Міністерство освіти і науки України
Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп’ютерних систем та мереж

Пояснювальна записка
до кваліфікаційної роботи магістра
за спеціальністю 123 «Комп’ютерна інженерія»

на тему: КОМПЛЕКСНІ МЕТОДИ ЗАХИСТУ МОДЕРНІЗОВАНОЇ ЛОКАЛЬНОЇ КОМП’ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Проектував _____ В. О. Микитюк

Керівник роботи _____ Ю. О. Кумченко

Нормоконтроль _____ Д. І. Кузнєцов

Завідувач кафедри _____ А. І. Купін

Кривий Ріг
2023

Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерних систем та мереж

Ступінь вищої освіти магістр
Спеціальність 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри, голова циклової комісії

_____ А. І. Купін

"____" _____ 20__ року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

_____
(прізвище, ім'я, по батькові)

1. Тема роботи _____
_____
_____
керівник роботи _____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "___"_____ 20__року №__
2. Строк подання студентом роботи _____
3. Вихідні дані до роботи _____
_____
_____
_____
_____
_____
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_____
_____
_____
_____
_____
_____
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)_____
_____
_____
_____
_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Строк виконання етапів роботи	Примітка

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 112 сторінок, 103 рисунки, 2 таблиць, 3 формули, 24 використаних джерел.

Мета даної кваліфікаційної роботи – комплексні методи захисту модернізованої локальної комп'ютерної мережі підприємства ТОВ «МетТрансСервіс».

Даний проект складається з 3 розділів.

У першому розділі виконано огляд стандартів безпеки, видів атак та методу комплексного захисту мережі.

Другий розділ виконана розробка топології мережі (логічна та фізична), розглянуто пом'якшення загроз модернізованої ЛКМ підприємства та зроблений кореляційний аналіз SIEM.

У третьому розділі проведно проектування модернізованої мережі у програмі Packet Tracert, налаштування безпеки та тестування мережі.

КОМП'ЮТЕРНІ МЕРЕЖІ, ЛОКАЛЬНА КОМП'ЮТЕРНА МЕРЕЖА, ЗАХИСТ КОМП'ЮТЕРНИХ МЕРЕЖ, КОМПЛЕКСНІ МЕТОДИ ЗАХИСТУ, МЕТОДИ ПОМ'ЯКШЕННЯ ЗАГРОЗ, КОРЕЛЯЦІЙНИЙ АНАЛІЗ, SIEM.

Explanatory note: 112 pages, 103 figures, 2 tables, 3 formulas, 24 used sources.

The purpose of this qualification work is to implement comprehensive methods for securing the modernized local computer network of the company “MetTransService.”

This project consists of 3 sections.

The first section provides an overview of security standards, types of attacks, and methods of comprehensive network protection.

In the second section, the development of the network topology (logical and physical), audit of existing equipment (active and passive), mitigation of threats to the modernized enterprise's local computer network, and correlation analysis of SIEM are performed.

The third section involves designing the modernized network in the Packet Tracer program, configuring security, and testing the network.

COMPUTER NETWORKS, LOCAL AREA NETWORK, COMPUTER NETWORK SECURITY, COMPREHENSIVE SECURITY METHODS, THREAT MITIGATION METHODS, CORRELATION ANALYSIS, SIEM.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ЛОМ – локальна комп’ютерна мережа.

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

СУІБ – система управління інформаційною безпекою ;

DHCP – dynamic host configuration protocol (Протокол динамічного налаштування вузла);

DNS – domain name system (Система доменних імен);

Firewall – мережевий екран;

ISMS – information security management system (система управління інформаційною безпекою);

ISO – international organization for standardization (міжнародна організація стандартизації);

ISO/IEC – information technology security techniques information security management systems requirements (інформаційні технології методи безпеки системи управління інформаційною безпекою вимоги);

NIST – the national institute of standards and technology (національний інститут стандартів і технології — національний орган зі стандартизації у США) ;

SIEM – security information and event management (інформація про безпеку та управління подіями);

VLAN – virtual local area network (віртуальна локальна комп'ютерна мережа);

VPN – virtual private network (віртуальна приватна мережа).

ВСТУП

У сучасних умовах, коли комп’ютерні технології займають все більш вагому роль у підприємницькій діяльності, особливу увагу приділяється захисту локальної комп’ютерної мережі підприємства. Захист мережі від несанкціонованого доступу, вірусів та інших шкідливих програм є надзвичайно важливим завданням, що допомагає зберегти конфіденційну інформацію та забезпечити нормальне функціонування системи.

Завдяки постійному розвитку обчислювальної техніки, сучасні комп'ютерні мережі стають більш швидкими, потужними та ефективними. Та разом з усім цим ростом приходить велика відповідальність щодо їхньої безпеки та надійності. Важливим аспектом стає збереження конфіденційності, доступності та цілісності даних, що зберігаються та обмінюються в локальних мережах підприємств.

Одразу після відкриття комп'ютерних мереж, почали з’являтися нові, надзвичайно широкі можливості застосування комп’ютерів. Раніше комп’ютери використовувались лише для обробки та зберігання інформації, але з цим новим відкриттям їх функціонал розширився до отримання та обміну інформації з іншими пристроями у цій мережі. На наш час локальні обчислювальні мережі (ЛОМ) отримали велике поширення серед малих та великих компаній. Локальна комп’ютерна мережа – це група, яка може складатись з необмеженої кількості комп’ютерів (мінімальна кількість починаючи з двох), які з’єднанні між собою за допомогою кабелів (з початком використанням таких мереж це були навіть телефоні лінії або кабелі для передачі радіоканалів), завдяки яким відбувалось передавання інформації між пристроями. Звичайно для побудови локальної мережі потрібне необхідне професійне обладнання та програмне забезпечення. Це обумовлено декількома причинами: об’єднання комп’ютерів у одну мережу дає можливість економічного розвитку, тобто економити гроші за рахунок зменшення витрат на вміст комп’ютерів (для простої роботи достатньо мати певний дисковий об’єм на головному комп’ютері мережі з установленим на ньому програмним забезпеченням та додатковими програмами, які можуть використовувати одразу декілька робітників мережі).

Однією з особливостей використання локальних мереж є те, що вони дозволяють застосувати поштову скриньку для відправки повідомлень на інші комп’ютери завдяки цьому за короткий термін можно передати усі документи та інформацію з одного пристроя на інший.

До того ж, у сучасному житті є сфери діяльності робота яких неможлива без використання ЛОМ. Приклад таких сфер є: банківська діяльність, великі компанії, електроні архіви лікарень, бібліотек та інші.

З кожним днем таких сфер становиться більше та усі вони потребують використання локальних мереж, адже один комп’ютер фізично не може зберігати усю інформацію компанії або інших закладів, основною причиною цього є занадто великий обсяг. Локальна мережа має багато особливостей та позитивних риси щодо її використання, але основною є те, що системний адміністратор, інакше – оператор, має особливий – привелійований статус, завдяки якому, наприклад, на файл-сервері можливо допускати лише зареєстрованих користувачів, які можуть отримувати доступ та спеціальний список дії до тієї інформації, до якої у них відкритий доступ.

Актуальність роботи «Комплексні методи захисту та модернізації локальної комп'ютерної мережі підприємства» виникла з усвідомлення актуальності проблеми захисту інформації та підвищення ефективності мережі в умовах постійних змін у технологічному середовищі. Швидкий розвиток кількості підключених пристроїв, зростання обсягу обміну даними та загрози кібербезпеки створюють необхідність впровадження новаторських методів захисту та оптимізації.

Мета і завдання дослідження. Мета дослідження полягає в створенні комплексного підходу до захисту та модернізації локальної комп'ютерної мережі підприємства, що сприятиме підвищенню її продуктивності та надійності.

Завдання дослідження спрямоване на виявлення та критичний аналіз сучасних проблем в області захисту локальних комп'ютерних мереж, а також порівняння із відомими рішеннями цих проблем.

Основні завдання дослідження включають:

1. Виявлення і аналіз існуючих проблем та слабких місць у системі захисту локальної мережі підприємства.
2. Сформулювання рекомендацій з удосконалення та модернізації заходів безпеки на різних рівнях локальної мережі.
3. Визначення оптимальних методів і засобів захисту, які враховують специфіку діяльності підприємства та його інформаційні потреби.
4. Розробка стратегії та плану впровадження комплексних методів захисту для забезпечення стійкості та безпеки локальної мережі.
5. Встановлення ефективних механізмів моніторингу та аудиту, спрямованих на постійне вдосконалення системи захисту

Об’єкт дослідження у контексті теми «Комплексні методи захисту та модернізації локальної комп'ютерної мережі підприємства» є локальна комп'ютерна мережа підприємства, зокрема, така, яка функціонує у ТОВ «МетТрансСервіс».

Предмет дослідження – комплексні методи захисту та модернізація локальної комп’ютерної мережі ТОВ «МетТрансСервіс».

Методи досліджень. Дослідження базується на аналізі даних, отриманих в ході огляду літератури, проведення експертних опитувань та практичних випробувань:

1. Аналіз літератури: Проведений огляд наукових робіт, статей, та методичних матеріалів у галузі захисту та модернізації локальних комп'ютерних мереж.
2. Експертні оцінки: Залучення фахівців із сфери інформаційної безпеки для отримання кваліфікованої думки та рекомендацій.
3. Практичні експерименти: Використання практичних експериментів для апробації та перевірки ефективності запропонованих методів захисту.

Наукова новизна одержаних результатів. Внесення нововведення у сферу захисту локальних комп'ютерних мереж, зокрема розробивши комплексні методи, які враховують сучасні виклики та ризики в цій області. Підходи спрямовані на підвищення стійкості та ефективності заходів безпеки.

Вперше на підприємстві ТОВ «МетТрансСервіс» опитані респонденти різної вікової категорії та на основі цих даних виконано кореляційний аналіз та вдосконалено систему навчання кібербезпеці серед користувачів Інтернету. У результаті перед навчанням, більшість респондентів (46%) відвідували фішингові сайти з цікавості, тоді як після навчання цей показник зменшився до 18.6%.

Практичне значення отриманих результатів. Запропоновано комплексний метод захисту локальної комп’ютерної мережі, який містить 5 етапів: антивірусне програмне забезпечення, фаєрвол та системи виявлення вторгнень, шифрування даних, створення резервних копій даних, навчання користувачів. Розробки пройшли експериментальну перевірку на підприємства ТОВ «МетТрансСервіс» та готові до практичного застосування.

Апробація роботи відбулась на двох конференціях КІСМ 2022 – 2023 роки:

1. Микитюк В. О., Кумченко Ю. О. Аудит та модернізація локальної комп’ютерної мережі . XV Всеукраїнська науково-практична WEB конференція аспірантів, студентів та молодих вчених «Комп’ютерні інтелектуальні системи та мережі» : 22–24 березня 2022 р. : матер. Кривий Ріг, 2022. С. 3–4.

2. Микитюк В. О., Кумченко Ю. О. Комплексні методи захисту локальної комп’ютерної мережі підприємства. XVI Всеукраїнська науково-практична WEB конференція аспірантів, студентів та молодих вчених «Комп’ютерні інтелектуальні системи та мережі» : 21–23 березня 2023 р. : матер. Кривий Ріг, 2023. С. 271–274.

1 ОГЛЯД СТАНДАРТІВ БЕЗПЕКИ, ВИДІВ АТАК ТА МЕТОДУ КОМПЛЕКСНОГО ЗАХИСТУ МЕРЕЖІ

1.1 Опис підприємства

Підприємство ТОВ «МетТрансСервіс» засноване в 2004 році. За період своєї діяльності на ринку промислового та цивільного будівництва компанія успішно створила потужну інжинірингову структуру. У їхньому розпорядженні є власний парк будівельних механізмів, завод для виготовлення металоконструкцій, а також сильний інженерний корпус та кваліфікований робочий персонал. Це дозволяє їм успішно втілювати навіть найскладніші інвестиційні проекти [1].

Види діяльності компанії підтверджені ліцензією та повним переліком дозвільних документів. Ця компанія пропонує широкий спектр послуг – від виробництва металоконструкцій, загально будівельних робіт, монтажу технологічного обладнання до будівництва об'єктів «під ключ», від будівництва торгових будівель до реконструкцій об'єктів підприємств легкої та важкої промисловості (рис.1.1).

Рисунок 1.1 – Об’єкти підприємства ТОВ «МетТрансСервіс»

У портфоліо компанії великі інвестиційні проекти в агросекторі (більше 25 проектів), гірничо-металургійному секторі (більше 15 проектів) та рітейл (більше 10 проектів).

Працювали та будували для: ПАТ «АрселорМіттал Кривий Ріг», «Метінвест», ТОВ «Інтерпайп», ТОВ «Астарта», ТОВ «Kernel», ТОВ СП «Нібулон», ТОВ «Укрлендфармінг», ТОВ «МРІЯ», ТОВ «Каргілл», ТОВ «Оллсідз», ТОВ «Фреш».

1.2 Міжнародні стандарти інформаційної безпеки

Існує багато систем поглядів та різних способів класифікації стандартів. Методи групування відрізняються залежно від цілей та завдань використання. Розглянемо стандарти з прикладної та процесної точок зору. Стандарти можна розділити на:

1. Технічні чи контрольні (контрольні), які регламентують різні аспекти реалізації заходів захисту.
2. Процесно-орієнтовані, які описують підхід до створення процесів та забезпечення інформаційної безпеки в цілому.

Технічні стандарти сприяють будівництву технічного захисту інформації - вибору необхідних заходів захисту та їх належній настройці. Процесно-орієнтовані стандарти описують підхід до створення окремих процесів. До процесно-орієнтованих стандартів відносяться: серія ISO/IEC 27XXX, управління ITIL, методологія COBIT і так далі. У відношенні до технічних стандартів варто відзначити проект OWASP Top 10, CIS Controls і CIS Benchmarks, які містять докладну інформацію щодо безпеки IT-елементів інфраструктури, що сприяє протидії широкому спектру загроз. Проте не завжди варто однозначно ділити стандарти на категорії. Один стандарт може агрегувати інформацію з кількох напрямів. Наприклад, стандарт PCI DSS (стандарт безпеки даних індустрії платіжних карток) відображає комплексний підхід до забезпечення інформаційної безпеки і містить як вимоги до управління безпекою, правила та процедури, так і великий перелік технічних вимог до критичних заходів захисту [2].

Міжнародні стандарти інформаційної безпеки є важливими нормативними документами, призначеними для визначення вимог та практик забезпечення безпеки інформації в організаціях і компаніях. Ось кілька ключових міжнародних стандартів інформаційної безпеки:

1. ISO/IEC 27002:
   Застосування: Цей стандарт надає конкретні рекомендації щодо контролів і заходів безпеки, які можуть бути впроваджені для виконання ISO/IEC 27001. Він надає більш детальні вказівки щодо конкретних аспектів інформаційної безпеки.
   Складові: Включає рекомендації з контролю доступу, шифрування, резервного копіювання даних, обробки даних, безпеки програмного забезпечення і багато іншого.
2. ISO/IEC 27005:
   Застосування: Цей стандарт визначає процеси та методи аналізу ризиків із застосуванням інформаційної безпеки. Він допомагає

організаціям визначати потенційні загрози та слабкі місця у їхніх системах.

Складові: Включає визначення методів аналізу ризиків, оцінку і прийняття рішень щодо ризиків та розробку стратегій зменшення ризиків.

3. ISO/IEC 27017:

   Застосування: Цей стандарт концентрується на вимогах безпеки хмарних служб. Він надає рекомендації та контрольні точки для захисту інформації, яка зберігається в хмарних середовищах.

   Складові: Включає рекомендації з безпеки віртуалізації, контролю доступу, ідентифікації та аудиту в хмарних середовищах.

4. ISO/IEC 27032:

   Застосування: Цей стандарт розглядає безпеку в глобальному інформаційному суспільстві. Він надає вказівки щодо захисту від кіберзагроз і кібератак на всіх рівнях.

   Складові: Включає принципи та методи захисту мереж, систем та інформаці.

Стандарти NIST 800-53 та ISO 27001 грають ключову роль у галузі кібербезпеки та управління інформаційною безпекою. Ці нормативні документи визначають вимоги та рекомендації для створення інформаційних систем та систем управління інформаційною безпекою, які допомагають організаціям забезпечувати конфіденційність, цілісність та доступність своєї інформації.

ISO/IEC 27001, також відомий як ISO 27001, є стандартом з безпеки, який визначає рекомендовані вимоги для створення, контролю та вдосконалення системи управління інформаційною безпекою (ISMS). ISMS - це набір політик для захисту та управління чутливою інформацією підприємства, наприклад, фінансовими даними, інтелектуальною власністю, даними клієнтів та кадровими записами.

ISO 27001 - це добровільний стандарт, який використовується постачальниками послуг для захисту інформації клієнтів. Це вимагає незалежного та акредитованого органу для офіційної аудиту організації для забезпечення відповідності [2].

Переваги співпраці з постачальником послуг, який має сертифікат ISO 27001, включають:

1. Управління ризиками - ISMS допомагає регулювати, хто в організації може мати доступ до конкретної інформації, зменшуючи ризик її крадіжки або іншого порушення.
2. Інформаційна безпека - ISMS містить протоколи управління інформацією, що детально визначають, як потрібно обробляти та передавати конкретні дані.
3. Бізнес-континуїті - Щоб залишити відповідність ISO 27001, ISMS постачальника послуг повинна постійно тестуватися та вдосконалюватися. Це допомагає запобігти порушенням

інформації, які можуть вплинути на основні функції вашого бізнесу.

Для постачальників послуг відповідність надає заспокоєння вашим клієнтам, дозволяючи вам виконувати належний обсяг обережності щодо безпеки даних.

Дотримання ISO 27001 може відігравати важливу роль у створенні політики управління інформаційною безпекою - плани, інструменти та бізнес-практики, які використовуються підприємством для захисту їх чутливих даних (рис.1.2).

Створення ISO-сумісної ISMS - це комплексний процес, який включає визначення обсягу, планування, навчання та підтримку. Нижче наведено деякі з найважливіших аспектів, які потрібно врахувати до отримання сертифіката підприємства [2].

Рисунок 1.2 – Аспекти ISO 27001

1. Організаційний контекст.

Необхідно визначити внутрішні та зовнішні питання, які можуть вплинути на можливість підприємства створити систему управління інформаційною безпекою (СУІБ), наприклад, інформаційну безпеку, а також юридичні, регуляторні та контрактні зобов'язання.

2. Обсяг.

Інформація, визначена на першому етапі, використовується для документування обсягу СУІБ, визначаючи відповідні області, а також межі. СУІБ потрібно реалізувати, підтримувати та постійно вдосконалювати відповідно до конкретних ризиків інформаційної безпеки та вимог ISO 27001.

Обсяг підкреслює важливість інтеграції СУІБ як частини загальної структури та процесу управління. Вимоги застосовуються до всіх організацій, незалежно від типу, розміру або галузі.

3. Керівництво

Управління підприємства повинно мати необхідні лідерські навички для підтримки СУІБ. Це включає в себе:

3.1 Створення політики інформаційної безпеки відповідно до стратегічного напрямку організації.

3.2 Інтеграція СУІБ в стандартні процеси організації.

3.3 Повідомлення деталей політики інформаційної безпеки та підкреслення важливості вимог СУІБ.

3.4 Поширення постійного вдосконалення СУІБ.

3.5 Забезпечення належної підтримки співробітників, які працюють над вдосконаленням системи.

4. Планування.

План для вирішення ризиків інформаційної безпеки повинен бути інтегрований в процес СУІБ. Це включає в себе:

4.1 Встановлення та застосування докладного процесу управління ризиками інформаційної безпеки, який включає критерії ризику, ідентифікацію загроз інформаційній безпеці, аналіз ризиків та оцінку ризиків відносно встановлених критеріїв.

4.2 Визначення та застосування процесу зниження ризиків, який включає контрольні заходи, необхідні для впровадження кожної опції зниження ризиків.

5. Підтримка.

Підприємство повинно отримати ресурси, персонал та інфраструктуру для ефективної реалізації СУІБ.

Підтримка включає навчання та наставництво персоналу з питань обробки чутливої інформації. Крім того, співробітникам повинно бути повідомлено, як вони можуть сприяти ефективності СУІБ і наслідки невідповідності політиці інформаційної безпеки.

Нарешті, повинні бути встановлені внутрішні та зовнішні політики комунікації, які стосуються СУІБ. Політики повинні включати визначення питань, які потрібно повідомляти, з ким ці питання повинні бути повідомлені і методи комунікації [2].

6. Операції.

Цей крок акцентує у виконанні планів і процесів, визначених на попередніх етапах. Організація повинна документувати всі дії, здійснювані для забезпечення виконання процесів, як заплановано. Крім того, потрібно визначити віддані процеси для оцінки та контролю ризиків інформаційної безпеки.

7. Оцінка продуктивності.

Оцінка продуктивності забезпечує продовження ефективності та майбутнє вдосконалення СУІБ.

Вона також регулярно визначає області для потенційного вдосконалення інформаційної безпеки.

Внутрішні аудити та обговорення керівництва повинні проводитися та документуватися через визначені регулярні інтервали для оцінки продуктивності СУІБ.

8. Вдосконалення.

Невідповідності вимогам ISO 27001 потрібно виправляти негайно після виявлення. Організації повинні визначити та виконати кроки для того, щоб запобігти повторенню тих самих проблем. Крім того, підприємства повинні постійно намагатися покращити відповідність, адекватність та ефективність своєї Системи управління інформаційною безпекою.

NIST 800-53: NIST 800-53 - це набір контрольних заходів, ретельно підібраних Лабораторією інформаційних технологій (ITL). Ці контроли надають комплексний фреймворк для захисту відчутливих даних від різних загроз, починаючи від природних катастроф і закінчуючи зловмисними атаками.

NIST 800-53 - це стандарт в області відповідності до вимог щодо безпеки, який містить перелік контрольних заходів, які підкреслюють створення безпечної та надійної інформаційної системи федерального рівня. Контроли в стандарті є технічними, операційними та управлінськими і пов'язані з підтриманням конфіденційності, доступності та цілісності. Цей стандарт виник з необхідності боротьби з розвиваються технологічними можливостями національних супротивників і є результатом співпраці Міністерства торгівлі США та Національного інституту стандартів і технологій [2].

Мета NIST SP 800-53 полягає в підвищенні рівня безпеки інформаційних систем, які використовуються федеральним урядом. Мета NIST полягає в наданні рекомендацій у вигляді каталогу контрольних заходів, які сприяють розробці безпечних інформаційних систем.

Процес передбачає категоризацію вашої інформаційної системи на рівні низької, середньої або високої безпеки. З цими категоріями ви порівнюєте каталог безпеки NIST 800-53 і визначаєте, які контрольні заходи застосовуються до вашої компанії (рис.1.3).

Рисунок 1.3 – Схема контрольних заходів

Кожна сфера уваги наповнена діями, які спільно сприяють забезпеченню безпеки вашої системи. І ці дії - це не просто звичайні, пересічні завдання - це передові практики забезпечення інформаційної безпеки та плани реагування на інциденти, які допоможуть вам бути вперед у грі.

NIST 800-53 рекомендує впровадження потужних інструментів оцінки безпеки для надання реального часу для розуміння поточного стану безпеки вашої організації. Інструменти, такі як Sprinto, дозволяють вам вимірювати ефективність ваших заходів забезпечення безпеки та робити рекомендації щодо поліпшення системи на основі зібраного доказового матеріалу [3].

Sprinto надає можливість отримувати об'єктивні дані щодо рівня безпеки, оцінюючи ефективність заходів, які вже впроваджені в вашій організації. Це дозволяє вам аналізувати ризики та визначати слабкі місця в системі безпеки для подальших вдосконалень. Рекомендації, надані Sprinto, можуть стати основою для стратегії посилення безпеки та впровадження кращих практик у сфері інформаційної безпеки.

Ось 5 кроків для впровадження рамки NIST 800-53 в вашій організації (рис.1.4):

Рисунок 1.4 – Схема реалізації NIST 800 53

1. Створення умов для успіху.

Ключ до досягнення успіху в області забезпечення безпеки даних - це встановлення чіткого набору цілей. Створивши такий набір цілей, ви можете розробити план дій, визначити обсяг вашої безпеки та переконатися, що всі члени вашої організації знають, що їм слід робити.

1. Визначення цілей.

Сформулюйте конкретні, вимірювані, досяжні, реальні та часові цілі (SMART) для безпеки даних [3].

Определіть основні аспекти безпеки, такі як конфіденційність, цілісність та доступність.

2. Розробка плану.

Створіть стратегічний план дій, який включає в себе кроки по забезпеченню виконання поставлених цілей. Визначте та реалізуйте необхідні технологічні та організаційні заходи.

3. Визначення обсягу.

Оцініть обсяг і види даних, які потребують захисту. Визначте рівень захисту для кожного типу даних.

4. Інформування команди.

Забезпечте те, що всі працівники організації розуміють їхню роль у забезпеченні безпеки даних.

Надайте навчання та інструкції щодо правил та процедур безпеки.

5. Аудит та вдосконалення.

Проводьте систематичні аудити безпеки для визначення вразливостей та виявлення порушень. Періодично переглядайте та оновлюйте план дій відповідно до змін у середовищі або загрозах.

6. Своєчасна реакція.

Розробіть процедури реагування на інциденти та забезпечте швидку реакцію на події безпеки.

7. Поширення свідомості.

Проводьте кампанії щодо безпеки для підвищення свідомості серед персоналу.

Встановлення і слідування цим крокам допомагає створити ефективну стратегію безпеки даних та забезпечити успішність її впровадження в організації..

2. Оцінка вашого поточного стану.

Наступним кроком є оцінка зусиль вашої організації в області кібербезпеки шляхом докладної оцінки ризиків. Це надає цінні відомості щодо того, які з ваших поточних заходів відповідають стандартам NIST і що потребує покращення. Ви можете використовувати відкритий джерела інформації або наймати спеціалістів з кібербезпеки для ретельної оцінки.

3. Інивідуалізація.

Рамка NIST надає добровільні рекомендації, які застосовні до широкого спектру галузей. Проте кожний бізнес унікальний і вимагає індивідуального підходу. Створення профілю, в якому описані ваші потреби, дозволяє налаштувати рамку під вимоги вашої організації. Використання Рівнів Впровадження може підняти рівень кібербезпеки вашої організації від реактивного до проактивного.

4. Виявлення прогалин та створення плану дій.

Повідомте ключовим учасникам результати оцінки ризиків, щоб визначити вразливості та загрози для вашої діяльності, активів та осіб. Використовуйте результати для проведення аналізу прогалин і визначення пріоритетних областей, які потребують першочергового врегулювання. Це буде основою вашого плану дій [3].

5. Вровадження та постійне вдосконалення.

Зараз прийшов час реалізувати рамку NIST в діяльності. Однак важливо враховувати, що впровадження - це лише початок. Постійний моніторинг та вдосконалення необхідні для того, щоб переконатися, що рамка налаштована під ваші потреби бізнесу.

Продовжуйте ітерувати та вдосконалювати, щоб залишатися вперед у постійно змінному ландшафті кібербезпеки.

1.3 Опис видів атак

Щоб зберегти інформацію в мережі і на комп'ютерах безпечною та конфіденційною, дуже важливо розуміти різноманітні види атак, на які вона піддається. Зловмисники постійно шукають нові способи злому систем та здобуття несанкціонованого доступу до даних. Ми докладно розглянемо різні види атак, відомі в сфері кібербезпеки, і надамо інформацію щодо їх розпізнавання та захисту від них. Знання цих видів атак та відповідних профілактичних заходів є важливою частиною будь-якого плану забезпечення інформаційної безпеки [4].

Види атак – це різноманітні способи та методи, які зловмисники використовують для порушення інформаційної безпеки систем та мереж. Ось деякі з найпоширеніших видів атак:

1. DDoS-атаки (атаки на відмову в обслуговуванні): У таких атаках зловмисники використовують велику кількість пристроїв або ботів для перевантаження мережі або сервера, що призводить до його відмови в обслуговуванні.

Розподілена атака типу «відмова в обслуговуванні» (DDoS) – це зловмисна спроба порушити звичайний трафік цільового сервера, служби чи мережі, перевантаживши ціль або навколишню інфраструктуру потоком Інтернет-трафіку.

DDoS-атаки (розподілені атаки на обслуговування) досягають своєї ефективності, використовуючи численні скомпрометовані комп'ютерні системи як джерела трафіку атак. Експлуатовані машини можуть включати комп'ютери та інші мережеві ресурси, такі як пристрої Інтернету речей (IoT). На високому рівні, DDoS-атака подібна до неочікуваного затору, який забиває шосе, не дозволяючи регулярному транспорту дістатися до місця призначення.

Розглянемо цей процес більш детально.

Розподілені атаки

DDoS використовує розподілені атаки, що означає, що атаки відбуваються з численних джерел, розподілених по всій мережі.

Скомпрометовані системи:

Атакуючи використовують скомпрометовані комп'ютери та інші пристрої для створення армії зомбі (botnet).

Ці комп'ютери можуть бути заражені вірусами, троянськими програмами або іншими зловмисними програмами.

Ботнет

Ботнет – це мережа комп'ютерів, які були заражені і використовуються атакуючим для виконання команд.

Кількість комп'ютерів у ботнеті може бути величезною, надаючи атакуючому значний обсяг трафіку.

Ефективність атаки:

Чим більше скомпрометованих ресурсів використовує атакуючий, тим більшою стає ефективність DDoS-атаки.

Забруднення мережі трафіком може призвести до тимчасового відмову в обслуговуванні на цільовому сервері.

Швидкість інфраструктури:

Атаки можуть бути виконані дуже швидко, і реагувати на них може виявитися вельми важким завданням.

Захист

Організації повинні мати ефективні заходи безпеки, такі як фільтрація трафіку, виявлення та блокування ненормально великого обсягу запитів із сумнівних джерел, та використання служб захисту від DDoS.

Розуміння та захист від DDoS-атак важливе для забезпечення стабільності та доступності мережі та онлайн-сервісів [4].

Як працює DDoS-атака

DDoS-атаки здійснюються за допомогою мереж підключених до Інтернету машин.

Ці мережі складаються з комп’ютерів та інших пристроїв (наприклад, пристроїв Інтернету речей), які були заражені зловмисним програмним забезпеченням, що дозволяє зловмиснику дистанційно керувати ними. Ці окремі пристрої називають ботами (або зомбі), а групу ботів називають ботнетом (рис.1.5).

Після встановлення ботнету зловмисник може керувати атакою, надсилаючи віддалені інструкції кожному боту.

Коли ботнет атакує сервер або мережу жертви, кожен бот надсилає запити на IP-адресу цілі, потенційно спричиняючи перевантаження сервера чи мережі, що призводить до відмови в обслуговуванні для нормального трафіку.

Оскільки кожен бот є законним Інтернет-пристроєм, відокремити трафік атаки від звичайного трафіку може бути важко [4].

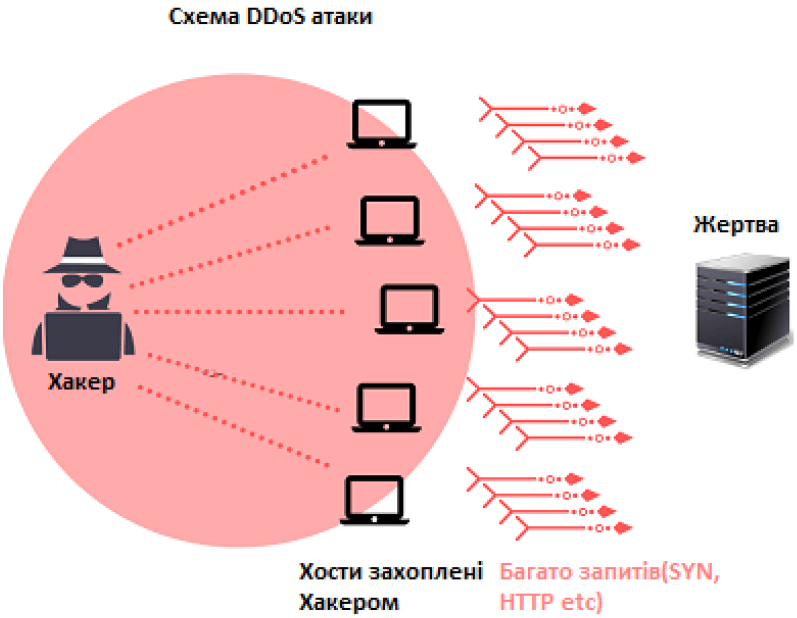


Рисунок 1.5 – Схема DDoS атаки

Як розпізнати DDoS-атаку.

Найбільш очевидним симптомом DDoS-атаки є те, що сайт або служба раптово стають повільними або недоступними. Але оскільки низка причин – такий законний сплеск трафіку – може спричинити схожі проблеми з продуктивністю, зазвичай потрібне подальше дослідження. Інструменти аналізу трафіку можуть допомогти вам помітити деякі з цих ознак DDoS-атаки:

1. Підозрілий обсяг трафіку, що надходить з однієї IP-адреси або діапазону IP-адрес
2. Потік трафіку від користувачів, які мають спільний профіль поведінки, як-от тип пристрою, геолокація або версія веб-переглядача
3. Незрозумілий сплеск запитів до однієї сторінки або кінцевої точки
4. Незвичайні моделі трафіку, такі як стрибки в непарні години дня або моделі, які здаються неприродними (наприклад, стрибки кожні 10 хвилин)

Існують інші, більш специфічні ознаки DDoS-атаки, які можуть відрізнятися залежно від типу атаки [4].

Поширені типи DDoS-атак.

Різні типи DDoS-атак спрямовані на різні компоненти мережевого з’єднання. Щоб зрозуміти, як працюють різні DDoS-атаки, необхідно знати, як здійснюється підключення до мережі.

Мережне підключення в Інтернеті складається з багатьох різних компонентів або «рівнів».

Як і будівництво будинку з нуля, кожен шар у моделі має різне призначення.

Модель OSI, показана нижче, є концептуальною структурою, яка використовується для опису підключення до мережі на 7 різних рівнях.

Модель OSI 7 рівнів: додаток, презентація, сеанс, транспорт, мережа, канал передачі даних, фізичний (рис.1.6).

Хоча майже всі DDoS-атаки включають перевантаження цільового пристрою або мережі трафіком, атаки можна розділити на три категорії. Зловмисник може використовувати один або кілька різних векторів атаки або циклічні вектори атаки у відповідь на контрзаходи, вжиті цілі.

Рисунок 1.6 – Схема OSI

2. Малиційне програмне забезпечення (шкідливе ПЗ): Шкідливе ПЗ, таке як віруси, троянські програми, шпигунське ПЗ та черв'яки, створені для впровадження в систему та заподіяння шкоди або крадіжки даних.

Шкідливе програмне забезпечення - це виробники зловживань та атак на комп'ютерні системи та мережі, яке створене зі зловживальними намірами. Це може включати в себе різноманітні види зловживань, такі як віруси, троянські програми, шпигунське ПЗ та черв'яки. Ось кілька ключових аспектів шкідливого програмного забезпечення [4]:

Віруси

Вірус – це програма, яка може впроваджуватися в інші програми та розповсюджувати себе, запускаючись при виконанні зараженої програми.

Метою вірусів може бути завдання різноманітних шкідливих наслідків, від видалення або пошкодження файлів до викрадення конфіденційної інформації.

Троянські програми

Троянська програма - це вид шкідливого програмного забезпечення, яке приховується під корисними програмами, але виконує шкідливі дії при їх використанні.

Троянські програми можуть відкривати доступ до системи для зловмисників, викрадати конфіденційні дані або завантажувати додаткове шкідливе програмне забезпечення.

Шпигунське програмне забезпечення

Шпигунське ПЗ призначене для відстеження та збору інформації про користувача без його знання.

Воно може перехоплювати логіни та паролі, відслідковувати веб-сайти, які відвідує користувач, або навіть реєструвати натискання клавіш.

Черв'яки

Черв'як - це самостійна програма, яка може розповсюджуватися та реплікувати себе через мережу без необхідності для введення виконавчого файлу.

Зловживання та крадіжка даних

Шкідливе ПЗ може бути використане для зловживання конфіденційних даних, таких як особисті ідентифікатори, фінансові дані або корпоративна інформація [4].

Антивірусна захист

Захист від шкідливого ПЗ включає в себе використання антивірусного програмного забезпечення, яке виявляє та блокує шкідливі програми перед їх виконанням.

Актуалізації та патчі

Регулярні апдейти та патчі для програм та операційних систем можуть допомогти у закритті вразливостей, через які шкідливе ПЗ може проникнути в систему.

3. Фішинг: Зловмисники надсилають підроблені повідомлення, які видають себе за легітимні запити на введення особистої інформації, такі як паролі, номери кредитних карток та інші чутливі дані (рис.1.7).

