

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

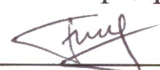
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Проектування комплексної системи захисту
інформаційно-телекомунікаційної інфраструктури
підприємства»

Виконав студент 2-го курсу групи КБм-22-1
спеціальності 125 «Кібербезпека»

 Б.С. Фальковський

Керівник старший викладач кафедри КІ та КБ

 О.А. Покотило

Рецензент доцент кафедри КІ та КБ, к.т.н., доцент

 Ю.М. Россінський

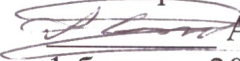
Житомир – 2023

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Фальковський Богдан Сергійович

Тема роботи: «Проектування комплексної системи захисту інформаційно-телекомунікаційної інфраструктури підприємства»

затверджена Наказом університету від 13 жовтня 2023 р. № 572/с

Термін здачі студентом закінченої роботи _____ 2023 р.

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

1. Розроблені технічні вимоги до проекту
2. Розроблена КСЗІ ІТС підприємства
3. Побудовані моделі порушника та загроз
4. Здійснено тестування КСЗІ

Обладнання та програмне забезпечення:

1. Міжмережевий екран PfSense
2. Комутатори MikroTik

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Шелуха О.О.		
2	Шелуха О.О.		
3	Шелуха О.О.		

Студент Б.С. Фальковський

Керівник О.А. Покотило

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Постановка задачі. Формулювання технічного завдання. Опрацювання літературних джерел.	13.10.23 - 14.10.23	Виконано
2	Проектування комплексної системи захисту інформації	14.10.23 - 16.10.23	Виконано
3	Налаштування проекту мережі та КСЗІ ІТС підприємства	17.10.23	Виконано
4	Тестування проекту	18.10.23 - 19.10.23	Виконано
5	Аналіз результатів	20.10.23 - 31.10.23	Виконано
6	Написання пояснювальної записки	01.11.23 - 05.11.23	Виконано
7	Підготовка презентації та виступу	25.11.23 - 15.12.23	Виконано
8	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	15.12.23 - 28.12.23	Виконано
9	Захист	29.12.23	Виконано

Студент Б.С. Фальковський

Керівник проекту О.А. Покотило

РЕФЕРАТ

Випускна кваліфікаційна робота магістра складається з проекту комплексної системи захисту інформації та пояснювальної записки. Пояснювальна записка до випускної роботи містить 58 сторінок, 20 ілюстрацій та 8 таблиць.

Метою роботи є забезпечення захисту інформації, що обробляється та зберігається в межах ІТС підприємства від несанкціонованого доступу, порушення конфіденційності, несанкціонованої модифікації, знищення та спостережності, а також забезпечення доступності зазначеної інформації.

В роботі визначено основні завдання для створення комплексної системи захисту інформації підприємства, проаналізовано інформацію котра буде використанна при створенні проекту. Представлено сценарій налаштування мережі, опис протоколів, зображено топології, які будуть використані протягом всієї роботи. Також наводяться результати тестування мережі.

КЛЮЧОВІ СЛОВА: КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, MIKROTIK, PFSENCE

ABSTRACT

The master's thesis consists of a project of a comprehensive information protection system and an explanatory note. The explanatory note to the final thesis contains 58 pages, 20 illustrations and 8 tables.

The purpose of the work is to ensure the protection of information processed and stored within the ITS of the enterprise from unauthorized access, breach of confidentiality, unauthorized modification, destruction and observation, as well as ensuring the availability of the specified information.

The work defines the main tasks for the creation of a comprehensive system of enterprise information protection, analyzes the information that will be used in the creation of the project. The scenario of setting up the network, the description of the protocols, and the topologies that will be used throughout the work are presented. The results of network testing are also given.

KEY WORDS: COMPLEX INFORMATION PROTECTION SYSTEM, MIKROTIK, PFSENCE

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП	8
РОЗДІЛ 1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІТС ПІДПРИЄМСТВА ТА УМОВИ ЇЇ ФУНКЦІОНУВАННЯ.....	11
1.1 Склад ІТС підприємства.....	11
1.2 Характеристика інформації, що обробляється.....	13
1.3 Технологія оброблення інформації в ІТС підприємства.....	19
РОЗДІЛ 2 ВИБІР КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ІТС ПІДПРИЄМСТВА А ТАКОЖ СТВОРЕННЯ МОДЕЛІ ПОРУШНИКА ТА МОДЕЛІ ЗАГРОЗ.....	25
2.1 Вимоги до КЗЗ ІТС підприємства	25
2.2 Опис операційних систем ІТС підприємства	27
2.3 Антивірусний захист.....	36
2.4 Опис моделі порушника безпеки інформації в підприємстві.....	37
2.5 Опис потенційних загроз інформації	40
РОЗДІЛ 3 ВПРОВАДЖЕННЯ КСЗІ, НАЛАШТУВАННЯ ТА ПЕРЕВІРКА РОБОТИ КОНФІГУРАЦІЇ	44
3.1 Приведення КСЗІ в дію	44
3.2 Налаштування мережі.....	45
ВИСНОВКИ.....	56
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	56
ДОДАТКИ.....	59

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АБ – адміністратор безпеки;

АРМ – автоматизоване робоче місце;

ІзОД – інформація з обмеженим доступом;

ЗІ – захист інформації;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ;

ОС – операційна система;

ПБ – політика безпеки;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

СА – системний адміністратор.

ВСТУП

Актуальність теми. Проект зі створення комплексної системи захисту інформації інформаційно-телекомунікаційної системи підприємства, призначеної для обробки конфіденційної інформації.

Створення комплексної системи захисту інформації інформаційно-телекомунікаційної системи (ІТС) підприємства, особливо при обробці конфіденційної інформації, є вкрай актуальною темою. Нижче наведено кілька ключових аргументів, що обґрунтовують цю актуальність:

1. Зростання кількості кіберзагроз, з кожним роком зростає кількість і складність кіберзагроз, спрямованих на підприємства. Атаки можуть бути спрямовані на викрадення конфіденційної інформації, шантаж, або навіть на руйнування роботи ІТС. [2] Створення ефективної системи захисту - це критичний крок для запобігання подібним загрозам.

2. Законодавчі вимоги та регуляції, законодавство щодо захисту персональних даних і конфіденційної інформації стає все більш суворим. Підприємства зобов'язані вживати заходів для забезпечення конфіденційності, цілісності та доступності інформації. Відповідність цим законодавчим нормам є необхідною, а система захисту інформації в цьому контексті стає ключовою.

3. Економічні витрати від кібератак, кібератаки можуть призвести до серйозних економічних втрат через втрату конфіденційної інформації, зупинку бізнес-процесів, штрафи за порушення законодавства, а також втрату довіри клієнтів та партнерів. Інвестування в систему захисту є невід'ємною частиною стратегії зменшення цих ризиків.

4. Зростання об'єму та значення інформації, інформація стає все важливішою для підприємств, особливо тієї, яка вважається конфіденційною. Зберігання, обробка та передача цієї інформації стає складнішою і ризикованою, вимагаючи високого рівня захисту.

5. Інновації та конкурентоспроможність, підприємства, які можуть гарантувати безпеку конфіденційної інформації, мають перевагу в очах клієнтів і партнерів. Захищена ІТС дозволяє підприємствам впевнено впроваджувати

інновації та залишатися конкурентоспроможними в швидкозмінюваному світі технологій.

Отже, створення комплексної системи захисту інформації ІТС підприємства є необхідним заходом для забезпечення безпеки, відповідності законодавству та збереження конкурентоспроможності в умовах сучасного бізнесу.

Об'єктом дослідження є інформаційно-телекомунікаційна система (ІТС) підприємства, яка обробляє конфіденційну інформацію. Це включає в себе всі аспекти, пов'язані з забезпеченням безпеки, цілісності та доступності конфіденційної інформації в рамках ІТС.

Методи дослідження:

1. Аналіз загроз і ризиків
2. Розробка стратегії захисту
3. Тестування на вразливість
4. Аудит безпеки

Практичне значення отриманих результатів:

1. Забезпечення безпеки конфіденційної інформації
2. Дотримання вимог законодавства
3. Збереження репутації підприємства
4. Ефективн використання ресурсів
5. Підвищення конкурентоспроможності

У кваліфікаційній роботі викладені основні технічні рішення, прийняті щодо організації та складу КСЗІ, принципів побудови та архітектури.[1]

За вмістом у роботі пропонується ряд інженерно-технічних та організаційних заходів, які повинні бути виконані на етапі створення та у процесі експлуатації КСЗІ.

Проект призначений для використання співробітниками підприємства.

При підготовці проекту використовувалися результати обстеження середовищ функціонування ІТС підприємства.

Метою кваліфікаційної роботи є забезпечення захисту інформації, що обробляється та зберігається в межах ІТС підприємства від несанкціонованого

доступу, порушення конфіденційності, несанкціонованої модифікації, знищення та спостережності, а також забезпечення доступності зазначеної інформації.

Для здійснення захисту інформації на всіх стадіях життєвого циклу ІТС підприємства у КСЗІ має бути передбачено застосування наступних заходів та засобів захисту інформації:

- організаційно-правові заходи, які реалізуються поза ІТС підприємства;
- інженерно-технічні заходи, що реалізуються поза обчислювальною системою ІТС підприємства;
- апаратні, програмно-апаратні та програмні несанкціонованого доступу (далі - НСД);
- забезпечення доступності інформації, що обробляється в ІТС підприємства.

Захист інформації повинен забезпечуватися на всіх технологічних етапах її обробки і в усіх режимах функціонування ІТС підприємства.

Предметом дослідження є створення комплексної системи захисту інформації інформаційно-телекомунікаційної системи підприємства, призначеної для обробки конфіденційної інформації.

Апробація результатів:

1. Фальковський Б.С., Байлюк Є.М., Вакалюк Т.А. Система запобігання вторгнень IPS // Тези доповідей V Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 01-02 грудня 2022 р. – Житомир: Житомирська політехніка, 2022.

2. Фальковський Б.С., Байлюк Є.М., Вакалюк Т.А. Модуль територіальних мереж(WAN EDGE) // Тези доповідей V Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 01-02 грудня 2022 р. – Житомир: Житомирська політехніка, 2022.

РОЗДІЛ 1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІТС ПІДПРИЄМСТВА ТА УМОВИ ЇЇ ФУНКЦІОНУВАННЯ

1.1 Склад ІТС підприємства

Інформаційно-телекомунікаційна система (ІТС) підприємства представляє собою комплекс технічних та програмних рішень, які забезпечують обробку, зберігання та передачу інформації. Важливо визначити різноманітні види інформації, що обробляються в межах цієї системи. Оскільки мета ІТС полягає в підтримці бізнес-процесів, прийнятті управлінських рішень та забезпеченні ефективного функціонування підприємства. Для досягнення цих цілей система обробляє інформацію різних типів та категорій.

До складу обчислювальної системи ІТС підприємства входять:

- АРМ зі стандартними засобами введення, накопичення та відображення інформації (клавіатура, маніпулятор типу «миша», дисководи та CD - приводи, жорсткий диск, монітор, порти введення - виведення інформації тощо);
- Сервери для функціонування прикладного ПЗ та збереження даних;
- Активне мережеве обладнання для організації локальної мережі та доступу до мережі Інтернет - D-Link, TP-Link[7], MikroTik;
- периферійні пристрої для введення, виведення та накопичення інформації (принтери, сканери, пристрої зовнішньої пам'яті і таке інше);
- системне ПЗ (ОС Microsoft Windows та драйвери периферійних пристроїв) під управлінням якого працюють АРМ та сервери - ОС Microsoft Windows 10 Professional[13], Microsoft Windows 7, Microsoft Windows Server 2019;
- антивірусне ПЗ - ESET NOD 32 Antivirus;[6]

Під час створення КСЗІ ІТС підприємства необхідно було спиратися на міжнародні стандарти. Найголовнішим з яких був, ISO/IEC 27001:2013.[16] Це міжнародний стандарт, що визначає вимоги до комплексної системи захисту інформації. Він описує, як встановити, впровадити, підтримувати та постійно вдосконалювати КСЗІ в організації.

Використання ISO/IEC 27001:2013 в ІТС підприємства може забезпечити:

Захист інформації: Стандарт допомагає захистити конфіденційність, цілісність та доступність інформації в ІТС.

Відповідність нормативним вимогам: Дотримання ISO/IEC 27001:2013 може допомогти підприємствам відповідати вимогам законодавства та нормативних актів, що стосуються інформаційної безпеки.

Підвищення довіри: Впровадження СУІБ на основі ISO/IEC 27001:2013 може підвищити довіру клієнтів, партнерів та інших зацікавлених сторін до ІТС підприємства.

Зниження ризиків: Стандарт допомагає ідентифікувати, оцінювати та управляти ризиками, пов'язаними з інформаційною безпекою.

Основні компоненти ISO/IEC 27001:2013:

Політика інформаційної безпеки: Визначає загальні цілі та зобов'язання підприємства щодо інформаційної безпеки.

Процедури управління інформаційною безпекою: Описують, як підприємство буде впроваджувати та контролювати заходи інформаційної безпеки.

Контроль інформаційної безпеки: Заходи, які використовуються для захисту інформації.

Заходи управління ризиками: Процеси, які використовуються для ідентифікації, оцінки та управління ризиками, пов'язаними з інформаційною безпекою.

Моніторинг, вимірювання, аналіз та вдосконалення: Процеси, які використовуються для моніторингу ефективності СУІБ та її постійного вдосконалення.

Впровадження ISO/IEC 27001:2013 в ІТС підприємства може бути складним завданням, але воно може принести значні переваги.

Ось кілька порад щодо впровадження ISO/IEC 27001:2013 в ІТС:

Отримайте підтримку керівництва: Важливо, щоб керівництво підприємства підтримувало впровадження ISO/IEC 27001:2013.

Проведіть оцінку ризиків: Визначте ризики, пов'язані з інформаційною безпекою в ІТС.

Розробіть політику та процедури інформаційної безпеки: Визначте, як підприємство буде захищати інформацію.

Впровадьте контролі інформаційної безпеки: Застосуйте заходи для захисту інформації.

Навчіть персонал: Навчіть персонал основам інформаційної безпеки.

Моніторте та переглядайте СУІБ: Регулярно переглядайте СУІБ, щоб переконатися, що вона відповідає потребам підприємства.

ISO/IEC 27001:2013 – це потужний інструмент, який може допомогти підприємствам захистити інформацію в ІТС.

1.2 Характеристика інформації, що обробляється

Інформаційно-телекомунікаційні системи (ІТС) відіграють важливу роль в сучасних підприємствах. Вони дозволяють автоматизувати бізнес-процеси, обробляти великі обсяги даних, приймати кращі управлінські рішення та підвищувати конкурентоспроможність.

Інформація ІТС підприємства являє собою сукупність інформації електронних документів, представлених у вигляді структурних компонентів файлової системи (файлів).

