Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Дослідження систем захисту роутерів на базі ТзОВ «Центр сервісного обслуговування»

Виконав(ла): студент(ка) IV курсу, групи СБс 42

спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Турчиняк М.А. (прізвище та ініціали)

Керівник (підпис) Стадник М.А. (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т.Б (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В (прізвище та ініціали)

Рецензент (підпис) Млинко Б.Б. (прізвище та ініціали)

Тернопіль
2021

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В
(підпис) (прізвище та ініціали)
«22 » червня 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(НАЗВА ОСВІТНЬОГО СТУПЕНЯ)

за спеціальністю 125 Кібербезпеа
(шифр і назва спеціальності)

студенту Турчиняку Мирону андрійовичу
(ПРІЗВИЩЕ, ІМ'Я, ПО БАТЬКОВІ)

1. Тема роботи Дослідження системи захисту роутерів на базі ТзОВ «Центр сервісного обслуговування»

Керівник роботи Стадник Марія Андріївна, кандидат технічних наук, старший викладач кафедри кібербезпеки
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «16» лютого 2021 року № 4/7-114

2. Термін подання студентом завершеної роботи 17.06.2021

3. Вихідні дані до роботи технічна документація, інтернет-джерела.

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ. Розділ 1. Ааналічтина частина, 1.1 Характеристика організації, 1.2 Поняття інформаційного ризику, 1.3 Класифікація інформаційних ризиків, 1.4 Методики аналізу, оцінки та управління ризиками інформаційної безпеки, Розділ 2. Проектно-практична частина, 2.1 Аналіз вразливостей захищеності інформ комунікаційної мережі організації, 2.3 Дослідження захищеності бездротових мереж, 2.4 Дослідження вразливостей словникових паролів,

2.5 Вразливості міжмережевого екрану, 2.6 Вразливості роутерів D-Link, Розділ 3. Практична частина, 3.1 Підключення роутера MikroTik, 3.2 Налаштування мережевої карти комп'ютера, 3.3 Вхід в налаштування роутера MikroTik, 3.4 Скидання налаштувань роутера, 3.5 Опис мережевих інтерфейсів, 3.6 Налаштування WAN інтерфейсу MikroTik, 3.7 Налаштування локальної мережі MikroTik, 3.8 Налаштування Wi-Fi точки доступу MikroTik, 3.9 Налаштування Firewall і NAT, Розділ 4. Безпека життєдіяльності, основи охорони праці, 4.1 Долікарська допомога при кровотечах, 4.2 Аналіз потенційних шкідливостей на дільниці. Заходи щодо їх зниженню, Висновки, Перелік використаних джерел.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Гурик О.Я., доцент кафедри МТ		

7. Дата видачі завдання 16.02.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	**Примітка**
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.02 – 19.02	*Виконано*
2.	Підбір джерел про загрози мережевій безпеці	16.02 – 19.02	*Виконано*
3.	Опрацювання джерел про загрози мережевій безпеці	19.02 – 02.03	*Виконано*
4.	Підбір джерел про існуючі засоби захисту мережевої інфраструктури	02.03 – 10.03	*Виконано*
5.	Опрацювання джерел про існуючі засоби захисту мережевої інфраструктури	10.03 – 16.03	*Виконано*
6.	Аналіз діяльності підприємства	16.03 – 01.04	*Виконано*
7.	Розробка політик безпеки	01.04 – 10.04	*Виконано*
8.	Вибір програмно-апаратних засобів	10.04 – 16.04	*Виконано*
9.	Оформлення розділу «Огляд мережевих систем»	16.04 – 25.04	*Виконано*
10.	Оформлення розділу «Дослідження об’єкта діяльності»	25.04 – 05.05	*Виконано*
11.	Оформлення розділу «Побудова мережевої системи безпеки»	05.05 – 16.05	*Виконано*
12.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи хорони праці»	16.05 – 22.05	*Виконано*
13.	Оформлення кваліфікаційної роботи	22.05 – 08.06	*Виконано*
14.	Нормоконтроль	08.06 – 10.06	*Виконано*
15.	Перевірка на плагіат	10.06 – 16.06	*Виконано*
16.	Попередній захист кваліфікаційної роботи	16.06 – 19.06	*Виконано*
17.	Захист кваліфікаційної роботи	24.06	

Студент _____ (підпис) Турчиняк М.А. (прізвище та ініціали)

Керівник роботи _____ (підпис) Стадник М.А. (прізвище та ініціали)

АНОТАЦІЯ

Аналіз систем захисту інформації для ТзОВ "Центр сервісного обслуговування" // Турчиняк Мирон Андрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБс–42 // Тернопіль, 2021 // с. - 64, ліст. - 4, рис. -39, табл. - 4, бібліогр. - 11.

Ключові слова: ІНТЕРНЕТ-ЗАГРОЗА, МЕРЕЖЕВА СЛУЖБА, ДЖЕРЕЛО ЗАГРОЗИ, ІНОФРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, РОУТЕР, ВРАЗЛИВОСТІ МЕРЕЖІ, CRAMM.

Кваліфікаційна робота присвячена дослідженню систем захисту роутерів на основі аналізу вразливостей системи. В роботі проведений порівняльний аналіз існуючих засобів аналізу журналів мережевих служб, на підставі якого виявлено їх недоліки. Реалізовано зміну апаратного забезпечення, яке вирішує задачу виявлення та захисту мережі від виявлених вразливостей.

ANNOTATION

Analysis of information security systems for LLC "Service Center" // Turchynyak Myron Andriyovych // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security // with. – 64, letter. - 4, fig. -39, table. - 4, bibliogr. - 11.

Keywords: INTERNET THREAT, NETWORK SERVICE, SOURCE OF DANGER, INFORMATION AND COMMUNICATION SYSTEM, ROUTER, NETWORK VULNERABILITIES, CRAMM.

Qualification work is devoted to the study of router protection systems based on the analysis of system vulnerabilities. The comparative analysis of the existing means of analysis of network service logs is carried out in the work, on the basis of which their shortcomings are revealed. Implemented a change in hardware that solves the problem of detecting and protecting the network from detected vulnerabilities.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

FTTB – Fiber To The Building.

WAF - міжмережевий екран для веб-додатків.

ОС - операційна система.

ПЗ - програмне забезпечення.

ІТ - інформаційні технології.

WAN – Wide Area Network.

LAN - Local Area Network.

Wi-Fi - Wireless Fidelity.

ЗМІСТ

ВСТУП

Система захисту роутерів - це важливий елемент функціонування комп'ютерної мережі, оскільки від роутера залежить безпека підключення до мережі Інтернет. Саме він контролює периметр мережі, весь її трафік та інформацію, що робить його привабливою ціллю для злочинців. У результаті вдалої атаки на роутер зловмисники можуть не тільки отримати доступ до даних розташованих на певному пристрої, але й використовувати мережу жертви для здійснення атак на інші системи та для поширення шкідливого програмного забезпечення в локальній мережі організації.

При побудові комп'ютерної мережі варто ретельно вибирати місце для розташування роутерів, комутаторів та іншого апаратного забезпечення. Воно має розташовуватись в захищеній зоні. В даній зоні повинна розташовуватись комплексна система захисту інформації, встановлені технічні засоби і системи обмеження і контролю доступу, всі засоби та пристрої в даній зоні повинні мати сертифікацію згідно з Положенням про сертифікацію засобів захисту інформації.

У даному дипломному проекті розглядається дослідження системи захисту роутерів для Товариства з обмеженою відповідальністю "Центр сервісного обслуговування ". Для виконання цієї мети буде проведено аналіз захист роутера та підвищення рівня безпеки за рахунок зміни налаштувань безпеки роутера MikroTik.

1. АНАЛІТИЧНА ЧАСТИНА

1.1 Характеристика організації

Центр Сервісного Обслуговування (ЦСО) займається продажем, обслуговуванням та ремонтом різної сервісної техніки.

Нижче подано послуги ЦСО у сфері ремонту ПК:

- Реанімація (відновлення) і встановлення операційних систем Windows, Linux, Mac OS X.
- Збереження важливої інформації із зруйнованої системи Windows, Linux.
- Оптимізація (пришвидшення) продуктивності роботи комп`ютера.
- Інсталяція драйверів: сканера, принтера, материнської плати, відео карти і т.д. (Windows, Linux, Mac OS X)
- Встановлення різного роду програмного забезпечення.
- Встановлення антивірусів, антишпигунів, фаєрволів. Пошук та знешкодження вірусів.
- З'єднання декількох комп'ютерів в локальну мережу, створення мережевих дисків, мережевого принтера.
- Підбір та встановлення програм під замовлення, а також вирішення інших комп`ютерних проблем.

На сайті компанії також подана інформація про основну сферу робити, а саме про роботу як провайдера інтернету у м. Золочів: « Сучасне обладнання, розгалужена мережа волоконно-оптичних магістралей та широкі зовнішні канали, дозволяють нам надавати "домашнім" користувачам високоякісний швидкісний доступ до Інтернет з гарантованою швидкістю та надзвичайно низькою вартістю. З 2010 року ми пропонуємо нашим абонентам виключно безлімітні тарифні плани без

жодних "прихованих" обмежень та додаткових доплат. Крім того, ми надаємо можливість післяоплати послуг, що дуже важливо і зручно у теперішній економічній ситуації. Для доступу до локальної мережі ЦСО не потрібно жодного додаткового обладнання, тому підключення до мережі у більшості випадків практично безкоштовне.

