

Міністерство освіти і науки України  
Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки

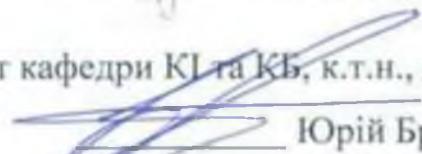
## ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра  
на тему: «Проект захищеної корпоративної мережі»

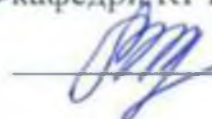
Виконав студент 4-го курсу групи КБ-19-2  
спеціальності 125 «Кібербезпека»

 Данило Решетнюк

Керівник Доцент кафедри КІ та КБ, к.т.н., доцент

 Юрій Бродський

Рецензент Професор кафедри КІ та КБ, д.т.н., доцент

 Володимир Воротніков

Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки  
Спеціальність 125 «Кібербезпека»  
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної  
інженерії та кібербезпеки

Андрій Єфіменко

2 серпня 2023 р.

### ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Решетнюк Данило Костянтинович

Тема роботи: «Проект захищеної корпоративної мережі»

Затверджена Наказом університету від 2 серпня 2023 р. №29/с

Термін здачі студентом закінченої роботи 23 серпня 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є захищена корпоративна мережа, яка включає в себе інфраструктуру, пристрої та ресурси, використовувані для обміну інформацією та забезпечення комунікацій між різними підрозділами організації.

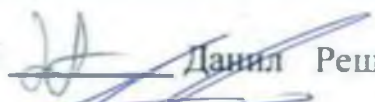
Предметом дослідження є розробка та впровадження заходів з кібербезпеки для забезпечення ефективного захисту корпоративної мережі. Це включає аналіз потенційних загроз, розробку архітектури безпеки, впровадження механізмів контролю доступу та захисту, а також налаштування систем моніторингу та реагування на інциденти безпеки.

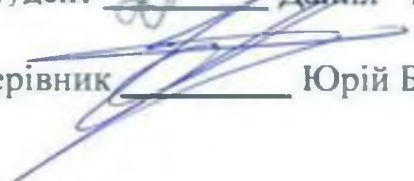
Обладнання та програмне забезпечення:

1. Мережевий симулятор Cisco Packet Tracer
2. Комутатор
3. Сервер DHCP
4. Веб-сервер
5. Сервер DNS

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

| Розділ | Консультант     | Підпис, дата   |                  |
|--------|-----------------|----------------|------------------|
|        |                 | Завдання видав | Завдання прийняв |
| 1      | Бродський Ю. Б. | 06.03.2023     | 06.03.2023       |
| 2      | Бродський Ю. Б. | 06.03.2023     | 06.03.2023       |
| 3      | Бродський Ю. Б. | 06.03.2023     | 06.03.2023       |

Студент  Данил Решетнюк

Керівник  Юрій Бродський

### Календарний план

| № з/п | Назви етапів випускної кваліфікаційної роботи | Термін виконання етапів роботи | Примітка |
|-------|-----------------------------------------------|--------------------------------|----------|
| 1     | Видача завдання                               | 06.03.2023                     | виконано |
| 2     | Розробка плану роботи                         | 30.05.2023                     | виконано |
| 3     | Розробка розгорнутого плану                   | 01.06.2023                     | виконано |
| 4     | Подача чернетки керівнику для перевірки       | 27.07.2023                     | виконано |
| 5     | Доопрацювання роботи та перевірка керівником  | 01.08.2023                     | виконано |
| 6     | Затвердження графічних матеріалів у керівника | 10.08.2023                     | виконано |
| 7     | Проведення попереднього захисту               | 10.08.2023                     | виконано |
| 8     | Отримання відгуку керівника                   | 10.08.2023                     | виконано |
| 9     | Допуск завідувача кафедри                     | 10.08.2023                     | виконано |
| 10    | Подання роботи на рецензування                | 10.08.2023                     | виконано |

Студент  Данил Решетнюк

Керівник  Юрій Бродський

## АНОТАЦІЯ

Дипломна робота присвячена розробці та реалізації проєкту захищеної корпоративної мережі з метою створення комплексної системи захисту, спрямованої на оптимальне забезпечення безпеки інформаційних ресурсів та даних підприємства. У роботі розглянуті різноманітні загрози та вразливості, що можуть вплинути на корпоративну мережу, та розроблені рекомендації та стратегії для ефективної протидії.

Практичне значення проведеної дослідницької роботи полягає в тому, що вона надає конкретні рекомендації та розробляє ефективні стратегії для захисту корпоративних мереж від різноманітних кіберзагроз. Наведено деякі методи захисту, що були реалізовані:

1. Автентифікація та авторизація: Використання паролів для привілейованого режиму та реалізація безпечного SSH доступу гарантує контрольний рівень доступу до системних ресурсів та надійний захищений віддалений доступ.

2. Розподіл на сегменти: Впровадження техніки VLAN та методу "Router-on-a-stick" дозволило розбити мережу на сегменти, скорочуючи можливість передачі даних та небажаної комунікації, що внесло вагомий внесок у загальний рівень безпеки.

3. Файрвол та керування доступом: Застосування списків керування доступом (ACL) дозволило ефективно контролювати та блокувати ризикові протоколи та забезпечити відповідний рівень доступу до мережевих сервісів.

4. Віртуальні приватні мережі (VPN): Використання VPN створило надійний та захищений канал зв'язку між різними відділеннями, гарантуючи конфіденційність та цілісність передачі даних.

Пояснювальна записка до випускної кваліфікаційної роботи містить в собі 66 сторінок, 28 рисунків та 5 додатків. Список використаних джерел містить 26 найменувань і займає 2 сторінки.

Ключові слова: КОРПОРАТИВНА МЕРЕЖА, ЗАХИСТ, БЕЗПЕКА, ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА (VPN), МОНІТОРИНГ МЕРЕЖІ,

|                       |                  |          |                 |          |                                          |  |  |  |  |
|-----------------------|------------------|----------|-----------------|----------|------------------------------------------|--|--|--|--|
| <b>АУТЕНТИФІКАЦІЯ</b> |                  |          |                 |          | КІК.КР.Б - 125 - 04 - ПЗ                 |  |  |  |  |
| Зм.                   | Арж.             | № докум. | Підпис          | Дата     | Проєкт захищеної<br>корпоративної мережі |  |  |  |  |
| Розроб.               | Решетинюк Д.К.   |          | <i>[Підпис]</i> | 23.08.23 |                                          |  |  |  |  |
| Керівник              | Бродський Ю.Б.   |          | <i>[Підпис]</i> | 23.08.23 |                                          |  |  |  |  |
| Реценз.               | Воротнішова В.П. |          | <i>[Підпис]</i> | 23.08.23 |                                          |  |  |  |  |
| Н. контр.             | Бродський Ю.Б.   |          | <i>[Підпис]</i> | 23.08.23 |                                          |  |  |  |  |
| Затверд.              | Сфіменко А.А.    |          | <i>[Підпис]</i> | 23.08.23 | ФІКТ, Гр. КБ-19-1                        |  |  |  |  |
|                       |                  |          |                 |          |                                          |  |  |  |  |

## ANNOTATION

The diploma thesis is devoted to the development and implementation of a secure corporate network project aimed at creating a comprehensive protection system to optimally secure the information resources and data of the organization. The work addresses various threats and vulnerabilities that may impact the corporate network, and provides recommendations and strategies for effective countermeasures.

The practical significance of the conducted research lies in its provision of specific recommendations and development of effective strategies to safeguard corporate networks from diverse cyber threats. Some implemented methods of protection are as follows:

1. Authentication and Authorization: The use of passwords for privileged mode and the implementation of secure SSH access ensure controlled access to system resources and reliable secure remote connectivity.

2. Segmentation: The adoption of VLAN techniques and the "Router-on-a-stick" method facilitated network segmentation, reducing the potential for data leakage and undesired communication, thus contributing significantly to overall security enhancement.

3. Firewall and Access Control: The application of Access Control Lists (ACL) effectively managed and blocked risky protocols, ensuring an appropriate level of access to network services.

4. Virtual Private Networks (VPN): The implementation of VPNs established a reliable and secure communication channel between various branches, guaranteeing data confidentiality and integrity.

The explanatory note for the graduation thesis consists of 66 pages, 28 figures, and 5 appendices. The list of used sources contains 26 references and covers 2 pages.

Keywords: CORPORATE NETWORK, SECURITY, PROTECTION, VIRTUAL PRIVATE NETWORK (VPN), NETWORK MONITORING, AUTHENTICATION.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 5    |

## ЗМІСТ

|                                                                                                                             |    |
|-----------------------------------------------------------------------------------------------------------------------------|----|
| ВСТУП .....                                                                                                                 | 8  |
| РОЗДІЛ 1 АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ КОРПОРАТИВНОЇ МЕРЕЖІ .....                                                           | 9  |
| 1.1. Основні поняття та визначення.....                                                                                     | 9  |
| 1.2 Кібератаки в Україні: огляд загальної ситуації .....                                                                    | 13 |
| 1.3 Аналіз існуючих підходів до захисту корпоративних мереж.....                                                            | 15 |
| 1.4 Аналіз потреб користувачів та вимоги до мережі.....                                                                     | 20 |
| 1.5 Постановка технічного завдання .....                                                                                    | 25 |
| ВИСНОВОК ДО РОЗДІЛУ 1 .....                                                                                                 | 27 |
| РОЗДІЛ 2 ПРОЕКТУВАННЯ ТА РОЗРОБКА ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ .....                                                      | 28 |
| 2.1 Опис симулятора Cisco Packet Tracer .....                                                                               | 28 |
| 2.2 Побудова моделі захищеної корпоративної мережі .....                                                                    | 32 |
| 2.3 Налаштування захисту корпоративної мережі .....                                                                         | 39 |
| ВИСНОВОК ДО РОЗДІЛУ 2 .....                                                                                                 | 53 |
| РОЗДІЛ 3 ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ КОРПОРАТИВНОЇ МЕРЕЖІ.....                                                                 | 55 |
| 3.1 Тестування та перевірка функціональності.....                                                                           | 55 |
| 3.2 Забезпечення стійкості та безпеки корпоративної мережі: механізми резервного копіювання та роль навчання персоналу..... | 60 |
| ВИСНОВОК ДО РОЗДІЛУ 3 .....                                                                                                 | 65 |
| ВИСНОВКИ.....                                                                                                               | 66 |
| СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ .....                                                                                        | 68 |
| ДОДАТКИ.....                                                                                                                | 71 |

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN – Віртуальна приватна мережа (Virtual Private Network)

IDS – Система виявлення вторгнень (Intrusion Detection System)

IPS – Система запобігання вторгненню (Intrusion Prevention System)

IT – Інформаційні технології (Information Technology)

LAN – Локальна обчислювальна мережа (Local Area Network)

WAN – Глобальна обчислювальна мережа (Wide Area Network)

CEF – Cisco Express Forwarding

HTTPS – Протокол захищеного гіпертекстового передавання (Hypertext Transfer Protocol Secure)

SQL – Мова структурованих запитів (Structured Query Language)

GUI – Графічний інтерфейс користувача (Graphical User Interface)

ATM – Асинхронний режим передавання (Asynchronous Transfer Mode)

MPLS – Многопротокольна мітка комутації (Multiprotocol Label Switching)

IP – Інтернет-протокол (Internet Protocol)

HTTP – Протокол передавання гіпертексту (Hypertext Transfer Protocol)

HTTPS – Протокол захищеного передавання гіпертексту (Hypertext Transfer Protocol Secure)

VLAN – Віртуальна локальна мережа (Virtual Local Area Network)

WAN – Wide Area Network

MAC – Медіа-адреса керування (Media Access Control)

DNS – Система доменних імен (Domain Name System)

DHCP – Протокол динамічної конфігурації хостів (Dynamic Host Configuration Protocol)

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 7    |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

## ВСТУП

**Актуальність теми.** У сучасному світі корпорації та підприємства все більше залежать від інформаційних технологій та комп'ютерних мереж для забезпечення своєї діяльності та обміну важливими даними. Розвиток цифрових технологій та збільшення обсягу інформації створюють нові можливості, але водночас і ставлять під загрозу конфіденційність, цілісність та доступність даних. Забезпечення безпеки корпоративних мереж стає критично важливим завданням для організацій у контексті зростаючих кіберзагроз.

**Мета і завдання роботи.** Метою роботи є створення та вдосконалення захищеної корпоративної мережі, спрямованої на підвищення рівня кібербезпеки та забезпечення надійного функціонування організаційної інформаційної інфраструктури.

Досягнення поставленої мети передбачає розв'язання наступних завдань:

- Аналіз сучасних підходів та технологій у галузі корпоративних мереж та кібербезпеки.
- Дослідження наявних рішень та методів захисту мережі.
- Розробка архітектури захищеної корпоративної мережі, враховуючи потреби організації та вимоги забезпечення безпеки..
- Експериментальне тестування та оцінка ефективності реалізованих заходів безпеки для підвищення рівня захисту мережі.

**Об'єктом дослідження** є захищена корпоративна мережа, яка включає в себе інфраструктуру, пристрої та ресурси, використовувані для обміну інформацією та забезпечення комунікацій між різними підрозділами організації.

**Предметом дослідження** є розробка та впровадження заходів з кібербезпеки для забезпечення ефективного захисту корпоративної мережі.

**Методи дослідження.** Для досягнення поставлених цілей в рамках даної дипломної роботи використовувалися такі методи дослідження: аналіз літературних джерел та наукової літератури, вивчення стандартів та практик з кібербезпеки, проведення експериментальних випробувань та аналіз отриманих результатів.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 8    |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

# РОЗДІЛ 1 АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ КОРПОРАТИВНОЇ МЕРЕЖІ

## 1.1. Основні поняття та визначення

Корпоративна мережа – це комп'ютерна мережа, яка об'єднує комп'ютери, сервери, пристрої, програмне забезпечення та інші ресурси в межах організації або підприємства. Вона дозволяє спільний доступ до даних, ресурсів і послуг всім співробітникам та користувачам організації.

Корпоративні мережі мають декілька ключових характеристик:

1. **Масштабність:** Корпоративні мережі можуть об'єднувати велику кількість пристроїв, від декількох десятків до тисяч комп'ютерів, що знаходяться на різних відділеннях або офісах організації.

2. **Доступність:** Корпоративні мережі зазвичай працюють цілодобово і забезпечують постійний доступ до даних і ресурсів для користувачів.

3. **Безпека:** Забезпечення безпеки важливих даних і інформації є однією з головних задач корпоративної мережі. Застосовуються різноманітні заходи, такі як фаєрволи, антивірусне програмне забезпечення, VPN (віртуальні приватні мережі) і шифрування для захисту даних від несанкціонованого доступу.

4. **Централізоване управління:** Корпоративна мережа зазвичай управляється централізовано, що дозволяє адміністраторам контролювати доступ до ресурсів, надавати права доступу, встановлювати політики безпеки та моніторити діяльність користувачів.

5. **Спільний доступ до ресурсів:** Корпоративна мережа дозволяє користувачам спільно працювати над документами, обмінюватися інформацією, використовувати спільні друкуючі пристрої, сервери, бази даних і програми.

6. **Ефективність:** Корпоративні мережі допомагають оптимізувати робочі процеси, знижуючи час та зусилля, потрібні для виконання завдань.

Важливо зазначити, що корпоративна мережа може мати зв'язок з Інтернетом або бути ізольованою внутрішньою мережею (Intranet) залежно від потреб організації.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 9    |

Узагальнена структура корпоративної мережі наведена на рис.1.1.

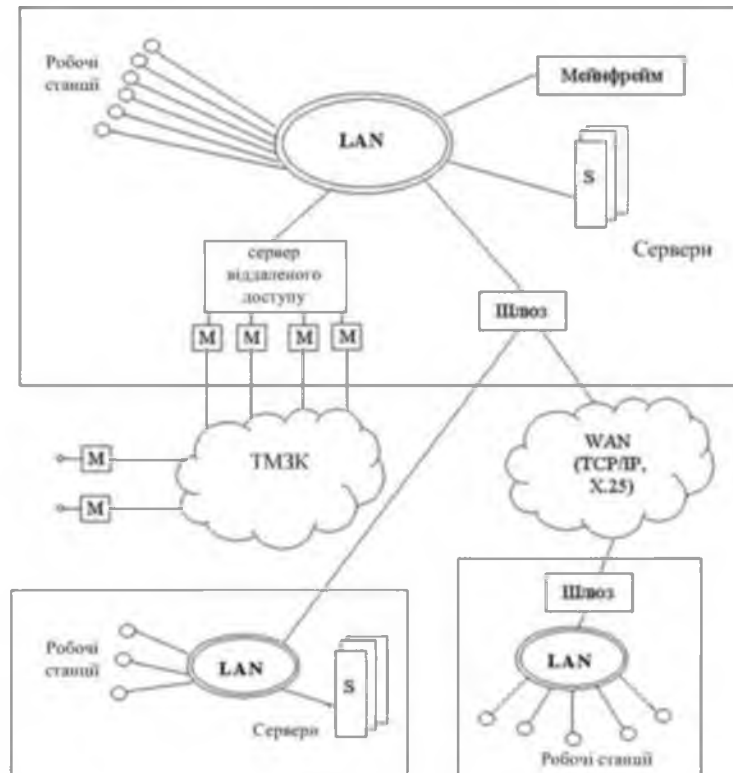


Рисунок 1.1 – Узагальнена структура корпоративної мережі

Такі мережі є важливою складовою сучасного бізнесу, оскільки забезпечують ефективний обмін інформацією між співробітниками та дозволяють підвищити продуктивність і координацію робочих процесів. Однак з моменту наявності багатьох цінних даних та інформації, забезпечення кібербезпеки в корпоративних мережах стає дедалі більш важливою та викликає рости увагу до захисту від кіберзагроз.