До основних видів інформації, що обробляється в ІТС підприємства, відносяться:

Функціональна інформація: кадрова, бухгалтерська, звітна, статистична, маркетингова, виробнича, логістична.

Технологічна інформація: журнали реєстрації подій, параметри конфігурування системи, системні дані.

Інформація про персонал: персональні дані співробітників, кадрові документи, табелі обліку робочого часу.

Інформація про клієнтів: контактні дані, історія замовлень, листування.

Інформація про партнерів: контактні дані, договори, умови співпраці.

Фінансова інформація: бухгалтерська звітність, бюджети, платіжні документи.

Інформація про продукти та послуги: характеристики, ціни, склад, описи.

Інформація, що циркулює в ІТС підприємства:

- за порядком доступу:
 - у відповідності до положень ст.20 Закону України «Про інформацію» - відкрита;
 - у відповідності до положень до вмісту переліку інформації, що підлягає автоматизованому обробленню в ІТС підприємства – «конфіденційна» (персональні дані);
- за правом власності: в тлумаченні п. 1 ст. 1 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» - належить до державних інформаційних ресурсів;
- за призначенням:
 - функціональна (кадрова, статистична, звітна, персональні дані);
 - технологічна (БД КЗЗ, журнали реєстрації подій ПЗ та КЗЗ, параметри конфігурування системи).

Важливою задачею є захист інформації, що обробляється в ІТС підприємства, від несанкціонованого доступу, використання, розкриття, порушення цілісності та знищення. Для цього використовуються різні методи та засоби захисту, такі як:

Організаційні заходи: політика інформаційної безпеки, інструкції, навчання персоналу.

Технічні заходи: антивірусний захист, фаєрволи, шифрування даних, системи резервного копіювання.

Інформація, що обробляється в ІТС підприємства, є важливим активом, який потребує захисту. Забезпечення інформаційної безпеки дозволяє підприємству мінімізувати ризики, пов'язані з втратою або розкраданням даних, а також збоями в роботі ІТС.

Програмне забезпечення відіграє важливу роль у сфері оброблення інформації на підприємствах. У цьому розділі розглянемо значення та функції програмного забезпечення в контексті інформаційно-технологічних систем.

Програми для оброблення інформації допомагають в організації та оптимізації бізнес-процесів. Вони включають в себе системи управління базами даних, програми аналізу даних, інструменти візуалізації і засоби автоматизації рутинних завдань.

Програмне забезпечення також грає ключову роль у забезпеченні безпеки інформації. Засоби криптографії, системи моніторингу та захисту від зловмисниць допомагають підприємствам забезпечувати конфіденційність і цілісність своїх даних.

З розвитком технологій з'являються нові програмні продукти, які включають в себе штучний інтелект та машинне навчання. Це відкриває нові можливості для аналізу великих обсягів даних та прийняття більш обґрунтованих стратегічних рішень.

У даному розділі ми розглянемо роль програмного забезпечення в обробленні інформації та його внесок у вдосконалення функціонування інформаційно-технологічних систем підприємства.

Завдання оброблення інформації на підприємствах супроводжується рядом викликів та перспектив, які визначають динаміку цього процесу. У цьому розділі розглянемо основні проблеми та тенденції, що впливають на сферу оброблення інформації в інформаційно-технологічних системах (ІТС) підприємств.

Один із викликів - це безпека інформації. Зі зростанням кількості та складності кіберзагроз, підприємства повинні надавати особливу увагу заходам кібербезпеки, щоб запобігти несанкціонованому доступу та втратам даних.

Іншим важливим аспектом є впровадження новітніх технологій, таких як штучний інтелект, для оптимізації оброблення інформації. Це може вимагати значних інвестицій та перепідготовки персоналу, але в той же час відкриває нові можливості для підвищення продуктивності та точності оброблення даних.

Перспективи розвитку оброблення інформації включають в себе розширення використання хмарних технологій, що дозволяє підприємствам зберігати та обробляти великі обсяги даних без значних витрат на обладнання.

Завдяки постійному розвитку технологій та вдосконаленню стратегій оброблення інформації, підприємства можуть ефективно працювати в умовах постійної зміни та високої конкуренції. У цьому розділі буде розглянуто важливі виклики та перспективи, які впливають на оброблення інформації в ІТС підприємства.

У цьому розділі надаються рекомендації, спрямовані на оптимізацію процесів оброблення інформації в інформаційно-технологічних системах (ІТС) підприємства.

Стратегія кібербезпеки є ключовою для захисту важливої інформації від потенційних загроз.

Оптимізація хмарних технологій може сприяти зниженню витрат та підвищенню доступності інформації.

Впровадження технологій штучного інтелекту та автоматизації сприяє підвищенню ефективності оброблення інформації.

Навчання персоналу є важливим елементом для ефективного використання нових технологій та програмного забезпечення.

Стратегія інтеграції систем дозволяє отримувати комплексну інформацію за допомогою взаємодії різних систем та джерел даних.

Моніторинг та аналіз продуктивності допомагають постійно вдосконалювати процеси оброблення інформації.

Розробка стратегії розвитку інформаційно-технологічних систем враховує технологічні та бізнес-тренди, сприяючи стійкому розвитку.

Ці рекомендації становлять комплексний підхід до оптимізації оброблення інформації та допомагають підприємствам утримувати конкурентну перевагу в сучасному бізнес-середовищі.

До інформації ІТС підприємства, що підлягає захисту, відноситься також загальне, функціональне та спеціальне ПЗ ІТС підприємства.

Інновації в обробленні інформації можуть значно покращити ефективність та результативність підприємства.

Використання передових технологій, таких як штучний інтелект та машинне навчання, сприяє автоматизації процесів та покращує якість оброблення даних.

Впровадження інноваційних підходів до аналізу даних може розкрити нові можливості для виявлення тенденцій та формування стратегічних рішень.

Спрощення рутинних завдань через інноваційні технології дозволяє персоналу зосередитися на більш складних та стратегічних аспектах діяльності.

Забезпечення гнучкості та адаптивності інформаційних систем до нових вимог бізнесу є ключовим аспектом інновацій.

Впровадження інновацій у процес оброблення інформації стає стратегічним кроком для підприємства, щоб забезпечити йому конкурентоспроможність та стійкість у динамічному світі бізнесу.

Безпека даних є одним із основних викликів, оскільки із зростанням кількості та складності кіберзагроз збільшується ймовірність порушення конфіденційності та цілісності інформації.

Використання новітніх технологій, хоча й є перевагою, може викликати труднощі у впровадженні через високі витрати та необхідність перепідготовки персоналу.

Недостатня гнучкість інформаційних систем може призвести до труднощів у впровадженні нових стратегій та швидкого реагування на зміни в бізнес-середовищі.

Ризик втрати даних через технічні або людські помилки завжди стоїть перед підприємством, вимагаючи надійних заходів з резервного копіювання та відновлення.

Сприйняття нових технологій персоналом може викликати опір та потребу у систематичному навчанні.

У таблиці 1.1 вказано тип її логічного та фізичного представлення.

Характеристика циркулюючої інформації в ІТС підприємства

№	Інформація	Логічне представлення	Фізичне представлення	Місце зберігання
Відкрита інформація				
1	Загальне, функціональне та спеціальне програмне забезпечення	Програмний засіб	Файл	НЖМД АРМ та серверів
2	Програмні засоби захисту	Програмний засіб	Файл	НЖМД АРМ та серверів
3	Дистрибутиви ПЗ, у тому числі ПЗ захисту	Дистрибутив	Файл	DVD-ROM, НЖМД АРМ та серверів
4	Документи, які містять відкриту інфомаці.	Текстовий документ, електронна таблиця	Файл	НЖМД АРМ та серверів та/або змінні диски
Конфіденційна інформація				
5	Документи з ІзОД	Текстовий документ, електронна таблиця, графічні документи	Файл	НЖМД серверів
6	Дані захисту	Бази облікових записів, журнал реєстрації, параметр конфігурації системи	Файл, параметр системного реєстру	НЖМД
7	Резервні копії даних захисту	Бази облікових записів, текстовий документ, журнал реєстрації	Файл	НЖМД
Технологічна інформація				
8	Дані захисту	Списки користувачів з їхніми атрибутами доступу, журнал реєстрації подій, параметри конфігурації КЗЗ та ін	Файл, параметр системного реєстру	НЖМД серверів та АРМ адміністраторів, АМО
9	Резервні копії даних захисту	Списки користувачів з їхніми атрибутами доступу, журнал реєстрації подій, параметри конфігурації КЗЗ та ін	Файл	ЗНІ

Збереження відповідності з правовими нормами у сфері захисту даних та конфіденційності представляє виклик у зв'язку з постійними змінами в законодавстві.

Управління цими викликами та ризиками стає важливим етапом для забезпечення стійкості та успіху ІТС підприємства в умовах постійної зміни технологічного та бізнес-середовища.

Розробка інтегрованої стратегії кібербезпеки є важливим елементом для забезпечення захисту конфіденційності та цілісності даних.

Створення гнучкої та адаптивної ІТ-інфраструктури є стратегічною метою для забезпечення швидкого реагування на зміни в бізнес-середовищі.

Впровадження систем моніторингу та аналізу продуктивності дозволяє ефективно виявляти та вирішувати проблеми в обробленні інформації.

Розробка систем автоматизації та використання штучного інтелекту сприяє оптимізації рутинних процесів та підвищенню продуктивності.

Стратегія постійного оновлення та навчання персоналу забезпечує їхню готовність до використання новітніх технологій.

Забезпечення відповідності з законодавством у сфері інформаційної безпеки є стратегічною вимогою для управління ризиками.

Стратегії управління обробленням інформації повинні бути гнучкими та адаптованими до змін у технологічному, правовому та економічному середовищі для забезпечення успішності ІТС підприємства.

1.3 Технологія оброблення інформації в ІТС підприємства

Технологія "Клієнт-Сервер" є ефективним та надійним рішенням для обробки інформації в ІТС підприємства. Вона забезпечує високу продуктивність, безпеку та масштабованість системи, а також гнучкість та універсальність для різних типів підприємств.[19]

В сучасному бізнес-середовищі оброблення інформації в інформаційно-технологічних системах (ІТС) визначає успішність функціонування підприємства. Цей розділ присвячений розгляданню основних понять та принципів, що лежать в основі цього процесу, а також визначенню ролі технологій у вдосконаленні оброблення інформації та їхнього впливу на ефективність підприємства.

Оброблення інформації в ІТС включає в себе низку ключових понять, що формують основу для подальшого розгляду. До них відносяться:

Дані: Сировинний матеріал для оброблення, який може набувати різних форматів та походжень.

Інформація: Результат оброблення даних, який має сенс та використовується для прийняття рішень.

Процеси оброблення: Алгоритми та методи, що використовуються для перетворення даних у корисну інформацію.

Принципи оброблення інформації визначають основні правила та методи, що регулюють цей процес. Ключовими з них є:

Цілісність: Забезпечення непорушності та повноти інформації в усьому циклі її оброблення.

Доступність: Забезпечення можливості отримання інформації в будь-який момент часу, коли це необхідно.

Конфіденційність: Захист інформації від несанкціонованого доступу та використання.

Технології відіграють ключову роль у вдосконаленні процесів оброблення інформації. Вони включають в себе:

Автоматизацію: Використання програмних рішень для автоматизації рутинних завдань та зменшення впливу людського фактору.

Швидкість і ефективність: Використання потужних обчислювальних ресурсів для швидкого оброблення великої кількості даних.

Інтеграція: Забезпечення взаємодії різних систем для отримання комплексної інформації.

Ефективне оброблення інформації має прямий вплив на успішність підприємства. Високоякісна інформація дозволяє приймати обґрунтовані рішення, оптимізувати бізнес-процеси та ефективно реагувати на зміни у внутрішньому та зовнішньому середовищі.

Технологія "Клієнт-Сервер" передбачає розподіл функцій між двома типами компонентів. Клієнтські компоненти, котрі встановлені на робочих станціях

користувачів і забезпечують інтерфейс для взаємодії користувачів з ІТС, прикладом є веб-браузер, програма для роботи з електронною поштою, тощо. Крім цього серверні компоненти, які розташовані на серверах вони зберігають дані, обробляють запити від клієнтів та надають доступ до інформації, як приклад можна привести веб-сервер, база даних, сервер прикладного програмного забезпечення.

Наведемо основні переваги технології "Клієнт-Сервер". Найголовніше це продуктивність, тобто розподіл функцій між клієнтськими та серверними компонентами дозволяє оптимізувати використання ресурсів та забезпечити високу продуктивність ІТС. Надійність, серверне зберігання даних забезпечує їх резервування та захист від втрати. Безпека, механізми авторизації та аутентифікації, а також шифрування даних гарантують конфіденційність та цілісність інформації. Масштабованість, технологія "Клієнт-Сервер" легко масштабується, що дозволяє розширювати ІТС в міру зростання потреб підприємства. Гнучкість, ця технологія підтримує різноманітні конфігурації та апаратні платформи, що робить її універсальною для різних типів підприємств.

Головні компоненти технології, мережева операційна система, вона забезпечує управління ресурсами сервера та зв'язок з клієнтськими компонентами. Другим компонентом і не менш важливим є, сервер прикладного програмного забезпечення, який забезпечує виконання прикладних програм, що обробляють дані та надають доступ до них. Також не можна забувати про, систему управління базами даних, яка зберігає дані та забезпечує доступ до них.

Технологія "Клієнт-Сервер" може використовуватися в широкому спектрі ІТС, таких як: Інформаційні системи управління: ERP, CRM, SCM, тощо; Системи електронного документообігу: EDI, DMS, тощо; Веб-сайти та веб-додатки; Системи електронної пошти; Файлові сервери;

Обробка інформації в ІТС здійснюється за технологією «Клієнт - Сервер», яка передбачає:

- внесення інформації до системи;
- зберігання інформації в системі;

- видалення інформації з системи;
- доступ до інформації, що зберігається в системі.

Внесення інформації до системи відбувається відповідно до визначених прав користувачів.

Дані, що зберігаються в ІТС підприємства, згруповані в окремі бази даних та знаходяться на серверах та АРМ користувачів підприємства. Забезпечення відповідних властивостей інформації, що зберігається в ІТС підприємства відбувається за допомогою спеціалізованого ПЗ та штатних засобів ОС.

Видалення інформації з системи здійснюється уповноваженим адміністратором відповідно до визначеного регламенту.

Доступ до інформації, що зберігається на серверах, здійснюється всіма групами користувачів ІТС підприємства через відповідні консолі, реалізовані функціонуванням ОС та прикладного ПЗ, за сукупністю відповідних унікальних персональних атрибутів доступу (пароль, логін). Атрибути доступу надаються кожному користувачу відповідно до його повноважень.