ТзОВ "Центр сервісного обслуговування" надає послуги по підключенню та постійного доступу до всесвітньої мережі "Internet". Високоякісні зовнішні канали та сучасне магістральне обладнання дозволяє нам забезпечити якісний та надійний доступ до Інтернет не лише у м. Золочів, але й в багатьох населених пунктах Золочівського району.

Для забезпечення потреб населення, підприємств та організацій міста Золочів нами була розгорнута міська оптично-волоконна мережа, що дало змогу реалізувати високошвидкісний доступ за технологією FTTB / Ethernet в більшості багатоквартирних будинків міста. FTTB – найбільш оптимальна сучасна архітектура доступу, що забезпечує високоякісний та одночасно дешевий доступ до мережі Internet. Отже, якщо Ви мешкаєте в багатоквартирному будинку, у Вас є ексклюзивна можливість отримати надзвичайно дешевий доступ до Internet з максимально можливою якістю. Вартість підключення у багатоквартирних будинках зазвичай не перевищує 200 гривень, і включає в себе вартість 20 метрів абонентського кабелю, вартість робіт по його прокладанні від обладнання провайдера до квартири абонента, грозозахисти, які значно зменшать ймовірність пошкодження кінцевого обладнання атмосферною електрикою.

Для підключення в приватному секторі міста, де наявне покриття оптичною мережею, у абонентів є змога підключитися до нашої мережі за технологією FTTH (оптичне волокно у власний будинок). Така технологія забезпечує найвищий на даний момент рівень якості, швидкості та надійності доступу до мережі.

Ніякого додаткового обладнання (модеми, тощо) для підключення за технологією Ethernet купувати не потрібно, але якщо у Вас в квартирі чи власному будинку є кілька комп'ютерів, або Ви активно користуєтеся ноутбуком, нетбуком, смартфоном ми рекомендуємо Вам придбати роутер з бездротовим інтерфейсом, що дасть змогу використовувати Інтернет одночасно на кількох комп'ютерах за єдиним тарифним планом.

Індивідуальні користувачі у віддалених населених пунктах району можуть отримати доступ до Internet за допомогою фіксованого бездротового доступу. Використання сучасних радіо технологій дозволяє отримати швидкісний доступ там, де використання інших технологій підключення неефективне або взагалі неможливе. При бажанні ми можемо організувати бездротовий доступ в Вашому будинку, для зручності використання ноутбуків та інших пристроїв з бездротовим доступом. Вартість індивідуального підключення за технологією фіксованого бездротового зв'язку дуже залежить від використаного обладнання та відстані від базової станції.

Для підключення до Internet Вам необхідно звернутися в наш офіс особисто, або зателефонувавши за телефоном. Термін підключення – від одного до кількох днів. Підключення здійснюється за Вашої присутності і в зручний для Вас час.»

Також я ознайомився з інформаційно-комунікаційною системою, на основі якої і було розглянуто систему захисту роутерів.

1.2 Поняття інформаційного ризику

На сьогодні немає єдиного визначення про те, що таке інформаційний ризик. Згідно з вітчизняними нормативними документами: *ризик (risk)* — функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Проте, деякі [4,5] фахівці розглядають інформаційний ризик як подію, що безпосередньо впливає на інформацію: її видалення, спотворення, порушення її конфіденційності або доступності. Інші розглядають дане поняття в більш вузькому аспекті, обмежуючи зону інформаційного ризику лише інфо-комунікаційними системами. У більшості понять не розглядаються деякі важливі аспекти, яким варто було б приділити увагу. В першу чергу, це фахівці, чия робота пов'язана безпосередньо з введенням інформації в систему і її обробкою. Адже вже на стадії отримання цієї інформації існують ризики, так як навіть на даній стадії існують події, які впливають на достовірність отриманих даних, їх повноту і актуальність.

Також в це визначення інформаційного ризику часто не включаються ризики, пов'язані з виникненням збоїв в алгоритмах обробки інформації, програмах, які використовуються для створення рішень щодо управління. Деякі фахівці підходять до поняття «інформаційні ризики» під іншим кутом зору – економічної. Під визначенням вони розуміють «небезпека виникнення збитків або шкоди внаслідок застосування компанією інформаційних технологій. Іншими словами, IT-ризики пов'язані з створенням, передачею, зберіганням і використанням інформації за допомогою електронних носіїв та інших засобів зв'язку».

1.3 Класифікація інформаційних ризиків

Всі інформаційні ризики можна класифікувати [3-7] на певні категорії за допомогою кількох критеріїв:

- За джерелами інформаційні ризики поділяють на внутрішні і зовнішні;
- За характером дії - на навмисні і ненавмисні;
- За видами - прямі або непрямі;

- За результатом дії- порушення достовірності інформації, порушення актуальності інформації, порушення повноти інформації, порушення конфіденційності та ін.
- За механізмами впливу: стихійні лиха, аварії, помилки фахівців і ін.

1.4 Методики аналізу, оцінки та управління ризиками інформаційної безпеки

Згідно з вітчизняними нормативними документами: *аналіз ризику* (risk analysis) — процес визначення загроз безпеці інформації та їх характеристик, слабких сторін комплексної СЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації інформаційно-телекомунікаційних систем.

Аналіз інформаційних ризиків - це процес сукупного оцінювання ступеня захисту інформаційної системи з визначенням кількісних (у формі грошових ресурсів) і якісних (рівні ризику: високий, середній, низький) показників ризику. Аналіз здійснюється за допомогою різних інструментів і методів формування процесів [6] захисту інформації. На основі його результатів виділяються самі високі ризики, які є небезпечною загрозою і потребують негайного вжиття додаткових захисних заходів.

Єдиної методики, за якою можна було б визначити кількісну величину ризику, на сьогоднішній день не існує. По-перше, це обумовлено відсутністю необхідного обсягу статистичної інформації про можливості виникнення будь-якої конкретної загрози. По-друге, відіграє важливу роль той факт, що визначити величину вартості конкретного інформаційного ресурсу часом дуже важко.

Наприклад, власник інформаційного ресурсу легко може вказати вартість обладнання і носіїв, проте назвати точну вартість даних, що знаходяться на цьому обладнанні та носіях, він фактично не в змозі. Тому

найчастіше користуються якісною оцінкою інформаційних ризиків, головні завдання якої - ідентифікувати фактори ризику, визначити можливі вразливі області ризику і оцінити вплив кожного з видів.

Найбільш відомий підхід до кількісного розрахунку інформаційних ризиків - британський метод CRAMM (рис 1.1). Його основними цілями є: автоматизація управління ризиками, оптимізація фінансових витрат на управління, оптимізація часу на супровід систем безпеки компанії, підтримка безперервності бізнесу.

CRAMM [5-7] передбачає поділ всієї процедури на три послідовні етапи. Завданням першого етапу є відповідь на питання: «Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції безпеки, або необхідно проведення більш детального аналізу?» На другому етапі проводиться ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується питання про вибір адекватних контрзаходів.

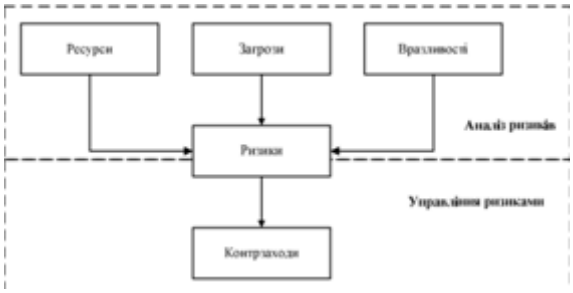

Рисунок 1.1 — Методика CRAMM

До недоліків методу CRAMM можна віднести наступні фактори:

- Використання методу CRAMM вимагає спеціальної підготовки і високої кваліфікації аудитора;
- CRAMM в набагато більшому ступені підходить для аудиту вже існуючих ІС, які знаходяться на стадії експлуатації, ніж для ІС, що знаходяться на стадії розробки;

- Аудит за методом CRAMM - процес досить трудомісткий і може зайняти багато місяців безперервної роботи аудитора;
- Програмний інструментарій CRAMM генерує велику кількість паперової документації, яка не завжди виявляється корисною на практиці;
- CRAMM не дозволяє створювати власні шаблони звітів або модифікувати наявні;
- Можливість внесення доповнень до бази знань CRAMM недоступна користувачам, що викликає певні труднощі при адаптації цього методу до потреб конкретної організації;
- Програмне забезпечення CRAMM існує тільки на англійській мові;
- Висока вартість ліцензії.

2. ПРОЕКТНО-ПРАКТИЧНА ЧАСТИНА

2.1 Аналіз вразливостей захищеності інформ комунікаційної мережі організації

Дана мережа реалізується як складна структура, що містить багато елементів. Ця структура постійно змінюється, оскільки якісь елементи старіють та потребують заміни або оновлення конфігурацій. Для знаходження недоліків захисту різних компонентів і визначення потенційних векторів атак на мережу, проводиться аналіз захищеності. Ефективний спосіб аналізу - тестування на проникнення[5], в ході якого моделюється реальна атака зловмисників. Такий підхід дозволяє об'єктивно оцінити стан захищеності системи і зрозуміти, чи можуть протистояти атакам існуючі засоби захисту.

При аналізі захищеності мережі, вразливості розділяють на чотири категорії:

- недоліки конфігурації;
- відсутність оновлень безпеки;
- вразливості в коді веб-додатків;
- недоліки політики паролів.

Для прикладу нижче буде таблиця (Таблиця 2.1) з вразливостями веб-додатків, та їх відсоткова частка.

