|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | | | | | | | |
| **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
| **КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ** | | | | | | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
| Пояснювальна записка | | | | | | | | | | | | | | | | |
| до бакалаврської роботи | | | | | | | | | | | | | | | | |
|  | | на тему: | | | | | | | | | | | | |  | |
| **«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕННОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ MIKROTIK»** | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | | Виконав студент 4 курсу, групи БСД-41 | | | | | | | | | |
|  | |  | | | | | спеціальності 125 Кібербезпека | | | | | | | | | |
|  | |  | | | | | освітньо-професійної програми «Інформаційна та кібернетична безпека» | | | | | | | | | |
|  | |  | | | | | (шифр і назва спеціальності) | | | | | | | | | |
|  | |  | | | | | Калабухов І.І. | | | | | | | | | |
|  | |  | | | | | (прізвище та ініціали) | | | | | | | | | |
|  | |  | | | | | Керівник | | Гайдур Г.І. | | | | | | | |
|  | |  | | | | |  | | | | (прізвище та ініціали) | | | | | |
|  | |  | | | | | Рецензент | | |  | | | | | | |
|  | |  | | | | | (прізвище та ініціали) | | | | | | | | | |
|  | |  | | | | | Нормоконтролер | | | | | | Чумак Н.С. | | | |
|  | |  | | | | |  | | | | (прізвище та ініціали) | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | | КИЇВ – 2023 | | | | | | | | | | | | |  | |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | | | | | | | |
| Інститут | | ННІЗІ | | | | |  | | | |  | | | |  | |
| Кафедра | | Інформаційної та кібернетичної безпеки | | | | | | | | | | | | | | |
| Ступінь вищої освіти | | | | Бакалавр | | | | | | |  | | | |  | |
| Спеціальність | | | 125 Кібербезпека | | | | | | | |  | | | |  | |
| Освітньо-професійна програма | | | | | | | Інформаційна та кібернетична безпека | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | | ЗАТВЕРДЖУЮ | | | | | |
|  | |  | | | | |  | | | | Завідувач кафедри ІКБ | | | | | |
|  | |  | | | | |  | | | |  | | | | Гайдур Г.І. | |
|  | |  | | | | |  | | | | “\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | | **З А В Д А Н Н Я** | | | | | | | | | | | | |  | |
|  | | **НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ** | | | | | | | | | | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
| Калабухову Іллі Ігоровичу | | | | | | | | | | | | | | | | |
| (прізвище, ім’я, по батькові) | | | | | | | | | | | | | | | | |
| 1. Тема бакалаврської роботи: | | | | | |  | | | | | | | | | | | |
| «Дослідження шляхів та розробка рекомендацій щодо забезпечення захищенної корпоративної мережі на базі обладнання Mikrotik» | | | | | | | | | | | | | | | | |
| керівник бакалаврської роботи | | | | | | | Гайдур Галина Іванівна, д.т.н., проф. | | | | | | | | | |
|  | |  | | | | | (прізвище, ім’я, по батькові, науковий ступінь, вчене звання) | | | | | | | | | |
| затверджені наказом закладу вищої освіти від « 12 » березня 2023 року № 65. | | | | | | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
| 2. Строк подання студентом бакалаврської роботи | | | | | | | | | | | | 28.05.2023 р. | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
| 3. Вихідні дані до бакалаврської роботи | | | | | | | |  | | | | | | |  | |
| 1. Програмні діагностичні утиліти; | | | | | | | | | | |  | | | |  | |
| 1. Експериментальне шкідливе програмне забезпечення | | | | | | | | | | | | | | |  | |
| 1. Кінцеві точки користувачів; | | | | | | | | | | | | | | | | |
| 1. Наукова та технічна література, експлуатаційна документація | | | | | | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
| 4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) | | | | | | | | | | | | | | | | |
| 1. Аналіз проблеми захисту корпоративної мережі. | | | | | | | | | | | | | | | | |
| 1. Актуальність проблеми захисту мереж. | | | | | | | | | | | | | | | | |
| 1. Методи та засоби захисту корпоративних мереж. | | | | | | | | | | | | | | | | |
| 1. Рекомендації щодо застосування методів та засобів захисту корпоративних мереж. | | | | | | | | | | | | | | | | |
| 5. Перелік графічного матеріалу | | | | | | | | | | |  | | | |  | |
| 1. Тема, мета, актуальність та предмет бакалаврської роботи. | | | | | | | | | | | | | | | | |
| 1. Аналіз вразливостей корпоративних мереж. | | | | | | | | | | | | | | | | |
| 1. Дослідження методів та засобів захисту даних в мережі. | | | | | | | | | | | | | | | | |
| 1. Рекомендації щодо побудови захищеної мережі на базі обладнання mikrtotik. | | | | | | | | | | | | | | | | |
| 1. Висновки за результатами роботи. | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | |
| 6. Дата видачі завдання | | | | | 24.02.2023 р. | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | | **КАЛЕНДАРНИЙ ПЛАН** | | | | | | | | | | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
| №  зп | Назва етапів  бакалаврської роботи | | | | | | | | | | | | | Строк виконання етапів бакалаврської роботи | | Примітка |
| 1. | Визначення актуальності проблеми захисту корпоративних мереж. | | | | | | | | | | | | | 24.02.2023 р. | |  |
| 2. | Аналіз наукової та технічної літератури з питань теми бакалаврської роботи. | | | | | | | | | | | | | 15.03.2023 р. | |  |
| 3. | Аналіз методів та засобів захисту даних в мережі. | | | | | | | | | | | | | 22.03.2023 р. | |  |
| 4. | Розроблення рекомендацій щодо застосування методів та засобів побудови захищених корпоративних мереж. | | | | | | | | | | | | | 12.04.2023 р. | |  |
| 5. | Оформлення результатів дослідження. | | | | | | | | | | | | | 10.05.2023 р. | |  |
| 6. | Підготовка доповіді до захисту. | | | | | | | | | | | | | 28.05.2023 р. | |  |
|  | | | | | | | | | | | | | |  | |  |
|  | |  | | | | | Студент | | | | Калабухов І.І. | | | | | |
|  | |  | | | | |  | | | | (підпис) | | | | прізвище та ініціали | |
|  | |  | | | | |  | | | |  | | | |  | |
| Керівник бакалаврської роботи | | | | | | | | | | |  | | | | Гайдур Г.І. | |
|  | |  | | | | |  | | | | (підпис) | | | | прізвище та ініціали | |
|  | |  | | | | |  | | | |  | | | |  | |

**РЕФЕРАТ**

Текстова частина бакалаврської роботи: 68 сторінок, 6 рисунків 18 джерел за посиланням.

*Об’єкт дослідження* — процес захисту корпоративних мереж.

*Предмет дослідження* ‒ методи та засоби захисту корпоративних мереж на базі обладнання Mikrotik.

*Мета роботи* ‒ розробити рекомендації щодо захисту корпоративних мереж на базі обладнання Mikrotik від сучасних атак.

*Методи дослідження* ‒ опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів, розробка рекомендацій та проведення експериментів.

В роботі проведено аналіз роботи корпоративних комп’ютерних мереж. На основі аналізу визначено види загроз та проведено їх класифікацію. Досліджено методи та засоби забезпечення безпеки корпоративних мереж на базі автоматизованих систем виявлення вторгнень на базі обладнання Mikrotik. Досліджено можливості програмних засобів захисту інформації в мережі.

Галузь використання ‒ кібербезпека корпоративних мереж.

ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ЛОКАЛЬНА КОМП’ЮТЕРНА МЕРЕЖА, ЗАХИСТ ЛОКАЛЬНИХ МЕРЕЖ, MIKROTIK, FIREWALL, NAT, МЕРЕЖЕВИЙ ТРАФІК.

**ЗМІСТ**

Стор.

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8](#_Toc134706239)

[ВСТУП 9](#_Toc134706240)

[1 АНАЛІЗ ПРОЦЕСУ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ 11](#_Toc134706241)

[1.1. Аналіз необхідності забезпечення мережевої безпеки корпоративної мережі 11](#_Toc134706242)

[1.2. Аналіз мережевих атак та загроз в корпоративній мережі 16](#_Toc134706243)

[1.2.2. Класифікація атак другого рівня моделі OSI 30](#_Toc134706244)

[1.3. Загальні підходи щодо вирішення проблеми побудови захищенної корпоративної мережі 33](#_Toc134706245)

[2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ В МЕРЕЖІ 37](#_Toc134706246)

[2.1. Методи ідентифікації та автентифікації користувачів корпоративної інформаційної системи 37](#_Toc134706247)

[2.2. Засоби цілісності та конфіденційності 41](#_Toc134706248)

[2.3. Методи віддаленого доступу до корпоративної інформаційної системи 45](#_Toc134706249)

[2.4. Архітектура мережі на базі Мikrotik та її функціональні можливості 47](#_Toc134706250)

[3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ MIKRTOTIK 49](#_Toc134706251)

[3.1. Призначення та функції RouterOS 49](#_Toc134706252)

[3.2. Рекомендації щодо налаштування Mikrotik 52](#_Toc134706253)

[3.3. Рекомендації налаштування firewall в RouterOS 60](#_Toc134706254)

[3.4 Основні рекомендації щодо побудові захищеної корпоративної мережі 66](#_Toc134706255)

[ВИСНОВКИ 68](#_Toc134706256)

[ПЕРЕЛІК ПОСИЛАНЬ 70](#_Toc134706257)

[ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 71](#_Toc134706258)

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ISP – internet service provider

CAR – committed access rate

SLA – service level agreement

HTTP – HyperText Transfer Protocol

FTP – File Transfer Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

ICMP – Internet Control Message Protocol

ARP – Address Resolution Protocol

SSL – Secure Sockets Layer

TLS – Transport Layer Security

NAT – Network Address Translation

DNS – Domain Name System

MNDP – Mikrotik Neighbors Discovery Protocol

WAN – Wide Area Network

LAN – Local Area Network

DDoS – Distributed Denial of Service

DoS – Denial Of Service

SNMP – Simple Network Management Protocol

# ВСТУП

*Актуальність теми.* У наш час мережеві технології розвиваються з величезною швидкістю. Зростають обчислювальні потужності, пропускна спроможність, розширюється спектр послуг, що пропонуються ISP, винаходять все нові механізми мережевої взаємодії.

Це націлено на об'єднання ресурсів та спільну роботу тисяч, мільйонів користувачів.

Все гостріше стоїть питання захисту ресурсів та розмежування доступу до них. На жаль, часто треті особи намагаються отримати (і отримують) доступ до конфіденційної інформації, що є інтелектуальною власністю компаній, до мережевих послуг, або ж спрямовують свої зусилля на руйнування працездатності окремих хостів чи всієї мережі.

Чим більше ресурсів компанія об'єднує у своїй корпоративній мережі, тим більше створюється загроз для них, тим важче забезпечити безпеку мережі.

Для надійного захисту ресурсів необхідно реалізовувати комплексний підхід забезпечення мережевої безпеки корпоративних мультисервісних мереж. Пропоновані рішення перед впровадженням мають бути всебічно (наскільки дозволяють час та можливості) протестовані у лабораторних умовах. Це стосується не тільки перевірки, обладнання та програмного забезпечення, а й підготовки кваліфікованого персоналу, здатного правильно з ним працювати.

*Об’єкт дослідження* — процес захисту корпоративних мереж.

*Предмет дослідження* ‒ методи та засоби захисту корпоративних мереж на базі обладнання Mikrotik.

*Мета роботи* ‒ розробити рекомендації щодо захисту корпоративних мереж на базі обладнання Mikrotik від сучасних атак.

Наукова новизна одержаних результатів. Новими науково-обґрунтованими результатами, які отримані в роботі, є опрацювання новітніх технологій в галузі безпеки мереж.

Практичне значення одержаних результатів. Нові наукові результати, отримані в роботі, можуть бути використані при подальшому проектуванні та захищених корпоративних мереж.

# 1 АНАЛІЗ ПРОЦЕСУ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ

## 1.1. Аналіз необхідності забезпечення мережевої безпеки корпоративної мережі

З колосальним сплеском кібератак і високою залежністю від технологій у цю цифрову епоху забезпечення **безпеки даних та інформації** стало складним завданням. Кіберзагрози значно прискорюються навіть швидше, ніж удосконалення компаній. Завдяки глобалізації комп’ютерні мережі стали більшими, і їх взаємозв’язок за допомогою глобальної мережі (WAN) поширений у всьому світі.

На базовому рівні безпека мережі – це захист даних, програм, пристроїв і систем, підключених до мережі.

Хоча безпека мережі та кібербезпека багато в чому перетинаються, безпеку мережі найчастіше визначають як підмножину кібербезпеки. Використовуючи традиційну «аналогію із замком і ровом» або підхід до безпеки на основі периметра, згідно з яким організація є фортецею, а дані, що зберігаються в замку, є короною, безпека мережі найбільше стурбована безпекою всередині замку.

У цьому сценарії, заснованому на периметрі, область у стінах замку може представляти ІТ-інфраструктуру підприємства, включаючи її мережеві компоненти, апаратне забезпечення, операційні системи, програмне забезпечення та сховище даних. Безпека мережі захищає ці системи від шкідливих програм/ [вимагачів](https://www-ibm-com.translate.goog/topics/ransomware?_x_tr_sl=en&_x_tr_tl=uk&_x_tr_hl=uk) , розподілених атак типу «відмова в обслуговуванні» (DDoS), мережевих вторгнень тощо, створюючи безпечну платформу для користувачів, комп’ютерів і програм для виконання своїх функцій у ІТ-середовищі.

Оскільки організації переходять до гібридних і багатохмарних середовищ, їхні дані, програми та пристрої розосереджуються по місцях і географіях. Користувачі хочуть отримати доступ до корпоративних систем і даних з будь-якого місця та з будь-якого пристрою. Таким чином, традиційний підхід до безпеки мережі, заснований на периметрі, поступово припиняється. Підхід до безпеки без [довіри](https://www-ibm-com.translate.goog/security/zero-trust?_x_tr_sl=en&_x_tr_tl=uk&_x_tr_hl=uk), коли організація ніколи не довіряє і завжди перевіряє доступ, швидко стає новим методом посилення безпеки організації.

Компанія Cisco розробила процес, який вони називають «Оцінка стану безпеки» (SPA), щоб описати зусилля компанії щодо безпеки мережі як живої сутності, що розвивається. SPA представлено графічно на рисунку 1.1.

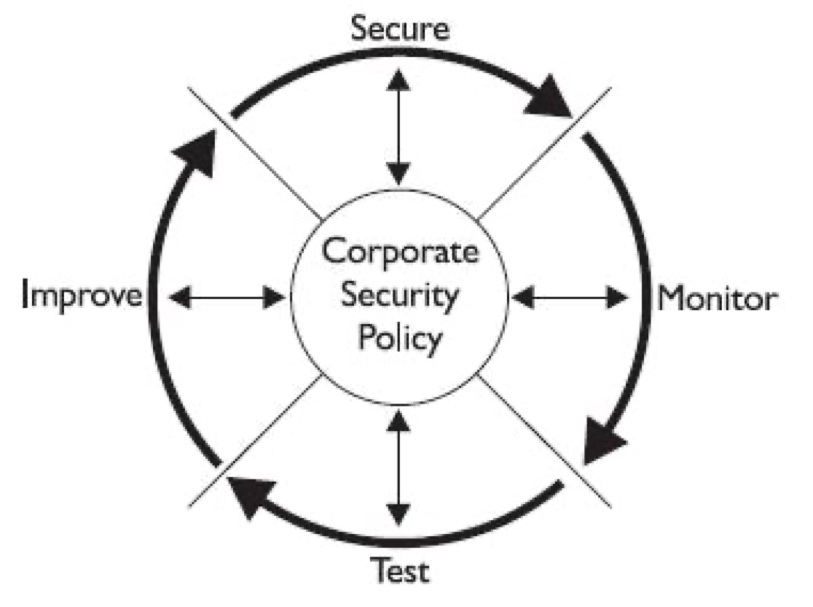


Рис. 1.1. Життєвий цикл безпеки Cisco Security Wheel

Як показано на рисунку, розробка програми мережевої безпеки — це повторюваний процес, яким необхідно постійно керувати, щоб зменшити ризик втрати, одночасно ефективно використовуючи ресурси компанії.

Припустимо, що ця графіка та процес, який вона представляє, можуть бути частиною всіх чотирьох іспитів безпеки. Коли стає відомо про нову технологію, потрібно переконатись, що ця технологія підходить до колеса безпеки. Наприклад, системи виявлення вторгнень (IDS) будуть частиною процесу моніторингу.

Навіть якби компанія мала капітальні ресурси та намагалася розробити «ідеальне» рішення безпеки мережі, це все одно було б лише початком поточного процесу. Подібно ідеальній хвилі для серфінгіста чи ідеальному бризу для моряка, ідеальна система безпеки – це в кращому випадку момент часу, якщо не ілюзія. Фактори, які змусили компанії запровадити систему безпеки, активно розвивалися та змінювалися водночас. Майже постійні зміни, що відбуваються в технологіях, що використовуються в мережі, типи та джерела загроз, навіть зміни в потоках даних всередині організації постійно створюють нові ризики, які необхідно передбачити та зменшити. Колесо визначає чотири етапи розробки безпечної системи.