### Загрози та вразливості корпоративних мереж

Корпоративні мережі, як і будь-які інші інформаційні системи, піддаються різноманітним загрозам та вразливостям, що можуть призвести до серйозних наслідків для безпеки організації та конфіденційності її даних. Вивчення цих загроз та вразливостей є важливим етапом при розробці захищеної корпоративної мережі.

#### 1. Загрози корпоративних мереж:

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 10   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

1.1. Кібератаки: Включають в себе різноманітні види атак, такі як DDoS (розподілене збове завантаження), фішинг, злам паролів, інженерія соціальних мереж та інші. Ці атаки спрямовані на викрадення даних, відмову в обслуговуванні або навіть отримання контролю над системою.

1.2. Віруси та шкідливі програми: Небажані програми, такі як віруси, черв'яки, троянські програми та шпигунське програмне забезпечення, можуть пошкоджувати файли, зламувати захист інформації та порушувати роботу мережі.

1.3. Виток інформації: Корпоративні мережі містять чутливу інформацію про організацію, клієнтів, партнерів, яка може стати об'єктом інтересу для зловмисників. Неналежний контроль доступу, незахищені з'єднання та недостатні заходи безпеки можуть призвести до небажаного розголошення цієї інформації.

1.4. Фізичні загрози: Включають в себе викрадення або пошкодження обладнання, спостереження за мережевим трафіком та злам фізичної інфраструктури мережі.

### **Вразливості корпоративних мереж:**

2.1. Недостатній контроль доступу: Недостатньо обмежений доступ до різних рівнів інформації в мережі може призвести до неправомірного доступу до конфіденційних даних.

2.2. Застаріле програмне забезпечення: Використання застарілого або неоновленого програмного забезпечення може створити лазів для зламу та експлуатації вразливостей.

2.3. Недостатні заходи шифрування: Відсутність або недостатнє застосування криптографічних методів шифрування може призвести до компрометації даних під час їх передачі чи зберігання.

2.4. Недостатня кваліфікація персоналу: Відсутність необхідних знань та навичок з кібербезпеки серед персоналу може призвести до випадкових помилок або незважливих дій, які створять ризики для мережі.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 11   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

2.5. Недостатній моніторинг та аудит безпеки: Відсутність постійного моніторингу та аудиту безпеки може призвести до несвоєчасного виявлення загроз та вразливостей, що зробить мережу більш уразливою.

З метою побудови успішної та захищеної корпоративної мережі, необхідно ретельно вивчити ці загрози та вразливості, а також розробити та впровадити ефективні заходи забезпечення кібербезпеки.

### **Основні принципи захисту інформації у мережах**

Забезпечення безпеки інформації у корпоративних мережах є критично важливим завданням для забезпечення конфіденційності, цілісності та доступності даних. Основні принципи захисту інформації у мережах включають різноманітні підходи та методи, які спрямовані на мінімізацію ризиків і підвищення рівня кібербезпеки. Ось деякі з них:

**Аутентифікація та авторизація:** Забезпечення ідентифікації користувачів та перевірки їх прав доступу є одним із найважливіших принципів захисту мережі. Сильні методи аутентифікації, такі як двофакторна аутентифікація, дозволяють перевірити справжність користувачів перед наданням прав доступу до ресурсів мережі.

**Шифрування:** Використання криптографічних алгоритмів для шифрування даних під час їх передачі через мережу або зберігання на серверах допомагає уникнути несанкціонованого доступу до конфіденційної інформації.

**Забезпечення цілісності даних:** Використання хеш-функцій та механізмів контролю цілісності даних допомагає виявляти незаконні зміни в інформації та забезпечує її недоторканість.

**Сегментація мережі:** Розділення корпоративної мережі на логічні сегменти або зони допомагає обмежити розповсюдження атак усередині мережі та мінімізувати шкоду в разі компрометації.

**Резервне копіювання:** Регулярне створення резервних копій даних допомагає уникнути втрати інформації у разі випадкових або зловмисних дій.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 12   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

Аудит безпеки: Постійне моніторинг і аналіз активності мережі допомагає вчасно виявляти підозрілі дії та потенційні загрози.

Контроль доступу: Налаштування прав доступу до різних ресурсів мережі забезпечує обмеження можливостей користувачів та підтримує приватність даних.

Періодична оновлення: Систематичне оновлення програмного забезпечення, операційних систем та антивірусного програмного забезпечення дозволяє уникнути використання вразливостей старих версій.

Навчання та свідомість користувачів: Освіта користувачів про основні загрози і правила кібербезпеки є ефективним засобом попередження соціального інжинірингу та інших атак, що залучають людський фактор.

Використання цих принципів захисту інформації у мережах дасть можливість підвищити рівень кібербезпеки та зменшити ризики компрометації даних.

## 1.2 Кібератаки в Україні: огляд загальної ситуації

Діяльність кіберзлочинців в Україні протягом першого півріччя 2022 року підтверджує загальну тенденцію зростання хакерських атак. Серед постраждалих - не тільки урядові організації, а й представники різних секторів економіки, таких як фінансовий, комерційний, телекомунікаційний і інші. За даними CERT-UA, лише за перше півріччя 2022 року було зафіксовано 1350 кібератак.

Навіть спортивні події не залишаються поза увагою хакерів. Це підтверджує інцидент, коли хакери перервали трансляцію футбольного матчу між Україною та Уельсом на платформі Oll.tv та замість гри відтворили російську пропаганду.

Не забуваючи про себе, українські хакери також здійснюють контратаки, блокуючи понад 600 російських онлайн-ресурсів за даними Міністерства цифрової трансформації.

Загальна ситуація змушує усіх працювати у режимі цифрової небезпеки. Основним завданням ІТ-спеціалістів є пошук критичних вразливостей, мінімізація ризиків та посилення стратегії безпеки компаній. У своєму проєкті я поділюсь досвідом, як ми це робимо, сподіваючись, що наші практичні рекомендації будуть корисними для інших фахівців з кібербезпеки.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 13   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

У світі 19% кібератак припадають на Україну, що ставить нашу країну на друге місце у світовому рейтингу після США. Цей статистичний факт підкреслює необхідність українським компаніям переглянути свої заходи захисту від кіберзлочинців і вдосконалити використовувані інструменти.

Оглядом інцидентів кібератак у світі можна зробити висновок, що хоча масштабні атаки рідше спрямовані на звичайних користувачів, проте злочинці часто вдаються до простих, але ефективних методів для проникнення у системи компаній. На жаль, помилково вважається, що в основному використовуються вразливості "zero-day", оскільки реальні атаки частіше здійснюються за допомогою фішингових листів та недостатньо захищених хмарних ресурсів.

Особливо уразливими сторонами компаній, які найчастіше стають причиною порушення захисту корпоративної мережі, є:

1. Надання необмежених дозволів у хмарних ресурсах, що може призвести до витоку конфіденційної інформації та її неналежного використання.

2. Використання платформ для співпраці та комунікації, які мають недостатній рівень захисту, що створює ризик проникнення в корпоративну мережу і викрадення даних.

3. Корпоративна пошта являє собою часту мішень для атак, зокрема через фішингові посилання та шкідливі вкладення.

Для покращення захисту корпоративної мережі, рекомендується:

- Регулярно оновлювати програмне забезпечення та операційну систему, щоб усунути вразливості.

- Використовувати надійні рішення для безпеки поштових серверів та рішення для запобігання втраті даних.

- Забезпечувати надійний контроль доступу до хмарних ресурсів та обмежувати права користувачів на додавання, зміну чи видалення інформації.

- Підвищити освідомленість користувачів щодо безпечного використання поштових сервісів та інших платформ співпраці.

- Впроваджувати методи аутентифікації для забезпечення додаткового рівня захисту.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 14   |

Враховуючи ці поради, компанії можуть зробити кроки для покращення безпеки своїх корпоративних мереж і запобігання можливим кібератакам.

### **1.3 Аналіз існуючих підходів до захисту корпоративних мереж**

Забезпечення надійного та ефективного захисту корпоративних мереж є однією з найбільш актуальних і складних задач у сфері кібербезпеки. З кожним днем загрози для інформаційної безпеки зростають, а кіберзлочинці стають все більш винахідливими та завзятими у своїх спробах зламати захист корпоративних мереж. Це ставить перед компаніями і організаціями набагато складніші вимоги щодо розробки та застосування захисних стратегій.

Однак, для успішного захисту мережі необхідно добре розуміти і проаналізувати існуючі підходи та методи захисту. Саме цей аналіз і є цільовим напрямком даного пункту дослідження. В рамках даного розділу будуть розглянуті традиційні методи, що довгий час були основою безпеки мережі, а також сучасні технології та підходи, які відповідають сучасним викликам кібербезпеки. Особлива увага буде приділена їх перевагам, недолікам та потенційним обмеженням.

Проведений аналіз допоможе зрозуміти, які підходи є більш ефективними у контексті захисту корпоративних мереж, а також виявити недоліки та прогалини, які можуть бути використані зловмисниками для ініціювання кібератак. На основі цих висновків будуть запропоновані рекомендації щодо розробки комплексних та надійних стратегій кібербезпеки для корпоративних мереж, які забезпечать оптимальний рівень захисту від різноманітних загроз та забезпечать стабільну та безпечну роботу інформаційних систем.

#### **Традиційні методи захисту мережі**

Традиційні методи захисту мережі є основою для забезпечення безпеки інформаційних систем, що охоплюють усі аспекти мережевої безпеки. Вони включають у себе різноманітні технології, процедури та підходи, які допомагають

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 15   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

запобігати, виявляти та відповідати на потенційні загрози. Нижче наведені детальні пояснення про традиційні методи захисту мережі:

1. Файрволи: Файрволи є першою лінією оборони у захисті мережі. Вони фільтрують трафік, що проходить між зовнішніми та внутрішніми мережами, а також між різними сегментами внутрішньої мережі. Файрвол використовує правила (rule sets), що визначають, який трафік дозволяється, а який блокується. Це допомагає обмежити доступ до мережевих ресурсів та забезпечити безпеку системи.

2. ВПН (Віртуальні приватні мережі): ВПН забезпечують захищене з'єднання між віддаленими користувачами та офісними мережами через незахищені мережі, такі як Інтернет. Всі дані, що передаються через ВПН, шифруються, забезпечуючи конфіденційність даних.

3. IDS (Системи виявлення вторгнень): Системи виявлення вторгнень моніторять мережевий трафік на предмет аномалій та підозрілих дій. Вони виявляють потенційно небезпечні атаки або поведінку інтрузивних систем.

4. IPS (Системи запобігання вторгненням): Системи запобігання вторгненням діють після IDS та автоматично реагують на виявлені загрози, блокуючи небезпечний трафік або виконуючи інші заходи для зниження ризику компрометації.

5. Антивірусне програмне забезпечення: Антивірусне програмне забезпечення використовується для виявлення, блокування та видалення шкідливих програм, таких як віруси, черв'яки та троянські програми, що можуть пошкодити мережу та комп'ютери.

6. Контроль доступу: Контроль доступу дозволяє обмежити доступ користувачів до різних ресурсів мережі на основі їх прав та ролей. Це забезпечує захист конфіденційних даних та знижує ризик витоку інформації.

7. Шифрування даних: Шифрування даних використовується для захисту конфіденційної інформації під час її передачі по мережі. Шифрування даних дозволяє уникнути несанкціонованого доступу та зрозуміння перехопленого трафіку.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 16   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

8. Безперервне моніторинг та аналіз: Постійний моніторинг мережі та аналіз системних логів допомагає вчасно виявляти аномалії та небажану активність, що дозволяє швидко реагувати на можливі загрози.

9. Резервне копіювання даних: Регулярне створення резервних копій даних забезпечує можливість відновлення інформації у разі випадкового або зловмисного видалення або пошкодження даних.

10. Фізична безпека: Традиційні методи захисту також включають фізичні заходи безпеки, такі як контроль доступу до серверних приміщень, використання замків та систем відеоспостереження.

Застосування цих традиційних методів захисту мережі забезпечує високий рівень кібербезпеки, але слід зазначити, що враховуючи постійний розвиток загроз, таких як нові види атак та складніші загрози, також важливо поєднувати їх з іншими сучасними підходами до кібербезпеки для максимальної ефективності захисту.

### Сучасні підходи до кібербезпеки

Сучасні підходи до кібербезпеки стали набагато складнішими і комплекснішими у порівнянні з традиційними методами. Швидкий розвиток технологій, зростання кількості підключених пристроїв і поширення хмарних сервісів привели до збільшення числа кіберзагроз та потенційних атак. Ось деякі сучасні підходи та технології, які застосовуються для забезпечення кібербезпеки:

1. Машинне навчання та штучний інтелект (AI): Машинне навчання та AI стали сильними інструментами для виявлення і протидії новим та складним загрозам. Системи, здатні до самонавчання, здатні виявляти аномалії в мережевому трафіку та поведінці користувачів, сприяючи вчасній реакції на загрози.

2. Аналіз мережевої поведінки (NBA): NBA дозволяє відстежувати звичний патерн поведінки у мережі та автоматично виявляти аномальність, що забезпечує детекцію інсайдерських загроз та складних атак.

3. Підписант-незалежні (Signature-less) технології: Застосування сигнатур (підписів) для виявлення загроз є обмеженим, тому сучасні системи все більше

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 17   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

переходять до використання signature-less (не залежних від сигнатур) технологій, таких як аналіз вмісту, поведінковий аналіз та інші.

4. Хмарна кібербезпека: Завдяки поширенню хмарних технологій, використання хмарних рішень у кібербезпеці стає все більш популярним. Хмарні платформи забезпечують постійний моніторинг, автоматичні оновлення та централізоване керування заходами безпеки.

5. IoT (Інтернет речей) безпека: Зростання кількості підключених пристроїв у сучасних мережах створює нові виклики для кібербезпеки. Сучасні підходи включають захист IoT-пристроїв, виявлення та моніторинг їх активності.

6. Blockchain технології: Blockchain може використовуватись для забезпечення безпеки даних та забезпечення невідтворюваності та недоступності даних.

7. Технології нульового дня (Zero-day): Це технології, які застосовуються для захисту від атак, які використовують вразливості, які ще не відомі розробникам або виробникам програмного забезпечення.

8. Біометричні методи аутентифікації: Застосування біометричних даних, таких як відбитки пальців, розпізнавання обличчя або іриса, може забезпечити більш безпечну аутентифікацію користувачів.

9. Безперервне моніторинг та SOAR (Security Orchestration, Automation and Response): SOAR використовується для автоматизації процесу відповіді на інциденти, що дозволяє здійснювати швидку та ефективну реакцію на загрози.

10. Сучасні аудиторські та аналітичні інструменти: Для виявлення слабких місць у системі та проактивного виявлення вразливостей використовуються сучасні аудиторські та аналітичні інструменти.

Сучасні підходи до кібербезпеки ґрунтуються на принципах превентивних заходів, виявлення та реакції на загрози, а також активного моніторингу і аналізу. Ці підходи вимагають комплексного підходу до кібербезпеки, який охоплює не тільки технологічні аспекти, а й освіту користувачів та проактивне управління безпекою в організації. Постійне оновлення та розвиток цих підходів дозволяє ефективно протистояти найновішим та найбільш складним загрозам кібербезпеки.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 18   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

Порівняння традиційних методів захисту та сучасних підходів наведено в Додатку А.

Виклики та обмеження існуючих методів захисту корпоративних мереж становлять важливу проблему у забезпеченні ефективної кібербезпеки. Незважаючи на постійний розвиток технологій та заходів безпеки, деякі виклики залишаються актуальними та потребують уваги. Нижче розглянемо деякі з них:

1. Постійно змінюючіся загрози: Кіберзагрози постійно еволюціонують, що робить традиційні методи виявлення та захисту менш ефективними. Нові види атак, такі як атаки "нульового дня" або цілеспрямовані атаки, можуть бути незрозумілими для підписант-залежних технологій, що ускладнює вчасне виявлення та реакцію на них.

2. Великий обсяг даних: Сучасні організації генерують та обробляють величезний обсяг даних, що ускладнює моніторинг та аналіз мережі. Традиційні методи можуть бути неефективними в обробці великої кількості даних та виявленні мінливих аномалій.

3. Швидкість реакції: У сучасному кіберпросторі швидкість реакції на загрози є критичним аспектом. Традиційні методи, які вимагають ручної настройки та втручання, можуть бути недостатньо швидкими для ефективної реакції на швидко розвиваючіся атаки.

4. Змовні загрози: Сучасні атаки можуть використовувати змовні техніки, використовуючи декілька видів атак одночасно, щоб уникнути виявлення та обійти захист. Традиційні методи можуть не бути достатньо комплексними для ефективного протистояння таким загрозам.

5. Інсайдерські загрози: Один з найбільш складних аспектів захисту корпоративних мереж - це захист від інсайдерських загроз, тобто загроз, які виникають зсередини самої організації. Традиційні методи можуть бути менш ефективними у виявленні та запобіганні таким атакам.

6. Вартість і доступність: Впровадження сучасних підходів до кібербезпеки, таких як машинне навчання та AI, може бути дорогим та недоступним для менших організацій з обмеженим бюджетом.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 19   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

7. Запобігання фальшивим позитивам: Сучасні методи виявлення загроз можуть виявляти підозрілу активність, яка насправді є легітимною, що призводить до фальшивих позитивів. Це може перенапружити інфраструктуру та ресурси безпеки.