Для виправлення вразливостей, зазвичай, потрібно редагувати певний сегмент коду, на що може знадобитися чимало часу. Щоб зберегти безперервність бізнес-процесів, рекомендується застосовувати міжмережевий екран додатків (web application firewall), який не дозволяє експлуатувати вразливість, поки її не усунули, а також захистить від нових і ще не знайдених вразливостей.

Таблиця 2.1 — Вразливості веб-додатків, які дозволяють подолати мережевий периметр

Вид вразливості	Частка векторів
Вразливість в коді додатків	83%
Словарні паролі	28%
Використання компонент з відомими вразливостями	17%
Недоліки конфігурації	17%

Web Application Firewall [5] (WAF, міжмережевий екран для веб-додатків) являє собою пристрій безпеки (апаратний або віртуальний), основним завданням якого є захист web-порталів і web-додатків шляхом перевірки XML / SOAP семантики потокового трафіку, а також перевірки HTTP / HTTPS трафіку з метою виявлення різних атак на рівні додатків. Міжмережевий екран для веб-додатків діє як проксі-сервер, але завдяки здатності аналізувати HTTPS трафік (шляхом імпорту сертифіката безпеки цільового сервера), також може виконувати й інші функції, такі як термінація SSL трафіку і балансування навантаження сервера. Крім того WAF підтримує кластеризацію, а також виконує акселерацію web-додатків. WAF підтримує два основні режими розгортання: Gateway (bridge mode, transparent proxy, reverse proxy) (рис.2.1); Monitor (режим мережевого моніторингу через SPAN порт) (рис. 2.2).

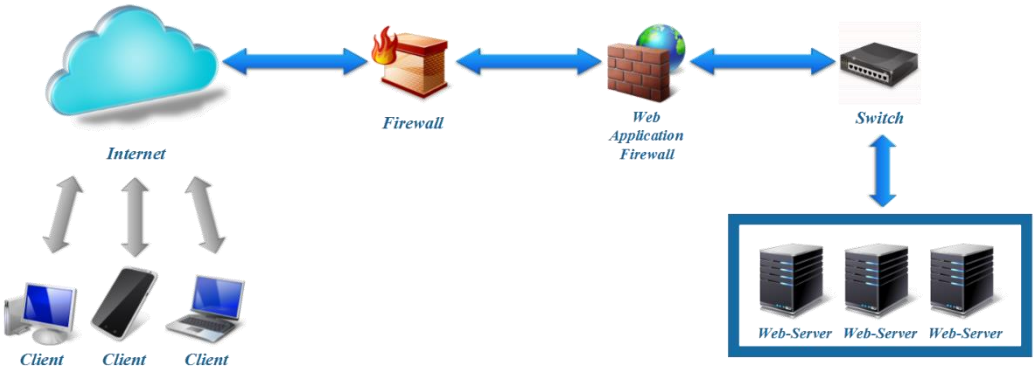

Рисунок 2.1 — Розгортання WAF в режимі Gateway

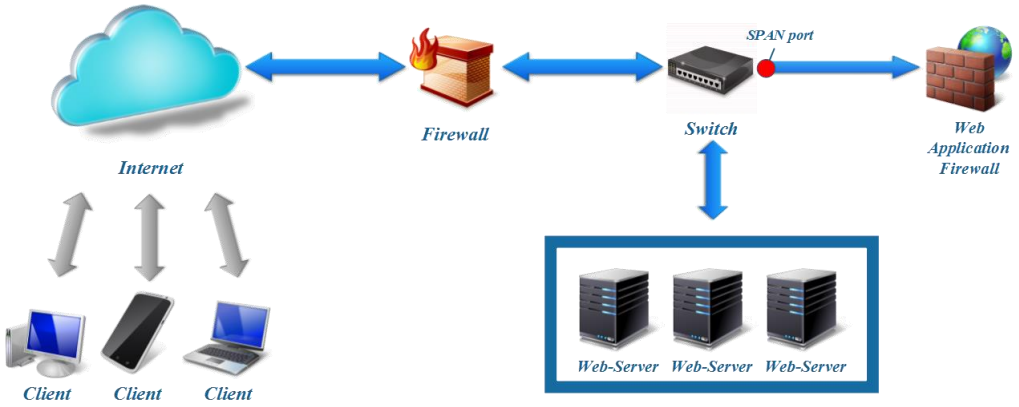

Рисунок 2.2 — Розгортання WAF в режимі Monitor

Інші загрози складаються переважно в підборі словникових паролів до різних систем - Outlook Web App (OWA), VPN-серверів і робочих станцій, а також у використанні недоліків конфігурації мережевого устаткування. Проникнення через периметр потенційно можливо і через застарілі версії ПЗ, які містять уразливості, що дозволяють отримати контроль над сервером. Для багатьох таких вразливостей є загальнодоступні експлойти, але їх експлуатація може порушити роботу систем.

Один [8] з найпоширеніших варіантів проведення успішних атак для подолання зовнішнього периметра - знаходження на мережевому периметрі інтерфейсів систем, які повинні бути доступні виключно з внутрішньої мережі. Дуже поширене некоректне налаштування і

вразливості в системах відеоспостереження (рис. 2.3). Зловмисники можуть не тільки переглядати відео з камер, але і виконати довільний код через застарілої версії прошивки відеореєстратора, причому одна з вразливостей (CVE-2013-0143) була опублікована вісім років тому, але досі не усунута. Саме тому варто варто чітко визначати межі мережевого периметру та стежити за станом захисту всієї системи.

Рисунок 2.3 — Експлуатація вразливостей в мережі відеоспостереження

Для каналів зв’язку можливі наступні атаки: перехоплення даних, зміна, умисні перешкоди при передачі; нестабільна передача даних не пов'язана безпосередньо з зловмисним втручанням.

Десятка найбільш поширених вразливостей (таблиця 2.2) на мережному периметрі залишається незмінною протягом останніх років. Раніше відзначалося істотне зниження частки компаній, де були виявлені словникові паролі, але в 2018 – 2019 рр.. вони повернулися на перші рядки рейтингу. Все ще широко поширене використання відкритих протоколів передачі даних, в тому числі для доступу до інтерфейсів адміністрування.

Таблиця 2.2 — Топ-десятка найпоширеніших вразливостей на мережному периметрі

№	Вид вразливості	Частка систем
1	Використання відкритих протоколів передачі даних	83%
2	Словникові паролі	75%
3	Вразливі версії програмного забезпечення	67%
4	Завантаження довільних файлів	67%
5	Інтерфейси віддаленого доступу, управління обладнанням і підключення до СУБД доступні будь-якому інтернет-користувачеві	58%
6	Зберігання важливих даних у відкритому вигляді або у відкритому доступі	58%
7	Надмірні привілеї додатків або СУБД	42%
8	Віддалене виконання коду	33%
9	Відсутність автентифікації при доступі до критично важливих ресурсів	25%
10	Впровадження SQL коду	17%

На ресурсах мережевого периметра часто зберігаються у відкритому вигляді важливі дані, які допомагають зловмисникам розвинути атаку. Це можуть бути резервні копії веб-додатків, конфігураційна інформація про систему, облікові дані для доступу до критично важливих ресурсів або ідентифікатори користувачів, до яких зловмисник може підібрати пароль.

Для зменшення ризику від цих вразливостей слід переконатися, що у відкритому вигляді (наприклад, на сторінках веб-додатку) не зберігається інформація, що важливою для безпеки мережі. До такої інформації можуть відноситися облікові дані для доступу до різних ресурсів, адресна книга компанії, яка містить електронні адреси і доменні ідентифікатори співробітників, і т. п. Якщо у компанії не вистачає ресурсів, щоб виконати такі перевірки власними силами, то слід залучати сторонніх експертів для тестування на проникнення.

Актуальною залишається і проблема несвоєчасного оновлення ПЗ. Найчастіше виявляються вразливі версії прикладного ПЗ, веб-серверів і веб-додатків, що поставляються вендорами – компаніями,[8] які розробляють і поставляють продукцію під своєю торгівельною маркою.

Якщо на сервері був виявлений інтерфейс внутрішньої мережі то далі зловмисник може розвивати атаку на ресурси локальної мережі. Тому варто своєчасно встановлювати оновлення безпеки для ОС і останні версії прикладного ПЗ.

2.2 Дослідження захищеності бездротових мереж

Бездротова мережа є потенційним вектором проникнення у внутрішню інфраструктуру компанії. Зловмиснику потрібно лише встановити на комп'ютер програмне забезпечення для атак на бездротові мережі і придбати недорогий модем, який може працювати в режимі моніторингу трафіку. У нашій системі бездротова мережа була доступна за межами контрольованої зони, отже зловмисник може проводити атаки, перебуваючи на прилеглій території, наприклад на вулиці поруч з офісом. Майже у мережі використовувався протокол WPA2 з методами автентифікації PSK або EAP.

В залежності від використовуваного методу автентифікації можлива реалізація різних типів атак. Для WPA2 / PSK [8] проводиться перехоплення «рукостискання» між точкою доступу і легітимним клієнтом точки доступу (рис 2.4) з наступним підбором паролів методом перебору. Успіх цієї атаки обумовлений складністю пароля.