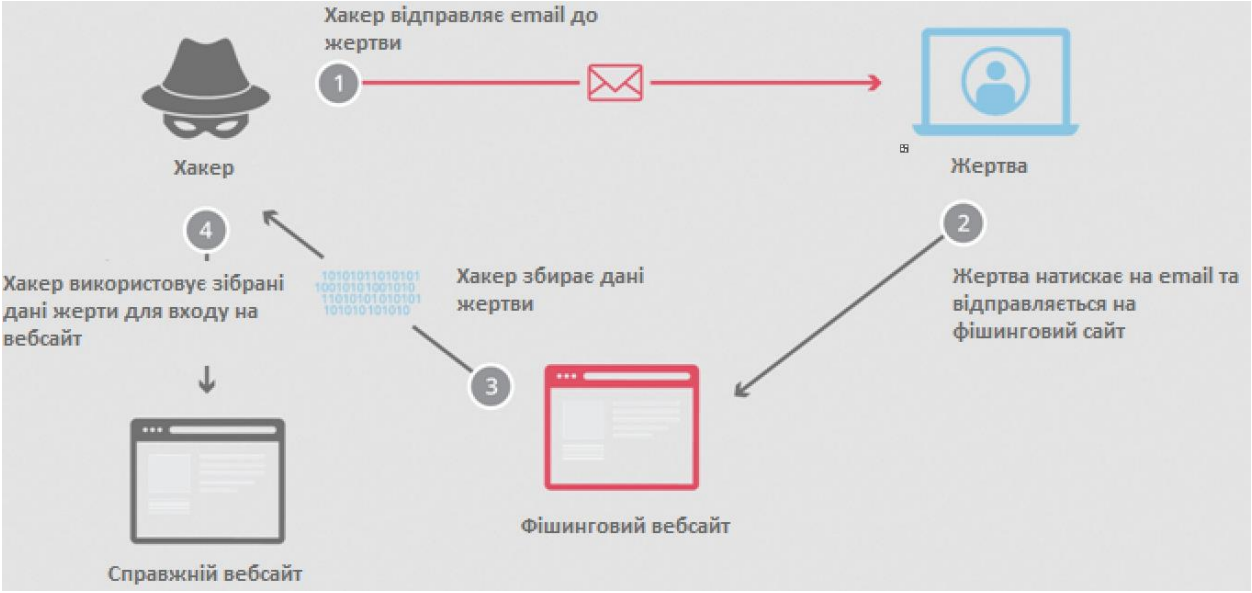


Рисунок 1.7 – Схема фішингових атака

Фішинг – починається з шахрайської електронної пошти чи іншого повідомлення, призначеного для заманювання жертви. Повідомлення виглядає так, ніби воно надійшло від надійного відправника. Якщо це вводить жертву в оману, її або її вмовляють надати конфіденційну інформацію, часто на веб-сайті шахраїв. Іноді зловмисне програмне забезпечення також завантажується на комп'ютер цілі [5].

Фішинг – це атака номер один, яка використовується проти малого та середнього бізнесу. Цей тип фішингу спрямований на конкретних осіб або компанії, звідси і термін «фішинг». Збираючи деталі або купуючи інформацію про певну ціль, зловмисник може влаштувати персоналізоване шахрайство. Наразі це найефективніший вид фішингу, на нього припадає понад 90% атак. Ось статистичні дані, які підкреслюють цей факт:

Фішинг є основною причиною витоку даних, на нього припадає 90% з них.

Щомісяця створюється майже 1,5 мільйона фішингових сайтів.

76% компаній повідомили, що стали жертвами фішингових атак у 2018 році

92% зловмисного програмного забезпечення доставляється через фішингові електронні листи.

4. SQL-ін'єкції: зловмисники використовують спеціально створені SQL-запити, щоб отримати несанкціонований доступ до баз даних.
5. Атаки на бездротові мережі: включають методи для злому або перехоплення трафіку в бездротових мережах, такі як атаки з перехоплення WEP-ключів.
6. Атаки на рівні програми: зловмисники досліджують і зламують слабкості у веб-додатках, щоб отримати доступ до даних або систем.

7. Міжмережні атаки (атаки на маршрутизатори та комутатори): Атаки, спрямовані на мережне обладнання, яке керує передачею даних між мережами.
8. Атаки із використанням соціальної інженерії: зловмисники маніпулюють людьми з метою отримання інформації або виконання певних дій.
9. Атаки на паролі: включають перебір паролів, використання словників та інші методи для злому паролів (рис.1.8).

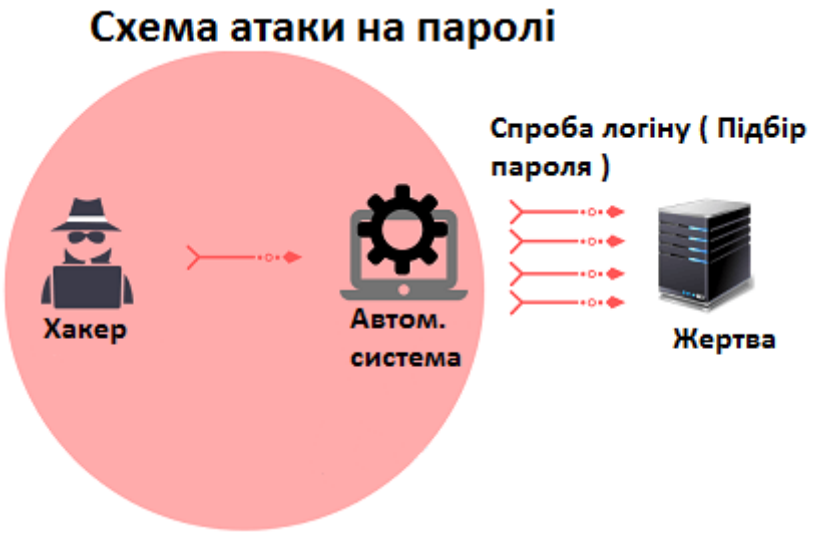


Рисунок 1.8 – Схема атаки на паролі

10. Атаки на системи керування доступом (ACS): зловмисники намагаються обійти системи контролю доступу для отримання несанкціонованого доступу до будівель або ресурсів.
11. Фізичні атаки: це включає фізичний вплив на обладнання, таке як крадіжка або пошкодження обладнання [5].
12. Атаки на перехоплення даних: зловмисники можуть спробувати перехопити дані, що передаються, використовуючи методи, такі як «прослуховування» або «втручання» в передачу даних (рис.1.9).

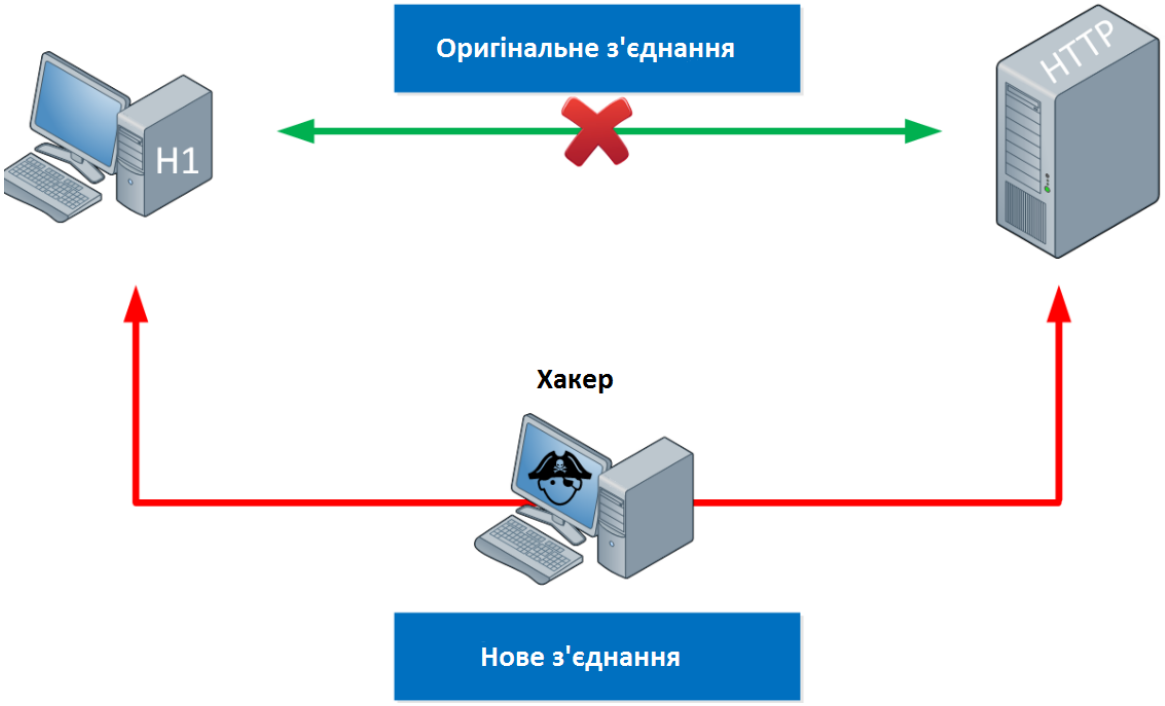


Рисунок 1.9 – Схема атаки виду “прослуховування”

13. Атаки на мережевий рівень: ці атаки включають мережне сканування, перехоплення трафіку та інші маніпуляції на рівні мережі.

Порти – це точки доступу до комп'ютера або сервера, які використовуються для обміну даними між різними програмами або службами. Ось кілька ключових аспектів сканера портів:

Визначення Відкритих Портів

Сканер портів проводить дослідження мережевих хостів для виявлення відкритих портів, які можуть свідчити про наявність активних служб або програм.

Аналіз Взаємозв'язку

Інформація про порти може бути використана для визначення, які програми чи служби працюють на хості. Знання цього може допомогти хакерам або адміністраторам з визначення потенційних вразливостей.

Безпека Мережі

Сканери портів також можуть використовуватися для тестування безпеки мережі. Адміністратори можуть сканувати свої власні системи, щоб виявити можливі ризики та вразливості [5].

Хакерські Атаки

Злоумисники можуть використовувати сканери портів для знаходження вразливих систем та впровадження атак. Вони можуть використовувати цю інформацію для здійснення атак на відкриті служби або програми.

Заходи Захисту

Адміністратори мереж можуть використовувати сканери портів для вдосконалення заходів безпеки, визначаючи та закриваючи непотрібні або вразливі порти.

Тестування Відповідності

У бізнес-середовищах сканери портів можуть використовуватися для тестування відповідності стандартам безпеки та виявлення будь-яких потенційних порушень.

Надзвичайно важливо знати поширені програми та відповідні їм номери портів. У таблиці 1.1 розглядаються програми, які використовують TCP, а в таблиці 1.2 розглядаються програми на основі UDP [6].

Таблиця 1.1 – Таблиця використання TCP портів

Назва порту(ів)	Номер порту(ів)
FTP	20, 21
Telnet	23
SMTP	25
DNS (zone transfers)	53
HTTP	80
POP3	110
NNTP	119
HTTPS	443

Таблиця 1.2 – Таблиця використання UDP портів

Назва порту(ів)	Номер порту(ів)
DHCP	67, 68
DNS (name resolution)	53
TFTP	69
NTP	123
SNMP	161

14. Атаки на фізичні слабкості: ці атаки включають злом замків, злом парасольок або злом сейфів для доступу до фізичних активів.

Атаки на фізичні слабкості відносяться до методів, що використовують фізичні засоби для здійснення несанкціонованого доступу або отримання контролю над фізичними активами організації. Ось деякі ключові аспекти таких атак [6]:

Злом Замків

Атаки на фізичні слабкості можуть включати методи злому замків, такі як використання недозволених ключів, взлом або підміна замків.

Злом Парасольок

При використанні електронних систем доступу, які можуть включати картки або парасольки, злоумисники можуть спробувати взламати або обійти ці системи для отримання доступу.

Злом Сейфів

Злом сейфів є ще одним способом атаки, де злоумисники використовують різноманітні техніки для відкриття сейфів і отримання доступу до цінних фізичних об'єктів.

Соціальний Інженеринг

Соціальний інженеринг може бути використаний для отримання фізичного доступу, наприклад, використовуючи переконливі та обманливі методи взаємодії з персоналом організації.

Атаки на Інфраструктуру

Злам інфраструктури, такої як електропостачання чи мережеві системи, може призвести до фізичних руйнувань і порушень безпеки.

Секретне Введення

Атаки можуть включати секретне введення в офісні приміщення, користуючись недостатнім контролем доступу або відсутністю адекватних систем безпеки.

Заходи Захисту

Заходи безпеки для захисту від фізичних атак включають встановлення надійних систем контролю доступу, використання камер спостереження, навчання персоналу та впровадження політик безпеки.

Фізична Аудиторія

Аудиторії фізичної безпеки можуть проводити інспекції та аудити для виявлення потенційних слабкостей та недоліків у заходах безпеки.

1.4 Комплексний метод захисту LAN

В умовах сьогодення комп’ютерні технології займають все більш вагому роль у підприємницькій діяльності, особлива увага приділяється захисту локальної комп’ютерної мережі (LAN) підприємства. Захист мережі від несанкціонованого доступу, вірусів та інших шкідливих програм є надзвичайно важливим завданням, що допомагає зберегти конфіденційну інформацію та забезпечити нормальне функціонування системи.

Побудуємо схему комплексного методу захисту модернізованої LAN підприємства (рис.1.10). Комплексні методи захисту полягають у використанні різних технологій та програм, що дозволяють забезпечити багаторівневу безпеку мережі.

Однією з головних проблем, пов’язаних з захистом LAN, є кількість кінцевих пристроїв (End Devices) підключених до мережі. Кожен пристрій може бути потенційною загрозою безпеці мережі, тому їх потрібно ретельно контролювати. Іншою проблемою є забезпечення безпеки при з’єднанні з Інтернетом [7].

Рисунок 1.10 – Схема комплексного методу захисту LAN підприємства

Першим і важливим кроком для забезпечення безпеки локальної комп'ютерної мережі є використання надійного антивірусного програмного забезпечення (Antivirus Software). Сучасні антивірусні програми мають високий рівень захисту і здатні ефективно виявляти та блокувати шкідливі програми, такі як віруси, троянці, шпигунські програми та інші загрози для комп'ютерної безпеки.

Однак успішна оборона не обмежується лише встановленням антивірусного програмного забезпечення. Щоб забезпечити максимальний рівень безпеки, рекомендується встановлювати антивірусне програмне забезпечення, яке має можливість автоматичного оновлення своїх баз даних. Це означає, що програма постійно оновлює свої вірусні сигнатури та інші складові для виявлення нових загроз. Оновлення дозволяє антивірусному програмному забезпеченню реагувати на останні види вірусів і шкідливих програм, збільшуючи його ефективність в боротьбі з ними [8].

Існує багато різних антивірусних програмних засобів, які використовуються для захисту комп'ютерних систем від шкідливих програм та інших загроз (рис.1.11). Деякі з найпопулярніших антивірусних програм на сьогоднішній день включають:

1. Norton Antivirus – відома антивірусна програма, що надає захист від шкідливих програм, вірусів та інших загроз. Має функцію «самозахисту», яка допомагає захистити систему від спроб відключити або видалити програму.

2. McAfee Antivirus – інший популярний антивірусний програмний засіб, гарантує захист від різноманітних загроз, таких як віруси, шпигунські програми та інші. Крім того, він також вміє захищати від фішингу та небезпечних веб-сайтів.

3. Avast Antivirus – безкоштовна антивірусна програма, яка надає захист від шкідливих програм, вірусів та інших загроз. Має різні функції, такі як антивірусний захист, захист від фішингу та анти-спам.

4. Bitdefender Antivirus – надійний антивірусний програмний засіб, який надає захист від шкідливих програм та інших загроз. Має функцію «автопілот», яка дозволяє автоматично керувати захистом системи та запобігати небезпечним діям

Рисунок 1.11 – Типи антивірусних програм

Важливо також пам'ятати, що антивірусне програмне забезпечення повинно працювати на всіх комп'ютерах в мережі, а не обмежуватися лише однією робочою станцією. Це забезпечить всебічний захист для всіх пристроїв у мережі та запобігатиме можливому поширенню шкідливих програм через внутрішню мережу [8].

Другий етап забезпечення безпеки локальної комп'ютерної мережі включає використання мережевих фаєрволів (Firewalls) та систем виявлення вторгнень (Intrusion Detection Systems), які є важливими компонентами системи захисту мережі.

Мережеві фаєрволи використовуються для контролю мережевого трафіку та блокування несанкціонованого доступу до ресурсів мережі. Їх функцією є аналіз кожного пакету даних, що проходить через мережу, і рішення про допуск або блокування цього пакету відповідно до встановлених

правил. Це допомагає уникнути несанкціонованого доступу до мережі та забезпечити захист від зовнішніх загроз, таких як хакерські атаки.

Системи виявлення вторгнень (IDS або Intrusion Detection Systems) застосовуються для виявлення спроб несанкціонованого доступу чи аномальної активності в мережі. Вони проводять аналіз мережевого трафіку та системних журналів, щоб виявити ознаки можливих атак. При виявленні підозрілої активності система IDS генерує сповіщення або сигнали тривоги для адміністраторів мережі. Це надає можливість реагувати на потенційні загрози та вживати заходів для їх запобігання або ліквідації. Третім етапом є використання систем шифрування даних. Шифрування забезпечує додатковий рівень захисту у випадку, якщо несанкціоновані особи отримають доступ до даних в мережі.

Шифрування може бути застосоване як для захисту даних під час передачі через мережу, так і для захисту даних, що зберігаються на пристроях в мережі.

Шифрування даних – це фундаментальний аспект кібербезпеки, і існують кілька різних методів шифрування, кожен із яких має свої особливості і використовується в різних сценаріях для захисту конфіденційності та цілісності даних. Ось більш детальний розгляд трьох основних методів шифрування [9]:

1. Симетричне шифрування: цей метод використовує один і той самий ключ як для шифрування, так і для розшифрування даних. Це означає, що якщо ви шифруєте дані з використанням певного ключа, то для їхнього розшифрування також потрібно використовувати той самий ключ (рис.1.12). Симетричне шифрування досить швидке і ефективне, але вимагає надійного способу обміну ключами між сторонами.

Рисунок 1.12 – Схема симетричного шифрування

2. Асиметричне шифрування: в асиметричному шифруванні використовуються два ключі – публічний та приватний. Публічний ключ використовується для шифрування даних, і будь-який може його використовувати, тоді як приватний ключ потрібен для розшифрування даних (рис.1.13). Цей метод дозволяє безпечно передавати публічний ключ, оскільки він не використовується для розшифрування. Асиметричне шифрування широко використовується для створення безпечних каналів для обміну ключами та іншою конфіденційною інформацією.

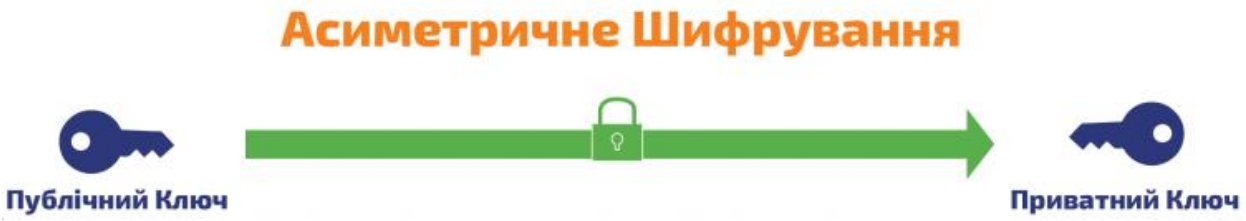


Рисунок 1.13 – Схема асиметричного шифрування

3. Хешування: хеш-функції використовуються для перетворення даних у неповторний хеш-код фіксованої довжини. Однак важливо зазначити, що хеш-коди не можуть бути розшифровані для відновлення оригінальних даних (рис.1.14) Хешування використовується для перевірки цілісності даних і часто використовується в паролях та для підпису даних.

Рисунок 1.14 – Схема хешування

Кожен з цих методів шифрування має свої переваги та недоліки і може бути використаний в залежності від конкретних потреб та загроз у вашій інформаційній системі. Важливо ретельно розглянути, який метод або комбінацію методів краще використовувати для забезпечення надійного захисту даних.

Четвертий етап забезпечення безпеки локальної комп'ютерної мережі включає в себе регулярне створення резервних копій даних (Data Backup), що є надзвичайно важливим аспектом для забезпечення безпеки та відновлення даних у випадку їх втрати або пошкодження [9].

Процедура резервного копіювання включає створення копій важливих даних та зберігання їх на окремих пристроях або в окремих мережах з обмеженим доступом. Це забезпечує, що дані будуть доступні для відновлення, навіть якщо вони будуть втрачені через випадкове видалення, атаки зловмисників, технічні проблеми або інші обставини.

Для максимальної ефективності та надійності резервних копій важливо дотримуватися деяких кращих практик:

1. Регулярність: резервні копії мають створюватися регулярно. Частота створення копій повинна відповідати чутливості даних і можливим втратам.
2. Зберігання в окремому місці: резервні копії повинні зберігатися в ізольованих просторах або мережах з обмеженим доступом, щоб зменшити ризик несанкціонованого доступу.
3. Перевірка цілісності та доступності: необхідно періодично перевіряти цілісність резервних копій і їх можливість відновлення. Це допомагає уникнути ситуацій, коли копії даних виявляються пошкодженими або недоступними саме у момент відновлення.
4. Автоматизація процесу: використання спеціалізованого програмного забезпечення для автоматизації процесу резервного копіювання допомагає забезпечити регулярність та надійність створення копій.
5. Шифрування і захист доступу: резервні копії повинні бути зашифрованими для забезпечення конфіденційності даних. Також важливо захищати доступ до резервних копій від несанкціонованих осіб.

Останнім і, безперечно, критично важливим етапом в забезпеченні безпеки локальної комп'ютерної мережі є регулярне навчання користувачів (Security Awareness Training). Навіть при наявності передових технологій та заходів безпеки, люди залишаються найсерйознішою слабкістю в системі безпеки, і саме через їхні недоліки у знаннях та поведінці в мережі можуть виникнути серйозні загрози.

Регулярне навчання користувачів є важливим для підвищення їх обізнаності в галузі кібербезпеки та зменшення ризику, пов'язаного з соціальними інженерними атаками, фішингом, слабкими паролями та іншими потенційними загрозами [9].

Це може включати в себе такі аспекти:

1. Зламостійкі паролі: Користувачі повинні бути навчені створювати сильні паролі і регулярно їх оновлювати. Це допомагає уникнути легкого доступу для зловмисників.
2. Правила безпеки в Інтернеті: Користувачам слід навчити визнавати підозрілі веб-сайти, уникати завантаження сумнівного вмісту, та не розголошувати особисту інформацію вільно в мережі.
3. Використання антивірусного програмного забезпечення: Пояснення та навчання користувачів встановлювати та регулярно оновлювати антивірусне програмне забезпечення для захисту від загроз.
4. Реагування на підозрілі ситуації: Користувачі повинні знати, як реагувати на підозрілі листи, повідомлення або події та до кого звертатися у випадку підозри на кіберзлочини.

5. Актуальність та обізнаність: Знання про останні кіберзагрози та обов'язковість дотримання актуальних стандартів безпеки є важливим аспектом.
6. Тестування навичок: Проведення тестів та симуляцій кіберзагроз допомагає перевірити реакцію користувачів та виявити області, де потрібно поліпшити навички.

Пароль, 123456, qwerty – хоча паролі, які зустрічаються в списку найпоширеніших, безперечно, варто припинити використовувати, навіть більш унікальний пароль може бути легко взламаний, якщо комп'ютерна програма взялася систематично його ламати.

Як показано в даних від веб-сайту Security.org, вже одна велика літера у паролі може драматично змінити його потенційну надійність. У випадку восьмизнакового пароля його тепер можна взламати за 22 хвилини, а не миттєво за одну секунду – це збільшення більше 1000 відсотків [9].

Хоча додатковий час у цьому випадку безумовно не дозволяє отримати задовільний пароль, вигоди високого рівня безпеки використання символів, відмінних від малих літер, можна помножити. При використанні хоча б однієї великої літери та однієї цифри восьмизнаковий пароль зараз буде ламатися комп'ютером 1 годину. Додайте інший символ - і це займе вже вісім. Щоб зробити пароль дійсно надійним, можна додати ще символи або більше одну велику літеру, цифру чи символ. Дванадцятизнаковий пароль із однією великою літерою, однією цифрою та одним символом практично непроникний, і комп'ютеру знадобиться 34 000 років, щоб його взламати (рис.1.15).

Рисунок 1.15 – Статистика надійних паролів

Це відбувається тому, що, коли ми використовуємо більше типів символів, потенційні комбінації, які створюють пароль, збільшуються експоненційно. З всього 26 малих літер, пароль з восьми знаків має 26^8, отже, приблизно 209 мільярдів можливих комбінацій. Додавши великі літери, ми вже отримуємо 52^8, приблизно 53,5 трильйона комбінацій. З цифрами у ньому, це 62^8 або 218 трильйонів комбінацій. Символи додають ще великий потенціал для безпеки, але оскільки зручно використовувати лише кілька з них, відображених на клавіатурах комп'ютерів, це знову підвищує кількість комбінацій до приблизно 90^8 або 430 трильйонів комбінацій [9].

Висновки за розділом

У цьому розділі, розглянуті пункти включають в себе ключові аспекти забезпечення інформаційної безпеки для підприємства. Опис видів атак допомагає розуміти загрози, з якими може стикатися організація, та підготовити ефективні заходи для їх запобігання. Міжнародні стандарти інформаційної безпеки визначають норми та практики, які допомагають впроваджувати системи управління інформаційною безпекою.

В результаті проведеного дослідження з питань захисту комп'ютерних мереж та існуючих видів заходів безпеки можна зробити кілька важливих висновків.

Визначено основні характеристики та особливості підприємства, які впливають на вибір методів захисту комп'ютерних мереж. Розглянуті фактори масштабу та структури компанії.

Проаналізовано дотримання підприємством міжнародних стандартів інформаційної безпеки, що є ключовим аспектом у забезпеченні ефективного захисту.

Проведений огляд різноманітних видів атак на комп'ютерні мережі, їхні методи та можливі наслідки для підприємства. Визначено основні вектори загроз та слабкі місця.

Проаналізовано комплексний підхід до захисту локальної комп'ютерної мережі, враховуючи різні аспекти, такі як фізична та програмна безпека, ідентифікація загроз, та автоматизовані засоби контролю.

Здійснено огляд та порівняльний аналіз різних аспектів захисту комп'ютерних мереж, що надає можливість визначити найбільш ефективні та адаптовані підходи для конкретного підприємства.

У результаті дослідження встановлено, що успішний захист комп'ютерних мереж вимагає інтегрованого підходу, який включає фізичні, програмні та організаційні заходи. Важливо надавати пріоритет безпеці даних та мережевим ресурсам для забезпечення стійкості та надійності операцій підприємства.

2 ПОМ’ЯКШЕННЯ ЗАГРОЗ МОДЕРНІЗОВАНОЇ ЛКМ ПІДПРИЄМСТВА ТА КОРЕЛЯЦІЙНИЙ АНАЛІЗ SIEM

2.1 Схеми приміщень та мережі

Топологія комп'ютерної мережі визначає фізичне розташування комп'ютерів у мережі щодо один одного та спосіб їхнього з'єднання лініями зв'язку. Фізична топологія мережі відображає, як саме виглядає ця мережа в реальному світі: розташування кабелів, встановлене обладнання, джерела живлення, підключення кабелів до конкретних портів, розгалуження оптичних з'єднань та розміщення крос-панелей.

Топологія визначає правила та вимоги до устаткування, тип використовуваного кабелю, варіанті можливих й найбільш зручних методів керування надійність роботи, обміном, можливості розширення мережі.

Адміністративна будівля, цех 1 та цех 2, кожна будівля представляє собою одноповерхову споруду, узагальнена схема рисунку 2.1.

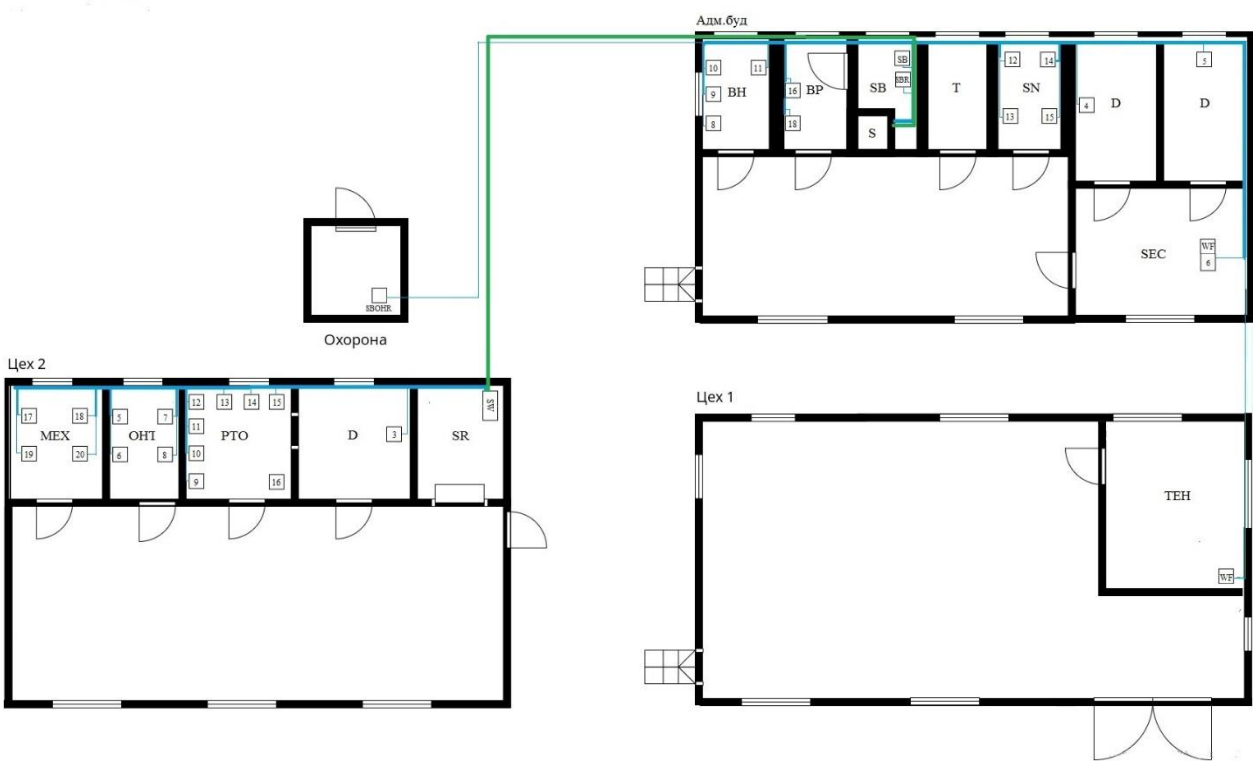


Рисунок 2.1 – Повна топологія будівель

Адміністративна споруда містить у собі 8 кімнат їх план можна побачити на наступному рисунку 2.3.

					КНУ.РМ.123.23.10.02.ПЗМЛПКА		
Змн.	Арк.	№ документа	Підпис	Дата			
Розробив		Микитюк			ПОМ’ЯКШЕННЯ ЗАГРОЗ МОДЕРНІЗОВАНОЇ ЛКМ ПІДПРИЄМСТВА ТА КОРЕЛЯЦІЙНИЙ АНАЛІЗ	Літера	Аркуш / Аркушів
Перевірив		Кумченко					
Н.контроль		Кузнєцов				КІ-22м	
Затвердив		Купін					

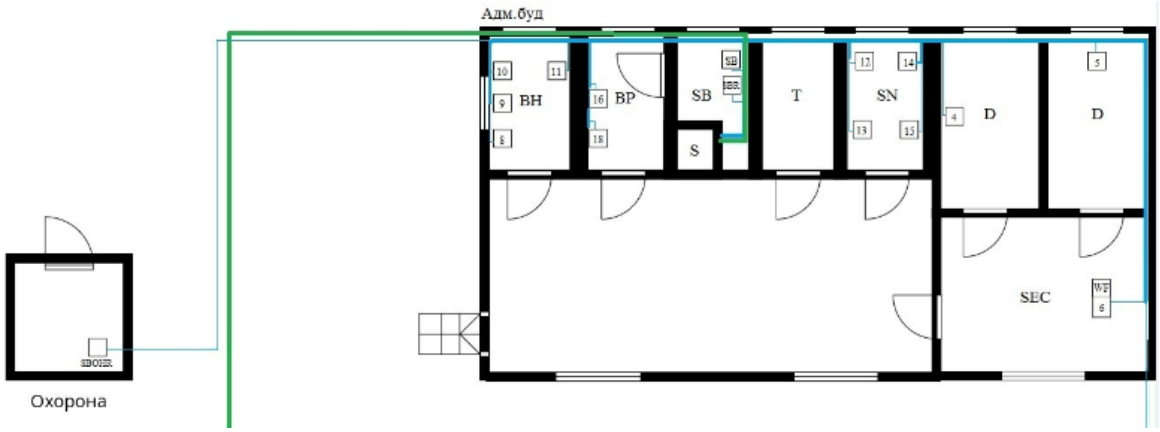


Рисунок 2.3 – Топологія адміністративної споруди

Позначення на рисунку наступні:

1) ВН – відділ бухгалтерії;
2) ВР – бюро пропусків;
3) SB – служба безпеки;
4) T – санітарна кімната;
5) SN – відділ постачання;
6) D – директор;
7) SEC – приймальня/секретар ;
8) S – серверна.

Адміністративна будівля включає 13 робочих станцій зі спеціальним програмним забезпечення, котре призначене для повного, якісного обслуговування локальної мережі, серверну кімнату та 2 сервера біля неї (рис.2.4). Біля адміністративної будівлі розташований охоронний пункт, який під’єднаний до головного серверного приміщення та містить у собі одну робочу станцію. Всі підрозділи повинні обмінюватись електронною інформацією та мати прямий доступ до мережевого обладнання.

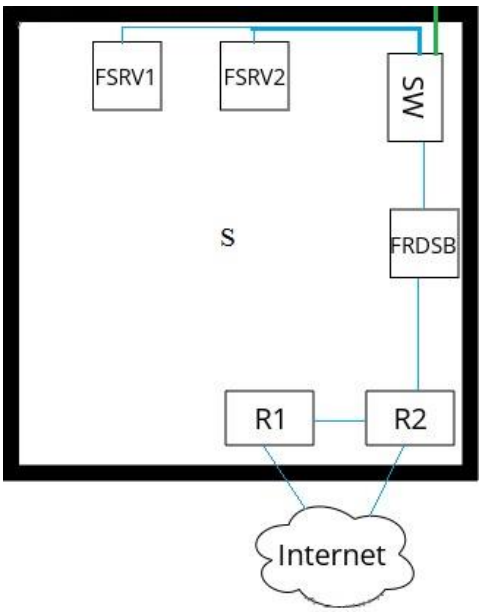


Рисунок 2.4 – Схема серверної

Біля попередніх описаних будівель розташованих цехи – цех 1 та цех 2 (рис.2.5). Цех 1 містить у себе одне службове приміщення ТЕН для роботи технічного персоналу та одну станцію бездротового доступу до мережі Інтернет, увесь інший вільний простір – сегмент для технічного обладнання (наприклад станки). На даному етапі функціонал приміщення планується розширити.

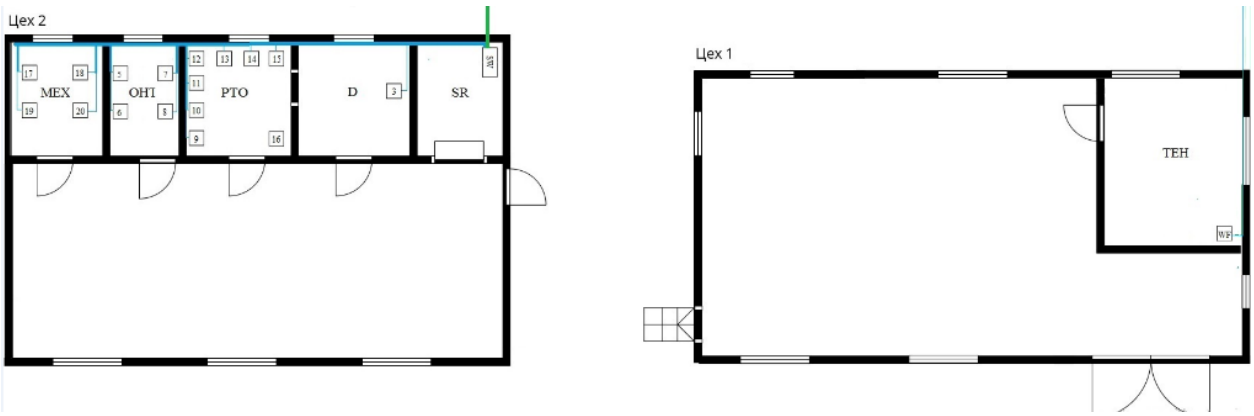


Рисунок 2.5 – Топологія цехів

Будівля цех 2 має 5 кімнат для роботи інформаційного сегмента.
Позначення на рисунку наступні:

1) МЕХ – відділ механіків;
2) ОНТ– відділ охорони;
3) РТО – планово-технічний відділ;
4) D – директор;
5) SR – серверна.

Логічна схема – це діаграма, яка відображає та пояснює різні процеси, що відбуваються у конкретних функціональних ланцюгах пристрою (устаткування) або в самому пристрої (устаткуванні). Узагальнено, функціональна схема мережі представляє собою комбінацію стандартів, топологій і протоколів, необхідних для створення ефективної мережі. На практиці часто використовуються структури, в яких комутатори взаємодіють між собою. Такі розподілені мережі описуються зараз у термінах моделі, яка відображена на рисунку 2.6 разом із відповідними позначеннями..