8. Сумісність з існуючими системами: При впровадженні нових сучасних методів захисту, важливо забезпечити їх сумісність з існуючими системами та інфраструктурою безпеки, щоб уникнути конфліктів та несправностей.

Отже, традиційні методи захисту можуть забезпечувати базовий рівень безпеки, але не завжди досить ефективні у протистоянні сучасним та складним кіберзагрозам. Сучасні методи, хоча і вимагають більшого зусилля та вкладення, пропонують більш високий рівень захисту і дозволяють виявляти та відповідати на загрози більш ефективно. Крім того, комбінування різних підходів може бути найбільш оптимальним рішенням для створення надійної та ефективної системи кібербезпеки для корпоративних мереж.

#### **1.4 Аналіз потреб користувачів та вимоги до мережі**

Вивчення потреб користувачів корпоративної мережі є ключовим етапом у розробці ефективної та збалансованої стратегії кібербезпеки. Користувачі виступають не тільки основними користувачами мережі, але і одними з найвразливіших ланок системи, оскільки їхні дії та рішення можуть суттєво впливати на рівень безпеки.

Основні аспекти вивчення потреб користувачів корпоративної мережі включають:

1. Аналіз ролей та прав доступу: Розуміння ролей різних користувачів та їхніх прав доступу є критичним для визначення, яка інформація та ресурси є найбільш цінними та вразливими. Доступ до конфіденційних даних повинен бути обмежений лише до тих, хто має необхідність у роботі з ними.

2. Опитування та аналіз практик безпеки: Вивчення того, як користувачі ставляться до питань кібербезпеки, чи дотримуються вони правил безпеки, які

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 20   |

проблеми чи недоліки існують в їхніх практиках, допомагає визначити області, що потребують поліпшення та освіти.

3. Свідомість та навчання: Проведення навчань та підвищення свідомості користувачів про потенційні кіберзагрози, методи атак та правила безпеки є важливим елементом вивчення потреб користувачів. Чим більше свідомих та освічених користувачів, тим менше ймовірність успішних атак.

4. Впровадження засобів безпеки: Вивчення потреб користувачів також допомагає визначити необхідність впровадження додаткових засобів безпеки, таких як багаторівнева аутентифікація, контроль доступу, системи виявлення вторгнень тощо, що можуть допомогти запобігти недбалості або несанкціонованому доступу.

5. Забезпечення зручності та продуктивності: При впровадженні заходів безпеки важливо забезпечити, щоб вони не перешкоджали зручності та продуктивності користувачів. Занадто складні або обтяжливі правила можуть спонукати користувачів обходити захист, що створює додаткові ризики.

6. Врахування особливостей бізнесу: Кожна організація має свої особливості та унікальні вимоги до безпеки, тому вивчення потреб користувачів мережі повинно бути спрямоване на врахування специфічних вимог та характеристик бізнесу.

Правильно вивчені потреби користувачів допомагають побудувати ефективну стратегію кібербезпеки, яка балансує безпеку та продуктивність, а також сприяє створенню свідомої та відповідальної культури безпеки в організації. Оцінка підходів до захисту мережі та визначення пріоритетних напрямків допоможе створити оптимальну систему захисту, яка задовольняє потреби користувачів та забезпечує високий рівень кібербезпеки.

### **Визначення вимог до функціональності та безпеки мережі**

Визначення вимог до функціональності та безпеки мережі є критичним етапом у процесі розробки і вдосконалення корпоративної інфраструктури. Цей процес допомагає установити об'єктивні та чіткі вимоги, які повинна задовольняти

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 21   |

мережа з точки зору її роботи, доступності, надійності та безпеки. Врахування вимог до функціональності дозволяє забезпечити ефективну роботу мережі та задоволення потреб користувачів, в той час як вимоги до безпеки гарантують захист інформації та ресурсів від різних кіберзагроз.

Для досягнення цієї мети, процес визначення вимог до функціональності та безпеки мережі включає наступні етапи:

1. Визначення цілей та потреб користувачів: Розуміння цілей та потреб користувачів є першочерговим завданням. Це допомагає з'ясувати, які функції та можливості мережі є найбільш важливими для забезпечення ефективної роботи організації та задоволення її потреб.

2. Аналіз бізнес-процесів: Аналіз бізнес-процесів дозволяє з'ясувати, які вимоги до функціональності мережі необхідні для підтримки різних операцій та діяльності організації. Наприклад, це можуть бути потреби в швидкому та надійному обміні даними між відділеннями, забезпеченні безперебійного доступу до хмарних сервісів або захисті конфіденційної інформації.

3. Визначення безпекових ризиків: Ідентифікація потенційних безпекових загроз допомагає зрозуміти, які вимоги до безпеки мережі необхідно враховувати. Це включає загрози ззовні (наприклад, хакерські атаки, віруси, фішинг) та внутрішні загрози (інсайдерські загрози, несанкціонований доступ персоналу).

4. Встановлення стандартів безпеки: Визначення стандартів та правил безпеки, які мають бути дотримані в мережі, допомагає забезпечити її захищеність та стабільність. Це можуть бути вимоги до паролів, шифрування даних, контролю доступу, аудиту дій користувачів тощо.

5. Врахування законодавства та регулювань: Вимоги до безпеки мережі також повинні враховувати відповідні законодавчі та регуляторні вимоги, які стосуються обробки та зберігання конфіденційної інформації, зокрема персональних даних.

6. Оцінка ризиків та прийняття рішень: Після зібрання інформації про вимоги до функціональності та безпеки мережі, проводиться оцінка ризиків. Це допомагає

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 22   |

визначити, які заходи забезпечення безпеки є найбільш ефективними та доцільними для досягнення поставлених цілей.

7. Формулювання стратегії безпеки: На основі результатів аналізу та оцінки ризиків розробляється стратегія безпеки мережі. Це включає вибір технологій, заходів та практик безпеки, які найкращим чином відповідають потребам та характеристикам організації.

Врахування вимог до функціональності та безпеки мережі допомагає побудувати максимально ефективну, безпечну та надійну інфраструктуру, яка задовольняє потреби організації та забезпечує захист її активів та даних.

### **Врахування правових норм і стандартів з кібербезпеки**

Врахування правових норм і стандартів з кібербезпеки є надзвичайно важливим аспектом при розробці, впровадженні та управлінні корпоративною мережею. Це допомагає забезпечити, що заходи з кібербезпеки відповідають вимогам законодавства та регуляторних органів, а також враховують найвищі стандарти безпеки для захисту інформації та даних.

Деякі з ключових аспектів врахування правових норм і стандартів з кібербезпеки включають:

1. Законодавство про кібербезпеку: Залежно від країни або регіону діяльності організації, можуть існувати різні законодавчі акти та нормативні документи, що стосуються кібербезпеки. Врахування таких норм допомагає забезпечити відповідність діяльності організації вимогам закону та уникнути можливих правових проблем.

2. Міжнародні стандарти: Існують багато міжнародних стандартів з кібербезпеки, таких як ISO 27001, NIST Cybersecurity Framework, CIS Controls тощо. Використання таких стандартів допомагає забезпечити високий рівень безпеки та встановити всесвітньо визнані практики безпеки.

3. Регуляторні вимоги: Деякі галузі діяльності можуть мати специфічні регуляторні вимоги щодо кібербезпеки. Наприклад, фінансові установи, організації

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 23   |

охорони здоров'я чи громадські служби можуть підлягати особливим вимогам щодо захисту даних та конфіденційної інформації.

4. Конфіденційність даних: Правові норми про захист персональних даних та інших конфіденційних інформаційних ресурсів зобов'язують організації вживати відповідних заходів для їх захисту від несанкціонованого доступу та витоку.

5. Звітність та аудит: Деякі правові норми можуть вимагати ведення звітності про кібербезпеку та регулярних аудитів для перевірки відповідності забезпечених заходів безпеки вимогам.

6. Страхування: Деякі компанії використовують страхування від кіберризиків як додатковий засіб забезпечення захисту від фінансових збитків у разі кібератак або інших інцидентів.

Особливості правових норм і стандартів з кібербезпеки для України мають важливе значення для забезпечення кібербезпеки в країні та захисту інформаційних ресурсів. Нижче перераховані деякі ключові аспекти правових норм та стандартів кібербезпеки для України:

1. Закон України "Про основні засади забезпечення кібербезпеки України": Цей закон був прийнятий з метою регулювання кібербезпеки в Україні та забезпечення захисту інформаційних ресурсів. Закон встановлює організаційні, технічні та правові механізми забезпечення кібербезпеки на державному рівні та в критичних інфраструктурах.

2. Стратегія національної кібербезпеки України: Україна розробила стратегію національної кібербезпеки, яка визначає основні напрямки діяльності у сфері кібербезпеки на довгострокову перспективу. Ця стратегія містить заходи щодо попередження, виявлення та реагування на кібератаки.

3. Державний центр кібербезпеки України: Україна створила Державний центр кібербезпеки, який відповідає за координацію діяльності з кібербезпеки на державному рівні, а також за аналіз загроз та реагування на інциденти.

4. Захист критичної інфраструктури: Україна приділяє особливу увагу захисту критичних інфраструктур від кіберзагроз. Критичні об'єкти, такі як

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 24   |

енергетика, транспорт, комунікації, банківська система та інші, підлягають додатковим вимогам до кібербезпеки.

5. Захист персональних даних: Україна впровадила законодавство про захист персональних даних, включаючи Закон "Про захист персональних даних", який вимагає від організацій дотримуватися високих стандартів збору, обробки та зберігання персональних даних громадян.

6. Міжнародне співробітництво: Україна активно співпрацює з іншими країнами та міжнародними організаціями у сфері кібербезпеки. Це включає обмін інформацією про загрози, розробку спільних проектів та участь у міжнародних ініціативах щодо кібербезпеки.

Врахування правових норм і стандартів з кібербезпеки для України допомагає створити цілісну та координовану систему кібербезпеки на державному рівні, забезпечити захист критичних інфраструктур, конфіденційності даних та ефективно реагувати на кібератаки та інциденти.

### 1.5 Постановка технічного завдання

Дана дипломна робота має на меті створення захищеної корпоративної мережі для Global IT Solutions Inc. з метою забезпечення конфіденційності, цілісності та доступності даних, запобігання несанкціонованому доступу та мінімізація потенційних загроз безпеці.

Завдання проекту:

- налаштування файрволу:
- використання VPN:
- використання SSH для віддаленого доступу:
- резервне копіювання даних.

Очікувані результати проекту:

- покращений рівень безпеки мережі Global IT Solutions Inc.
- зменшення ризику несанкціонованого доступу до конфіденційної інформації.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 25   |

- забезпечення високої доступності мережесервісів.
- зниження ймовірності виникнення загроз інформаційній безпеці.
- забезпечення можливості відновлення мережевої інфраструктури у разі непередбачених ситуацій.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                          | 26   |

## ВИСНОВОК ДО РОЗДІЛУ 1

У даному розділі були розглянуті загрози та вразливості, які можуть вплинути на безпеку корпоративних мереж. Відомо, що корпоративні мережі в сучасному інформаційному середовищі стають об'єктом постійних атак та спроб несанкціонованого доступу, що може призвести до значних наслідків для організації та її інформаційної безпеки. Дослідження цих загроз та вразливостей виявило необхідність розробки комплексних стратегій та методів захисту корпоративних мереж.

Загрози, такі як кібератаки, поширення вірусів та шкідливих програм, виток інформації та фізичні загрози, вимагають від організацій ретельної підготовки та впровадження ефективних заходів захисту. Недостатній контроль доступу, застаріле програмне забезпечення, недостатні заходи шифрування, недостатня кваліфікація персоналу та недостатній моніторинг та аудит безпеки можуть стати вразливостями, через які загрози можуть проникнути в мережу.

Основні методи традиційного захисту мережі, такі як використання файрволів, віртуальних приватних мереж, систем виявлення та запобігання вторгнення, антивірусного програмного забезпечення, контролю доступу, шифрування даних та безперервного моніторингу, є важливими елементами для забезпечення безпеки інформаційних систем.

Сучасні підходи до кібербезпеки, такі як використання машинного навчання та штучного інтелекту, аналіз мережевої поведінки, підписант-незалежні технології, хмарна кібербезпека, безпека Інтернету речей, використання blockchain технологій та біометричних методів аутентифікації, свідчать про постійний розвиток і вдосконалення підходів до захисту мереж.

Основними принципами сучасних підходів до кібербезпеки є превентивні заходи, виявлення та реакція на загрози, а також активний моніторинг і аналіз. Ці підходи вимагають інтегрованого підходу, що об'єднує технологічні, організаційні та освітні аспекти для забезпечення ефективного захисту корпоративних мереж від сучасних та майбутніх загроз кібербезпеки.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 27   |

## РОЗДІЛ 2 ПРОЕКТУВАННЯ ТА РОЗРОБКА ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

### 2.1 Опис симулятора Cisco Packet Tracer

Cisco Packet Tracer – це програма для моделювання мережевих схем і протоколів, розроблена компанією Cisco Systems. Вона широко використовується в академічних середовищах, особливо для навчання та навчання студентів та професіоналів інформаційних технологій.

Основною метою Cisco Packet Tracer є надання можливості візуального та практичного моделювання мережевих конфігурацій, включаючи комутатори, маршрутизатори, кабелі, комп'ютери, сервери, IP-телефони та інші мережеві пристрої. Вона дозволяє створювати складні мережеві топології, імітувати різні мережеві протоколи та перевіряти їх роботу в інтерактивному режимі.

Основні можливості Cisco Packet Tracer:

1. Створення мережевої топології: Користувачі можуть вирізати і вставляти різні мережеві пристрої з палітри і розташовувати їх у потрібному порядку для створення бажаної мережевої топології.

2. Налаштування пристроїв: Користувачі можуть налаштовувати різні параметри пристроїв, такі як IP-адреси, маршрутизацію, VLAN, безпеку та інші налаштування, які використовуються для побудови функціональної мережі.

3. Симуляція мережевих протоколів: Cisco Packet Tracer надає можливість перевіряти роботу різних мережевих протоколів, таких як OSPF, EIGRP, RIP, STP та інші, що дозволяє користувачам розуміти, як вони взаємодіють у реальному середовищі.

4. Побудова Інтернет-мережі: Крім локальних мереж, Cisco Packet Tracer дозволяє створювати підключення до Інтернету та моделювати роботу мережі з використанням публічних IP-адрес.

5. Відлагодження та налагодження: Cisco Packet Tracer дозволяє користувачам відлагоджувати та налагоджувати мережеві проблеми, щоб знайти та виправити неполадки в мережевій конфігурації.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 28   |

6. Візуалізація даних: В програмі присутні інструменти для візуалізації трафіку, що допомагає аналізувати та моніторити даних у мережі.

7. Навчальні матеріали: Крім інтерактивної моделювання мереж, Cisco Packet Tracer містить також навчальні матеріали, включаючи інтерактивні курси, документацію та демонстраційні сценарії, які допомагають в оволодінні основами мережевих технологій та протоколів.

Загалом, Cisco Packet Tracer є потужним інструментом для навчання, тестування та експериментів з мережевими технологіями, що дозволяє користувачам здійснювати практичне моделювання мережевих сценаріїв і вдосконалювати свої навички у сфері інформаційних технологій.

Унікальною особливістю даного симулятора є наявність в ньому режиму симуляції (рис. 2.4). Під час використання цього режиму, всі пакети, які передаються в мережі, ілюструються графічно. Така можливість дозволяє студентам чітко відображати маршрут пакетів у даному моменті, а також використані протоколи. Працюючи в іншому режимі, такому як режим реального часу, неможливо візуально відстежити переміщення пакетів, і відразу ж відображається кінцевий результат здійснених дій.

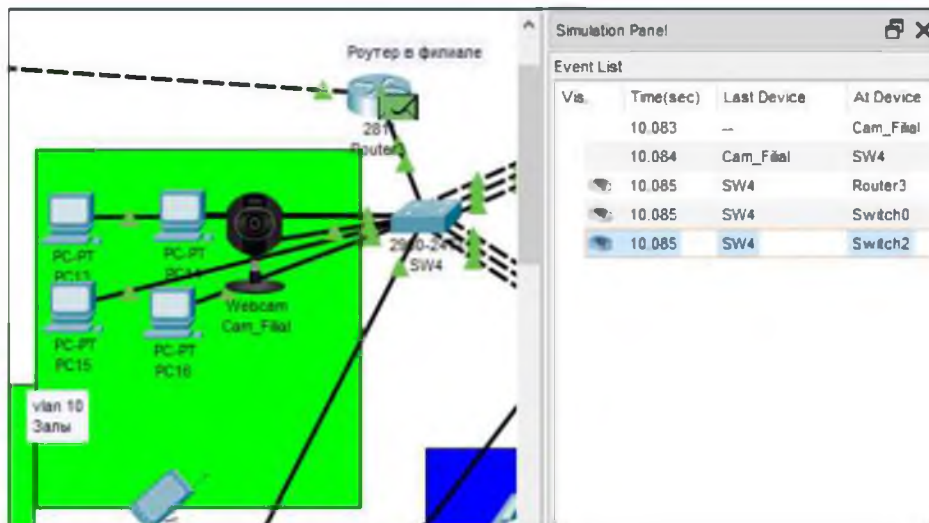


Рисунок 2.1 – Режим симуляції в Packet Tracer

Однак, переваги Cisco Packet Tracer не обмежуються лише можливістю відслідковування використовуваних протоколів. В режимі симуляції студент може

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 29   |

також бачити, на якому з семи рівнів моделі OSI даний протокол задіяний, а також отримувати доступ до вмісту пакета та його формату. Packet Tracer здатний моделювати значну кількість пристроїв різного призначення, включаючи комутатори другого і третього рівнів, маршрутизатори, мережеві концентратори, кінцеві пристрої, бездротові пристрої та глобальні мережі WAN, що дозволяє проектувати мережі будь-якого розміру з високим рівнем складності [5].

