісту, представлення інформації у вигляді, зручному для навігації, пошуку.

Велика частина сучасних систем управління вмістом реалізується у вигляді візуального *WYSIWYG редактора* – програми, яка створює html-код зі спеціальної спрощеної розмітки, що дозволяє користувачеві простіше додавати, редагувати й керувати вмістом сайту. Сайти, що використовують CMS, потребують для своєї роботи власне web-сервер, сховище даних (як правило, СУБД) і додаток, який власне реалізовує CMS (написаний на PHP, Perl або інших мовах програмування).

Однією з популярних CMS є *WordPress* — це проста у встановленні та використанні система керування вмістом з відкритим кодом. Сфера її застосування від блогів до складних

web-сайтів. Вбудована система тем і плагінів в поєднанні з вдалою архітектурою дозволяє конструювати на основі WordPress практично будь-які web-проекти. Написана на мові програмування PHP з використанням бази даних MySQL. Оскільки WordPress є широковживаною системою, вона також є об'єктом кібератак. Тому при її використанні дуже важливо здійснювати захист web-сайтів.

Безпекові аспекти використання web-інтерфейсів у енергетиці. Веб-інтерфейси SCADA- та Smart Grid-систем, попри зручність і доступність, є потенційною точкою проникнення до промислової мережі. Через помилки конфігурації, уразливі web-додатки або відсутність шифрування зловмисники можуть отримати доступ до критичних систем управління. Тому захист веб-інтерфейсів є критично важливим елементом кібербезпеки енергетичних підприємств. Для захисту web-ресурсів енергетичних компаній необхідно впроваджувати такі заходи:

– використання HTTPS для шифрування трафіку;

– впровадження багаторівневої автентифікації (2FA, сертифікати доступу);

– сегментація мережі, щоб веб-сервери були ізольовані від контролерів нижнього рівня;

– регулярне оновлення ПЗ та перевірка на уразливості;

– дотримання вимог стандартів IEC 62443 і ISO/IEC 27001.

Wordfence є засобом захисту web-додатків на базі WordPress, який поєднує функції firewall, сканування на шкідливий код та захисту доступу. Він дозволяє виявляти віруси, шкідливі скрипти, змінені файли сайту, а також забезпечує двофакторну автентифікацію, захист від brute-force атак, блокування підозрілих IP-адрес і моніторинг активності користувачів. Це дозволяє контролювати цілісність web-ресурсу та запобігати несанкціонованому доступу до адміністративної частини сайту.

У контексті електроенергетичних систем такі засоби доцільно використовувати для захисту web-ресурсів верхнього рівня, зокрема корпоративних сайтів, кабінетів споживачів, систем звітності або web-інтерфейсів SCADA та АСКОЕ, що надають доступ до даних, але не здійснюють безпосереднього керування обладнанням. Використання Wordfence дозволяє виявляти

несанкціоновані зміни, контролювати доступ адміністраторів та знижувати ризики компрометації інформаційних ресурсів.

Водночас Wordfence слід розглядати як допоміжний інструмент захисту web-рівня. У реальних енергосистемах такі сервіси повинні бути ізольовані від технологічної мережі (наприклад, розміщені в DMZ), а взаємодія з критичними компонентами (ПЛК, RTU, РЗА) має здійснюватися лише через SCADA-сервери або захищені шлюзи. Таким чином, застосування Wordfence підвищує безпеку web-компонентів, але не замінює комплексних заходів кіберзахисту енергетичних систем.

Програма роботи

1. Ознайомитися з принципами побудови web-інтерфейсів та їх роллю в інформаційних системах електроенергетики.
2. Виконати розгортання web-сервера, бази даних та CMS WordPress як прикладу web-інтерфейсу.
3. Налаштувати роботу web-додатку та перевірити його доступність у мережі.
4. Реалізувати базові механізми захисту web-ресурсу з використанням плагіну Wordfence.
5. Проаналізувати виявлення несанкціонованих змін та оцінити рівень захищеності web-інтерфейсу.

Порядок виконання роботи

1. Виконати підготовку середовища.

1.1. Запустити віртуальну машину Oracle VM VirtualBox, задавши тип підключення до мережі — *проміжний адаптер/мережевий міст*.

1.2. Оновити індекс доступного в репозиторії програмного забезпечення командою *sudo apt-get update*. Встановити наявні оновлення командою *sudo apt-get upgrade.*

1.3. Визначити IP-адресу віртуальної машини (ip a) та зафіксувати її у звіті.