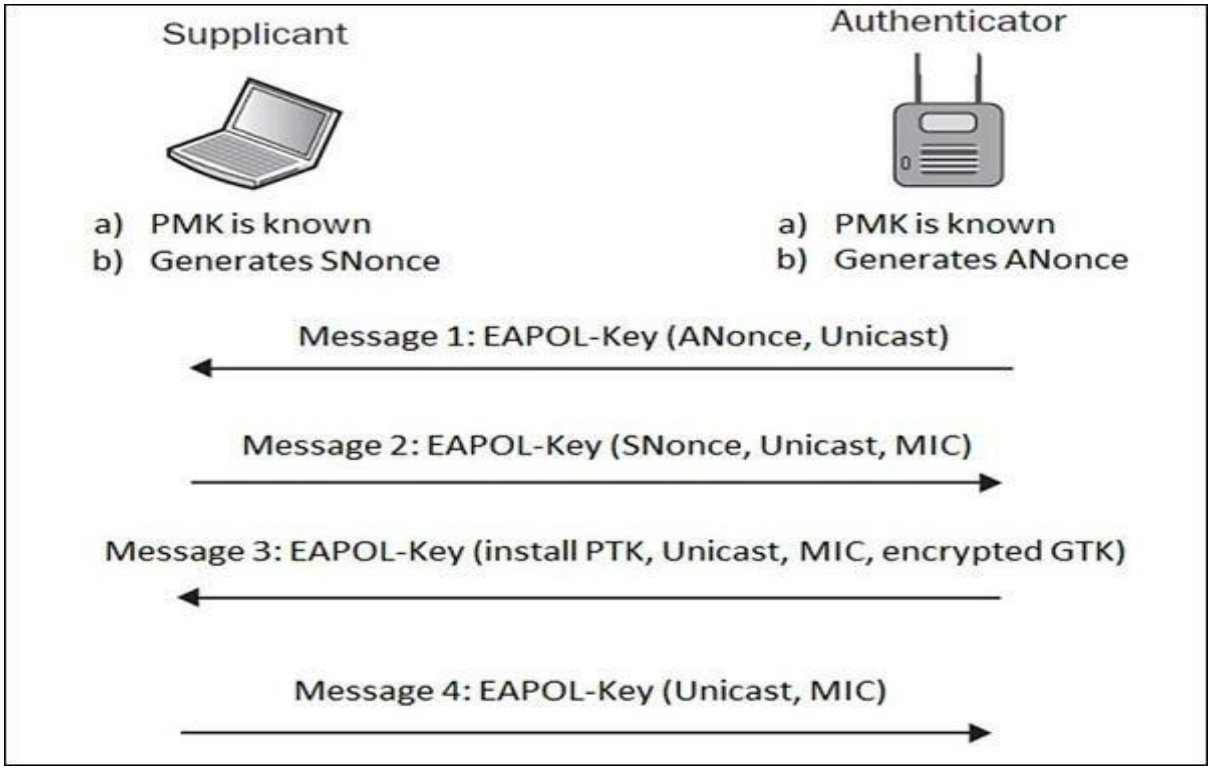

Рисунок 2.4 — Алгоритм «рукостискання» у бездротовій мережі

Наступний спосіб атаки «створення підробленої [6] точки доступу» (рис 2.5) - застосовується для будь-якого методу автентифікації. Якщо при підключенні до бездротової мережі не проводиться перевірка достовірності сертифікатів, то зловмисник може створити підроблену точку доступу з ідентичною назвою мережі (ESSID) і більш потужним сигналом, ніж у оригінальної. У разі підключення клієнта до цієї точки доступу зловмисник отримує його ідентифікатор у відкритому вигляді і значення NetNTLM v1 challenge-response, за допомогою якого може підібрати пароль методом перебору .

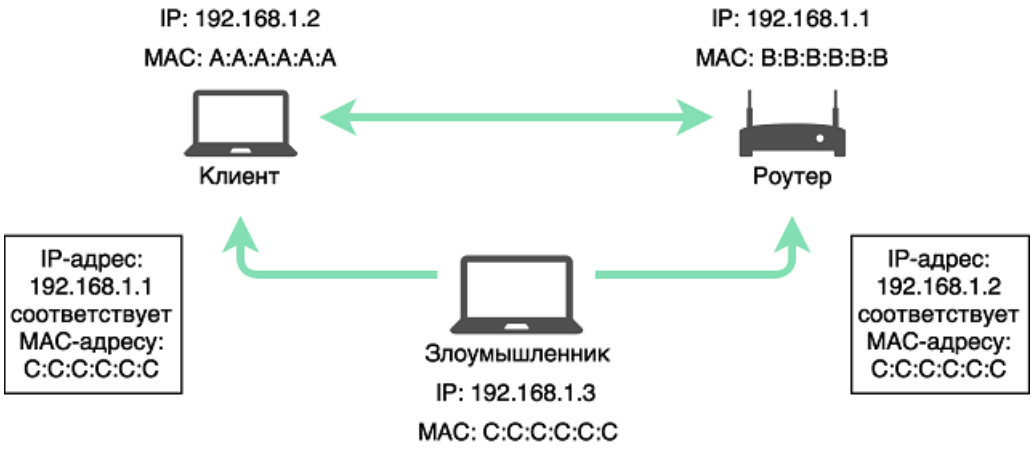

Рисунок 2.5 — Створення підробленої точки доступу

Навіть якщо оригінальна точка доступу використовує механізми захисту, підроблена точка може бути відкритою і підключення до неї пройде непомітно для користувача. Більше вірогідне можливе проведення так званої «KARMA-атаки» (рис 2.6). Багато пристроїв відправляють запити з метою знайти раніше збережені мережі. Зловмисник може створювати підроблені відкриті точки доступу, представляючись тієї мережею, назва якої міститься в запиті. Такі атаки застосовуються в сукупності з використанням неправдивої форми автентифікації. При підключенні до мережі користувач перенаправляється на сторінку з формою автентифікації, де йому пропонується ввести свій обліковий запис мережі організації.

Рисунок 2.6 — Проведення KARMA-атаки з використанням фішингової форми автентифікації

2.3 Дослідження вразливостей словникових паролів

Дані паролі найчастіше зустрічаються в доменних облікових записах і при доступі до веб-додатків [6] - як на мережному периметрі, так і у внутрішній інфраструктурі компаній.

Нижче подано таблицю (таблиця 2.3) з відсотковою часткою використання словникових паролів.

Таблиця 2.3 — Словникові паролі

Місце застосування	Частка систем
Домен, електронна пошта	63%
Веб-додатки	63%
СУБД	38%
Файлові сервери	13%

Qwerty123 і інші поєднання близьких клавіш залишаються найпопулярнішими паролями серед звичайних користувачів, admin найпоширеніший пароль серед привілейованих користувачів. Таблиця (таблиця 2.4) з найпоширенішими паролями та їх відсотком використання подано нижче.

Таблиця 2.4 — Найпоширеніші словникові паролі

	Адміністратор	Користувач
Близькі поєднання клавіш на клавіатурі	25%	38%
Admin	31%	-
p@sswOrd	13%	19%
123456	13%	13%
%username%	6%	13%

2.4 Вразливості міжмережевого екрану

Для покращення безпеки мережі компанія мала ціль додати в систему міжмережевий екран Cisco ASA. Тому додатково було проведено аналіз вразливостей даного екрану.

Міжмережеві екрани Cisco ASA, які використовуються в мережі, схильні до критичної вразливості CVE-2018-0101[5-8], що дозволяє зловмисникам здійснювати віддалене виконання довільного коду. Крім того, помилка може призводити до відмови в обслуговуванні і провокувати перезавантаження системи. Для експлуатації цієї вразливості зловмисникам необхідно сформувати спеціальні XML-пакети і відправити їх на інтерфейс, на якому налаштований webvpn - це відкриє можливість виконання

довільного коду і дасть зломщикові повний контроль над системою або призведе до перезавантаження пристрою. Уразливість отримала найвищий бал критичності CVSS. Серед вразливих продуктів Cisco ASA: 3000 Series Industrial Security Appliance (ISA); ASA 5500 Series Adaptive Security Appliances; міжмережеві екрани ASA 5500-X Series Next-Generation; ASA Services Module для коммутаторів Cisco Catalyst 6500 Series и маршрутизаторов Cisco 7600 Series; міжмережевий екран ASA 1000V Cloud; Adaptive Security Virtual Appliance (ASAv); Firepower 2100 Series Security Appliance; Firepower 4110 Security Appliance; Модуль Firepower 9300 ASA Security; Firepower Threat Defense (FTD) .

Для подолання цієї вразливості Cisco запропонувала користувачам свою політику безпеки.

2.5 Вразливості роутерів D-Link

Оскільки у даній мережі використовуються роутери D-Link, було проведено аналіз їх вразливостей, для визначення подальшої доцільності використання пристроїв.

У роутерах D-Link виявлена [1,5-8] небезпечна вразливість (CVE-2019-16920), яка дозволяє віддалено виконати код на стороні пристрою через відправку спеціального запиту до обробника "ping_test", доступному без проходження автентифікації. Варто зазначити, що за задумом розробників прошивки виклик "ping_test" повинен виконуватися тільки після автентифікації, але реально він викликається в будь-якому випадку, незалежно від входу в web-інтерфейс. Зокрема, при зверненні до скрипту apply_sec.cgi з передачею параметра "action = ping_test", скрипт перекидає на сторінку аутентифікації, але при цьому виконує пов'язане з ping_test дію. Для виконання коду використана ще одна уразливість в самому ping_test, який викликає утиліту ping без належної перевірки коректності переданого

для тестування IP-адреси. Наприклад, для виклику утиліти wget і передачі на зовнішній хост результатів виконання команди "echo 1234" досить вказати параметр "ping_ipaddr = 127.0.0.1% 0awget% 20-P% 20 / tmp /% 20http: //test.test/? $ (echo-1234) " .