Безпека

Після ретельного вивчення політики безпеки настав час захистити мережу, впровадивши процеси та технології, необхідні для захисту даних та інтелектуальних ресурсів організації. Вони можуть включати такі технології, як VPN для дистанційної роботи та розташування відділень, або додавання брандмауерів у мережу.

Моніторинг

Необхідно відстежувати процеси та технології безпеки, щоб переконатися, що вони забезпечують очікувану безпеку. Це може включати різноманітні дії, починаючи від сканування файлів журналу до використання програмного забезпечення для керування мережею для виявлення вторгнень, невдалих спроб і внутрішнього зловживання ресурсами.

Тестування

Етап тестування може включати тестування нових процесів, щоб переконатися, що вони відповідають очікуванням, тестування встановлених процесів, щоб перевірити, чи внутрішні чи зовнішні зміни не зробили їх менш безпечними, а також періодичні аудити, щоб переконатися, що всі процеси та політики впроваджуються відповідно до плану та чи належним чином вирішуються проблеми безпеки.

Удосконалення

Етап удосконалення передбачає розробку нових планів коригування програми безпеки відповідно до змін у внутрішньому та зовнішньому середовищі. Від впровадження «поетапних» удосконалень, які були вбудовані в початковий план, до реакції на останню загрозу безпеці, яка може переслідувати мережу, вдосконалення як технологій, так і процесів є обов’язковими.

У центрі колеса знаходиться політика безпеки мережі, яку іноді називають корпоративною або корпоративною політикою безпеки мережі. Цей компонент, якщо він правильно реалізований, є планом для чотирьох еволюційних процесів колеса, яким слідувати.

В основі даного представлення лежить корпоративна політика безпеки (Corporate Security Policy), на яку спираються чотири складові: Secure (Забезпечення безпеки), Monitor (Моніторинг), Test (Перевірка), Improve (Поліпшення системи).

Перш ніж проектувати реальну схему захисту мережі, слід виробити адекватну безпекову політику, що визначає ряд моментів:

* План придбань та реалізацій щодо забезпечення безпеки
* Допустимі та заборонені технології
* План дій у разі інцидентів
* Допустима поведінка персоналу
* Санкції на порушення
* Ієрархію відповідальності за реалізацію, підтримку, аудит, моніторинг
* Напрямок подальшого розвитку системи безпеки

Політика безпеки – це формальний виклад правил, яким повинні підпорядковуватися особи, які отримують доступ до корпоративної технології та інформації, це затверджений документ, що є результатом компромісу між безпекою та простотою використання, безпекою та послугами, що надаються, і, нарешті, між ціною системи та ризиками втрати доступу.

Сам документ розбивається на частини – субполітики, що описують окремі елементи схеми безпеки, такі, наприклад, як:

* Віддалений доступ (Remote Access Policy)
* Аутентифікацію (Authentication Policy)
* Антивірусні засоби (Antivirus Policy)
* Парольна політика (Password Policy)

Слід окремо згадати позицію компанії (організації) щодо підготовки персоналу. Наприклад, стаття «Кожен співробітник як брандмауер» описує позиції компаній, які витрачають не малих грошей на постійну перепідготовку та перевірку персоналу. Результатом таких дій є різке зниження успішності проведення соціальної інженерії та посилення системи безпеки щодо внутрішніх загроз. Якою б якісною і дорогою не була система, якщо персонал не дотримується правил, закріплених у політиці, то вона марна.

Як би не намагалися, і скільки б коштів не вкладали, абсолютної безпеки досягти неможливо. Безпека та доступність – в асимптотиці речі обернено пропорційні. Завжди є причини, що викликають труднощі у захисті. Їх можна класифікувати на 3 групи.

Технологічні вразливості – спочатку TCP/IP винаходився без урахування будь-яких вимог безпеки. Усі операційні системи містять уразливі місця, які постійно виявляються та усуваються. Вразливість ОС несе загрозу ресурсам, якими вона управляє.

Слабкість політики безпеки – сюди можна віднести недолік моніторингу системи, відсутність плану відновлення у разі збою, або відсутність політики безпеки як такої.

Неправильне налаштування обладнання – використання паролів за замовчуванням або взагалі їх відсутність, залишення непотрібних послуг та портів увімкненими.

Отже, аналіз забезпечення мережевої безпеки корпоративної мережі є важливою складовою для покращення безпеки в організаціях. З метою забезпечення безпеки, організації мають проводити аналіз наявних мереж для ідентифікації потенційних загроз та слабких місць.

Під час аналізу вдосконалення мережевої безпеки організаціям необхідно провести оцінку наступних аспектів:

* Аналіз архітектури мережі - включає оцінку наявних компонентів мережі, в тому числі пристроїв мережевої інфраструктури;
* Аналіз ідентифікації та аутентифікації - має на меті перевірку, наскільки ефективним є процес ідентифікації та аутентифікації користувачів мережі, а також перевірку наявності системи контролю доступу;
* Аналіз захисту мережевих ресурсів - оцінює наявність заходів захисту мережевих ресурсів від несанкціонованого доступу, вірусів, шкідливого програмного забезпечення та інших загроз.
* Аналіз моніторингу та логування - включає перевірку наявності системи моніторингу та логування, які дозволяють виявляти та аналізувати потенційні загрози та атаки.

## 1.2. Аналіз мережевих атак та загроз в корпоративній мережі

**1.2.1. Класифікація мережевих атак та загроз**

Мережеві атаки — це несанкціоновані дії з цифровими активами в організаційній мережі. Зловмисники зазвичай здійснюють мережеві атаки, щоб змінити, знищити або викрасти особисті дані. Зловмисники під час мережевих атак намагаються націлитися на периметр мережі, щоб отримати доступ до внутрішніх систем.

Існує два основних типи мережевих атак: пасивні та активні. Під час пасивних мережевих атак зловмисники отримують несанкціонований доступ до мереж, контролюють і викрадають особисті дані, не вносячи жодних змін. Активні мережеві атаки передбачають зміну, шифрування або пошкодження даних.

Після проникнення зловмисники можуть використовувати інші хакерські дії, такі як застосування зловмисного програмного забезпечення та атаки на кінцеві точки, щоб атакувати мережу організації. Оскільки все більше організацій використовують віддалену роботу, мережі стають більш вразливими до крадіжки та знищення даних.

Сучасні організації покладаються на Інтернет для спілкування, і конфіденційні дані часто обмінюються між мережами. Віддалений доступ також надає зловмисникам вразливі цілі для перехоплення даних. Це може порушити налаштування конфіденційності користувача та зламати пристрої, підключені до Інтернету.

Мережеві атаки відбуваються в різних формах. Підприємствам необхідно переконатися, що вони підтримують найвищі стандарти кібербезпеки, політики мережевої безпеки та навчання персоналу для захисту своїх активів від дедалі складніших кіберзагроз.

Загроза – це ризик втрати внаслідок настання низки подій випадково або чиїхось навмисних дій.

Зняття ризиків збитків від випадковості здійснюється за допомогою надмірності схеми мережі. Надмірність досягається за рахунок додавання додаткового обладнання, що призводить до підвищення ціни на мережеве обладнання. Однак це неминуче, якщо компанії хочуть досягти високої надійності системи. Наприклад, може знадобитися забезпечити середній час між збоями (MTBF – mean time between fail) 99.9%. Це приблизно 1 година простою на 11 років роботи.

Ризики втрат від чиїхось навмисних дій знімаються застосуванням комплексного підходу до забезпечення безпеки корпоративної мережі.

Існує чотири основні типи загроз даної категорії:

* непідготовлені загрози (unstructured threats)
* підготовлені погрози (structured threats)
* внутрішні загрози (internal threats)
* зовнішні загрози (external threats)

Непідготовлені загрози ⎯ реалізуються не кваліфікованими суб'єктами, з обмеженими навичками та знаннями у сфері мережевої безпеки. Вони не створюють і не модифікують інструменти злому, а використовують вже готові продукти.

Підготовлені загрози ⎯ здійснюються високо кваліфікованим, мотивованим зловмисником або групою осіб. Усі їхні атаки заздалегідь добре сплановані і ведуться не в сліпу або навмання, а за цілком конкретними точками певної мережі. Вони можуть самі створювати та модифікувати існуючі інструменти злому.

Основою внутрішніх загроз ⎯ є особа, яка має доступ до внутрішніх ресурсів організації, тобто є внутрішнім резидентом компанії. Якщо до всього іншого ця особа вступить у змову із зовнішньою професійною групою, то отримаємо підготовлену внутрішню загрозу, захиститися від якої дуже складно, оскільки практично неможливо уникнути втрат. Їх ступінь визначатиметься рівнем доступу службовця до ресурсів.

Зовнішня загроза ⎯ походить від осіб, що знаходяться поза периметром оборони (може бути як підготовленою, так і ні).

Метою мережевої атаки може бути:

* розвідка (reconnaissance attack)
* отримання доступу (access attack)
* відмова в обслуговуванні (DoS attack)
* маніпуляція даними (data manipulation attack)

У загальному доступі є безліч програм – інструментів злому. Так, наприклад, будь-хто може дістати собі такі відомі утиліти підбору паролів як L0pht Crack, PWLVIEW, Pwlhack, PWL\_Key, ntPassword; або утиліти розвідки: NMAP, SATAN, Portscanner, Strobe. Їх можна використовувати й у і в своїх цілях – перевірка якості пароля або виявлення недоліків конфігурації апаратури та програмного забезпечення (наприклад, не вимкнено SNMP там, де не передбачається його використовувати).

**Сніфери пакетів**

Атаки з перехопленням — це крадіжка даних, здійснена шляхом захоплення мережевого трафіку за допомогою сніферів пакетів, які можуть незаконно отримувати доступ до незашифрованих даних і зчитувати їх. Пакети даних збираються, коли вони проходять через комп’ютерну мережу. Перехоплювальні пристрої або медіа, які використовуються для здійснення цієї атаки та збору пакетів мережевих даних, відомі як перехоплювачі пакетів.

Загалом, сніфер пакетів відноситься до апаратного чи програмного забезпечення, яке відстежує мережевий трафік шляхом захоплення пакетів. Він також відомий як аналізатор пакетів, аналізатор протоколів або аналізатор мережі. Сніфери аналізують потоки пакетів даних, які проходять між комп’ютерами в мережі, а також між мережевими системами та Інтернетом. Ці пакети розроблено для конкретних машин, але за допомогою аналізатора пакетів у «безладному режимі» ІТ-фахівці, кінцеві користувачі чи зловмисники можуть перевірити будь-який пакет, незалежно від місця призначення.

Сніфери можна налаштувати двома способами.

Перший — «нефільтрований», який захоплює всі можливі пакети та зберігає їх на локальному жорсткому диску для подальшої перевірки.

Другий — «відфільтрований», що означає, що аналізатори збиратимуть лише пакети, що містять певні компоненти даних. Системні адміністратори часто використовують сніфери для усунення несправностей або дослідження мережі. Проте хакери можуть скористатися цією технологією для проникнення в мережу, що призведе до атаки з перехопленням пакетів.

За замовчуванням мережеві карти ігнорують неадресований трафік. Атаки з перехопленням вимагають, щоб мережеві карти були налаштовані на безладний режим, який дозволяє мережевим картам отримувати весь мережевий трафік. Сніфери можуть прослуховувати весь трафік, що проходить через мережеві карти, декодуючи закодовану інформацію в пакетах даних. Сніфінгові атаки стають більш доступними завдяки слабко зашифрованим пакетам даних.

Сніфінг можна класифікувати на два види: активний і пасивний.

Активне перехоплення: це техніка введення в мережу протоколів розпізнавання адрес (ARP) для перевантаження таблиці пам’яті адрес комутатора (CAM). У результаті законний трафік перенаправляється на інші порти, дозволяючи зловмиснику прослухати трафік від комутатора. Методології активного перехоплення використовуються для атак спуфінгу, атак на протокол динамічної конфігурації хоста (DHCP) і отруєння системи доменних імен (DNS).

Пасивне перехоплення:воно складається виключно з прослуховування та зазвичай використовується в мережах, з’єднаних концентраторами. Трафік видимий для всіх хостів у цій формі мережі. Щоб непомітно контролювати мережу компанії, хакери часто використовують один із двох підходів до пасивного перехоплення.

У випадку організацій, які використовують концентратори для з’єднання кількох пристроїв в одній мережі, хакери можуть використовувати сніфер, щоб пасивно «шпигувати» за всім трафіком, що проходить через систему. Цей вид пасивного нюхання неймовірно важко виявити.

**IP-спуфінг**

Комп’ютерні мережі спілкуються через обмін мережевими пакетами даних, кожен з яких містить кілька заголовків, які використовуються для маршрутизації та забезпечення безперервності передачі. Одним із таких заголовків є «Source IP Address», який вказує IP-адресу відправника пакету.

Підробка IP-адреси — це акт фальсифікації вмісту в заголовку Source IP, як правило, за допомогою випадкових чисел, щоб приховати особу відправника або запустити відображену DDoS-атаку, як описано нижче. IP-спуфінг є функцією за замовчуванням у більшості наборів шкідливих програм DDoS і сценаріїв атак, що робить його частиною більшості DDoS-атак на мережевому рівні.

Підробка IP-адреси використовується в DDoS-атаках з двох причин: для маскування розташування пристроїв ботнету та для організації відображеного нападу.

**Відмова в обслуговуванні (Denial of Service - DoS).**

DoS є найвідомішою формою атак хакерів. Вони прості у реалізації і можуть завдати величезної шкоди. Крім того, проти атак такого типу складно створити стовідсотковий захист.

Атаки DDoS (розподілена відмова в обслуговуванні) передбачають розгортання мереж ботнетів — доступ до яких був отриманий за допомогою зловмисного програмного забезпеченням пристроїв, підключених до Інтернету. Вони атакують і переповнюють корпоративні сервери великими обсягами шахрайського трафіку. Зловмисники зазвичай обирають чутливі до часу дані, наприклад дані, що належать установам охорони здоров’я, перериваючи доступ до важливих записів бази даних пацієнтів.

Типи DoS атак:

* TCP SYN Flood
* Ping of Death
* Tribe Flood Network (TFN) та Tribe Flood Network 2000 (TFN2K)
* Trinco
* Stacheldraht
* Trinity

Атаки DoS відрізняються від інших типів атак. Вони не націлені на отримання доступу до вашої мережі або на отримання будь-якої інформації. Атака DoS робить вашу мережу недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми. У разі використання деяких серверних програм (таких як web-сервер або FTP-сервер) атаки DoS можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих програм, і тримати їх у зайнятому стані, не допускаючи обслуговування звичайних користувачів. Під час атак DoS можуть використовуватися звичайні Інтернет-протоколи, такі як TCP та ICMP. Більшість атак DoS спирається не на програмні помилки або проломи в системі безпеки, а на загальні слабкості системної архітектури. Деякі атаки зводять до нуля продуктивність мережі, переповнюючи її небажаними та непотрібними пакетами або повідомляючи неправдиву інформацію про поточний стан мережевих ресурсів.

Існує два різновиди атак даного типу: DDoS (distributed denial of service) – розподілена відмова в обслуговуванні та DRDoS (distributed reflection denial of service) – це форма розподіленої атаки на відмову в обслуговуванні (DDoS), яка покладається на загальнодоступні сервери UDP і коефіцієнти посилення пропускної здатності (BAF), щоб перевантажити систему жертви трафіком UDP.

Атака типу DDoS починається з розміщення на різних комп'ютерах програм-ботів (Zombie), які координуються з єдиної машини (Zombie-master), що ініціює атаку.

Завдання ботів – здійснювати безперервну посилку пакетів (флуд) на цільову адресу (це може бути як окремий хост, так і точка виходу цілої мережі). Таким чином здійснюється перекриття всієї доступної пропускної спроможності (або заняття інших важливих ресурсів).

Відмінність атаки DRDoS від попередньої полягає у використанні як посередників між атакуючим і ціллю легальних TCP серверів. Джерело (або кілька джерел) посилає на них ехо-запити (ping) або запити на TCP з'єднання зі спуфнутою (підмінененою) адресою джерела, в якості якого вказує адресу мети. І відповіді багатьох хостів приходять у єдину точку, поглинаючи всю пропускну спроможність.

Загроза атак типу DoS може знижуватися трьома способами:

Функції антиспуфінгу. Правильна конфігурація функцій антиспуфінгу на маршрутизаторах і мережевих екранах допоможе знизити ризик DoS. Ці функції, як мінімум, повинні включати фільтрацію RFC 2827. Якщо хакер не зможе замаскувати свою справжню особистість, він навряд чи наважиться провести атаку.

Функції анти-DoS. Правильна конфігурація функцій анти-DoS на маршрутизаторах та мережевих екранах може обмежити ефективність атак. Ці функції часто обмежують кількість напіввідкритих каналів у будь-який час.

Обмеження обсягу трафіку (traffic rate limiting). Якщо трафік, призначений для переповнення вашої мережі, не зупинити до точки входу в мережу, то зупинити його вже не можна, тому що вся смуга пропускання буде зайнята. Звичайним прикладом є обмеження обсягів трафіку ICMP. Під час укладання договору з провайдером на надання послуг (SLA – service level agreement) слід обговорити застосування технології обмеження доступу (CAR – committed access rate).