2. Виконати встановлення програмного забезпечення.

2.1. Встановити найновіші компоненти, необхідні для роботи CMS Wordpress: web-сервер Apache, систему керування базами даних MySQL, інтерпретатор мови PHP, а також phpMyAdmin та

MySQL-клієнт для адміністрування, командою *sudo apt-get install apache2 php7.4 php7.4-mysql mariadb-server mariadb-client.*

Зауваження. У цьому пункті вказано команди для інсталяції *php8.2 php8.2-mysql* з версією 8.2 (https://packages.debian.org/bookworm/php). Але якщо під час інсталяція ОС Debian виявиться, що версія вказаних програмних продуктів застаріла, або не існує, то потрібно визначити найновіші на момент встановлення версії та виконати їх встановлення.

2.2. Перевірити працездатність web-сервера, відкривши у браузері IP-адресу сервера.

3. Виконати завантаження та підготовку CMS.

3.1. Завантажити CMS Wordpress командою *wget https://uk.wordpress.org/latest-uk.tar.gz.*

3.2. Розпакувати архів з CMS Wordpress командою *tar -xzvf latest-uk.tar.gz.*

4. Виконати налаштування бази даних.

4.1. Створити базу даних та користувача. За допомогою MySQL-клієнта під'єднатись до СУБД командою *mysql -u root -p* та виконати команди створення бази даних з ім'ям *wordpressdb* і надання користувачеві *wordpressuser* з паролем *passwordforwp* всіх прав при роботі з усіма таблицями цієї БД. Виконати вихід з MySQL-клієнта командою *exit*.

5. Виконати налаштування конфігурації WordPress.

5.1. Відредагувати та зберегти файл *wp-config.php*. Для цього відкрити зразок файлу конфігурації командою *nano ./wordpress/wp-config-sample.php* та вказати дані, потрібні для доступу до бази даних. Замість фрагментів тексту *database_name_here, username_here, password_here* вписати вказані раніше ім'я бази даних логін та пароль так, як показано на рис 1.

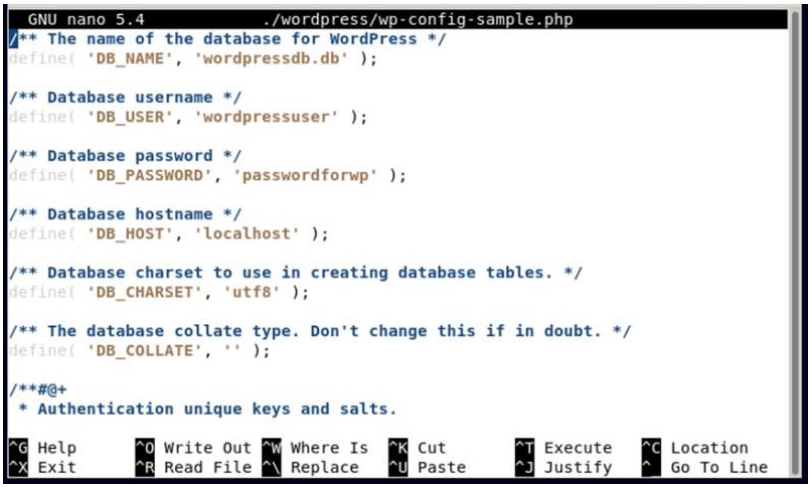


Рис. 1. Внесення змін у файл *wp-config-sample.php*

5.2. Зберегти змінений файл з ім'ям *wp-config.php* (Ctrl+O для збереження файлу, *Y* для підтвердження, Ctrl+X для виходу).

5.3. Зазначити у звіті, які параметри забезпечують підключення до БД.

6. Виконати розміщення CMS на сервері.

6.1. Перемістити каталог із сконфігурованою CMS у */var/www* командою *sudo cp -R ./wordpress /var/www* (рис. 2).

```
root@debian:~# nano ./wordpress/wp-config-sample.php
root@debian:~# nano ./wordpress/wp-config-sample.php
root@debian:~# sudo cp -R ./wordpress /var/www
root@debian:~#
```

Рис. 2. Виконання переміщення сконфігурованої CMS

7. Виконати налаштування web-сервера.

7.1. У файлі налаштувань web-сервера Apache вказати в якості кореневого каталогу web-сервера шлях до каталогу */var/www/wordpress*: вікрити файл командою *sudo nano /etc/apache2/sites-enabled/000-default.conf* та замінити значення властивості DocumentRoot на */var/www/wordpress.* Зберегти зміни (рис. 3).