В симуляторі моделюються різні типи пристроїв, такі як комутатори другого і третього рівнів, маршрутизатори, мережеві концентратори, кінцеві пристрої (такі як робочі станції, ноутбуки, сервери, принтери), бездротові пристрої (включаючи точки доступу та бездротові маршрутизатори) і глобальна мережа WAN. При цьому підтримуються різні типи зв'язків між пристроями, такі як консольні з'єднання, мідні кабелі з прямим та перехрещеним підключенням, волоконно-оптичні кабелі, телефонні лінії та серійні з'єднання DCE/DTE.

Кожен пристрій в програмному продукті Cisco Packet Tracer може бути налаштований через вікно властивостей, яке викликається подвійним кліком на пристрої. Перша вкладка, "Physical" (рис. 2.5), дозволяє налаштовувати фізичні параметри пристрою. При налаштуванні маршрутизаторів і комутаторів можна додавати нові модулі, а для робочих станцій і серверів можна вставляти мережеві адаптери.

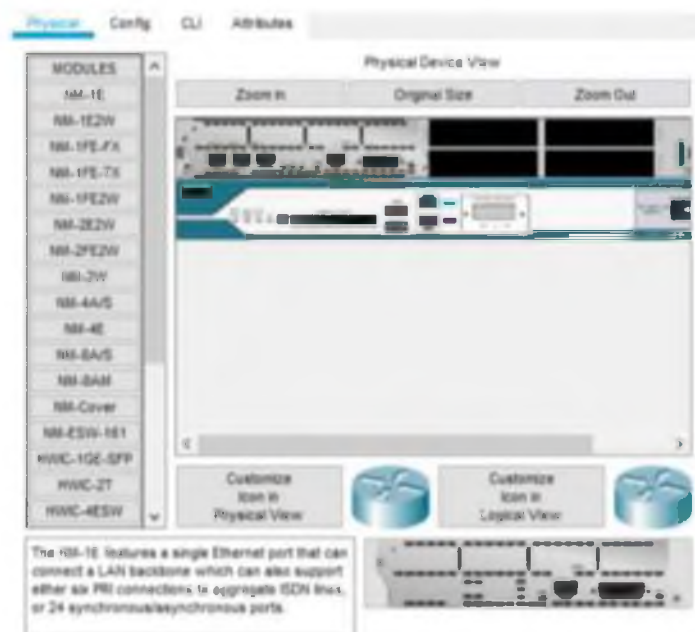


Рисунок 2.2 – Фізичний вигляд пристрою (маршрутизатора)

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 30   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                          |      |

На вкладці Config (рис. 2.6) користувач має можливість встановлювати основні параметри мережевих інтерфейсів, такі як IP-адреси, маски підмережі, параметри бездротової мережі та інші. Крім того, у мережевих пристроях можна налаштовувати маршрутизацію – статичну або динамічну, а в серверах здійснювати налаштування служб.

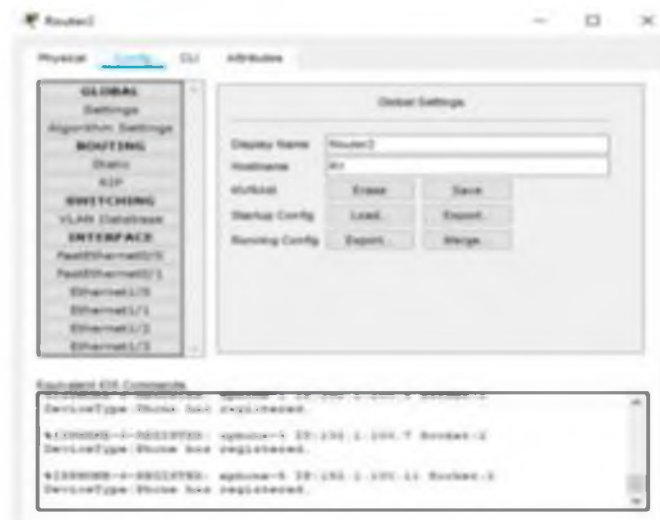


Рисунок 2.3 – Конфігурація сервера

При запуску програми відкривається головне вікно симулятора (рис. 2.7):

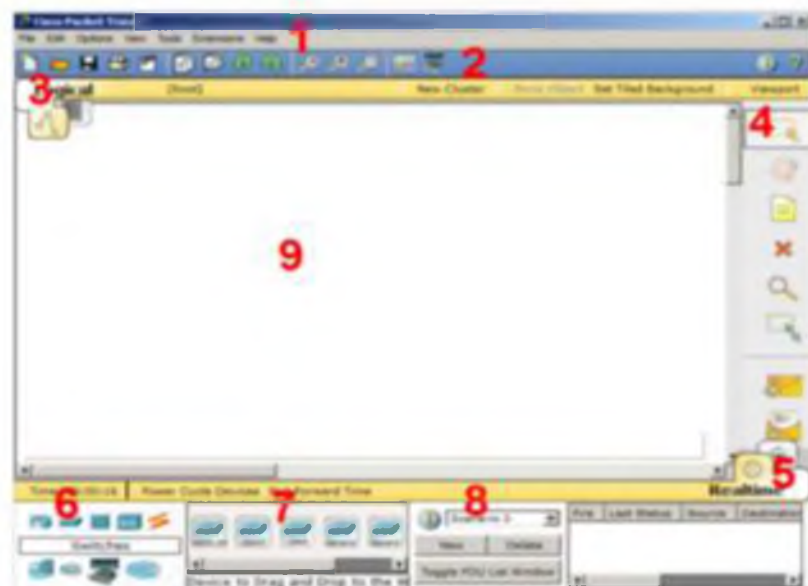


Рисунок 2.4 – Інтерфейс програми Cisco Packet Tracer

Симулятор Packet Tracer підтримує широкий діапазон мережевих з'єднань (Додаток Б). Кожен тип кабелю може бути з'єднаний лише з певним типом інтерфейсу.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 31   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                          |      |

Cisco Packet Tracer – це зручний інструмент для моделювання мереж передачі даних. Робота з цим симулятором надає високо правдоподібне відчуття налаштування реальної мережі з різноманітними пристроями. Налаштування мережевого обладнання можна здійснювати як за допомогою команд операційної системи Cisco IOS, так і через графічний інтерфейс.

Додатково, завдяки режиму симуляції, користувач може простежити переміщення даних по мережі, вивчити процес зміни параметрів пакетів при проходженні через мережеві пристрої, а також дослідити швидкість і шляхи руху пакетів. Аналіз подій, які відбуваються в цій віртуальній мережі, дозволяє зрозуміти механізм її роботи і виявити можливі несправності або недоліки.

## 2.2 Побудова моделі захищеної корпоративної мережі

Проект захищеної корпоративної мережі будується для компанії з галузі інформаційних технологій (IT), що має кілька відділень та діяльність на міжнародному рівні.

“Global IT Solutions Inc.” – це компанія, яка спеціалізується на наданні інформаційних технологій та послуг у всьому світі. У компанії є чотири головні відділення: США, Європа, Азія та Африка, які обслуговують клієнтів з усіх галузей промисловості та бізнесу.

Розміщення мережі:

– Мережа А: Головне відділення в США, яке забезпечує управління всіма глобальними операціями компанії та має доступ до центральних серверів та баз даних.

– Мережа В: Відділення в Європі, яке спеціалізується на розробці програмного забезпечення та інноваційних IT-рішень для клієнтів у регіоні.

– Мережа С: Відділення в Азії, яке забезпечує технічну підтримку та обслуговування клієнтів у Південно-Східній Азії.

– Мережа D: Відділення в Африці, яке фокусується на розвитку IT-інфраструктури та послуг для клієнтів у регіоні.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 32   |

ISP-з'єднання: Усі головні відділення підключені до Інтернету через мережу постачальника послуг Інтернету для забезпечення зв'язку зі світовими клієнтами та інтернет-послугами.

Ця мережа дозволяє “Global IT Solutions Inc.” ефективно керувати своїми глобальними операціями, обмінюватися даними та інформацією між відділеннями, надавати ІТ-послуги клієнтам з усього світу та забезпечувати безпеку та надійність своїх інфраструктур. Мережа забезпечує динамічний розподіл IP-адрес, обмеження доступу до різних ресурсів для забезпечення безпеки та можливість взаємодії між відмінними віртуальними та фізичними мережами підприємства.

Для налаштування корпоративної мережі були використані наступні пристрої:

– Маршрутизатор: В мережі використано 3 маршрутизатори. Перший призначений для мереж А та В, другий - для мережі С, а третій використовується для з'єднання всієї корпоративної мережі з маршрутизатором постачальника Інтернет-послуг. Мережа D підключена до третього маршрутизатора. Також у мережі присутній додатковий маршрутизатор постачальника Інтернет-послуг.

– Комутатор: У мережі використано 4 комутатори. Два з них призначені для створення мереж А та В з використанням VLAN, один - для мережі С, а останній - для мережі D.

– Сервер DHCP: У мережах А та В використовуються 2 сервери DHCP для динамічного призначення IP-адрес. Також у мережі С використовується ще один сервер DHCP.

– Веб- та FTP-сервер: У мережі D розміщений комбінований веб- та FTP-сервер, який забезпечує доступ до веб-ресурсів та FTP-файлів для всієї мережі.

– Сервер DNS: У мережі присутній 1 сервер DNS для всієї мережі, що дозволяє надавати доменні імена для веб-серверу замість доступу за IP-адресою.

Технології, що використовувалися в конфігурації корпоративної мережі:

– Variable Length Subnet Mask (VLSM): Застосовано для розподілу наданого IP-адресного простору 202.195.32.0/24 між різними мережами та зв'язками. Зв'язок між маршрутизатором корпоративної мережі та маршрутизатором постачальника

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 33   |

Інтернет-послуг не входить до схеми підмереж, і для нього використано окрему IP-адресу.

– Віртуальна локальна мережа (VLAN): Використана для створення віртуальних мереж А та В. Міжмережевий маршрутизатор для взаємодії між VLAN реалізовано за допомогою методу "Router-on-a-stick".

– Протокол динамічної конфігурації хостів (DHCP): Використовується для динамічного призначення IP-адрес у мережах А, В та С. Мережа D використовує статичні IP-адреси.

– Протокол Open Shortest Path First (OSPF): Застосований для динамічної маршрутизації в межах корпоративної мережі. З'єднання з маршрутизатором постачальника Інтернет-послуг виконано за допомогою протоколу маршрутизації за замовчуванням.

– Система доменних імен (DNS): Використовується для налаштування DNS та надання доменних імен для веб-сервера замість доступу за IP-адресою.

– Списки контролю доступу (ACL): Використовуються в маршрутизаторах мереж А, В та С для обмеження доступу хостів з відповідних мереж, згідно з вимогами проекту.

Для виконання дипломної роботи була застосована поетапна методологія, виконуючи вимоги проекту крок за кроком. Спочатку була розроблена схема змінної довжини підмереж, перш ніж розміщати різні пристрої у логічному макеті. Схема змінної довжини підмереж була розроблена таким чином:

– Вихідна IP-адресна ділянка: 202.195.32.0/24

– Мережа С - потребує 60 хостів. Тому використовуємо  $\log_2 60$  біт, що дорівнює  $5.9 \approx 6$ . Призначені IP-адреси: 202.195.32.00 000000/26, тобто IP-адреси від 202.195.32.0 до 202.195.32.63.

– Мережа А - потребує 30 хостів. Тому використовуємо  $\log_2 30$  біт, що дорівнює  $4.9 \approx 5$ . Призначені IP-адреси: 202.195.32.010 000000/27, тобто IP-адреси від 202.195.32.64 до 202.195.32.95.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 34   |

– Мережа В - потребує 30 хостів. Тому використовуємо  $\log_2 30$  біт, що дорівнює  $4.9 \approx 5$ . Призначені IP-адреси: 202.195.32.011 00000/27, тобто IP-адреси від 202.195.32.96 до 202.195.32.127.

– Мережа D - потребує 12 хостів. Тому використовуємо  $\log_2 12$  біт, що дорівнює  $3.58 \approx 4$ . Призначені IP-адреси: 202.195.32.1000 0000/28, тобто IP-адреси від 202.195.32.128 до 202.195.32.143.

– Зв'язки SL1, SL2 та SL3 - в підмережах використовуються 2 біти. Відповідні IP-адреси: 202.195.32.100100 00/30, 202.195.32.100101 00/30 та 202.195.32.100110 00/30, тобто IP-адреси від 202.195.32.144 до 202.195.32.155.

Після розробки цієї схеми були розміщені всі мережі одна за одною. Віртуальні локальні мережі А та В були налаштовані за допомогою комутаторів 1 та 2, і між ними було встановлено транк-з'єднання для забезпечення взаємодії між VLAN, розподіленими по обох комутаторах.

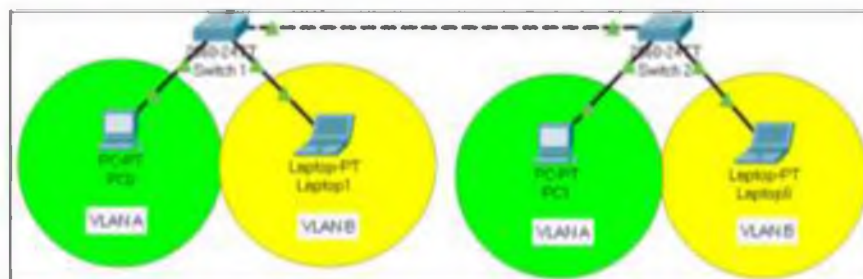


Рисунок 2.5 – Схема взаємодії VLAN A та VLAN B

На цьому етапі VLAN A та VLAN B можуть взаємодіяти в межах своїх мереж, але ще неможлива між-VLAN комунікація. Це досягається за допомогою методу маршрутизації між-VLAN на основі “Router-on-a-stick”, при якому один з роутерів підключається до одного з комутаторів, створюючи загальний транк, через який роутер дозволяє пакетам проходити з одного VLAN до іншого.

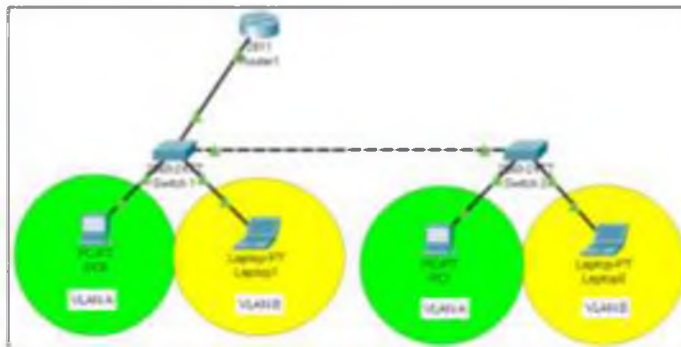


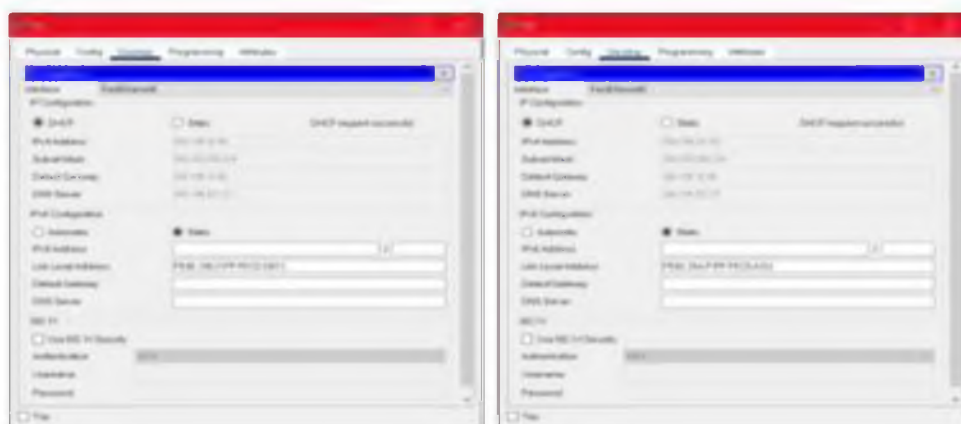
Рисунок 2.6 – Метод "Router-on-a-stick" для маршрутизації між-VLAN

Однак, на відповідному роутері потрібно налаштувати деякий CLI-код для дозволу між-VLAN маршрутизації, що наведено в додатку. Після цього кроку, DHCP-сервер приєднується до комутатора 2, і динамічний розподіл IP-адрес у мережах А та В налаштовується наступним чином:



Рисунок 2.7 – Налаштування між-VLAN маршрутизації та DHCP на комутаторі 2

У цьому випадку створено два пули серверів: serverPool 1 з шлюзом 202.195.32.66 та serverPool 2 з шлюзом 202.195.32.98, які обслуговують мережі А та В відповідно. Динамічний розподіл IP-адрес вдалий, як показано в розділі конфігурації IP цих комп'ютерів.