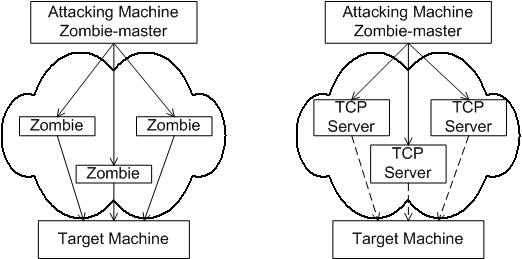


Рис. 1.2. Схема атак типу DDoS, DRDoS

**Парольні атаки**

Атаки на паролі передбачають використання несправної вразливості авторизації в системі в поєднанні з інструментами автоматичної атаки паролів, які пришвидшують перебір та злам паролів. Зловмисник використовує різні методи для доступу до облікових даних легітимного користувача та викриття його, отримуючи його особу та привілеї. Комбінація імені користувача та пароля є одним із найстаріших відомих методів автентифікації облікового запису, тому зловмисники мали час створити багато методів отримання паролів, які можна зламати. Крім того, програми, які використовують паролі як єдиний фактор автентифікації, вразливі до парольних атак, оскільки вразливості добре зрозумілі.

Атаки на паролі мають серйозні наслідки, оскільки зловмисникам потрібен лише логін та пароль щоб отримати доступ до одного з привілейованих облікових записів, щоб зламати веб-програму. Залежно від даних, які розміщує програма, скомпрометовані паролі можуть прокласти шлях до розкриття конфіденційної інформації, розподіленої відмови в обслуговуванні, фінансового шахрайства та інших складних атак.

Для цих атак використовують програмне забезпечення, яке пришвидшує злам паролів. Найпоширеніші методи атаки включають грубий перебір, атаки за словником та введення облікових даних.

Перебір — це спроба вгадати пароль шляхом перебору всіх можливих комбінацій набору допустимих символів.

Словникові атаки намагаються вгадати паролі шляхом повторення часто використовуваних паролів, таких як слова зі словника та їх прості варіації.

Замість того, щоб спробувати кілька паролів для одного облікового запису, розпилення паролів перевіряє невелику кількість загальних паролів для багатьох облікових записів, сподіваючись отримати доступ принаймні до одного з них. Цей метод допомагає уникнути правил блокування облікового запису, і його важче виявити.

**Атаки на рівні додатків**

Атаки на прикладному рівні – це спроби отримати неавторизований доступ до серверів організації через уразливості програмного забезпечення. Ці атаки різняться за серйозністю, складністю та технікою, залежно від типу програми, яку ви використовуєте. Ці атаки можуть бути численними та різноманітними, тому не існує єдиної точки входу для хакерів. Таким чином, кількість атак на прикладному рівні дорівнює кількості вразливостей у мережевій інфраструктурі організації. Атаки на прикладному рівні можуть бути наслідком веб-скриптів, які обманом змушують користувачів відкривати шкідливі документи надіслані електронною поштою чи заражених через флеш-накопичувач USB. Існують тисячі способів знайти та використати вразливості для доступу до незахищених мереж.

Зловмисники розробляють нові типи атак і вектори, які будуть. Коли захисник добре блокує ці нові атаки, зловмисник розробляє новий тип атаки та повторює цей цикл. Зростання небезпечних пристроїв IoT за останні роки принесло користь зловмисникам DDoS, оскільки кількість інтелектуальних пристроїв, які можна використовувати для більш просунутих атак на прикладному рівні, майже необмежена.

Деякі поширені типи атак прикладного рівня:

* BGP hijacking
* Slowloris
* Show post
* Slow read
* HTTP(/s) flooding
* Low and slow attack
* Large payload post
* Mimicked user browsing

Ось деякі заходи, які можна зробити, щоб знизити вразливість від атак цього типу:

* Читання лог-файлів операційних систем та мережевих лог-файлів, їх аналіз за допомогою спеціальних програм.
* Оформлення підписки на послуги з розсилки даних про слабкі місця прикладних програм (Bugtrad та CERT).
* Використання найсвіжіших версій операційних систем і додатків та останніх корекційних модулів (патчів).
* Використання програмно-апаратних систем розпізнавання атак (IDS).

**Мережева розвідка**

Мережевою розвідкою називається збір інформації про мережу за допомогою загальнодоступних даних та програм. Під час підготовки атаки проти будь-якої мережі хакер, як правило, намагається отримати про неї якомога більше інформації. Мережева розвідка проводиться у формі запитів DNS, луна-тестування (ping sweep) та сканування портів. Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цього домену надано. Ехо-тестування (ping sweep) адрес, розкритих за допомогою DNS, дозволяє побачити, які хости реально працюють у цьому середовищі. Отримавши список хостів, хакер використовує засоби сканування портів, щоб скласти повний список послуг, що підтримуються цими хостами. І, нарешті, хакер аналізує характеристики додатків, які працюють на хостах. В результаті видобувається інформація, яку можна використовувати для злому.

Повністю позбутися мережевої розвідки неможливо. Якщо, наприклад, відключити ICMP на периферійних маршрутизаторах, можна позбавитись ехо-тестування, але втрачаються дані, необхідні діагностики мережевих збоїв. Крім того, сканувати порти можна і без попереднього ехо-тестування. Просто це займе більше часу, тому що сканувати доведеться і неіснуючі IP-адреси. Системи IDS на рівні мережі і хостів зазвичай добре справляються із завданням повідомлення адміністратора про мережну розвідку, що ведеться, що дозволяє краще підготуватися до майбутньої атаки і оповістити провайдера (ISP), в мережі якого встановлена система, що виявляє надмірну цікавість.

**Зловживання довірою**

Зловживання довірою є потужним інструментом для зловмисників, оскільки воно дозволяє їм обійти заходи безпеки та отримати доступ до конфіденційної інформації чи мереж, не будучи виявленими. Це може статися, коли зловмисник отримав привілейований доступ, наприклад обліковий запис адміністратора, і використовує його для отримання доступу до конфіденційної інформації або для здійснення зловмисних дій. Його також можна використовувати для маніпулювання системами, а також здійснювати атаки на відмову в обслуговуванні, крадіжку даних і атаки програм-вимагачів.

Зловживання довірою з DNS і SMTP – це різновид кіберзагрози, яка передбачає несанкціоноване використання протоколу DNS (система доменних імен) або SMTP (простий протокол передачі пошти) для отримання доступу до конфіденційних даних або мереж. Ці шахрайства зазвичай здійснюються зловмисниками, які можуть використовувати слабкі місця в протоколі DNS або SMTP, щоб отримати доступ до конфіденційної інформації або мереж.

Наприклад, зловмисники можуть використовувати DNS або SMTP для надсилання зловмисних електронних листів із шкідливими посиланнями або запитами.

Зловживання довірою може мати серйозні наслідки. Організаціям важливо переконатися, що їхні співробітники та інші користувачі знають про ризики, пов’язані зі зловживанням довірою, і переконатися, що вжито відповідних заходів для захисту їхніх даних і мереж.

**Переадресація портів**

Переадресація портів — це метод тунелювання та перенаправлення мережевого трафіку через різні порти для обходу брандмауерів або доступу до обмежених ресурсів. ЇЇ можна використовувати щоб отримати доступ до системи без відома або згоди користувача. Наприклад, зловмисник може використовувати переадресацію портів, щоб отримати доступ до мережі або зламати систему без відома користувача. Крім того, перенаправлення портів можна використовувати для обходу заходів безпеки та збільшення поверхні атаки системи.

Цей тип атаки є різновидом зловживання довірою, коли скомпрометована машина використовується для передачі даних через мережевий екран, який інакше був би обов'язково скинутий. Прикладом такої програми, яка має такі можливості, є netcat.

Основним способом боротьби із переадресацією портів є використання надійних моделей довіри. Крім того, завадити встановленню небажаних програмних засобів на хості може хост-система IDS (HIDS).

**Несанкціонований доступ**

Несанкціонований доступ означає отримання особами доступу до даних, мереж, кінцевих точок, програм або пристроїв організації без дозволу. Це тісно пов’язане з автентифікацією – процесом, який перевіряє особу користувача під час доступу до системи. Зламані або неправильно налаштовані механізми автентифікації є основною причиною доступу неавторизованих сторін.

Блокування несанкціонованого доступу відіграє центральну роль у запобіганні витоку даних. Однак надійна програма безпеки використовує «поглиблений захист» – кілька рівнів захисту безпеки, намагаючись пом’якшити атаки задовго до того, як зловмисники досягнуть чутливої системи. Додаткові рівні безпеки включають захист мережі, захист кінцевої точки та захист даних.

Типове порушення безпеки відбувається в три етапи:

Дослідження — зловмисник шукає слабкі місця або вразливі місця в організаційних системах, людях або процесах.

Мережева/соціальна атака — зловмисник намагається проникнути на периметр мережі, уникаючи захисту мережі або використовуючи соціальну інженерію, щоб обманом змусити людей надати доступ, дані чи облікові дані.

Ексфільтрація — як тільки зловмиснику вдається отримати доступ, він може викрасти цінні активи або завдати шкоди в точці входу, а також виконати бічний рух, щоб отримати доступ до додаткових, більш цінних систем.

**Віруси та троянські коні**

Віруси та трояни є одними з найнебезпечніших загроз кібербезпеці та безпеці мережі через їх здатність поширюватися мережами та пристроями, викрадати конфіденційну інформацію та пошкоджувати чи видаляти дані.

Традиційне антивірусне програмне забезпечення є важливим для виявлення та видалення вірусів і троянів, але цього недостатньо для захисту від найсучасніших загроз. Щоб зменшити ризик зараження, важливо мати багаторівневу безпеку, включаючи надійні брандмауери, регулярні виправлення та оновлення, навчання користувачів та інші заходи для забезпечення безпеки мереж.

Ефективним засобом боротьби можна вважати технологію IAS (Intelligent Application Switching). В основі лежить фільтрація на основі змісту трафіку. IAS дозволяє виловлювати шкідливі програми та спам. Згідно дослідженнями деякі компанії, які використовують у себе на магістральних вузлах IAS, звільнили до 20% їхньої пропускної спроможності від непотрібного трафіку.

**Соціальна інженерія**

Соціальна інженерія – це тип атаки, який використовують хакери та кіберзлочинці для отримання доступу до конфіденційної інформації чи облікових даних. Це форма маніпуляції, призначена для використання людської психології та поведінки, часто шляхом використання довіри та стосунків людини.

Існує кілька методів захисту від атак соціальної інженерії. Одним із найважливіших є усвідомлення потенційних загроз і розпізнавання будь-якої підозрілої діяльності. Організації також повинні навчати своїх співробітників про небезпеку соціальної інженерії та впроваджувати заходи безпеки, такі як обмеження доступу до конфіденційної інформації та вимога двофакторної автентифікації для певних операцій.

Крім того, організації повинні запровадити захищену мережеву архітектуру та використовувати програмне забезпечення, розроблене спеціально для виявлення та запобігання атакам соціальної інженерії. Нарешті, важливо мати план реагування на інциденти, щоб забезпечити швидке й ефективне усунення будь-якого потенційного порушення безпеки.

**Статистика атак на організації**

Cybersecurity Ventures також повідомляє, що кіберзлочинність є найбільшим переміщенням економічного багатства в історії. До 2025 року кіберзлочинність коштуватиме компаніям у всьому світі приблизно 10,5 трлн доларів щорічно, порівняно з 3 трлн доларів у 2015 році. При темпах зростання на 15 відсотків за рік.

Згідно з дослідженням Accenture Cost of Cybercrime Study, 43% кібератак спрямовані на маленькі організації, але лише 14% готові захистити себе.

Кібератака не тільки порушує нормальну роботу, але й може завдати шкоди важливим ІТ-активам та інфраструктурі, які неможливо відновити без бюджету чи ресурсів для цього.

Організації намагаються захистити себе через це. Згідно зі звітом про стан кібербезпеки Інституту Ponemon, повідомляє ситуацію у всьому світі про нещодавній досвід кібератак:

* Недостатні заходи безпеки: 45% кажуть, що їхні процеси неефективні для пом’якшення атак;
* Частота атак: 66% зазнавали кібератак за останні 12 місяців;
* Історія атак: 69% стверджують, що кібератаки стають більш цілеспрямованими.

Найпоширеніші типи атак на 2023 рік:

* Фішинг/соціальна інженерія: 57%
* Зламані/викрадені пристрої: 33%
* Крадіжка облікових даних: 30%

Розуміючи цілі атак і наслідки, фахівці з кібербезпеки можуть мінімізувати та навіть запобігти майбутнім атакам.

## 1.2.2. Класифікація атак другого рівня моделі OSI

Атаки на другому рівні моделі OSI стосуються атак, спрямованих на рівень каналу даних. Цей рівень відповідає за фізичну адресацію, виявлення та виправлення помилок, а також надійний мережевий зв’язок між пристроями. Зловмисники можуть використовувати атаки на відмову в обслуговуванні, ARP-спуфінг і MAC-флуд, щоб скомпрометувати цей рівень і перехопити трафік або збити мережу. Оскільки цей рівень є основою для всіх інших рівнів і є інтерфейсом між фізичною та логічною частинами мережі, зловмисники можуть сильно вплинути на всю систему, націлившись на цей рівень.

**ARP-злом та САМ-переповнення.**

Багато мережевих адміністраторів вважають, що підключення сервера через комутатор є панацеєю від перехоплення мережного трафіку. Однак, це не так. Існує низка програм – активних сніферів, здатних реалізовувати такий злом.

Активний сніфер (наприклад, angst) здатний працювати у двох режимах. Перший називається man-in-the-middle. Після старту програма починає моніторити адреси arp-запитів, а потім включає arp forwanding на станції, де вона запущена, посилаючи на arp-запит відповідь, що mac-адреса псевдофорвардера відповідає всім ip-адресам в даній мережі.

Для роботи комутатор динамічно будує таблицю відповідності MAC – порт. Другий метод полягає в наповненні мережі помилковими (спуфнутими) МАС адресами, САМ-пам'ять комутатора переповниться і він переходить у режим роботи «концентратор» (hub). Ефект мікросегментації усувається, і сніфер починає слухати весь трафік на своєму порту.

**Атака на STP**

Шляхом підключення пристрою з низьким пріоритетом або за допомогою інструмента генерації пакетів STP (BPDU – bridge protocol data unit) можна частково або повністю перекласти весь трафік VLAN і успішно його аналізувати. Якщо зловмисник має доступ до двох портів на різних комутаторах, видаючи себе за корінь дерева STP, він отримує трафік віртуальної локальної мережі.

Якщо через невеликі проміжки часу хакер мінятиме пріоритет, змушуючи протокол постійно перераховувати дерево, вийде атака типу DoS.

Для захисту від STP-злому компанія Mikrotik доповнила програмне забезпечення для комутаторів опціями:

* захист порту – заборона порту приймати BPDU (bpdu filter)
* захист кореня – заборона знаходження за цим портом кореня.

Зловмисник здебільшого зможе підключитися лише до портів доступу комутатора. Ці заходи повністю блокують його від будь-яких впливів на STP.

**Атака на HSRP**

Протокол HSRP (Hot Standby Router Protocol) реалізує надмірну експлуатацію кількох маршрутизаторів, доступних під одним віртуальним IP та МАС. Між собою маршрутизатори обмінюються багатоадресними пакетами (224.0.0.2). На основі пріоритету визначається активний, який відповідає за обробку та передачу всього трафіку.

Якщо порушник може розсилати HSRP-пакети з найбільшим пріоритетом, він може:

* перевести всі маршрутизатори в неактивний стан, таким чином реалізуючи атаку типу DoS
* перевести весь трафік на себе

Для захисту рекомендується використовувати протокол IPSec для шифрування трафіку HSRP.

Найбільш відомим інструментом атаки на HSRP та STP є Irpas.

**Атака на DTP та VTP**

Зазвичай мережеві адміністратори вручну конфігурують усі транкові порти. Однак цей процес можна автоматизувати за допомогою DTP (Dynamic Trunk Protocol). Комутатори самі визначатимуть, що за пристрої підключені до портів і, за потреби, переводити їх у режим магістралі.

Процес настроювання параметрів віртуальних локальних мереж можна автоматизувати за допомогою VTP (VLAN Trunking Protocol). Тоді, налаштувавши VLAN на VTP-сервері, на клієнтах цього робити не доведеться.

За промовчанням DTP знаходиться в режимі активовано. Таким чином, підключаючись до порту доступу, хакер оволодіває транком. Він здатний здійснювати:

* читання широкомовного та багатоадресного трафіку всіх віртуальних локальних мереж (у тому числі протоколів маршрутизації OSPF та EIGRP)
* участь у VTP, зміна налаштувань VLAN
* спуфінг ARP

Для захисту необхідно не забувати змінювати стандартні налаштування, блокувати режим магістралі на портах доступу.

# 1.3. Загальні підходи щодо вирішення проблеми побудови захищенної корпоративної мережі

Мережі є однією з головних цілей атак, оскільки їх дизайн рідко враховує ризики безпеці. Це зазвичай призводить до:

* Відсутність систем і процедур управління доступом;
* Відсутність механізмів шифрування;
* Погане або недостатнє управління та налаштування мережевого обладнання;
* Відсутність політики управління виправленнями та оновленнями;
* Відсутність або погана сегментація мережі;
* Відсутність оцінки безпеки мережі та системи.