Рис. 3. Внесення змін у файл *000-default.conf*

7.2. Пояснити призначення кореневого каталогу web-сервера.

8. Виконати запуск та перевірку сервера.

8.1. Перезапустити web-сервер командою *sudo service apache2 restart.*

8.2. Перевірити доступ до web-сервера через браузер.

8.3. Оцінити ризик використання HTTP (відсутність шифрування, можливість перехоплення даних).

9. Встановлення та запуск WordPress.

9.1. Виконати встановлення CMS через браузер. Ввести в рядок адреси web-браузера IP-адресу сервера (команда *ip a*), перейти на сторінку встановлення CMS Wordpress та виконати встановлення системи керування вмістом (ввести необхідну інформацію для створення сайту).

9.2. Після встановлення увійти з вашим логіном та паролем у адмін-панель CMS Wordpress та створити запис на сайті, останній рядок якого повинен містити ваше прізвище, та натиснути «*Опублікувати*».

9.3. Відкрити знову головну сторінку сайту та переконатись, що запис опубліковано (web-сторінку створено). Після розгортання web-додатку виконується налаштування засобів захисту.

10. Налаштування захисту (Wordfence).

10.1. Встановити плагін Wordfence. Для цього у адмін-панелі CMS Wordpress необхідно перейти в розділ плагіни і додати новий плагін Wordpress.

10.2. Ознайомитися з функціями плагіну (firewall, сканування, захист входу).

11. Перевірка механізмів захисту.

11.1. Перевірити можливості плагіну Wordfence виявляти несанкціоновані зміни структури. Для цього необхідно додати у файл *wp-login.php* за допомогою текстового редактора *nano* рядок *echo 'wordfence Test'.*

11.2. Запустити сканування Wordfence.

11.3. Проаналізувати виявлені зміни як приклад несанкціонованого втручання.

Зауваження. Плагін Wordfence буде шукати всі відмінності файлів встановленого WordPress від оригінальних і видасть інформацію про те, що відбулися несанкціоновані зміни (якщо вони були).

12. Виконати аналіз результатів.

12.1. Оцінити: доступність web-сервера та рівень захисту доступу.

12.2. Визначити: потенційні загрози (HTTP, слабкі паролі, відкритий доступ).

12.3. Зробити висновок щодо безпечності web-інтерфейсу в енергетичних системах.

13. Результати виконання всіх пунктів оформити у вигляді звіту на стандартних аркушах формату А4.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму роботи;
- результати виконання всіх пунктів порядку роботи з коротким описом виконаних дій;
- скріншоти основних етапів: оновлення системи; встановлення Apache, PHP, MySQL; налаштування wp-config.php та 000-default.conf; сторінка встановлення WordPress; створений запис на сайті; результати роботи плагіну Wordfence (виявлення

змін);

- аналіз: доступності web-сервера; ризиків використання HTTP (відсутність шифрування); результатів перевірки Wordfence;
- висновок.

Контрольні запитання

1. Яке призначення web-сервера в інформаційних системах електроенергетики?
2. Чому web-сервери не повинні мати прямого доступу до ПЛК, RTU та РЗА?
3. Що таке демілітаризована зона і яка її роль у енергосистемах?
4. Яке призначення Apache HTTP Server?
5. Яку роль виконує база даних у роботі CMS WordPress?
6. Які основні функції систем керування вмістом (CMS)?
7. Які основні загрози існують для web-інтерфейсів SCADA та АСКОЕ?
8. Чому використання HTTP є небезпечним у енергетичних системах?
9. Яке призначення плагіну Wordfence і які механізми захисту він реалізує?
10. Які заходи необхідно застосовувати для забезпечення безпеки web-інтерфейсів в енергетиці?

Лабораторна робота 10
Аналіз та діагностика мереж передачі даних в електроенергетичних системах

Мета роботи

Навчитись використовувати засоби аналізу та діагностики мереж для оцінки доступності вузлів, визначення затримок, аналізу маршрутів передачі даних та виявлення проблем у мережах електроенергетичних систем.

Теоретичні відомості

ARP (англ. Address Resolution Protocol — протокол визначення адрес) — мережевий протокол, призначений для перетворення IP-адрес (адрес мережевого рівня) в MAC-адреси (адреси канального рівня) в мережах TCP/IP. Він визначений в стандарті RFC 826.