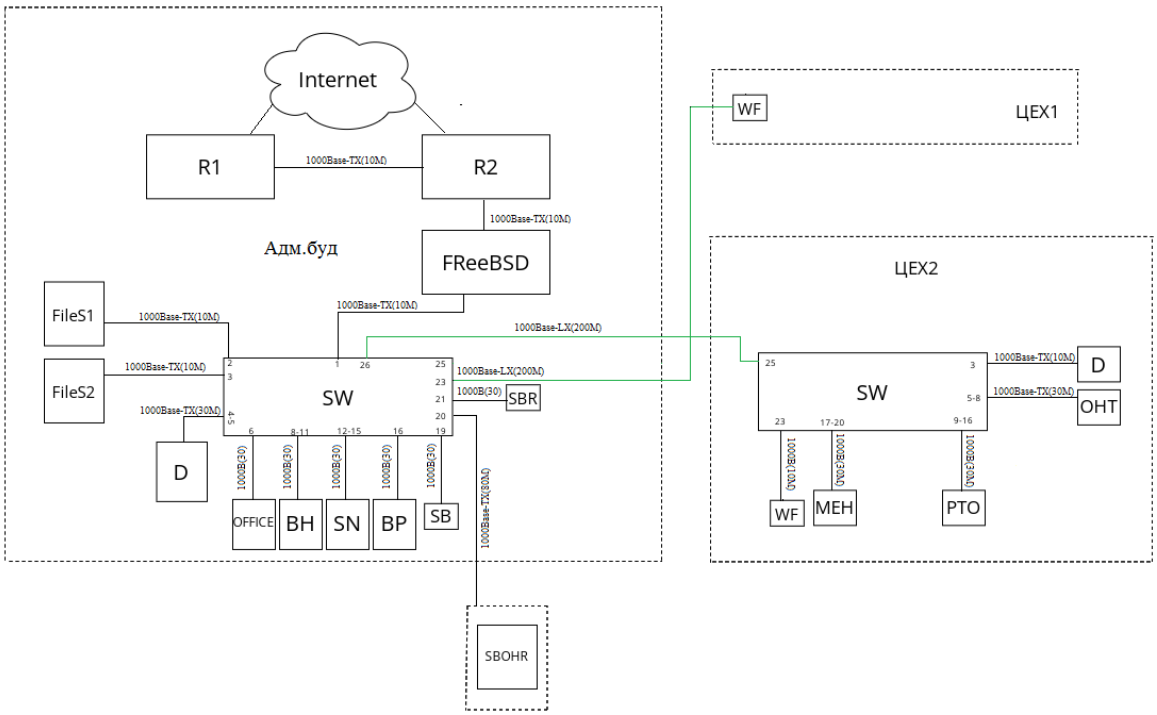


Рисунок 2.6 – Логічна топологія

На попередніх малюнках вже розписали значення ВН, SN, ВР, SB, МЕН, РТО, ОНТ до цих визначень (приміщення/будівля) додається SBOHR – охоронний пункт. Визначення технічного обладнання: R1 та R2 – роутер, FreeBSD – сервер, SW – комутатор, FileS1 та FileS2 – файлові сервери, WF – бездротова точка доступу.

2.2 Модернізована схема локальної мережі

Після проведених етапів модернізації нижче наведено фізичну схему, яка описує основні зміни в системі (рис.2.7).

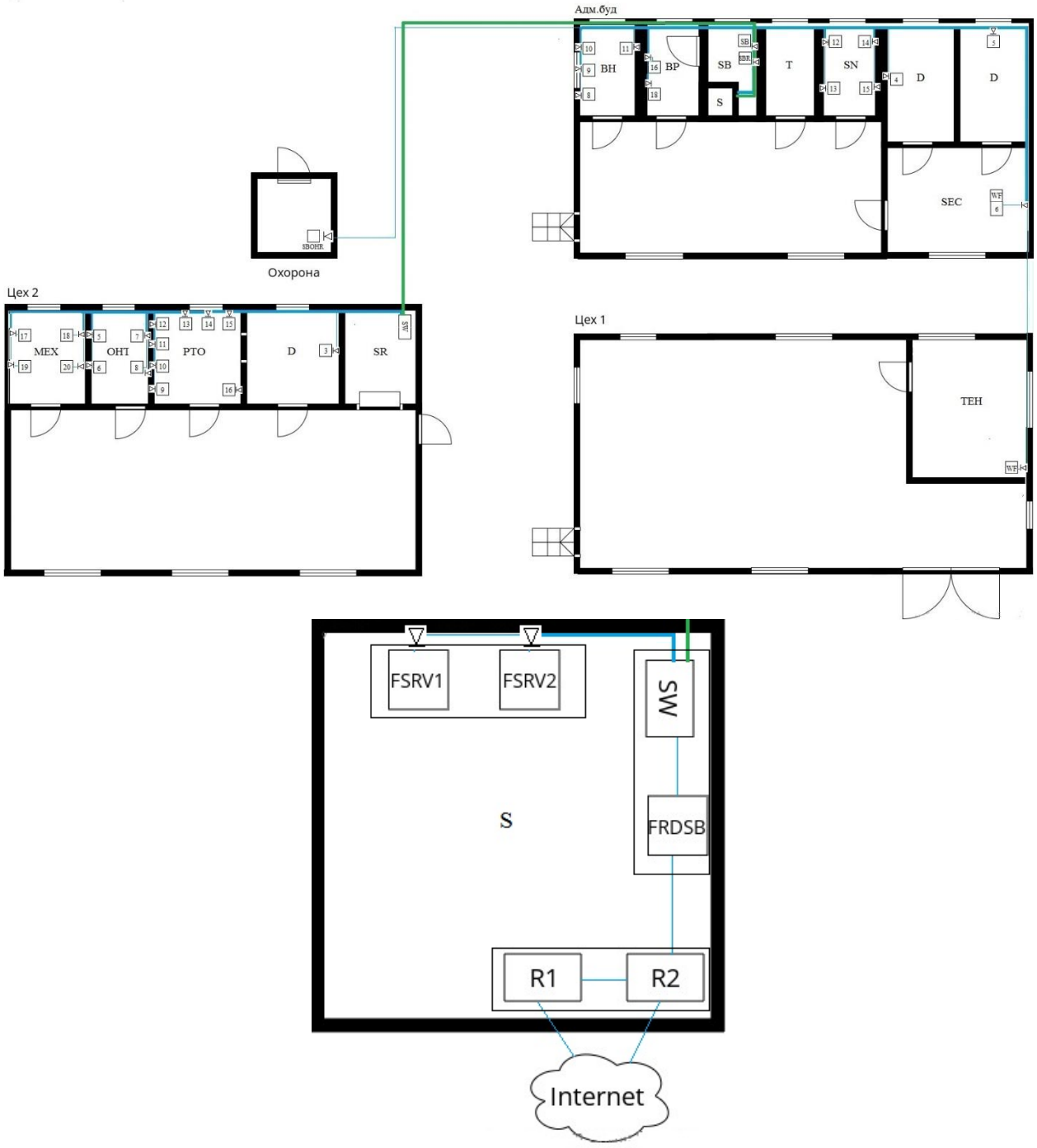


Рисунок 2.7 – Оновлена фізична топологія

2.3 Методи пом’якшення загроз

В умовах стрімкого розвитку технологій та постійної зміни інформаційного середовища, питання безпеки стає найважливішим аспектом функціонування комп'ютерних систем і мереж. Модуль «Mitigating Threats», який розглядає методи пом'якшення загроз, є ключовим компонентом в забезпеченні цілісності, конфіденційності та доступності інформації.

Сучасні загрози інформаційної безпеки стають все більш вдосконаленими, і, відповідно до цього, потрібно розглядати нові та ефективні методи для зменшення впливу потенційних небезпек на комп'ютерні системи та мережі. Даний модуль присвячений вивченню стратегій та інструментів, спрямованих на пом'якшення цих загроз [10].

Забезпечення найвищого рівня безпеки та захист інформації від небезпек - це основні завдання, які вирішуються через вивчення та впровадження передових методів пом'якшення загроз. У цьому контексті вступ спрямований на визначення важливості дослідження та застосування заходів забезпечення безпеки в сучасних інформаційних технологіях.

Чотири етапи запобігання загрозам.

Забезпечення достатнього запобігання загрозам може бути важким завданням. У нашому переліку заходів з мережевої безпеки ми визначаємо п'ять простих кроків для запобігання кіберзагрозам. Нижче ми розглядаємо основні компоненти [11].

1. Захист периметра.

Спочатку слід звернути увагу на перший компонент - периметр. Традиційні брандмауери та антивірусні рішення вже не є достатніми. Проте брандмауери нового покоління (NGFW) інтегрують захист від шкідливих програм (AMP), систему запобігання вторгнень нового покоління (NGIPS), відстеження застосунків та управління доступом (AVC) та фільтрацію URL для забезпечення багаторівневого підходу.

NGFW є ключовим першим кроком для захисту периметра та впровадження інтегрованого рішення.

2. Захист користувачів незалежно від місця роботи.

На сьогоднішній день понад половина працівників є мобільними. Оскільки робочі практики зазнають змін, IT-системи повинні пристосовуватися. Засоби IT-безпеки мають акцентувати увагу на захисті працівників, незалежно від їхнього місця роботи, чи то центральний офіс, філія або будь-яке мобільне робоче місце.

Для більшості відділів IT безпека мобільних пристроїв стала головним викликом. Незважаючи на її складність, вирішення питань безпеки мобільних пристроїв є важливим, оскільки компанії продовжують збільшувати кількість таких пристроїв. Технології, такі як віртуальні приватні мережі (VPN) та системи перевірки користувача та довіри пристрою, можуть негайно покращити безпеку мобільних пристроїв.

3. Розумна сегментація мережі.

Сегментація, визначена програмним забезпеченням, розділяє вашу мережу, щоб загрози можна було легко ізолювати. Зі зростанням бізнес-застосунків та користувачів важко визначити взаємозалежності. Для достатнього запобігання загрозам компаніям необхідно мати високотехнологічні аналітику та видимість в мережі для визначення всіх взаємозалежностей.

Надто розділені мережі можуть уповільнити роботу. Недостатня сегментація може дозволити поширення атак. Компанії повинні бути розумними та ефективними при сегментації.

4. Швидке виявлення та управління проблемами.

Порушення безпеки стануться. Важливим елементом запобігання загрозам є виявлення та усунення проблем. Це вимагає обширної видимості та контролю. Це також потребує готового до цього IT-персоналу. Щоб допомогти у підготовці, ми часто рекомендуємо компаніям розробляти план відповіді на інциденти та тестувати поточні мережеві рішення за допомогою тестування на проникнення.

Типи рішень щодо запобігання та виявлення загроз.

NGFW (Next-Generation Firewall)

Як зазначено вище, NGFW є ключовим першим кроком до запобігання загрозам. Традиційні брандмауери просто надають чи відмовляють в доступі. Хоча це здається інтуїтивно зрозумілим, ефективність його залежить від точності політик та обмежень, які були програмно встановлені. Наприклад, якщо загроза нова і невідома, IT, ймовірно, ще не встановило політики для відмови їй в доступі (рис.2.8) [11].

NGFW, однак, інтегрується з додатковим програмним забезпеченням, таким як NGIPS та AMP. Якщо невідома загроза ухиляється від автоматично застосованих політик, ці додаткові рішення надають засоби виявлення та усунення для захисту вашої мережі. З усіма цими додатковими інструментами NGFW забезпечує покращену видимість, автоматизацію та контроль над вашою мережею.

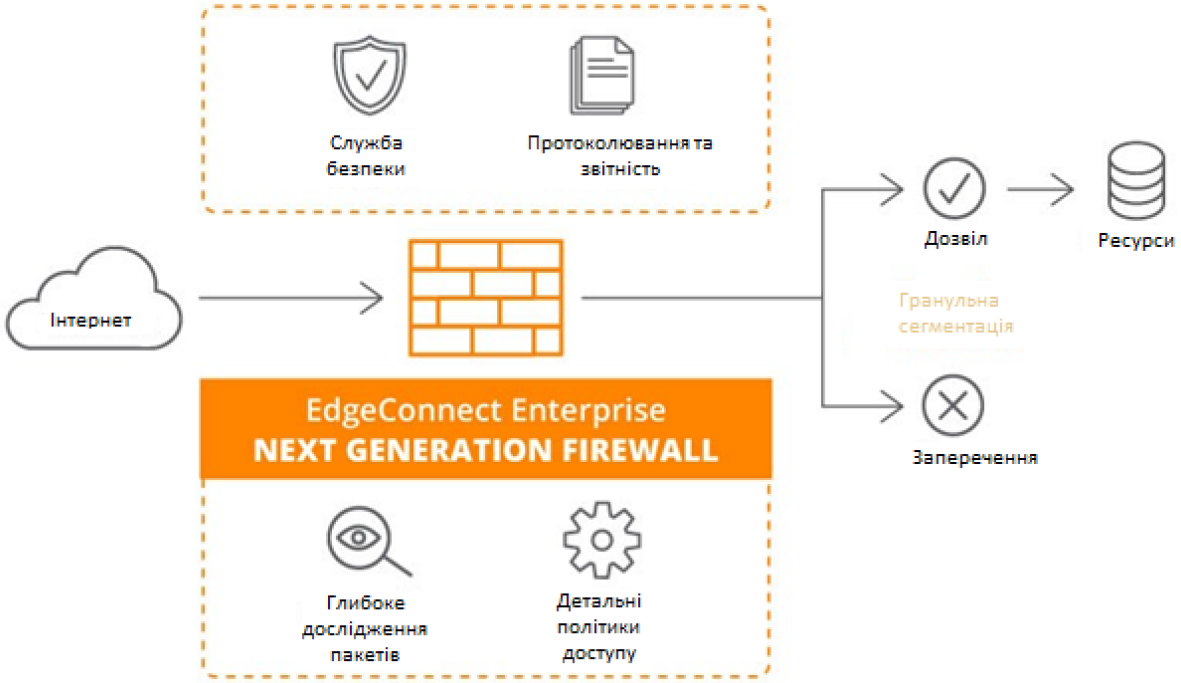


Рисунок 2.8 – Схема роботи NGF

NGIPS (Next-Generation Intrusion Prevention System)

NGIPS надає високоефективний захист від загроз у виявленні вторгнень, внутрішньому сегментації мережі, громадському хмарному середовищі, а також управлінні вразливостями та патчами.

Виявлення вторгнень вимагає технології, що відповідає швидкому розвитку загроз. NGIPS надає стійкий захист та уявлення про користувачів, застосунки, пристрої та вразливості в вашій мережі. З проведенням інспекції файлів та інтегрованим пісочницям NGIPS може швидко виявляти загрози. Якщо загроза ухиляється від захисту, NGIPS надає ретроспективний аналіз для видалення та усунення загроз пізно в їхньому життєвому циклі.

Внутрішня сегментація мережі дозволяє організаціям надавати послідовний механізм забезпечення, що охоплює вимоги кількох внутрішніх організацій. Сегментація може враховувати різні вимоги мережі та різні робочі завдання з легкістю.

NGIPS надає послідовний захист ефективності, що застосовується як у громадських, так і приватних хмарах. Ваш NGIPS повинен підтримувати кілька гіпервізорів, включаючи Azure, AWS і VMWare. Ці застосунки є незалежними від віртуальних перемикачів під ними. NGIPS дозволяє виконання політики забезпечення на мережі на пристроях на місці, в інфраструктурі громадської хмари та загальних гіпервізорах, проводячи глибоку інспекцію пакетів між контейнеризованими середовищами [11].

З управлінням вразливостями та патчами ви маєте можливість бути більш вибірковими на основі висновків з NGIPS. Часто процес або середовище тестування організації може затримати патчення вразливостей високого пріоритету. Здійснюйте ці зміни протягом коротшого періоду часу з меншими ресурсами. Ніколи не доводиться відкатувати патч; зміни налаштувань IPS набагато простіше.

AMP (Advanced Malware Protection).

Продвинута захист від шкідливих програм є ключовим компонентом наступного покоління рішень. Шкідливі програми продовжують еволюціонувати і адаптуватися. З цього приводу шкідливі програми можуть бути надзвичайно важко виявити на периметрі мережі. Комбінування NGFW з AMP та розвідкою загроз дозволяє мережам виявляти значно більше раніше невідомих загроз шкідливих программ (рис.2.9).

Хоча розвідка загроз може виявляти більше загроз, ваша мережа все одно стикається з новими, раніше невідомими шкідливими програмами. Деякі з цих шкідливих програм можуть мати таймери та інші хитрі атрибути, які маскують зловмисну поведінку до того, як вона потрапить в мережу. Однак існують рішення AMP, які постійно аналізують файли протягом їхнього життєвого циклу. Це критично. З цими можливостями AMP негайно визначатиме шкідливі програми, які починають виявляти зловмисну поведінку у подальшому [11].

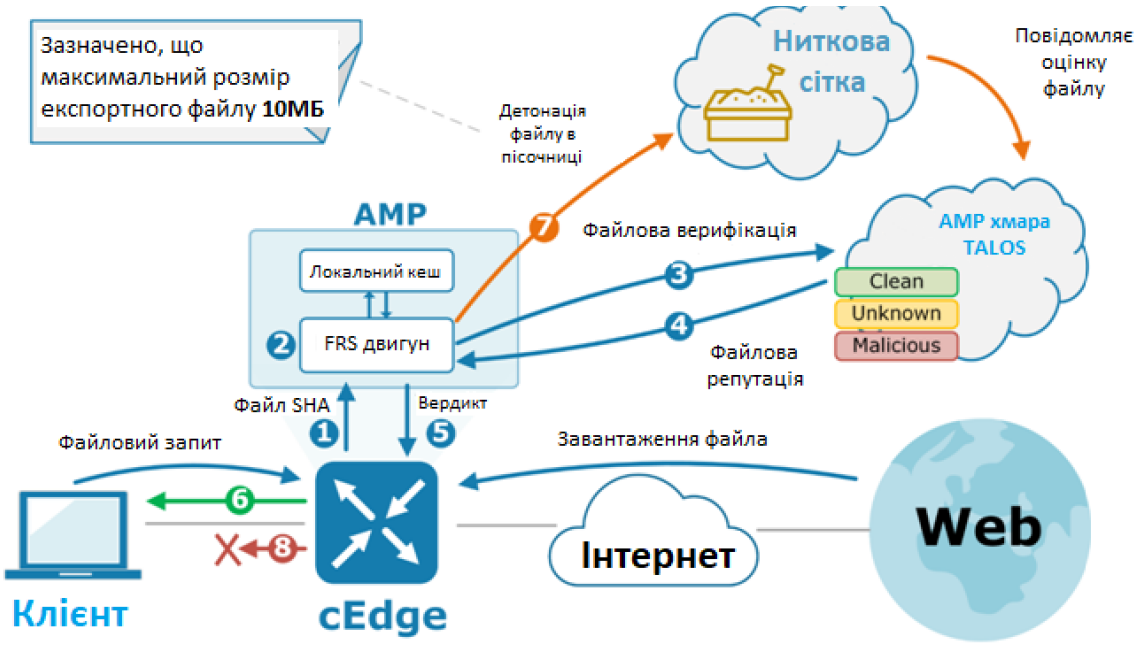


Рисунок 2.9 – Схема роботи AMP

AVC (Application Visibility and Control).

Підприємства використовують більше додатків, ніж будь-коли раніше. З технологією видимості та контролю додатків (AVC) організації можуть створити справжню мережу, освідомлену про додатки. Глибокий інспекційний пакет (DPI) може класифікувати додатки, а разом зі статистичною класифікацією, кешуванням сокетів, виявленням служб, автоматичним вивченням та DNS-AS, AVC може надавати видимість та контроль для мережевих додатків (рис.2.10).

З покращеною видимістю організації можуть швидше вирішувати проблеми з погрозами. Іноді додатки можуть бути джерелом вразливостей мережі. Якщо організація не може повністю бачити всі свої додатки, вона не може їх захищати. Аналітика та моніторинг додатків дають миттєве уявлення про продуктивність додатків. Погана продуктивність може бути ознакою для перевірки загроз [11].

Рисунок 2.10 – Схема роботи AVC

Threat intelligence.

Рівень загроз, наданий розвідкою загроз, підвищує ефективність усіх цих рішень. Загроза світового класу перетворює ці технології з хороших на великі. Захист мережі та видимість збільшують можливість організації протистояти загрозам. Однак все це передбачає, що організація може визначити, чи є файл зловмисним чи безпечним [11]. Це малоймовірно. Більшість загроз не відомі мережі (рис.2.11).

Загрозова розвідка може сповістити вашу мережу, якщо невідома загроза була визнана зловмисною десь на іншому кінці світу. Раптово значна кількість невідомих загроз стає повністю відомою та зрозумілою завдяки загрозовій розвідці.

Рисунок 2.11 – Схема роботи Threat intelligence

User verification and device trust.

Контроль доступу до мережі є обов'язковим для безпеки. За допомогою рішень з перевірки користувача та довіри до пристроїв, мережі можуть встановлювати довіру до користувацьких ідентифікаторів та пристроїв та накладати політику доступу до додатків. Двофакторна аутентифікація може перевіряти доступ користувача безпосередньо перед доступом до корпоративної інформації та ресурсів [11]. Крім перевірки користувача, рішення довіри до пристроїв можуть інспектувати пристрої під час доступу для визначення їхнього стану безпеки та надійності (рис.2.12).

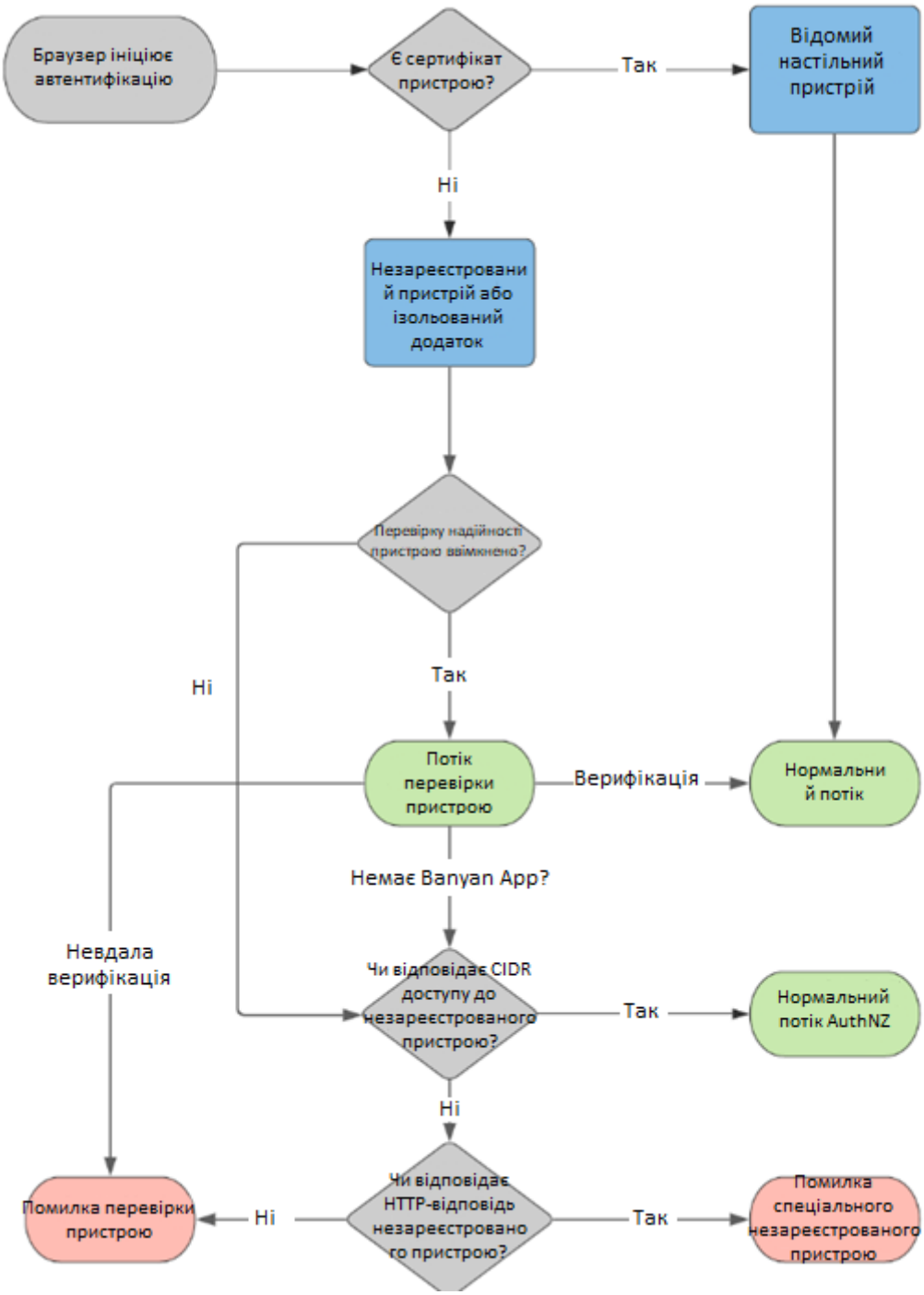


Рисунок 2.12 – Блок-схема User verification and device trust

2.4 Кореляційний аналіз Security Information and Event Management (SIEM)

Кожен випадок неполадок в комп'ютерній мережі може призвести до серйозних наслідків не тільки для працівників підприємства та мережевих адміністраторів, але і для самого підприємства. Особливо це стосується розвитку електронних платежів та “безпаперового” документообігу. Якщо локальна мережа зазнає серйозних неполадок, то це може призвести до паралізації роботи всього підприємства та значних фінансових втрат.

Тому захист даних в комп'ютерних мережах стає однією з найбільш актуальних проблем

Для забезпечення безпеки інформації у комп'ютерних мережах необхідно створювати перешкоди для будь-яких несанкціонованих спроб розкрадання або модифікації переданих даних. Важливо зберігати властивості інформації, такі як:

1. Доступність;
2. Цілісність;
3. Конфіденційність.

Доступність, цілісність та конфіденційність - це три основних складові інформаційної безпеки, які є необхідними для забезпечення захисту інформації в організації.

Доступність означає, що інформація повинна бути доступна для тих, хто має на це право в потрібний час і місце. Це означає, що система повинна бути стійкою до атак та відмов, щоб забезпечити доступність інформації для користувачів [12].

Цілісність – це захист інформації від несанкціонованих змін. Інформація повинна бути захищена від випадкових або зловмисних змін, щоб зберігати цілісність даних.

Конфіденційність - це захист інформації від несанкціонованого доступу. Інформація повинна бути доступна тільки тим, хто має на це право. Це означає, що необхідно забезпечити безпеку доступу до даних, наприклад, за допомогою аутентифікації та авторизації.

Для забезпечення безпеки інформації в організації використовуються різні методи та технології, призначені для забезпечення високого рівня захисту для кожної компоненти інформаційної безпеки. Наприклад, для гарантування доступності використовуються технології, такі як резервне копіювання даних та мережеві пристрої, які забезпечують резервне копіювання та відновлення мережі у випадку відмови. Для забезпечення цілісності можуть використовуватися методи, такі як цифровий підпис та захист від вірусів. Крім того, залежно від конкретних потреб і вимог, можуть бути використані інші додаткові принципи захисту, такі як аутентифікація, авторизація, невідмовність тощо.

Для гарантованого захисту інформації в комп'ютерних системах обробки даних необхідно спочатку визначити мету захисту інформації і визначити перелік необхідних заходів для її захисту. Це можливо здійснити шляхом систематизації можливих факторів (загроз), які можуть призвести до втрати або спотворення вихідної інформації.

Під загрозою безпеки комп'ютерної системи розуміється подія або вплив, які, якщо стануть фактом, можуть призвести до порушення цілісності, втрати або зміни інформації. Загрози можуть мати випадковий або навмисний характер (рис.2.13).

Серед можливих випадкових загроз можна виділити:

1. Випадкові помилки персоналу та користувачів;
2. Втрата даних через некоректне зберігання архівних даних;

3. Неочікуване знищення або зміна даних;
4. Випадкові збої обладнання та живлення;
5. Випадкові збої в кабельних системах;
6. Неочікувані перебої в електроживленні;
7. Випадкові збої дискових систем;
8. Випадкові збої систем архівування даних;
9. Випадкові збої роботи серверів, робочих станцій, мережевих карт тощо;
10. Некоректна робота програмного забезпечення;
11. Зміна даних у разі помилок у програмному забезпеченні;
12. Зараження системи комп'ютерними вірусами;
13. Несанкціонований доступ до даних;
14. Неочікуване ознайомлення з конфіденційною інформацією сторонніх осіб.

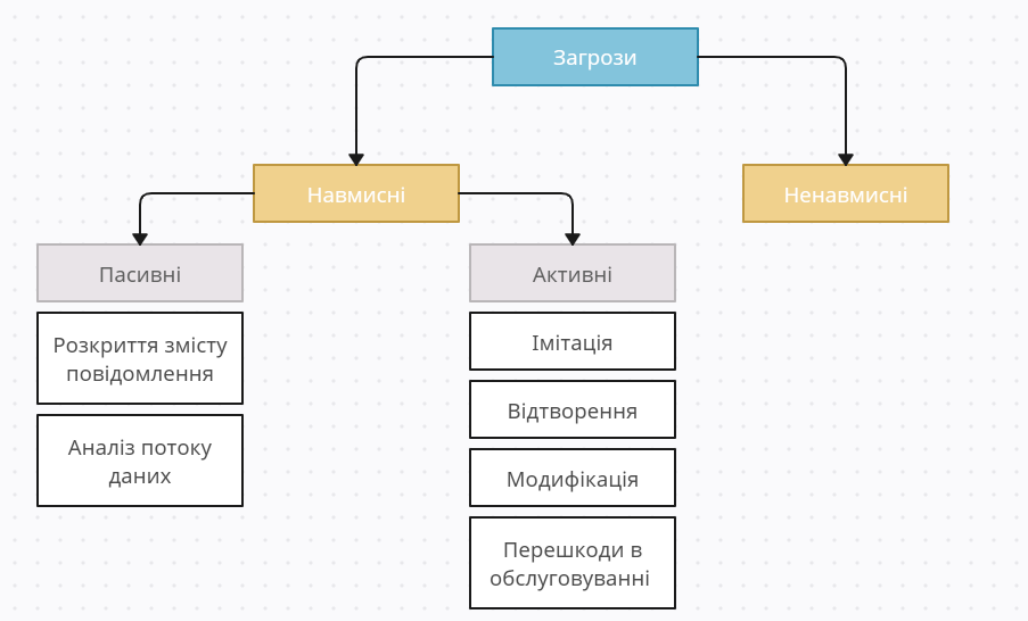


Рисунок 2.13 – Види загроз

Відповідно до досліджень, проведених AlienVault , більшість підприємств стурбовані загрозами хмарної безпеки, 55% підприємств стурбовані фішингом, а 45% - вимогами.

Нижче наведено рисунок 2.14, який покаже вам деталі дослідження, проведеного AlienVault [12].

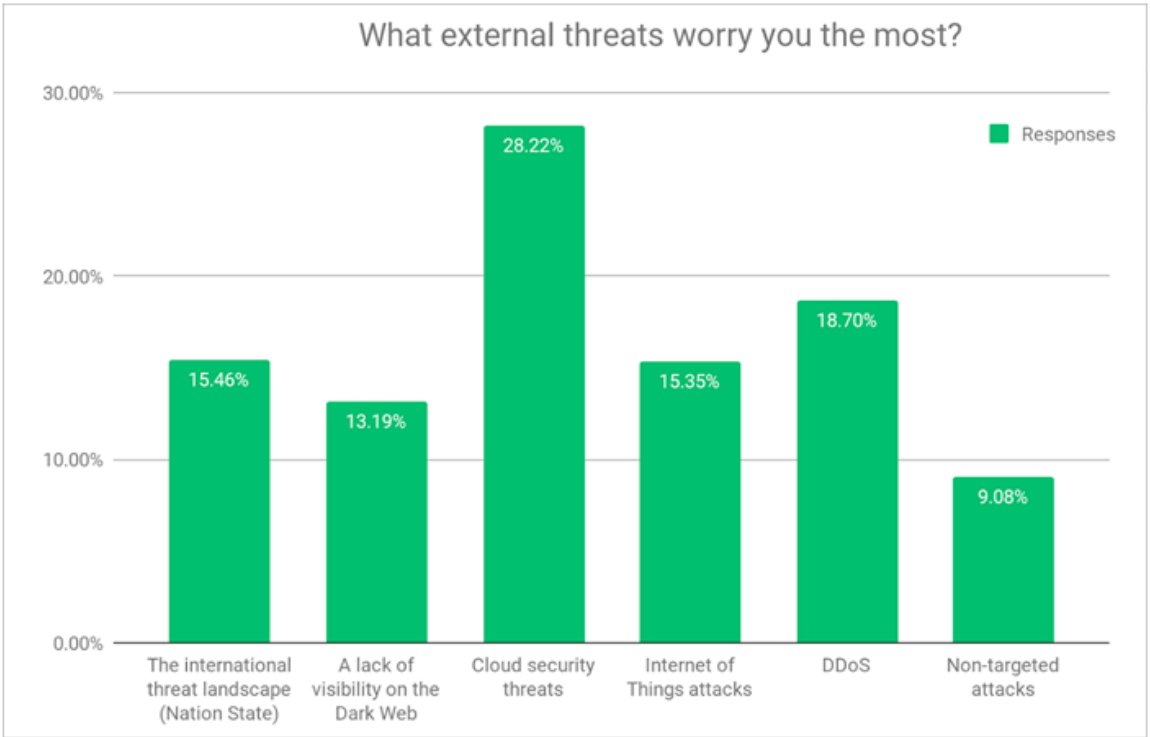


Рисунок 2.14 – Дослідження AlienVault

Середнє кількість кіберзагроз, з якими можуть зіткнутися підприємства, такі як заводи, може значно варіюватися в залежності від різноманітних факторів, таких як розмір підприємства, вид діяльності, географічне розташування, рівень захисту, використовувані технології та багато інших.

Загальноприйнятою думкою серед експертів у галузі кібербезпеки є те, що кількість кіберзагроз та кібератак на підприємствах зростає. Зловмисники постійно розвивають нові методи атак та використовують вразливості у системах безпеки для здійснення атак на корпоративні мережі та інформаційні системи.

Зважаючи на це, багато підприємств приділяють значну увагу кібербезпеці та вживають заходів для захисту своїх систем від кіберзагроз. Проте, в середньому підприємства можуть бути піддані сотням атак щодня, включаючи фішинг, рансомвар, віруси, атаки на слабкі місця в мережах, DDoS-атаки та багато інших видів кіберзагроз [12].

Кількість осіб, які потрапляють на фішингові атаки, може варіюватися в залежності від різних факторів, таких як розповсюдженість фішингу у певному регіоні, тип атаки, рівень кібербезпеки та знання користувачів.

За даними різних досліджень та статистики, кількість осіб, які потрапляють на фішингові атаки, залишається високою. Наприклад, згідно «Annual State of Phish Report» 2021 року компанії KnowBe4, середній рівень успішності фішингових атак складає більше 25% від відправлених фішингових листів. Інші дослідження також підтверджують високий рівень успішності фішингу.

SIEM (Security Information and Event Management) – це система безпеки, яка збирає, аналізує та керує інформацією про події у комп'ютерній мережі, включаючи події, пов'язані з порушеннями безпеки (рис.2.15).

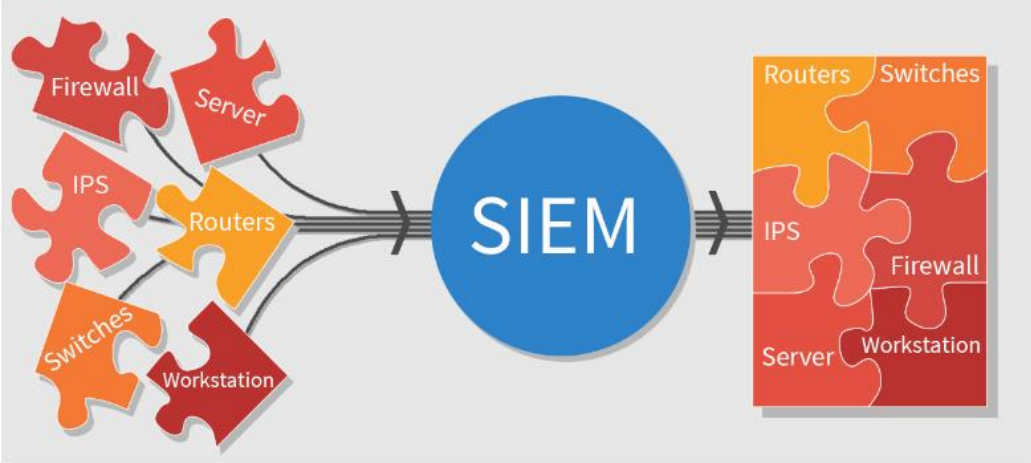


Рисунок 2.15 – Система безпеки SIEM

Принцип роботи SIEM системи складається з кількох етапів:

Збір даних: SIEM система збирає дані з різних джерел у комп'ютерній мережі, включаючи журнали подій (event logs), системи моніторингу безпеки, пристрої захисту периметра, програми тощо.

Агрегація та нормалізація даних: Система агрегує дані з різних джерел та нормалізує їх відповідно до загальної схеми ідентифікації подій.

Аналіз даних: Система проводить аналіз подій та виявляє підозрілі активності, які можуть вказувати на порушення безпеки. Аналіз може включати порівняння подій з зумовленими шаблонами, виявлення аномальних патернів, аналіз поведінки користувача тощо.

Повідомлення та реагування: Після виявлення підозрілих активностей система генерує повідомлення про події та сповіщає адміністраторів безпеки. Адміністратори можуть вживати заходів щодо реагування на інциденти, включаючи блокування пристроїв, керування доступом тощо.

Зберігання даних: Система зберігає дані про події для подальшого аналізу та використання з метою покращення безпеки [12].

Основною метою SIEM системи є підвищення рівня безпеки комп'ютерної мережі шляхом раннього виявлення та швидкого реагування на потенційні загрози безпеці.

Частим способом, яким організації обмежують ефективність свого SIEM-рішення, є неподання йому даних з усіх відповідних джерел. Щоб вирішити цю потребу, справжнім першим кроком є дізнання про ваше середовище. Це включає створення інвентарю ваших активів та розуміння ваших систем для ідентифікації того, що саме ви намагаєтеся логувати. Після того, як ви провели свою докладну роботу, настав час звертатися до питання покриття.