Проектування архітектури мережі є складним процесом. Однак правильний дизайн не повинен базуватися лише на функціональних вимогах. Він також повинен враховувати міркування безпеки, щоб уникнути критичних вразливостей, які можуть поставити під загрозу всю інформаційну систему. Тому необхідно включити вимоги безпеки на етапі проектування мережі, що має забезпечити наступні цілі:

* Конфіденційність, щоб гарантувати, що авторизовані користувачі або системи мають доступ тільки до ресурсів і даних, на які вони мають право.
* Цілісність, щоб гарантувати, що ресурси, дані та інформація не будуть змінені, викрадені або знищені неавторизованими користувачами або ресурсами.
* Доступність, щоб забезпечити безперебійну роботу та безперебійний доступ до послуг і ресурсів.
* Відстеження, щоб гарантувати, що всі модифікації та зміни в системі відстежуються та контролюються.

Таким чином, забезпечення безпеки внутрішньої мережі є життєво важливим і обов’язково передбачає впровадження найкращих практик щодо конфігурації, інтеграції, моніторингу та тестування безпеки.

**Деякі підходи для вирішення проблем з безпекою мережі**

Сегментація мережі – це поділ мережі на фізичний і логічний домени, кожен з яких захищений певним периметром безпеки. На практиці це передбачає поділ мережі на менші сегменти мережі, ізольовані один від одного у віртуальних локальних мережах (VLAN) або фізичних мережах (LAN).

З одного боку, це дозволяє групувати робочі станції, пристрої, додатки, сервери та інші системи з різними рівнями критичності в окремі зони для оптимізації рівнів управління та безпеки. З іншого боку, сегментація дозволяє обмежити авторизовані з’єднання, відокремлюючи, наприклад, внутрішню мережу, для якої не авторизоване з’єднання з Інтернету, від мережі, доступної з Інтернету. Це зазвичай називають демілітаризованою зоною або DMZ. Крім того, реалізація такої DMZ вимагає встановлення брандмауерів між розділеними мережами, щоб контролювати вхідні та вихідні потоки інформації.

VLAN дозволяють створювати віртуальні мережі, підключені до фізичного пристрою (комутатора), розділяючи трафік між різними визначеними логічними мережами. Це гарантує, що машини в одній VLAN не можуть спілкуватися з машинами, що належать до іншої VLAN, якщо не потрібне взаємоз’єднання. Таким чином, VLAN не тільки забезпечують кращий контроль, але й спрощують керування та адміністрування мережі.

Однак VLAN не забезпечують жодного механізму безпеки як такого. Дійсно, сегментація мережі на VLAN не перешкоджає атакам, але залишається важливою мірою безпеки, оскільки це один із основних способів зменшити вплив успішної атаки.

**Розбиття мережі Wi-Fi**

Мережі Wi-Fi також можна використовувати як вектори атак. Тому необхідно розрізняти з’єднання Wi-Fi персональних пристроїв або гостьових від з’єднань систем організації та фільтрувати потоки робочих станцій, які підключаються до мережі Wi-Fi. Для цього можна налаштувати кілька розділених мереж Wi-Fi, щоб обмежити доступ до певних критично важливих ресурсів, гарантуючи, що лише необхідні елементи доступні для різних попередньо визначених груп користувачів.

**Захист адміністрування та управління мережевими пристроями**

Адміністрування та керування активними мережевими пристроями є критично важливим аспектом, який потрібно обробляти відповідним чином із достатніми заходами безпеки, щоб запобігти несанкціонованому вторгненню. Щоб повернутися до теми сегментації мережі, рекомендовано створити область, присвячену адмініструванню мережевих пристроїв. Цей сегмент дає змогу керувати та перевіряти належне функціонування всіх компонентів у певному периметрі безпеки.

Крім того, трафік керування також має бути відокремлений від решти комунікацій, щоб виключити можливість його перехоплення під час проходження. За необхідності трафік керування має проходити через захищений протокол.

Таким чином, оскільки адміністрування та керування мережевими пристроями за своєю природою є особливо чутливим, воно має бути належним чином захищене за допомогою відповідної фільтрації, обмежень і протоколів. Тому для цього необхідно:

Майте перелік мережевої інфраструктури з розташуванням, роллю, правами та версією кожного компонента системи.

Переконайтеся, що програмне забезпечення та операційні системи (ОС) компонентів мережевої інфраструктури постійно оновлюються.

Посилити безпеку обладнання:

* Змінити облікові записи адміністратора за замовчуванням і паролі.
* Вимкнути всі служби та інтерфейси, які не використовуються.
* Обмеження фізичного доступу до обладнання лише уповноваженим особам.
* Обмеження доступу до інтерфейсів адміністрування обладнання лише авторизованим особам.
* Використання зашифрованих протоколи зв’язку (SSH, HTTPS, SMBv3, LDAPS тощо).

Отже, щоб зменшити ризик зламу вашої мережі, переконайтеся, що:

* Сегментуйте та розділяйте мережу відповідно до критичності інформації та систем у мережі (DMZ, внутрішні мережі, критичні мережі тощо).
* Враховуйте вимоги до сегментації при будь-якому новому розширенні мережі.
* Виділіть адміністративну область для мережі, яка логічно або фізично відокремлена від інших мереж.

# 2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ В МЕРЕЖІ

## 2.1. Методи ідентифікації та автентифікації користувачів корпоративної інформаційної системи

Методи ідентифікації та автентифікації можна розділити на п’ять категорій: біометрія пристрою, голосова біометрія, апаратні ключі безпеки, поведінкова біометрія і технології ідентифікації пристрою.

Біометрія пристрою є найпопулярнішим типом технології автентифікації, але вона не ідеальна та має недоліки безпеки. Голосова біометрія демонструє цікавий потенціал, а поведінкова біометрія стає точнішою. Апаратні ключі безпеки стають все більш поширеними, а поведінкова біометрія може використовуватися для виявлення підозрілої поведінки. Вхід на основі пароля, багатофакторна автентифікація, біометрична автентифікація (включаючи обличчя) і автентифікація на основі сертифіката також є популярними технологіями автентифікації. Технологія автентифікації забезпечує контроль доступу для систем, перевіряючи, чи збігаються облікові дані користувача з обліковими даними в базі даних авторизованих користувачів або на сервері автентифікації даних.

Автентифікація важлива в кібербезпеці, оскільки вона дозволяє лише авторизованим користувачам або процесам отримувати доступ до ІТ-ресурсів компанії. Автентифікація використовується для різних цілей, але найпоширенішою реалізацією є однофакторна автентифікація (SFA), яка вимагає ідентифікатора користувача та пароля. Однак зараз компанії частіше використовують двофакторну автентифікацію (2FA) і багатофакторну автентифікацію (MFA), для яких потрібен ідентифікатор користувача, пароль і один або кілька додаткових факторів автентифікації. MFA використовується для спрощення автентифікації користувачів для веб-додатків.

**S/Key**

S/Key (Secure/Key) — система одноразових паролів. Система використовує серію попередньо згенерованих паролів і часто використовується як додатковий рівень безпеки для онлайн-акаунтів і веб-сайтів. S/Key працює, генеруючи унікальний одноразовий пароль для кожної спроби доступу. Цей пароль генерується на основі хеш-алгоритму та секретної парольної фрази, яка використовується спільно між користувачем і сервером. Коли користувач намагається отримати доступ до облікового запису, він повинен ввести поточний пароль S/Key, який перевірено сервером. Після перевірки пароля сервер генерує новий пароль S/Key для наступної спроби доступу. S/Key розроблено для забезпечення безпеки, оскільки паролі дійсні лише для одноразового використання, що значно ускладнює зловмисникам їх перехоплення та використання. Крім того, секретна парольна фраза користувача ніколи не надсилається на сервер, що унеможливлює зловмисникам створити паролі S/Key. S/Key — це ефективний спосіб для організацій захистити свої онлайн-акаунти та веб-сайти від несанкціонованого доступу.

**Автентифікація за допомогою апаратних засобів. Token Password Authentication**

Автентифікація за допомогою апаратних засобів працює за однією з двох альтернативних схем: запит-відповідь чи синхронізація за часом.

У першому випадку користувач підключається до сервера автентифікації, який пропонує ввести персональний автентифікаційний номер (PIN). Потім сервер передає випадкове число, яке користувач вводить у спеціальний апаратний пристрій, де воно шифрується за допомогою ключа користувача. Далі результат відправляється на сервер автентифікації. Отримавши відповідь від користувача, сервер порівнює його з власним, отриманим за допомогою користувача ключа, що зберігається в базі даних. Якщо обидва результати збігаються, можна отримати доступ до мережі.

При використанні схеми з синхронізацією за часом на апаратному пристрої користувача та сервері працює секретний алгоритм, який через певні синхронізовані проміжки часу генерує ідентичні паролі та замінює старі паролі на нові. Користувач підключається до сервера автентифікації, який запитує доступ. Після цього користувач вводить свій PIN в апаратний пристрій, і в результаті на екран виводиться деяка величина, яка є одноразовим паролем. Цей пароль і надсилається на сервер.

**Автентифікація PPP**

Автентифікація за протоколом «Point-to-Point Protocol» (PPP) — це протокол, який використовується для автентифікації двох комп’ютерів у мережі. Він використовується для перевірки ідентичності комп'ютерів, а також для встановлення з'єднання між ними. PPP-автентифікація використовує двоетапний процес, коли обидві машини надсилають запит, а потім перевіряють відповідь. Відповідь базується на спільному секреті, наприклад паролі, який відомий лише двом машинам. Автентифікація PPP є безпечним методом автентифікації, оскільки паролі зашифровані та ніколи не передаються через мережу. Він використовується для автентифікації підключень як до Інтернету, так і до приватних мереж. Крім того, його легко встановити та налаштувати, що робить його популярним вибором для цілей автентифікації.

До його складу PPP входять три основні компоненти:

* метод інкапсуляції датаграм у послідовних каналах
* протокол Link Control Protocol (LCP), який використовується для встановлення, конфігурування та тестування зв'язку
* сімейство протоколів Network Control Protocols (NCP) для встановлення та конфігурування різних протоколів мережного рівня.

Протокол автентифікації пароля (PAP) — це метод автентифікації, який використовується в протоколі Point-to-Point (PPP). PAP — це простий протокол двосторонньої автентифікації, який використовується для перевірки ідентичності користувача або пристрою в мережі. Він працює шляхом надсилання імені користувача та пароля на сервер, який потім перевіряє правильність облікових даних. Якщо облікові дані правильні, користувачеві надається доступ до мережі. Паролі передаються по каналу який вже псевдо захищений, але цей метод не дає захисту від переборів паролю та використання чужих паролів

CHAP (Challenge Handshake Authentication Protocol) використовується для періодичної автентифікації центрального комп'ютера або кінцевого користувача за допомогою узгодження трьох параметрів. Автентифікація відбувається у момент встановлення зв'язку, але може повторюватися і після.

**TACACS+**

Terminal Access Controller Access Control System Plus (TACACS+) — це протокол, який використовується для автентифікації, авторизації та обліку користувачів у мережі. Це відкритий протокол автентифікації, який базується на протоколі TACACS і використовує централізований сервер автентифікації для перевірки користувачів. TACACS+ є більш безпечним, ніж інші протоколи автентифікації, оскільки він шифрує кожен пакет даних, який передається між користувачем і сервером. Крім того, він здатний забезпечувати детальний контроль над доступом користувачів, дозволяючи адміністраторам обмежувати або надавати доступ на основі особи користувача або групи. TACACS+ використовується в різноманітних мережах і є популярним вибором для цілей автентифікації.

**RADIUS**

Протокол RADIUS (Remote Authentication Dial In User Service) — це мережевий протокол, який використовується для керування доступом до мережі. Він працює, дозволяючи користувачеві автентифікуватися на сервері RADIUS, який потім перевіряє, чи дозволено користувачеві доступ до мережі. RADIUS є безпечним протоколом, оскільки він шифрує дані між користувачем і сервером і надає додаткові методи автентифікації, наприклад двофакторну автентифікацію. Його також легко налаштувати та використовувати, що робить його популярним вибором для автентифікації та контролю доступу.

Облікові функції RADIUS дозволяють на початку та в кінці кожної сесії надсилати дані про кількість використаних ресурсів.

Транзакції між клієнтом та сервером RADIUS автентифікуються за допомогою загального «секрету», який ніколи не передається мережевими каналами. Крім того, обмін будь-якими користувачами йде тільки в зашифрованому вигляді, що виключає підслуховування чужих паролів.

## 2.2. Засоби цілісності та конфіденційності

Засоби цілісності та конфіденційності — це інструменти, які використовуються для забезпечення безпеки та конфіденційності цифрових даних. Він включає широкий спектр тем, таких як криптографія, шифрування, автентифікація, цілісність даних, авторизація та контроль доступу. Технологія цілісності та конфіденційності може допомогти захистити організації від зловмисників, забезпечити безпеку даних і запобігти витоку даних. Це невід’ємна частина будь-якої сучасної цифрової інфраструктури, і вона стає все більш важливою, оскільки цифрові технології та дані стають все більш поширеними.

**SSL**

SSL (Secure Socket Layer) SSL (Secure Socket Layer) — це протокол безпеки, який використовується для захисту зв’язку між веб-сервером і браузером. Це криптографічний протокол, який створює зашифрований зв’язок між двома пристроями, гарантуючи безпеку будь-яких даних, що передаються між ними. SSL також допомагає переконатися, що автентичність веб-сервера встановлена, і що дані не змінюються під час передачі. SSL сьогодні використовується на більшості веб-сайтів і стає все більш важливим, оскільки кібератаки стають все більш складними.

SSL працює шляхом встановлення зашифрованого з’єднання між веб-сервером і браузером. З’єднання встановлюється, коли браузер надсилає серверу повідомлення з проханням ідентифікувати себе. Потім сервер надсилає цифровий сертифікат, що містить його відкритий ключ. Потім браузер використовує цей ключ для шифрування даних, які він надсилає на сервер, а сервер використовує свій закритий ключ для розшифровки даних. Цей процес повторюється для кожної частини надісланих або отриманих даних, гарантуючи, що весь зв’язок є безпечним і конфіденційним.

Протокол SSL підтримує безпеку зв'язку, надаючи їй такі властивості:

* захищеність – після початкового квітування зв'язку застосовуються засоби шифрування, та визначається секретний ключ. Для шифрування даних використовуються засоби симетричної криптографії (наприклад, DES, RC4 тощо).
* учасник сеансу зв'язку може бути автентифікований за допомогою спільних ключі які є засобами асиметричної криптографії (наприклад, RSA, DSS тощо).
* Надійність – транспортні засоби перевіряють цілісність повідомлень за допомогою зашифрованого коду, для обчислення якого використовуються безпечні хеш-функції (SHA, MD5 тощо).

**SSH**

Протокол Secure Shell (SSH) — це безпечний спосіб підключення до віддалених комп’ютерів через незахищену мережу. Він широко використовується для безпечного доступу до серверів, а також для передачі файлів між хостами. Він використовує криптографію з відкритим ключем для автентифікації з’єднань, а потім шифрує дані за допомогою безпечних алгоритмів шифрування. Після встановлення з’єднання користувачі можуть виконувати команди на віддаленій машині, а також передавати файли

SSH широко використовується в системному адмініструванні та вважається одним із найбезпечніших методів віддаленого доступу. SSH зазвичай використовує різноманітні алгоритми шифрування для захисту передачі даних. До них належать симетричні алгоритми, такі як AES, Blowfish і 3DES, а також методи автентифікації з відкритим ключем, такі як DSA, RSA та ECDSA. SSH також використовує код автентифікації повідомлення (MAC) для забезпечення цілісності даних. Алгоритм, який використовується, залежить від версії SSH, яку використовує сервер і клієнт, що підключається до нього. Наприклад, найновіша версія SSH (версія 2) за замовчуванням використовує шифр AES, тоді як версія 1 може використовувати різні шифри.

**S-HTTP**

S-HTTP (Secure HTTP) — це протокол для безпечного зв’язку через Інтернет. Він схожий на HTTPS, але використовує інші алгоритми шифрування та інші протоколи. S-HTTP забезпечує безпечне з'єднання для обміну даними, а також підтримує цифрові підписи та шифрування повідомлень. Він не так широко використовується, як HTTPS, оскільки підтримується не всіма браузерами та не такий безпечний, як HTTPS. Однак його можна використовувати за певних обставин, коли HTTPS недоступний.

Протокол S-HTTP забезпечує безпечні наскрізні (end-to-end) транзакції, що вигідно відрізняє його від базових механізмів автентифікації HTTP, які вимагають, щоб клієнт спробував отримати доступ та отримав відмову, і лише потім включають механізм безпеки.

У S-HTTP використовується механізм узгодження опцій, криптографічних алгоритмів – RSA або Digital Signature Standard [DSA] для підпису, DES чи RC2 для шифрування тощо.

**SOCKS**

SOCKS v4 — це інтернет-протокол, який використовується для ретрансляції мережевого трафіку. Зазвичай він використовується як проксі-сервер для обходу брандмауерів і доступу до обмежених мереж. Це дозволяє користувачам встановлювати з’єднання через проміжний сервер, дозволяючи їм обходити обмеження, накладені їхньою локальною мережею. SOCKS v4 також забезпечує автентифікацію та шифрування даних, що робить його безпечним протоколом. Він часто використовується компаніями, щоб забезпечити безпечний доступ до своїх внутрішніх мереж, а також окремими особами, щоб обійти онлайн-цензуру або отримати доступ до геозаблокованого вмісту.