Наявність уразливості офіційно підтверджено в моделях:

DIR-655 з прошивкою 3.02b05 або старішою;

DIR-866L з прошивкою 1.03b04 або старішою;

DIR-1565 з прошивкою 1.01 або старішою;

DIR-652 (даних про версії проблемних прошивок не наводиться) .

Час супроводу даних моделей вже минув, тому компанія D-Link заявила, що не буде випускати для них оновлення з усуненням уразливості, не рекомендує використовувати і радить замінити на нові пристрої. Для припинення обхідного шляху захисту можна обмежити доступ до web-інтерфейсу тільки для тих IP-адрес, які заслуговують на довіру. Пізніше з'ясувалося, що уразливість також стосується моделі DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835 і DIR-825. Враховуючи отримані результати було вирішено замінити пристрої D-Link на пристрої іншого виробника, для цього було проведено аналіз вразливостей наступних пристроїв, а саме:

- роутерів Linksys;

На так давно,в літку 2019 р., майже одночасно з інформацією про проблеми з роутерами Cisco, [1]в мережі з'явилися новини про вразливість тисяч розумних роутерів Linksys. Діра в захисті цих пристроїв дозволяє отримати віддалений неавторизований доступ до них. Сканування мережі виявило 25,617 Linksys Smart Wi-Fi пристроїв, які відкриті для дій зловмисників. Останнім доступні не тільки MAC-адреси пристроїв, але і дані про модель, версії ОС, налаштування WAN, версії прошивки, настройках, конфігурації DDNS. Зловмисникам можуть стати в нагоді як всі ці дані, так і доступ до самим роутера для формування з них ботнетів. Вразливі десятки моделей роутерів .

– роутерів MicroTik;

Наприкінці 2018 р. стало відомо про те, що невідомі зловмисники скомпрометували тисячі роутерів MikroTik [1]для створення ботнету. Незважаючи на те, що вразливість виявили в квітні 2018 року, вона залишалася актуальною ще довгий час, оскільки далеко не всі власники роутерів стали встановлювати оновлення прошивки. Спочатку проблема привела до того, що багато тисяч роутерів були скомпрометовані. 240 тисяч роутерів були атаковані і перетворені в SOCKS4 проксі, які використовуються для своїх потреб зловмисниками. На кінець 2018 р. в мережі працювало кілька сотень тисяч роутерів, вразливість в яких не була виправлена. Можна думати, що не виправлена вона і досі. Скомпрометовані роутери теж працюють, перенаправляючи мережевий трафік, включаючи FTP і e-mail. Дослідники з мережевої безпеки виявили і дані, що характерні для процесів віддаленого управління мережевими пристроями. Пакети даних відправляються на IP провайдера з Белізу (держави в Центральній Америці)[7] - невідомо, це лише маскування, або ж зловмисники фізично знаходяться в цьому регіоні. Як би там не було, якщо комусь із зловмисників інших груп кіберзлочинців прийде в голову використовувати роутери компанії для, наприклад, формування ботнету, це можна зробити без проблем.

– роутерів Huawei;

У грудні 2017 року було зафіксовано масивна атака на роутери китайської компанії Huawei. Зловмисники використовували вразливість CVE-2017-17215 для отримання доступу до пристроїв Huawei[1] HG532. Як виявилося, цю дірку активно використовували ботнети Brickerbot і Satori. Фахівці з інформаційної безпеки, які виявили проблему, повідомили про неї в компанію. Але, на жаль, невідомо, наскільки оперативно ця діра була прикрита і чи прикрита вона взагалі.

В середині 2018 року всього за один день було інфіковано близько 18 000 мережних пристроїв Huawei, з яких зловмисник сформував ботнет. Як стало відомо, кіберзлочинець скористався все тієї ж вразливістю CVE-2017-17215, про яку йшла мова вище.

Цілком ймовірно, що, як і в попередніх випадках, в мережі до сих пір працюють десятки тисяч пристроїв, схильні до зазначеної уразливості, що робить роутери модельного ряду HG532 відкритими для зовнішніх факторів.

3. ПРАКТИЧНА ЧАСТИНА

3.1 Підключення роутера MikroTik

Схема підключення роутера MikroTik (Рис. 3.1):

- кабель провайдера інтернету підключаємо в перший порт роутера;
- комп'ютер підключаємо до роутера MikroTik мережевим кабелем в будь-який LAN порт від 2 до 5;
- ноутбук та інші бездротові пристрої підключено по Wi-Fi;
- блок живлення під’єднано в роз'єм «Power» роутера MikroTik.
-

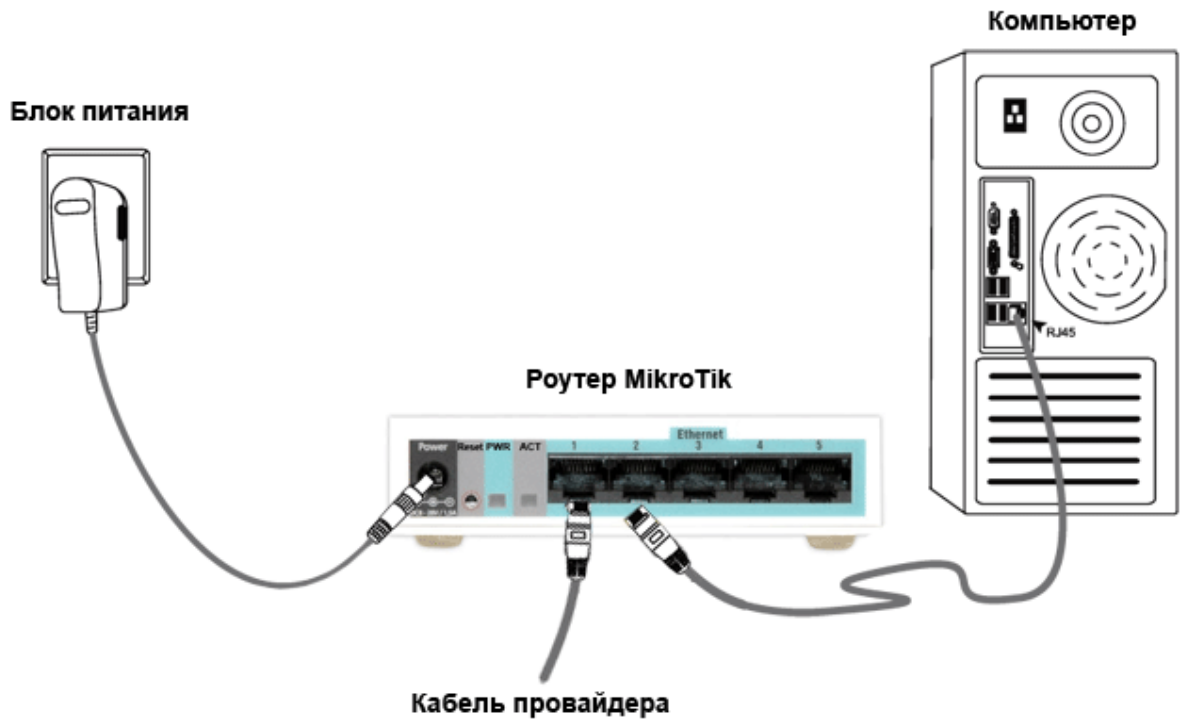

Рисунок. 3.1 — Схема підключення роутера MikroTik

3.2 Налаштування мережевої карти комп’ютера

Щоб на комп'ютері можна було зайти в налаштування роутера Mikrotik (Рис 3.2), налаштовується мережева карта на отримання автоматичних налаштувань.

Переходиться за наступним посиланням «Пуск» → «Панель управління» → «Центр управління мережами і загальним доступом».

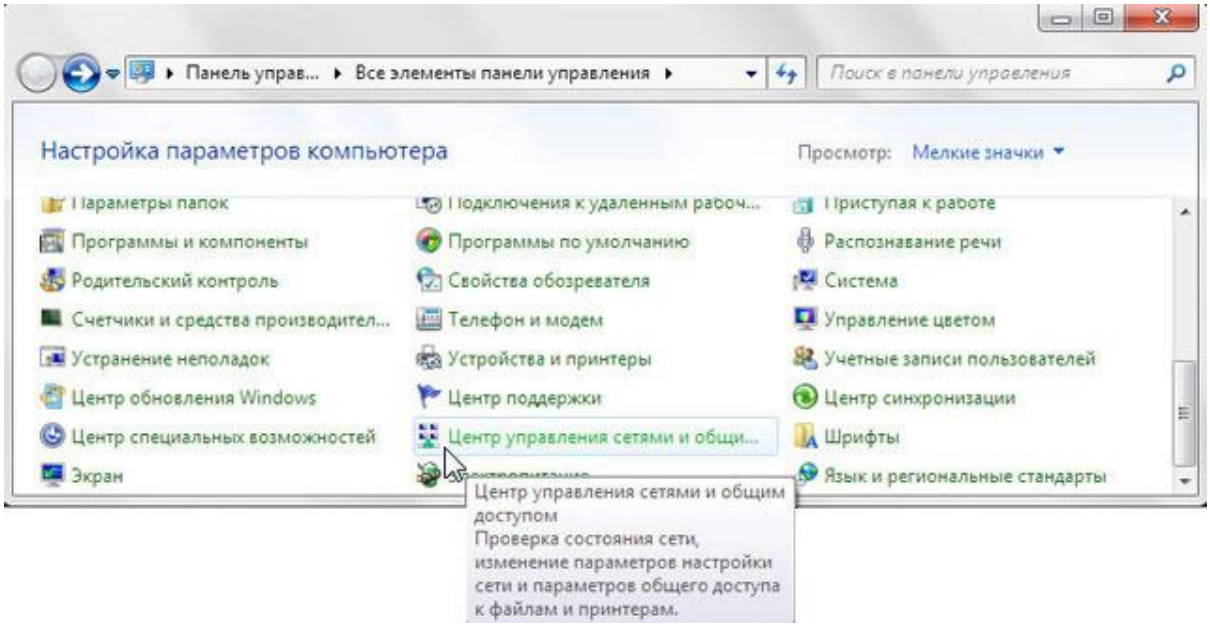

Рисунок. 3.2 — Панель управління

Далі в «Зміна параметрів адаптера» (Рис. 3.3).