SIEM призначений для агрегації даних з кількох різних джерел та використання отриманого контексту для надання розумних сповіщень аналітику.

Якщо SIEM налаштований лише для обробки даних від брандмауера організації або лише від критичних систем, він може пропустити небезпечні події через відсутність повної видимості навколишнього середовища. Кожен хост у середовищі має кілька потенційних джерел корисних даних (логи брандмауера, логи застосунків тощо), і SIEM може (і повинен) мати доступ до всіх цих джерел.

У ідеальному світі досягнення повного покриття та видимості можливе. Однак у всесвіті, в якому більшість з нас живе, існують обмеження бюджету та ресурсів. В цьому сценарії наступною найкращою відповіддю є розроблення стратегічного плану присвоєння рівнів критичності вашим активам, щоб ви знали, яким надавати пріоритет для ідентифікації відповідних джерел даних, які слід вносити в SIEM першими.

1.Огляд існуючих SIEM програм з відкритим кодом.

Графіки кореляційного аналізу у SIEM можуть бути використані для візуалізації зв'язків між різними типами даних та подій у системі. Ось кілька прикладів графіків, які можуть бути використані у кореляційному аналізі у SIEM:

Графік матриці кореляції – це графік, який відображає кореляційні коефіцієнти між різними типами даних. Кореляційний коефіцієнт показує, наскільки сильним є зв'язок між двома змінними. Матриця кореляції може допомогти ідентифікувати найсильніші зв'язки між різними типами даних у системі.

1. Графік розподілу подій – це графік, який показує розподіл різних типів подій у системі. Він може допомогти ідентифікувати найпоширеніші події і допомогти визначити, які типи подій є найбільш критичними для безпеки системи.
2. Графік часових рядів – це графік, який показує зміну різних типів даних протягом часу. Він може допомогти ідентифікувати тимчасові тренди та аномалії, які можуть свідчити про загрози безпеці.
3. Графік дерева рішень - це графік, який відображає ієрархію різних типів даних та подій у системі. Він може допомогти ідентифікувати основні категорії подій та допомогти визначити, які типи подій найбільше критично впливають на безпеку системи.

Графіки кореляційного аналізу можуть допомогти аналітикам безпеки краще зрозуміти зв'язки між різними типами даних у системі та визначити найбільш критичні вразливості та загрози для безпеки.

У сучасну епоху на ринку існує багато підприємств і рішень SIEM з відкритим кодом. Деякі з них наведені нижче [12]:

Alienvault USM – це рішення SIEM, призначене для організацій малого та середнього бізнесу. Він має всі основні функції рішення SIEM і може бути розгорнутий як апаратне, віртуальне або хмарне обладнання. Він має вбудовані 150 шаблонів звітів і надає канали від спільноти OSSIM.

Управління подіями безпеки може здійснювати моніторинг загроз, кореляцію подій та реагування на інциденти, аналізуючи дані журналу та

подій у реальному часі. Управління інформацією про безпеку здійснює збір, аналіз та звітування про дані журналу [12].

Rapid7 провела опитування щодо виявлення інцидентів та реагування на них, і більше 50% людей відповіли, що використовують SIEM (рис.2.16).

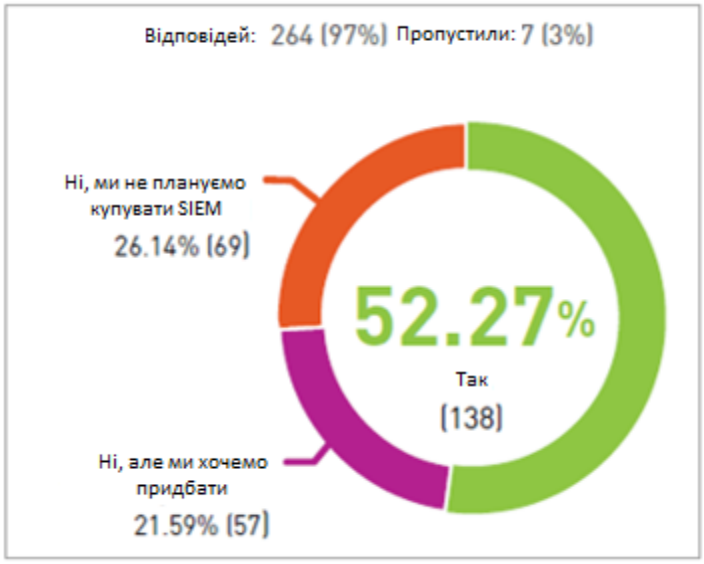


Рисунок 2.16 – Результати опитування Rapid7

ArcSight ESM збирає та обробляє журнали з джерел даних і більше підходить для великих організацій. ArcSight ESM інтегрується зі сторонніми джерелами аналізу загроз, щоб надавати актуальні канали (рис.2.17).

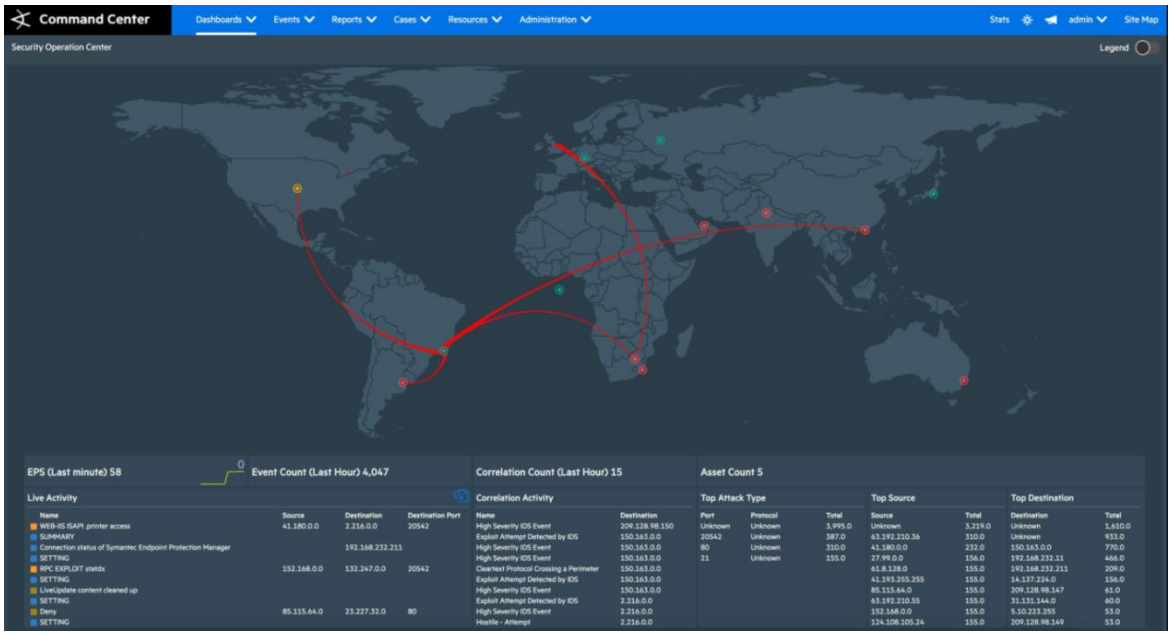


Рисунок 2.17 – Інтерфейс програми ArcSight ESM

IBM QRadar також отримує журнали з широкого діапазону джерел даних, таких як мережеві пристрої, операційні системи та програми.

Він також аналізує журнали в реальному часі та дозволяє аналітикам безпеки швидко виявляти загрози безпеці [13].

QRadar підтримує аналіз загроз, а також отримує журнали з джерел даних, розгорнутих у хмарі(рис.2.18).

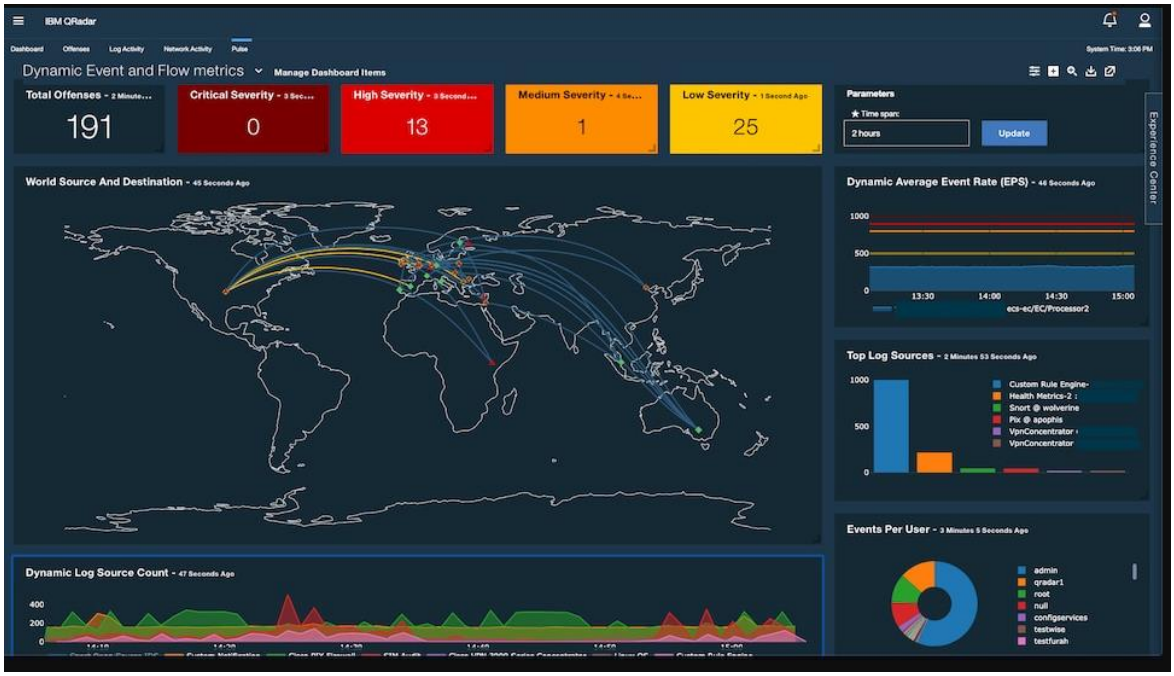


Рисунок 2.18 – Інтерфейс програми IBM QRadar

LogRhyThm також є хорошим рішенням SIEM для організацій малого бізнесу. Він також включає моніторинг кінцевих точок, цифрову криміналістику та аналітику безпеки для команд безпеки [13]. Якщо джерело даних відключено від Logrhythm, він також має функцію серцебиття для визначення підключених і відключених джерел даних (рис.2.19).

Рисунок 2.19 – Інтерфейс програми LogRhyThm

Кібератаки можуть приймати різні форми, такі як використання шкідливих програм, викрадення даних, атаки шляхом фішингу чи розподіленого відмову в обслуговуванні (DDoS), серед інших. Ці атаки можуть призвести до порушень безпеки комп'ютерних систем, мереж, або індивідуальних пристроїв і можуть викликати витоки даних, фінансові втрати, погіршення репутації та перебої в обслуговуванні.

Програма управління інформаційною безпекою та подіями (SIEM) збирає дані з журналів безпеки, які генеруються різними джерелами, такими як хост-системи та пристрої безпеки, наприклад, брандмауери та антивіруси. Наступним етапом є обробка цих журналів для їх перетворення в стандартний формат [14].

Наступним кроком є проведення аналізу для виявлення та категоризації інцидентів та подій. Отже, попередження генеруються, якщо виявляється проблема безпеки. Інструмент може також надавати звіти, що стосуються інцидентів та подій у сфері безпеки.

Кореляційний аналіз – це статистичний метод, використовуваний вивчення зв'язку між двома чи більше змінними. Цей метод дозволяє визначити, наскільки сильно пов'язані між собою дві чи більше змінні (рис.2.20).

Рисунок 2.20 – Компоненти кореляційного аналізу на прикладі SIEM

Кореляція може бути позитивною, якщо значення двох змінних змінюються в одному напрямку, і негативною, якщо значення двох змінних змінюються у різних напрямках. Коефіцієнт кореляції може приймати значення від -1 до 1 де -1 означає повну негативну кореляцію, 0 - відсутність кореляції, а 1 - повну позитивну кореляцію.

Кореляційний аналіз може бути використаний для різних цілей, таких як:

1) оцінка ступеня взаємозв'язку між змінними;

2) вивчення напряму та сили зв'язку між змінними;
3) перевіряє гіпотезу про наявність кореляції між змінними;
4) визначення, які змінні є найбільш значущими для пояснення змін до інших змінних.

Кореляційний аналіз широко використовують у різних галузях, включаючи науку, економіку, маркетинг, соціологію тощо. Він дозволяє дослідникам виявити зв'язки між різними змінними та надає важливу інформацію для прийняття рішень у різних сферах діяльності [15].

Види кореляційного аналізу

1. Пірсона кореляційний аналіз - це метод вивчення лінійного зв'язку між двома змінними. Він використовується, коли змінні мають нормальний розподіл.
2. Спірменова рангова кореляція – це метод, що вивчає зв'язок між змінними, які мають ранговий характер. Використовується, коли досліджувані змінні не мають нормального розподілу або коли дані отримані в результаті рангових оцінок.
3. Кендаллова кореляційна міра – це метод, який вивчає зв'язок між змінними, які мають ранговий характер. Він також використовується, коли досліджувані змінні не мають нормального розподілу.
4. Частковий кореляційний аналіз - це метод, який дозволяє вивчити зв'язок між двома змінними, з урахуванням впливу інших змінних. Використовується, коли досліджувані змінні взаємодіють з іншими змінними.
5. Кореляційний аналіз коефіцієнта детермінації - це метод, який дозволяє встановити, наскільки змінна Y залежить від змінної X. Він використовується для прогнозування значень Y на основі знань про значення X.

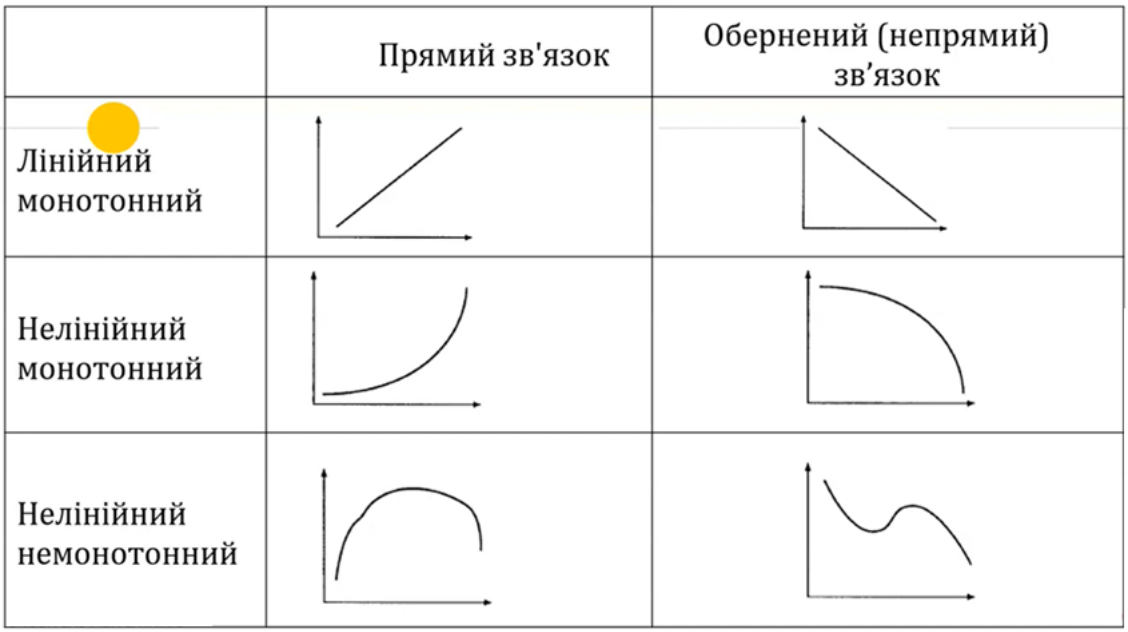


Рисунок 2.32 – Методи кореляційного аналізу

Прямий кореляційний аналіз (Pearson correlation analysis) – це статистичний метод, що використовується для визначення сили та напряму зв'язку між двома неперервними змінними. Пряма кореляція означає, що зі збільшенням значення однієї змінної збільшується значення іншої змінної, а зі зменшенням значення однієї змінної зменшується значення іншої змінної.

Наприклад, якщо вивчається зв'язок між висотою людини та її вагою, то прямий кореляційний аналіз допоможе визначити, чи існує статистично значущий зв'язок між цими двома змінними та якою є його сила.

Непрямий кореляційний аналіз (Spearman correlation analysis) – це статистичний метод, що використовується для визначення зв'язку між двома ранговими змінними. Рангова змінна – це змінна, яка не має числового значення, але може бути відсортована за певною ознакою, наприклад, за розміром або часом (рис.2.21).

Наприклад, якщо вивчається зв'язок між рейтингом та продажами продукту, то непрямий кореляційний аналіз допоможе визначити, чи існує статистично значущий зв'язок між цими двома змінними на основі рангування даних.

Основна різниця між прямим та непрямим кореляційним аналізом полягає в тому, що перший використовується для аналізу двох неперервних змінних, а другий – для аналізу двох рангових змінних.

Кореляційний аналіз є важливим інструментом для аналізу даних у Security Information and Event Management (SIEM). SIEM є системою, яка збирає, аналізує та відслідковує інформацію про події в інформаційній системі або мережі.

Кореляційний аналіз може бути використаний у SIEM для виявлення та відслідковування злочинних дій та кібератак. Кореляція полягає в тому, щоб знайти зв'язок між різними подіями, які можуть бути пов'язані з кіберзлочинністю [15].

Наприклад, якщо зловмисник намагається зламати систему, він може спробувати ввести неправильний пароль для входу. Це може бути зафіксовано системою SIEM. Якщо система SIEM знає, що зловмисник повторно намагається увійти до системи з різних IP-адрес, це може вказувати на те, що зловмисник використовує ботнет для атаки. Кореляційний аналіз може автоматично виявити ці зв'язки та повідомити про них відповідним особам.

На наступних графіках кореляції показано приклади різних діапазонів значень коефіцієнта кореляції (рис.2.22).

Коефіцієнт кореляції можна розрахувати, спочатку визначивши коваріацію заданих змінних. Потім це значення ділиться на добуток стандартних відхилень для цих змінних. Рівняння, наведене нижче, узагальнює наведену вище концепцію (формула 2.1).

$$\rho_{xp} = \frac{Cov(x,p)}{\sigma_x \sigma_p}, \qquad (2.1)$$

де: ρ_{xp} = коефіцієнт кореляції продукт-момент Пірсона;
Cov(x,p) = коваріація змінних;
$p\sigma_x$ = стандартне відхилення від $x\sigma_p$=стандартне відхилення від p.

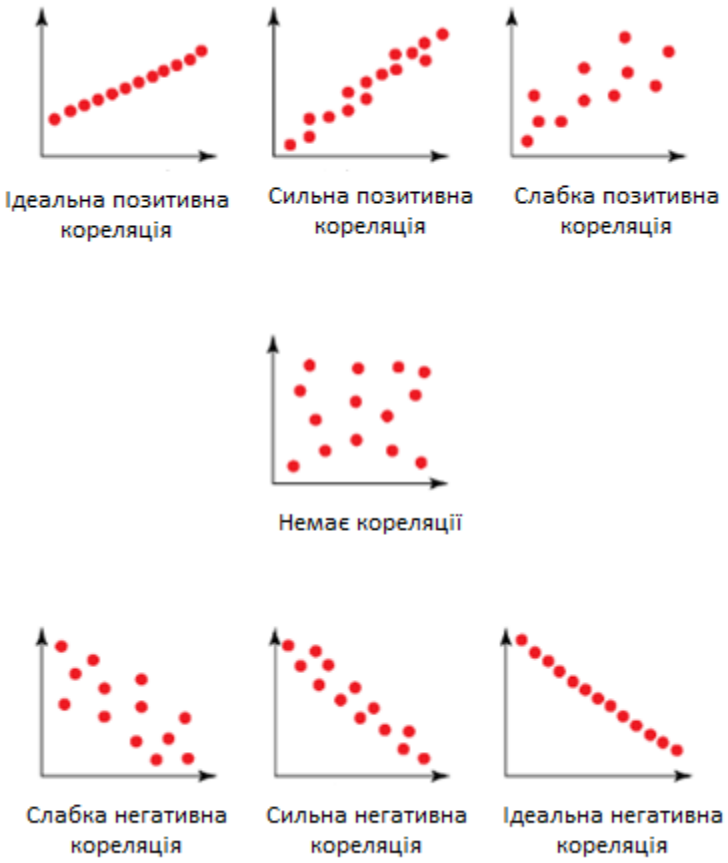


Рисунок 2.22 – Діапазон значень коефіцієнта кореляції

Дослідження: Вплив аудиту та проведення навчання на Користувацьку Безпеку Інтернету.

У проведеному опитуванні було опитано 300 респондентів з питань їхньої поведінки в Інтернеті щодо відвідування підозрілих або неперевірених веб-сайтів, а також відкриття невідомих листів. Результати були аналізовані до і після проведення навчання з питань кібербезпеки [15].

Детальна інформація про результати опитування щодо відвідування підозрілих або неперевірених веб-сайтів та відкриття невідомих листів:

У рамках дослідження було проведено опитування серед 300 респондентів з різних вікових груп та різних соціальних груп на питання про їхню поведінку в Інтернеті. Головними питаннями були: «Чи відвідуєте ви підозрілі або неперевірені веб-сайти?» та «Чи відкриваєте ви невідомі листи?».

До проведення навчання з питанням щодо відкриття невідомих листів, 30% респондентів відповіли, що вони цього роблять, тоді як 22% стверджували, що не відкривають невідомі листи та решта 48% відкриває час від часу (рис.2.23).

Чи відкриваєте Ви невідомі листи?

Вік	Так	Ні	Іноді
18-24	8	10	7
25-30	18	2	20
30-35	10	12	15
35-40	13	10	15
40-45	15	15	17
45-50	15	8	15
50+	11	9	10

Кількість респондентів
300

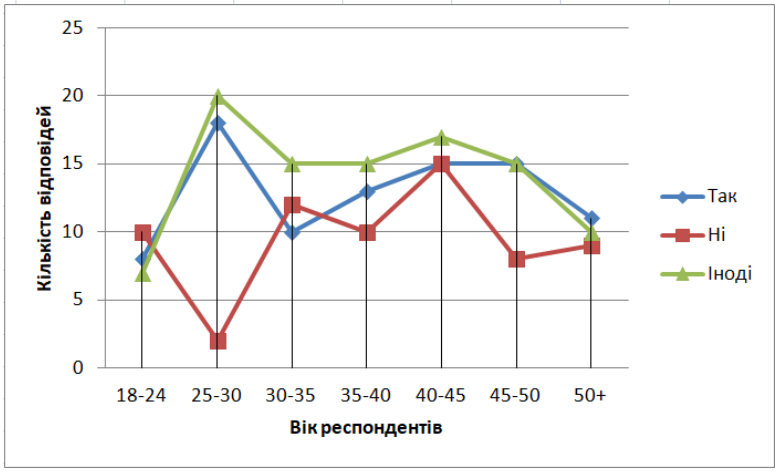


Рисунок 2.23 – Таблиці та графіки до проведення навчання

Однак, після проведення навчання з питань кібербезпеки, було відзначено позитивний зсув в поведінці респондентів. Що стосується відкриття невідомих листів, зменшилась кількість респондентів, які відкривають невідомі листи з цікавості (з 30% до 15.6%), тоді як збільшилась кількість тих, хто відмовився від такої практики (з 22% до 52.6%). Лише 31.8% респондентів продовжують відкривати невідомі листи час від часу(рис.2.24).

Після проведення навчання

Вік	Так	Ні	Іноді
18-24	3	18	4
25-30	9	21	10
30-35	2	27	8
35-40	9	23	6
40-45	11	26	10
45-50	8	23	7
50+	5	20	5

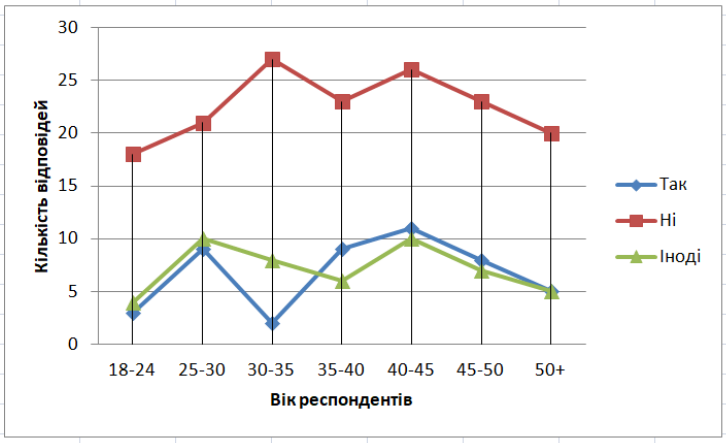


Рисунок 2.24 – Таблиці та графіки після проведення навчання

Також результати та дані щодо другого питання до проведення навчання з питань кібербезпек : 46% респондентів відповіли, що вони відвідують підозрілі або неперевірені веб-сайти, тоді як 44% відповіли, що цього не роблять та решта 10% відкриває час від часу (рис.2.25).

Чи відвідуєте підозрілі або неперевірені сайти?

Вік	Так	Ні	Іноді
18-24	13	16	1
25-30	28	20	10
30-35	24	23	6
35-40	11	20	3
40-45	21	21	8
45-50	15	18	2
50+	26	14	0

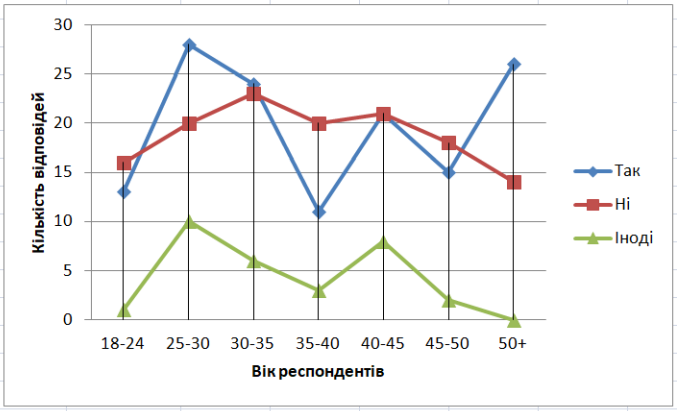


Рисунок 2.25 – Таблиці та графіки до проведення навчання

При аналізі відповідей на питання про відвідування підозрілих або неперевірених веб-сайтів після навчання, було відмічено, що основні причини, які вказували респонденти на відвідування таких сайтів, змінилися. Перед навчанням, більшість респондентів (46%) відвідували такі сайти з цікавості, тоді як після навчання цей показник зменшився до 18.6%. Зокрема, 77.6% респондентів заявили, що не відвідують підозрілі або неперевірені веб-сайти взагалі, а 3.73% вказали, що роблять це дуже рідко(рис.2.26).

Після проведення навчання

Вік	Так	Ні	Іноді
18-24	5	24	1
25-30	10	43	5
30-35	9	41	3
35-40	6	27	1
40-45	10	36	4
45-50	10	28	2
50+	6	34	0

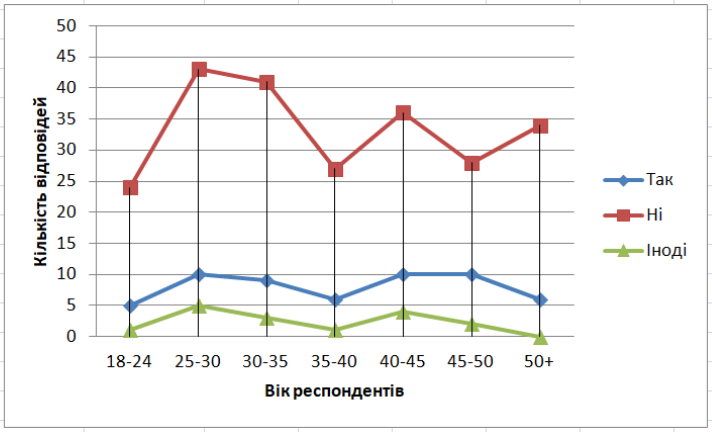


Рисунок 2.26 – Таблиці та графіки після проведення навчання

Ці результати свідчать про позитивний вплив проведення навчання на кібербезпеку на поведінку користувачів Інтернету. Зменшення кількості відвідування підозрілих або неперевірених веб-сайтів та відкриття невідомих листів свідчить про більш обережний підхід респондентів до кібербезпеки. Це може бути наслідком збільшеної освідомленості про потенційні загрози в Інтернеті та засоби їх запобігання, які були надані в ході навчання.

2.2 Обчислення коефіцієнтів Пірсона та Спірмена.

2.2.1 Коефіцієнт Пірсона

Коефіцієнт Пірсона, також відомий як коефіцієнт кореляції Пірсона, є одним з найпоширеніших методів вимірювання лінійного взаємозв'язку між двома змінними. Він використовується для визначення ступеня статистичної залежності між двома наборами даних, які мають лінійну взаємодію.

Коефіцієнт Пірсона розраховується шляхом вимірювання ступеня лінійної залежності між двома змінними на основі їх середніх значень та стандартних відхилень[9].

Розглянемо прямолінійну кореляцію, яка відображається коефіцієнтом кореляції. Для відображення прямолінійного кореляційного зв'язку, двох ознак x_j і y_j, які виражені в абсолютних одиницях, використовують парний коефіцієнт кореляції Браве-Пірсона, який визначається наступною формулою 2.2 :

$$r_{xy} = \frac{\sum_1^n (x_j - x)(y_j - \bar{y})}{\sqrt{\sum_1^n (x_j - \bar{x})^2 \sum_1^n (y_j - \bar{y})^2}} \qquad (2.2)$$

де: r_{xy} – коефіцієнт кореляції між ознаками *x* та *y*;

x_j та y_j – значення величин *x* та *y*;

x , y – середнє арифметичне значення *x* та *y*;

n – об'єм сукупності.

Властивість коефіцієнта кореляції в тому, що його значення не перевищує одиниці. Якщо прийняти до уваги абсолютне значення r_{xy}, тобто, без врахування знака, його можливі значення можуть бути заключні в інтервалі $0<|r_{xy}|<1$. Цей інтервал дозволяє досліднику орієнтуватись за тіснотою взаємозв'язку: чим ближчий розрахунковий коефіцієнт до одиниці, тим тісніше взаємозв'язок між ознаками; чим ближче до нуля – тим менший взяємозв'язок.

На практиці фізичної культури і спорту умовно прийняті наступні інтервали:

$0 < | r_{xy} | <0,3$ – слабкий зв'язок;

$0,3 < | r_{xy}| < 0,7$ – середній зв'язок;

$0, 7 < | r_{xy}| < 1,0$ – тісний зв'язок.

Крім того, при розрахунку взаємозв'язку і оцінки показників спортсменів високої кваліфікації, тісна кореляція може дорівнювати 0,85 і вище. За знаком коефіцієнту кореляції визначається, позитивний чи негативний взаємозв'язок.

Для вивчення кіберзагроз була створена таблиця з трьома стовпцями, в яких відображалися кількість кіберзагроз, відповідна кількість вдалих цих загроз за один місяц та відповідні періодичність виникнення цих загроз (1 період) (рис.2.27).

Період	Кількість кіберзагроз	Кількість вдалих
1 період	112	74
	234	73
	278	139
	312	145
	345	123
	365	73
	407	81
	445	89
	487	73
	542	54
	588	58
	623	62

Рисунок 2.27 – Таблиця кількості кіберзагроз

Після цього, використовуючи отримані дані, був побудований графік (рис.2.28), що відображав кількість кіберзагроз у залежності від періоду часу (1 місяц) та кількості вдалих кібератак. Графік дав можливість візуально оцінити динаміку зміни кількості кіберзагроз та вдалих протягом розглянутого періоду.

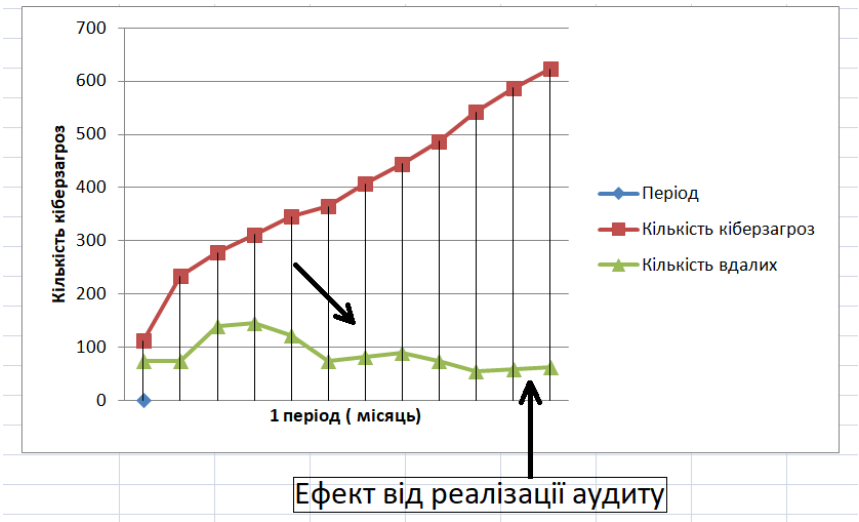


Рисунок 2.28 – Графік кількості кіберзагроз та вдалих кібератак

Далі, з використанням MS Excel було обчислено значення коефіцієнта Пірса для оцінки статистичної залежності між кількістю кіберзагроз та відповідним періодом їх виникнення. Результатом обчислення було отримання значення коефіцієнта кореляції -0.457146675.

Від'ємне значення коефіцієнта кореляції (-0.457146675) свідчить про наявність негативної кореляційної залежності між кількістю кіберзагроз та відповідним вдалими кібератаками. Це означає, що зі збільшенням кібератак, кількість вдалих схильна до зниження.

2.2.2 Коефіцієнт Спірмена

Коефіцієнт Спірмена, також відомий як ранговий коефіцієнт кореляції Спірмена, є одним з методів вимірювання статистичної взаємозв'язку між

двома ранговими величинами. Він використовується для визначення ступеня монотонності взаємодії між двома наборами даних, які можуть бути нелинійно залежні.

Коефіцієнт Спірмена розраховується шляхом порівняння рангів відповідних даних у двох вибірках. Він може приймати значення від -1 до 1, де значення -1 вказує на повну зворотну монотонність, 1 – на повну пряму монотонність, а 0 – на відсутність монотонної залежності (формула 2.3) [15].

$$r_s = 1 - \frac{6\sum d^2}{n\left(n^2 - 1\right)} \tag{2.3}$$

де: n – Число спостережень;

rxi – ранг i-ого значення випадкової величини x, що спостерігається;

ryi – ранг i-ого значення випадкової величини y, що спостерігається;

di – різниця рангів i-их значень випадкових величин x і y, що спостерігаються;

ρxy – коефіцієнт рангової кореляції Спірмена – статистика з асимптотично нормальним розподілом N(0;1/(n-1)).

Коефіцієнт Спірмена є корисним інструментом в аналізі даних, зокрема в випадках, коли дані мають рангову або порядкову шкалу вимірювання, або коли взаємодія між змінними може бути нелінійною. Він також може бути використаний для порівняння взаємозв'язку між різними змінними та виявлення взаємодій, які можуть бути складними для виявлення за допомогою інших методів кореляційного аналізу.

Була створена таблиця з результатами опитування: Чи відвідуєте підозрілі або неперевірені сайти з двома стовпцями, в яких відображалися дані “Так” та “Ні” відповідно “до” та “після”. Для кожного рядка таблиці було визначено ранг, який відображав позицію кожного значення в порядку зростання та побудовано графік(рис.2.29). Наприклад, якщо в таблиці було значення “Так” у двох рядках, то кожному з цих значень був присвоєний ранг 1, оскільки вони мають однакове значення.

Так	Ні	Rank_Yes	Rank_No
13	16	6	13
28	20	1	10
24	23	3	8
11	20	7	10
21	21	4	9
15	18	5	12
26	14	2	14
5	24	14	7
10	43	8	1
9	41	11	2
6	27	12	6
10	36	8	3
10	28	8	5
6	34	12	4

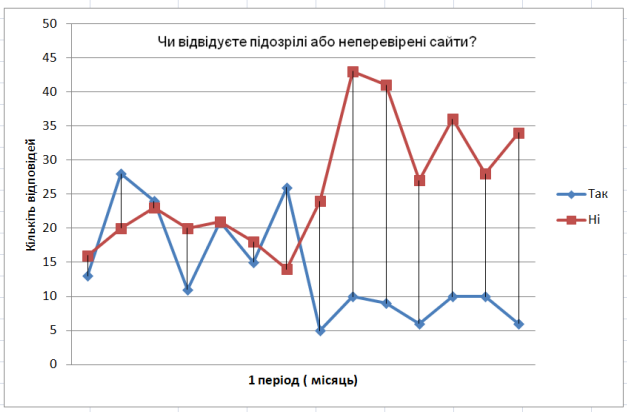


Рисунок 2.29 – Графік та таблиця опитування

Далі, використовуючи MS Excel, було обчислено значення коефіцієнта Спірмена для оцінки рангової кореляції між даними “Так” та “Ні”(рис.2.30). Результатом обчислення було отримання значення коефіцієнта кореляції -0.615874072.