Функціонування SOCKS полягає в заміні стандартних мережевих системних дзвінків у додатку їх спеціальними версіями, які встановлюють зв'язок із проксі-сервером SOCKS (він конфігурується самим користувачем у додатку або системним файлом конфігурації), підключаючись до добре відомого порту (зазвичай це порт 1080/TCP). Після встановлення зв'язку із сервером SOCKS програма відправляє серверу ім'я машини та номер порту, до якого хоче підключитися користувач. Сервер SOCKS реально встановлює зв'язок із віддаленим центральним комп'ютером, а потім прозоро передає дані між програмою та віддаленою машиною. Користувач навіть не підозрює, що в каналі зв'язку присутній сервер SOCKS.

**IPSec**

Цей протокол використовується для захисту даних та автентифікації на рівні IP. Поточні стандарти IPSec включають незалежні від алгоритмів базові специфікації, RFC 2401-2412.

IPSec побудований на застосуванні двох протоколів для здійснення взаємодії: ESP (Encrypting Security Payload), що відповідає за шифрування, та IKE (Internet Key Exchange), що використовується для узгодження методів та ключів.

Існує два режими роботи IPSec:

* транспортний
* тунельний

У транспортному режимі відбувається шифрування лише поля даних IP-пакету, а заголовок залишається недоторканим. Якщо хакер прослуховуватиме сеанс, він отримає лише адреси сторін, а інформація залишиться закритою.

У тунельному режимі відбувається повне шифрування пакета та додавання нового заголовка. Таку схему взаємодії зручно використовуватиме організації зв'язку двох відділень організації із застосуванням технології VPN. Перехоплені (наприклад, на магістралі провайдера) повідомлення не дають змоги розкрити зловмиснику навіть внутрішню структуру приватної мережі.

## 2.3. Методи віддаленого доступу до корпоративної інформаційної системи

Методи віддаленого доступу до корпоративної інформаційної системи надають можливість поширювати єдину мережу в кількох місцях була надзвичайно важливою як для окремих осіб, так і для організацій. Незважаючи на те, що виділені канали «точка-точка» є високозахищеними, вони надзвичайно дорогі та можуть призвести до збою, якщо пошкодження єдиної лінії, яка може надавати цю послугу.

Віртуальні приватні мережі (VPN) усувають багато з цих обмежень, дозволяючи користувачам підключаєтися з віддаленого місця до центральної мережі організації. Далі буде розглянуто VPN і технологій віддаленого доступу в цілому, а також деякі переваги та проблеми, пов’язані з використанням VPN.

Безумовно, найпопулярнішим рішенням є програмний клієнт, який підключається через захищений тунель до організації через існуюче з’єднання, де б користувач зараз не перебував.

Це дозволяє користувачеві мати можливість перемикатися між тим, коли йому потрібен доступ до ресурсів організації, і коли йому потрібен лише загальний веб-доступ до локального підключення. З іншого боку, є також варіанти апаратного забезпечення, такі як повітряні карти або вбудовані з’єднання на певних типах вбудованих пристроїв, які можуть створити безпечне з’єднання до того, як операційна система завершить завантаження. Таким чином, користувач ніколи не виходить з мережі; вони кожного разу входять безпосередньо.

**Site-to-site VPN**

Site-to-site VPN забезпечують безпечне з’єднання між двома чи більше мережами в різних фізичних місцях. Вони використовуються для об’єднання локальних мереж кількох офісів в одну приватну мережу або для того, щоб дозволити компанії використовувати загальнодоступний Інтернет для з’єднання своєї локальної мережі з мережами інших компаній, клієнтів або спільнот. Мережі VPN типу «сайт-сайт» зазвичай налаштовуються за допомогою з’єднання «маршрутизатор-маршрутизатор» і не вимагають від користувачів додаткового програмного чи апаратного забезпечення. Вони забезпечують безпечне з’єднання та часто використовуються в бізнес-цілях, наприклад для з’єднання двох офісів.

**Secure socket layer virtual private network (SSL VPN)**

Цей тип з’єднання стане у пригоді коли організації потрібно поділитися даними з користувачами, але не обов’язково користувачу надати доступ до всієї мережі

Потенційно можна використовувати такі методи, як електронна пошта, але для цього потрібно, щоб хтось насамперед надсилав дані користувачеві. Можна спробувати розмістити ці дані на сайті, доступному у відкритому Інтернеті, але якщо вони конфіденційні, організація ризикуєте втратити доступ до сайту або дані. SSL VPN дозволяє користувачам отримувати доступ до внутрішніх програм через захищений портал, надаючи їм доступ для самообслуговування до всього, що організація вирішить дозволити, але без карт-бланш доступу, який дозволив би повний тунель VPN.

**Протоколи VPN**

Щоб захистити базовий трафік, протоколи VPN розвивалися протягом багатьох років, щоб створювати зашифровані тунелі, при цьому дані, що передаються, доступні лише з обох кінців з’єднання. Безпека Інтернет-протоколу (IPsec) може керувати автентифікацією та шифруванням кількома способами, забезпечуючи величезну кількість універсальності. Протокол тунелювання «точка-точка» (PPTP) і протокол тунелювання рівня 2 (L2TP), що його замінив, можуть підтримувати передачу даних у мережах VPN, але не забезпечують жодного суттєвого захисту цих даних. З цією метою їх можна інкапсулювати IPsec, забезпечуючи шифрування трафіку, що проходить через нього.

Захищена оболонка (SSH) спочатку була призначена для забезпечення безпечного методу доступу до термінального сеансу на віддаленому пристрої. Його можна використовувати для тунелювання майже для всього через безпечне з’єднання, яке він створює. Тож, наприклад, якщо раніше використовували базове підключення до віртуальної мережі (VNC) для отримання доступу до віддаленого графічного інтерфейсу користувача, дуже незахищеного, можна маршутизувати з’єднання через сеанс SSH, щоб виконати ту саму дію набагато безпечніше.

# 2.4. Архітектура мережі на базі Мikrotik та її функціональні можливості

MikroTik RouterOS - це операційна система, яка може бути встановлена на роутери MikroTik, що дозволяє налаштувувати та управляти різними функціями мережі.

Основна функціональність RouterOS базується на наступних компонентах:

Firewall: RouterOS може фільтрувати трафік, що проходить через мережу, використовуючи firewall правила. Це дозволяє блокувати небезпечний трафік та захищати мережу від атак.

* VPN: RouterOS підтримує різні протоколи VPN, такі як PPTP, L2TP/IPsec, OpenVPN, що дозволяє настроювати безпечне з'єднання між різними мережами або віддаленими користувачами.
* Routing: RouterOS може настроювати різні протоколи маршрутизації, такі як OSPF, RIP, BGP, що дозволяє забезпечити ефективну маршрутизацію мережі та високу доступність мережевих з'єднань.
* DHCP: RouterOS може використовуватись в якості DHCP сервера, що дозволяє автоматично настроювати IP-адреси для підключених до мережі пристроїв.
* Hotspot: RouterOS може працювати як Hotspot, що дозволяє забезпечити доступ до Інтернету для користувачів, що підключаються до мережі за допомогою Wi-Fi або LAN.
* QoS: RouterOS має різні інструменти для контролю та обмеження пропускної здатності мережі та підтримки різноманітних QoS-політик.
* Безпека: RouterOS підтримує різні методи шифрування трафіку, такі як WPA2, HTTPS, SSH, що дозволяє забезпечити безпеку мережі та захистити її від несанкціонованого доступу.

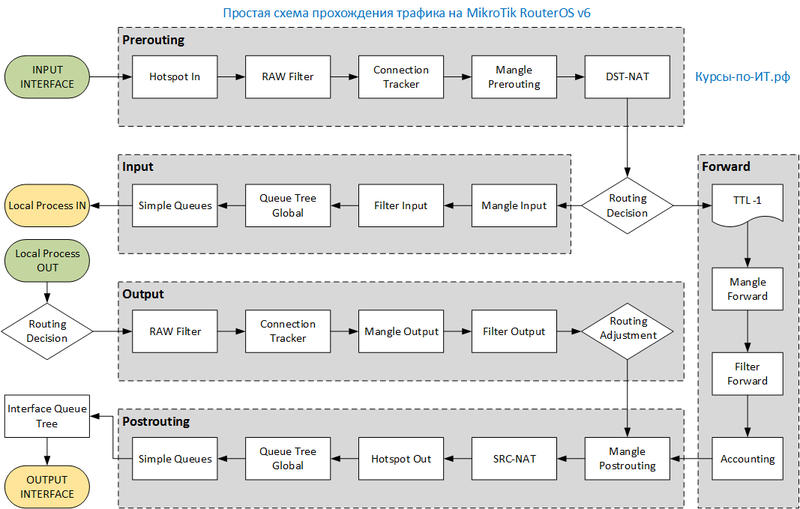


Рис.2.1. Схема проходження трафіку на обладнанні Mikrotik

# 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ MIKRTOTIK

## 3.1. Призначення та функції RouterOS

Брандмауер MikroTik RouterOS знаходиться між мережею компанії та загальнодоступною мережею, ефективно захищаючи комп'ютери організації від зловмисної активності та контролюючи потік даних на маршрутизатор через маршрутизатор і від маршрутизатора. Брандмауер MikroTik RouterOS підтримує функції фільтрації та безпеки, що формують інтернет-політику організації.

**Фільтрування з відстеження стану**

Брандмауер MikroTik RouterOS заснований на технології Stateful Filterig, яка може використовуватися для виявлення та блокування багатьох прихованих сканувань, DoS-атак, SYN-флудів. Мережева взаємодія складається з невеликих фрагментів даних, які називають пакетами, і деякі з цих пакетів використовуються виключно для створення, підтримки та завершення з'єднання. Брандмауер MikroTik RouterOS Stateful зберігає в пам'яті інформацію про кожне з'єднання, що проходить через нього. Коли чужий пакет намагається увійти до мережі, стверджуючи, що він є частиною існуючого з'єднання, брандмауер звертається до списку з'єднань. Коли він виявляє, що пакет не відповідає жодному, він може відкинути цей пакет і скасувати сканування.

**Системне адміністрування**

MikroTik RouterOS Firewall дуже простий у керуванні. Архітектура системи дозволяє легко налаштувати трансляцію мережевих адрес (NAT), прозорі проксі та перенаправлення. Правила фільтрації брандмауера згруповані у ланцюжки. Дуже вигідно, якщо пакети можуть бути зіставлені за одним загальним критерієм в одному ланцюжку, а потім передані для обробки за якимись іншими загальними критеріями в інший ланцюжок. Це робить систему набагато простіше в адмініструванні, використовуючи меншу кількість правил для створення більш якісного захисту.

**Брандмауер MikroTik RouterOS заснований на:**

* Фільтрування IP-адрес
* Фільтрування протоколу порту
* Фільтрування мережного інтерфейсу
* Фільтрування MAC-адрес джерела
* Варіант протоколу TCP

**Захист роутера від несанкціонованого доступу**

Можливість відстежувати підключення до адрес, призначених самому маршрутизатору, і дозволяти доступ лише з певних хостів до певних TCP-портів маршрутизатора. Брандмауер контролює всю інтернет-інформацію та попереджає та блокує спроби вторгнення на основі правил, налаштованих користувачем.

**Захист хостів користувача**

Можливість відстежувати підключення до адрес, призначених клієнтам мережі та дозволити доступ лише до певних хостів та служб. Надання клієнтам ефективного захисту від шкідливих атак.

**Використання маскарадингу для приховування приватної мережі за однією зовнішньою адресою**

Всі з'єднання з приватних адрес можуть бути замасковані, і вони виглядають як вихідні з однієї зовнішньої адреси - адреси маршрутизатора. Брандмауер буде діяти як шлюз для всієї мережі, дозволяючи мережі офісу використовувати єдине безпечне підключення до Інтернету.

**Застосування політики використання інтернету в мережі клієнта**

Брандмауер дозволяє контролювати з'єднання з мережі користувача та надає докладну статистику трафіку за всіма посиланнями.

**Приорітизація трафіку**

Можливість позначити пріоритетні пакети, щоб забезпечити найшвидше з'єднання з більш важливими пакетами. Це гарантує, що всі групи завжди отримають відповідні пропускну здатність, забезпечуючи керований потік мережного трафіку і запобігаючи нестачі пропускної здатності.

**Застосування черги до вихідних пакетів**

Ця функція дозволяє обмежити швидкість з'єднання певною групою пакетів. Ієрархія класів дозволяє побудувати гнучке і дуже логічне подання трафіку.

**Winbox**

Winbox — це невелика утиліта, яка дозволяє адмініструвати MikroTik RouterOS за допомогою швидкого та простого графічного інтерфейсу. Це рідний двійковий файл Win32, але його можна запускати в Linux і MacOS (OSX) за допомогою Wine.

Починаючи з Winbox версії 3.14, використовуються такі функції безпеки:

* Winbox.exe підписаний сертифікатом розширеної перевірки, виданим SIA Mikrotīkls (MikroTik).
* WinBox використовує ECSRP для обміну ключами та автентифікації (потрібна нова версія winbox).
* Обидві сторони перевіряють, що інша сторона знає пароль (неможлива атака посередині).
* Winbox у режимі RoMON вимагає, щоб агент мав останню версію, щоб мати можливість підключатися до маршрутизаторів останньої версії.
* Winbox використовує AES128-CBC-SHA як алгоритм шифрування (потрібна версія winbox 3.14 або вище).

## 3.2. Рекомендації щодо налаштування Mikrotik

Перед початком роботи з обладнанням від компанії Mikrotik потрібно перш за все оновити систему RouterOS та загрузчик цієї системи – RouterBOARD.

Це можна зробити в графічному інтерфейсі Winbox.

Оновлення RouterOS - у вкладці System зайти в Packeges та у вікні яке відобразилось натиснути на кнопку Check For Updates. Система перевірить можливість оновитись до останньої версії відштовхуючись від того який Channel обраний у налаштуваннях. Після встановлення оновлень потрібно перезавантажити пристрій.

Відмінності Channel:

Stable – це найбільш перевірена і найнадійніша версія прошивки. ЇЇ оновлюють з виправленнями помилок і патчами безпеки, але не обов’язково додавання нових функцій. Стабільну версію використовує переважна більшість користувачів.

Long term – версія прошивки, яка періодично оновлюється та має на меті надати користувачам стабільну версію, яка буде підтримуватись протягом більш тривалого періоду часу. Ця версія отримуватиме менше оновлень, але все ще може отримувати деякі виправлення помилок і патчі безпеки.

Testing – це версія прошивки, яку можна використовувати для перевірки експериментальних функцій перед випуском стабільної версії. Ця версія може містити помилки та може зазнавати зміни, але стане у пригоді тим хто хоче тестувати нові функції.

Development – це версія прошивки, яка використовується розробниками. Саме на ній тестуються нові функції перед випуском стабільної версії.

Upgrade - це версія прошивки, яка використовується для оновлення однієї версії до іншої. Вона може бути корисною для встановлення нових функцій або виправлення помилок.

Для оновлення RouterBOARD потрібно в вкладці System перейти у пункт RouterBOARD та натиснути на пункт Upgrade та перезавантажити пристрій.