Перетворення адрес виконується шляхом їх пошуку за спеціальною таблицею. Ця таблиця називається ARP-таблицею, зберігається у пам'яті і містить рядки для кожного вузла мережі. В двох стовпчиках містяться IP- та Ethernet-адреси. Якщо потрібно перетворити IP-адресу в Ethernet-адресу, то відбувається пошук запису з відповідною IP-адресою. У ході звичайної роботи мережева програма відправляє прикладне повідомлення, користуючись транспортними послугами TCP. Модуль TCP посилає відповідне транспортне повідомлення через модуль IP. В результаті, складається IP-пакет, який має бути переданий драйверу Ethernet. IP-адреса місця призначення відома прикладній програмі, модулю TCP та IP. Необхідно на її основі знайти Ethernet-адресу місця призначення. Для пошуку відповідної Ethernet-адреси використовується ARP-таблиця.

ping — службова комп'ютерна програма (утиліта), призначена для перевірки з'єднань в мережах на основі TCP/IP. Вона відправляє запити (англ. Echo-Request) протоколу ICMP зазначеному вузлу мережі й фіксує відповіді (англ. Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати двосторонні затримки у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв.

Повна відсутність ICMP-відповідей може також означати, що віддалений вузол (або якийсь із проміжних маршрутизаторів) блокує ICMP Echo-Reply або ігнорує ICMP Echo-Request.

Утиліта *ping* є одним з основних діагностичних засобів у мережах TCP/IP і входить у поставку всіх сучасних мережевих операційних систем. Функціональність утиліти *ping* також реалізована в деяких вбудованих операційних системах маршрутизаторів, доступ до результатів виконання *ping* для таких пристроїв за протоколом SNMP визначається відповідними стандартами.

Для отримання шляху проходження пакетів до певного вузла мережі використовують утиліту *tracert/traceroute*. Це службова комп'ютерна програма, яка призначена для визначення маршрутів прямування даних в мережах TCP/IP. *Traceroute* може використовувати різні протоколи передачі даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери з встановленою операційною системою Windows використовують ICMP-протокол, операційні системи Linux і маршрутизатори Cisco – протокол UDP.

Для сканування цілих мереж найчастіше використовується утиліта *nmap* (Network Mapper) – це безкоштовне відкрите програмне забезпечення для дослідження та аудиту безпеки мереж і виявлення активних мережевих сервісів. Утиліта *nmap* — це потужний інструмент, який використовується для дослідження мережі, виявлення пристроїв і перевірки безпеки. Її основне призначення — збирати інформацію про вузли в мережі та їхні відкриті порти. Її широко використовують адміністратори, фахівці з кібербезпеки та розробники систем моніторингу.

Nmap підтримує розширені можливості мережевого аналізу, зокрема: визначення операційної системи віддаленого хоста, різні режими сканування (у тому числі приховане та паралельне), аналіз відкритих портів і фільтрів пакетів, виявлення активних і неактивних вузлів, а також використання сценаріїв (Lua) для автоматизації досліджень мережі.

Основні параметри *Nmap*, що можуть застосовуються для аналізу мереж електроенергетичних систем:

-sn — визначення активних вузлів у мережі (без сканування

портів);

-p — задання діапазону портів для перевірки;

-sT — TCP-сканування (базовий і безпечніший режим);

-sU — UDP-сканування (актуально для промислових протоколів);

-sV — визначення версій служб на відкритих портах;

-O — визначення операційної системи вузла;

-T3 — стандартна швидкість сканування (рекомендована для стабільності мережі).

Приклади типових застосувань утиліти *nmap*:

- сканування всієї локальної мережі - *nmap -sn 192.168.0.0/24*
- сканування конкретного вузла мережі - *nmap 192.168.0.5*
- перевірка портів -*nmap -p 1-1024 192.168.0.5*
- визначення ОС - *nmap -O 192.168.0.5*
- визначення версій сервісів - *nmap -sV 192.168.0.5*

У сучасних електроенергетичних системах, зокрема в автоматизованих системах комерційного обліку електроенергії (АСКОЕ), а також у SCADA-системах та цифрових підстанціях, засоби діагностики мереж є невід'ємною частиною забезпечення надійності передачі даних. Цифрова інфраструктура комерційного обліку включає лічильники електроенергії, концентратори даних (DCU), сервери збору та обробки інформації, а також канали зв'язку (Ethernet, GSM/GPRS, VPN). Безперервність обміну даними між цими елементами є важливою для коректного обліку та управління енергоспоживанням.