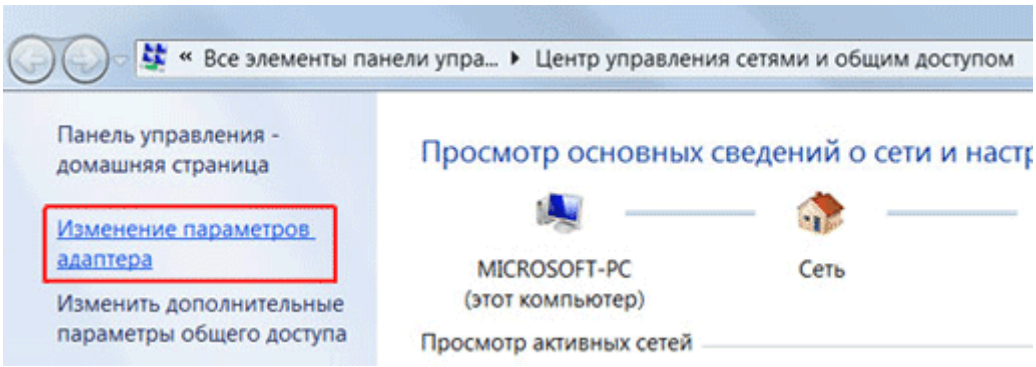

Рисунок. 3.3 — Зміна параметрів адаптера

Відкривається контексте меню на «Підключення по локальній мережі» і вибирається «Властивості»(Рис. 3.4).

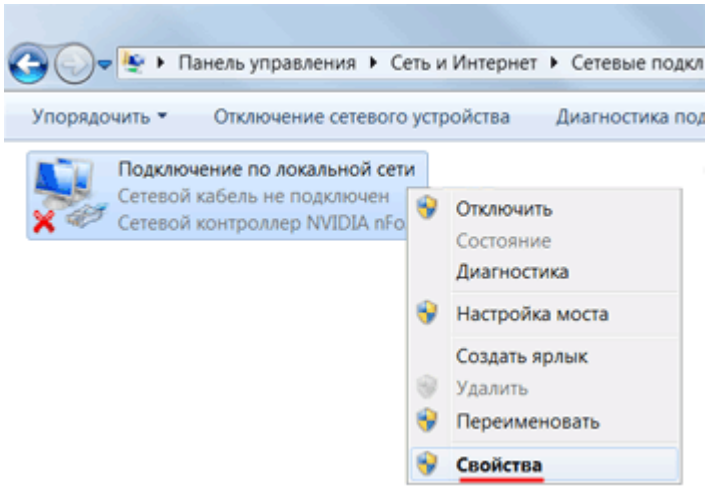

Рисунок 3.4 — Контекстне меню

Натискається на «Протокол Інтернету версії 4 (TCP / IPv4)» і кнопку «Властивості»(Рис 3.5).

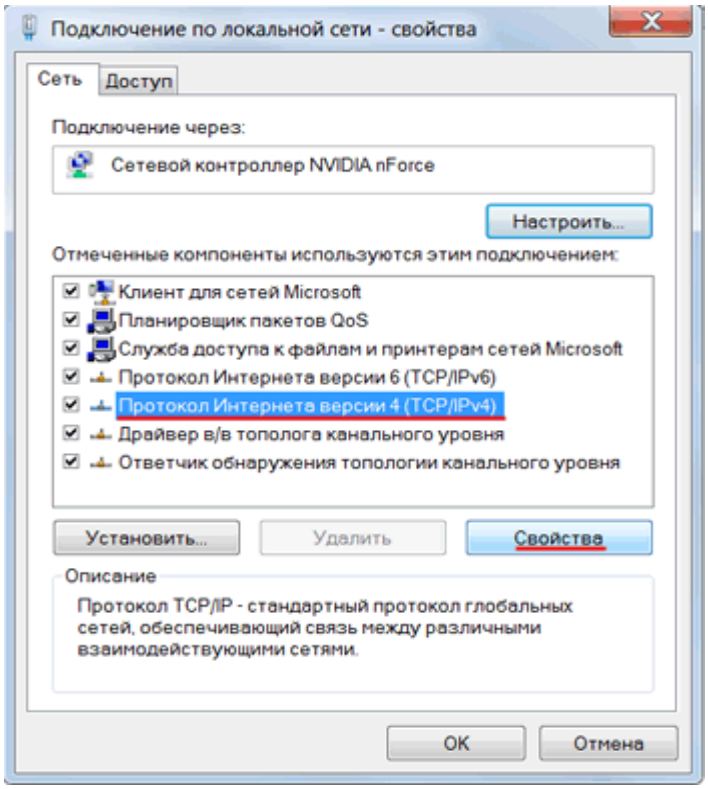

Рисунок 3.5 — Властивості

Вибирається «Отримати IP-адресу автоматично»(Рис 3.6) і натискається кнопку «ОК».

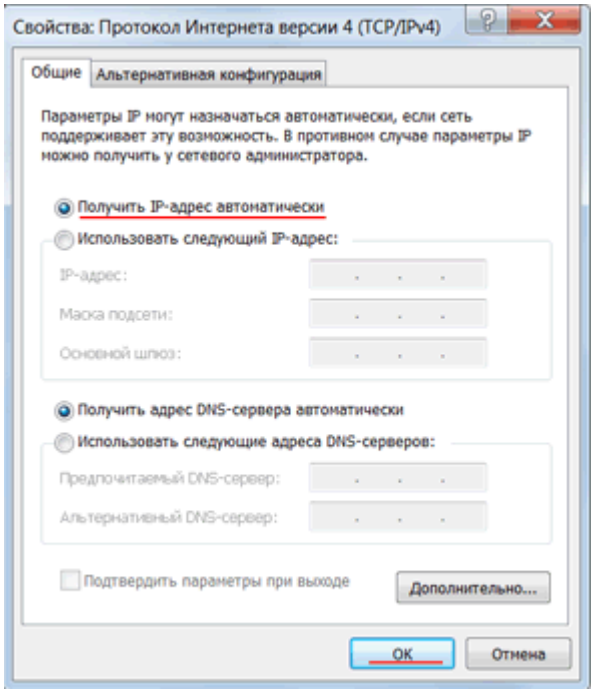

Рисунок 3.6 — Отримання ip-адреси

3.3 Вхід в налаштування роутера MikroTik

Виконати налаштування роутера MikroTik можна різними способами:

- За допомогою спеціальної програми Winbox для ОС Windows. Завантажити на офіційному сайті.
- За допомогою браузера, перейшовши за адресою 192.168.88.1. В налаштуваннях браузера не повинен бути зазначений proxy-сервер!
- Налаштування через Telnet.

В даному проекті роутерMikroTik налаштовується за допомогою програми Winbox.

Підключення до роутера MikroTik (Рис 3.7) здійснюється наступним чином:

- Запускається програма Winbox і переходиться на вкладку Neighbors;

– У списку відобразиться мій роутер. Натискається лівою кнопкою миші на його MAC адресу;
– Натискається кнопку Connect.

  Login за замовчуванням admin, пароль відсутній.