Так	Ні	Rank_Yes	Rank_No
13	16	= РАНГ(D103,D103:D116,0)	= РАНГ(E103,E103:E116,0)
28	20	= РАНГ(D104,D103:D116,0)	= РАНГ(E104,E103:E116,0)
24	23	= РАНГ(D105,D103:D116,0)	= РАНГ(E105,E103:E116,0)
11	20	= РАНГ(D106,D103:D116,0)	= РАНГ(E106,E103:E116,0)
21	21	= РАНГ(D107,D103:D116,0)	= РАНГ(E107,E103:E116,0)
15	18	= РАНГ(D108,D103:D116,0)	= РАНГ(E108,E103:E116,0)
26	14	= РАНГ(D109,D103:D116,0)	= РАНГ(E109,E103:E116,0)
5	24	= РАНГ(D110,D103:D116,0)	= РАНГ(E110,E103:E116,0)
10	43	= РАНГ(D111,D103:D116,0)	= РАНГ(E111,E103:E116,0)
9	41	= РАНГ(D112,D103:D116,0)	= РАНГ(E112,E103:E116,0)
6	27	= РАНГ(D113,D103:D116,0)	= РАНГ(E113,E103:E116,0)
10	36	= РАНГ(D114,D103:D116,0)	= РАНГ(E114,E103:E116,0)
10	28	= РАНГ(D115,D103:D116,0)	= РАНГ(E115,E103:E116,0)
6	34	= РАНГ(D116,D103:D116,0)	= РАНГ(E116,E103:E116,0)
		=КОРРЕЛ(F103:F116,G103:G116)	

Рисунок 2.30 – Знаходження кореляції Спірмена

Від'ємнє значення коефіцієнта Спірмена (-0.615874072) свідчить про наявність від'ємної рангової кореляції між даними «Так» та «Ні». Це означає, що зі збільшенням значень «Так», значення «Ні» схильні до зменшення, та навпаки. Значення коефіцієнта кореляції -0.615874072 показує, що ця взаємозв'язок між даними є помірним, але від'ємним.

Висновки за розділом

Ретельно розглянули структуру приміщень та локальної мережі підприємства, що вказує на важливість адекватної організації просторового розташування технічного обладнання та вивчення архітектурних особливостей мережі.

У оновленій схемі локальної мережі розглянуто покращення в структурі локальної мережі, що визначає напрямки розвитку і покращення забезпечення безпеки та ефективності обміну даними на підприємстві.

Відповідно до «Методів пом’якшення загроз», розглянуті практичні заходи щодо підвищення рівня кібербезпеки, що вказує на високий ступінь відповідальності захисту інформації та ресурсів підприємства.

Кореляційний аналіз SIEM зосередив увагу на важливості використання системи SIEM для виявлення та аналізу інцидентів безпеки, що створює можливість оперативного реагування на потенційні загрози.

Загальний висновок з цих розділів вказує на важливість інтеграції сучасних технологій та систем безпеки для забезпечення стійкості підприємства до кіберзагроз та покращення його загальної ефективності.

3 МОДЕЛЮВАННЯ, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ БЕЗПЕКИ МОДЕРНІЗОВАНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Побудова комп'ютерної мережі в Packet Tracer

У даному розділі буде проводитись моделювання на прикладі окремих сегментів мережі (підключення, створення та базове налаштування VLAN, точки доступу, серверів) компанії ТОВ «МетТрансСервіс» в середовищі Cisco Packet Tracer. Причиною цього є те, що даний продукт містить у собі обмежені інструменти для налаштування та створення мережі у тому вигляді, яка вона є, також основною причиною цього є використання компанією обладнання Mikrotic та FreeBSD сервера, яке відсутнє у Packet Tracer, а заміна цього обладнання на інше, наприклад Cisco, повністю змінить логічну та фізичну топологію комп'ютерної мережі (рис.3.1).

Для створення/моделювання, візуалізації, розробки, експерименту локальної мережі обрано середовище Cisco Packet Tracer.

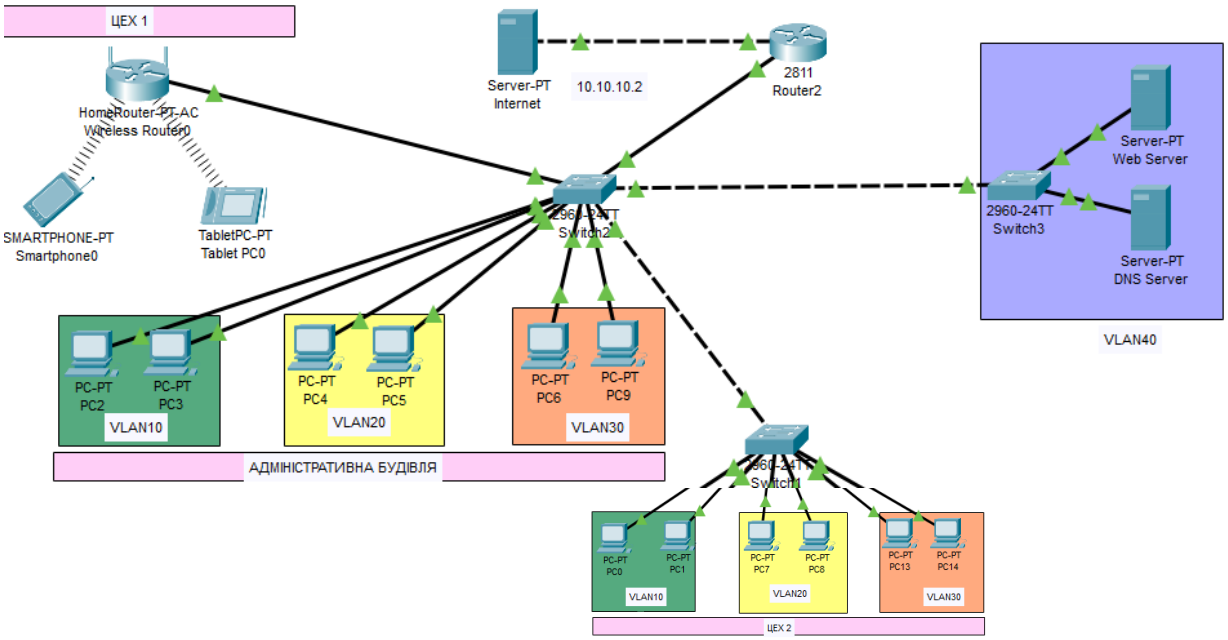


Рисунок 3.1– Мережева схема підприємства

Для ідентифікації пристрою в Інтернеті або для зв'язку комп'ютерів чи пристроїв у локальній мережі, що побудовані з використанням протоколу TCP/IP використовується IP-адреса.

Для ефективного та зручного використання єдиного адресного простору Internet введено класи мереж (табл.3.1).

Таблиця 3.1 – Клас мереж

Клас мережі	Початкова адреса пулу	Кінцева адреса пулу	Кількість мереж	Кількість вузлів у мережі
A	1.0.0.0	126.255.255.255	126	16 777 214
Зарезервовані	127.0.0.0	127.255.255.255	-	-
B	128.0.0.0	191.255.255.255	16 384	65 534
C	192.0.0.0	223.255.255.255	2 097 152	254
D	224.0.0.0	239.255.255.255	-	-
E	240.0.0.0	254.255.255.255	-	-

Адреси класу D використовують для процесу звернення до груп комп'ютерів. Мережі класу E (240–255) зарезервовані для майбутнього користування [16].

Для зменшення трафіку в мережах з великою кількістю пристроїв використовується розділення вузлів на підмережі потрібного розміру. У структурі IP-адрес визначаються адреси мережі, підмережі та приватні IP-адреси. Для побудови адреси підмережі використовуються старші біти хост-частини IP-адреси, а решта молодші біти встановлюються як нульові. Деякі комбінації зарезервовані для broadcast повідомлень та службових цілей.

Була розроблена схема IP-адресації мережі, де використовується блок класу A (10.0.0.0) з маскою підмережі 255.255.255.0. Зазначено, що в локальній мережі використовується динамічне розподілення адрес з часом оренди.

Оскільки на підприємстві працює багато користувачів з різних сфер праці, іноді віддалено, буде використано VLAN для взаємодії кінцевих пристроїв з певними правилами, незалежно від їх фізичного розташування.Перелік переваг навіщо поділяти мережу на VLAN:

- побудова мережі у якої логічна структура не залежить від фізичної. На канальному рівні мережева топологія будується незалежно від фізичного розташування складових компонентів мережі;
- можливість розбиття одного широкомовного домену на кілька широкомовних доменів. Таким чином, широкомовний трафік одного домену не проходить до іншого домену і навпаки. У результаті цього зменшується навантаження на мережеве обладнання;
- Безпека мережі від несанкціонованого доступу. На канальному рівні кадри з інших віланів будуть відкидатись портом комутатора незалежно від того, з якою вихідною IP-адресою інкапсульований пакет у цей кадр;
- можливість застосування різних наборів правил на групу пристроїв, які знаходяться в одному вілані;

– можливість використання віртуальних інтерфейсів для маршрутизації [16].

Таким чином, у даній локальній мережі було виділено 6 VLANів разом з IP адресою, які будуть визначені далі. Таблиці були створені на основі конфігурацій та налаштувань, які створив та підтримує працездатність системний адміністратор (табл.3.2).

Таблиця 3.1 – Розподіл IP-адресів

№ VLAN	Назва відділу	IP-адреса	Маска мережі
VLAN 110	Перший цех	10.50.110.0- 10.50.110.255/24	255.255.255.0
VLAN 120	Другий цех	10.50.120.0- 10.50.120.255/24	255.255.255.0
VLAN 130	Бухгалтерія	10.50.130.0- 10.50.130.255/24	255.255.255.0
VLAN 210	Директори	10.50.210.0- 10.50.210.255/24	255.255.255.0
VLAN 220	Сумісний	10.50.220.0- 10.50.220.255/24	255.255.255.0
VLAN 230	Служба безпеки	10.50.230.0- 10.50.230.255/24	255.255.255.0

Адреси серверів мають наступний вигляд (табл.3.3):

Таблиця 3.3 – IP-адресація серверів

№ Серверу	IP-адреса	Маска мережі
FileServer1	10.150.3.100/24	255.255.255.0
FileServer2	10.150.3.150/24	255.255.255.0
FreeBSD	10.150.3.1/24	255.255.255.0

Створення VLAN у Packet Tracer. Для створення VLAN потрібно зайти в CLI на комутаторі та виконати покроково наступні команди, перед цим перейти у режим конфігурації (рис 3.2).

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vl
Switch(config)#vlan 50
Switch(config-vlan)#nam
Switch(config-vlan)#name V50
Switch(config-vlan)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.2 – Створення VLAN

Для кожного відділу створюється власний VLAN, що призводить до налаштування портів на комутаторі для кожного підключеного пристрою в

залежності від того, до якого VLAN він відноситься. Основне конфігурування включає у себе встановлення порту у режим access та вказівку, до якого VLAN належить даний інтерфейс (рис.3.3).

```
Switch(config)#interface f0/4
Switch(config-if)#sw
Switch(config-if)#switchport m
Switch(config-if)#switchport mode av
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport ac
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
```

Рисунок 3.3 – Створення VLAN

За допомогою «show vlan», можна контролювати та бачити зміни створених або видалених віртуальних мереж (рис.3.4).

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
10   V10                               active    Fa0/4, Fa0/5
20   V20                               active    Fa0/6, Fa0/7
30   V30                               active    Fa0/8, Fa0/9
40   server                            active
50   internet                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.4 – Таблиця VLAN

Для забезпечення доступу до мережі та її ресурсів кожен пристрій у мережі повинен мати унікальну IP-адресу на основі TCP/IP одноадресної розсилки. При переміщенні нових комп'ютерів або пристроїв з однієї підмережі в іншу без використання DHCP, необхідно вручну налаштувати їх IP-адреси. IP-адреси для комп'ютерів, які виходять з мережі, слід звільняти за допомогою людських ресурсів.

При використанні DHCP весь процес автоматизовано та керується централізовано. DHCP-сервер підтримує пул IP-адрес та орендовану адресу будь-якому клієнту з підтримкою DHCP при запуску в мережі. Через те що IP-адреси є динамічними (орендованими), а не статичними (без постійного призначення), адреси, які не використовуються, автоматично повертаються в пул для перерозподілу. Для уникнення та зменшення кількості помилок при ручному налаштуванні комп’ютерної мережі системний адміністратор може визначити діапазон адрес, які розподіляються сервером між пристроями (рис.3.5) [16].

DHCP надає такі переваги:

- конфігурація надійних IP-адрес. DHCP усуває помилки зроблені при ручної конфігурації IP-адрес, наприклад друкарські помилки, або конфлікти адрес, викликані призначенням IP-адреси більш ніж одному комп'ютеру одночасно.
- автоматизована та централізована конфігурація TCP/IP;
- можливість визначати конфігурації TCP/IP із центрального розташування;
- можливість за допомогою параметрів DHCP призначити повний діапазон додаткових значень конфігурації TCP/IP;
- швидка та ефективна обробка змін IP-адрес для клієнтів, які повинні оновлюватися часто, наприклад, для портативних пристроїв, що переміщуються в різні місця в бездротовій мережі.

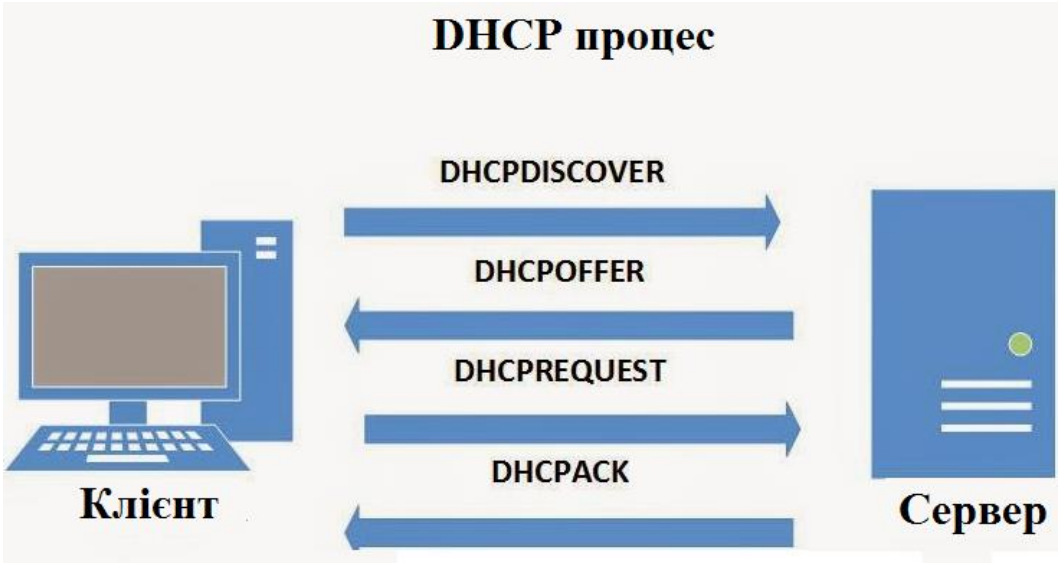


Рисунок 3.5 – Робота DHCP

Для отримання налаштувань використовується механізм DORA (Discover-Offer-Request-Acknowledge). Сам процес складається з наступних етапів:

Discover, або етап виявлення, розпочинається негайно після того, як клієнт підключається до мережі. У цей момент відбувається ініціалізація, під час якої клієнт відправляє спеціальний запит DHCPDISCOVER на широкомовну адресу 255.255.255.255, зазначаючи при цьому нульовий IP-адресу та MAC-адресу, оскільки пристрій ще не має власного IP-адреси. Цей запит розсилається на всі комп'ютери відповідного сегменту мережі, але відповідь на нього надсилають лише DHCP-сервери.

Коли DHCP-сервер отримує запит від клієнта, він проводить обробку і вибір мережевої конфігурації, яку надсилає клієнту через повідомлення DHCPOFFER. Це повідомлення передається на вказану раніше MAC-адресу клієнта, а в деяких випадках може використовуватися широкомовна розсилка. У разі наявності кількох серверів у мережі клієнт отримує відповідну кількість пропозицій DHCPOFFER, і зазвичай вибирається перша отримана.

Request – це спеціальне повідомлення, яке клієнт надсилає серверу після отримання DHCPOFFER і яке містить запит налаштувань. У цьому запиті повторюється інформація з DHCPDISCOVER, а також вказується IP-адреса обраного DHCP-сервера на попередньому етапі.

Acknowledge – це підтвердження, яке обраний DHCP-сервер відправляє клієнту після отримання DHCPREQUEST. Воно фіксує відповідну прив'язку клієнта та надсилає повідомлення DHCPACK на адресу MAC клієнта, вказану на попередньому етапі. В повідомленні DHCPACK підтверджуються надані автоматичні налаштування. Коли клієнт отримує DHCPACK, він автоматично перевіряє надані налаштування та застосовує отриману конфігурацію мережі [17].

Базове налаштування DHCP у Packet Tracer. Дане налаштування проводиться у CLI Router. Налаштування DHCP сервера (рис.3.6):

```
Router(config)#ip dhcp pool V10
Router(dhcp-config)#ne
Router(dhcp-config)#network 91.196.10.0 255.255.255.0
Router(dhcp-config)#de
Router(dhcp-config)#default-router 91.196.10.1
Router(dhcp-config)#exit
Router(config)#ip dh
Router(config)#ip dhcp  ex
Router(config)#ip dhcp  excluded-address 91.196.10.1
Router(config)#ip dh
Router(config)#ip dhcp p
Router(config)#ip dhcp pool V20
Router(dhcp-config)#ne
Router(dhcp-config)#network 91.196.20.0 255.255.255.0
Router(dhcp-config)#default-router 91.196.20.1
Router(dhcp-config)#ip dhcp  excluded-address 91.196.20.1
Router(config)#ip dhc
Router(config)#ip dhcp p
Router(config)#ip dhcp pool V30
Router(dhcp-config)#network 91.196.30.0 255.255.255.0
Router(dhcp-config)#default-router 91.196.30.1
Router(dhcp-config)#ip dhcp  excluded-address 91.196.30.1
```

Рисунок 3.6 – Налаштування DHCP

Отримання адрес DHCP серверу на PC.

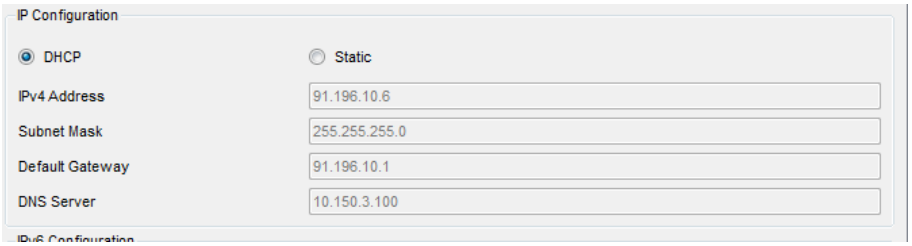


Рисунок 3.7 – Результат роботи серверу

Для зберігання та обміну даними про домені імена між серверами використовується DNS сервер. Після відкритті сайту в браузері для знаходження певного домену беруть участь одразу кілька DNS-серверів (рис.3.8).

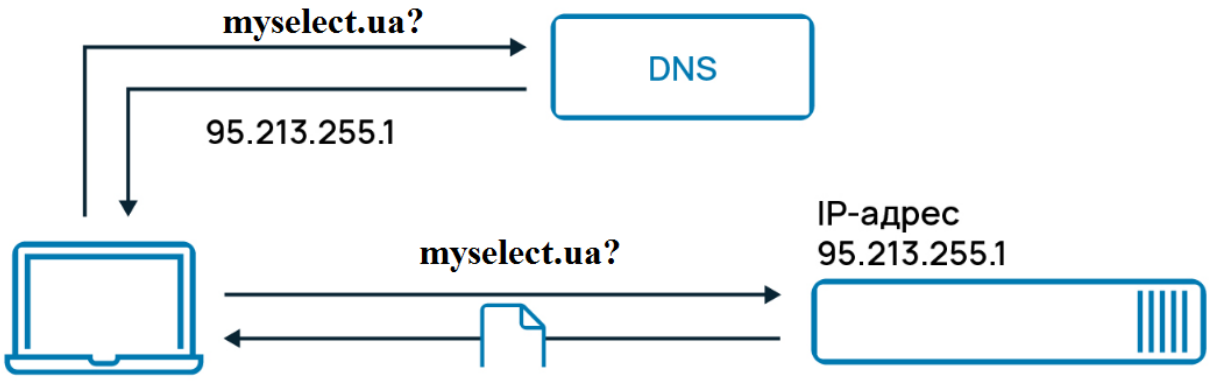


Рисунок 3.8 – Робота DNS

Локальний DNS-сервер обраного інтернет-провайдера, який поставляє послуги підключення. Щоб дізнатись IP-адресу сервера, де знаходиться сторінка сайту, браузери використовують DNS-сервер провайдера. За допомогою спеціальної програми, такі як DNS-клієнт, що використовує браузер надсилається запит до сервера. Якщо споживач не користується послугами інтернет-провайдера, то в мережевих налаштуваннях можна замість локальних серверів провайдера вказати публічні DNS сервери, наприклад від Google [18].

Налаштування веб-серверу (рис.3.9):

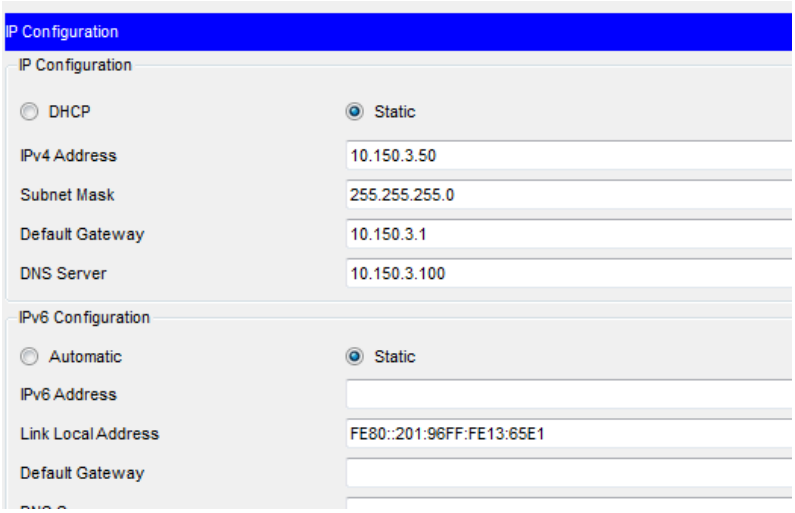


Рисунок 3.9 – Налаштування веб-серверу

Налаштування DNS (рис.3.10).

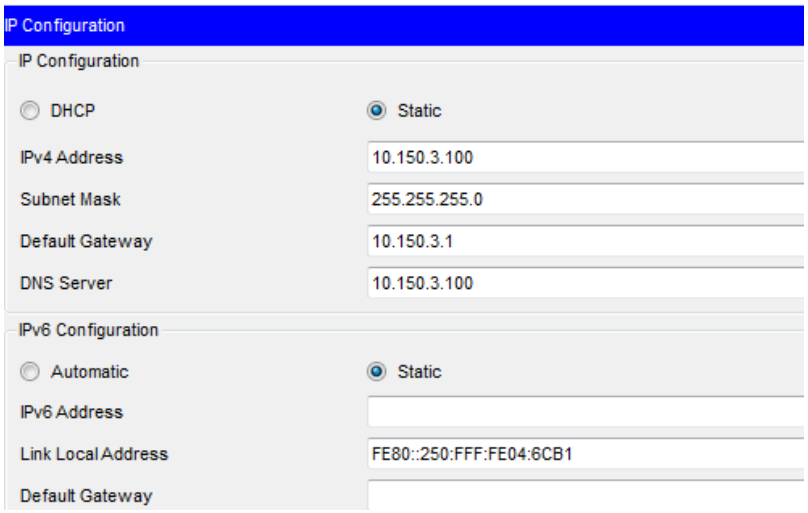


Рисунок 3.10 – Налаштування DNS

Налаштування DNS-записів (рис.3.11).

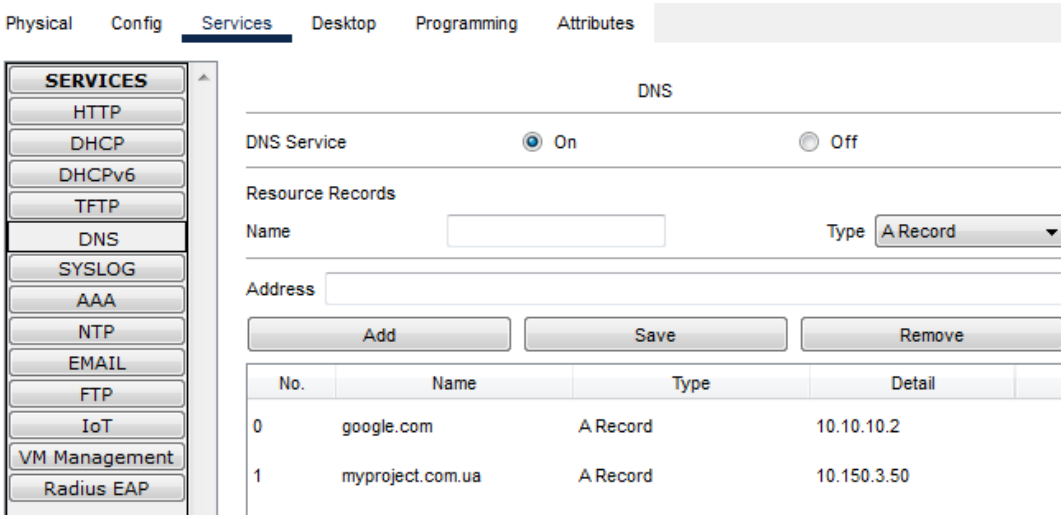
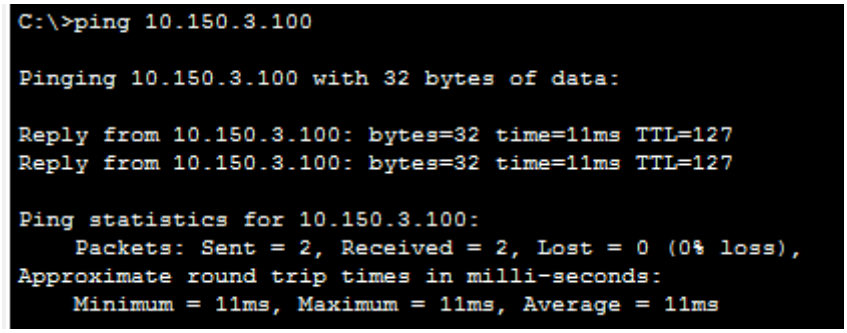


Рисунок 3.11 – Налаштування DNS записів

Перевіряємо підключення між PC та серверами (DNS та DHCP) (рис.2.12).



```
C:\>ping google.com

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time=11ms TTL=127
Reply from 10.10.10.2: bytes=32 time=10ms TTL=127

Ping statistics for 10.10.10.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 11ms, Average = 10ms
```

```
C:\>ping 10.150.3.50

Pinging 10.150.3.50 with 32 bytes of data:

Reply from 10.150.3.50: bytes=32 time=10ms TTL=127
Reply from 10.150.3.50: bytes=32 time=10ms TTL=127

Ping statistics for 10.150.3.50:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

Рисунок 3.12 – Перевірка з’єднань між серверами

Для забезпечення безпечного з'єднання віддалених користувачів із мережею підприємства використовується VPN, яке дозволяє зберігати конфіденційність та уникає локальних обмежень. При використанні віртуальної приватної мережі ніхто не матиме доступу до вашої реальної IP-адреси під час завантаження чи відправлення даних. Замість цього буде використовуватися IP-адреса VPN, а весь обмін інформацією під час підключення до Інтернету буде зашифрованим. (рис.3.13). Шифрування – це спосіб перетворення тексту в набір кодівр [19].

Є чотири причини використання VPN на підприємстві:

Надійний захист. Інформація, що передається, доступна тільки за наявності ключа шифрування.

Рисунок 3.13 – Робота VPN

Змінення геолокації. Інформація про геолокацію надходять не з пристрою, а з сервера VPN. Сервер може бути в іншій країні, тож визначити фізичне місце розташування стає неможливим.

Отримання доступу до місцевого контенту може бути обмеженим при відвідуванні міст за межами своєї країни. Використання VPN дозволяє змінити ваше місце розташування на регіон сервера, що встановлюється посередником у іншій країні, забезпечуючи змогу переглядати контент, призначений для цього регіону. Захищена передача даних. У разі віддаленої роботи використовується доступ до конфіденційних корпоративної інформації. Щоб знизити ймовірність їх розповсюдження, застосовують підключення із шифруванням даних [19].

Є два основні типи підключення:

— віддалений доступ. Це актуально при роботі з ненадійною точкою доступу, наприклад публічний Wi-Fi. Дозволяє підключатися до корпоративної мережі приватного зашифрованого тунелю;

— вузол-вузол. Застосовується у більшості в корпоративному середовищі, наприклад, коли компанія має кілька офісів з різним фізичним місцезнаходженням. Він з'єднує основний офіс із філією: так створюється закрита внутрішня мережа, де всі офіси підключені та взаємодіють між собою.

Один з протоколів, який буде використано при побудові VPN тунелю та за допомогою якого будуть засекречені дані віддалених користувачів при підключенні на підприємстві – L2TP/IPSec.

Створення та налаштування VPN тунелю GRE на прикладі іншої схеми, так як для налаштування потрібно щонайменше 2 рутера, наприклад 2069 (рис.3.14).

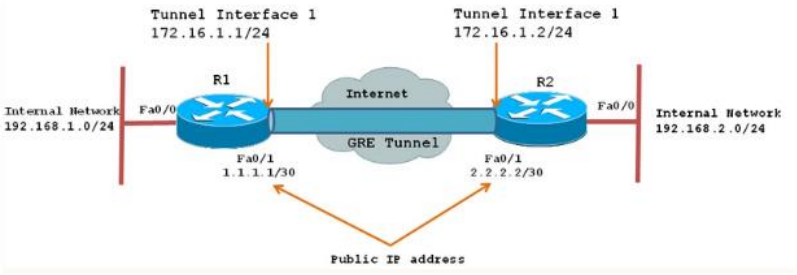


Рисунок 3.14 – Налаштування тунелю між роутерами

Для базового налаштування потрібно створити тунельні інтерфейси на R1 та R2 (рис.3.15).

R1(config)# interface Tunnel1	R2(config)# interface Tunnel1
R1(config-if)# ip address 172.16.1.1 255.255.255.0	R2(config-if)# ip address 172.16.1.2 255.255.255.0
R1(config-if)# ip mtu 1400	R2(config-if)# ip mtu 1400
R1(config-if)# ip tcp adjust-mss 1360	R2(config-if)# ip tcp adjust-mss 1360
R1(config-if)# tunnel source 1.1.1.1	R2(config-if)# tunnel source 2.2.2.2
R1(config-if)# tunnel destination 2.2.2.2	R2(config-if)# tunnel destination 1.1.1.1

Рисунок 3.15 – Налаштування тунелю

Для перевірки працездатності налаштувань можна використати команду «ping» та «tracer».

3.2 Налаштування обладнання

Далі приводимо проведені налаштування на новому обладнані. Перший крок розподіл адресів у першому, другому цехах та адміністративній будівлі, кроки створення та базового налаштування були приведені у попередньому пункті. На зображені присутні робочі станції та їх адреси, які були увімкнуті у мить отримання цього знімку. Кількість робочих станцій набагато менша від оголошеної, ця причина виникла внаслідок переходу більшості персоналу на дистанційний режим роботи через воєнний стан країни (рис.3.16).

```
MTS-NS[root]#cat AA2
MTS-NS[root]#cat AA2

 -------------- STATIC : 17  --------------
 - - - - - - - -  VLAN 110 - - - - - - - - -
bh-51-p1-08.local-110 (10.50.110.51) at 00:1f:66:3c:91:c4 on re1.110 expires in 1194 seconds [vlan]
bh-52-p1-09.local-110 (10.50.110.52) at 00:03:73:d8:a7:a0 on re1.110 expires in 1197 seconds [vlan]
bh-53-p1-10.local-110 (10.50.110.53) at 00:45:c4:25:15:82 on re1.110 expires in 1199 seconds [vlan]
bh-54-p1-11.local-110 (10.50.110.54) at 00:03:73:ba:db:f6 on re1.110 expires in 266 seconds [vlan]
 - - - - - - - - VLAN 120 - - - - - - - - -
free-of-p1-07.local-120 (10.50.120.50) at 00:03:73:db:27:00 on re1.120 expires in 1197 seconds [vlan]
 - - - - - - - - VLAN 130 - - - - - - - - -
sb-reg.local-130 (10.50.130.30) at 00:af:29:cf:71:c3 on re1.130 expires in 1175 seconds [vlan]
sb-ohr.local-130 (10.50.130.45) at 00:ba:db:fc:3c:27 on re1.130 expires in 1076 seconds [vlan]
sb-srv.local-130 (10.50.130.50) at 00:19:d1:04:01:11 on re1.130 expires in 486 seconds [vlan]
 - - - - - - - - VLAN 210 - - - - - - - - -
snb-22-p1-13.local-210 (10.50.210.22) at 00:69:95:f5:82:44 on re1.210 expires in 1188 seconds [vlan]
p-p-33-p1-16.local-210 (10.50.210.33) at 00:5f:f4:d3:93:d8 on re1.210 expires in 1192 seconds [vlan]
prnt-90.local-210 (10.50.210.90) at 00:81:39:e8:25:a6 on re1.210 expires in 1195 seconds [vlan]
 - - - - - - - - VLAN 220 - - - - - - - - -
ceh1-31.local-220 (10.50.220.31) at 00:97:5a:43:95:f4 on re1.220 expires in 1182 seconds [vlan]
prnt-90.local-220 (10.50.220.90) at 00:40:ca:9d:c7:35 on re1.220 expires in 1195 seconds [vlan]
 - - - - - - - - VLAN 230 - - - - - - - - -
pto-32-p2-11.local-230 (10.50.230.32) at 00:27:ea:60:df:0a on re1.230 expires in 1200 seconds [vlan]
pto-36-p2-15.local-230 (10.50.230.36) at 00:1b:0d:cf:e1:6c on re1.230 expires in 1196 seconds [vlan]
prnt-090.local-230 (10.50.230.90) at 00:40:ca:9d:c7:42 on re1.230 expires in 1072 seconds [vlan]
prnt-100.local-230 (10.50.230.100) at 00:00:85:95:1e:a5 on re1.230 expires in 1172 seconds [vlan]
 - - - - - - - - WIFI 192: 0 - - - - - -
 -------------- WARNING: 0  --------------
 ----------------------------------------
  TOTAL MAC ACTIVE:      27
 ----------------------------------------
  TOTAL BAN [www + postfix] items: 5
 ----------------------------------------
```

Рисунок 3.16 – Налаштування VLAN на сервері підприємства

Для налаштувань DHCP використали програмне забезпечення ISC-DHCP – це програма DHCP-сервера, яка працює на сервері як демон, надаючи в мережу службу протоколу динамічної конфігурації хосту (рис.3.17).