Обґрунтування технології:

Ефективність: Розподіл функцій між клієнтськими та серверними компонентами дозволяє оптимізувати використання ресурсів та забезпечити високу продуктивність ІТС.

Надійність: Серверне зберігання даних забезпечує їх резервування та захист від втрати.

Безпека: Механізми авторизації та аутентифікації, а також шифрування даних гарантують конфіденційність та цілісність інформації.

Масштабованість: Технологія "Клієнт-Сервер" легко масштабується, що дозволяє розширювати ІТС в міру зростання потреб підприємства.

Гнучкість: Ця технологія підтримує різноманітні конфігурації та апаратні платформи, що робить її універсальною для різних типів підприємств.

Оброблення інформації в інформаційно-технологічних системах (ІТС) підприємства має вирішальне значення у сучасному бізнес-середовищі. Ця

технологія стає каталізатором ефективного управління даними та оптимізації бізнес-процесів.

Важливо розуміти основні принципи та поняття, які лежать в основі оброблення інформації. Дані, будучи основним ресурсом, вимагають ретельної обробки, зберігання та передачі. Принципи конфіденційності, доступності та цілісності стають фундаментом для ефективного управління інформацією.

Роль технологій у вдосконаленні процесів оброблення інформації надзвичайно важлива. Сучасні інструменти та системи дозволяють автоматизувати багато рутинних завдань, підвищуючи ефективність та точність оброблення даних. Технології допомагають із забезпеченням безпеки інформації, контролем доступу та розвитком стратегій збереження даних.

Важливо враховувати, що технологія оброблення інформації в ІТС підприємства не лише віддзеркалює поточний стан, але і визначає напрямки для майбутнього розвитку. Постійні зміни в технологічному ландшафті вимагають гнучкості та готовності до інновацій для успішного функціонування підприємства в умовах сучасного бізнесу.

Оброблення інформації в інформаційно-технологічних системах (ІТС) є необхідним елементом для успішного функціонування підприємства в умовах сучасного бізнесу. Потужності та можливості, які вона відкриває, визначають конкурентоспроможність та гнучкість організації.

Основні поняття, такі як дані, конфіденційність, доступність та цілісність, стають фундаментом, на якому ґрунтується весь процес оброблення інформації. Управління цими поняттями вимагає не лише технічної компетентності, але й стратегічного мислення.

Технології оброблення інформації в ІТС підприємства включають в себе використання сучасних інструментів для збору, аналізу та використання даних. Автоматизація рутинних операцій, використання штучного інтелекту та розвиток хмарних технологій роблять оброблення інформації більш ефективним та доступним.

У світлі постійних змін у технологічному середовищі, підприємства повинні мати стратегії для адаптації до нових викликів та можливостей. Технологія оброблення інформації в ІТС підприємства стає ключовим інструментом для досягнення цієї мети, допомагаючи забезпечити ефективність та конкурентоспроможність в динамічному світі бізнесу.

Висновок до розділу 1

В розділі була розглянута загальна характеристика ІТС підприємства, умови її функціонування та основні вимоги які будуть поставлені перед нею. Надається загальний огляд інформаційно-телекомунікаційної системи (ІТС) підприємства, визначаючи її структуру, характеристики і основні завдання.

ІТС є комплексом технічних і програмних рішень, спрямованих на обробку, зберігання та передачу інформації. Склад ІТС включає різноманітні компоненти, такі як робочі станції, сервери, мережеве обладнання та периферійні пристрої.

Інформація в ІТС підприємства поділяється за різними критеріями, такими як рівень доступу, право власності та призначення. Зокрема, визначено різні види інформації, яку система обробляє, включаючи конфіденційні дані та різні категорії програмного забезпечення.

Важливий аспект ІТС – це технологія "Клієнт-Сервер", яка визначає етапи внесення, зберігання, видалення та доступу до інформації в системі. Забезпечення властивостей інформації та керування доступом до неї відбувається за допомогою спеціалізованого програмного забезпечення та операційних систем.

Визначено ключові аспекти функціонування ІТС підприємства, структури та обробки інформації. Враховуючи сучасні вимоги до ІТ-рішень, система демонструє комплексність та ефективність в підтримці бізнес-процесів та прийнятті управлінських рішень.

РОЗДІЛ 2 ВИБІР КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ІТС ПІДПРИЄМСТВА А ТАКОЖ СТВОРЕННЯ МОДЕЛІ ПОРУШНИКА ТА МОДЕЛІ ЗАГРОЗ

2.1 Вимоги до КЗЗ ІТС підприємства

При розробці КСЗІ ІТС підприємства необхідно було врахувати щоб ІТС забезпечувала вимоги конфіденційності, цілісності, доступності та спостережності інформації. Виходячи з цього до ІТС повинні входити апаратні та програмні засоби захисту від НСД, а також організаційні заходи, спрямовані на керування засобами захисту, регламентацію дій користувачів і контроль за цими діями.

Відповідно до цих вимог КСЗІ повинна забезпечувати:

- цілісність, доступність та спостережність інформації, що обробляється в ІТС, а також конфіденційність, цілісність, доступність та спостережність технологічної інформації компонентів ІТС;
- захист від НСД компонентів ІТС;
- захист від мережових атак, створення та ефективне функціонування системи мережевого захисту інформації;
- ідентифікацію користувачів ІТС;
- реєстрацію дій користувачів ІТС;
- розмежування доступу до об'єктів захисту, серверів, ресурсів та процесів ІТС.

Також відповідно до вимог, комплекс засобів захисту ІТС повинен мати такий функціональний профіль захищеності, який відповідатиме нормативному документу НД ТЗІ 2.5-004-99, який установлює критерії оцінки (рисунок 2.1) захищеності інформації, яка обробляється в системі, від несанкціонованого доступу.[20]

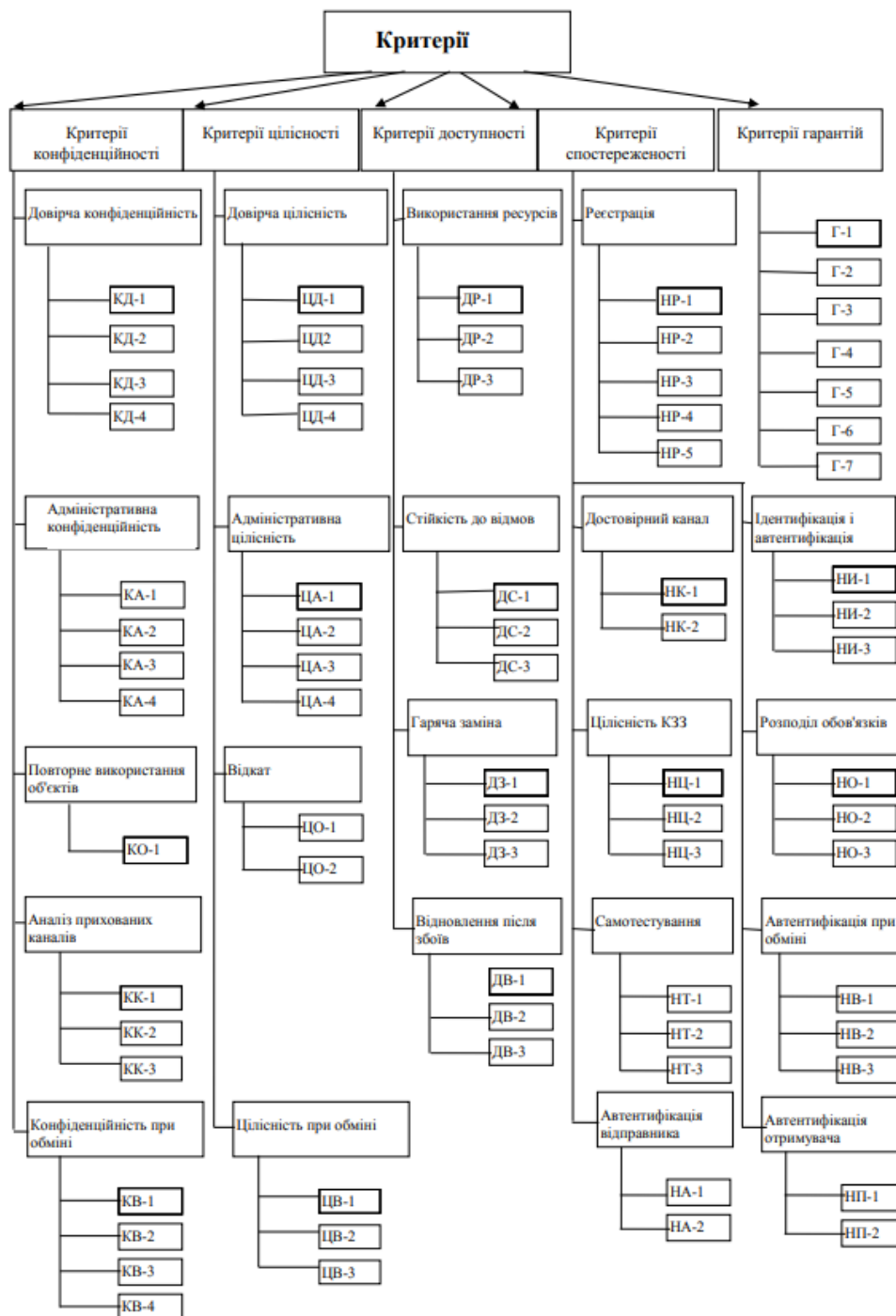


Рис. 2.1. Критерії захищеності інформації

Згідно документу було обрано наступні критерії: КД-2, КА-2, КО-1, КВ-1, ЦД-1, ЦА-1, ЦО-1, ЦВ-1, ДЗ-1, ДВ-1, ДС-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НТ-2, НВ-1, НА-2 де:

- КД-2 – базова довірча конфіденційність;
- КА-2 – базова адміністративна конфіденційність;
- КО-1 – повтерно використання об'єктів;

- KB-1 – мінімальна конфіденційність при обміні;
- ЦД-1 – мінімальна довірча цілісність;
- ЦА-1 – мінімальна адміністративна цілість;
- ЦО-1 – обмежений відкат;
- ЦВ-1 – мінімальна цілісність при обміні;
- ДВ-1 – ручне відновлення;
- ДЗ-1 – модернізація;
- ДС-1 – стійкість при обмежених відмовах;
- НР-2 – захищений журнал;
- НИ-1 – зовнішня ідентифікація і автентифікація;
- НИ-2 – одиночна ідентифікація і автентифікація;
- НК-1 – однонаправлений достовірний канал;
- НО-2 – розподіл обов’язків адміністраторів;
- НЦ-1 – КЗЗ з контролем цілісності;
- НТ-2 – самотестування при старті;
- НВ-1 – автентифікація вузла;
- НА-2 – автентифікація відправника з підтвердженням.

2.2 Опис операційних систем ІТС підприємства

Відповідно до потреб, було сформовано вимоги до програмно-апаратного забезпечення:

1. Використання Windows server 2019;
2. Робочі станції з встановленими ОС Windows 10 та 7;[14]
3. Міжмережний екран на базі Pfsense, задля забезпечення надійного захисту мережі.

Детально розглянемо кожен пункт.

Microsoft Windows Server 2019 — це операційна система загального призначення, яка функціонує на серверному обладнанні як ОС в режимі взаємодії з іншими серверними та клієнтськими операційними системами так і відокремлено. До складу Windows Server входять ряд сервісів, служб та додатків,

які забезпечують функціонування як самої операційної системи, так і відповідних технологій (сервер доменного контролю, DHCPсервер, DNS-сервер, веб-сервер, сервер додатків, файл сервер, сервер терміналів, гіпервізор, служба оновлення та ін.).[12]

Можливості Microsoft Windows Server 2019:

1. Компоненти захисту Microsoft Windows Server 2019:

- монітор стану безпеки (Security Reference Monitor, SRM);
- процес входу в систему (Winlogon);
- графічний інтерфейс ідентифікації і автентифікації (LogonUI);
- постачальник облікових даних (Credential Provider, CP);
- диспетчер локальної авторизації (LSA);
- служба мережного входу (Netlogon);
- сервер локальної автентифікації (LSA Server, Lsassrv);
- реєстратор подій (Event Log);
- інтерфейс служби каталогів (NTDS API, Ntdsapi);
- диспетчер облікових записів (Security Accounts Manager, SAM, Samsrv);
- пакети автентифікації (Authentication Packages);
- служба каталогів (NTDS, Active Directory)[18].

2. Ідентифікатор безпеки (Security Identifier - SID) - структура даних змінної довжини, яка ідентифікує обліковий запис користувача, групи, домену, комп'ютера або служби в ОС. SID ставиться у відповідність кожного облікового запису (групи, служби, тощо) в момент її створення або модифікації. Система оперує з SID'ами облікових записів, а не їх іменами. У контролі доступу користувачів до захищених об'єктів (файлів, ключів реєстру тощо) беруть участь також тільки SID'и.

3. Маркер доступу. Для ідентифікації контексту захисту процесу або потоку менеджер системних ресурсів (System Resource Manager - SRM) використовує об'єкт, що має назву маркер (token), або маркер доступу (access token). В процесі входу в систему Winlogon створює початковий маркер, що представляє користувача, який входить в систему, і порівнює його з початковим

процесом (або процесами) - за умовчанням запускається Userinit.exe. З огляду на те, що дочірні процеси за замовчуванням успадковують копію маркера свого створювача, всі процеси в сеансі даного користувача виконуються з одним і тим же маркером. Генерація маркера здійснюється викликом Windows-функції LogonUser і застосовується для створення процесу, який буде виконуватися в контексті захисту користувача, зареєстрованого за допомогою функції LogonUser. Для цього отриманий маркер передається Windows-функції CreateProcessAsUser. Функція CreateProcessWithLogon також створює маркер, створюючи новий сеанс входу з початковим процесом (саме так команда runas запускає процеси з альтернативними маркерами).

4. Дескриптори безпеки (Security Descriptor - SD) є структурою, що містить всю інформацію про безпеку, асоційовану з захищеним об'єктом.

5. Запис керування доступу (Access-Control entries - ACE) входить до складу ACL та визначає спосіб взаємодії SID з захищеним об'єктом. ACE не має фіксованого розміру, з огляду на те що містить SID, який може мати змінний розмір.

6. Міжмережевий екран, забезпечує контроль та фільтрацію IP-пакетів, які імпортуються (вхідний трафік) або експортуються (вихідний трафік) при мережевому обміні засобами вбудованого міжмережевого екрану (брандмауеру) ICF (Internet Connection Firewall). Мета застосування міжмережевого екрану (МЕ) в ОС полягає у протидії несанкціонованому обміну захищеними об'єктами між інтерфейсними процесами ОС та іншими учасниками мережевого обміну.