PC from Network A

Laptop from Network B

Рисунок 2.8 – Розділена серверна пула для мереж А та В

Тепер створено фізичну мережу С, яка включає комутатор, маршрутизатор, ПК, ноутбук та DHCP-сервер. Маршрутизатор використовується для підключення до майбутнього маршрутизатора мереж А та В, а також до маршрутизатора Enterprise (який буде налаштований пізніше) та для надання стандартного шлюзу для мережі С. Тут також потрібна динамічна розподіл адрес, і DHCP-сервер налаштований так само, як і в попередніх мережах. Мережа формується наступним чином:

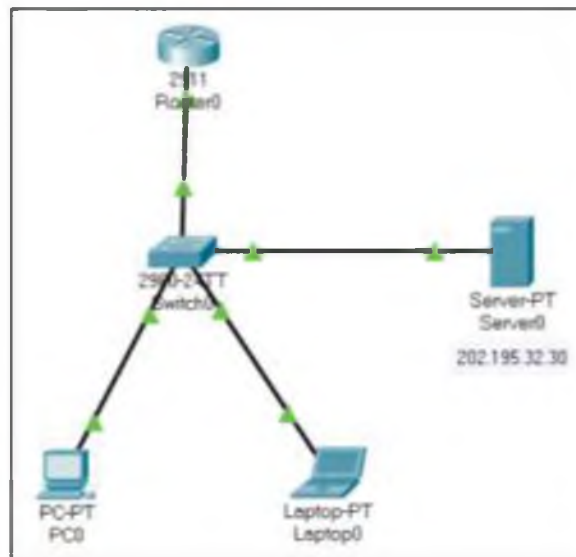
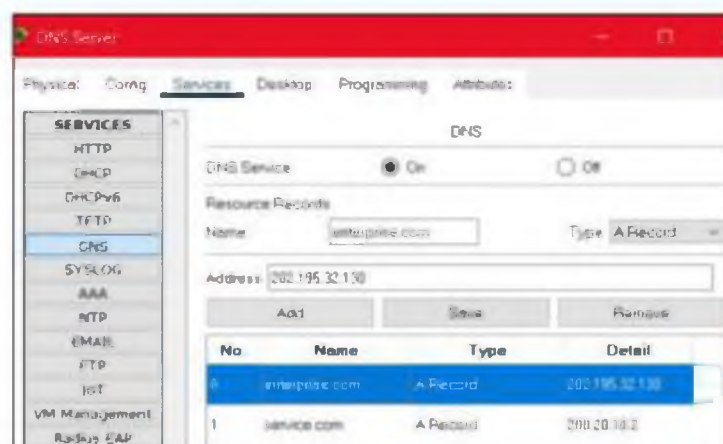


Рисунок 2.9 – Мережа С з маршрутизатором та комутатором

Далі, створено мережу D з маршрутизатором Enterprise, комутатором, двома серверами та ноутбуком. Один з серверів перетворено на DNS-сервер, а інший - на комбінований веб-сервер та FTP-сервер. Налаштування в кожному з них просте і проілюстровано нижче:



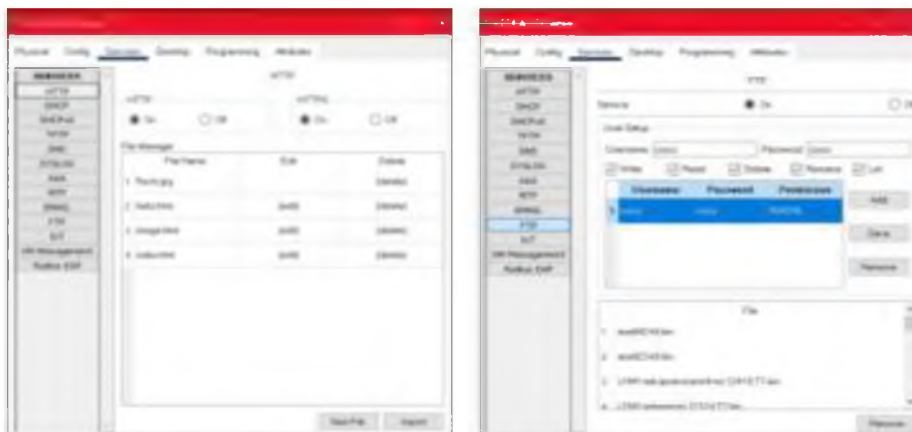
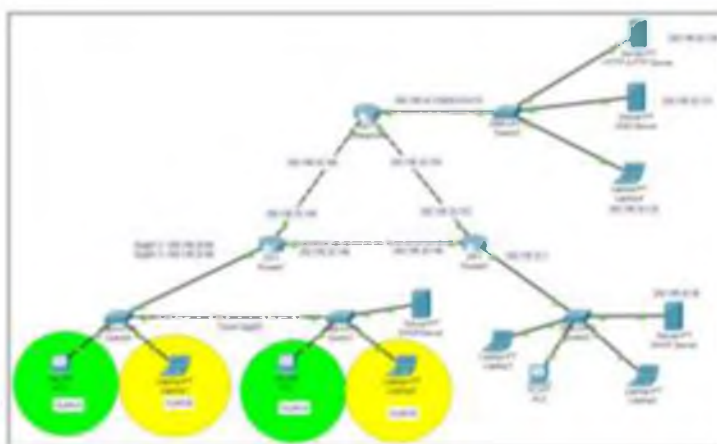


Рисунок 2.10 – Мережа D з маршрутизатором Enterprise, комутатором, DNS-сервером, комбінованим веб-сервером та FTP-сервером

У мережі D було використано статичні IP-адреси, на відміну від попередніх трьох мереж. Це зроблено для того, щоб IP-адреси серверів були статичними і їх можна було використовувати для доступу до веб-сервера та FTP-сервера для доступу до Інтернету та обміну файлами. Крім того, DNS-сервер потрібен для розпізнавання IP-адреси інших серверів за доменними іменами. Тепер чотири мережі мають бути маршрутизовані разом, щоб обмінюватися інформацією (пакетами) одна з одною. Маршрутизатори з'єднані між собою за допомогою ланок SL1, SL2 та SL3. В якості протоколу динамічної маршрутизації в межах мережі підтримується OSPF, і він налаштований у кожному з маршрутизаторів за допомогою деяких команд CLI, наданих у додатку. До цього моменту мережа мала логічну структуру, як показано нижче, і всі мережі можуть взаємодіяти та обмінюватися пакетами одна з одною.



## Рисунок 2.11 –Інтеграція мереж з використанням OSPF як протоколу динамічної маршрутизації

Мережу під'єднано до маршрутизатора постачальника послуг (ISP), на якому розташований веб-сервер (HTTP). З'єднання з ISP виконано за допомогою послідовного з'єднання, тому що порти Ethernet уже використані для підключення до всіх попередніх мереж. Мережа підприємства має стандартний маршрут до маршрутизатора ISP для відправки всіх пакетів, адресованих IP-адресам, що не доступні в мережі підприємства.

Завершальним етапом є накладання обмежень на хости мереж А, В та С за допомогою списків керування доступом (ACL). ACL налаштовані для інтерфейсів маршрутизаторів, до яких підключені ці мережі. У VLAN А обмеження доступу до мережі може призвести до того, що вона навіть не зможе спілкуватися з DHCP-сервером для динамічного призначення IP-адрес. Тому ACL був налаштований так, щоб враховувати DHCP-сервер. Всі команди CLI, пов'язані з налаштуванням ACL, наведені в додатку.

### 2.3 Налаштування захисту корпоративної мережі

З метою забезпечення надійного захисту корпоративної мережі “Global IT Solutions Inc.”, необхідно детально розглянути різноманітні технології та практики, спрямовані на забезпечення високого рівня безпеки. Важливість ефективного захисту від сучасних кіберзагроз та небезпек важко переоцінити, і лише широкий спектр заходів може гарантувати захист від потенційних ризиків. В цьому контексті варто ретельно розглянути наступні принципи та практики, які допоможуть забезпечити цілісність та конфіденційність важливих даних та ресурсів компанії.

Для захисту корпоративної мережі ми налаштували аутентифікацію на роутерах для обмеження доступу до настройки мережі.

Конкретні кроки, які були виконані для налаштування аутентифікації на роутерах, включають:

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 39   |

1. Було увійдено в командний інтерфейс кожного роутера використовуючи програмне забезпечення Cisco Packet Tracer.

2. Налаштування паролю для привілейованого режиму було здійснено за допомогою команди `enable secret <пароль>`, де `<пароль>` - це обраний пароль для привілейованого режиму доступу.

3. Налаштування паролю для режиму конфігурації було виконано за допомогою команди `line console 0`, після чого було встановлено пароль за допомогою команди `password <пароль>`, де `<пароль>` - обраний пароль для входу в режим привілейованого конфігурації. Крім того, було використано команду `login` для активування процесу аутентифікації.

4. Після налаштування паролів, було збережено конфігурацію за допомогою команди `#write memory`, що дозволяє зберігати настройки і застосовувати їх після перезавантаження роутера.

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#password password
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#write memory
```

Рисунок 2.12 – Налаштування паролю для привілейованого режиму

Таким чином, в результаті успішної реалізації цих кроків, на кожному роутері були встановлені паролі для привілейованого режиму та режиму конфігурації. Це додало додатковий рівень захисту до корпоративної мережі, оскільки тепер доступ до настройок роутерів заборонено без правильного введення відповідних паролів.

Для забезпечення надійного захисту корпоративної мережі, ми успішно використали такі стратегії та технології:

1. VLAN і сегментація мережі: Ми розробили та впровадили структуру віртуальних LAN (VLAN), що дозволило нам ефективно розділити мережу на окремі сегменти. Зокрема, ми використали VLAN для сегментації мережі на VLAN А та VLAN В, обмеживши взаємодію між ними. Ця практика значно підвищила

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 40   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

безпеку, адже обмеження взаємодії між VLAN знижує ризик перетоку даних та можливість злому з одного сегмента мережі до іншого.

2. Метод “Router-on-a-stick”: Для забезпечення комунікації між різними VLAN ми використали метод “Router-on-a-stick”. Цей підхід дозволив нам налаштувати роутер для маршрутизації пакетів між VLAN, дозволяючи контролювати потік трафіку та забезпечити безпеку при обміні даними між різними сегментами мережі.

Ці стратегії та технології допомогли нам створити ефективний захист мережі, знижуючи можливість злому та несанкціонованому доступу. Використання VLAN та методу “Router-on-a-stick” в сукупності з іншими заходами створює високий рівень безпеки, який відповідає сучасним стандартам та вимогам до захисту корпоративних мереж.

Для налаштування файрволу в Cisco Packet Tracer можна використовувати список керування доступом (ACL). ACL дозволяє контролювати потік трафіку на інтерфейсах маршрутизаторів та комутаторів, дозволяючи або блокуючи певні типи трафіку на основі визначених правил.

Переходячи до ефективних методів захисту, розглянемо такі можливості:

1. Блокування небезпечних протоколів: Список керування доступом (ACL) може бути налаштований для блокування небезпечних протоколів, таких як ICMP (Ping) або Telnet, які можуть стати джерелом атак або зламу мережі. Наприклад, ACL може блокувати вхідні ICMP-запити, забороняючи пінгування мережевих пристроїв ззовні.

Для цього потрібно необхідно виконати наступні команди:

```
Router(config)# access-list 1 deny icmp any any
Router(config)# access-list 1 permit ip any any
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip access-group 1 in
```

2. Контроль доступу до сервісів: ACL може дозволяти або блокувати доступ до певних сервісів чи портів. Наприклад, можна налаштувати ACL таким чином, щоб дозволити доступ до важливих служб, таких як HTTP (порт 80) або HTTPS (порт 443), та блокувати небезпечні порти, які не повинні бути відкриті для публічного доступу.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 41   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

Для захисту корпоративної мережі ми реалізували наступні заходи за допомогою списків доступу (ACL) на маршрутизаторі RouterD:

1. Створення списку доступу ACL 101:

```
RouterD(config)# access-list 101 permit udp any eq bootpc any eq bootps
RouterD(config)# access-list 101 deny ip any any
RouterD(config)# access-list 101 deny ip 192.168.2.0 0.0.0.255 any
RouterD(config)# access-list 101 permit ip any any
```

2. Призначення списку доступу ACL 101 на інтерфейсі GigabitEthernet0/2 для фільтрації вхідного трафіку:

```
RouterD(config)# interface GigabitEthernet0/2
RouterD(config-if)# ip access-group 101 in
```

Перші два правила ACL 101 дозволяють UDP-трафік між портами bootpc та bootps, який використовується для протоколу DHCP (Dynamic Host Configuration Protocol) для надання IP-адрес клієнтам. Це дозволяє правильне функціонування DHCP в мережі.

Третє правило в ACL 101 є “загальним відхиленням” (deny ip any any). Воно забороняє всі інші типи IP-трафіку, який не був відповідним з попередніми правилами. Це дозволяє захистити мережу, блокуючи весь неавторизований трафік.

Четверте правило в ACL 101 (deny ip 192.168.2.0 0.0.0.255 any) забороняє IP-трафік з підмережі 192.168.2.0/24 до будь-якої адреси. Це дозволяє обмежити доступ до цієї конкретної підмережі зовнішніх користувачів і може використовуватися для захисту окремої частини мережі.

Останнє правило ACL 101 (permit ip any any) є “загальним дозволом”. Воно дозволяє всім іншим типам IP-трафіку, який не заборонений попередніми правилами. Це гарантує, що легітимний трафік від і до будь-яких адрес не буде заблокований.

Ці налаштування забезпечують захист мережі шляхом блокування небажаного трафіку та дозволу лише необхідних типів комунікації.

3. Забезпечення конфіденційності: ACL може блокувати доступ до певних ресурсів або послуг для зовнішнього трафіку, забезпечуючи конфіденційність інформації та даних в мережі. Шляхом використання розширених списків доступу,

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 42   |

ми можемо створити додатковий рівень захисту та заборонити зовнішньому трафіку доступ до конкретних ресурсів.

Що стосується забезпечення конфіденційності, ось як можна це реалізувати з використанням розширених списків доступу:

1. Створюємо розширений список доступу, який блокуватиме конкретну IP-адресу 203.0.113.10:

```
Router(config)# access-list 102 deny ip host 203.0.113.10 any
```

2. Додаємо правило, яке дозволить всім іншим IP-адресам проходити:

```
Router(config)# access-list 102 permit ip any any
```

3. Застосовуємо створений розширений список доступу до інтерфейсу GigabitEthernet0/3 на вхідних пакетах:

```
Router(config)# interface GigabitEthernet0/3
```

```
Router(config-if)# ip access-group 102 in
```

За допомогою цих команд створюється розширений список доступу з номером 102, який блокує конкретну IP-адресу 203.0.113.10 і дозволяє всім іншим IP-адресам проходити через інтерфейс GigabitEthernet0/3.

4. Заборона несанкціонованого доступу: Завдяки ACL можна дозволити лише певним IP-адресам або діапазонам IP-адрес отримувати доступ до важливих мережевих ресурсів чи пристроїв, що допомагає забезпечити безпеку мережі.

Щоб реалізувати заборону доступу до певних ресурсів ззовні, необхідно змінити список доступу так, щоб він блокував трафік, який приходить зовнішніми IP-адресами до внутрішнього IP-адреси 192.168.1.10 на порту 22 (SSH):

1. Створюємо розширений список доступу, який блокуватиме SSH-з'єднання з зовнішніх IP до IP-адреси 192.168.1.10 на порту 22 (SSH):

```
Router(config)# access-list 103 deny tcp any host 192.168.1.10 eq 22
```

2. Додаємо правило, яке дозволить всім іншим IP-адресам проходити:

```
Router(config)# access-list 103 permit ip any any
```

3. Застосовуємо створений розширений список доступу до інтерфейсу GigabitEthernet0/4 на вхідних пакетах:

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 43   |

```
4. Router(config)# interface GigabitEthernet0/4
```

```
Router(config-if)# ip access-group 103 in
```

За допомогою використання цих команд створюється розширений список доступу з номером 103, який блокує SSH-з'єднання з зовнішніх IP до внутрішнього IP-адреси 192.168.1.10 на порту 22 (SSH), а всім іншим IP-адресам дозволяє проходити через інтерфейс GigabitEthernet0/4.

Послідовність дій при налаштуванні ACL для файрволу в Packet Tracer полягає в створенні правил блокування або дозволу трафіку, їх прив'язку до відповідних інтерфейсів маршрутизатора або комутатора та збереженні налаштувань. Після цього файрвол готовий до застосування і забезпечує контроль трафіку в мережі.

Налаштуємо VPN між двома маршрутизаторами Cisco.

Кроки налаштування Site-to-Site VPN в Cisco Packet Tracer:

1. Перевіряємо мережеві налаштування: Необхідно переконатися, що мережеві параметри (IP-адреси, маски підмережі тощо) налаштовані правильно для обох маршрутизаторів (Router A та Router B).

2. Генерування ключів: На обох маршрутизаторах потрібно згенерувати ключі шифрування, які будуть використовуватись для захищеного з'єднання. Виконаємо наступні команди на кожному маршрутизаторі:

```
RouterA# configure terminal
```

```
RouterA(config)# crypto key generate rsa general-keys modulus 1024
```

```
RouterA(config)# end
```

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname RouterA
RouterA(config)#ip domain-name mycompany.com
RouterA(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: RouterA.mycompany.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable... [OK]
*Mar 1 1:14:06.381: %SSH-5-ENABLED: SSH 1.99 has been enabled
RouterA(config)#
```

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 44   |

```

Switch(config)#crypto key generate rsa general-keys modulus 1024
% Please define a hostname other than Switch.
Switch(config)#hostname RouterB
RouterB(config)#crypto key generate rsa general-keys modulus 1024
% Please define a domain-name first.
RouterB(config)#ip domain-name networklab.com
RouterB(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: RouterB.networklab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 1:3:8.405: %SSH-5-ENABLED: SSH 1.99 has been enabled
RouterB(config)#

```

Рисунок 2.13 – Генерування ключів на маршрутизаторах

### 3. Налаштування IPsec VPN:

Необхідно виконати налаштування IPsec VPN на обох маршрутизаторах. Для Router A введемо такі команди:

```

RouterA# configure terminal
RouterA(config)# crypto isakmp policy 1
RouterA(config-isakmp)# encr aes
RouterA(config-isakmp)# hash sha256
RouterA(config-isakmp)# authentication pre-share
RouterA(config-isakmp)# group 2
RouterA(config-isakmp)# exit

```

```

RouterA(config)# crypto isakmp key mysharedkey address <IP Router B>
RouterA(config)# exit

```

Аналогічні команди потрібно виконати і для Router B.