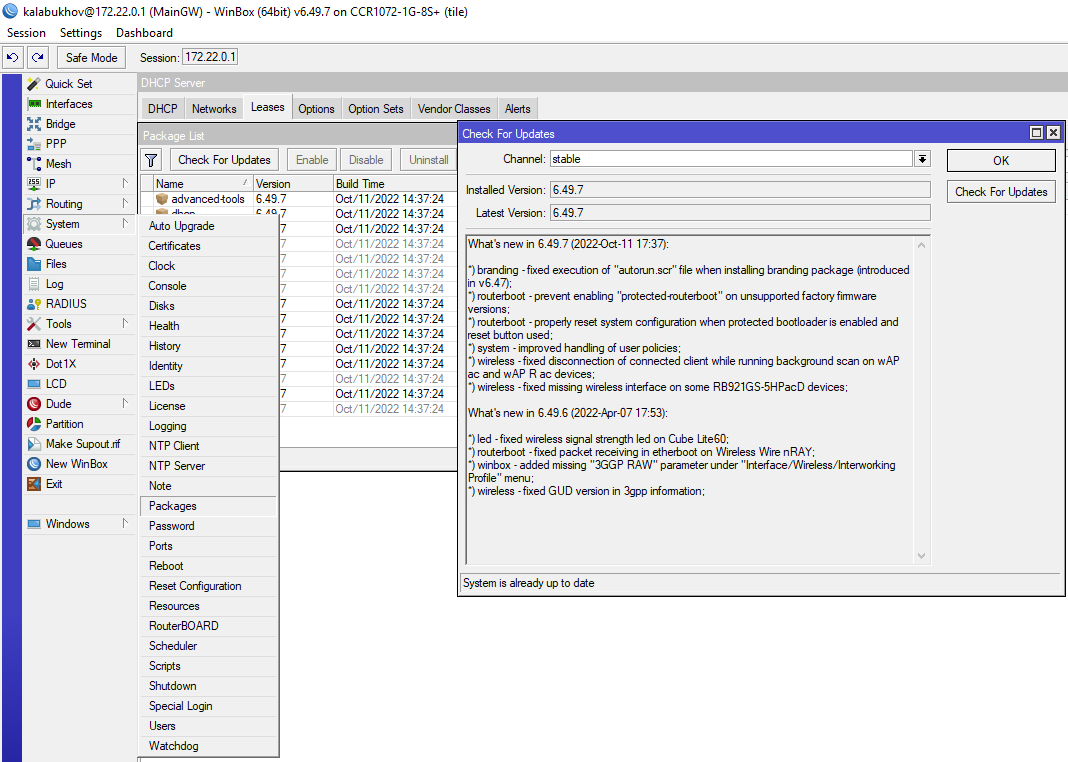
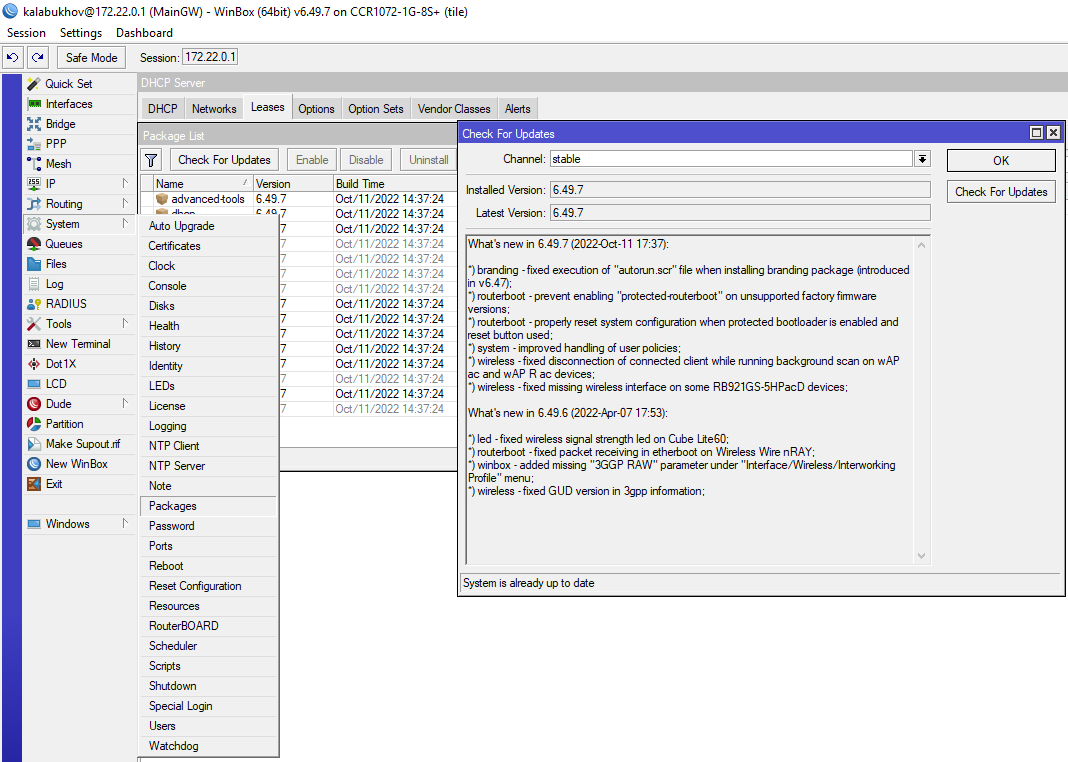


Рис.3.1. Оновлення прошивки RouterOS

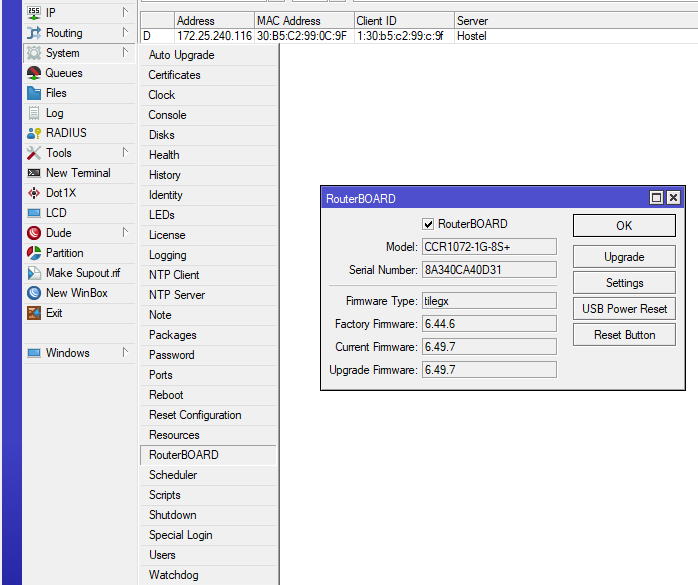


Рис.3.2. Оновлення загрузчика RouterBOARD

На не пропатчені версії програмного забезпечення існує багато експлойтів навіть у відкритому доступі на GitHub. Приклад роботи одного з таких експлойтів наведено нижче. Після застосування експлойту можна отримати логін та пароль адміністратора.

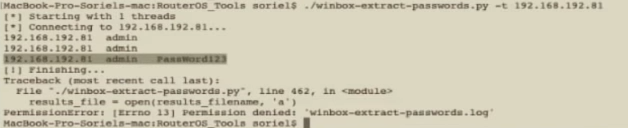


Рис.3.3. Приклад роботи експлойту на версії RouterOS 6.41

**Вимкнення пакетів які не використовуються**

Після оновлення прошивки пристрою потрібно вимкнути всі пакети які в подальшому не будуть використовуватись, щоб зменшити кількість вразливих місць у RouterOS. Для цього потрібно перейти до вкладки Packages, обрати непотрібні пакети та натиснути на кнопку Disable. Після того як вимкнули всі непотрібні пакети треба перезапустити пристрій.

Залишаємо ввімкненими пакети:

Advanced-tools — це пакет, що надає розширені мережеві можливості та можливості безпеки, такі як формування трафіку, керування користувачами та групами, налаштування DHCP-сервера та багато іншого.

DHCP - протокол динамічної конфігурації хоста, який використовується для налаштування мережних пристроїв, щоб вони могли обмінюватися даними в мережі.

NTP - Network Time Protocol, який використовується для синхронізації часу на кількох мережних пристроях.

PPP – це пакет, який використовується для створення приватного віртуального мережного з'єднання між двома або більше комп'ютерами.

Routing – це пакет, який використовується для визначення шляхів, якими проходять пакети даних при їх проходженні через мережу.

Security — це пакет, призначений для захисту від загроз та вразливостей у мережі, включаючи шифрування даних та виявлення вторгнень.

System – це пакет, який надає можливості системного адміністрування та обслуговування, такі як ведення журналу, моніторинг та діагностика системи.

User-manager –це пакет, що надає уніфікований інтерфейс керування користувачами та групами, що дозволяє адміністраторам створювати та керувати користувачами, групами користувачів та дозволами.

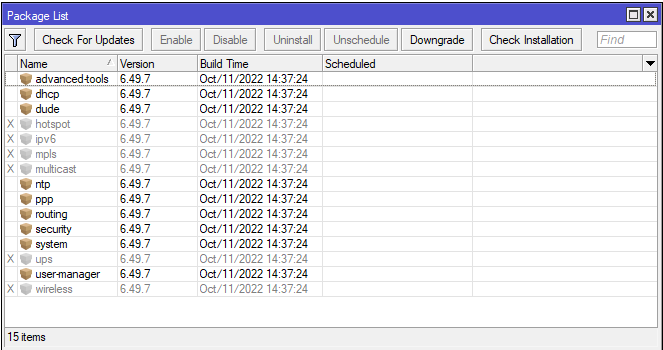


Рис.3.4. Вимкнення пакетів які не використовуються

**Налаштування сервісів у RouterOS**

Щоб ввімкнути або вимкнути сервіси потрібно знайти вкладку Services у IP. Відкриється список доступних сервісів. Потрібно вимкнути все, що зв’язане з не шифрованим з’єднанням та те, що не буде використовуватись, таке як:

API - означає інтерфейс прикладного програмування і представляє собою спосіб спілкування програм для взаємодії один з одним. Він зазвичай використовується для виконання запитів між різними веб-службами, наприклад, для запиту даних із бази або запиту контенту з веб-сторінки.

FTP - спосіб передачі файлів через Інтернет. Він зазвичай використовується для завантаження файлів на веб-сервер, таких як зображення, документи або веб-сторінки.

Telnet - це протокол прикладного рівня, який дозволяє користувачам керувати віддаленим пристроєм. Він зазвичай використовується для віддаленого доступу, наприклад для входу на веб-сервер і виконання команд з командного рядка.

WWW - велика колекція взаємопов'язаних гіпертекстових документів, розміщених в Інтернеті. Він зазвичай використовується для доступу до веб-сторінок та контенту з веб-сайтів.

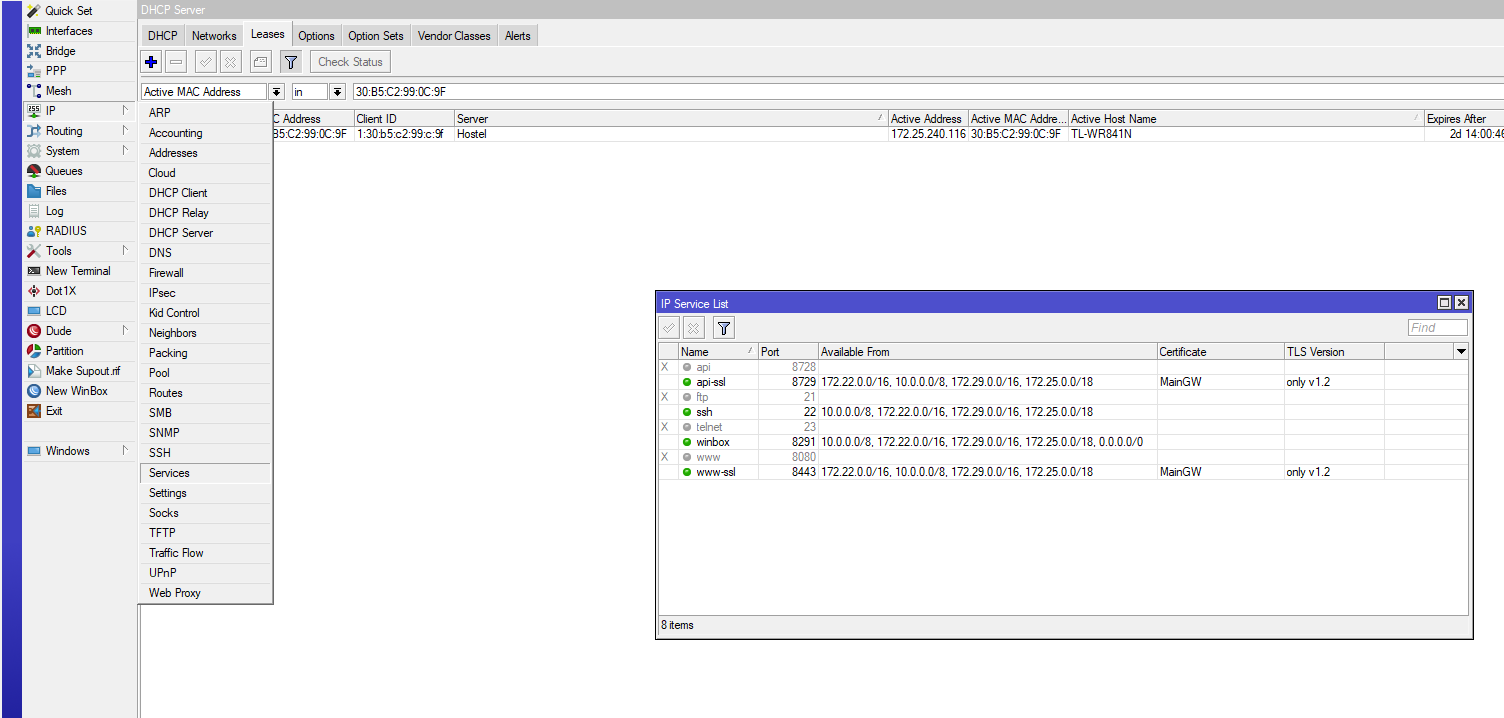
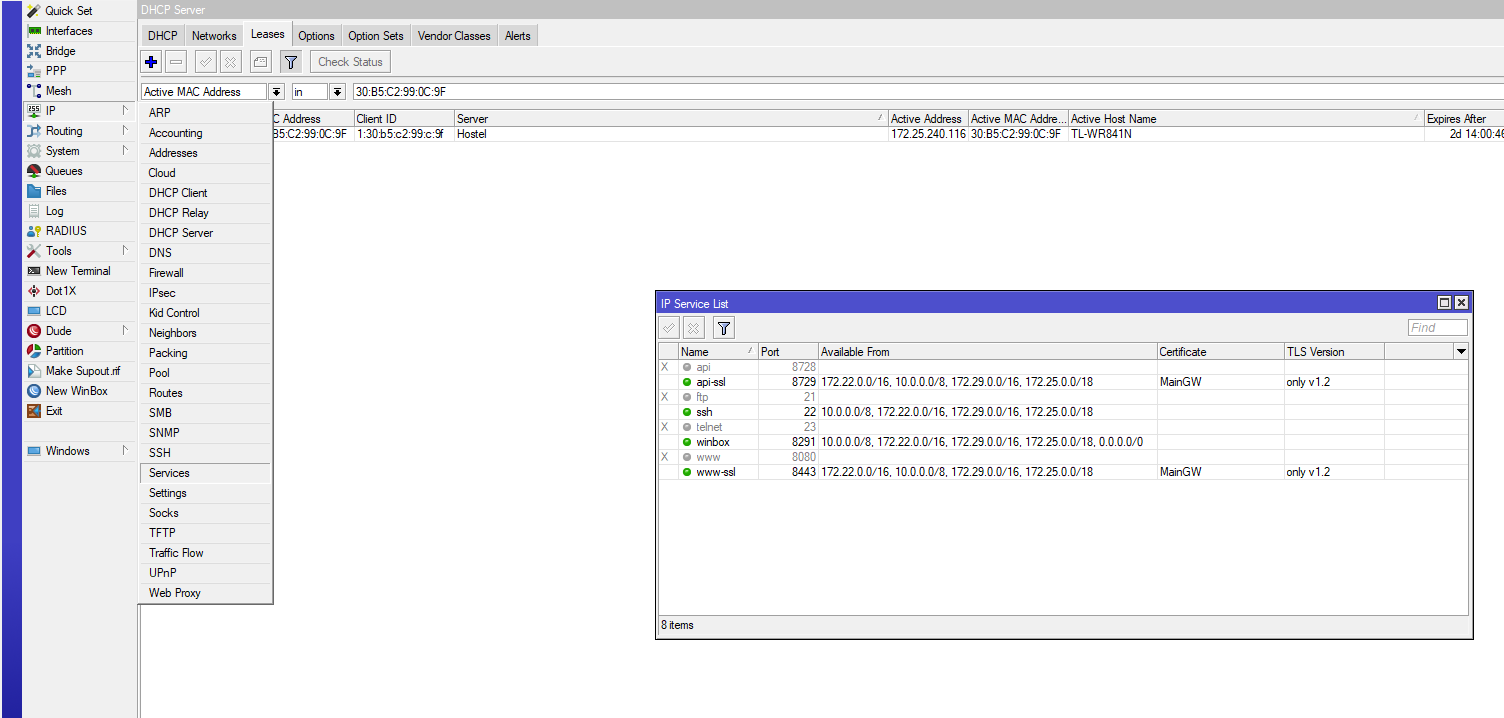


Рис.3.5. Вимкнення сервісів які не використовуються

**Mikrotik neighbors discovery protocol**

MNDP — це власний протокол, розроблений компанією Mikrotik, який використовується для виявлення та керування пристроями Mikrotik у одній локальній мережі. Він базується на протоколі багатоадресної IP-адреси та використовується для визначення наявності та конфігурації маршрутизаторів Mikrotik у мережі. MNDP можна використовувати для перегляду інформації про пристрій, такої як MAC-адреса, ім’я хоста, IP-адреса, ідентифікатор маршрутизатора, час безвідмовної роботи та версія програмного забезпечення. Цю інформацію можна використовувати для швидкого виявлення та діагностики проблем, а також для швидкого огляду топології мережі. MNDP також дозволяє дистанційно керувати пристроями Mikrotik, а також здатність швидко ідентифікувати та керувати змінами в мережі.

Правильно налаштований MNDP не дасть хакеру можливості дізнатись яка версія операційної системи встановлена на пристрої та які сервіси залишаються ввімкнутими. Тому точок входу стане менше.

Налаштування MNDP починається з того, що на інтерфейсі створюється Interface list наприклад MAC server.

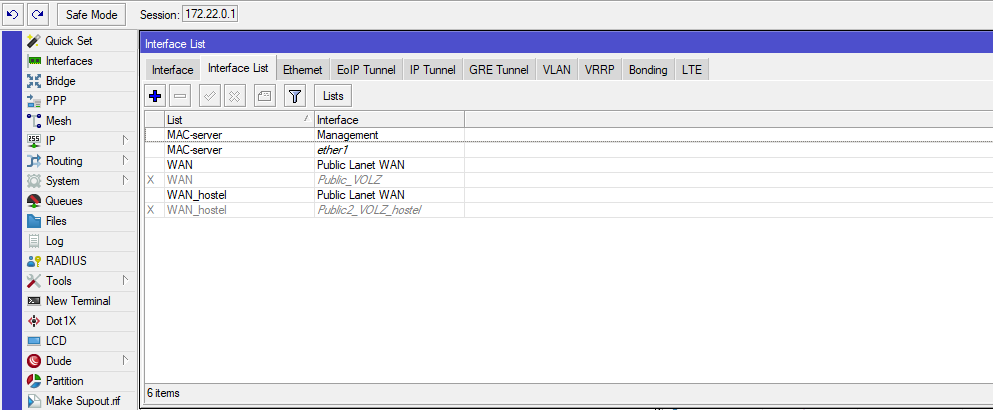


Рис.3.6. Вкладка налаштування інтерфейсів

Переходимо у вкладку Interface та натискаємо Interface list. Переходимо у вкладку Lists додаємо MAC server.