7. Відкат із використанням тіньового копіювання захищених об'єктів файлової системи NTFS підтримується компонентом «Попередні версії», який використовує технологію тіньового копіювання для створення миттєвих знімків томів. Тіньове копіювання включене в ОС за умовчанням, виконується автоматично, як правило, один раз в день, не вимагає додаткового керування з боку авторизованого користувача та дозволяє йому переглядати, відновлювати і копіювати попередні версії файлів і каталогів, які могли бути випадково змінені або видалені. Відкат драйвера дозволяється виконувати для одного рівня відкату,

оскільки тільки одна версія попереднього драйвера може зберігатися при виконанні відновлення. Відкат файлу або каталогу доступний авторизованому користувачу через команду контекстного меню «Відновити попередні версії» або діалогове вікно властивостей об'єкта. При відкаті використовуються копії файлів або каталогів, створені службою тіньового копіювання томів у певний момент часу.

8. Відкат драйверів пристроїв ОС дозволяє повернутися до попередньої версії драйверу шляхом повторного встановлення драйвера, який використовувався раніше, та відновлення всіх параметрів драйвера, що змінювалися при додаванні нового драйвера. Якщо попередня версія драйвера відсутня, тобто драйвер встановлено вперше, можливість відкату драйверу недоступною.

9. Система архівації даних Windows Server, котра складається з оснащення консолі керування (MMC), програм командного рядка і командлетів Windows PowerShell. Систему архівації даних Windows Server можна використовувати для архівації всього сервера (всіх томів), обраних томів або стану системи, а також для архівації окремих папок і файлів і створення архівних копій для подальшого відновлення початкового стану. Наявна можливість відновлювати томи, папки, файли, певні програми та стан системи. У випадку збоїв, наприклад неполадок з жорстким диском, можна виконати відновлення системи до початкового стану, в результаті чого система буде відновлена цілком на новому жорсткому диску з використанням архівації всього сервера і середовища відновлення Windows.

10. Дискові квоти. В ОС реалізована можливість обмежувати на певному томі NTFS обсяг доступного для користувача дискового простору (встановлювати дискові квоти).

11. Квоти на ресурси процесора і пам'ять серверу. В ОС реалізовано можливість управляти використанням ресурсів процесора і пам'яттю серверу із використанням Диспетчера системних ресурсів Windows.

12. Відновлення після збоїв. ОС має засоби відновлення системи після збоїв, що має назву Середовище відновлення Windows (Windows RE).

13. Реєстрація подій безпеки ОС. Журнал реєстрації містить інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події, а також інформацію про користувача, процес і/або об'єкт, що мали відношення до зареєстрованої події.

14. Журнал безпеки, в якому містяться усі події і мають безпосереднє відношення до безпеки. ОС визначає спеціальні категорії та підкатегорії подій, які пов'язані з безпекою КЗЗ і реєструються у журналі.

15. Перегляд журналу безпеки в якому, для аналізу дій і подій, пов'язаних з безпекою, адміністратор, використовуючи засіб «Перегляд подій», може створити фільтр з певними параметрами. Для журналу безпеки такими параметрами можуть бути задані: рівень і категорія події, ідентифікатор подій або діапазон ідентифікаторів подій, ключові слова, користувач(и), комп'ютер(и). Події, відібрані за створеним фільтром, зберігаються як «Замовлене представлення» («Custom View»).

16. Ідентифікація та автентифікація в ОС визначається як процедура перевірки відповідності пред'явленого ідентифікатора (SID) облікового запису користувача на предмет належності ідентифікатора цьому обліковому запису користувача. ОС засісовує механізми автентифікації при кожному вході облікового запису користувача в ОС незалежно від типу входу. Кожний користувач автентифікується до того, як йому буде надане право виконувати будь-які дії в системі.

В роботі користувачі мережі використовують ОС Windows 10 та 7, штатні засоби захисту яких, надають наступні можливості щодо забезпечення безпеки інформації:

1. Списки доступу надають доступ до ресурсів ОС тільки авторизованим користувачам. Модель захисту включає компоненти, які реалізують контроль доступу суб'єктів і аудит подій.

2. Групи безпеки, дозволяють спростити керування доступом до ресурсів, дозволяючи призначати дозволи і права для групи користувачів, а не окремому обліковому запису користувача. Таким чином, для надання доступу до нових ресурсів, обліковий запис може бути просто добавлений або видалений з групи користувачів. Крім користувачів, в групу можна додавати комп'ютери та інші групи. Шляхом додавання комп'ютера до групи, спрощується надання доступу системної задачі одного комп'ютера до ресурсів іншого.

3. Керування та збереження облікових даних користувачів, дана функція забезпечує безпечне збереження облікових даних користувача. Користувачам в домені надається можливість погодженої однократної реєстрації. При здійсненні першої спроби доступу до застосування в мережі потрібно виконати перевірку дійсності, у ході якої користувачу буде запропоновано ввести свої облікові дані. Після введення ці дані зв'язуються із запитаним застосуванням. При здійсненні наступних спроб доступу до цього застосування будуть використовуватися збережені облікові дані, тобто їх не потрібно буде вводити повторно. Збереження імен користувачів і паролів здійснюється в безпечному сховищі SAM. Доступ до облікових даних регулюється параметрами локальної безпеки LSS (Local Security Settings).

4. Реєстрація подій. В ОС сімейства Windows присутній набір засобів аудиту, призначених для моніторингу та виявлення небажаних умов і подій, які виникають в обчислювальному середовищі. Моніторинг системних подій дозволяє виявляти порушників системи безпеки, а також фіксувати спроби фальсифікації та видалення даних, які знаходяться на локальному комп'ютері. При аудиті, частіше за все, реєструються такі події як доступ до об'єктів, керування групами користувачів і обліковими записами груп, а також вхід користувачів в систему і вихід з неї. Аудит дозволяє вести моніторинг конкретних подій, наприклад, неуспішних спроб входу до системи. Перегляд журналу безпеки виконується за допомогою засобів перегляду подій. Політика аудиту дозволяє визначати події, для яких повинен проводитися аудит.

5. Захист ядра системи. В основі ОС лежить код, який характеризується захищеною моделлю пам'яті. Критично важливі структури ядра системи доступні тільки для читання, завдяки чому драйвери та застосування не можуть їх пошкодити. Код драйверів пристроїв в пам'яті також доступний тільки для читання та має захист на рівні сторінок пам'яті.

6. Групові політики, які можуть застосовуватися для керування конфігураційними даними користувачів і налагодженням комп'ютера в конкретному обчислювальному середовищі. Застосування групової політики здійснюється з метою контролю використання програм, мережевих ресурсів і операційної системи користувачами і комп'ютерами. Призначення відповідних параметрів групової політики для визначених користувачів в сполученні з дозволами NIPS, механізмом обов'язкових профілів та іншими засобами безпеки, дозволяє забезпечити безпечне середовище для користувачів, здійснивши обмеження їх доступу до певних програм і даних, системних параметрів ОС, виключаючи, таким чином, ймовірність модифікації файлів конфігурації системи.

Задля захисту мережі від вторгнень застосовуються міжмережевий екран PfSense. PfSense — це вільно поширювана операційна система на базі FreeBSD, спроектована для використання як міжмережевий екран (firewall) та маршрутизатор. Ось основні можливості PfSense:

1. Firewall. Повноцінний міжмережний екран з можливістю налаштування правил фільтрації трафіку.
2. VPN. Підтримка VPN-протоколів, таких як IPsec, OpenVPN, PPTP, L2TP, для забезпечення безпечного з'єднання мереж через Інтернет.[17]
3. Load Balancing та Failover. Можливість розподілу навантаження та автоматичного переключення на інші канали у разі відмови.
4. Captive Portal. Система перехоплення та авторизації користувачів у гостьових мережах.
5. Інспекція та фільтрація пакетів. Підтримка Deep Packet Inspection (DPI) для більш детального аналізу трафіку.

6. DNS та DHCP сервер. Вбудовані служби DHCP-сервера та сервера доменних імен (DNS).

7. Журнал подій. Можливість налаштування системи сповіщень та детального ведення журналів подій.

Також в мережі використовуватиметься обладнання фірми MikroTik.[4] MikroTik є популярним виробником обладнання для мережевого управління та маршрутизації, і його продукція має кілька переваг порівняно з іншими компаніями. Ось деякі з основних переваг MikroTik:

1. Гнучкість та налаштування:

- MikroTik пропонує широкий спектр продуктів, які підходять для різних застосувань - від невеликих підприємств до великих провайдерів послуг.
- Операційна система RouterOS дозволяє розширювати функціоналітет, додавати плагіни та використовувати різноманітні налаштування[5].

2. Ціна та вартість:

- Продукція MikroTik часто є більш доступною порівняно з аналогічними продуктами конкурентів.
- Мережеві рішення MikroTik надають можливість отримати потужне обладнання за доступну ціну.

3. Продуктивність та відмінна маршрутизація:

- Продукція MikroTik зазвичай відзначається високою продуктивністю та ефективністю роботи.
- RouterOS підтримує розширені маршрутизаційні можливості, включаючи BGP, OSPF, RIP і інші протоколи.

4. Спільнота та підтримка:

- Існує активна спільнота користувачів MikroTik, яка може надавати допомогу та поради.
- Компанія також забезпечує технічну підтримку для своїх продуктів.

5. Безпека:

- MikroTik активно вдосконалює свою систему безпеки та випускає оновлення для усунення вразливостей.

- Можливість налаштовувати файрвол та VPN-з'єднання дозволяє забезпечити високий рівень безпеки для мережі.

6. Простота управління:

- Інтерфейс користувача MikroTik досить інтуїтивний, що полегшує управління обладнанням.
- Наявність графічного інтерфейсу (Winbox) і можливість конфігурування через командний рядок (CLI) дає користувачам вибір у способі управління.

Задля перевірки трафіку та вразливостей мережі буде використовуватися програма WireShark.

Wireshark - програма-аналізатор трафіку для комп'ютерних мереж Ethernet та деяких інших. Має графічний інтерфейс користувача. Спочатку проект називався Ethereal, але через проблеми з торговою маркою у червні 2006 року проект був перейменований на Wireshark[15].

Функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, проте Wireshark має графічний інтерфейс користувача і набагато більше можливостей по сортуванню та фільтрації інформації. Програма дозволяє користувачеві переглядати весь трафік, що проходить по мережі, в режимі реального часу, переводячи мережеву карту в нерозбірливий режим.

Wireshark — це програма, яка «знає» структуру різних мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Оскільки для захоплення пакетів використовується rpsar, існує можливість захоплення даних лише з тих мереж, які підтримуються бібліотекою. Тим не менш, Wireshark вміє працювати з безліччю форматів вхідних даних, відповідно можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення.



Рис.2.2. Мережевий комутатор CRS226-24G-2S+1N

2.3 Антивірусний захист

Антивірусний захист у підприємстві є важливою складовою інформаційної безпеки. Вимоги можуть варіюватися в залежності від потреб та характеристик підприємства, але основні аспекти повинні включати наступне:

1. Комплексність захисту, антивірусний захист повинен бути комплексним і охоплювати виявлення та захист від різних видів загроз, таких як віруси, трояни, шпигунське ПЗ.
2. Оновлення баз даних, повинне регулярно оновлюватися для виявлення нових загроз, оскільки кіберзлочинці постійно створюють нові шкідливі програми.
3. Централізоване управління, дозволить адміністраторам відстежувати стан захисту на всіх пристроях та здійснювати керування параметрами захисту.
4. Охоплення всіх пристроїв, котрі наявні у підприємстві.
5. Виявлення і запобігання витокам даних.

6. Регулювання доступу, до антивірусного програмного забезпечення та його налаштувань, що попереджатиме про неправомірні зміни.
7. Регулярні тестування ефективності антивірусного захисту допомагатиме перевірити, наскільки він ефективний та актуальний.
8. Інтеграція з іншими системами безпеки, оскільки важливо щоб програмне забезпечення можна було легко з такими системами як виявлення вторгнень та засобами моніторингу безпеки.

Ці вимоги допоможуть забезпечити ефективний антивірусний захист та зменшити ризики виникнення кіберзагроз.

2.4 Опис моделі порушника безпеки інформації в підприємстві

Потенційним порушником безпеки інформації в ІТС підприємства є особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим наміром або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення конфіденційності, цілісності, та доступності інформації.

Враховуючи особливості обробки інформації та функціонування ІТС підприємства, виділені такі категорії потенційних порушників:

1. Адміністратор безпеки (A1);
2. Системний адміністратор (A2);
3. Внутрішній користувач (Us1);
4. Службовий персонал без доступу до ІТС підприємства.

Модель порушника відображає його практичні та потенційні можливості, знання, час та місце дії тощо.[10]

Визначення категорій порушників, що прийняті у моделі, наведено у таблиці 4.1. У таблицях 4.2-4.6 наведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ІТС підприємства, за показником можливостей використання засобів ІТС підприємства для реалізації загроз, за часом дії. У графі «Рівень загроз» зазначених таблиць наведено рейтингову оцінку загроз порушника.

Рівень загрози характеризується наступними категоріями:

- 1 – незначний;
- 2 – нижче середнього;
- 3 – середній;
- 4 – вище середнього;
- 5 – високий.

Таблиця 4.1

Категорії порушників, що зазначені в моделі

Позначення	Визначення категорії	Потенційний рівень загрози
П1	Адміністратор безпеки	5
П2	Системний адміністратор	5
П3	Внутрішній користувач	4
П4	Службовий персонал без доступу до ІТС	2

Таблиця 4.2

Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив	Ефективний рівень загрози
М1	Безвідповідальність	3
М2	Корисна цілеспрямованість	5

Таблиця 4.3

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС підприємства

Позначення	Основні кваліфікаційні ознаки порушника	Еф. рівень загрози
К1	Не володіє знаннями та інформацією про функціонування мережі	1
К2	Має навички користування АРМ на рівні користувача	2
К3	Володіє базовими знаннями щодо функціонування ПЗ та ОС підприємства	4
К4	Володіє знаннями щодо функціонування засобів та механізмів захисту, що викор	5

Таблиця 4.4

**Специфікація моделі порушника за показником можливостей
використання засобів ІТС підприємства**

Позначення	Характеристика можливостей порушника	Еф. рівень загрози
31	Має фізичний доступ до АРМ, але не є користувачем ІТС	1
32	Має можливість запуску набору завдань	3
33	Має можливість керування елементів ІТС	5

Таблиця 4.5

Специфікація порушника за часом дії

Позначення	Характеристика часу дії порушника	Еф. рівень загрози
Ч1	Під час бездіяльності компонентів системи	4
Ч2	Під час функціонування ІТС	5
Ч3	Під час перерв на обслуговування та ремонт	3

Таблиця 4.6

Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Еф. рівень загрози
31	Усередині будівлі, але без доступу до мережі	1
32	З робочих місць	5
33	З інших об'єктів	2

З урахуванням особливостей, було побудовано модель порушника, на основі, технологій обробки інформації яка циркулює в мережі, категорій персоналу котрий має доступ до ІТС підприємства, що наведено вище. Сукупність цих характеристик визначає профіль можливостей порушника.