Утиліта *ping* використовується для перевірки доступності вузлів мережі та оцінки затримок передачі даних. У практиці експлуатації АСКОЕ та SCADA вона застосовується для контролю зв'язку з серверами збору даних, програмованими логічними контролерами (ПЛК), пристроями телемеханіки (RTU), а також комунікаційними шлюзами. Аналіз часу відгуку (RTT) дозволяє виявити перевантаження мережі або проблеми в каналах зв'язку, що особливо важливо при використанні мобільних або радіоканалів передачі даних.

Утиліта *traceroute* (tracert) використовується для визначення маршруту проходження пакетів до віддалених вузлів. У системах електроенергетики вона дозволяє аналізувати шлях передачі даних між, наприклад, сервером АСКОЕ та віддаленими

лічильниками або підстанціями. Це дає змогу виявити вузли, на яких виникають затримки або втрати пакетів, що є критично важливим при побудові багаторівневих мереж передачі даних.

Протокол ARP використовується для встановлення відповідності між IP- та MAC-адресами у локальних мережах. У контексті АСКОЕ та локальних мереж підстанцій він застосовується для діагностики конфліктів IP-адрес, а також перевірки доступності мережевих пристроїв, таких як лічильники з Ethernet-інтерфейсом, комутатори та шлюзи збору даних. Наявність некоректних або дубльованих записів у ARP-таблиці може свідчити про помилки конфігурації мережі.

Утиліта *Nmap* використовується для виявлення активних вузлів у мережі та аналізу відкритих портів і сервісів. У мережах електроенергетики вона може застосовуватись під час аудиту мережевої інфраструктури, зокрема для перевірки доступності серверів, комунікаційних пристроїв та інших елементів цифрової інфраструктури. Водночас її використання повинно здійснюватися з обережністю та лише в межах дозволених систем, оскільки активне сканування може впливати на роботу промислового обладнання.

Таким чином, засоби діагностики мереж є важливими інструментами забезпечення стабільної роботи інформаційних систем електроенергетики. Їх використання дозволяє своєчасно виявляти проблеми зв'язку, аналізувати стан мережі та забезпечувати надійне функціонування систем комерційного обліку електроенергії та автоматизованого управління технологічними процесами.

Програма роботи

1. Ознайомитися з принципами роботи та застосуванням засобів діагностики мереж (ARP, ping, traceroute, Nmap) у електроенергетичних системах.
2. Виконати дослідження доступності вузлів, визначення затримок та маршрутів передачі даних у мережі.
3. Виконати сканування мережі та аналіз активних вузлів і сервісів.
4. Провести аналіз отриманих результатів та оцінити стан мережі електроенергетичної системи.

Порядок виконання роботи

1. Виконати підготовку робочого середовища.

1.1. Запустити віртуальну машину в середовищі Oracle VM VirtualBox.

1.2. Перевірити тип мережевого підключення (NAT або мережевий міст).

1.3. Відкрити термінал у гостьовій операційній системі.

1.4. Оновити систему командами *apt-get update* та *apt-get upgrade*.

2. Визначити мережеві параметри та виконати аналіз ARP.

2.1. Визначити IP-адресу віртуальної машини командою *ip a*.

2.2. Переглянути ARP-таблицю: у ОС Windows — *arp -a*; у ОС Debian — *ip neigh*.

2.3. Занести отримані дані у звіт.

2.4. Проаналізувати: відповідність IP- та MAC-адрес; наявність невідомих або дубльованих записів.

3. Виконати перевірка доступності вузлів.

3.1. Виконати перевірку доступності вузлів за допомогою команди *ping*: до доменного імені (наприклад, *ping -a nuwm.edu.ua*, *ping -a google.com*); до IP-адреси.

3.2. Повторити перевірку в обох системах (ОС Windows і ОС Debian).

3.3. Визначити:

- чи відповідає вузол;
- середній час затримки (RTT);
- наявність втрат пакетів.

4. Виконати аналіз маршруту передачі даних.

4.1. Визначити маршрут до вузла: у ОС Windows — команда *tracert*; у ОС Debian — команда *sudo traceroute*.

4.2. Проаналізувати отриманий маршрут:

- кількість вузлів (стрибків);
- вузли із затримками;
- можливі місця втрати пакетів.

Зауваження. За допомогою цього аналізу можливо зрозуміти, через які пристрої проходять дані та де можуть виникати проблеми.