```
server-name "MTS DHCP server";
authoritative;
local-address 10.50.110.1;
option ip-forwarding off;
option time-offset 3;
ddns-updates off;
ddns-update-style none;
log-facility local7;
dhcp-cache-threshold 0;
default-lease-time 600;
max-lease-time 1200;

# ------------------------------------------------
# ---------  system dev static ip VLAN 110  --------
# ------------------------------------------------
subnet 10.50.110.0 netmask 255.255.255.0 {
#  range 10.50.110.220 10.50.110.249;
  deny unknown-clients;
  option routers 10.50.110.1;
  option subnet-mask 255.255.255.0;
  option broadcast-address 10.50.110.255;
  option domain-name-servers 10.50.110.100;
  option domain-name "local";
  deny client-updates;
  deny bootp;
  use-host-decl-names true;
  default-lease-time 1800;
  max-lease-time 3600;
}
# ------------------------------------------------------------------------------
host dev1100 { hardware ethernet 00:bc:12:75:d2:24; fixed-address 10.50.110.100; }
host dev1110 { hardware ethernet 00:34:97:69:8f:49; fixed-address 10.50.110.110; }
host dev1090 { hardware ethernet 00:38:b7:f8:65:27; fixed-address 10.50.110.90; }
# ------------------------------------------------

......
```

Рисунок 3.17 – Налаштування DHP на підприємстві

Default-lease-time 600 – час у секундах, після якого клієнт повинен запросити продовження оренди.

Max-lease-time 1200 – час оренди IP адреси за секунди, клієнт повинен звільнити IP-адресу, якщо протягом заданого часу оренду продовжити не вдалося, якщо оренда не продовжена, сервер може видати цю адресу іншому клієнту.

Log-facility local7 – джерело, яке буде вказано під час надсилання повідомлень до Syslog.

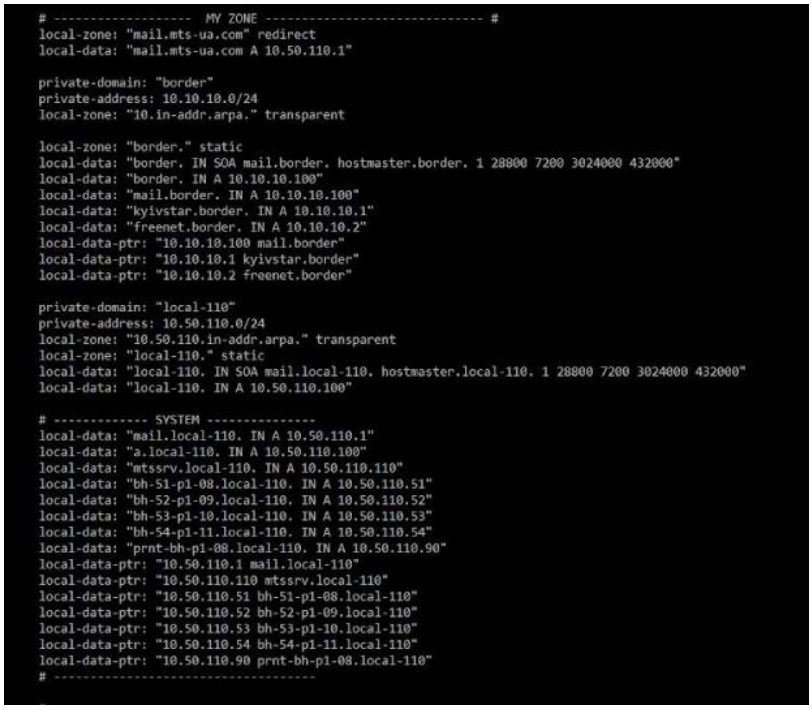
Декларація підмережі subnet 10.110.50.0 netmask 255.255.255.0 {}.

Range 10.110.50.220 10.110.50.249 – пул динамічних адрес.

Option routers 10.110.50.0 – шлюз.

Задати фіксовану IP-адресу для хоста – host Name { hardware ethernet 00:bc:12:75:d2:24; fixed-address 10.50.110.100;}.

Перейдемо до налаштування DNS, ключове налаштування здійснюється за допомогою програмного забезпечення Unbound DNS-сервер із відкритим кодом. Unbound це кешуючий DNS сервер, який обслуговує виключно рекурсивні запити. Під час роботи сервера кеш повністю міститься у пам'яті, яке розмір обмежений зазначеним обсягом. Unbound підтримує розширення DNSSEC і може працювати як validator. Один з плюсів Unbound у порівнянні з BIND треба відзначити ті самі скромні розміри і швидкість (рис.3.18).

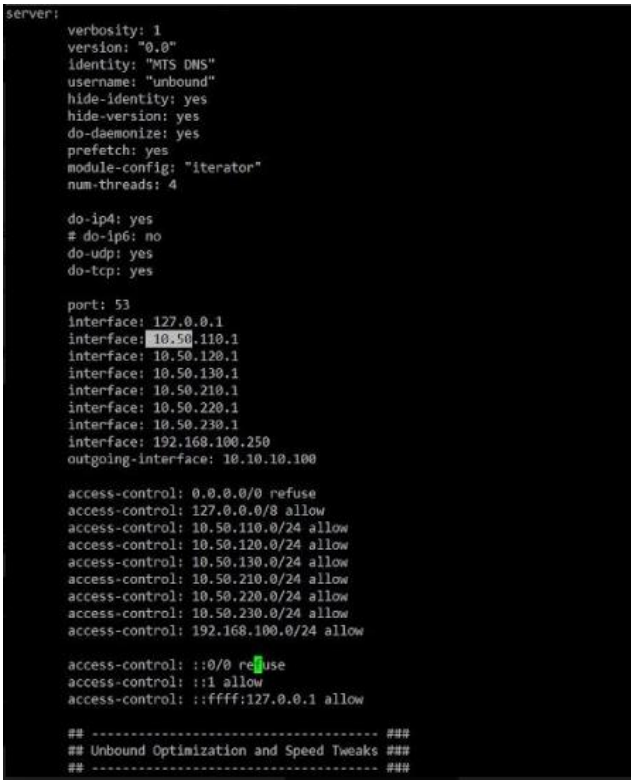


```
# ------------------  MY ZONE ----------------------------- #
local-zone: "mail.mts-ua.com" redirect
local-data: "mail.mts-ua.com A 10.50.110.1"

private-domain: "border"
private-address: 10.10.10.0/24
local-zone: "10.in-addr.arpa." transparent

local-zone: "border." static
local-data: "border. IN SOA mail.border. hostmaster.border. 1 28800 7200 3024000 432000"
local-data: "border. IN A 10.10.10.100"
local-data: "mail.border. IN A 10.10.10.100"
local-data: "kyivstar.border. IN A 10.10.10.1"
local-data: "freenet.border. IN A 10.10.10.2"
local-data-ptr: "10.10.10.100 mail.border"
local-data-ptr: "10.10.10.1 kyivstar.border"
local-data-ptr: "10.10.10.2 freenet.border"

private-domain: "local-110"
private-address: 10.50.110.0/24
local-zone: "10.50.110.in-addr.arpa." transparent
local-zone: "local-110." static
local-data: "local-110. IN SOA mail.local-110. hostmaster.local-110. 1 28800 7200 3024000 432000"
local-data: "local-110. IN A 10.50.110.100"

# ------------- SYSTEM ---------------
local-data: "mail.local-110. IN A 10.50.110.1"
local-data: "a.local-110. IN A 10.50.110.100"
local-data: "mtssrv.local-110. IN A 10.50.110.110"
local-data: "bh-51-p1-08.local-110. IN A 10.50.110.51"
local-data: "bh-52-p1-09.local-110. IN A 10.50.110.52"
local-data: "bh-53-p1-10.local-110. IN A 10.50.110.53"
local-data: "bh-54-p1-11.local-110. IN A 10.50.110.54"
local-data: "prnt-bh-p1-08.local-110. IN A 10.50.110.90"
local-data-ptr: "10.50.110.1 mail.local-110"
local-data-ptr: "10.50.110.110 mtssrv.local-110"
local-data-ptr: "10.50.110.51 bh-51-p1-08.local-110"
local-data-ptr: "10.50.110.52 bh-52-p1-09.local-110"
local-data-ptr: "10.50.110.53 bh-53-p1-10.local-110"
local-data-ptr: "10.50.110.54 bh-54-p1-11.local-110"
local-data-ptr: "10.50.110.90 prnt-bh-p1-08.local-110"
# ------------------------------------
```

Рисунок 3.18 – Налаштування DNS

Перш за все додаємо локальні зони DNS такі як, наприклад MyZone, System для використання локального DNS сервер для прямого та зворотного пошуку локальних адрес, наприклад: lozal-zone: mail.mts-ua.com [23].

Також додали localhost для переадресації та зворотного пошуку за допомогою наступних рядків:
local-zone: “10.50.110.in addr.arpa.” transparent.
local-data: “local-110 IN A 10.50.110.100”.



```
server:
        verbosity: 1
        version: "0.0"
        identity: "MTS DNS"
        username: "unbound"
        hide-identity: yes
        hide-version: yes
        do-daemonize: yes
        prefetch: yes
        module-config: "iterator"
        num-threads: 4

        do-ip4: yes
        # do-ip6: no
        do-udp: yes
        do-tcp: yes

        port: 53
        interface: 127.0.0.1
        interface: 10.50.110.1
        interface: 10.50.120.1
        interface: 10.50.130.1
        interface: 10.50.210.1
        interface: 10.50.220.1
        interface: 10.50.230.1
        interface: 192.168.100.250
        outgoing-interface: 10.10.10.100

        access-control: 0.0.0.0/0 refuse
        access-control: 127.0.0.0/8 allow
        access-control: 10.50.110.0/24 allow
        access-control: 10.50.120.0/24 allow
        access-control: 10.50.130.0/24 allow
        access-control: 10.50.210.0/24 allow
        access-control: 10.50.220.0/24 allow
        access-control: 10.50.230.0/24 allow
        access-control: 192.168.100.0/24 allow

        access-control: ::0/0 refuse
        access-control: ::1 allow
        access-control: ::ffff:127.0.0.1 allow

        ## ------------------------------------ ###
        ## Unbound Optimization and Speed Tweaks ###
        ## ------------------------------------ ###
```

Рисунок 3.19 – Продовження налаштування DNS

Далі пояснимо деякі команди, які використовувались при налаштуванні серверу (рис.3.19).

Verbosity: 1, рівень деталізації журналу подій (0 – лише помилки; 1 – кожен запит; 3 – детальний розбір).

Hide-version: yes, «ховаємо версію» софту.

Username: unbound, від чийого імені працює daemon unbound.

do-ip4: yes; do-ip6: no; do-udp: yes; do-tcp: yes, дозволяємо ip4 tcp/udp та забороняємо підтримку ipv6.

Port: 53, Порт, на якому «слухати» запити.

Interface: 127.0.0.1.

Interface: 10.3.159.254, описуємо інтерфейси, на яких «слухатимемо» запити

Outgoing-interface: 10.12.59.30, вказуємо вихідний інтерфейс, вказуємо мережі, чиї запити оброблятимемо.

Access-control: 10.3.159.0/24 allow, перелічуємо мережі, рекурсивні запити від яких обслуговуються (за замовчуванням заборонено все недозволене).

```
        # ------------------------------------------------------------ #

forward-zone:
       name: "outbound.protection.outlook.com"
       forward-addr: 8.8.8.8
       forward-addr: 1.1.1.1

        # ------------------------------------------------------------ #

remote-control:
        control-enable: yes
        control-interface: 127.0.0.1
        control-port: 8953
        server-key-file: "/usr/local/etc/unbound/keys/unbound_server.key"
        server-cert-file: "/usr/local/etc/unbound/keys/unbound_server.pem"
        control-key-file: "/usr/local/etc/unbound/keys/unbound_control.key"
        control-cert-file: "/usr/local/etc/unbound/keys/unbound_control.pem"

        # ------------------------------------------------------------ #
```

Рисунок 3.20 – Налаштування DNS

Рядки потрібні для роботи зворотного пошуку:
Forward-zone: name: “outbound.protection.outlook.com.”
Forward-addr: 8.8.8.8 remote-control, дана команда відповідає за налаштування віддаленого доступу до серверу (рис.3.20).

Переходимо до створення та конфігурації тунелю VPN. Перш за все налаштували набір протоколів IPsec. Протокол IKEv1 або Internet Key Exchange v1 дозволяє створювати прямі тунелі IPSec між сервером та клієнтом [24]. IPSec забезпечує шифрування мережевого трафіку у віртуальних приватних мережах IKEv1 (рис.3.21).

```
# ------------------------------------------------------------
# ipsec.conf - strongSwan IPsec configuration file
# ------------------------------------------------------------
config setup
      uniqueids = yes

conn my-base-l2tp
   compress=no
   dpdaction=clear
   dpddelay=35s
   dpdtimeout=300s
   fragmentation=yes
   forceencaps=yes

# ------------------------------------------------------------
 conn L2TP/IPsec-PSK
   also=my-base-l2tp
   type = transport
   keyexchange=ikev1
   forceencaps=yes
   keyingtries=1

   leftsendcert = no
   leftauth = psk
   rightauth = psk
   right = %any
   mark = %unique
   auto = add
# ------------------------------------------------------------
```

Рисунок 3.21 – Налаштування VPN

Uniqueds – видача унікального індетифікатора при вході кожному користувачу, декілька підключень з одного акаунта неможлива.
Commress = no, вимикається стиснення трафіку, завдяки цьому швидше працює.
Dpdaction = clear, вмикає механізм Dead Peer Detection (DPD) і вказує, що потрібно «відкинути» клієнта, якщо він не відповів швидше закінчення таймауту.
Dpddelay = 35s – затримка до включення DPD.
Dpdtimeout = 300s – тайм-аут для DPD.
Fragmentation = yes – увімкнення внутрішньої фрагментації пакетів. Дозволяє використовувати IPsec із провайдерами, у яких зламана IP-фрагментація пакетів.
Forceencaps = yes, встановлення шифрування, перевірка протоколів.
Also = my-base-12tp, вид запуску налаштованих параметрів.
Type = transport, вид протоколу.
Keyexchange = ikev1, тип обміну с сертифікатами.
Keyingtries = 1, кількість спроб передачі сертифікату.
Leftsendcert = no, відправка сертифікату на інший бік, якщо він не знайден.

Leftauth = psk, кодова фраза для піключення, знаходиться в окремому файлі. right=%any, звідки йдуть запити, якщо потрібно зробити обмеження прописуються сітки.
Auto = add, сервер чекає підключення від клієнту.

Налаштування MPD. MPD – це заснована на netgraph реалізація ppp-протоколу мультизв'язку для FreeBSD. MPD спроектований бути швидким та гнучким, обробляючи конфігурацію та звернення в режимі користувача, спрямовуючи пакети даних безпосередньо в ядро (рис.3.22).

```
startup:
        set user admin
        set console self 127.0.0.1 5005
        set console open
        # set web self 0.0.0.0 5555
        # set web open

default:
        load l2tp_server

l2tp_server:
        # Define dynamic IP address pool
        set ippool add pool_l2t 10.50.110.85 10.50.110.94

        # Create clonable bundle template named B
        create bundle template B_l2t
        set bundle enable encryption
        set bundle enable compression
        set iface enable proxy-arp
        set iface enable tcpmssfix
        # set iface mtu 1400
        set iface idle 1800
        set ipcp yes vjcomp
        set ipcp ranges 10.50.10.95/32 ippool pool_l2t
        set ipcp dns 8.8.8.8
        set ccp yes mppc
        set mppc yes e40
        set mppc yes e128
        set mppc yes stateless

        create link template L_l2t l2tp
        set link action bundle B_l2t
        set link enable multilink
        set link yes acfcomp protocomp
        set link max-children 500
        set link no pap chap eap
        set link enable chap-msv2
        set link keep-alive 10 60
        set link mtu 1400
        set l2tp self 10.10.10.100
        set l2tp enable length
        set l2tp disable dataseq
        set link enable incoming
```

Рисунок 3.22 – Налаштування MPD

Startup: set user admin, визначаємо користувачів.
Set console self 127.0.0.1 5005, set console open, конфігурація консолі.
Set web self 0.0.0.0 5006, set web open, конфігурація веб-сервера.
Set ippool add pool_12t 10.50.110.85 10.50.110.94, визначаємо, який адресний пул використовувати.
Create bundle template B_l2t, створюємо клонований шаблон B_l2t.
Set iface enable proxy – arp, дозволяємо на інтерфейсі проксіювання MAC-адрес.

Set iface idle 1800, задаємо час простою.
Set iface enable tcpmssfix, задаємо виправляти помилки з визначенням MSS.
Set ipcp yes vjcomp, включаємо стиснення даних.
Set ipcp ranges 10.50.10.95/32 ippool pool_l2t, конкретизуємо адресний пул для динамічного присвоєння параметрів.
Set ipcp dns 8.8.8.8, вказуємо, які адреси DNS-серверів надавати клієнтам.
Set bundle enable compression, set ccp yes mppc, set mppc yes e40, set mppc yes e128, set mppc yes stateless, ці рядки необхідні для підтримки Microsoft Point-to-Point шифрування.
Налаштування l2_tp:
Set link action bundle B_l2t, вказуємо, який шаблон використовувати;
Set link disable multilink, set link yes acfcomp protocomp. забороняємо режим мультилінк;
Set link no pap chap eap, set link enable chap, вимагаємо chap авторизацію.
Set link mtu 1400, зменшення розміру mtu для запобігання фрагментації.
Задаємо адресу для вхідних повідомлень: set 12pt self 10.10.10.100.
Дозволяємо вхідні підключення: set link enable incoming.

Додамо StrongSwan, демон IPSec з відкритим вихідним кодом, використовується для реалізації L2Tp IPSec та налаштуємо його як наш сервер VPN (рис.3.23).

```
charon
{
   load_modular = yes
   threads = 32
   interfaces_use = re0
   install_virtual_ip = no
   install_routes = no
   process_route = no

   filelog {
      charon {
         path = /var/log/Security/s_charon.log
         # add a timestamp prefix
         time_format = %b %e %T
         # prepend connection name, simplifies grepping
         ike_name = yes
         # overwrite existing files
         append = no
         # flush each line to disk
         flush_line = yes
         default = 0
         ike = 0
      }
      stderr {
         ike = 3
         knl = 3
      }
   }

   syslog
   {
      identifier = ipsec
      daemon {
         ike_name = yes
         default = -1
         ike = 0
      }
      auth {
         default = 1
         ike = 1
      }
   }
```

Рисунок 3.23 – Налаштування StrongSwan

Load_modular = yes, загрузка модулів для StrongSwan.
Treads = 32, кількість потоків.
Interfaces_use = re0, назва інтерфейсу до якого підключена мережева картка.
Install_routes = no, програма не обновлює самостійно маршрути для маршрутизації.
Identifier = ipsec, для базового захищеного тунелю із попереднім загальним ключем встановлюється також одноранговий партнера, до якого поширюється ця особистість.
Auth – налаштування для демону IPSec [24].

3.3 Налаштування безпеки

Домашня панель моніторингу включає дані вашого облікового запису, журнали, метрики, трасування, оповіщення, винятки та аналітику.

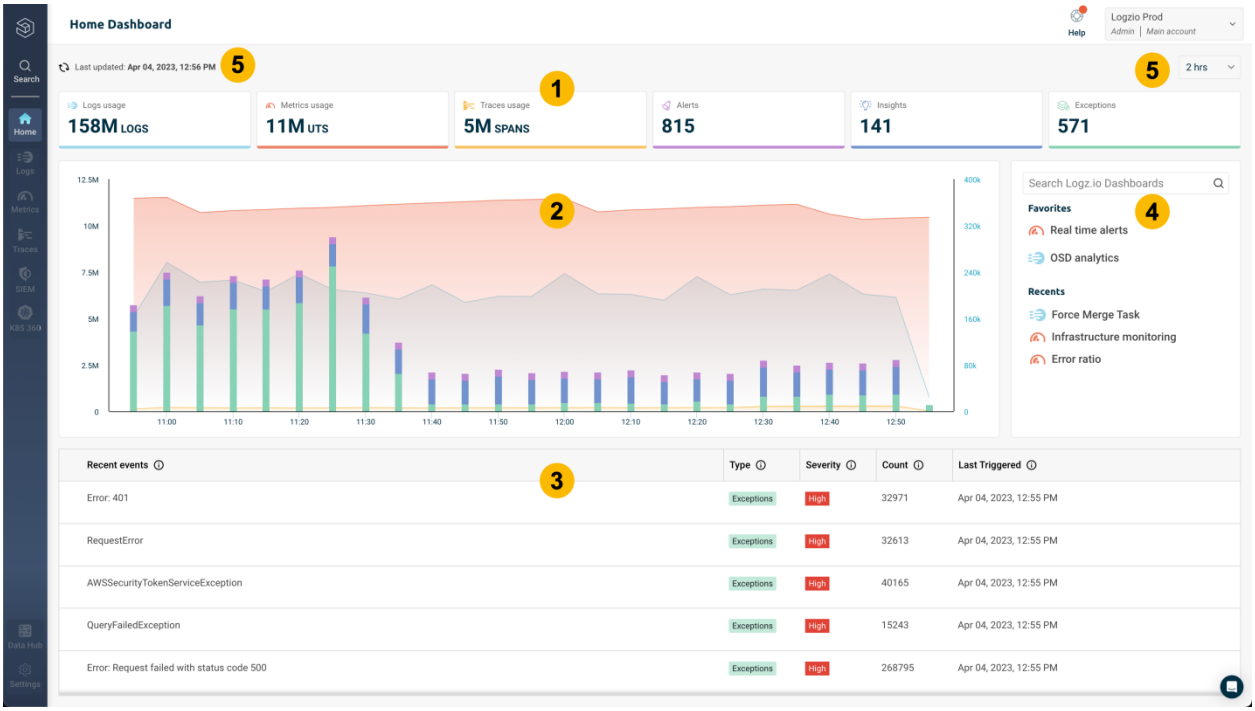


Рисунок 3.24 –Домашня панель Logz

Це візуальне представлення даних вашого облікового запису (рис.3.25).

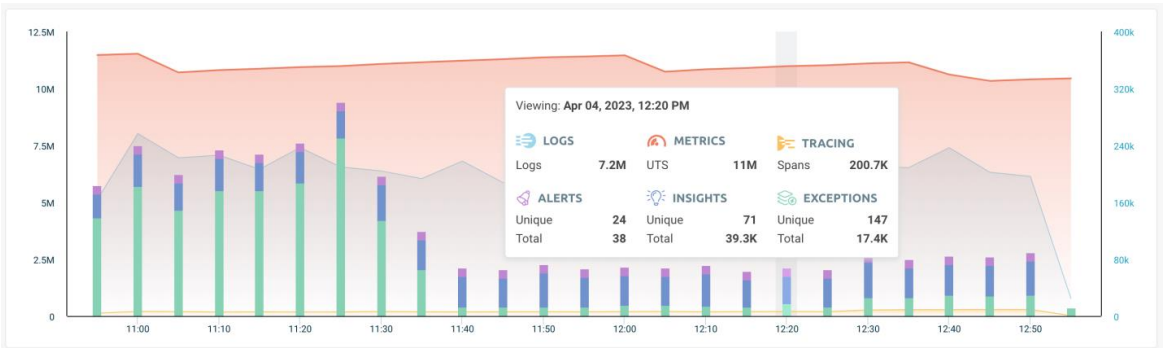


Рисунок 3.25 – Панель налаштування Logz

Додали додатковий рівень безпеки у свій обліковий запис Logz.io, увімкнувши перемикач двофакторної автентифікації (2FA).

2FA вимагає двох форм ідентифікації для доступу до облікового запису, і ви можете вибрати метод, який підходить саме вам, будь то фізичний токен, перевірка SMS, автентифікація на основі телефонного дзвінка або додаток для аутентифікації (рис.3.26).

Як тільки перемкнули опцію 2FA, маємо можливість отримувати електронного листа з інструкціями з налаштування двофакторної автентифікації [20].

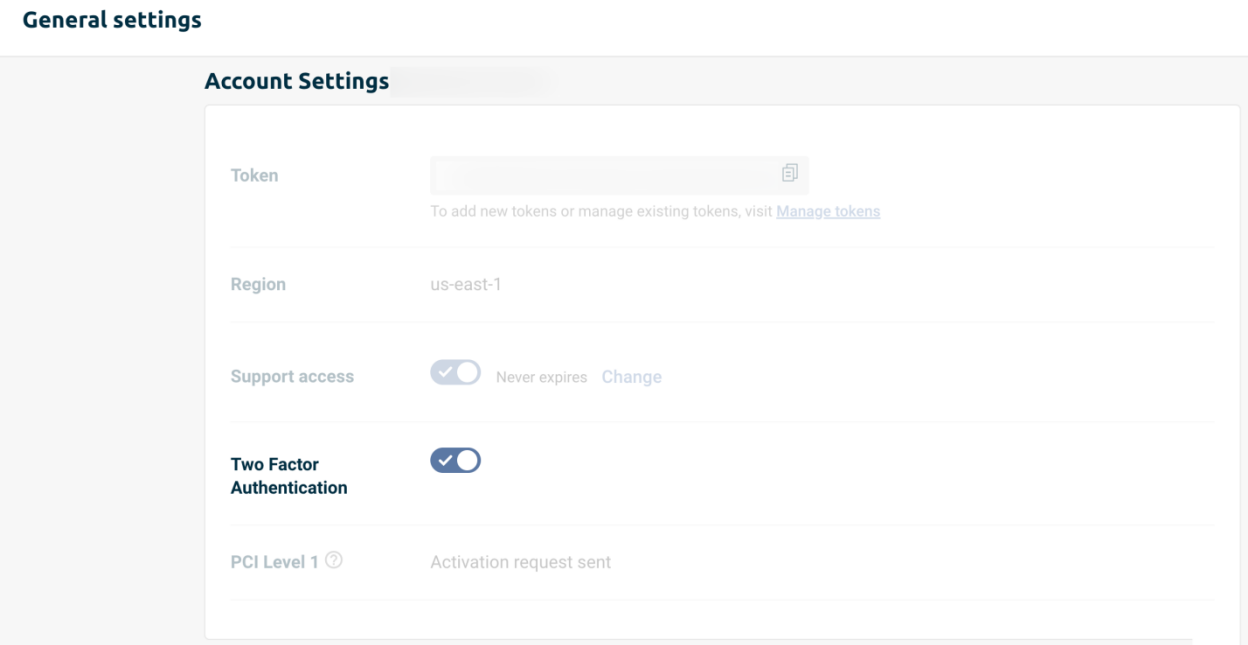


Рисунок 3.26 – Налаштування 2FA

Налаштувати сповіщення журналу Logz.io, щоб автоматично отримувати сповіщення про проблеми, які потребують уваги.

Налаштували компоненти пошуку. Це визначає, які журнали шукати і які облікові записи (рис.3.27 -3.29).

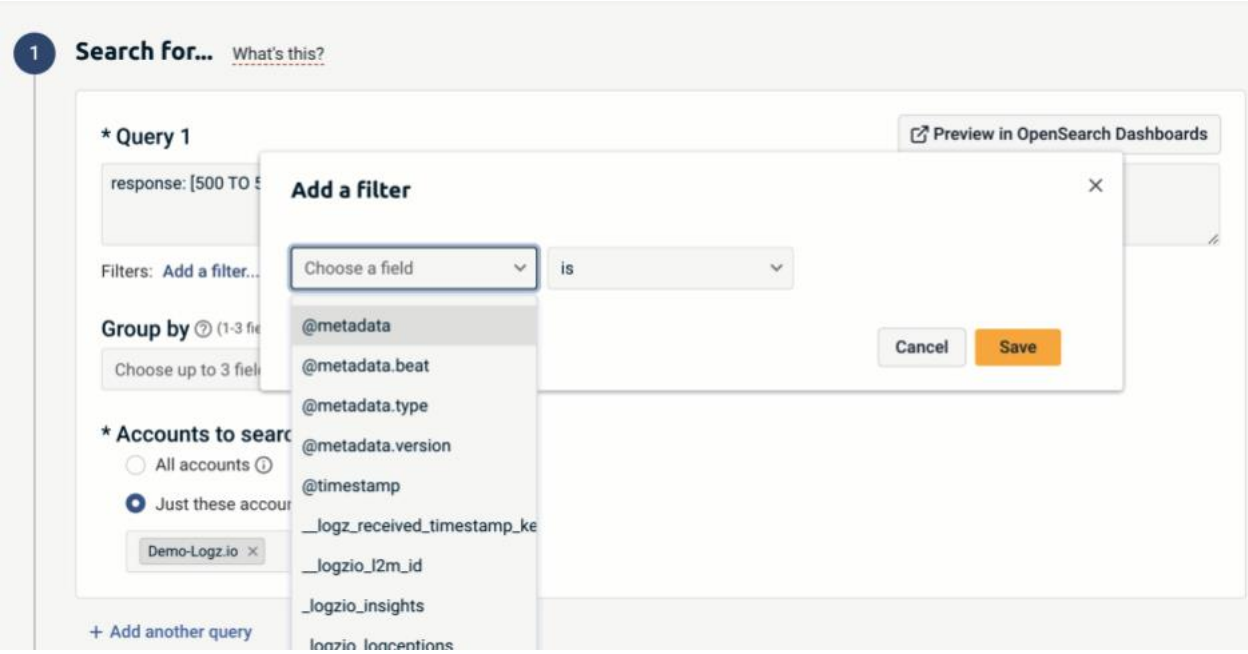


Рисунок 3.27 – Налаштування фільтрів

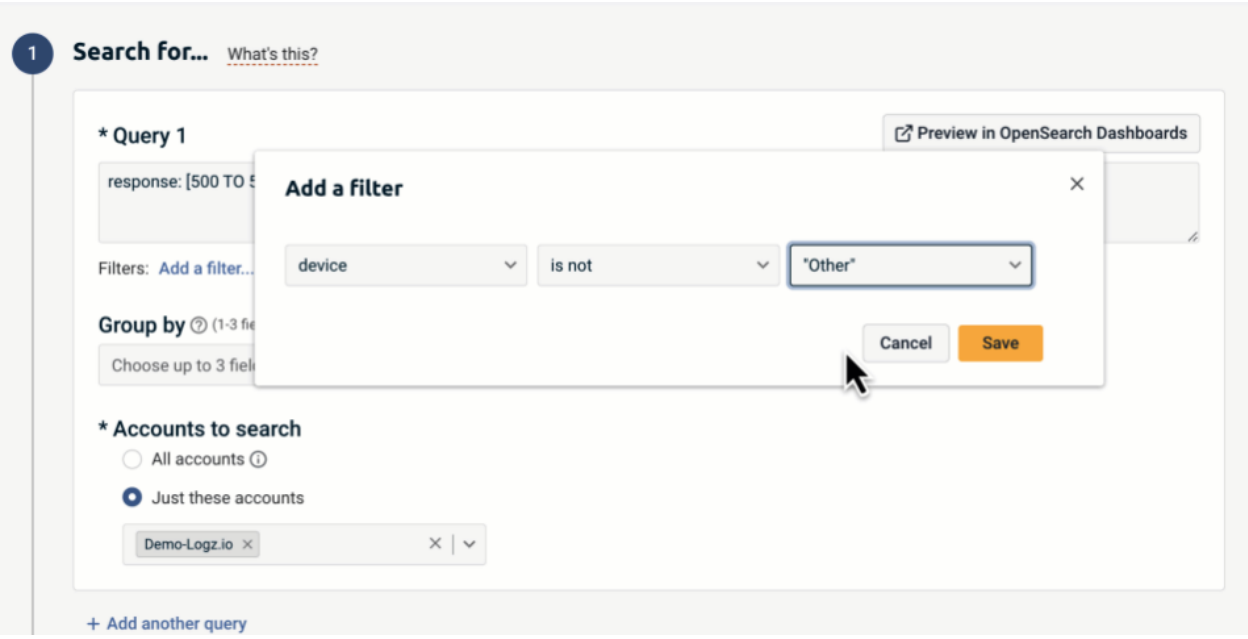


Рисунок 3.28 – Додавання фільтрів

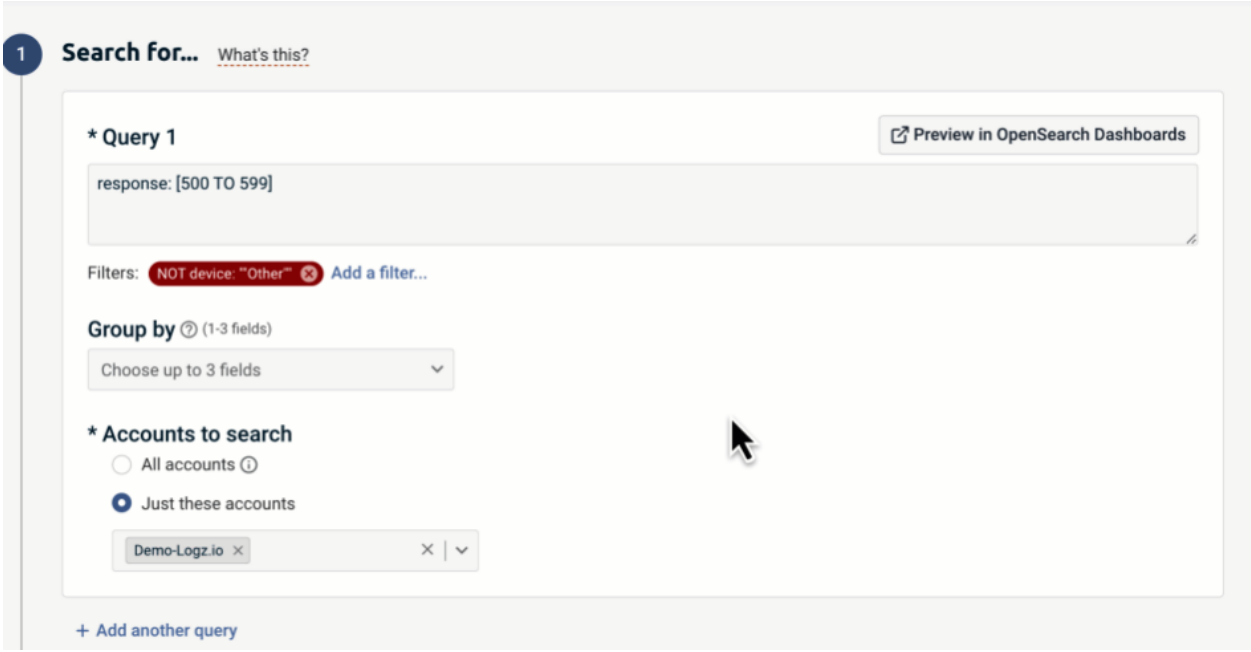


Рисунок 3.29 – Результат додавання фільтрів

Встановили поріг та рівні серйозності.

У розділі «Тригер, якщо...» натиснули « + Додати поріг» , щоб налаштувати до 5 порогових умов, кожна з яких має власний тег серйозності (рис. 3.30).

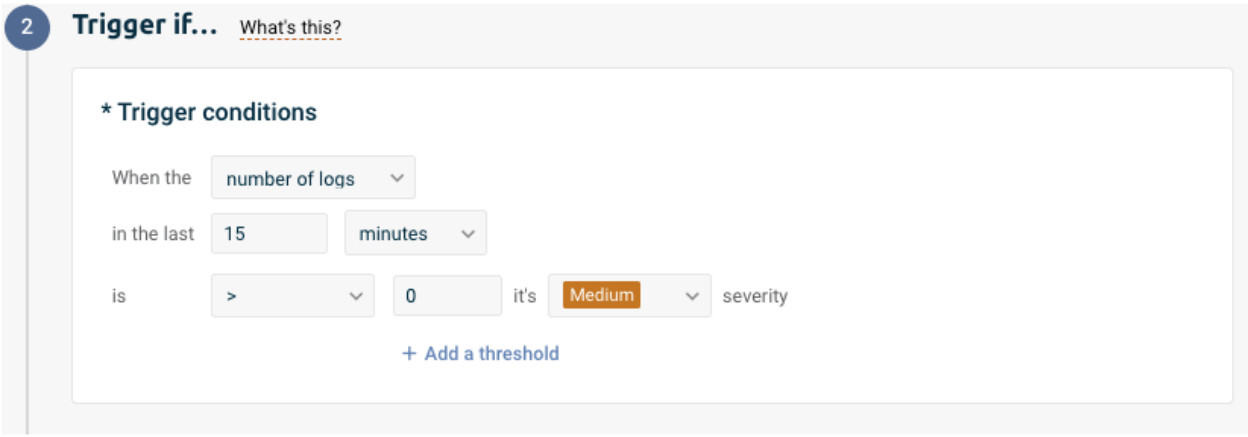


Рисунок 3.30 – Налаштування тригерів

За умовчанням умови тригера виконуються приблизно щохвилини. Якщо є затримка, попередження не перевіряється, доки не будуть отримані всі дані. Крім того, як тільки попередження відповідає своїй умові і спрацьовує, воно більше не перевіряється протягом тимчасового діапазону умов спрацьовування оповіщення, що залишився (рис.3.31).

Опис відображається на сторінці визначення сповіщень і є частиною електронних листів та повідомлень Slack, що надсилаються при спрацюванні оповіщення.

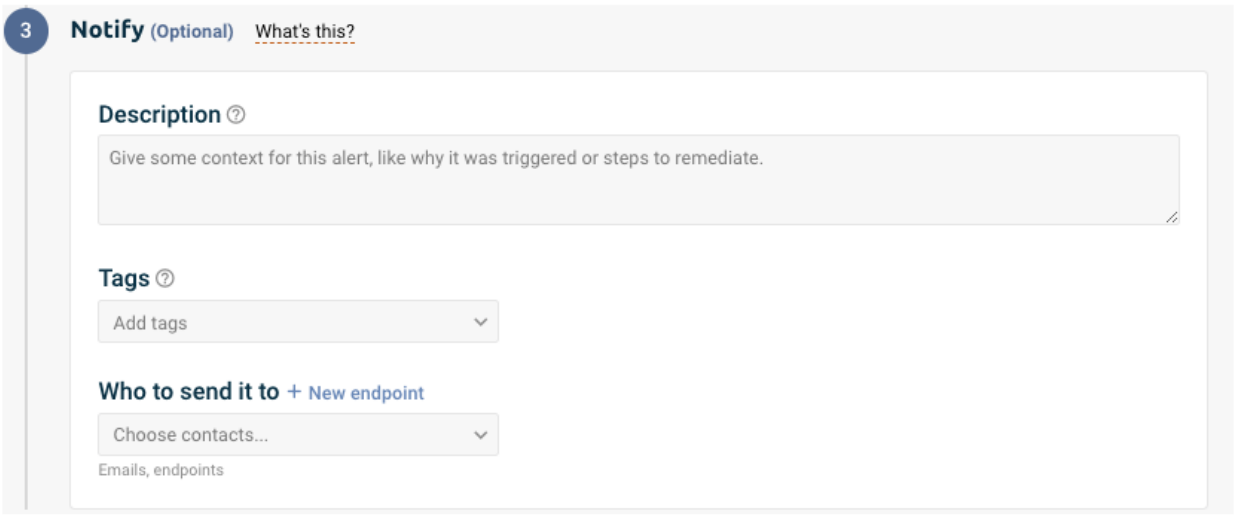


Рисунок 3.31 – Налаштування повідомлень

Обрали кінцеві точки сповіщень, для того, щоб надсилати повідомлення або електронні листи під час спрацювання оповіщення (рис.3.32). Однак це не обов'язково – активовані оповіщення, як і раніше, реєструються та доступні для пошуку на панелях моніторингу OpenSearch.

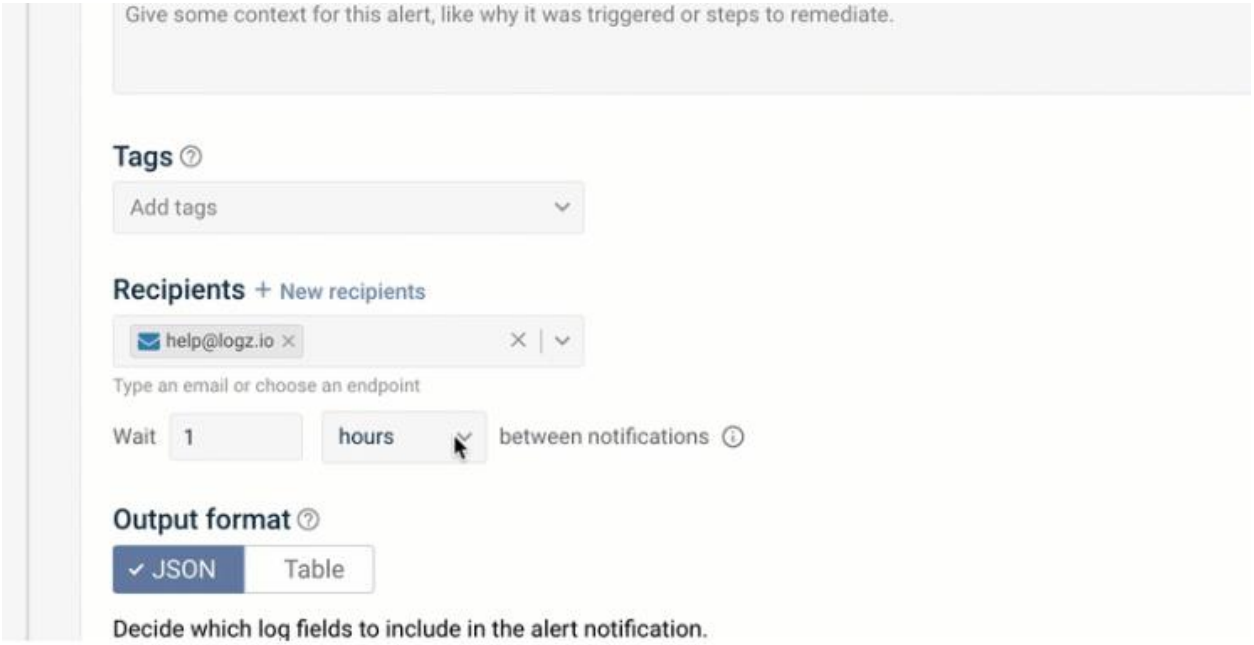


Рисунок 3.32 – Налаштування тегів

FastNetMon – програмний пакет для виявлення DDoS атак та їх подальшого відображення [21].

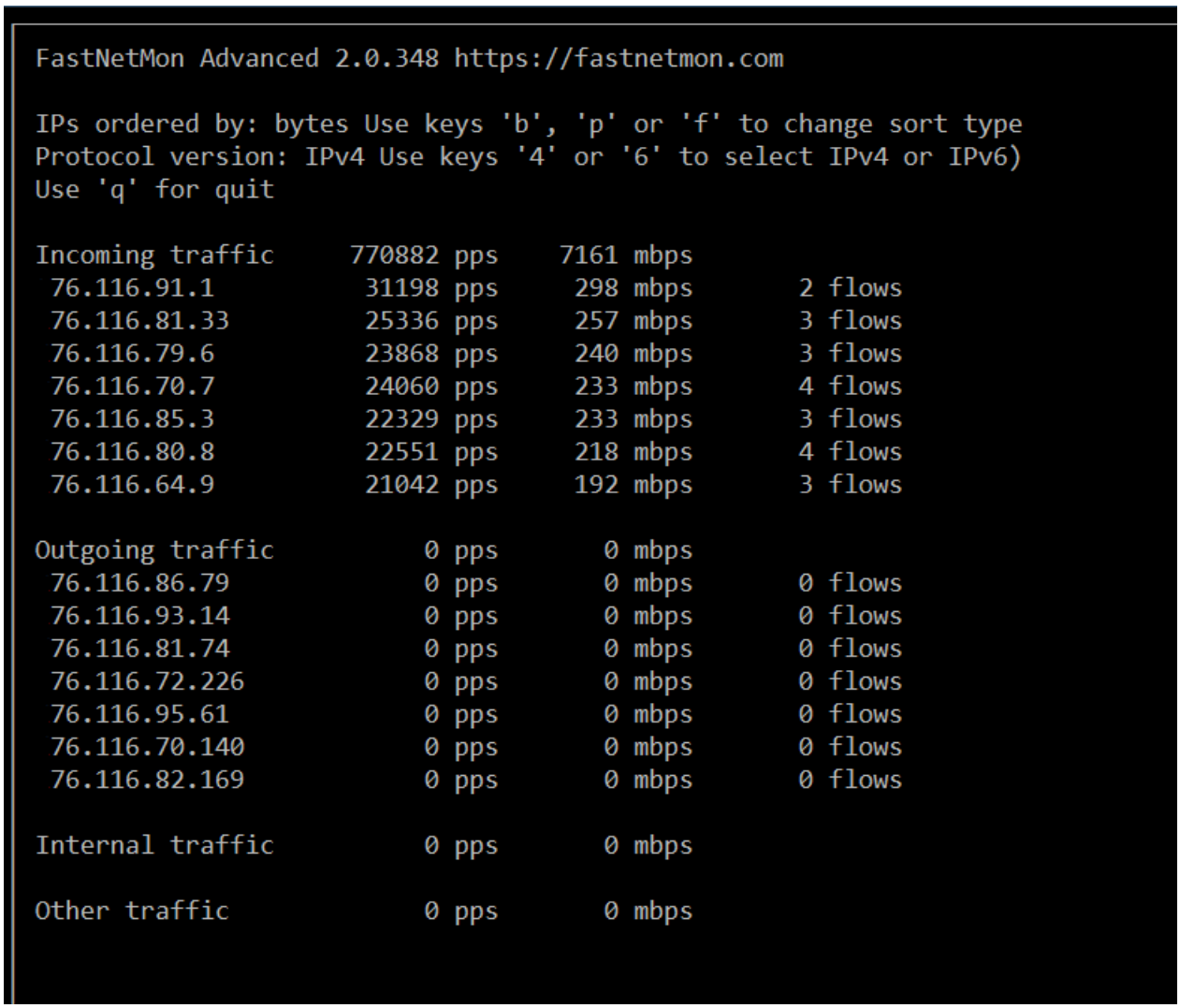


Рисунок 3.33 – Налаштування Fastnetmon

FastNetMon client відображає 7 (конкретне значення задається за допомогою параметра (max_ips_in_list) споживачів трафіку у вхідному та вихідному напрямку (рис.3.33).

Сортування здійснюється стандартно за кількістю пакетів, змінити це можна за допомогою параметра конфігурації sort_parameter (він може набувати значення packets, bytes, flows).

Крім інформації про вхідний та вихідний трафік відображається ще ряд полів:

• Internal traffic – трафік між нашими вузлами

• Other traffic – трафік, який ми не змогли ідентифікувати на факт приналежності

нашим мережам

• Total amount of IPv6 packets – загальна кількість зафіксованих IPv6 пакетів

• Total amount of not processed packets - загальна кількість пакетів, які з тим чи іншим причин не були розпізнані коректно (arp та інший службовий трафік не використовує протокол IP)