Профілі можливостей порушників всіх категорій наведені в таблиці 4.7. У графі «Ефективний сумарний рівень загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Профілі можливостей порушників

Позначення	Категорія	Характер дій порушника					Еф. сум. рівень загрози
		Мотив	Кваліфікація	Можливості	Час дії	Місце дії	
П1	Адміністратор безпеки	M1, M2	K4	33	Ч1-Ч3	Д2-Д3	5
П2	Системний адміністратор	M1, M2	K4	33	Ч1-Ч3	Д2-Д3	5
П3	Внутрішній користувач	M1, M2	K3	32	Ч1-Ч3	Д2	4
П4	Службовий персонал без доступу	M1, M2	K1	31	Ч1-Ч3	Д2	2

2.5 Опис потенційних загроз інформації

За результатом впливу на інформацію та систему її обробки загрози поділяються на такі класи:

- 1) Порушення конфіденційності інформації;
- 2) Порушення цілісності інформації;
- 3) Порушення доступності інформації.
- 4) Втрата керованості системи обробки.

За джерелом впливу можливі загрози поділяються на:

- загрози, обумовлені діями людини;
- загрози обумовлені технічними засобами;
- загрози обумовлені стихійними факторами.

За характером впливу на ІТС підприємства, котра описується у роботі можливі загрози поділяються на:

- активні;
- пасивні.

За способом впливу на об'єкт атаки можливі загрози поділяються на:

- загрози з безпосереднім впливом на об'єкт атаки;
- загрози з впливом на систему прав доступу;
- загрози з опосередкованим впливом.

За використанням для атаки компонентом ІТС підприємства можливі загрози поділяються на:

- загрози, які використовують технічні засоби ІТС підприємства;
- загрози, які використовують технологічну інформацію ІТС підприємства;
- загрози, які використовують програмні засоби ІТС підприємства.

За засобами атаки можливі загрози поділяються на:

- загрози з використанням стандартного ПЗ або технічних засобів;
- загрози з використанням спеціально розробленого ПЗ або технічних засобів.

За станом об'єкту атаки можливі загрози поділяються на:

- загрози на об'єкт атаки, який знаходиться в стані зберігання;
- загрози на об'єкт атаки, який знаходиться в стані обробки.

За локалізацією джерела, можливі загрози поділятимуться на внутрішні та зовнішні. До зовнішніх відноситимуться загрози, джерело яких знаходиться поза межами підприємства. Внутрішні загрози реалізуються в межах контрольованої зони, яка діє на території підприємства, тобто в приміщеннях, де розташовані засоби обробки та збереження інформації, яка циркулює у мережі підприємства.

Відповідно до цього основними порушниками є зовнішній і внутрішній.

1. Зовнішній порушник – це можливий порушник, котрий діє поза межами території підприємства. Тобто, це людина котра не має доступу до приміщень і не є авторизованим користувачем, проте він має можливості реалізувати загрозу інформації, тільки впливаючи на інформацію з боку інших автоматизованих систем.

До категорій осіб, котрі відносяться до зовнішнього порушника у даному випадку є:

- сторонні особи, що знаходяться за межами контрольованої зони;
- обслуговуючий персонал;
- відвідувачі;
- представники організацій що взаємодіють з питань технічного забезпечення;
- представники організацій, що взаємодіють з питань обслуговування мережі ІТС.

2. Внутрішній порушник – це можливий порушник, котрий діє зсередини ІТС. В даному випадку розглядається як особа котра має доступ до приміщень, у яких розташовані засоби обчислювальної техніки. Цей порушник має можливість реалізувати загрозу інформації, й може бути як авторизованим користувачем, так і не авторизованим.

До можливих порушників відносяться:

1. Адміністратор безпеки;
2. Системний адміністратор;
3. Внутрішній користувач.

Основними припущеннями, що були зроблені при аналізі та розробці моделі загроз, що існують для ІТС описаного підприємства, є те, що;

- дія функцій захисту КСЗІ, яка створюється, розповсюджується на інформаційні ресурси ІТС;
- виконуватимуться припущення, зроблені при аналізі потенційного порушника.

Висновок до розділу 2

В розділі було враховано щоб ІТС забезпечувала вимоги конфіденційності, цілісності, доступності та спостережності інформації. Виходячи з цього до ІТС повинні входити апаратні та програмні засоби захисту від НСД, а також організаційні заходи, спрямовані на керування засобами захисту, регламентацію дій користувачів і контроль за цими діями.

Було описано задачі, які будуть поставлені перед антивірусним захистом підприємства.

З обладнання будемо використовувати провідного виробника – MikroTik, так як на пристроях даної фірми можна налаштувати всі обрані протоколи та технології.

В результаті аналізу були описані та сформульовані моделі порушника та моделі загроз, котрі можуть виникати в ІТС підприємства. Загрози були поділені на класи, а також визначено що загрозою може бути, як зовнішній так і внутрішній порушник.

РОЗДІЛ 3 ВПРОВАДЖЕННЯ КСЗІ, НАЛАШТУВАННЯ ТА ПЕРЕВІРКА РОБОТИ КОНФІГУРАЦІЇ

3.1 Приведення КСЗІ в дію

Відповідно до усіх поставлених вимог, здійснюється отримання засобів захисту інформації та їх інсталяція у мережу підприємства. Потрібно розуміти що цей процес має бути постійним, оскільки загрози і технології безпеки постійно змінюються. Тому важливо регулярно апгрейдувати та адаптувати засоби захисту для ефективного протистояння сучасним інформаційним загрозам, це включає в себе не лише поновлення антивірусного програмного забезпечення та використання останніх патчів безпеки, але й перегляд архітектури системи, виявлення нових загроз та вибір інноваційних рішень. Постійний моніторинг загроз та ефективне реагування на них стає ключовим елементом стратегії інформаційної безпеки.

Під час інсталяції мають бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС підприємства, повинен здійснюватися контроль за діями користувачів, а також контроль цілісності ПЗ та баз даних підприємства.

До баз даних повинні бути внесені відомості про користувачів мережі, встановлені їх повноваження щодо доступу до захищених об'єктів, їх створення, модифікації, архівування, знищення, експорту/імпорту із/в систему.

Після проведення усіх дій, починаються пусконаладжувальні роботи, метою яких є налагодження КЗЗ та перевірка працездатності засобів захисту інформації.

У разі необхідності, можуть бути впроваджені додаткові заходи захисту та здійснене відповідне коригування.

Відразу після запуску, повинне бути проведене навчання користувачів основним положенням політик безпеки інформації підприємства та експлуатації засобів захисту інформації. Оскільки персонал є першою лінією оборони проти інформаційних загроз. Регулярне навчання та підвищення обізнаності

співробітників щодо останніх методів атак та стратегій захисту є важливим елементом. Навчання повинно включати не лише теоретичні аспекти безпеки, але й практичні сценарії для реалістичного навчання реагування на інциденти.

Після завершення навчання, повинна бути проведена перевірка умінь користувачів користуватися впровадженими технологіями захисту інформації.

Навколо захисту інформації необхідно створити ефективні та гнучкі процеси, які дозволяють швидко реагувати на нові загрози. Це включає в себе розробку та практичне впровадження інцидентних планів, а також систематичне оновлення цих планів відповідно до змін у загрозах.

Загальною метою є створення гнучкої та відповідальної системи інформаційної безпеки, яка забезпечить ефективний захист в умовах постійних змін в технологіях та загрозах.

3.2 Налаштування мережі

В даному пункті буде розглянуто основні налаштування пристроїв мережі. Спочатку повністю складемо схему, яку спроектували в попередньому розділі (рис.4.1).

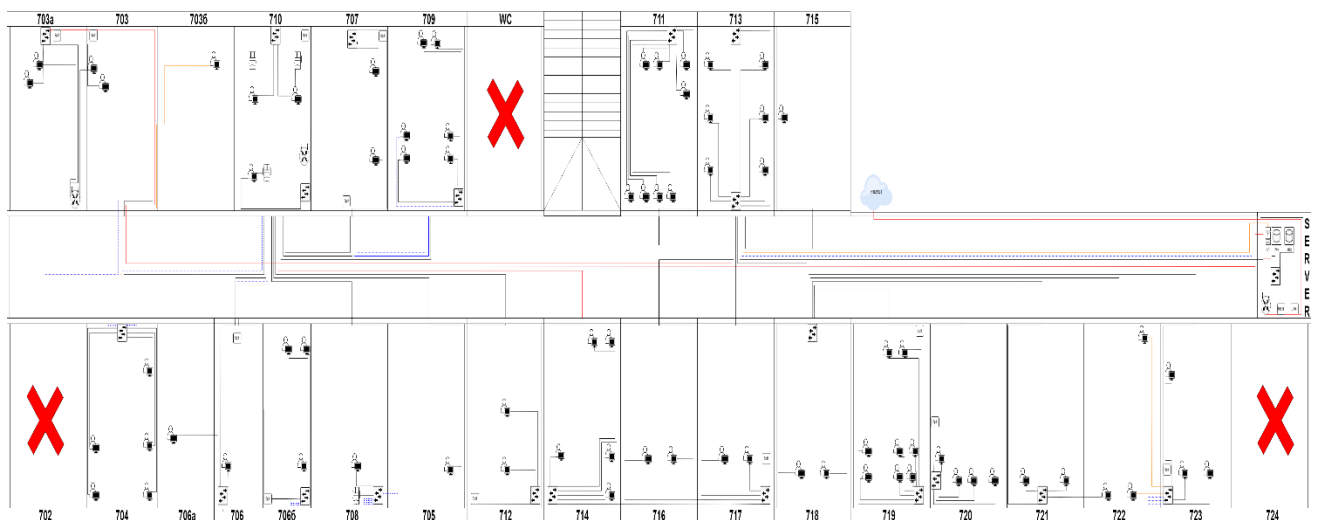


Рис. 3.1 Повна схема мережі

Перш за все, перед початком основних налаштувань, необхідно забезпечити надійний захист пристроїв, як від віддаленого доступу так і фізичного. Оскільки для входу на пристрій Cisco IOS, існує два варіанти через консоль або віддалено

через ssh чи telnet, тому необхідно, щоб кожен із цих способів був надійно захищений, без цього зловмисник за допомогою декількох команд, зможе зібрати достатньо інформації про мережу і тип самим знайти її слабкості(рис.3.2).

Для прикладу налаштувань було створено віртуальну мережу.



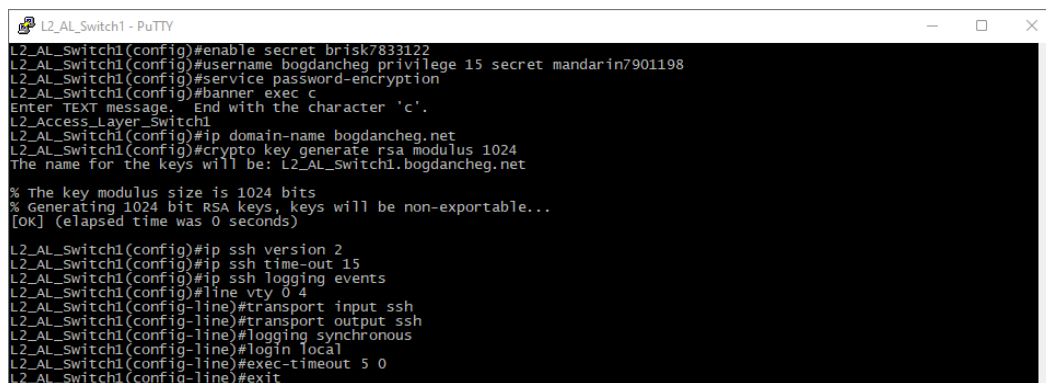
```
L2_AL_Switch1#sh cdp neighbors detail
-----
Device ID: L3_DL_Switch1.bogdancheg.net
Entry address(es):
  IP address: 192.168.6.2
Platform: Linux Unix, Capabilities: Router Switch IGMP
Interface: Ethernet0/0, Port ID (outgoing port): Ethernet0/0
Holdtime : 154 sec

Version :
Cisco IOS Software, Solaris Software (I86BI_LINUXL2-ADVENTERPRISEK9-M), Experimental version 15.1(20130726:213425) [dstivers-july26-2013-team_track 104]
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 26-Jul-13 15:56 by dstivers

advertisement version: 2
VTP Management Domain: ''
Native VLAN: 1
Duplex: half
Management address(es):
  IP address: 192.168.6.2
L2_AL_Switch1#
```

Рис.3.2 Виконання команди show cdp neighbors detail

Як можна побачити зловмисник може дізнати IP-адреси мережевих адаптерів, версії приладів, саме тому необхідно забороняти доступ до консолі навіть для користувацького режиму. Що ж, приступимо до налаштувань.



```
L2_AL_Switch1(config)#enable secret brisk7833122
L2_AL_Switch1(config)#username bogdancheg privilege 15 secret mandarin7901198
L2_AL_Switch1(config)#service password-encryption
L2_AL_Switch1(config)#banner exec c
Enter TEXT message. End with the character 'c'.
L2_Access_Layer_Switch1
L2_AL_Switch1(config)#ip domain-name bogdancheg.net
L2_AL_Switch1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: L2_AL_Switch1.bogdancheg.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

L2_AL_Switch1(config)#ip ssh version 2
L2_AL_Switch1(config)#ip ssh time-out 15
L2_AL_Switch1(config)#ip ssh logging events
L2_AL_Switch1(config)#line vty 0 4
L2_AL_Switch1(config-line)#transport input ssh
L2_AL_Switch1(config-line)#transport output ssh
L2_AL_Switch1(config-line)#logging synchronous
L2_AL_Switch1(config-line)#login local
L2_AL_Switch1(config-line)#exec-timeout 5 0
L2_AL_Switch1(config-line)#exit
```

Рис.3.3 Налаштування доступу по консолі, віддаленого доступу та користувача

Тепер необхідно пояснити, чому в ході налаштувань використовувався SSH, а не Telnet, покажемо це все на прикладі. Спершу побудуємо просту мережу(рис. 3.4).

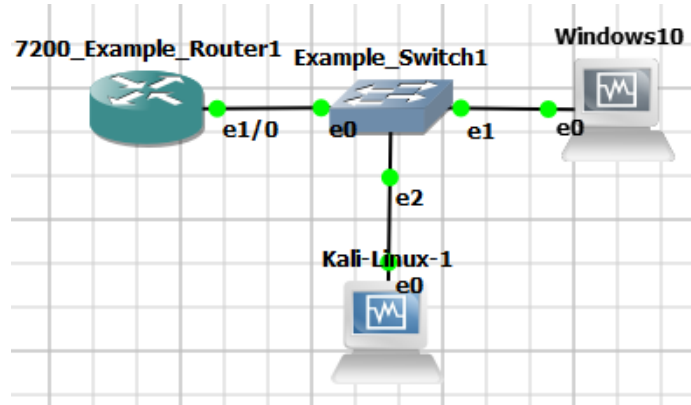


Рис. 3.4 Приклад мережі

Припустимо, що зломисник підключився до нашої мережі, а адміністратор нічого про це не знає і підключається по Telnet до маршрутизатора. В цей час зломисник перехоплює увесь цей трафік.