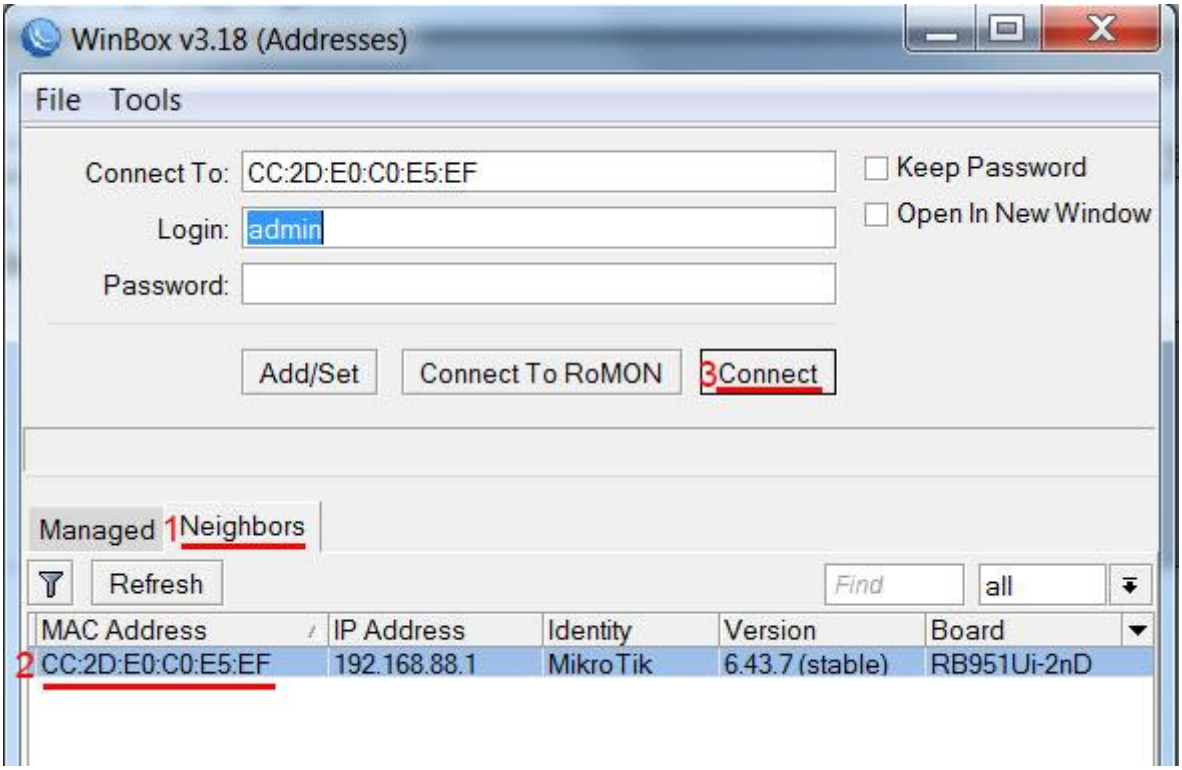

Рисунок 3.7 — Підключення до маршрутизатора MikroTik

3.4 Скидання налаштувань роутера

При першому вході з'явиться вікно (Рис 3.8). Натискається кнопку Remove Configuration і очікується перезавантаження пристрою.

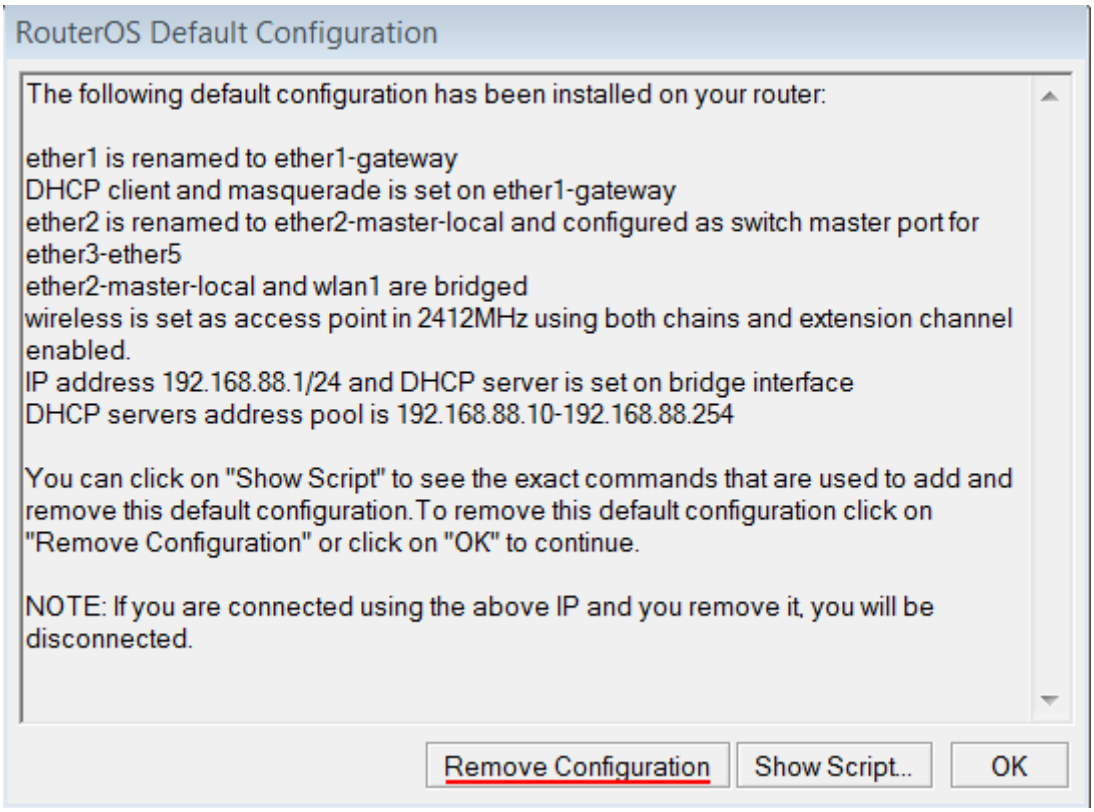

Рисунок 3.8 — Конфігурація за замовчуванням

У випадку якщо дане вікно чомусь не з’явилось, попередню конфігурацію можна скинути вручну(Рис 3.9):

- Вибирається зліва меню System - Reset Configuration;
- Ставиться галочку No Default Configuration;
- Натискається кнопку Reset Configuration.
- Підтверджується скидання (натискаючи кнопку Yes) і очікується перезавантаження пристрою.

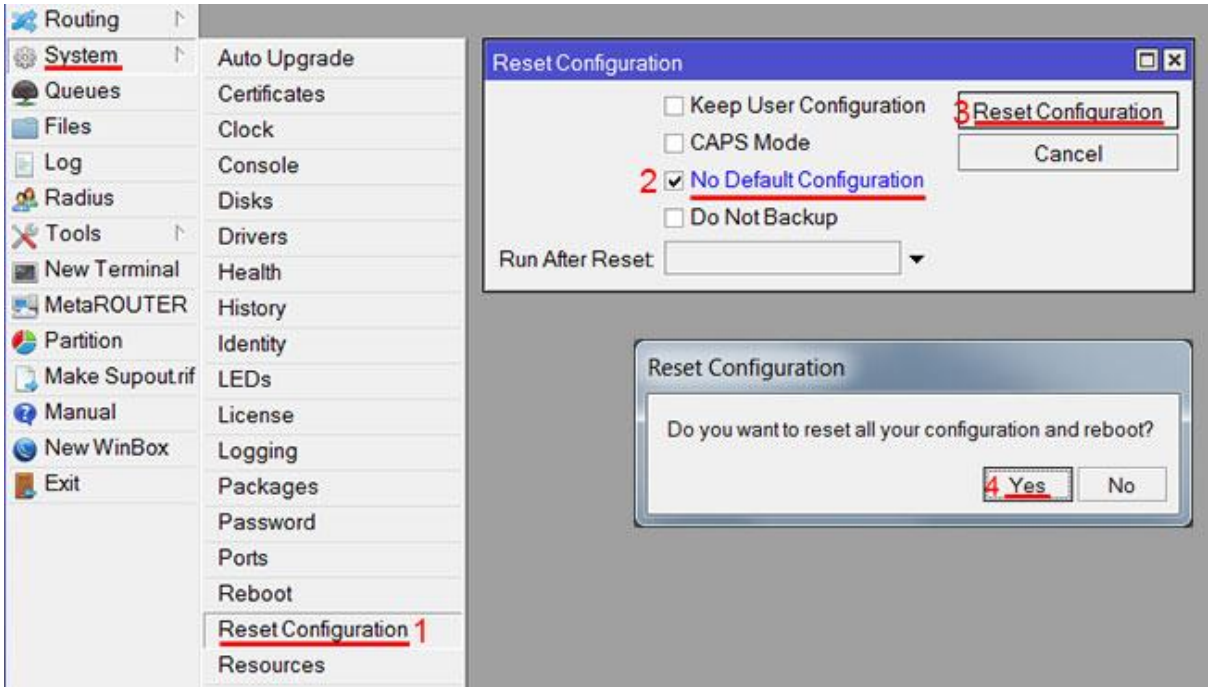

Рисунок 3.9 — Скидання вручну

3.5 Опис мережевих інтерфейсів

Конфігурація мережевих інтерфейсів MikroTik буде виглядати наступним чином: перший порт ether1 буде підключений до провайдера (WAN порт), інші порти ether2-5 працюватимуть в режимі комутатора для підключення комп'ютерів локальної мережі.

Щоб не плутати мережеві інтерфейси, описується їх за допомогою коментарів.

Запис для першого порту ether1 коментар (Рис 3.10)"WAN":

- Відкривається меню Interfaces;
- Вибирається перший інтерфейс ether1;
- Натискається жовту кнопку Comment;
- У вікні вводиться коментар "WAN";
- Натискається кнопку OK.