```
fcli create_configuration
fcli set main networks_list 61.230.198.0/23
fcli set main networks_list 76.116.64.0/19
fcli set main networks_whitelist 61.230.198.0/24
fcli set hostgroup global threshold_mbps 2000
fcli set hostgroup global threshold_pps 200000
fcli set hostgroup global enable_ban true
fcli set hostgroup global ban_for_bandwidth enable
fcli set hostgroup global ban_for_ip_fragments_bandwidth true
fcli set hostgroup global enable_ban_incoming enable
fcli set main enable_ban true
fcli set main per_direction_hostgroup_thresholds enable
fcli set main netflow_host 10.0.0.205
fcli set main netflow_ports 2055
fcli set main netflow on
fcli set main email_notifications_enabled true
fcli set main email_notifications_host mail.gt.net
fcli set main email_notifications_from fastnetmon@gt.net
fcli set main email_notifications_host mail.local
fcli set main email_notifications_username fastnetmon@gt.net
fcli set main email_notifications_password my-pass
fcli set main email_notifications_disable_certificate_checks true
fcli set main email_notifications_recipients admin@gt.net
```

Рисунок 3.34 – Файл конфігурації Fastnetmon

Налаштуємо аналіз лише вхідного трафіку (рис.3.34):
process incoming traffic = on
process_outgoing_traffic = off

Створення конфігурації:
fcli create_configuration

Налаштування мережевих списків:
fcli set main networks list 61.230.198.0/23
fcli set main networks_list 76.116.64.0/19

Встановлення білого списку мереж:
fcli set main networks_whitelist 61.230.198.0/24

Налаштування глобальної групи хостів:
fcli встановлює для групи хостів глобальний threshold_mbps 2000
fcli встановлює для групи хостів глобальний threshold_pps 200000
fcli встановити глобальну заборону групи хостів
fcli встановлює глобальну заборону групи хостів для ввімкнення пропускної здатності

fcli встановити глобальну заборону групи хостів для_ip_fragments_bandwidth true

fcli встановити глобальну групу хостів увімкнути ban_incoming увімкнути

Активація блокування:
fcli set main enable_ban true

Налаштування меж для групи хостів:
fcli set main per_direction_hostgroup_thresholds enable

Налаштування NetFlow:
fcli set main netflow host 10.0.0.205
fcli set main netflow ports 2055
fcli set main netflow on

Налаштування електронної пошти для сповіщення:
fcli встановлює main email_notifications_enabled true
fcli set main email_notifications_host mail.gt.net
fcli встановлює основні email_notifications_from fastnetmon@gt.net
fcli set main email_notifications_host mail.local
fcli встановлює основне ім'я_користувача email_notifications fastnetmon@gt.net
fcli set main email_notifications_password my-pass
fcli встановив main email_notifications_disable_certificate_checks true
fcli встановлює основні email_notifications_recipients admin@gt.net

Додаткове налаштування безпеки Apache на підприємстві (рис.3.35).

```
# ----------------------------------------------------------
<IfModule headers_module>
  # HSTS (mod_headers is required) (15768000 seconds = 6 months)
  Header always set Strict-Transport-Security "max-age=15768000"
  Header set X-XSS-Protection "1; mode=block"
  Header merge Cache-Control public env=!NO_CACHE
  <FilesMatch "\.cmd$">
    Header set Content-Disposition attachment
  </FilesMatch>
</IfModule>
# ----------------------------------------------------------
```

Рисунок 3.35 – Налаштування Apache

Цей скрипт Apache містить налаштування для модуля Headers. Нижче наведено пояснення для кожної команди:

<IfModule headers module>: Перевіряє, чи модуль headers включений.

Header always set Strict-Transport-Security “max-age=15768000”: Встановлює заголовок Strict-Transport-Security для встановлення політики HSTS (HTTP Strict Transport Security) на протязі 6 місяців (рис.3.36).

Header set X-XSS-Protection “1; mode-block”: Встановлює заголовок X-XSS-Protection для включення захисту від атак типу “Cross-Site Scripting” (XSS).

Header merge Cache-Control public env=INO_CACHE: Об'єднує та встановлює заголовок Cache-Control для керування кешуванням.

<FilesMatch “\.cmd$”>: Починає блок налаштувань, які застосовуються тільки до файлів, які відповідають шаблону “.cmd$”.

Header set Content-Disposition attachment: Встановлює заголовок Content-Disposition зі значенням “attachment” для файлів, що відповідають шаблону, щоб вказати браузеру обробляти їх як вкладення.

</FilesMatch>: Завершує блок налаштувань для визначених файлів.

</IfModule>: Завершує блок налаштувань, якщо модуль headers включений.

```
# ------------------------------------------------------------------------------------------------------
<VirtualHost 10.5.5.5:443>
        RewriteEngine On
        RewriteCond "%{HTTP_HOST}" "!^mail\.gt\.net" [NC] [OR]
        RewriteRule "^/?(.*)"      "https://mail.gt.net/$1" [R=301,L,NE]

        ServerName mail.gt.com
        ServerAdmin admin@gt.com
        DocumentRoot "/usr/local/www/data/roundcube"
        DirectoryIndex  index.php index.html index.htm

        SSLUseStapling on
        SSLStaplingResponderTimeout 5
        SSLStaplingReturnResponderErrors off

        SSLEngine on
        SSLCertificateFile    "/usr/local/etc/letsencrypt/live/mail.gt.com/fullchain.pem"
        SSLCertificateKeyFile "/usr/local/etc/letsencrypt/live/mail.gt.com/privkey.pem"

        Alias /roundcube/ "/usr/local/www/data/roundcube/"
        <Directory "/usr/local/www/data/roundcube">
            SetOutputFilter DEFLATE
            Options -Indexes -ExecCGI +FollowSymLinks
            AllowOverride All
            Require all granted
        </Directory>

        SetEnvIf Request_URI \.gif image-request
        SetEnvIf Request_URI \.jpg image-request
        SetEnvIf Request_URI \.png image-request
        SetEnvIf Request_URI \.ico image-request
        SetEnvIf Request_URI \.css image-request
        SetEnvIf Request_URI \.js  image-request
        SetEnvIf Request_URI \.woff  image-request
        SetEnvIf Request_URI \.woff2  image-request

        # Possible values include: debug, info, notice, warn, error, crit, alert, emerg.
        LogLevel notice core:info

        LogFormat "\"%{X-Forwarded-For}i\" \"%{Host}i\" %l %u %t \"%r\" %>s %b \"%{User-Agent}i\"" combined
        CustomLog "| /usr/local/sbin/cronolog  /var/log/apache/%Y/%m/%d/postfix-access.log" combined env=!image-request
        ErrorLog "/var/log/apache/vhost-err.log"

</VirtualHost>
# ------------------------------------------------------------------------------------------------------
```

Рисунок 3.36 – Налаштування Apache

Цей конфігураційний файл Apache VirtualHost містить налаштування для обробки HTTPS-запитів на порті 4435. Нижче наведено роз'яснення кожної команди (рис.3.37):

<VirtualHost 10.5.5.5:4435: Вказує на те, що ця конфігурація стосується віртуального хоста для адреси 10.5.5.5 на порті 4435.

RewriteEngine On: Увімкнення модуля перезапису.

RewriteCond %{HTTP_HOST} “mail\.gt\.net” [NC] [OR] RewriteRule “/(.*) “https://mail.gt.net/$1 [R=301,L,NE]: Перевірка, чи HTTP_HOST містить “mail.gt.net”. Якщо так, виконується правило перезапису для перенаправлення на HTTPS.

ServerName mail.gt.com: Вказує основне ім'я сервера для цього віртуального хоста.

ServerAdmin admin@gt.com: Вказує email адміністратора сервера.

DocumentRoot “/usr/local/www/data/roundcube”: Вказує кореневий каталог для віртуального хоста.

SSLEngine on: Увімкнення підтримки SSL для віртуального хоста.

SSLCertificateFile “/usr/local/etc/letsencrypt/live/mail.gt.com/fullchain.pem”: Вказує шлях до файла сертифіката SSL.

SSLCertificateKeyFile “/usr/local/etc/letsencrypt/live/mail.gt.com/privkey.pem”: Вказує шлях до файла ключа SSL.

Alias /roundcube/ “/usr/local/mm/data/roundcube/”: Встановлює аліас для шляху “/roundcube/”.

<Directory “/usr/local/www/data/roundcube”>: Вказує налаштування для директорії “/usr/local/www/data/roundcube”.

SetOutputFilter DEFLATE: Увімкнення стиснення вихідних даних.

Options Indexes ExecCGI FollowSymLinks: Встановлює опції для директорії.

AllowOverride All: Увімкнення використання файлу .htaccess.

Require all granted: Дозволяє доступ усім.

CustomLog “/usr/local/sbin/cronolog ErrorLog /var/log/apache/vhost-err.log”: Вказує шлях та формат лог-файлу помилок.

</VirtualHost>: Завершує блок конфігурації для віртуального хоста.

CustomLog /var/log/apache//in/d/postfix-access.log combined env=image-request: Вказує шлях та формат лог-файлу доступу для запитів до postfix, коли вони є image-request.

```
Listen 10.5.5.100:80

<VirtualHost 10.5.5.100:80>
        ServerName adm.local
        ServerAdmin admin@gt.net
        DocumentRoot "/usr/local/www/data/postfixadmin/public"
        DirectoryIndex  index.php index.html index.htm

        RewriteEngine on
        RewriteCond %{REMOTE_ADDR} !^10\.5\.5\.55
        RewriteCond %{REMOTE_ADDR} !^10\.5\.5\.70
        RewriteCond %{REMOTE_ADDR} !^10\.255\.0\.[0-9]{1,3}$
        RewriteRule ^(.*)$ https://mail.gt.com/ [r=301,L]

        Alias /postfixadmin/ "/usr/local/www/data/postfixadmin/public/"
        <Directory "/usr/local/www/data/postfixadmin">
            Options -Indexes +Includes +FollowSymLinks
            SetOutputFilter DEFLATE
            AllowOverride All
            Order allow,deny
            Allow from 10.5.5.55 10.5.5.70 10.255.0.
        </Directory>

        <ifmodule mod_expires.c>
                ExpiresActive On
                ExpiresByType image/gif "access plus 1 weeks"
                ExpiresByType image/png "access plus 1 weeks"
                ExpiresByType application/javascript "access plus 1 weeks"
                ExpiresDefault "access plus 3 days"
        </ifmodule>

        SetEnvIf Request_URI \.gif image-request
        SetEnvIf Request_URI \.jpg image-request
        SetEnvIf Request_URI \.png image-request
        SetEnvIf Request_URI \.css image-request
        SetEnvIf Request_URI \.js  image-request

        LogLevel error
        LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %v \"%{X-Forwarded-For}i\" \"%{Host}i\"" combined
        ErrorLog "/var/log/apache/vhost-err.log"
        CustomLog "| /usr/local/sbin/cronolog  /var/log/apache/%Y/%m/%d/postfix-access.log" combined env=!image-request
</VirtualHost>
```

Рисунок 3.37 – Налаштування Apache

Цей конфігураційний файл Apache має на меті обробку HTTP-запитів на порті 80 для хоста з IP-адресою 10.5.5.100. Нижче подано роз'яснення кожної команди:

Listen 10.5.5.100:80: Вказує Apache слухати на порту 80 для IP-адреси 10.5.5.100.

<VirtualHost 10.5.5.100:80>: Вказує початок конфігурації для віртуального хоста на IP-адресі 10.5.5.100 на порті 80.

ServerName ade.local: Встановлює ім'я сервера.

ServerAdmin admin@gt.net: Встановлює email адміністратора сервера.

DocumentRoot /usr/local/wow/data/postfixadmin/public”: Задає кореневий каталог для віртуального хоста.

DirectoryIndex index.php index.html index.htm: Вказує порядок виконання файлів індексу для директорії.

RewriteEngine on: Увімкнення модуля перезапису.

Alias /postfixadmin/ “/usr/local/www/data/postfixadmin/public/”: Встановлює аліас для шляху “/postfixadmin/”.

<Directory “/usr/local/wow/data/postfixadmin”>: Вказує налаштування для директорії “/usr/local/wow/data/postfixadmin”.

<IfModule mod_expires.c>: Перевірка, чи встановлений та ввімкнений модуль Expires.

ExpiresDefault “access plus 3 days”: Встановлює таймаут для застосування заголовку Expires до всіх файлів за замовчуванням.

SetEnvIf Request_URI \.gif image-request: Встановлює змінну оточення для запитів, які мають URI з розширенням .gif.

CustomLog “/usr/local/sbin/cronolog /var/log/apache//m/id/postfix-access.log combined env=image-request”: Вказує шлях та формат лог-файлу доступу для запитів до postfix, коли вони є image-request.

</VirtualHost>: Завершує блок конфігурації для віртуального хоста.

Налаштування безпеки локальної мережі (рис.3.38).

```
# ------------------------------------------------------
# -----          ACCESS FOR VLAN 20                -----
# ------------------------------------------------------
${cmd} table vlan-20 add 10.5.5.100            # Apache
${cmd} table vlan-20 add 10.5.20.1             # Server
${cmd} table vlan-20 add 10.5.50.5             # Base
${cmd} table vlan-20 add 10.5.5.10             # Exchange
${cmd} table vlan-20 add 10.5.5.91             # Canon
${cmd} table vlan-20 add 10.5.5.100            # Net Printer
# ------------------------------------------------------
# -----          ACCESS FOR VLAN 30                -----
# ------------------------------------------------------
${cmd} table vlan-30 add 10.5.5.100            # Apache
${cmd} table vlan-30 add 10.5.30.1             # Server
${cmd} table vlan-30 add 10.5.50.5             # Base
${cmd} table vlan-30 add 10.5.5.20             # Exchange
# ------------------------------------------------------
# -----          ACCESS FOR VLAN 100               -----
# ------------------------------------------------------
${cmd} table vlan-100 add 10.5.5.100           # Apache
${cmd} table vlan-100 add 10.5.5.1             # Server
${cmd} table vlan-100 add 10.5.50.5            # Base
${cmd} table vlan-100 add 10.5.5.30            # Exchange
# ------------------------------------------------------
# -----          ACCESS FOR VLAN 5                 -----
# ------------------------------------------------------
${cmd} table vlan-5 add 10.5.5.100             # Apache
${cmd} table vlan-5 add 10.5.5.1               # Server
${cmd} table vlan-5 add 10.5.50.7              #
${cmd} table vlan-5 add 10.5.5.40              # Exchange
# ------------------------------------------------------
# -----          ACCESS FOR VLAN 120               -----
# ------------------------------------------------------
${cmd} table vlan-120 add 10.5.5.100           # Apache
${cmd} table vlan-120 add 10.5.5.1             # Server
${cmd} table vlan-120 add 10.5.50.7            # Base
${cmd} table vlan-120 add 10.5.5.40            # Exchange
```

Рисунок 3.38 – Налаштування локальної мережі

Ці команди використовуються для внесення IP-адрес у таблиці для відповідних VLAN. Вони визначають, які IP-адреси мають право доступу до конкретних VLAN у вашій мережі. (рис.3.39).

```
#-------------------------------------------------------------------------------------------
#----                          ACCESS LOCAL INTERFACE
#-------------------------------------------------------------------------------------------
#---- ACCESS TO SWITCH ADM VLAN --------------
${cmd} add 1000 allow ip   from "table(vlan-adm)" to "table(vlan-adm)" via ${Inface2}
#---- ACCESS TO WAN --------------------------
${cmd} add 7010 allow ip   from 10.5.5.0/24    to "table(vlan-10)"      in via ${Inface10}
${cmd} add 7020 allow ip   from 10.5.20.0/24    to "table(vlan-20)"      in via ${Inface20}
${cmd} add 7030 allow ip   from 10.5.30.0/24    to "table(vlan-30)"      in via ${Inface30}
${cmd} add 7040 allow ip   from 10.5.5.0/24   to "table(vlan-100)"     in via ${Inface100}
${cmd} add 7050 allow ip   from 10.5.5.0/24   to "table(vlan-5)"     in via ${Inface5}
#---- ACCESS FROM WI_FI ----------------------
${cmd} add 7110 allow ip   from 192.168.1.0/24  to 192.168.1.0/24              via ${InfaceWiFi}
${cmd} add 7120 allow tcp  from 192.168.1.0/24  to 10.5.5.100 443           in via ${InfaceWiFi}
${cmd} add 7130 allow icmp from 192.168.1.0/24  to 10.5.5.100 icmptype 0,3,8 in via ${InfaceWiFi}
#---- ACCESS TO PRINTER ----------------------
${cmd} add 7200 allow ip   from 10.5.5.91     to 10.5.0.0/16         in via ${Inface5}
#---- DON'T CHANGE NUMBER RULES !!!!
${cmd} add 8010 allow ip   from 10.5.5.5     to "table(5-lan)" in via ${Inface10}
${cmd} add 8020 deny  ip   from 10.5.5.5 to not "table(5-wan)" in via ${Inface10}
#---- RFC DENY ROUTE -------------------------
${cmd} add 8110 deny  ip  from any to "table(deny-lan)" in via ${Inface10}
${cmd} add 8120 deny  ip  from any to "table(deny-lan)" in via ${Inface20}
${cmd} add 8130 deny  ip  from any to "table(deny-lan)" in via ${Inface30}
${cmd} add 8140 deny  ip  from any to "table(deny-lan)" in via ${Inface100}
${cmd} add 8170 deny  ip  from any to "table(deny-lan)" in via ${InfaceWiFi}
#---- FULL ACCESS ----------------------------
${cmd} add 8510 allow ip  from any to any via ${Inface10}
${cmd} add 8520 allow ip  from any to any via ${Inface20}
${cmd} add 8530 allow ip  from any to any via ${Inface30}
${cmd} add 8540 allow ip  from any to any via ${Inface100}
${cmd} add 8550 allow ip  from any to any via ${Inface5}
${cmd} add 8560 allow ip  from any to any via ${Inface120}
${cmd} add 8570 setfib 1  ip from  192.168.1.0/25  to any recv ${InfaceWiFi}
${cmd} add 8571 allow ip  from any to any via ${InfaceWiFi}
#----
${cmd} add 8900 deny log logamount 50 tcp from "table(acl-nat)" to any 21,22,25,137,138,139 out via ${Inetface}
${cmd} add 8999 skipto 20001 ip from "table(acl-nat)"  to any out via ${Inetface}
#-------------------------------------------------------------------------------------------
```

Рисунок 3.39 – Налаштування інтерфейсів

Ці команди призначені для конфігурації доступу до різних мережевих інтерфейсів та VLAN (Virtual Local Area Network). Нижче наведено роз'яснення кожної команди:

Доступ до локального інтерфейсу. Доступ до VLAN ADM (адміністративний).

$(cmd) add 1000 allow ip from “table(vlan-adm)” to “table(vlan-adm)” via $(Inface2)

Доступ до WAN.

$(cmd) додати 7010 дозволити ip

$(cmd) додати 7020 дозволити ip від 10.5.5.0/24 від 10.5.20.0/24 до “table(vlan-10)” до “table(vlan-20)” через $(Inface10)

$(cmd) додати 7030 дозволити ip з 10.5.30.0/24 через $(Inface30)

$(cmd) додати 7040 дозволити ip з 10.5.5.0/24 через $(Inface100)

$(cmd) додати 7050 дозволити ip з 10.5.5.0/24 до “table(vlan-30)” до “table(vlan-100)” через $(Inface5)

$(cmd) додати 7110 дозволити ip з 192.168.1.0/24 на 192.168.1.0/24 через $(InfaceWiFi)

$(cmd) додати 7120 дозволити tcp від 192.168.1.0/24 до 10.5.5.100 443 від 192.168.1.0/24 до 10.5.5.100 icmptype 0,3,8 in через $(InfaceWiFi)

$(cmd) add 7130 дозволити icmp через $(InfaceWiFi)

Доступ до принтера.

$(cmd) add 7200 allow ip from 10.5.5.91

Нумерація правил, яку не слід змінювати (1111).

$(cmd) add 8010 allow ip from 10.5.5.5

$(cmd) add 8020 deny ip from 10.5.5.5 to not “table(5-wan)” in via $(Inface10)

Відхилення маршрутів RFC.

$(cmd) додати 8110 deny ip з будь-якого до “table(deny-lan)” через $(Inface10)

$(cmd) додати 8120 deny ip from any до “table(deny-lan)” через $(Inface20)

$(cmd) додати 8130 deny ip from any до “table(deny-lan)” через $(Inface30)

$(cmd) додати 8140 deny ip з будь-якого до “table(deny-lan)” через $(Inface100)

$(cmd) додати 8170 deny ip з будь-якого до “table(deny-lan)” через $(InfaceWiFi)

Повний доступ

$(cmd) додати 8510 дозволити ip від будь-якого до будь-якого через $(Inface10)

$(cmd) додати 8520 дозволити ip

$(cmd) додати 8530 дозволити ip від будь-якого до будь-якого через $(Inface30)

$(cmd) додати 8540 дозволити ip від будь-якого до будь-якого через $(Inface100)

$(cmd) додати 8550 дозволити ip від будь-якого до будь-якого через $(Inface5)

$(cmd) add 8560 enable ip from 192.168.1.0/25 to any recv $(InfaceWiFi)

$(cmd) додати 8570 setfib 1

$(cmd) додати 8571 дозволити ip від будь-якого до будь-якого через $(InfaceWiFi)

$(cmd) add 8900 deny log logmount 50 tcp from “table(acl-nat)” to any 21,22,25,137,138,139 out через $(Inetface)

$(cmd) додати 8999 skipto 20001 ip з “table(acl-nat)” до будь-якого виходу через $(Inetface)