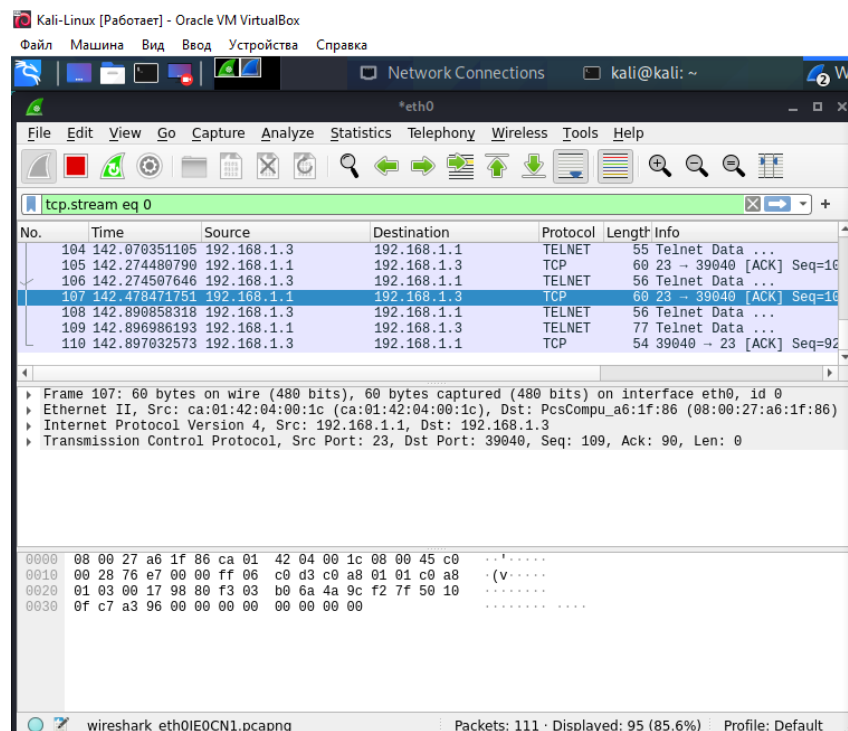


Рис. 3.5 Потік пакетів через інтерфейс

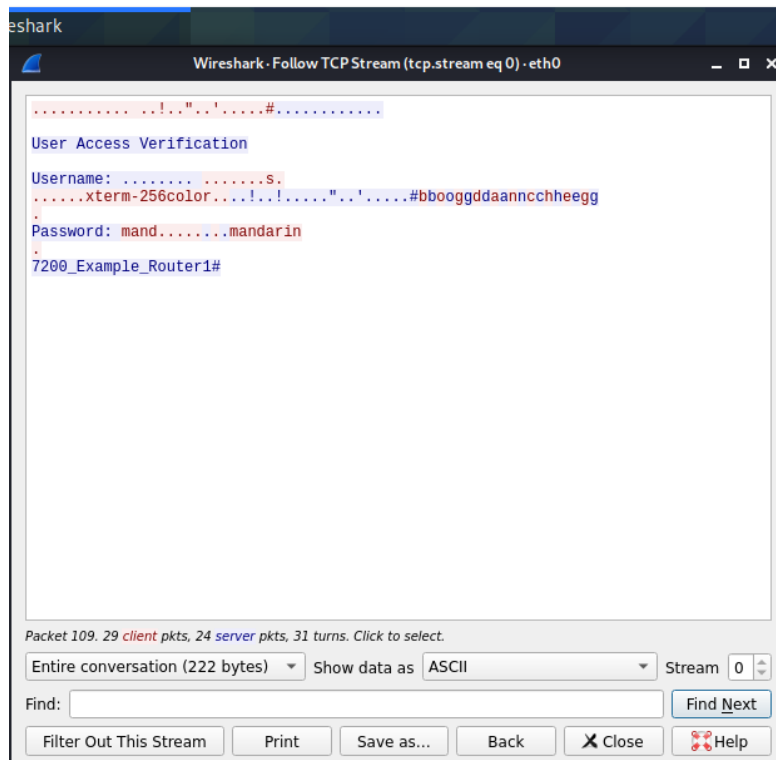


Рис 3.6 Перехоплений пакет

Як можна побачити (на рис.3.5 і 3.6) перехопивши пакет зломисник дізнався логін і пароль. Саме тому в ході налаштувань мережі використовувався більш захищений протокол SSH, оскільки він створює захищений канал між двома пристроями. Пристрій до якого ми намагаємося підключитися виступає у вигляді SSH-серверу, а наш комп'ютер з якого ми починаємо сесію є SSH-клінтом[11].

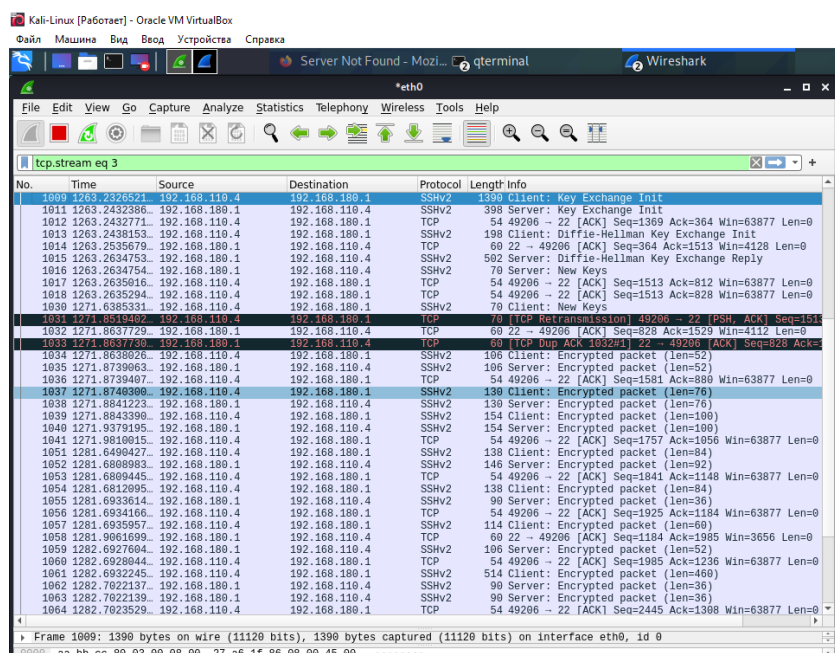


Рис. 3.7 Перехоплені пакети

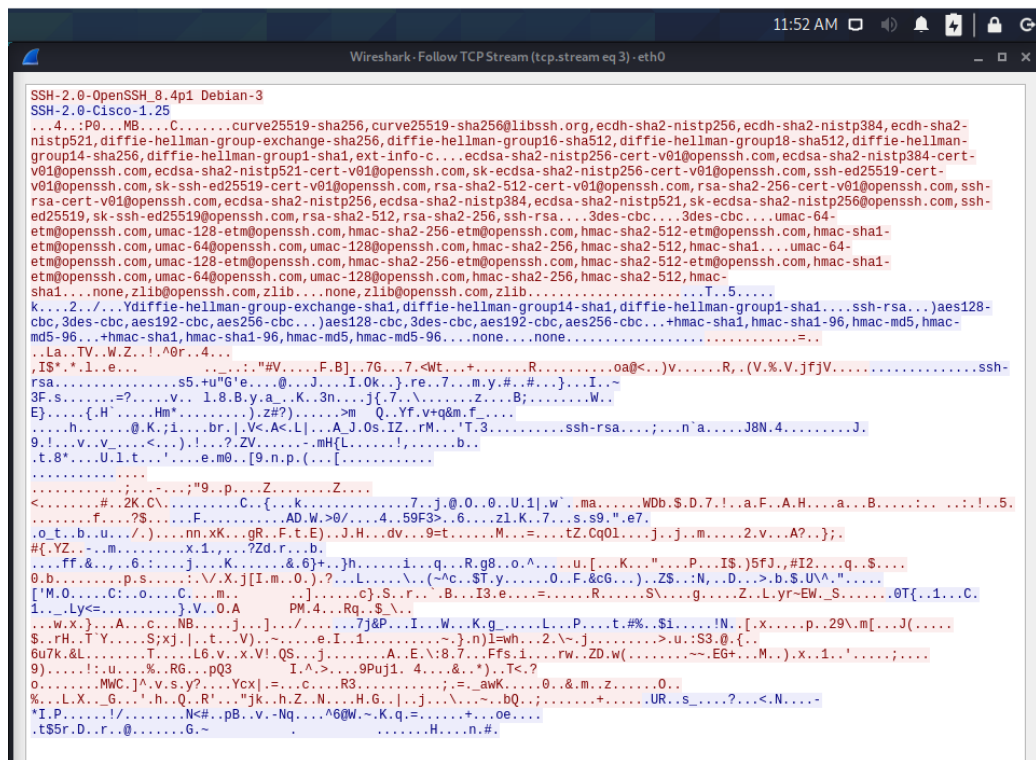


Рис. 3.8 Захищений протокол SSHv2

У даному випадку зломисник уже не зможе побачити логін і пароль, це робить перехоплення SSH трафіку не ефективним.

Далі налаштуємо машину PfSense, котра буде виступати в ролі міжмережевого екрану в нашій мережі.[3]

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgewf

Domain: ZhitomirKRU.local
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server: 110.110.110.1

Secondary DNS Server: 110.110.110.7

Override DNS: ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

Next

Рис. 3.9 Вказуємо ім'я і домен шлюзу

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname:
Enter the hostname (FQDN) of the time server.

Timezone:

[Next](#)

Рис. 3.10 Налаштування синхронізації часу

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address:
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask:

[Next](#)

Рис. 3.11 Налаштування внутрішнього інтерфейсу

Status / Dashboard

System Information

Name: pfSense.ZhitomirKRU.local

User: admin@110.110.110.2 (Local Database)

System: VirtualBox Virtual Machine
Netgate Device ID: 573d7d52bf8b51c42ea0

BIOS: Vendor: innotek GmbH
Version: VirtualBox
Release Date: Fri Dec 1 2006

Version: 2.7.0-RELEASE (amd64)
built on Wed Jun 28 03:53:34 UTC 2023
FreeBSD 14.0-CURRENT

The system is on the latest version.
Version information updated at Fri Dec 15 12:03:40 EET 2023

CPU Type: AMD A6-7400K Radeon R5, 6 Compute Cores 2C+4G
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No

Hardware crypto: Inactive

Kernel PTI: Disabled

MDS Mitigation: Inactive

Uptime: 00 Hour 22 Minutes 24 Seconds

Current date/time: Fri Dec 15 12:25:02 EET 2023

DNS server(s):
• 127.0.0.1
• 110.110.110.7
• 110.110.110.1

Last config change: Fri Dec 15 12:23:18 EET 2023

State table size: 0% (89/96000) [Show states](#)

MBUF Usage: 0% (3556/1000000)

Load average: 0.51, 0.49, 0.42

CPU usage: 6%

Memory usage: 25% of 961 MiB

SWAP usage: 0% of 409 MiB

Disks

Mount	Used	Size	Usage
/	2.0G	7.3G	29% of 7.3G (ufs)

Interfaces

Interface	Speed	IP Address
WAN	1000baseT <full-duplex>	110.110.110.17
LAN	1000baseT <full-duplex>	110.110.110.112

Traffic Graphs

WAN

LAN

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by Netgate](#)
- [Netgate Professional Services](#)
- [Visit Netgate.com](#)

Рис. 3.12 Інтерфес PfSense

Часто в організації бувають користувачі, яким доводиться дозволяти необмежені підключення до інтернет-ресурсів. Це може призвести до забивання всього каналу і утруднення в роботі інших користувачів і сервісів. На допомогу прийде обмеження ширини каналу. Шейпер має безліч налаштувань, розглянемо один із найчастіших сценаріїв його використання.

Керується у розділі Firewall - Traffic Shaper на вкладці Limiters.

Виміряємо поточну швидкість.

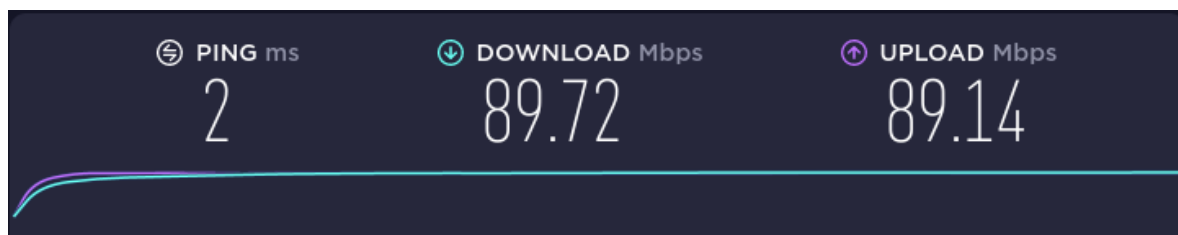


Рис. 3.13 Поточна швидкість інтернету

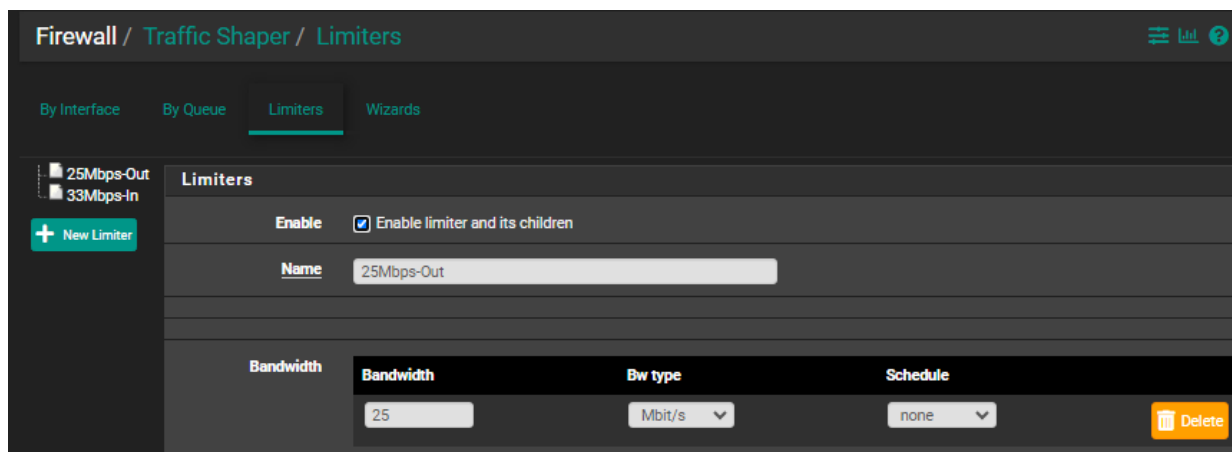


Рис. 3.14 Створюємо правила для трафіку

Включаємо правило, надаємо зрозуміле ім'я, вказуємо ширину смуги. Для вхідного та вихідного обмеження створюються окремі правила.