4. Визначення тунельних інтерфейсів: Визначаємо інтерфейси, які будуть використовуватись для VPN-тунелю на обох маршрутизаторах:

```

Router(config)# interface Tunnel0
Router(config-if)# ip address 192.168.1.2 255.255.255.0
Router(config-if)# tunnel source GigabitEthernet0/2
Router(config-if)# tunnel destination 202.195.32.129
Router(config-if)# exit

```

```

Router(config)# interface Tunnel0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# tunnel source GigabitEthernet0/0

```

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 45   |

```
Router(config-if)# tunnel destination 202.195.32.149
Router(config-if)# exit
```

5. Налаштування маршрутизації: Визначаємо, які мережі будуть перенаправлені через VPN-тунель. Налаштуємо маршрутизацію для тунельних інтерфейсів на обох маршрутизаторах:

```
RouterA# configure terminal
RouterA(config)# ip route 192.168.2.0 255.255.255.0 Tunnel0
RouterA(config)# exit
```

```
RouterB# configure terminal
RouterB(config)# ip route 192.168.1.0 255.255.255.0 Tunnel0
RouterB(config)# exit
```

VPN-тунель працює належним чином, ми отримали відповідь від комп'ютера на іншому маршрутизаторі.

За допомогою цих кроків ми налаштували VPN із захищеним тунелем між двома маршрутизаторами. Кожен пакет, який буде передаватися між мережами, буде зашифрований та захищений, забезпечуючи безпеку обміну даними між мережами А та В.

Для налаштування віддаленого доступу до мережевих пристроїв Cisco Packet Tracer необхідно виконати наступні кроки:

1. Створимо ключі SSH на маршрутизаторі. Виконаємо команду:

```
Router(config)# crypto key generate rsa
```

Вибираємо розмір ключа, наприклад, 1024 біти або більше.

2. Увімкнемо SSH на маршрутизаторі:

```
Router(config)# ip ssh version 2
Router(config)# line vty 0 4
Router(config-line)# transport input ssh
```

3. Встановимо ім'я користувача та пароль для віддаленого доступу:

```
Router(config)# username ваше_ім'я_користувача secret ваш_пароль
```

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 46   |

Тепер SSH має бути налаштований для віддаленого доступу до маршрутизатора.

Використання SSH для віддаленого доступу є більш безпечним способом порівняно з Telnet, оскільки SSH забезпечує шифрування даних під час передачі. Тому рекомендується використовувати SSH для віддаленого управління мережевими пристроями.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto key generate rsa
% Please define a hostname other than Router.
Router(config)#hostname RouterE
RouterE(config)#crypto key generate rsa
% Please define a domain-name first.
RouterE(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
RouterE(config)#line vty 0 4
RouterE(config-line)#transport input ssh
RouterE(config-line)#username admin password
^
% Invalid input detected at '^' marker.

RouterE(config-line)#username admin secret password
RouterE(config)#
```

Рисунок 2.14 – Налаштування віддаленого доступу до мережевих пристроїв

Додаткові заходи безпеки для захисту віддаленого доступу SSH можуть значно підвищити рівень безпеки корпоративної мережі. Ось детальний опис кроків для реалізації цих заходів:

– Обмеження невдалих входів

Створюємо список контролю доступу для захисту SSH:

```
RouterE(config)# ip access-list standard SSH-ACL
RouterE(config-std-nacl)# permit host 202.195.32.146
```

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 47   |

Використаємо команду “login block-for” для блокування входів після певної кількості невдалих спроб.

```
RouterE(config)# login block-for 120 attempts 3 within 60
```

Тепер використаємо списки контролю доступу (ACL) для обмеження доступу до пристрою через SSH. Так як ми вже створили список контролю доступу “SSH-ACL” з дозволом доступу лише для конкретних IP-адрес. Тепер потрібно прив’язати цей список до протоколу SSH з допомогою команди “transport input ssh”:

```
RouterE(config-line)# line vty 0 4
RouterE(config-line)# transport input ssh
RouterE(config-line)# access-class SSH-ACL in
```

Використавши такі команди ми обмежили доступ до пристрою через SSH для тих IP-адрес, які вказані у списку контролю доступу SSH-ACL.

Завершивши ці кроки, конфігурація безпеки SSH буде підвищена, і доступ до маршрутизатора через SSH буде обмежений за допомогою списку контролю доступу.

### Створення ключової пари

В Cisco Packet Tracer, ми не можемо створити ключову пару за допомогою командного рядка, оскільки Cisco Packet Tracer є симулятором мережевого обладнання і не має повноцінного операційного середовища, яке підтримує генерацію ключових пар.

Однак, ми можемо створити ключову пару на своєму комп’ютері, а потім завантажити публічний ключ на Cisco Packet Tracer за допомогою GUI. Для цього нам потрібно:

1. Створити ключову пару на своєму комп’ютері за допомогою команди ssh-keygen в командному рядку.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 48   |

```
C:\Users\HP>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\HP\.ssh/id_rsa):
Created directory 'C:\Users\HP\.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\HP\.ssh/id_rsa.
Your public key has been saved in C:\Users\HP\.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:LaAjuHyluxFrM0mKcjbFP3bAqFVsZUZCNi4R7tDYn90 hp@DESKTOP-7T5CE3K
The key's randomart image is:
```

Рисунок 2.15 – Створення ключової пари

2. Зберегти приватний ключ на своєму комп'ютері з конфіденційністю. Ми зможемо використовувати цей приватний ключ для аутентифікації під час SSH-з'єднань.

Для того щоб зберегти приватний ключ з конфіденційністю, необхідно виконати наступні кроки:

1. Зайти до папки .ssh у домашній директорії. Зазвичай це C:\Users\Ваш\_Ім'я\_Користувача.ssh.

2. Знайти файл “id\_rsa” – приватний ключ.

3. Скопіювати файл “id\_rsa” в безпечне і захищене місце на комп'ютері. Наприклад, можна створити окрему папку, яку захистити паролем.

4. Запам'ятати місце збереження приватного ключа, і переконатися, що він зберігається в надійному місці.

5. Не ділитися приватним ключем з іншими особами і не зберігайте його на загальнодоступних або ненадійних пристроях.

Потрібно зберегти свій приватний ключ таким чином, щоб можна було зручно використовувати його для аутентифікації під час SSH-з'єднань, але при цьому потрібно забезпечити максимальний рівень конфіденційності та безпеки для ключа.

3. Для налаштування віддаленого доступу за допомогою публічного ключа SSH в Cisco Packet Tracer, необхідно виконати наступні кроки:

а. Увійти до конфігураційного режиму маршрутизатора:

RouterE# conf t

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 49   |

b. Включити аутентифікацію через публічний ключ на VTY лініях:

```
RouterE(config)# ip ssh pubkey-chain
```

Встановити доменне ім'я для маршрутизатора, наприклад:

```
RouterE(config)# ip domain-name cybersecuritylab.com
```

Потім згенерувати RSA-ключі: RouterE(config)# crypto key generate rsa

Це дасть можливість успішно створити RSA-ключі на маршрутизаторі. Після цього можемо додавати публічний ключ SSH.

Процес генерації ключів показаний на рис. 2.16.

```
RouterE(config)#crypto key generate rsa
% Please define a domain-name first.
RouterE(config)#ip domain-name cybersecuritylab.com
RouterE(config)#crypto key generate rsa
The name for the keys will be: RouterE.cybersecuritylab.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

RouterE(config)#
```

Рисунок 2.16 – Генерація RSA-ключів на маршрутизаторі RouterE

Ми встановили ім'я користувача “Danilo” та активували SSH на маршрутизаторі:

1. Використаємо команду “username Danilo” для створення акаунта користувача.

2. Маршрутизатор повідомить про активацію SSH протоколу.

Тепер у нас є акаунт “Danilo” та активований SSH 2 для віддаленого доступу.

Налаштування списків контролю доступу (ACL) для SSH:

1. Встановимо обмеження на доступ SSH через інтерфейси VTY:

1. Збережемо налаштування: RouterE# write memory

2. Перезавантажимо маршрутизатор: RouterE# reload

Підключення через SSH та зміна порту:

1. Після перезавантаження, підключимося через SSH з IP-адресою 192.168.1.2.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 50   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

3. Щоб змінити порт SSH, потрібно ввести команди:

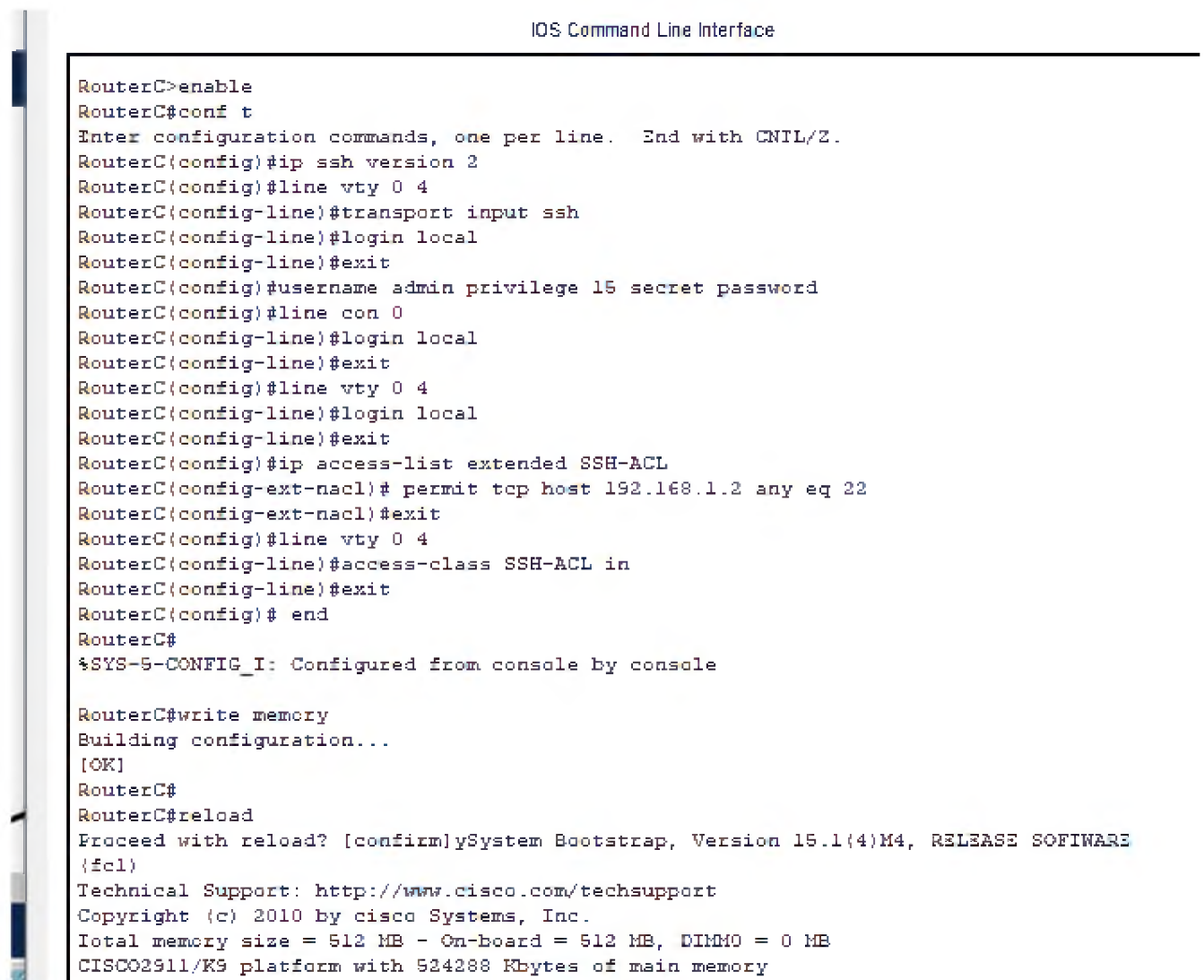
```
RouterC(config)# line vty 0 4
RouterC(config-line)# transport input ssh
RouterC(config-line)# rotary 1
```

Змінюємо IP-адресу в access-list 1 permit host на ту, з якої підключається.

Додаємо access-class 1 in для аутентифікації за допомогою ACL.

Додаємо login local для локальної аутентифікації.

2. Зберігаємо налаштування: RouterC(config)# end RouterC# write memory



```
IOS Command Line Interface

RouterC>enable
RouterC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterC(config)#ip ssh version 2
RouterC(config)#line vty 0 4
RouterC(config-line)#transport input ssh
RouterC(config-line)#login local
RouterC(config-line)#exit
RouterC(config)#username admin privilege 15 secret password
RouterC(config)#line con 0
RouterC(config-line)#login local
RouterC(config-line)#exit
RouterC(config)#line vty 0 4
RouterC(config-line)#login local
RouterC(config-line)#exit
RouterC(config)#ip access-list extended SSH-ACL
RouterC(config-ext-nacl)# permit tcp host 192.168.1.2 any eq 22
RouterC(config-ext-nacl)#exit
RouterC(config)#line vty 0 4
RouterC(config-line)#access-class SSH-ACL in
RouterC(config-line)#exit
RouterC(config)# end
RouterC#
%SYS-5-CONFIG_I: Configured from console by console

RouterC#write memory
Building configuration...
[OK]
RouterC#
RouterC#reload
Proceed with reload? [confirm]ySystem Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE
(fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by Cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2911/K9 platform with 524288 Kbytes of main memory
```

Рисунок 2.17 – Налаштування підключення через SSH

Після перезавантаження маршрутизатора налаштування SSH будуть активні, і SSH-з'єднання з локального комп'ютера з IP-адресою 192.168.1.2 будуть дозволені.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 51   |

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 52   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                          |      |

## ВИСНОВОК ДО РОЗДІЛУ 2

Підсумовуючи проведену дослідницьку роботу, нами була розроблена та реалізована корпоративна мережа для "Global IT Solutions Inc.", світової компанії, що спеціалізується на наданні інформаційних технологій та послуг. Розподілена мережа включає головне відділення у США (Мережа А), відділення в Європі (Мережа В), Азії (Мережа С) та Африці (Мережа D). Ця інфраструктура дозволяє компанії керувати глобальними операціями, обмінюватися даними та надавати ІТ-послуги клієнтам з усього світу.

Для забезпечення надійного та безпечного функціонування мережі були використані такі стратегії захисту:

1. Автентифікація та авторизація: Впровадження паролів для привілейованого режиму та SSH забезпечує контрольний рівень доступу до системних ресурсів та забезпечує захищений віддалений доступ.

2. Розділення на сегменти: Застосування VLAN та методу "Router-on-a-stick" допомогло розділити мережу на сегменти, знижуючи ризик перетоку даних та небажаної комунікації.

3. Файрвол та керування доступом: Використання списків керування доступом (ACL) дозволило ефективно блокувати небезпечні протоколи та контролювати доступ до мережевих сервісів.

4. Віртуальні приватні мережі (VPN): Використання VPN створило безпечний канал зв'язку між віддаленими відділеннями, гарантуючи захищену передачу даних.

5. Захист від атак із зовнішньої мережі: Застосування технологій та стратегій допомагає захистити мережу від різних кіберзагроз, таких як DDoS-атаки та несанкціонований доступ.

Результати дослідження вказують на те, що впроваджені заходи безпеки забезпечують конфіденційність, цілісність даних та надійний доступ до ресурсів для всіх відділень компанії. Мережа "Global IT Solutions Inc." може ефективно

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 53   |

функціонувати у сучасному цифровому середовищі, забезпечуючи стійкість до різних загроз та відповідність вимогам безпеки.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                          | 54   |

## РОЗДІЛ 3 ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ КОРПОРАТИВНОЇ МЕРЕЖІ

### 3.1 Тестування та перевірка функціональності

У процесі забезпечення безпеки корпоративної мережі було успішно реалізовано низку заходів, спрямованих на налаштування аутентифікації на роутерах, з метою обмеження доступу до налаштувань мережі. Конкретні кроки, які були здійснені, дозволили підвищити рівень безпеки і зменшити можливість несанкціонованого доступу до системи. Важливою складовою цього процесу стала налаштування паролів для привілейованого режиму та режиму конфігурації, що забезпечує контроль над доступом до різних рівнів налаштувань.

```
User Access Verification

Password:

Switch>enable
Password:
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

---

Рисунок 3.1 – Заблокований доступ без пароля

Цей комплексний підхід до налаштування аутентифікації на роутерах визначає важливий етап в підвищенні безпеки мережі та допоможе ефективно запобігати можливим загрозам та атакам.