5. Виконати дослідження структури мережі та доступні

сервіси.

5.1. Встановити утиліту Nmap: *sudo apt-get install nmap.*

5.2. Виконати:

- пошук активних вузлів у мережі (-sn);
- сканування окремого вузла;
- перевірку відкритих портів (-p).

Зауваження. Приклад введення команди з використанням атрибутів: *nmap -sn 192.168.1.1/24*).

5.3. Проаналізувати: які вузли доступні; які служби працюють; чи є відкриті порти.

6. Виконати порівняння режимів роботи мережі для визначення того, як тип підключення впливає на її роботу.

6.1. Змінити тип підключення віртуальної машини: *NAT* та *мережевий міст* (Bridged)

6.2. Повторити основні перевірки утиліт: *ping*, *traceroute*, *Nmap*.

6.3. Порівняти результати: доступність вузлів; маршрути; кількість виявлених пристроїв.

7. Провести узагальнення результатів дослідження.

7.1. Оцінити: доступність вузлів мережі; стабільність зв'язку; затримки передачі даних.

7.2. Визначити: можливі проблеми мережі; вузли, що впливають на якість зв'язку.

7.3. Зробити загальний висновок про стан мережі.

8. Оформити результати роботи у вигляді звіту відповідно до встановлених вимог.

Вимоги до оформлення звіту:

Звіт повинен містити:

- титульну сторінку;
- мету роботи;
- програму роботи;
- результати виконання кожного етапу роботи (відповідно до пунктів порядку виконання);
- скріншоти виконання основних команд (ARP, ping, traceroute, Nmap);
- пояснення отриманих результатів для кожного етапу (що було зроблено та що отримано);

- аналіз: відповідності IP- та MAC-адрес (ARP); доступності вузлів і затримок (ping); маршрутів передачі даних (traceroute); активних вузлів і відкритих портів (Nmap);
- порівняння результатів для режимів NAT і мережевого мосту;
- висновок щодо стану мережі та якості передачі даних.

Контрольні запитання

1. Яке призначення протоколу ARP і яку інформацію містить ARP-таблиця?
2. Які проблеми мережі можна виявити за допомогою ARP-таблиці?
3. Яке призначення утиліти ping і які параметри вона дозволяє оцінити?
4. Що означає час RTT та втрати пакетів при виконанні ping?
5. Яке призначення утиліти traceroute (tracert) і яку інформацію вона надає?
6. Як за допомогою traceroute визначити проблемні ділянки мережі?
7. Яке призначення утиліти Nmap і які задачі вона вирішує?
8. Яку інформацію можна отримати при скануванні мережі за допомогою Nmap?
9. У чому полягає різниця між режимами NAT і мережевого мосту?
10. Які основні показники характеризують стан мережі в електроенергетичних системах?

ЛІТЕРАТУРА

1. Технології розробки WEB-ресурсів [Електронний ресурс]: навчальний посібник / В. П. Молчанов, О. К. Пандорін. Харків : ХНЕУ ім. С. Кузнеця, 2019. 130 с.

2. Карпалюк І. Т. Комп'ютерні інформаційні технології в енергетиці / Харків. нац. ун–т міськ. госп–ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2018. 118 с.

3. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.

4. Передача інформації в електроенергетиці: засоби, протоколи, стандарти, кібербезпека : навчальний посібник / О. В. Дяченко, Д. А. Гапон, Н. В. Рудевіч, С. В. Швець, Т. С. Донецька, Р. С. Ложкін. Харків : НТУ «ХПІ», 2025. 256 с.

5. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.

6. ДСТУ EN ISO/IEC 27002:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки.

7. Комп'ютерні мережі : навчальний посібник / Азаров О. Д., Захарченко С. М., Кадук О. В. та ін. Вінниця : ВНТУ, 2013. 371 с.

8. Сидорчук Б. П. Ідентифікація та моделювання. Частина ІІ. Ідентифікація та моделювання технологічних об'єктів за методами комп'ютерного моделювання [Електронне видання] : навч. посіб. / Б. П. Сидочук, О. М. Наумчук, С. К. Матус. Рівне : НУВГП, 2023. 201 с.

9. Сидорчук Б. П., Наумчук О. М. Ідентифікація та моделювання. Частина І. Ідентифікація та моделювання об'єктів автоматизації за пасивними експериментами : навч. посіб. / Б. П.Сидорчук, О. М. Наумчук. Рівне : НУВГП, 2021. 133 с.