Безпосереднє включення шейпера виконується у правилах брандмауера (Fire-wall → Rules). Оскільки нас цікавить обмеження наших внутрішніх клієнтів, правила необхідно модифікувати/додавати для інтерфейсу LAN. При цьому ліміти розглядаються з боку інтерфейсу: In - вхідний, Out - вихідний з інтерфейсу трафік. Таким чином, обмеження трафіку від клієнта назовні використовується правило In.

Таким чином, відкриваємо пункт Rules меню Firewall, переходимо на вкладку LAN і в секції Extra Options потрібного (ново створеного або існуючого)

правила включають відображення розширених налаштувань (кнопка Display Advanced):

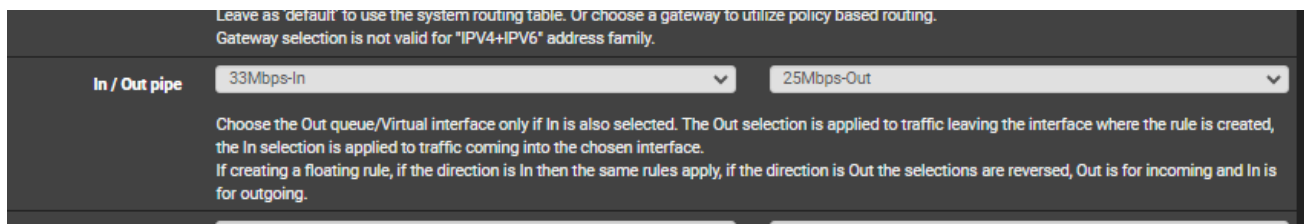


Рис. 3.15 Створюємо межі для трафіку

Після збереження та застосування налаштувань pfSense повідомляє про фонове перезавантаження правил фільтрації та пропонує перевірити статус на сторінці Status/Filter Reload.

Після оновлення правил виконаємо повторну перевірку швидкості.

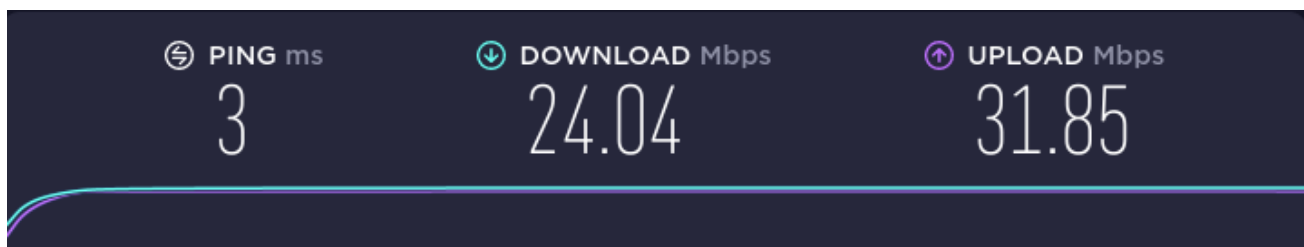


Рис. 3.16 Кінцева швидкість інтернету

Додаткові функції

Функціональність pfSense розширюється великою кількістю пакетів, доступних через пакетний менеджер, їх кілька десятків, ось деякі: `arcsnpsd` – демон для зв'язку з ДБЖ APC (нині Schneider); `arpwatch` – моніторинг активності MAC/IP-адрес; `cron` – планувальник; `filer` – файловий менеджер; `squid/lightsquid/squidGuard` – проксі, генератор звітів та фільтр; `lldpd` – надає підтримку виявлення Link Layer Discovery Protocol, крім того підтримує пропрієтарні CDP, EDP, FDP, NDP; `mailreport` – надсилання звіту поштою; `net-snmp` – GUI для SNMP; `nmap` – `nmap`, класика сканування мереж; `snort/suricata/zeek` – рішення класу IDS/IPS.

Необхідно розуміти, що за використання цих функцій потрібно заплатити підвищенням продуктивності обладнання. Інтенсивне використання VPN може вимагати додатково одне або більше ядер ЦПУ, а IDS/IPS також потребує додатково 1-2 ГіБ ОЗУ.

Проведемо демонстрацію розширення функціональності на популярному сканері nmap. У меню System заходимо до пункту Package Manager, вкладка Available Packages, поруч із пакетом NMap натискаємо на кнопку Install, чекаємо і отримуємо вбудований сканер:

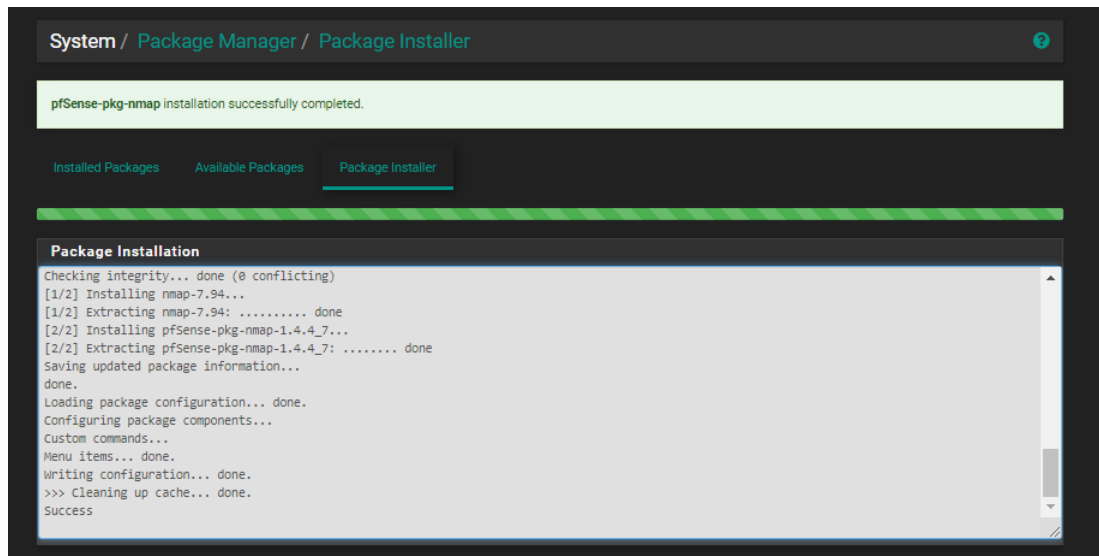


Рис. 3.17 Завантаження пакету

В меню Diagnostics додався пункт NMap, запускаємо:

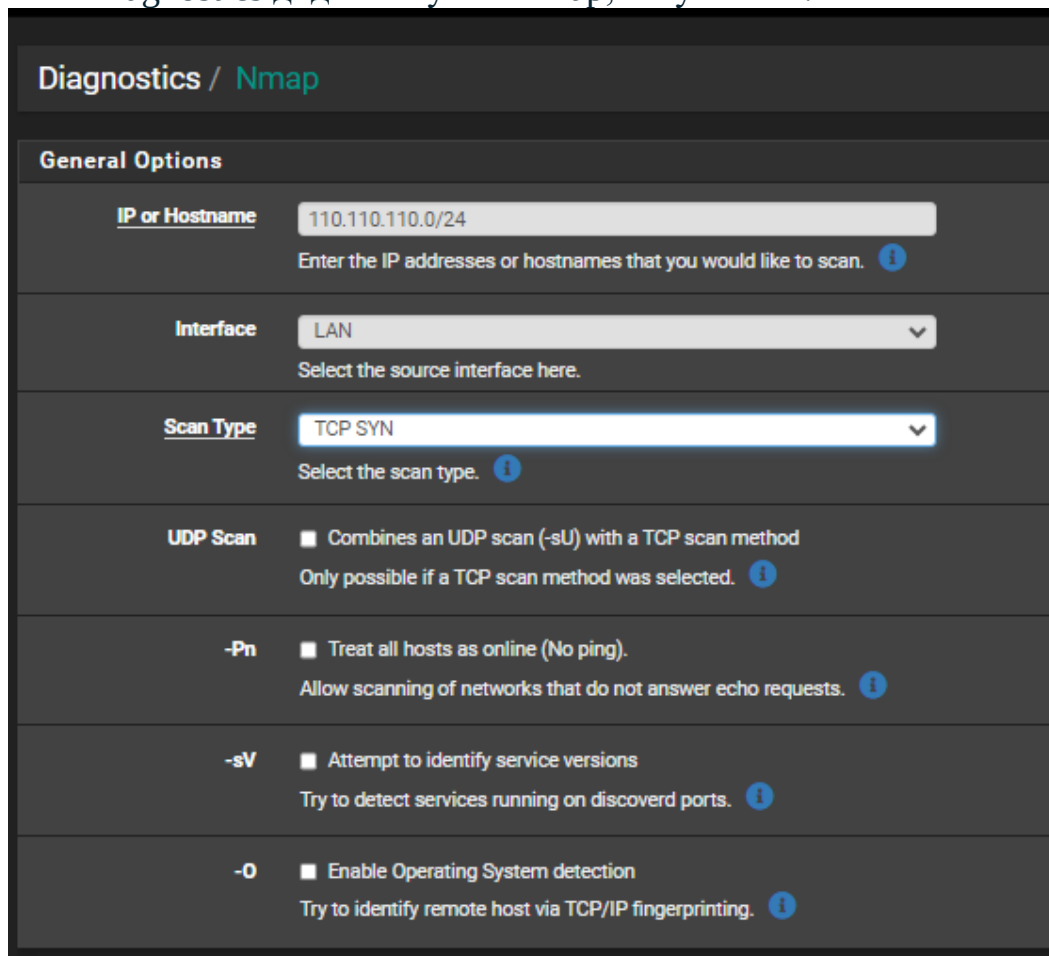


Рис. 3.18 Запуск діагностики

Висновок до розділу 3

Було виконано всі вимоги, які ставились раніше. В майбутньому дана мережа може бути збільшена та покращена під якісь певні завдання. Для цього є всі можливості.

Був встановлений PfSense, що забезпечить надійний захист мережі від втручання злоумисників із мережі інтернет.

Щодо недоліків даної мережі, чим більш професійне та якісне обладнання, тим воно буде дорожче. Тобто комутатори та маршрутизатори від компанії MikroTik є досить дорогими через їх надійність, якість, гарантію на заміну пристрою чи його компонентів при неполадках в малі строки, що досить вигідно великим компаніям, коли кожна хвилина коштує грошей.

ВИСНОВКИ

У проекті була спроектована та описана комплексна система захисту інформаційно телекомунікаційної системи підприємства.

Для початку було проведено аналіз та вибір існуючих технологій, продумано всі задачі, котрі можуть бути поставлені перед КСЗІ ІТС підприємства. Змодельовано моделі порушника та загроз.

На етапі розробки мережі було визначено, що комп'ютерна мережа міститиме міжмережевий екран PfSense, котрий забезпечить мережу від зовнішніх втручань, а також надасть можливість фільтрації та перевірки трафіку для мережі.

В мережі спроектовано логічну модель комп'ютерної мережі. Це дозволить забезпечити зміни мережі в майбутньому – масштабованість та надійність роботи. Комп'ютерна мережі має в собі робочі станції та сервери.

Для побудови мережі використовувалися технології від компанії MikroTik, через їх надійність та гнучкість в налаштуваннях. Це ще раз доводить те, що система буде досить надійною.

Проведено налаштування пристроїв та аналіз результатів, сформовано висновки стосовно модернізації та вдосконалення роботи. Реалізована мережа є готовою реалізацією проекту, а конфігурації можуть застосовуватися для реального обладнання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

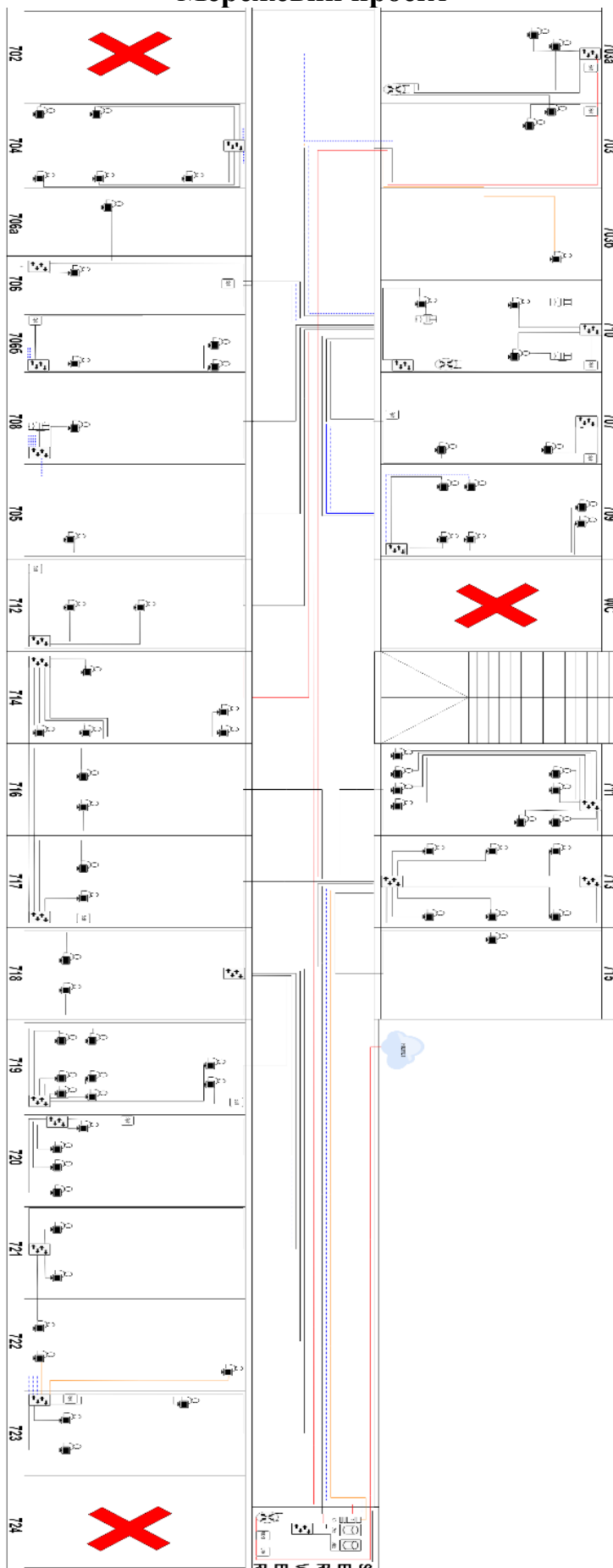
1. Комплексна система захисту інформації. [Електронний ресурс] // КСЗІ. – 2023. – Режим доступу до ресурсу: [https://uk.wikipedia.org/wiki/Комплексна система захисту інформації](https://uk.wikipedia.org/wiki/Комплексна_система_захисту_інформації)
2. Що таке інформаційно телекомунікаційні системи? [Електронний ресурс] // КЛАСТЕР. – 2012. – Режим доступу до ресурсу: <https://klaster.ua/ua/statii-obzory/informacionno-telekommunikacionnaja-sistema/>.
3. PfSense [Електронний ресурс] – Режим доступу до ресурсу: <https://www.pfsense.org/>.
4. MikroTik [Електронний ресурс] // Wikipedia. – 2023. – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/MikroTik>.
5. RouterOS [Електронний ресурс] // MSTREAM. – 2023. – Режим доступу до ресурсу: <https://mstream.com.ua/uk/routerboard/routeros-mikrotik/>.
6. ESET NOD 32 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.eset.com/ua/home/nod32/>.
7. TP-LINK [Електронний ресурс] // Wikipedia. – 2023. – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/TP-LINK>.
8. Коммутатор MikroTik Cloud Router Switch 326-24G-2S+IN (CRS326-24G-2S+IN) [Електронний ресурс] // MikroTik Ukraine – Режим доступу до ресурсу: <https://www.mikrotik.ua/ru/product/mikrotik-crs326-24g-2splusin>.
9. Kali Linux [Електронний ресурс] // Kali – Режим доступу до ресурсу: <https://www.kali.org/get-kali/#kali-virtual-machines>.