Для максимальної захищеності корпоративної мережі ми застосували команди та налаштування на маршрутизаторах для блокування небезпечних протоколів (ICMP).

Для перевірки необхідно ввести команду ping 192.168.1.1 (або IP-адресу RouterD) і переконатися, що пінг не проходить, оскільки маємо правило, що блокує ICMP:

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 55   |

```

Router#
Router#write memory
Building configuration...
[OK]
Router#
18:01:50: %OSPF-5-ADJCHG: Process 1, Nbr 202.195.32.150 on GigabitEthernet0/0 from INIT
to DOWN, Neighbor Down: Dead timer expired

18:01:50: %OSPF-5-ADJCHG: Process 1, Nbr 202.195.32.150 on GigabitEthernet0/0 from INIT
to DOWN, Neighbor Down: Interface down or detached

Router#
Router#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Router#

```

Рисунок 3.2 – Звіт із блокування ICMP під час тесту пінгу з IP-адресою 192.168.1.1

Налаштування доступу до сервісів можемо перевірити командою `show access-lists 101`

```

RouterD#show access-lists 101
RouterD#show access-lists 101
Extended IP access list 101
    permit udp any eq bootpc any eq bootps (8 match(es))
    deny ip any any (11 match(es))
    deny ip 192.168.2.0 0.0.0.255 any
    permit ip any any
RouterD#

```

Рисунок 3.3 – Результат виведення ACL 101 на маршрутизаторі RouterD

Результатом проведених тестів та налаштувань є створення ефективної та надійної системи контролю та фільтрації трафіку за допомогою списку керування доступом (ACL). Описані дії призвели до створення таких правил, які забезпечують оптимальне функціонування мережі та забезпечують безпеку на різних рівнях.

- Перші два правила ACL 101 дозволяють UDP-трафік між портами bootpc та bootps для протоколу DHCP. Це важливий крок для належного функціонування DHCP і забезпечення коректної адресації для клієнтів.

- Третє правило є загальним відхиленням (`deny ip any any`), що блокує будь-який неавторизований трафік. Це забезпечує високий рівень безпеки, запобігаючи несанкціонованому доступу та можливим загрозам.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 56   |

- Четверте правило (deny ip 192.168.2.0 0.0.0.255 any) забороняє IP-трафік з підмережі 192.168.2.0/24 до будь-якої адреси, що впроваджує додатковий контроль над доступом та забезпечує захист важливих ресурсів.

- Останнє правило (permit ip any any) є загальним дозволом для легітимного трафіку, що не заборонений попередніми правилами. Це забезпечує гарантовану можливість обміну даними в рамках безпечно налаштованої мережі.

За використання вищезазначених практик та створення ACL з конкретними правилами, ми досягли підвищення безпеки мережі та забезпечили оптимальну функціональність, контролюючи доступ та фільтруючи трафік згідно з потребами організації.

Забезпечення конфіденційності (блокування доступу до певних ресурсів). За допомогою виконаних команд створюється розширений список доступу з номером 102, який блокує конкретну IP-адресу 203.0.113.10 і дозволяє всім іншим IP-адресам проходити через інтерфейс GigabitEthernet0/3.

```
RouterD#
RouterD#ping 203.0.113.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

RouterD#
```

Рисунок 3.4 – Результат виконання команди ping до IP-адреси 203.0.113.10 на маршрутизаторі RouterD

У результаті наших дій ми успішно реалізували заходи для забезпечення додаткового рівня безпеки та контролю над доступом до певних ресурсів у мережі. Проаналізувавши та адаптуючи команди, ми створили розширений список доступу з номером 103, який успішно блокує SSH-з'єднання з зовнішніх IP-адрес до внутрішнього IP-адреси 192.168.1.10 на порту 22 (SSH). Це дозволило нам заборонити несанкціонованим зовнішнім джерелам доступ до цієї конкретної системи через SSH.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 57   |

```
RouterD#show access-lists 103
Extended IP access list 103
  deny tcp any host 192.168.1.10 eq 22
  permit ip any any (4 match(es))

RouterD#
```

Рисунок 3.5 – Результат виведення ACL 103 на маршрутизаторі RouterD

Адаптувавши команди та використовуючи створений розширений список доступу, ми забезпечили контроль за трафіком, що надходить до цієї системи, та заблокували можливість неавторизованого доступу. Ця дія сприяє підвищенню безпеки мережі, а отримані результати та перевірка ACL 103 на маршрутизаторі підтверджують успішну реалізацію запроваджених заходів та їхню ефективність.

Цей крок є важливою частиною нашої стратегії захисту мережі, оскільки він дозволяє обмежити можливість злому та несанкціонованого доступу до конкретних систем, що забезпечує надійний рівень захисту та конфіденційності важливої інформації.

Завдяки налаштуванню файрволу ми успішно змогли захистити доступ до маршрутизатора від незаконних атак і небажаних з'єднань. Це важливий крок у забезпеченні безпеки мережі та обладнання. Шляхом додавання відповідного правила до файрволу, ми створили фільтр, який дозволяє лише обраним користувачам підключатися до маршрутизатора через протокол SSH.



Рисунок 3.6 – Підтвердження неможливості SSH-з'єднань

Таким чином, закритий порт 22 на вказаному IP-адресі є результатом роботи файрволу, який успішно фільтрує трафік та відхиляє небажані з'єднання, що вказує на ефективність заходів для забезпечення безпеки мережі та захисту доступу до маршрутизатора.

Перевіримо налаштування VPN між двома маршрутизаторами Cisco.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 58   |

```
RouterC#show ip interface brief
Interface          IF-Address      OK? Method Status  Protocol
GigabitEthernet0/0 202.195.32.129 YES NVRAM  up      up
GigabitEthernet0/1 202.195.32.153 YES NVRAM  up      up
GigabitEthernet0/2 202.195.32.149 YES NVRAM  up      up
Serial0/3/0         200.10.10.2    YES NVRAM  up      up
Serial0/3/1         unassigned     YES NVRAM  down    down
Tunnel0             192.168.1.2    YES manual up      up
Vlan1               unassigned     YES NVRAM  admini down
RouterC#
```

Рисунок 3.7 – Стан інтерфейсу

Тунельний інтерфейс Tunnel0 на ньому виглядає піднятим (up) і має IP-адресу 192.168.1.2.

Перевірка з'єднання: Після завершення налаштування перевіряємо з'єднання між мережами. Виконаємо пінг із комп'ютера на Router A до комп'ютера на Router B або навпаки:

```
RouterA# ping 192.168.2.1
```

```
RouterB# ping 192.168.1.1
```

```
RouterD#ping 192.168.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/27 ms
```

```
RouterD#
```

Рисунок 3.8 – Успішний пінг з RouterD до RouterC

Отже, пінг з RouterD до RouterC (192.168.1.1) був успішним. Success rate становить 100 percent, що означає, що всі 5 пакетів, які були надіслані, були успішно отримані від RouterC.

Тепер VPN-тунель між RouterC і RouterD працює належним чином, і можна пінгувати інші пристрої в мережах кожного маршрутизатора через цей тунель.

Налаштування списків контролю доступу (ACL) на маршрутизаторі відображено на рис. 3.9.

```

RouterE#show access-lists
Extended IP access list 103
  10 deny ip any host 202.195.32.130
  20 permit ip any any (22 match(es))
Standard IP access list 1
  10 deny any (144253 match(es))
Standard IP access list SSH-ACL
  10 permit host 202.195.32.146
Extended IP access list sl_def_acl
  0 deny tcp any any eq telnet
  0 deny tcp any any eq www
  0 deny tcp any any eq 22
  0 permit tcp any any eq 22

```

Рисунок 3.9 – ACL\_Конфігурація

Цей скріншот показує конфігурацію різних ACL та їх правила, які використовуються для обмеження та контролю доступу до різних ресурсів у вашій мережі.

```

RouterC#show running-config | include line vty
line vty 0 4
RouterC#show access-list
Extended IP access list SSH-ACL
  10 permit tcp host 192.168.1.2 any eq 22

```

Рисунок 3.10 – Перевірка внесення в список

Це означає, що ми можемо встановити SSH-з'єднання з локального комп'ютера, який має IP-адресу 192.168.1.2. Тепер ми можемо безпечно та віддалено управляти маршрутизатором через зашифроване SSH-з'єднання з локального комп'ютера.

### 3.2 Забезпечення стійкості та безпеки корпоративної мережі: механізми резервного копіювання та роль навчання персоналу

Резервне копіювання даних дозволяє забезпечити безпечне збереження даних та відновлення інформації в разі випадкового видалення, втрати, атаки зломисників або виходу з ладу обладнання. Для того, щоб налаштувати резервне копіювання даних в корпоративній мережі необхідно виконати кілька кроків:

1. Ідентифікація важливих даних:

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 60   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

В ході аналізу ми визначили ключові аспекти щодо ідентифікації важливих даних для різних відділень компанії. Кожне з відділень має свою унікальну роль і специфіку, що вимагає окремого підходу до захисту та управління даними.

У Мережі А (США), ми визначили наступні критичні дані:

- Конфігураційні файли серверів: Ці дані містять налаштування, необхідні для коректної роботи серверів, і, отже, є ключовими для забезпечення стабільності і безпеки мережі.
- База даних клієнтів: Інформація про клієнтів є цінним активом компанії і вимагає особливої уваги в плані забезпечення конфіденційності та відповідності нормам захисту даних.
- Важливі документи: Це можуть бути юридичні документи, угоди та інші матеріали, які мають важливе значення для бізнесу компанії.

У Мережі В (Європа), наш аналіз фокусувався на наступних важливих даних:

- Розроблене програмне забезпечення: Ці дані представляють собою результат інтелектуальної праці та важливі для подальшого розвитку продуктів і послуг компанії.
- Інноваційні проекти: Інновації можуть бути ключовим чинником конкурентоспроможності компанії, тому їх захист і збереження є надзвичайно важливим завданням.
- Дані для клієнтів Європи: Клієнти є серцем бізнесу, і їхні дані повинні бути оброблені з повагою до їхньої приватності та відповідності регулятивним вимогам ЄС.

Мережа С (Азія) містить наступні критичні дані:

- Технічна підтримка: Ці дані допомагають забезпечити належне функціонування продуктів та послуг компанії для клієнтів Південно-Східної Азії, тому вони потребують ефективного управління та захисту.
- Дані обслуговування клієнтів: Інформація про взаємодію з клієнтами, їх запити та звернення мають важливе значення для покращення якості обслуговування.

У Мережі D (Африка) наш аналіз сфокусований на таких важливих даних:

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 61   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

- Дані для розвитку ІТ-інфраструктури та послуг в Африці: Ці дані допомагають забезпечити ефективне розширення бізнесу в регіоні та розвиток інфраструктури.

Загальний результат аналізу полягає в тому, що визначені важливі дані є ключовими активами для кожної мережі, і їх захист, збереження та належне управління є стратегічно важливими завданнями для компанії.

## 2. Категоризація даних:

Необхідно розділити дані на категорії важливості: критичні, важливі та менш важливі. В додатку В наведено категоризацію даних, яка допоможе краще орієнтуватися в важливості та обсягу даних в кожному відділенні та визначити стратегії резервного копіювання для кожної категорії.

## 3. Вибір джерел резервного копіювання:

Потрібно визначити джерела резервного копіювання для кожного відділення: центральні сервери, бази даних, робочі станції.

Вибір джерел резервного копіювання для мережі підприємства “Global IT Solutions Inc.” з оглядом на різні відділення наведено в Додатку Д.

План резервного копіювання допоможе забезпечити захист даних у різних відділеннях компанії та в разі потреби відновлення інформації у випадку.

## 4. Вибір методу резервного копіювання:

Необхідно врахувати можливості обладнання та інфраструктури: локальне збереження, віддалене збереження в хмарних сховищах.

Вибір методу резервного копіювання для мережі підприємства “Global IT Solutions Inc.” з оглядом на різні відділення наведено в Додатку Ж.

Кожен метод резервного копіювання має свої переваги та обмеження, і вибір залежить від вимог та потреб кожного відділення мережі “Global IT Solutions Inc.”.

## 5. Створення резервних копій:

Використовувати наявні інструменти для створення резервних копій згідно з обраною стратегією.

Для того, щоб налаштувати резервне копіювання на сервері необхідно:

### 1. Встановити програми для резервного копіювання.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 62   |

В терміналі сервера потрібно виконати команду для встановлення програми rsync:

```
sudo apt-get install rsync
```

2. Створити каталог для зберігання резервних копій.

Для цього в терміналі сервера потрібно створити каталог для зберігання резервних копій (якщо він ще не створений):

```
mkdir /backup
```

3. Налаштувати автоматичне резервне копіювання.

Для налаштування автоматичного резервного копіювання, в терміналі сервера потрібно відредагувати файл налаштувань cron для поточного користувача:

```
crontab -e
```

А також додати рядок для виконання резервного копіювання щоденно о 2 годині ночі:

```
0 2 * * * rsync -avz /var/ important-data /backup/
```

Та завершити сесію SSH на сервері.

Однак, слід зазначити, що Cisco Packet Tracer не надає можливості реалістичного використання командного рядка операційних систем і обмежує можливості налаштування резервного копіювання. Це обмеження створює певні труднощі у плані проведення повноцінного тестування процесу резервного копіювання за допомогою Cisco Packet Tracer.

Безпека корпоративної мережі є невід’ємною складовою успішної та стійкої діяльності будь-якої організації. Однак, наявність високої технологічності та розроблених методів захисту не завжди гарантує безпеку мережі від сучасних загроз та кібератак. Нерідко, найбільш вразливою ланкою у системі захисту виявляється чинник, який залежить від людського фактору.

Відповідно до цього, розуміння та своєчасне впровадження базових принципів безпеки мережі стає важливим завданням для організації. Досягнення цієї мети вимагає активної участі та навчання персоналу, який взаємодіє з корпоративною мережею на повсякденній основі.

Зміцнення культури безпеки в організації включає:

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 63   |

– Навчання персоналу про визначення та розпізнавання загроз безпеці, що сприяє попередженню можливих атак, ідентифікації підозрілих активностей та налагодженню превентивних заходів.

– Включення безпекових практик у щоденну роботу персоналу, знання та усвідомлення основних правил поведінки зі створеними ресурсами, обмеження доступу, шифрування даних та інших аспектів, що сприяють зниженню ризиків інцидентів.

– Навчання персоналу про правильні дії в разі виявлення або підозри на кібератаку, що дозволяє забезпечити швидку та ефективну реакцію на інциденти та мінімізувати можливі збитки.

– Постійна оновленість та розвиток знань персоналу з питань безпеки мережі, що допомагає у впровадженні нових технологій, ідентифікації нових загроз та застосуванні кращих практик.

Отже, навчання персоналу є ключовим елементом забезпечення безпеки корпоративної мережі та успішного функціонування організації в цілому. Розуміння загроз, здатність вчасно реагувати на інциденти та дотримання культури безпеки стають невід’ємною частиною діяльності кожного співробітника, що сприяє стійкості та успішності діяльності корпоративної мережі “Global IT Solutions Inc.”.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 64   |

## ВИСНОВОК ДО РОЗДІЛУ 3

В рамках третього розділу нашої дипломної роботи було проведено комплексне тестування працездатності розробленої корпоративної мережі, а також досліджено процес резервування та вагомість навчання персоналу з питань кібербезпеки.

Результати проведеного тестування демонструють ефективність розробленої захищеної корпоративної мережі. Це свідчить про важливий етап у реалізації проекту, адже підтверджується, що заходи та методи, розглянуті у попередніх розділах, дійсно сприяють забезпеченню високого рівня безпеки мережі.

Процес резервування, відведення альтернативних шляхів та резервних джерел забезпечення мережевого зв'язку, виявився надзвичайно важливим для забезпечення неперервності роботи корпоративної мережі. Він дозволяє зменшити вплив можливих відмов або атак на одну частину мережі та забезпечити нормальний функціонування організації.

Слід відмітити, що навчання персоналу є ключовим аспектом в забезпеченні кібербезпеки корпоративної мережі. Знання та усвідомлення працівниками загроз та вразливостей допомагає попередити можливі атаки та вчасно реагувати на них. Важливою частиною навчання є ознайомлення з правилами безпеки, процедурами реагування та використанням захисних технологій. Навчений та підготовлений персонал є невід'ємною складовою успішної реалізації проекту захищеної корпоративної мережі.

Загалом, результати дослідження показали, що розроблена корпоративна мережа відповідає стандартам безпеки та ефективності. Резервування мережі та належне навчання персоналу відіграють важливу роль у забезпеченні надійності та неперервності роботи мережі.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 65   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

## ВИСНОВКИ

Корпоративні мережі сьогодні стикаються з різноманітними загрозами, що можуть серйозно підірвати їх безпеку та надійність. Кібератаки, такі як незаконний доступ та поширення шкідливих програм, загрожують конфіденційності та цілісності даних. Малювери, такі як віруси та троянські програми, можуть призвести до втрати файлів та вразливостей систем. Фішингові атаки використовують соціальний інжиніринг для викрадення конфіденційних даних. DDoS-атаки можуть перевантажити сервери та обмежити доступ до ресурсів. Несанкціонований доступ та злам можуть призвести до витоку конфіденційної інформації. Фізичні загрози, такі як втручання у фізичну інфраструктуру, також не можна ігнорувати. Крім того, можливе незаконне спостереження за трафіком та ризику втрати даних через технічні неполадки. З метою захисту корпоративних мереж важливо реалізувати стратегії та технології, які забезпечать надійний захист від цих загроз і забезпечать стійкість мережі у сучасному цифровому середовищі.