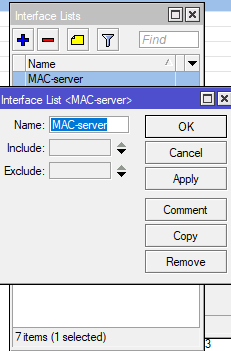


Рис.3.7. Створення нового List

У вкладці interface list створюємо новий інтерфейс де вказуємо list та інтерфейс на який цей list буде поширюватись.

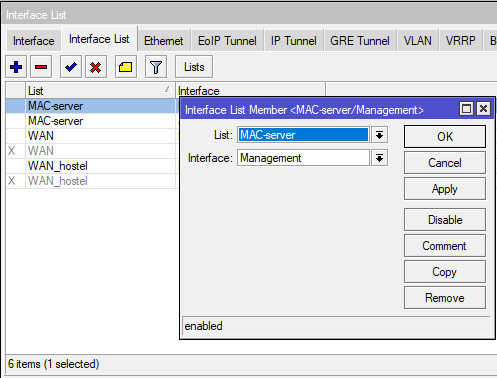


Рис.3.8. Створення нового Interface list

Відкриваємо neighbors у вкладці IP та натискаємо Discovery settings.

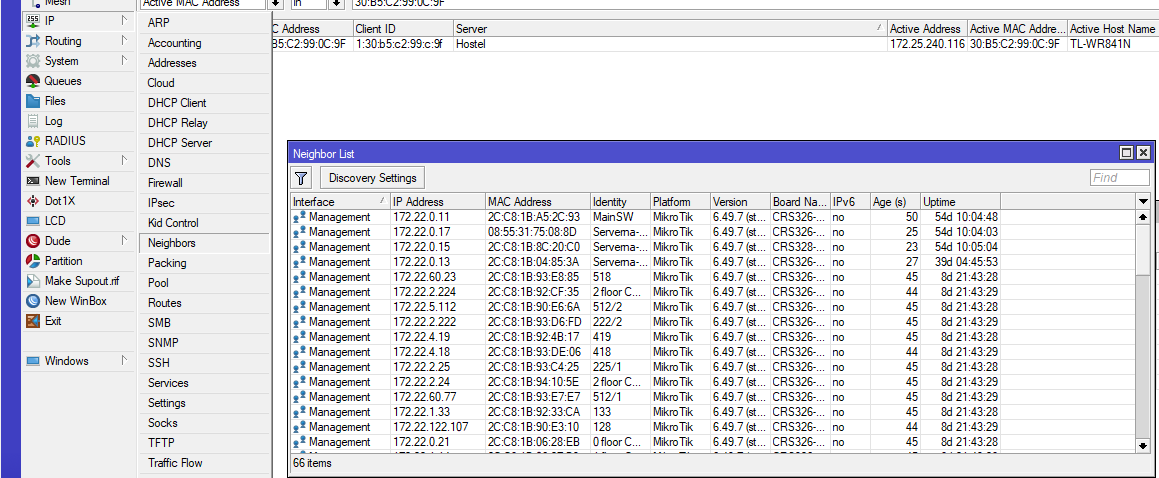


Рис.3.9. Вікно налаштувань MNDP

У Discovery settings обираємо створений раніше інтерфейс ліст MAC Server та обираємо протоколи MNDP і LLDP, які будуть поширюватись на цей інтерфейс.

Таким чином, прибирається небажаний флуд у мережу провайдера та корпоративну.



Рис.3.10. Створення правила для інтерфейс ліста MAC server

**Облікові записи**

Для зменшення ймовірності злому паролю адміністратора методом брутфорсу по словникам або просто грубого перебору потрібно вимкунти профіль стандартного адміністратора, який за замовчуванням налаштований без паролю та створюємо нові профілі з іменами відмінними від типових root та admin. До новостворених облікових записів створюємо криптостійкий пароль.

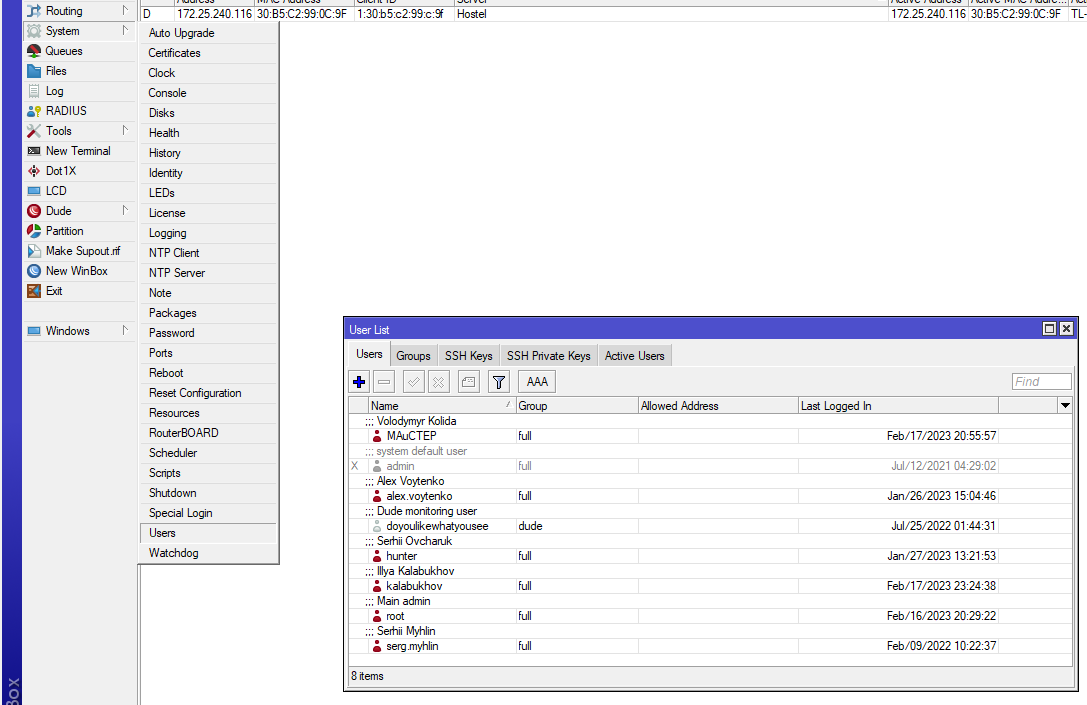


Рис.3.11. Створення нових користувачів

Можна піти далі та створити групи, які знаходяться у вкладці Group, для користувачів, де є можливість забрати деякі права або ж залишити тільки перегляд, як наприклад права в групі dude.

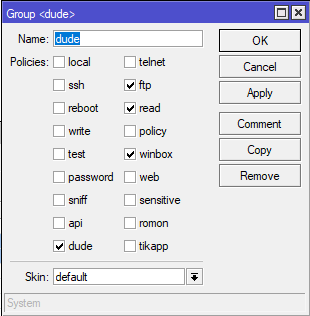


Рис.3.12. Приклад списку політик групи dude

## 3.3. Рекомендації налаштування firewall в RouterOS

Налаштування firewall знаходяться у вкладці IP – Firewall.

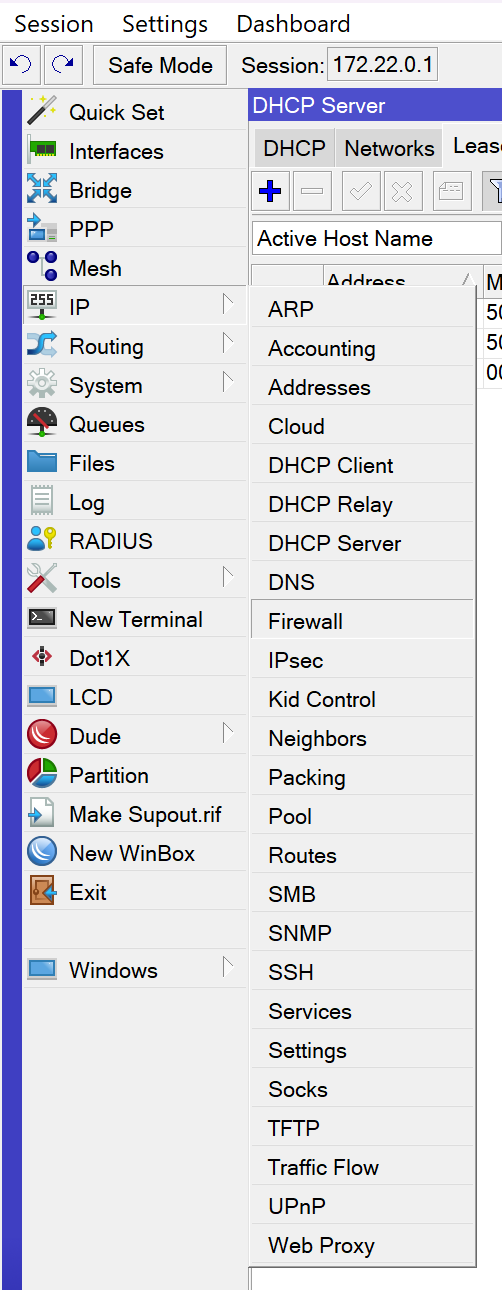


Рис.3.13. Вкладка firewall в winbox

Відкривши вкладку filter rules можна побачити стандартні налаштування брандмауеру Mikrotik.

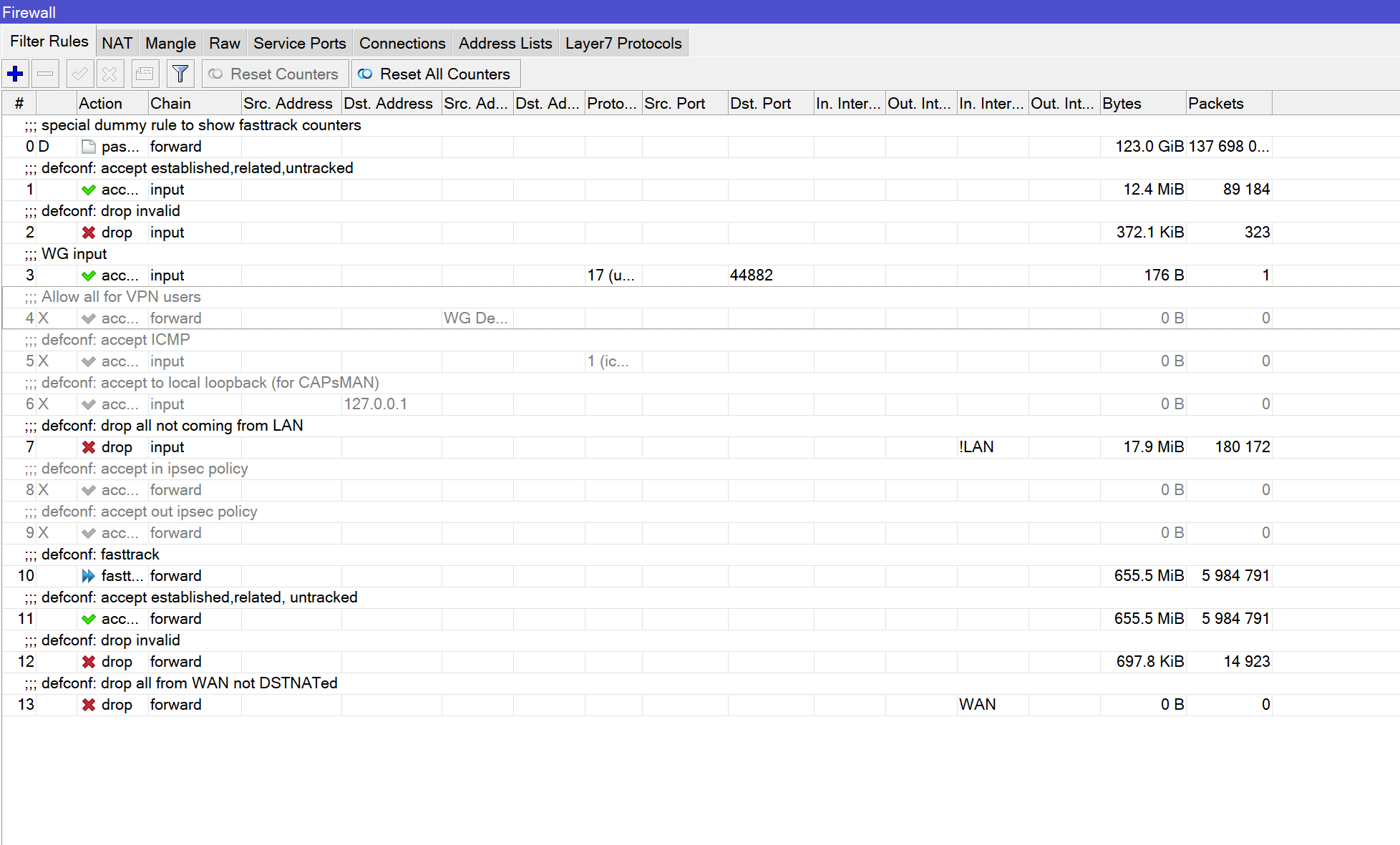


Рис.3.14. Стандартні налаштування filter rules

**Port knocking**

Перед початком роботи з firewall mikrotik створюємо правила для Port knocking для закриття доступу до роутера з WAN.

Port Knocking — це метод автентифікації, який передбачає надсилання послідовності пакетів на закритий порт перед відкриттям порту. Ідея Port Knocking полягає в тому, щоб не дозволити неавторизованим користувачам отримати доступ до портів.

Для налаштування Port knicking потрібно перейти в вкладку firewall в ip та натиснути filter rules. Далі потрібно створити нове правило для Chain – input, з вказанням протоколу ICMP, яке поширюється на інтерфейс list WAN. У вкладці action вказується дія jump, log prefix зазначається як ICMP\_on\_WAN, jump target створюємо KnockKnockKnock. Наступними створюються правила для обробки пакету ICMP певного розміру. Обробка буде тривати в три етапи.

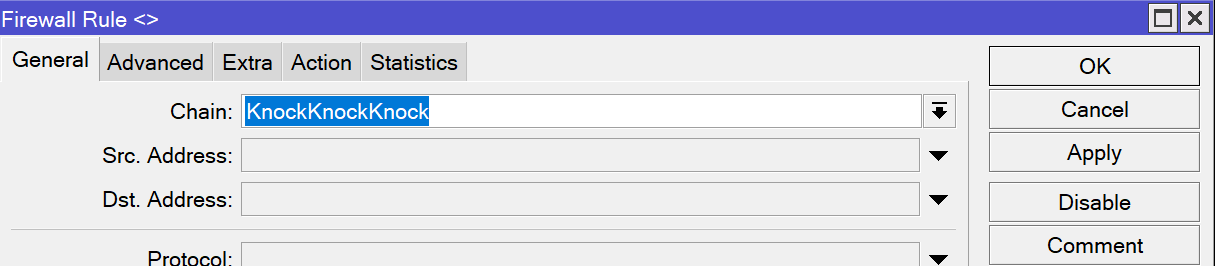
Перший етап: створюємо правило для chain – KnockKnockKnock. У вкладці advanced вказуємо package size 667, а в actions обираємо дію додавання IP адреси в address list з назвою Gate1 та подальшим логуванням з префіксом Knock1\_accepted та таймаутом в 20 мс.

Другий етап: створюється правило відмінне від минулого тим, що в advanced вказується src. Address list – Gate1 та розмір пакету 732. В action – add src to address list Gate2 з логуванням Knock2\_accepted та таймаутом в 20 мc

Третій етап: створюється правіло в якого у вкладці advanced вказуємо src. Address list Gate2, package size 293. В actions – add src to address list з назвою knocking-allowed та логування з префіксом knocking-allowed та таймаутом в 10 с.

Четвертий етап: додається правило в general якого вказано chain – KnockKnockKnock, у вкладці advanced src address list – knocking-allowed та в action ставиться дія – accept.

Останній етап: додається правило для не правильних запитів ICMP в general якого вказується Chain- KnockKnockKnock та в action – return.