10. МАТЕМАТИЧНА МОДЕЛЬ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ [Електронний ресурс] // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2023. – Режим доступу до ресурсу: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/21>.
11. SSH [Електронний ресурс] // Wikipedia. – 2023. – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/SSH>.
12. Windows Server 2019 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.microsoft.com/ru-ru/evalcenter/evaluate-windows-server-2019>.
13. Windows 10 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.microsoft.com/uk-ua/software-download/windows10>.
14. Установка Windows 7 с пакетом обновления 1 (SP1) [Електронний ресурс] – Режим доступу до ресурсу: <https://support.microsoft.com/ru-ru/windows/установка-windows-7-с-пакетом-обновления-1-sp1>
15. Download Wireshark [Електронний ресурс] // Wireshark – Режим доступу до ресурсу: <https://www.wireshark.org/download.html>.
16. ISO/IEC 27001 [Електронний ресурс] // Wikipedia. – 2023. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/ISO/IEC_27001.
17. OpenVPN [Електронний ресурс] // Wikipedia. – 2023. – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/OpenVPN>.
18. Active Directory [Електронний ресурс] // Wikipedia. – 2023. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Active_Directory.

19. Клієнт-серверна_архітектура [Електронний ресурс] // Wikipedia. – 2023. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Клієнт-серверна_архітектура.
20. НД ТЗІ 2.5-004-99 [Електронний ресурс] // Нормативні документи системи ТЗІ – Режим доступу до ресурсу: <https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi>.

ДОДАТКИ

Мережевий проект



Конфігураційні файли пристроїв мережі

Конфігураційний файл комутатора MikroTik

```
[admin@RouterOS] > export
# jan/02/1970 04:38:35 by RouterOS 6.48.7
# software id = VBTQ-U294
#
# model = CRS326-24G-2S+
# serial number = HF30985SD49
/interface bridge
add admin-mac=78:9A:18:61:AA:78 auto-mac=no comment=defconf name=bridge
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot profile
set [ find default=yes ] html-directory=hotspot
/interface bridge port
add bridge=bridge comment=defconf interface=ether1
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=ether11
add bridge=bridge comment=defconf interface=ether12
add bridge=bridge comment=defconf interface=ether13
add bridge=bridge comment=defconf interface=ether14
add bridge=bridge comment=defconf interface=ether15
add bridge=bridge comment=defconf interface=ether16
add bridge=bridge comment=defconf interface=ether17
add bridge=bridge comment=defconf interface=ether18
add bridge=bridge comment=defconf interface=ether19
add bridge=bridge comment=defconf interface=ether20
add bridge=bridge comment=defconf interface=ether21
add bridge=bridge comment=defconf interface=ether22
add bridge=bridge comment=defconf interface=ether23
add bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf interface=sfp-sfpplus1
add bridge=bridge comment=defconf interface=sfp-sfpplus2
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
add interface=ether6 list=LAN
add interface=ether7 list=LAN
add interface=ether8 list=LAN
add interface=ether9 list=LAN
add interface=ether10 list=LAN
add interface=ether11 list=LAN
add interface=ether12 list=LAN
add interface=ether13 list=LAN
add interface=ether14 list=LAN
add interface=ether15 list=LAN
add interface=ether16 list=LAN
add interface=ether17 list=LAN
add interface=ether18 list=LAN
add interface=ether19 list=LAN
add interface=ether20 list=LAN
add interface=ether21 list=LAN
add interface=ether22 list=LAN
add interface=ether23 list=LAN
add interface=ether24 list=LAN
add interface=sfp-sfpplus1 list=LAN
add interface=sfp-sfpplus2 list=LAN
/ip address
```

```

add address=110.110.110.51/24 comment=defconf interface=ether2 network=110.110.110.0
/system identity
set name=RouterOS
/system routerboard settings
set boot-os=router-os
[admin@RouterOS] >

```

Конфігураційни файл комутатора MikroTik

```

[admin@RouterOS] > export
# jan/02/1970 04:38:35 by RouterOS 6.48.7
# software id = VBTQ-U294
#
# model = CRS326-24G-2S+
# serial number = HF30985SD49
/interface bridge
add admin-mac=78:9A:18:61:AA:78 auto-mac=no comment=defconf name=bridge
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot profile
set [ find default=yes ] html-directory=hotspot
/interface bridge port
add bridge=bridge comment=defconf interface=ether1
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=ether11
add bridge=bridge comment=defconf interface=ether12
add bridge=bridge comment=defconf interface=ether13
add bridge=bridge comment=defconf interface=ether14
add bridge=bridge comment=defconf interface=ether15
add bridge=bridge comment=defconf interface=ether16
add bridge=bridge comment=defconf interface=ether17
add bridge=bridge comment=defconf interface=ether18
add bridge=bridge comment=defconf interface=ether19
add bridge=bridge comment=defconf interface=ether20
add bridge=bridge comment=defconf interface=ether21
add bridge=bridge comment=defconf interface=ether22
add bridge=bridge comment=defconf interface=ether23
add bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf interface=sfp-sfpplus1
add bridge=bridge comment=defconf interface=sfp-sfpplus2
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
add interface=ether6 list=LAN
add interface=ether7 list=LAN
add interface=ether8 list=LAN
add interface=ether9 list=LAN
add interface=ether10 list=LAN
add interface=ether11 list=LAN
add interface=ether12 list=LAN
add interface=ether13 list=LAN
add interface=ether14 list=LAN
add interface=ether15 list=LAN
add interface=ether16 list=LAN
add interface=ether17 list=LAN
add interface=ether18 list=LAN
add interface=ether19 list=LAN
add interface=ether20 list=LAN
add interface=ether21 list=LAN
add interface=ether22 list=LAN
add interface=ether23 list=LAN
add interface=ether24 list=LAN
add interface=sfp-sfpplus1 list=LAN
add interface=sfp-sfpplus2 list=LAN
/ip address

```

```
add address=110.110.110.52/24 comment=defconf interface=ether2 network=110.110.110.0
/system identity
set name=RouterOS
/system routerboard settings
set boot-os=router-os
[admin@RouterOS] >
```

Конфігураційни файл комутатора MikroTik

```
[admin@RouterOS] > export
# jan/02/1970 04:38:35 by RouterOS 6.48.7
# software id = VBTQ-U294
#
# model = CRS326-24G-2S+
# serial number = HF30985SD49
/interface bridge
add admin-mac=78:9A:18:61:AA:78 auto-mac=no comment=defconf name=bridge
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot profile
set [ find default=yes ] html-directory=hotspot
/interface bridge port
add bridge=bridge comment=defconf interface=ether1
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=ether11
add bridge=bridge comment=defconf interface=ether12
add bridge=bridge comment=defconf interface=ether13
add bridge=bridge comment=defconf interface=ether14
add bridge=bridge comment=defconf interface=ether15
add bridge=bridge comment=defconf interface=ether16
add bridge=bridge comment=defconf interface=ether17
add bridge=bridge comment=defconf interface=ether18
add bridge=bridge comment=defconf interface=ether19
add bridge=bridge comment=defconf interface=ether20
add bridge=bridge comment=defconf interface=ether21
add bridge=bridge comment=defconf interface=ether22
add bridge=bridge comment=defconf interface=ether23
add bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf interface=sfp-sfpplus1
add bridge=bridge comment=defconf interface=sfp-sfpplus2
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
add interface=ether6 list=LAN
add interface=ether7 list=LAN
add interface=ether8 list=LAN
add interface=ether9 list=LAN
add interface=ether10 list=LAN
add interface=ether11 list=LAN
add interface=ether12 list=LAN
add interface=ether13 list=LAN
add interface=ether14 list=LAN
add interface=ether15 list=LAN
add interface=ether16 list=LAN
add interface=ether17 list=LAN
add interface=ether18 list=LAN
add interface=ether19 list=LAN
add interface=ether20 list=LAN
add interface=ether21 list=LAN
add interface=ether22 list=LAN
add interface=ether23 list=LAN
add interface=ether24 list=LAN
add interface=sfp-sfpplus1 list=LAN
add interface=sfp-sfpplus2 list=LAN
/ip address
```

```

add address=110.110.110.53/24 comment=defconf interface=ether2 network=110.110.110.0
/system identity
set name=RouterOS
/system routerboard settings
set boot-os=router-os
[admin@RouterOS] >

```

Конфігураційни файл комутатора MikroTik

```

[admin@RouterOS] > export
# jan/02/1970 04:38:35 by RouterOS 6.48.7
# software id = VBTQ-U294
#
# model = CRS326-24G-2S+
# serial number = HF30985SD49
/interface bridge
add admin-mac=78:9A:18:61:AA:78 auto-mac=no comment=defconf name=bridge
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot profile
set [ find default=yes ] html-directory=hotspot
/interface bridge port
add bridge=bridge comment=defconf interface=ether1
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=ether11
add bridge=bridge comment=defconf interface=ether12
add bridge=bridge comment=defconf interface=ether13
add bridge=bridge comment=defconf interface=ether14
add bridge=bridge comment=defconf interface=ether15
add bridge=bridge comment=defconf interface=ether16
add bridge=bridge comment=defconf interface=ether17
add bridge=bridge comment=defconf interface=ether18
add bridge=bridge comment=defconf interface=ether19
add bridge=bridge comment=defconf interface=ether20
add bridge=bridge comment=defconf interface=ether21
add bridge=bridge comment=defconf interface=ether22
add bridge=bridge comment=defconf interface=ether23
add bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf interface=sfp-sfpplus1
add bridge=bridge comment=defconf interface=sfp-sfpplus2
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
add interface=ether6 list=LAN
add interface=ether7 list=LAN
add interface=ether8 list=LAN
add interface=ether9 list=LAN
add interface=ether10 list=LAN
add interface=ether11 list=LAN
add interface=ether12 list=LAN
add interface=ether13 list=LAN
add interface=ether14 list=LAN
add interface=ether15 list=LAN
add interface=ether16 list=LAN
add interface=ether17 list=LAN
add interface=ether18 list=LAN
add interface=ether19 list=LAN
add interface=ether20 list=LAN
add interface=ether21 list=LAN
add interface=ether22 list=LAN
add interface=ether23 list=LAN
add interface=ether24 list=LAN
add interface=sfp-sfpplus1 list=LAN
add interface=sfp-sfpplus2 list=LAN
/ip address

```

```
add address=110.110.110.54/24 comment=defconf interface=ether2 network=110.110.110.0
/system identity
set name=RouterOS
/system routerboard settings
set boot-os=router-os
[admin@RouterOS] >
```

Конфігураційни файл комутатора MikroTik

```
[admin@RouterOS] > export
# jan/02/1970 04:38:35 by RouterOS 6.48.7
# software id = VBTQ-U294
#
# model = CRS326-24G-2S+
# serial number = HF30985SD49
/interface bridge
add admin-mac=78:9A:18:61:AA:78 auto-mac=no comment=defconf name=bridge
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot profile
set [ find default=yes ] html-directory=hotspot
/interface bridge port
add bridge=bridge comment=defconf interface=ether1
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=ether11
add bridge=bridge comment=defconf interface=ether12
add bridge=bridge comment=defconf interface=ether13
add bridge=bridge comment=defconf interface=ether14
add bridge=bridge comment=defconf interface=ether15
add bridge=bridge comment=defconf interface=ether16
add bridge=bridge comment=defconf interface=ether17
add bridge=bridge comment=defconf interface=ether18
add bridge=bridge comment=defconf interface=ether19
add bridge=bridge comment=defconf interface=ether20
add bridge=bridge comment=defconf interface=ether21
add bridge=bridge comment=defconf interface=ether22
add bridge=bridge comment=defconf interface=ether23
add bridge=bridge comment=defconf interface=ether24
add bridge=bridge comment=defconf interface=sfp-sfpplus1
add bridge=bridge comment=defconf interface=sfp-sfpplus2
/interface list member
add interface=ether1 list=WAN
add interface=ether2 list=LAN
add interface=ether3 list=LAN
add interface=ether4 list=LAN
add interface=ether5 list=LAN
add interface=ether6 list=LAN
add interface=ether7 list=LAN
add interface=ether8 list=LAN
add interface=ether9 list=LAN
add interface=ether10 list=LAN
add interface=ether11 list=LAN
add interface=ether12 list=LAN
add interface=ether13 list=LAN
add interface=ether14 list=LAN
add interface=ether15 list=LAN
add interface=ether16 list=LAN
add interface=ether17 list=LAN
add interface=ether18 list=LAN
add interface=ether19 list=LAN
add interface=ether20 list=LAN
add interface=ether21 list=LAN
add interface=ether22 list=LAN
add interface=ether23 list=LAN
add interface=ether24 list=LAN
add interface=sfp-sfpplus1 list=LAN
add interface=sfp-sfpplus2 list=LAN
/ip address
```

```
add address=110.110.110.55/24 comment=defconf interface=ether2 network=110.110.110.0
/system identity
set name=RouterOS
/system routerboard settings
set boot-os=router-os
[admin@RouterOS] >
```