```
# ------------------------------------------------------
# -----                LOCAL DENIED                  -----
# ----- includes RESERVED-1, DHCP auto-configuration ----
# ----- NET-TEST, MULTICAST (class D), and class E) -----
# ------------------------------------------------------
${cmd} table deny-lan add 10.5.0.0/16
${cmd} table deny-lan add 192.168.0.0/16
${cmd} table deny-lan add 169.254.0.0/16
${cmd} table deny-lan add 172.16.0.0/12
${cmd} table deny-lan add 224.0.0.0/4
${cmd} table deny-lan add 240.0.0.0/4
# ------------------------------------------------------
```

Рисунок 3.40 – Налаштування заборонених IP адрес

Ці команди забороняють використання зазначених адресних просторів на локальному інтерфейсі, оскільки вони часто використовуються для різноманітних служб та функцій, які не повинні бути доступні або не використовуються в локальній мережі (рис.3.40).

Включає зарезервовані адресні простори, DHCP auto-configuration NET-TEST, MULTICAST (клас D) та клас E.

${cmd} table deny-lan add 10.5.0.0/16 # Додає адресний простір 10.5.0.0/16 для відхилення

$(cmd) table deny-lan add 192.168.0.0/16 # Додає адресний простір 192.168.0.0/16 для відхилення

$ {cmd} table deny-lan add 169.254.0.0/16 # Додає адресний простір 169.254.0.0/16 для відхилення

${cmd) table deny-lan add 172.16.0.0/12 # Додає адресний простір 172.16.0.0/12 для відхилення

$(cmd) table deny-lan add 224.0.0.0/4 # Додає адресний простір 224.0.0.0/4 для відхилення

$(cmd) table deny-lan add 240.0.0.0/4 # Додає адресний простір 240.0.0.0/4 для відхилення

3.4 Налаштування робочого місця

Налаштування Firewall.

Завантажили та відкрити файл cmd_fw_installer, знизу натиснули на опції-компоненти та залишили тільки COMODO Firewall (рис.3.41 – 3.42):

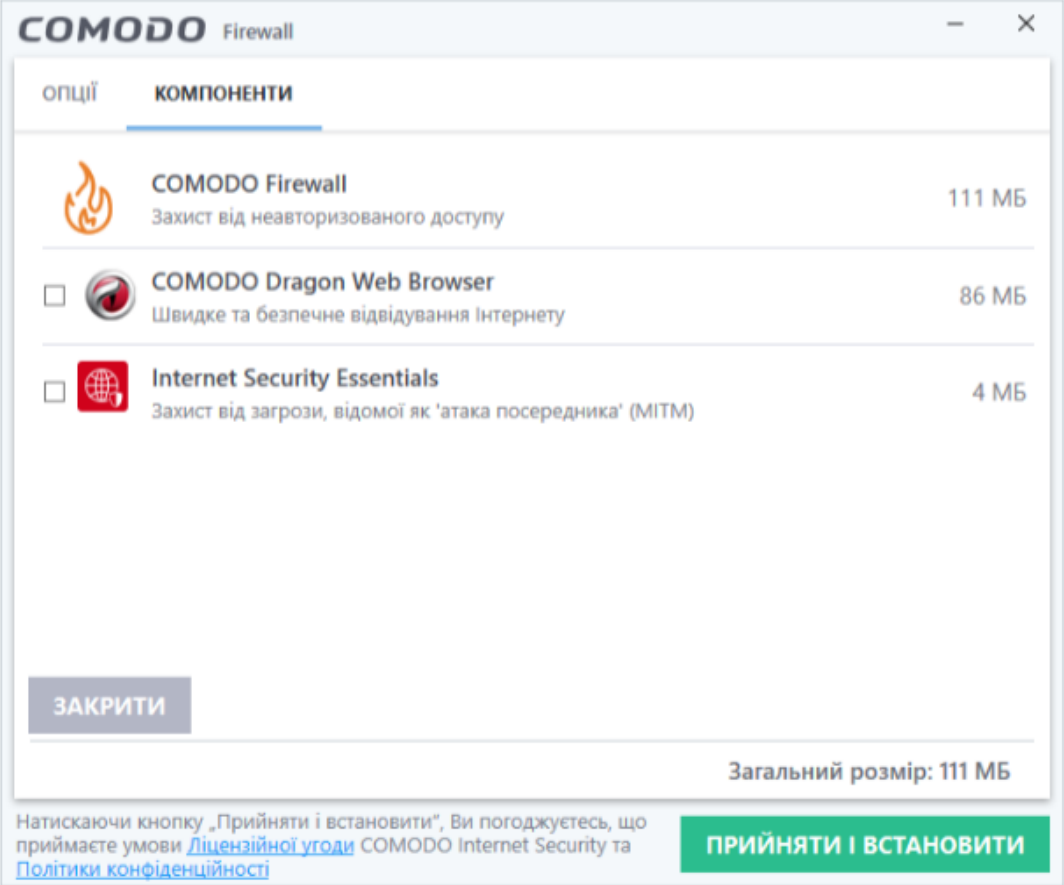


Рисунок 3.41 – Налаштування Firewall

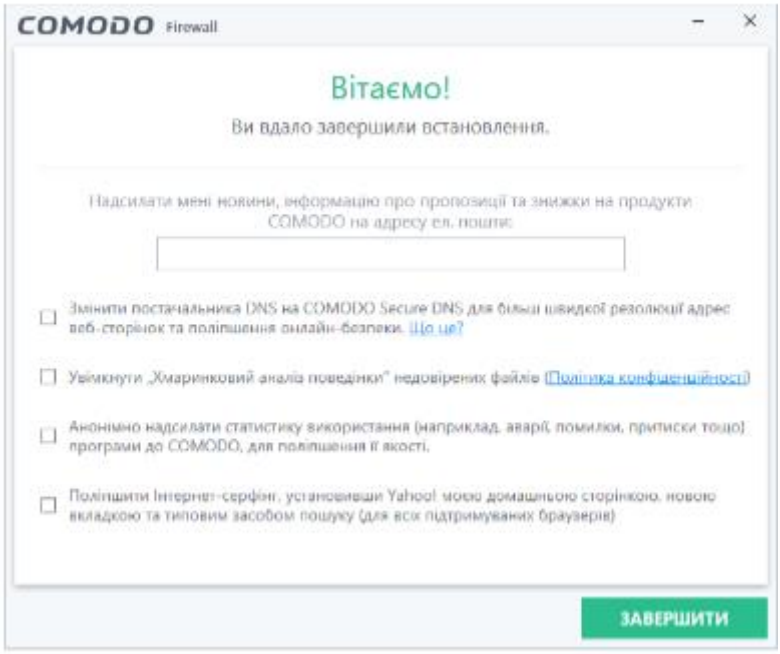


Рисунок 3.42 – Налаштування Firewall

Після встановлення, перейшли до розширених налаштувань та переконалися, що COMODO Firewall увімкнено (рис.3.43):

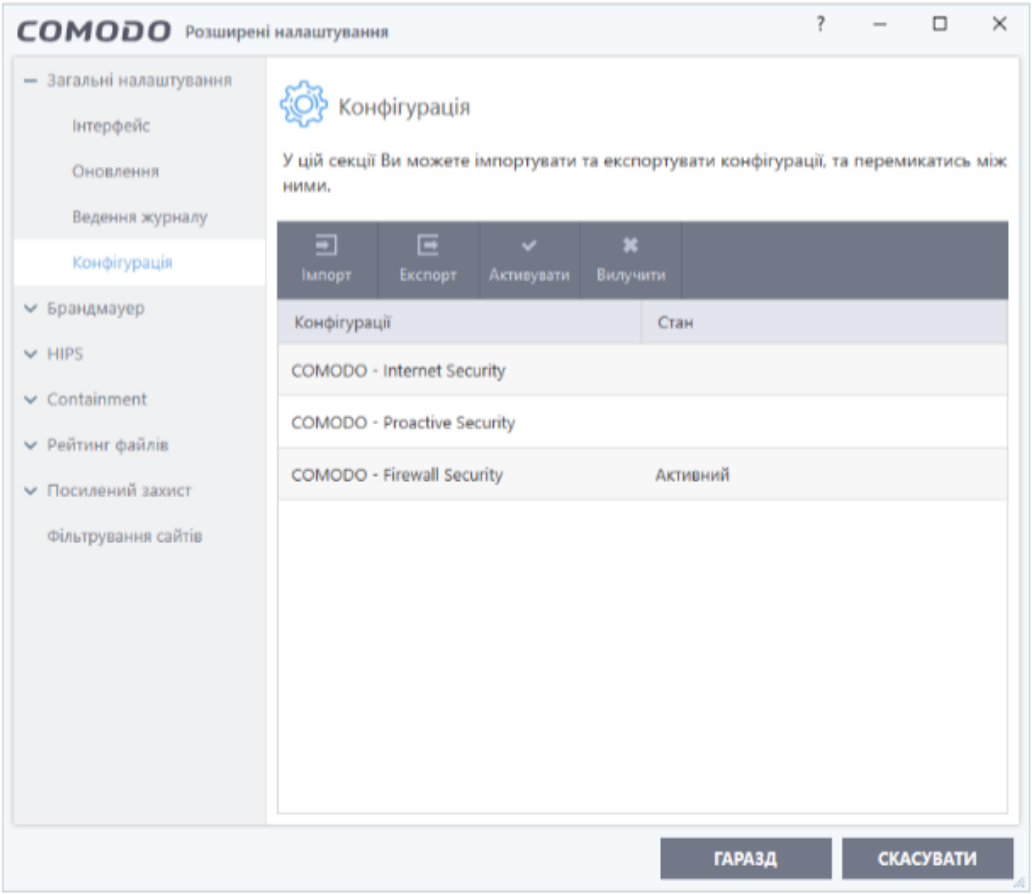


Рисунок 3.43 – Налаштування Firewall

У меню розширених налаштувань обрали Брандмауер та вибрали його налаштування (встановити Власні правила та відмітити маркери у полях) (рис.3.44):

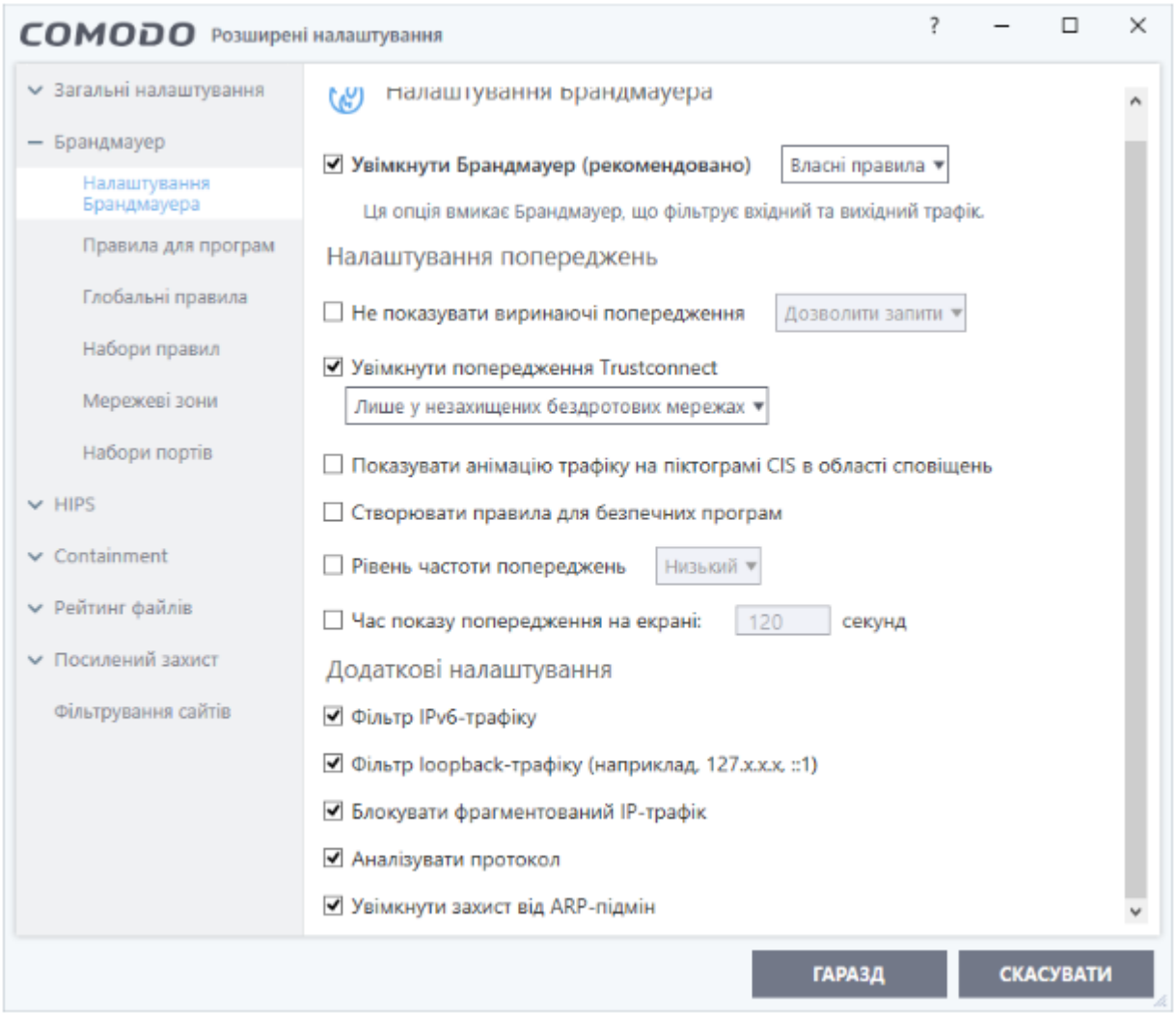


Рисунок 3.44 – Налаштування Firewall

Додали власні програми до списку правил (рис.3.45):

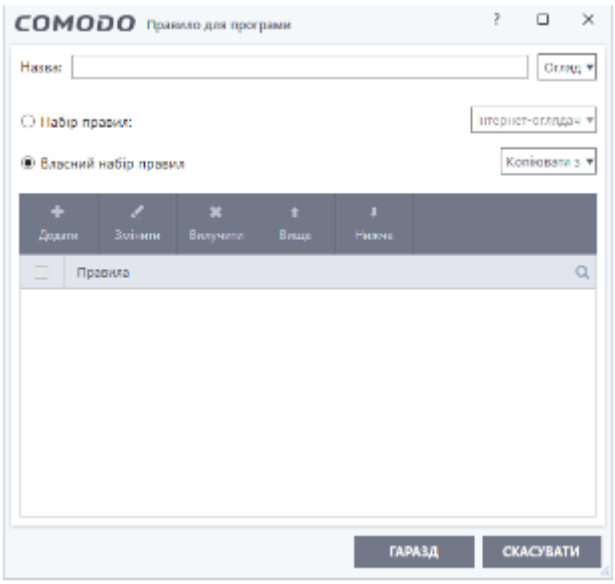


Рисунок 3.45 – Налаштування Firewall

Перевірили роботу систем безпеки (рис.3.46 – 3.47):

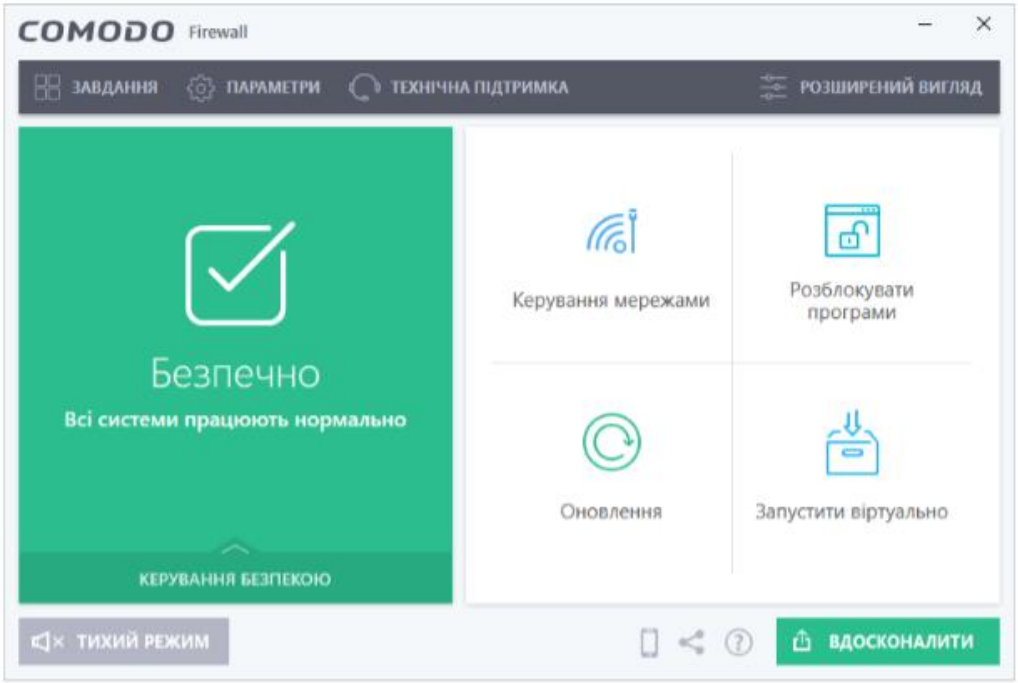


Рисунок 3.46 – Налаштування Firewall

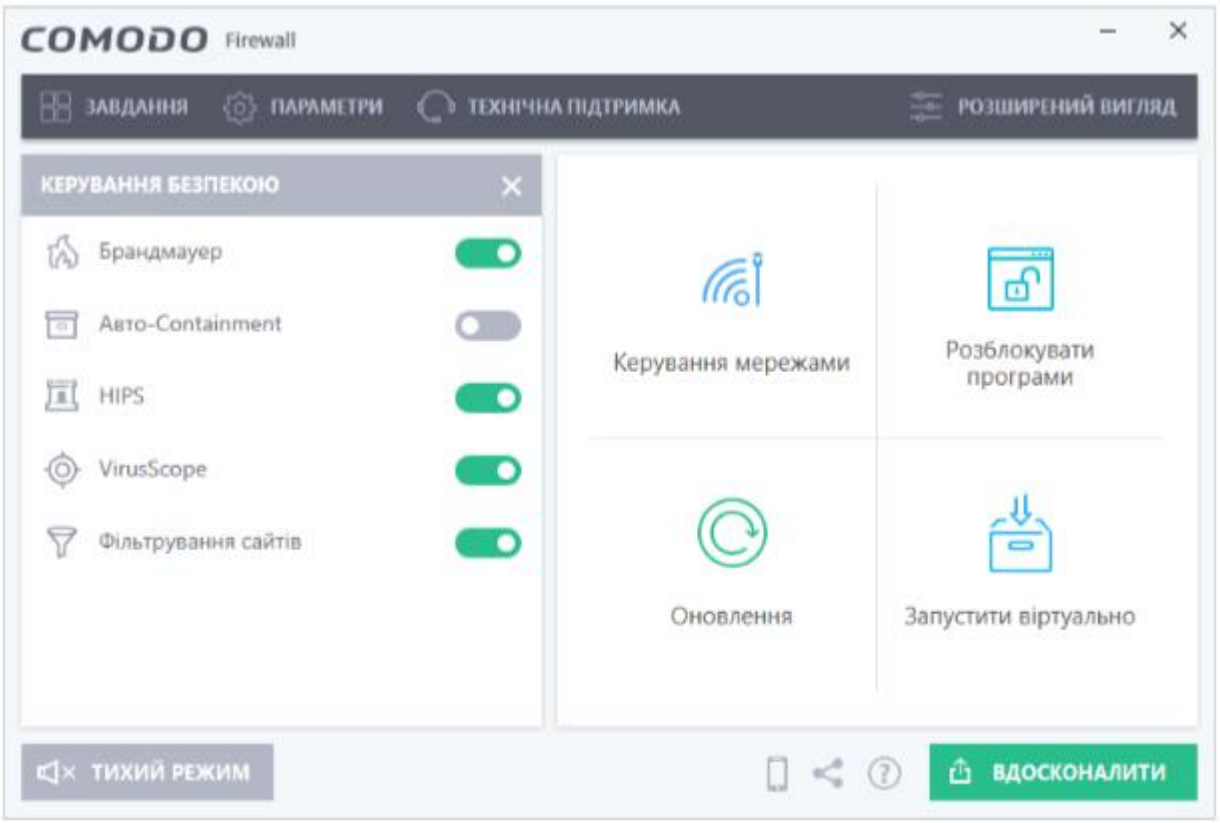


Рисунок 3.47 – Налаштування Firewall

Перевірили мережеву активність (рис.3.48):

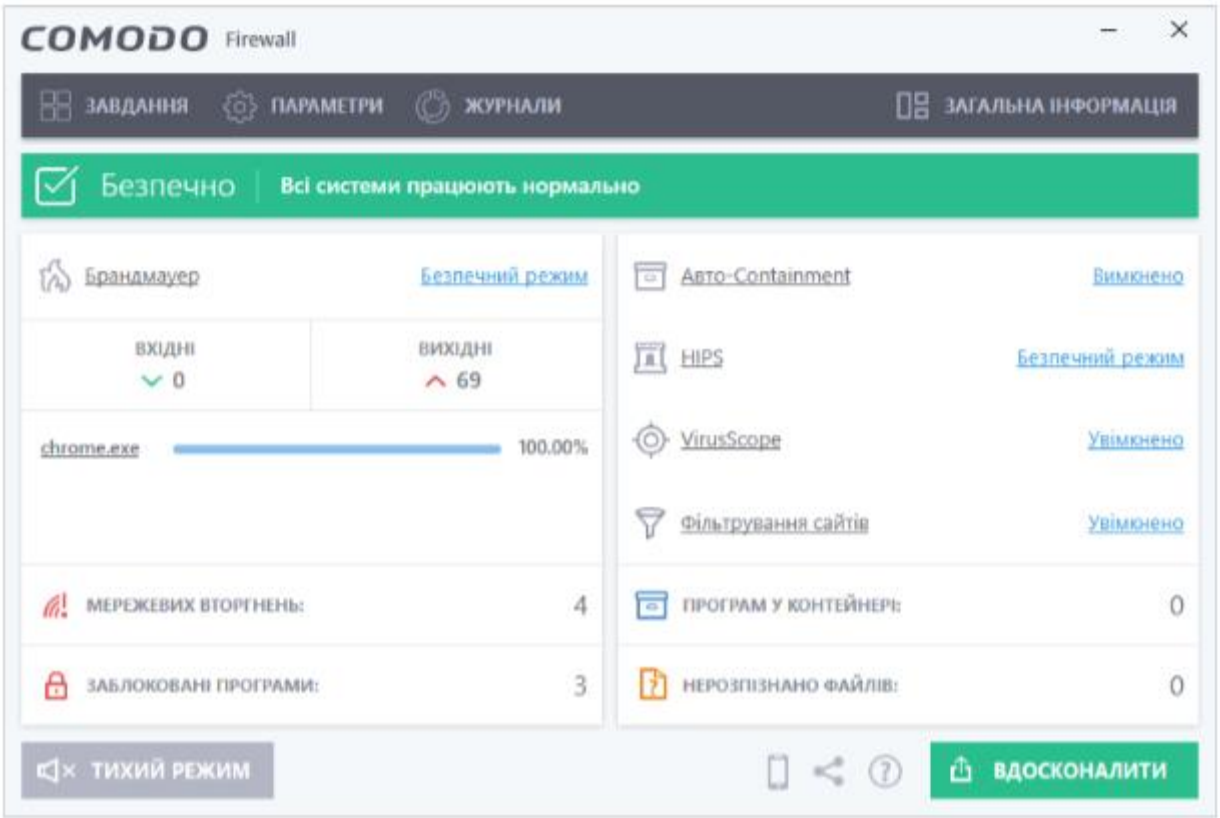


Рисунок 3.48 – Налаштування Firewall

На підприємстві використовуються як старі, так і нові моделі комп'ютерів, які відрізняються обсягом оперативної пам'яті. З цієї причини були придбані ліцензії на дві операційні системи: Windows 7 і Windows 10. Тож далі потрібно провести налаштування VPN IPsec l2tp у операційній системи Windows 7 та 10 (рис.3.49).

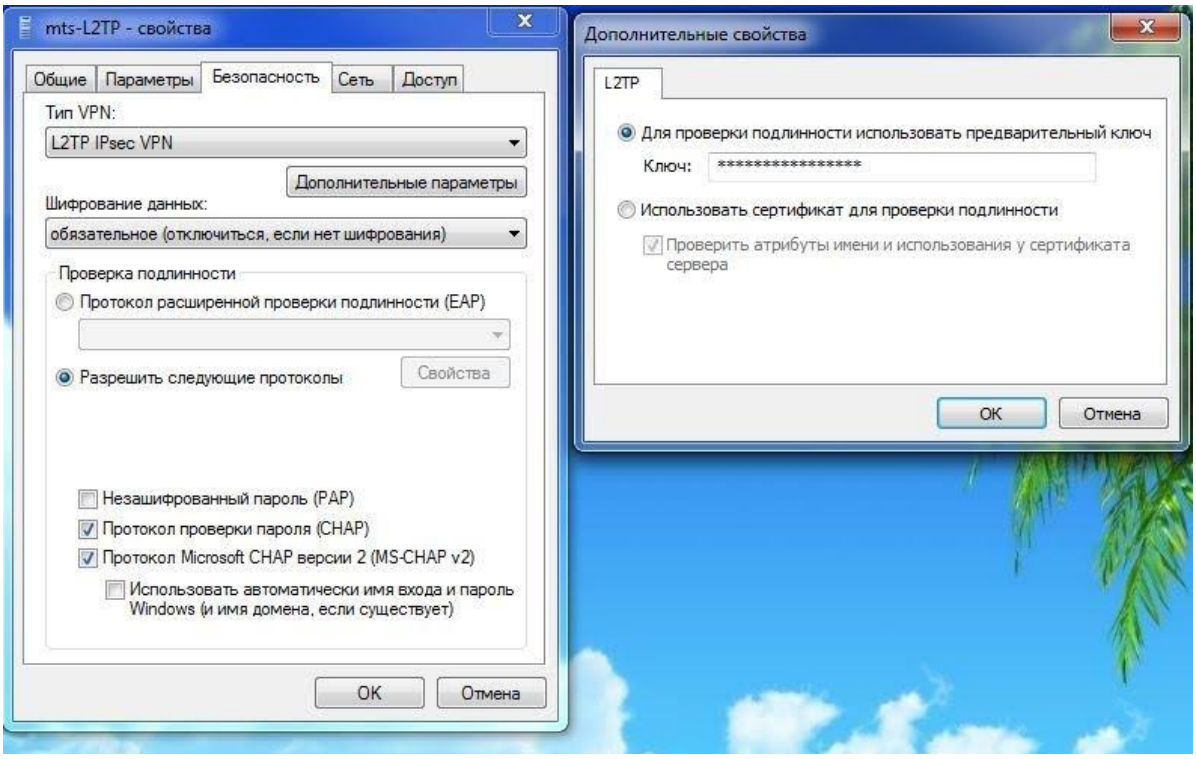


Рисунок 3.49 – Налаштування VPN в ОС Windows 7

3.5 Тестування обладнання та програмного забезпечення

Після налаштування тунелю VPN перевіримо підключення до маршрутизаторів за допомогою вінбокс через VPN (рис.3.50).

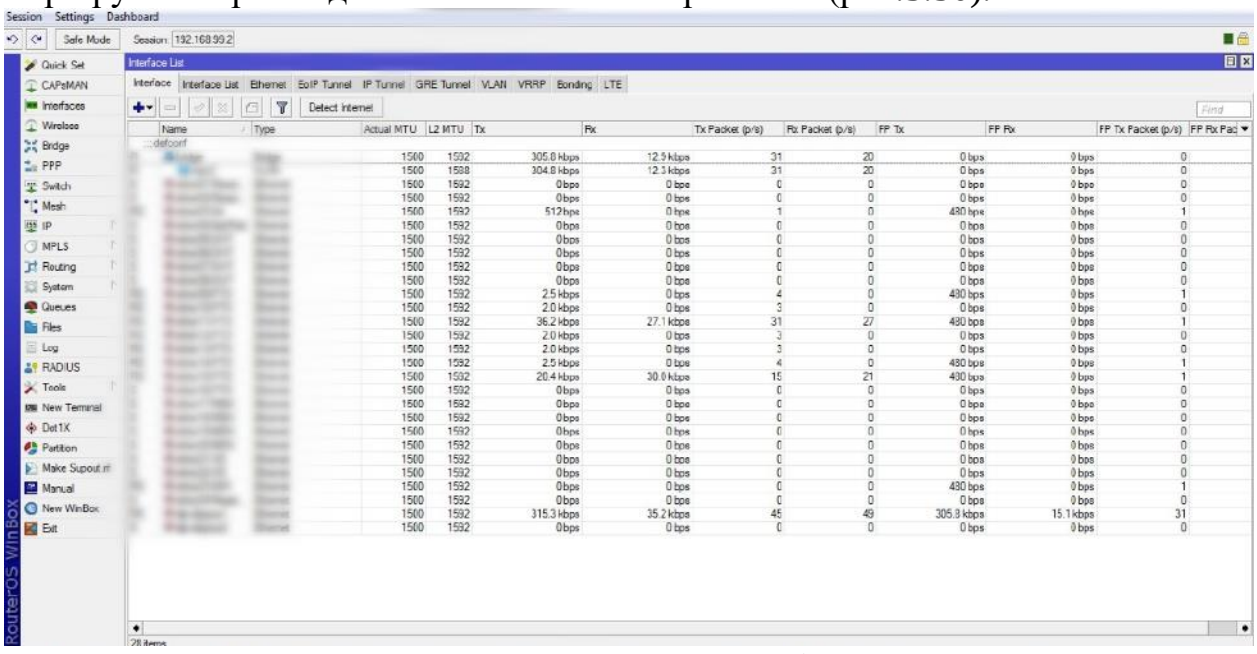


Рисунок 3.50 – Головний екран підключень

Перевірка з’єднання між вузлами комп’ютерної мережі за допомогою команди «ping» (рис.3.51 – 3.52).

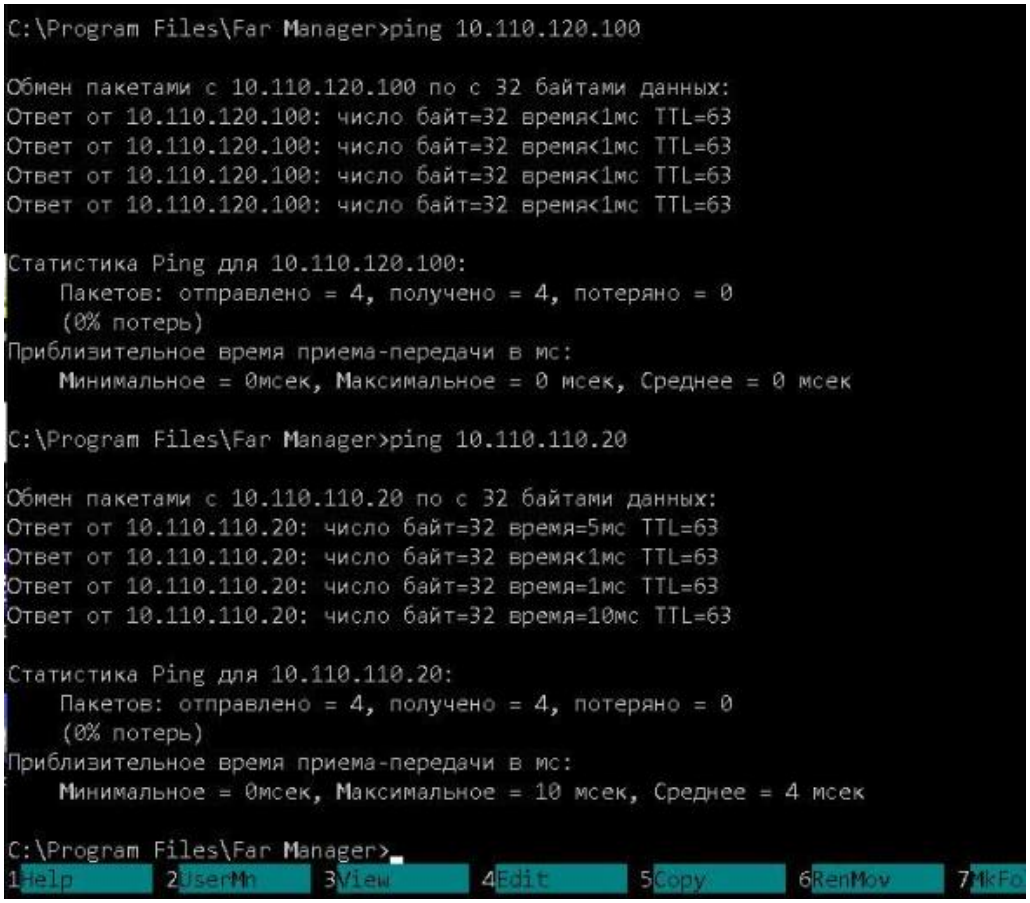


Рисунок 3.51 – Перевірка з’єднання з вузлом

Перевірка цілісності та якості з’єднання з сервером.

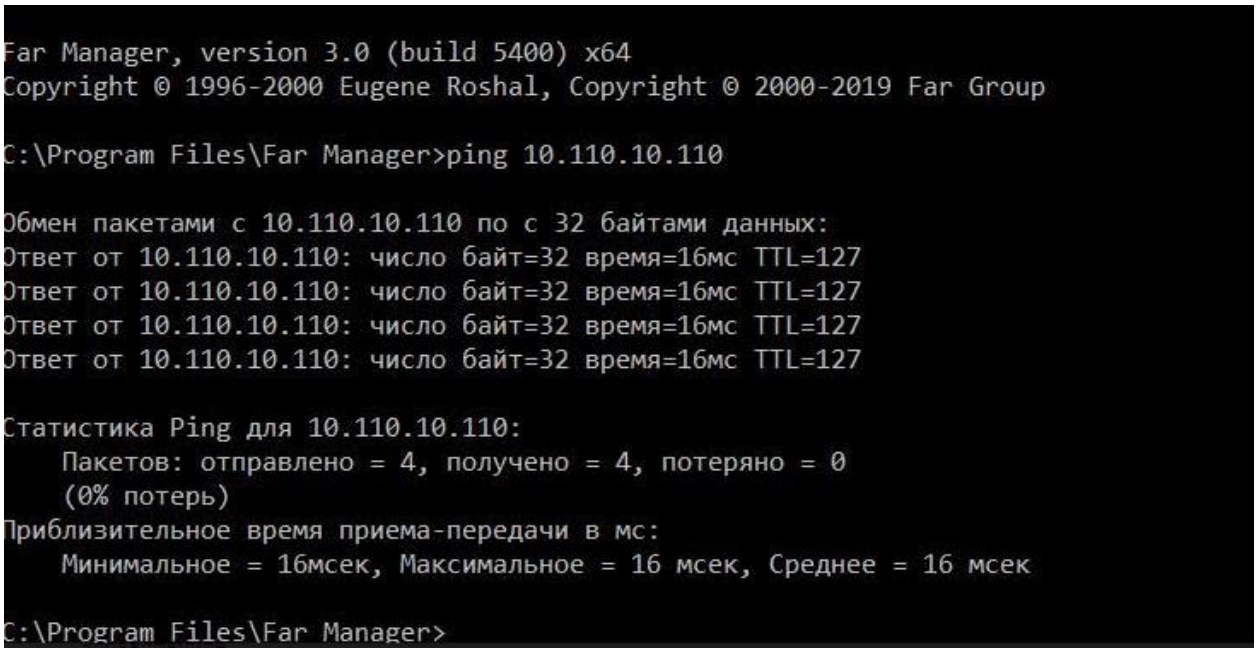


Рисунок 3.52 – З’єднання з сервером

Також, використовуючи диспетчер завдань, ми можемо спостерігати за тим, як змінилася завантаженість центрального процесора на сервері після модернізації обладнання під час виконання визначених завдань та цілей (рис.3.53).

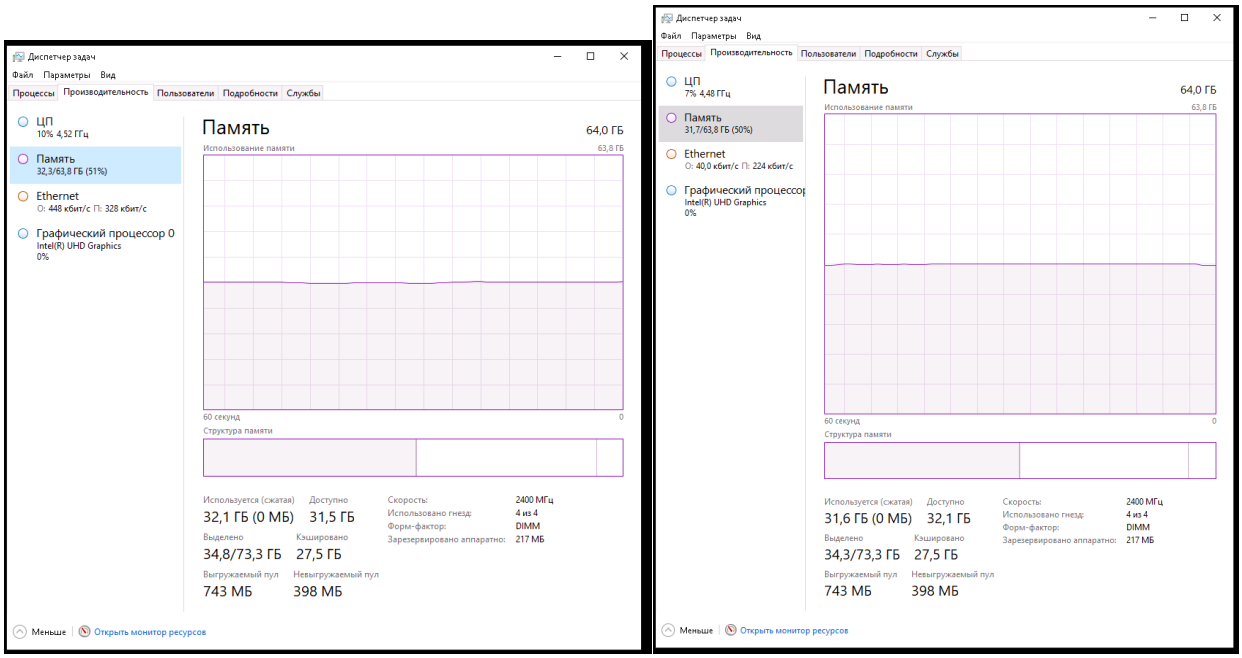


Рисунок 3.53 – Перевірка навантаження серверу

Наступним кроком для перевірки результату модернізації комп'ютерної мережі проведен SpeedTest, перевірка швидкості інтернету по кабелю та бездротове з'єднання (рис.3.54).

Рисунок 3.54 – Тест на швидкість Інтернет

У попередньому розділі було зазначено, що для підключення користувачів буде використано кабель типу вита пара зі швидкістю 100 мбіт.

Виходячи з рисунку (номер) бачимо швидкість Інтернет з’єднання, яка близька до обраного значення.

Нижче, на рисунку 3.55 після базового налаштування приведен «стан» бездротового з’єднання.

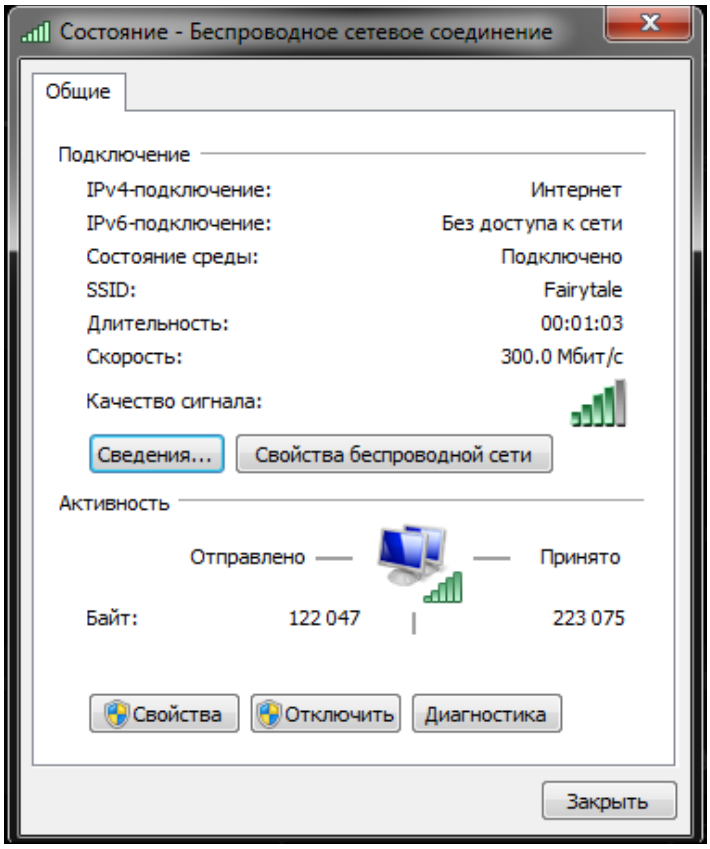


Рисунок 3.55 – Швидкість бездротового Інтернету

Висновки за розділом

У даному розділі проведено успішне моделювання комп'ютерної мережі в середовищі Packet Tracer, що дозволило визначити оптимальну архітектуру та структуру мережі для підприємства. Налаштування обладнання проведено з урахуванням вимог до безпеки та ефективності роботи мережі. Ретельно підібрані налаштування сприяють оптимальному функціонуванню обладнання. Проведені налаштування безпеки включають заходи з захисту мережевого трафіку, доступу до ресурсів та персональних даних. Це підвищує ступінь стійкості мережі до потенційних кіберзагроз. Розділ висвітлює важливість правильного налаштування робочих місць користувачів та Firewall для забезпечення безпеки та ефективності їхньої роботи в мережі. Завершальний етап розділу включає тестування обладнання та програмного забезпечення для виявлення можливих вразливостей та ефективності запланованих заходів забезпечення безпеки. Загальний висновок після розділу вказує на успішну модернізацію та забезпечення безпеки комп'ютерної мережі підприємства, враховуючи сучасні вимоги до кібербезпеки та оптимальної продуктивності. Виконані заходи гарантують стабільну та безпечну роботу інформаційної інфраструктури підприємства.

ВИСНОВКИ

У кваліфікаційній роботі магістра на базі оцінки технічних та економічних показників локальної мережі на підприємстві ТОВ «МетТрансСервіс», загальна площа території об’єкта аналізу становить 5 тис. кв. м., запропоновано захист модернізованої мережі.

Поставлені та виконані цілі кваліфікаційної роботи:

– огляд стандартів безпеки, видів атак та методу комплесного захисту мережі;

– пом’якшення загроз модернізованої лкм підприємства та кореляційний аналіз SIEM;

– моделювання, налаштування та тестування безпеки модернізованої комп’ютерної мережі.

Розглянуто, опрацьовано та створено 2 топології. У логічній топології описано пасивне та активне обладнання, спосіб з’єднання між собою. Фізична топологія характеризується розташуванням активним та пасивним обладнання у будівлі. Розглянули, розробили та налаштували програми для пом’якшення загроз та безпеки локальної комп’ютерної мережі підприємства. Кожен крок продемонстровано далі.

1) Проаналізовано ряд стандартів безпеки та видів атак зі встановленими заздалегідь критеріями вибору.

2) Складено специфікацію пом’якшення загроз та зроблено кореляційний аналіз SIEM,

3) Створено та протестовано модернізовану схему локальної комп’ютерної мережі у програмі PacketTracer.

4) Проаналізовано, обрано та налаштовано покроково з описом використовуваних команд програмне забезпечення на робочі станції та сервери, таких як DNS-, DHCP-, VPN-серверів в операційній системі FreeBSD, а також Firewall та Windows 7. Для перевірки результату налаштування зробили підключення до серверів та користувачів, проведено тест якості підключення та швидкості мережі Інтернет. Під час тестування мережі помилок не було виявлено.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) МетТрансСервіс. URL: https://www.mts-ua.com/#services (дата звернення: 11.11.2023).
2) NIST URL: https://sprinto.com/blog/nist-800-53-guide/- 800-53 (дата звернення: 29.10.2023).
3) DDOS-атаки. URL: https://www.weforum.org/agenda/2023/11/biggest-ddos-attack-cybersecurity-news-to-know-november-2023/ (дата звернення: 11.11.2023).
4) DDOS-атаки. URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (дата звернення: 11.05.2023).
5) Фішингова атака. URL: https://www.cloudflare.com/learning/access-management/phishing-attack/ (дата звернення: 11.11.2023).
6) Ping-атаки. URL:https://www.pearsonitcertification.com/articles/article.aspx?p=1151753&seqNum=2 (дата звернення: 11.11.2023).
7) Мережеві атаки. URL: https://networklessons.com/cisco/ccna-200-301/network-security-threats-vulnerabilities-and-countermeasures (дата звернення: 10.11.2023).
8) Мережеві атаки. URL: https://ipcisco.com/lesson/cyber-attacks-network-attacks/ (дата звернення: 10.11.2023).
9) Захист паролів. URL: https://www.weforum.org/agenda/2021/12/passwords-safety-cybercrime/ (дата звернення: 19.11.2023).
10) Мережі. URL: https://www.imperva.com/learn/data-security/iso-27001/ (дата звернення: 29.10.2023).- 27001
11) Види пом’якшення загроз. URL: https://www.cisco.com/c/en/us/products/security/what-is-threat-prevention.html#~how-threat-prevention-works (дата звернення: 15.11.2023).
12) SIEM URL: https://www.ibm.com/topics/siem (дата звернення: 15.11.2023).
13) ArcSight ESM https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm (дата звернення: 15.11.2023).
14) SIEM URL: https://www.ibm.com/topics/siem (дата звернення: 15.11.2023).
15) Кореляційний аналіз https://cdn.snau.edu.ua/moodle/mod/page/view.php?id=10970&lang=uk(дата звернення: 15.11.2023).
16) Класи IP-мереж. URL: https://web.posibnyky.vntu.edu.ua/fitki/3yarovijk_komp_merezhi/1.2.html (дата звернення: 06.11.2023).
17) DHCP. URL: https://docs.microsoft.com/ru-ru/windows-server/networking/technologies/dhcp/dhcp-top (дата звернення: 11.11.2023).
18) Налаштування DNS. URL: https://www.umgum.com/unbound (дата звернення: 18.11.2023).
19) Налаштування VPN. URL: https://habr.com/ru/post/250859/ (дата звернення: 20.11.2023).
20) Налаштування SIEM logz.io. URL: https://docs.logz.io/docs/user-guide/quick-start (дата звернення: 19.11.2023).

21) FastNetMoon. URL: https://docs.mitigator.ru/v22.06/integrate/fastnetmon/ (дата звернення: 19.11.2023).
22) Налаштування VLAN. URL: https://community.cisco.com (дата звернення: 08.11.2023).
23) DNS. URL: https://hostiq.ua/blog/ukr/how-does-dns-work/ (дата звернення: 13.11.2023).
24) Налаштування IPSec. URL: https://wiki.mikrotik.com/wiki/Manual:IP/IPsec# Identities (дата звернення: 19.11.2023).