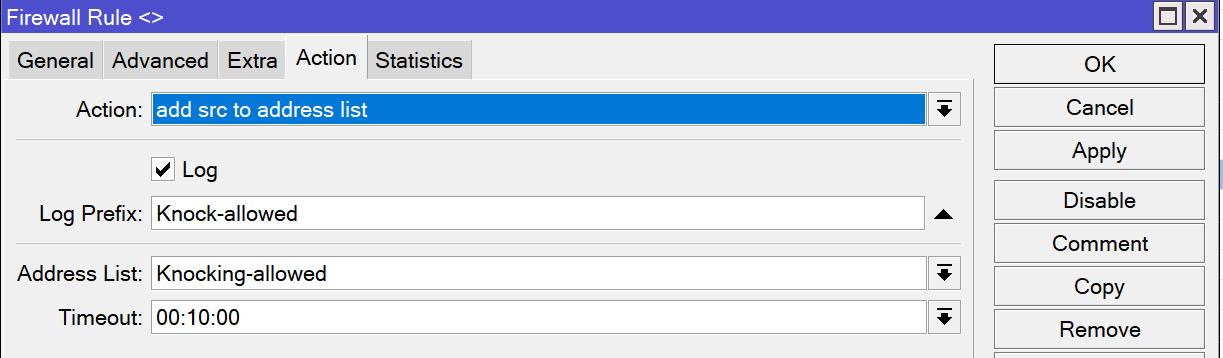


Рис.3.14. Приклад одного з етапів обробки запиту ICMP

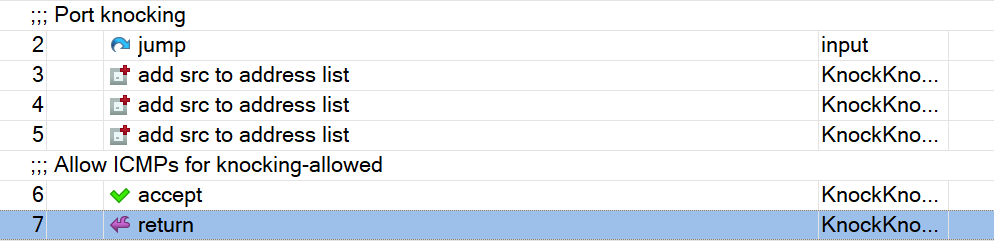


Рис.3.15. Приклад створених правила для Port Knocking

Після налаштування port knocking додаються три правила для віддаленого адміністрування та VPN сервісів користувачів які пройшли перевірку нокінгом.

У першому правилі chain – input, protocol – 6 (tcp), dst port - 1194, 1723, 8291, 8888, 22, 2000. У вкладці advanced обираємо src. Address list – Knocking-allowed та в action – accept та логування з префіксом control/VPN.

Наступне правило створюється для доступу L2TP VPN Connection. Chain – input, protocol – 17 (udp), dst port - 1701,500,4500. У вкладці advanced вказуємо src address list – Knicking-allowed та у action – accept з логуванням L2TP.

Останнє правило створюється для chaint – input та протоколу – 50 (ipsec-esp). В advanced вказуємо src address list – knocking-allowed. В action – accept та логування з префіксом ipsec.

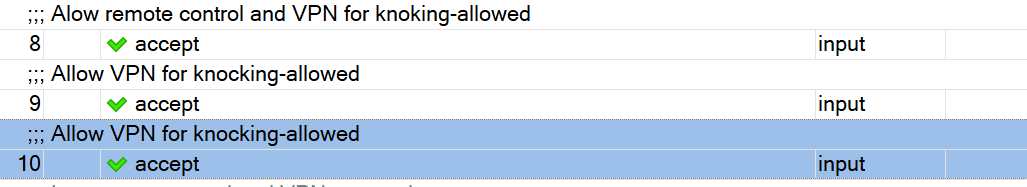


Рис.3.16. Приклад створених правил для віддаленого управління та VPN користувачів Knocking-allowed

Якщо запити ICMP були відправлені не того розміру або ж не з тими таймаутами то це з’єднання треба скинути. Реалізувати це можна для всіх не коректних підключень з WAN таким чином: створюється правило chain – input, на інтерфейсі WAN, та в action – drop.

Оскільки в мережі використовується management підмережа то потрібно створити правило для доступу усім пристроям з цієї підмережи до інших підмереж. Для цього створюємо правило в якому chain – forward, src address – 172.22.0.0./16 та в action – accept.

Аналогічно створюємо правило доступу для серверної мережі, де chain – forward, src address – 10.0.0.0/8 та action -accept.

Таке правило доступу до ресурсів можна створити для пристроїв які не перебувають у підмережі management або servers. Для цього потрібно створити address list з назвою admins та додати туди адреси яким потрібно надати доступ. Правило доступу для такої групи створюється аналогічно до інших тільки замість підмережі вказується в вкладці advanced src. Address list – admins.

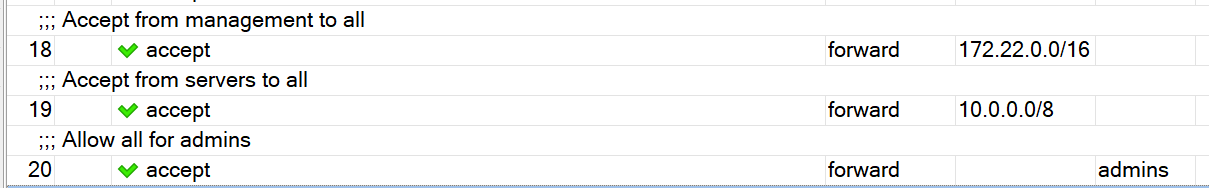


Рис.3.17. Приклад створення правил для доступу в усі підмережі

Для того, щоб захистити сервіси які знаходяться у серверній підмережи потрібно створити правило де chain – forward, protocol – 6 (tcp), dst. Port - 3389, 22, 23 та інтерфейс на на який накладається це правило out. Interface – servers. В action – drop та логування з префіксом - to servers control.

Для забезпечення доступу з певної підмережі до якогось ресурсу потрібно створити address list та додати в нього адресу до якої необхідно надати доступ. Після цього створюється правило в chain – forward, в src. Address прописується пул адрес або один IP з якого потрібно підключатись до списку IP, які знаходяться в створеному address list, який вказується в advanced dts. Address list, action – accepted.

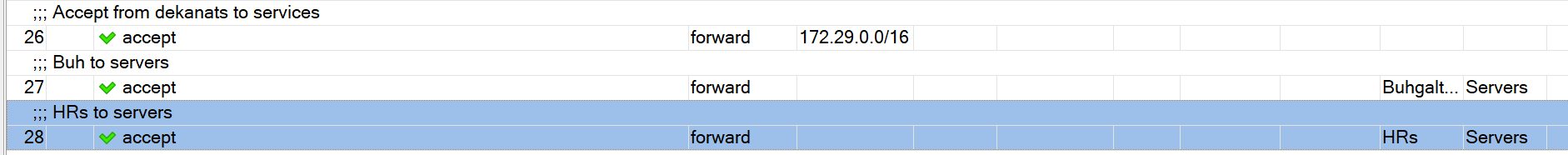


Рис.3.18. Приклад правила для доступу до певних IP адрес

**NAT**

NAT — це тип мережевого програмного забезпечення, що використовується для маскування IPv4 за білими IP адресами. Він заснований на ядрі Linux і забезпечує безпеку та інші функції, спеціально адаптовані до потреб користувачів. Використовується для створення віртуальних приватних мереж (VPN), а також для керування віддаленим доступом і безпекою. Це робить його корисним для адміністраторів мереж. NAT Mikrotik розроблений таким чином, щоб бути простим у використанні та налаштуванні.

Для збільшення рівня безпеки та відмовостійкості, у разі бану однієї з публічних IP адрес створюємо правила для виходу в інтернет для кожної підмережі окремо.

Щоб це зробити потрібно перейти в вкладку NAT у вікні налаштувань firewall. Далі створити правило де chain – srcnat, src.address - 172.25.240.0-172.25.255.254, out interface list – WAN, у викні action – src-nat, to address 86.111.90.226.

За аналогією створюються всі інші правила для підмереж.

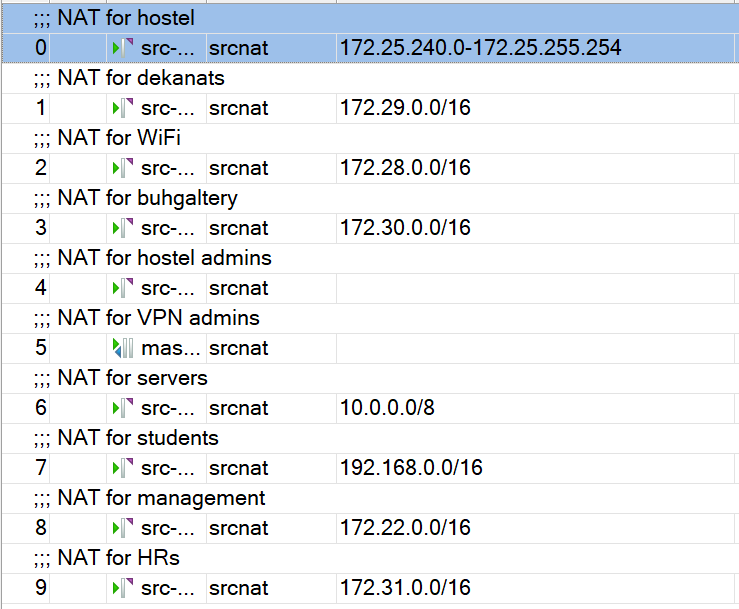


Рис.3.19. Приклад створення правил NAT для виходу в інтернет

Якщо є потреба організувати доступ до внутрішніх ресурсів через білу IP адресу треба створити правило в якому chain – dstnat, protocol – 17 (udp), dst. Port - 14888, 44882 та action – dst-nat, to addresses – 172.25.14.88.

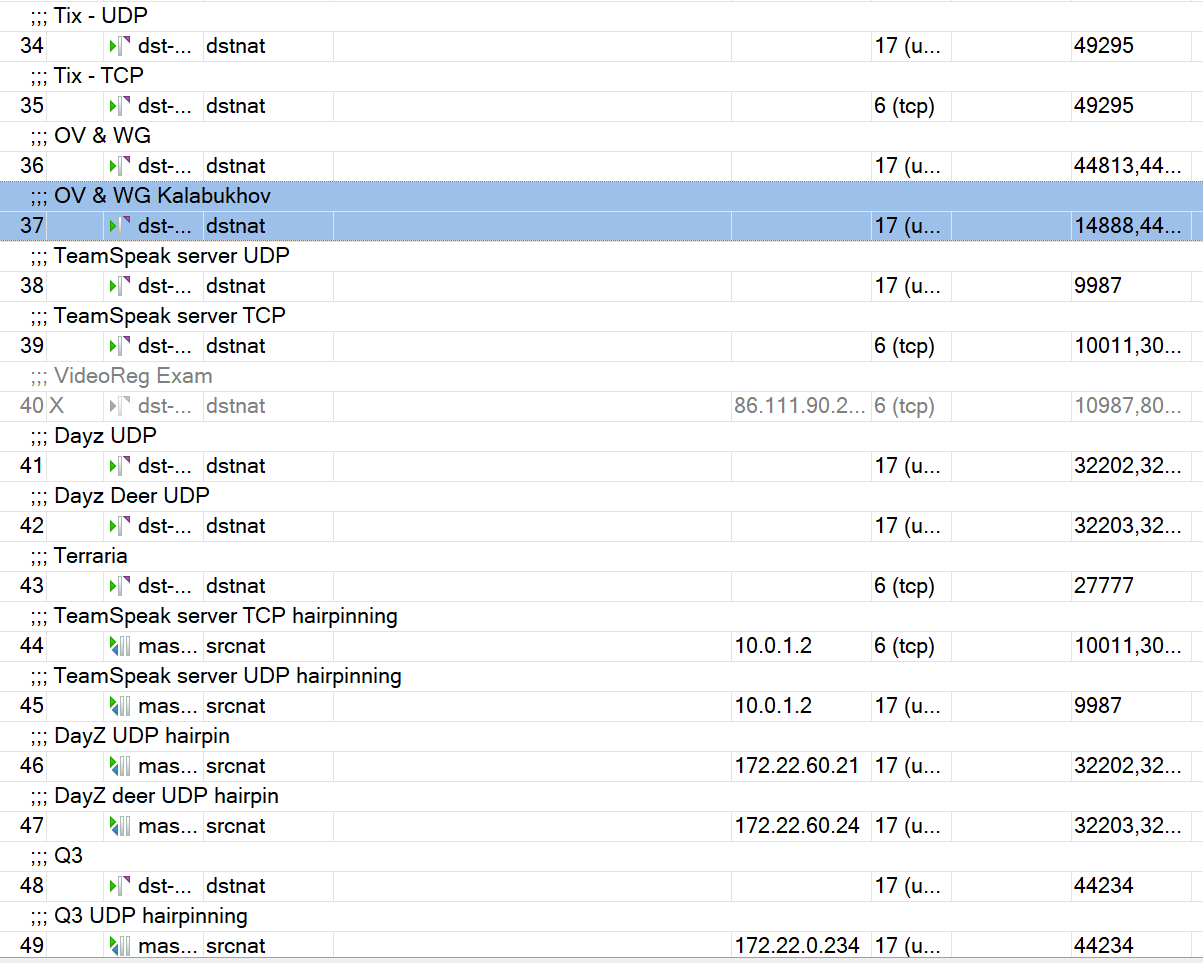


Рис.3.20. Приклад створених правил для доступу до внутрішніх ресурсів через білу IP адресу

## 3.4 Основні рекомендації щодо побудові захищеної корпоративної мережі

Створення захищеної корпоративної мережі необхідне будь-якої організації. Мережа є основою, на якій будуються всі інші заходи безпеки, та забезпечує безпечне середовище для збереження та використання даних, зв'язку та інших дій. Щоб забезпечити безпеку корпоративної мережі, важливо дотримуватися основних рекомендацій:

Правильна конфігурація мережевого обладнання та його захист на рівні L2. Потрібно вимикати всі сервіси які не будуть використовуватись в подальшій роботі. Не від’ємною частиною побудови захищеної системи є парольна політика, яка виключає використання словникових логінів та паролів користувачів з привілейований доступом.

Наступною рекомендацією є налаштування firewall з правилами, які чітко обмежують чи надають доступ до певних сервісів в мережі. Використання шифрованих VPN з’єднань типу L2TP з IPsec. Налаштування технології fail2ban для користувачів які намагаються отримати несанкціонований доступ в мережі.

Захист робочої бездротової мережї за допомогою надійного протоколу шифрування та паролю. Створення повністю ізольованої гостьової мережї, з максимально заблокованим доступом до внутрішніх сервісів.

Для забезпечення конфіденційності та цілісності даних потрібно побудувати повний ланцюжок довіри для сервісів з генерацією SSL сертифікатів.

Використовуйте технологію VLAN для сегментації мережі, щоб обмежити доступ до конфіденційної інформації та ресурсів.

Використовуйте системи моніторингу сервісів та пристроїв в мережі для швидкого реагування на інциденти.

Регулярно перевіряйте оновлення програмного забезпечення та слідкуйте за новими вразливостями, які виявляють після апдейтів,

Перевіряйте мережу щодо будь-яких підозрілих дій чи аномалій.

# ВИСНОВКИ

В бакалаврській роботі було розглянуті питання процесу забезпеченя безпеки мереж в інформаційній системі. Основним завдання є захист даних, програм, пристроїв і систем, підключених до мережі. Мережеві атаки — це зловмисні спроби отримання доступу або зміни даних в мережі без дозволу її власника. Мережеві атаки покладаються на вразливі місця в інфраструктурі, такі як слабкі паролі, незахищені порти або відсутність шифрування. Ці атаки можуть включати перехоплення пакетів, атаки на відмову в обслуговуванні (DoS), впровадження шкідливого коду, фішингові шахрайства тощо.

В другому розділі були розгялнуті методи та засоби захисту даних в мережі, такі як:

* автентифікація оскільки вона дозволяє лише авторизованим користувачам або процесам отримувати доступ до ресурсів компанії;
* шифрування даних яке забезпечує цілісність та конфіденційність даних в мережі;
* технології віддаленого доступу які дозволяють користувачам підключатись з віддаленого місця до центральної мережі організації за допомогою шифрованого каналу зв’язку.

В третьому розділі було розглянуто приклад налаштувань захищеної корпоративної мережі на базі обладнання Mikrotik. Проаналізовано основні функції захисту мережі на рівні L2 та L3. Основними налаштуваннями для захисту в RouterOS є:

* Firewall
* NAT
* User manager
* Package manager
* Network services

Отже, щоб запобігти мережевим атакам, організації повинні забезпечити регулярний моніторинг і перевірку мереж на вразливості, використовувати надійні методи автентифікації та шифрувати конфіденційні дані, оновлювати програмне забезпечення, правильно налаштовувати мережеве обладнання та проводити постійні навчання для співробітників.

# ПЕРЕЛІК ПОСИЛАНЬ

1. https://wiki.mikrotik.com/wiki/Manual:Winbox
2. https://treolink.ru/articles/WI-FI-roaming0.
3. https://uk.wikipedia.org/wiki/VPN
4. https://www.cisco.com/
5. https://glci.net/how-to-build-a-secure-network/
6. https://www.gflesch.com/elevity-it-blog/ways-to-secure-a-computer-network
7. https://www.cisa.gov/uscert/ncas/alerts/TA14-017A
8. https://www.hanovercomms.com/2016/04/20/a-breach-of-trust/
9. https://www.ukca.in/wp-content/uploads/2019/08/ABUSE-OF-DOMINANCE-IN-CYBERSPACE.pdf
10. https://www.techradar.com/vpn/remote-access-vpn
11. https://www.ncp-e.com/en/solutions/vpn/remote-access-vpn-technologies/ipsec-vpn/
12. https://www.remoteaccessworks.com/Remote-Access-Technologies.asp
13. https://resources.infosecinstitute.com/topic/vpns-and-remote-access-technologies/

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)