Підсумовуючи проведену дослідницьку роботу, можемо стверджувати, що виконані заходи та налаштування забезпечують надійний та ефективний рівень безпеки для корпоративної мережі компанії. Наявність відповідних стратегій та технологій є гарантом захисту конфіденційної інформації та запобігання несанкціонованому доступу до ресурсів мережі.

Встановлення паролів для привілейованого режиму та режиму конфігурації на кожному роутері додає додатковий шар захисту, роблячи неможливим несанкціонований доступ до налаштувань роутерів. Використання VLAN та методу "Router-on-a-stick" дозволяє ефективно розділити мережу на сегменти, обмежуючи взаємодію між ними та знижуючи ризик перетоку даних.

Однією з центральних стратегій стало використання списків керування доступом (ACL) для реалізації файрволу. Ця технологія дозволила ефективно блокувати небезпечні протоколи та здійснювати контроль доступу до різних мережевих сервісів. Додатково, використання ACL сприяло забезпеченню конфіденційності даних шляхом регулювання комунікації між різними сегментами мережі.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 66   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

Одним із важливих аспектів було також використання технології віртуальної приватної мережі (VPN). Ця технологія дозволила створити безпечний канал зв'язку між віддаленими мережевими пристроями, забезпечивши захищену передачу даних між ними. Це відкрило можливість для безпечного обміну інформацією між віддаленими локаціями організації.

Також, особлива увага була приділена використанню SSH (Secure Shell) для віддаленого доступу. Ця технологія забезпечила шифрування даних під час передачі, що надалі зробило процес з'єднання надійним та захищеним від можливих атак злому та перехоплення інформації з боку зломисників. Використання SSH сприяло створенню безпечних з'єднань із віддаленими мережевими пристроями, зберігаючи конфіденційність та інтегритет даних.

В цілому, застосування комплексу технологій та стратегій забезпечило ефективний захист корпоративної мережі, гарантуючи конфіденційність даних, захист від несанкціонованого доступу та відповідність сучасним стандартам безпеки мереж. Відомо, що справжній успіх полягає в поєднанні технічних рішень з правильними підходами до управління та використанням ресурсів.

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                          | 67   |

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 10 порад з кібербезпеки для віддаленої роботи. Як організувати безпечну роботу працівників 'з дому', щоб не стати жертвою зловмисників? [Електронний ресурс]. URL: <https://www.epravda.com.ua/columns/2022/07/14/689184/>
2. 7 способів вас зламати або як захистити компанію від кібератак [Електронний ресурс]. URL: <https://hub.kyivstar.ua/news/7-sposobiv-vas-zlamaty-abo-yak-zahystyty-kompaniyu-vid-kiberatak/#4>
3. Academic journals and conference papers on topics related to network security, cybersecurity, intrusion detection, and encryption.
4. Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems (2nd ed.). Wiley.
5. CIS Controls - Center for Internet Security.
6. Cisco Networking Academy Course Materials on Network Security.
7. ENISA (European Union Agency for Cybersecurity) Reports and Guidelines.
8. General Data Protection Regulation (GDPR). (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
9. Industry standards and best practices documents related to corporate network security (e.g., PCI DSS for payment card security, HIPAA for healthcare, etc.).
10. ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements.
11. ISO/IEC 27001:2013. (2013). Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization.
12. ISO/IEC 27002:2013. (2013). Information technology - Security techniques - Code of practice for information security controls. International Organization for Standardization.

|      |      |                |        |      |                                 |      |
|------|------|----------------|--------|------|---------------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | <i>КІК.КР.Б – 125 – 07 – ПЗ</i> | Арк. |
|      |      | Бродський Ю.Б. |        |      |                                 |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                                 | 68   |

13. National Cyber Security Centre (NCSC) (UK) Publications.
14. NIST Cybersecurity Framework. (Version 1.1). (2018). National Institute of Standards and Technology, U.S. Department of Commerce. [Електронний ресурс]. URL: {посилання на документ}.
15. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations.
16. Official documentation from network equipment vendors (e.g., Cisco, Juniper, Huawei) about configuring secure network devices.
17. RFC (Request for Comments) documents from IETF related to network security protocols and practices.
18. Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.
19. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Pearson.
20. White papers and technical documentation from leading cybersecurity solution providers (e.g., Palo Alto Networks, Fortinet, Cisco, Check Point, etc.).
21. Закон України “Про захист персональних даних”. (2010). [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
22. Закон України “Про основні засади забезпечення кібербезпеки України”. (2017). [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
23. Кіберзахист компанії в умовах війни: перемагають сучасні технології [Електронний ресурс]. URL: <https://hub.kyivstar.ua/news/kiberzahyst-kompaniyi-v-umovah-vijny-peremagayut-suchasni-tehnologiyi/>
24. Стратегія кібербезпеки України від 26 серпня 2021 року № 447/2021. [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.
25. Як підтримувати комплексну IT-безпеку компанії — на прикладі інструментів Microsoft [Електронний ресурс]. URL: <https://dou.ua/forums/topic/40067/>
26. Яких помилок у захисті корпоративних мереж найчастіше припускаються співробітники? [Електронний ресурс]. URL:

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          | 69   |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          |      |

<https://cybercalm.org/novyny/yakyh-pomylok-u-zahysti-korporatyvnyh-merezh-najchastishe-prypuskayutsya-spivrobitnyky/>

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                          | 70   |

ДОДАТКИ

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                          | 71   |

## Порівняння традиційних методів захисту та сучасних підходів

| Ознака порівняння                  | Традиційні методи захисту:                                                                                                                                                                                                                                                                    | Сучасні методи захисту                                                                                                                                                                                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Технологічна складність            | Традиційні методи захисту мережі, такі як файрволи, антивірусне програмне забезпечення та системи виявлення вторгнень, зазвичай менш складні у реалізації та використанні. Вони вже довгий час є стандартом безпеки та мають добре вивірені технології                                        | Сучасні підходи до кібербезпеки, як машинне навчання, аналіз мережевої поведінки та безперервний моніторинг, можуть бути складнішими у впровадженні та налаштуванні. Вони вимагають більш високої кваліфікації та експертизи, але можуть забезпечити більш високий рівень захисту, особливо проти нових та несподіваних загроз |
| Ефективність проти сучасних загроз | Традиційні підходи часто не здатні ефективно протистояти новим та складним загрозам, таким як цілеспрямовані атаки або атаки "нульового дня". Вони можуть бути здатні виявляти попередньо відомі сигнатури вірусів або атак, але їх недостатньо для виявлення нових, неідентифікованих загроз | Сучасні підходи, такі як машинне навчання та аналіз мережевої поведінки, можуть бути більш ефективними у виявленні незвичайних та аномальних активностей, що робить їх більш придатними для боротьби з новими та розумними загрозами                                                                                           |
| Автоматизація                      | Багато традиційних методів захисту потребують ручної настройки та управління. Вони можуть бути менш автоматизованими, що утруднює швидку реакцію на кібератаки                                                                                                                                | Сучасні підходи до кібербезпеки, особливо з використанням машинного навчання та AI, можуть бути більш автоматизованими. Вони можуть надавати можливість швидко виявляти та реагувати на загрози без значної участі людини, що підвищує ефективність і швидкість реакції                                                        |
| Вартість                           | Традиційні методи часто можуть бути менш витратними, особливо для менших організацій. Вони вже забезпечують базовий рівень захисту і можуть бути більш доступними з точки зору вартості                                                                                                       | Сучасні підходи, такі як машинне навчання та аналіз мережевої поведінки, можуть бути більш дорогими у впровадженні та обслуговуванні. Вони можуть вимагати високотехнологічного обладнання та спеціалістів з відповідною експертизою                                                                                           |

## Типи кабелів в Cisco Packet Tracer

| Тип кабелю                                                                                           | Описання                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Консоль<br>         | Консольне з'єднання може бути виконано між ПК і маршрутизаторами або комутаторами. Повинні бути виконані деякі вимоги для роботи консольного сеансу з ПК: швидкість з'єднань з обох сторін повинна бути однаковою, має бути 7 біт даних (або 8 біт) для обох сторін, контроль парності повинен бути однаковий, має бути 1 або 2 степових бита (але вони не обов'язково повинні бути однаковими), а потік даних може бути чимось завгодно для обох сторін. |
| Мідний прямий<br>   | Цей тип кабелю є стандартним середовищем передачі Ethernet для з'єднання пристроїв, який функціонує на різних рівнях OSI. Він повинен бути з'єднаний з наступними типами портів: мідний 10 Мбіт / с (Ethernet), мідний 100 Мбіт / с (Fast Ethernet) і мідний 1000 Мбіт / с (Gigabit Ethernet)                                                                                                                                                             |
| Мідний кросовер<br> | Цей тип кабелю є середовищем передачі Ethernet для з'єднання пристроїв, які функціонують на однакових рівнях OSI. Він може бути з'єднаний з наступними типами портів: мідний 10 Мбіт / с (Ethernet), мідний 100 Мбіт / с (Fast Ethernet) і мідний 1000 Мбіт / с (Gigabit Ethernet)                                                                                                                                                                        |
| Оптика<br>        | Оптоволоконне середовище використовується для з'єднання між оптичними портами (100 Мбіт / с або 1000 Мбіт / с).                                                                                                                                                                                                                                                                                                                                           |
| Телефонний<br>    | З'єднання через телефонну лінію може бути здійснено тільки між пристроями, що мають модемні порти. Стандартне подання модемного з'єднання – це кінцевий пристрій (Наприклад, ПК), додзвонюється в мережеве хмара.                                                                                                                                                                                                                                         |
| Коаксіальний<br>  | Коаксіальне середовище використовується для з'єднань між коаксіальними портами, такі як кабельний модем, з'єднаний з хмарою Packet Tracer                                                                                                                                                                                                                                                                                                                 |
| Серійний DCE<br>Серійний DTE                                                                         | З'єднання через послідовні порти, часто використовуються для зв'язків WAN. Для настройки таких з'єднань необхідно встановити синхронізацію на стороні DCE-пристроїв. Синхронізація DTE виконується за вибором.                                                                                                                                                                                                                                            |

## Категоризація даних для Global IT Solutions Inc.

| Підрозділ                                                   | Критичні дані                                                                                                                                                                                                                                                                | Важливі дані                                                                                                                                                                                                                     | Менш важливі дані                                                                                                                                              |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Мережа А<br>(США): Головне відділення                       | <ul style="list-style-type: none"> <li>Конфігураційні файли центральних серверів.</li> <li>Бази даних клієнтів із замовленнями та контактною інформацією.</li> <li>Фінансові звіти та бюджети компанії.</li> <li>Архіви пошти та комунікацій внутрішнього обміну.</li> </ul> | <ul style="list-style-type: none"> <li>Робочі теки та файли співробітників.</li> <li>Інвентаризація обладнання та програмного забезпечення.</li> <li>Документація з проектів та стратегій компанії.</li> </ul>                   | <ul style="list-style-type: none"> <li>Внутрішні звіти з нарад та зборів.</li> <li>Дані з відділу кадрів.</li> </ul>                                           |
| Мережа В<br>(Європа): Розробка програмного забезпечення     | <ul style="list-style-type: none"> <li>Вихідний код та проекти розробки програмного забезпечення.</li> <li>Копії баз даних для розробки та тестування.</li> <li>Інформація про патенти та права на інтелектуальну власність.</li> </ul>                                      | <ul style="list-style-type: none"> <li>Документація з проектів та планів розробки.</li> <li>Звіти з тестування та якості продукції.</li> <li>Дані для комунікації з клієнтами щодо вимог до програмного забезпечення.</li> </ul> | <ul style="list-style-type: none"> <li>Робочі теки співробітників.</li> <li>Дані зі спільних зборів та нарад.</li> </ul>                                       |
| Мережа С (Азія): Технічна підтримка та обслуговування       | <ul style="list-style-type: none"> <li>Документація з технічної підтримки та інструкції для клієнтів.</li> <li>Конфігураційні файли серверів обслуговування.</li> </ul>                                                                                                      | <ul style="list-style-type: none"> <li>Журнали обліку та відстеження заявок на техпідтримку.</li> <li>Дані для звітності щодо роботи та завдань технічного відділу.</li> </ul>                                                   | <ul style="list-style-type: none"> <li>Кореспонденція з клієнтами та запити на підтримку.</li> <li>Внутрішні звіти щодо вирішення технічних питань.</li> </ul> |
| Мережа D<br>(Африка): Розвиток ІТ-інфраструктури та послуги | <ul style="list-style-type: none"> <li>Дані про розгортання та налаштування ІТ-інфраструктури клієнтів.</li> <li>Конфігурації мережевого обладнання та серверів.</li> </ul>                                                                                                  | <ul style="list-style-type: none"> <li>Звіти про проведення аудитів безпеки та рекомендації.</li> <li>Дані щодо підключення клієнтів та їхніх потреб.</li> </ul>                                                                 | <ul style="list-style-type: none"> <li>Запити на техпідтримку від клієнтів.</li> <li>Робочі теки співробітників.</li> </ul>                                    |

## Методи резервного копіювання для Global IT Solutions Inc.

| Підрозділ                                                   | Методи резервного копіювання                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Мережа А (США):<br>Головне відділення                       | <b>1. Повне зеркальне резервне копіювання (Full Backup):</b><br>– Щоденне повне зеркальне копіювання серверів баз даних, центральних серверів та важливих даних на локальні та віддалені сховища.<br>– Забезпечує швидке відновлення в разі повної втрати даних.<br><b>2. Інкрементальне резервне копіювання (Incremental Backup):</b><br>– Щоденне інкрементальне копіювання файлів, змінених з попереднього резервування, на зовнішні сховища.<br>– Забезпечує збереження простору та часу під час резервування. |
| Мережа В (Європа):<br>Розробка програмного забезпечення     | <b>1. Використання системи керування версіями (Version Control System):</b><br>– Автоматичне резервне копіювання вихідного коду та проектів на центральний репозиторій (наприклад, Git).<br>– Забезпечує відстеження змін та відновлення попередніх версій.<br><b>2. Локальне резервне копіювання:</b><br>– Тижневе архівування репозиторію на локальні сховища для подовження зберігання.                                                                                                                         |
| Мережа С (Азія):<br>Технічна підтримка та обслуговування    | <b>1. Резервне копіювання конфігурацій:</b><br>– Щоденне копіювання конфігураційних файлів серверів та мережного обладнання на центральний сервер.<br><b>2. Зберігання логів та звітів:</b><br>– Тижневе резервне копіювання логів та звітів технічної підтримки на локальні сховища.                                                                                                                                                                                                                              |
| Мережа D (Африка):<br>Розвиток ІТ-інфраструктури та послуги | <b>1. Автоматичне резервне копіювання конфігураційного обладнання:</b><br>– Щоденне автоматичне резервне копіювання конфігураційних файлів мережного обладнання на центральний сервер.<br><b>2. Зберігання аудиту та аналізу інфраструктури:</b><br>– Щоквартальне архівування звітів з аудиту безпеки та аналізу інфраструктури на зовнішні сховища.                                                                                                                                                              |

## Вибір джерел резервного копіювання для Global IT Solutions Inc.

| Підрозділ                                                | Джерела резервного копіювання                                                                                                                                                                                                                               | Регулярність копіювання                                                                                                                                                                      |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Мережа А (США): Головне відділення                       | <ul style="list-style-type: none"> <li>– Центральні сервери з базами даних та важливими даними компанії.</li> <li>– Сховище на підставах для конфігураційних файлів серверів.</li> <li>– Зовнішні сховища для архіву пошти та комунікацій.</li> </ul>       | <ul style="list-style-type: none"> <li>– Щоденне резервне копіювання даних серверів.</li> <li>– Тижневе архівування баз даних та фінансових звітів.</li> </ul>                               |
| Мережа В (Європа): Розробка програмного забезпечення     | <ul style="list-style-type: none"> <li>– Вихідний код та проекти розробки, збережені в репозиторії.</li> <li>– Сховище для копій баз даних розробки та тестування.</li> <li>– Зовнішні сховища для збереження патентів та документів із правами.</li> </ul> | <ul style="list-style-type: none"> <li>– Щотижневе резервне копіювання вихідного коду та проектів.</li> <li>– Щомісячне архівування баз даних розробки та звітів із тестування.</li> </ul>   |
| Мережа С (Азія): Технічна підтримка та обслуговування    | <ul style="list-style-type: none"> <li>– Сховище з документацією для технічної підтримки та інструкціями.</li> <li>– Конфігураційні файли серверів обслуговування.</li> </ul>                                                                               | <ul style="list-style-type: none"> <li>– Щоденне резервне копіювання документації та конфігураційних файлів.</li> <li>– Тижневе архівування звітів з технічної підтримки.</li> </ul>         |
| Мережа D (Африка): Розвиток IT-інфраструктури та послуги | <ul style="list-style-type: none"> <li>– Сховище для конфігураційних файлів обладнання та серверів.</li> <li>– Архіви звітів з аудиту безпеки та аналізу інфраструктури.</li> </ul>                                                                         | <ul style="list-style-type: none"> <li>– Щоденне резервне копіювання конфігураційних файлів обладнання.</li> <li>– Місячне архівування звітів з аудиту та аналізу інфраструктури.</li> </ul> |

|      |      |                |        |      |                          |      |
|------|------|----------------|--------|------|--------------------------|------|
|      |      | Решетнюк Д.К.  |        |      | КІК.КР.Б – 125 – 07 – ПЗ | Арк. |
|      |      | Бродський Ю.Б. |        |      |                          |      |
| Змт. | Арк. | № докум.       | Підпис | Дата |                          | 76   |