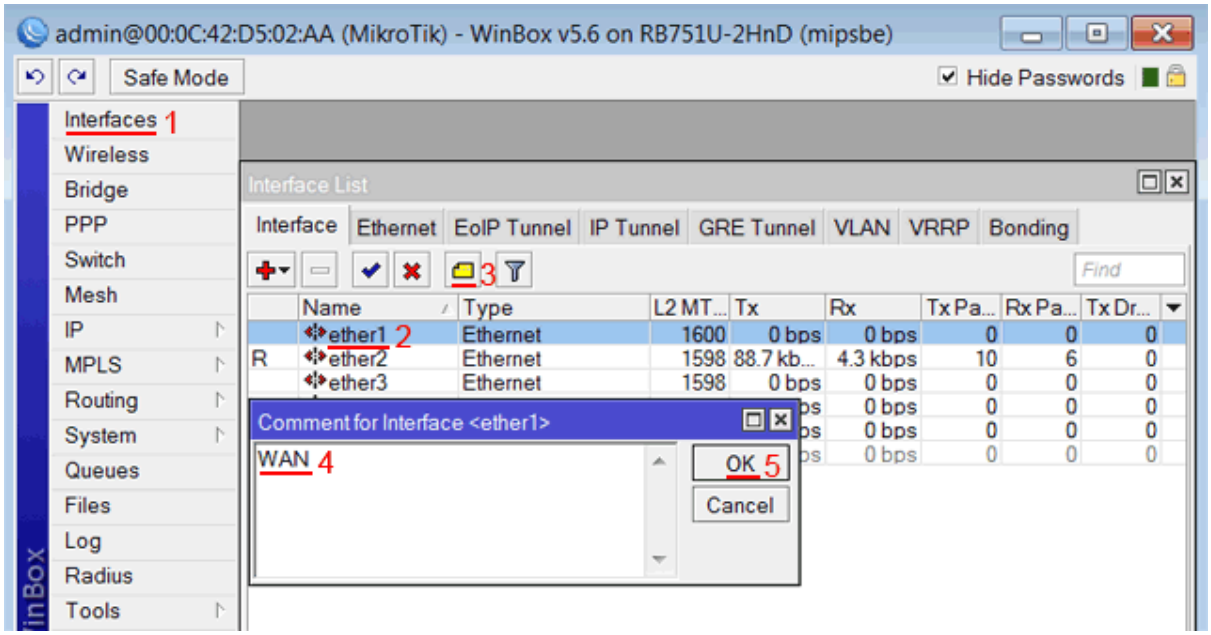

Рисунок 3.10 — Коментар до ether1

Так само записується для другого порту ether2(Рис 3.11) коментар "LAN":

- Вибирається інтерфейс ether2;
- Натискається жовту кнопку Comment;
- У вікні вводиться коментар "LAN";
- Натискається кнопку OK.

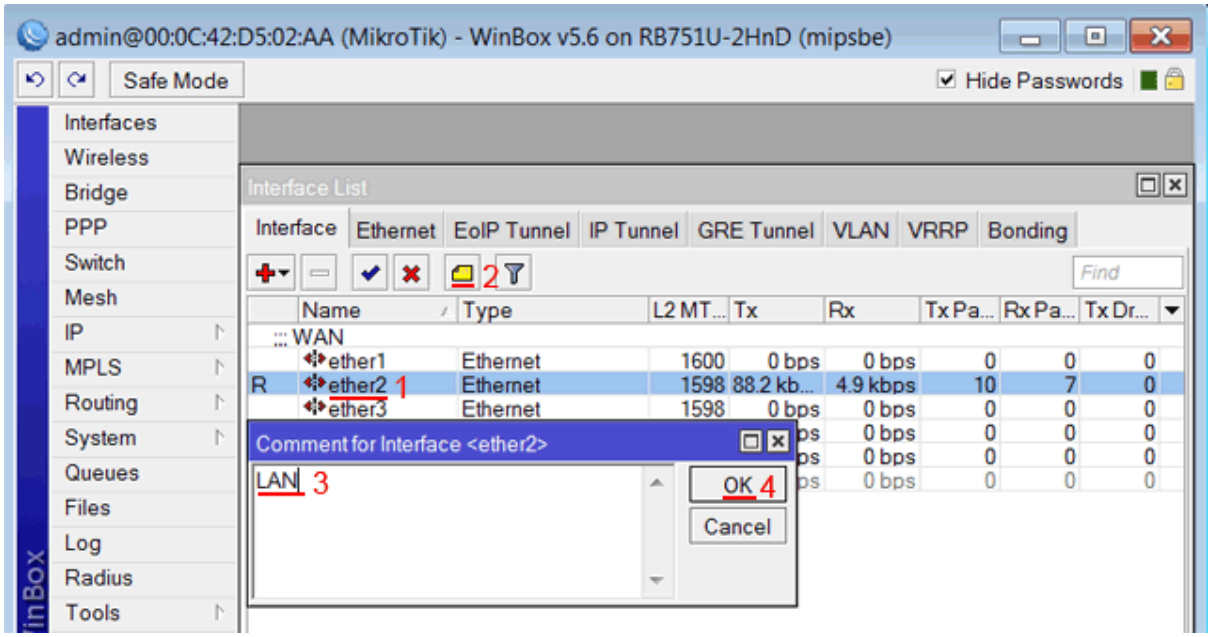

Рисунок 3.11 — Коментар до ether2

3.6 Налаштування WAN інтерфейсу MikroTik

– Налаштування Dynamic IP

Необхідно налаштувати WAN порт(Рис 3.12) маршрутизатора MikroTik на отримання налаштувань по DHCP:

– Відкривається меню IP;
– Вибирається DHCP Client;
– У вікні натискається кнопку Add (плюсик);
– У новому вікні в списку Interface: вибирається WAN інтерфейс ether1;
– Натискається кнопку OK для збереження налаштувань.

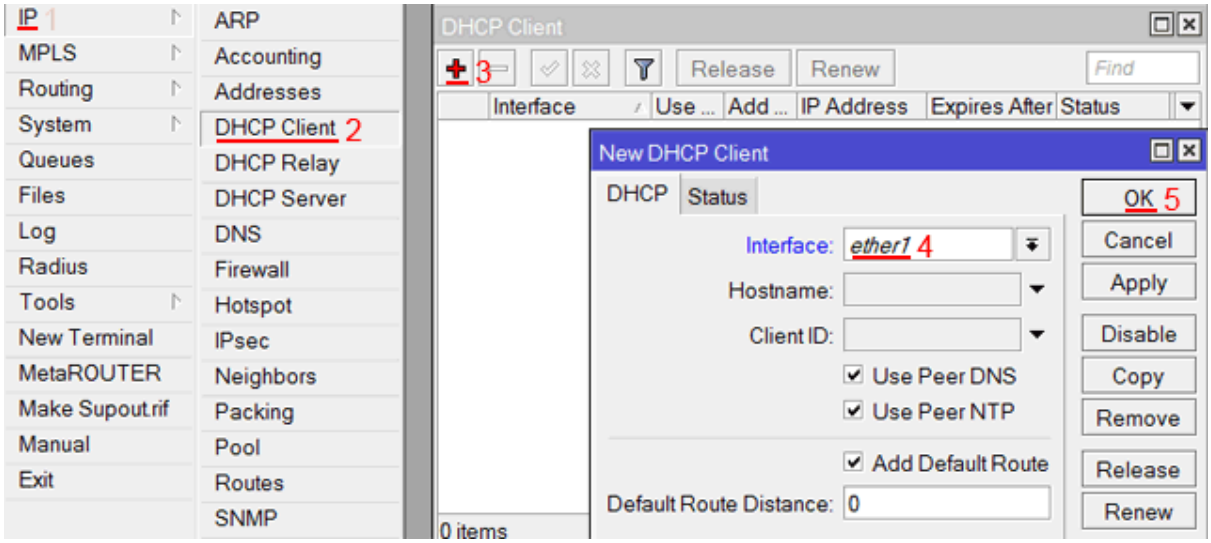

Рисунок 3.12 — DHCP Client

– Налаштування Static IP

Налаштування статичної IP адреси (Рис 2.13) і маски підмережі WAN порту MikroTik:

– Відкриваю меню IP;
– Вибираю Addresses;
– У вікні натискаю кнопку Add (плюсик);
– У новому вікні в полі Address: прописую статичну IP адресу/ маску підмережі;
– У списку Interface: вибираю WAN інтерфейс ether1;
– Для збереження налаштувань натискаю кнопку OK.

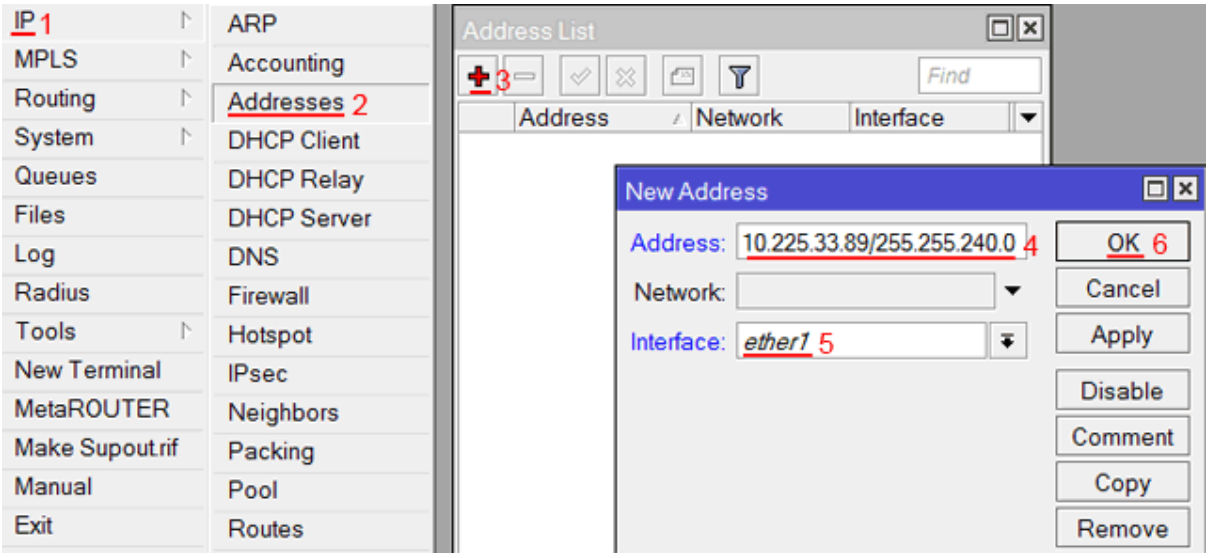

Рисунок 2.13 — New Address

Налаштування адреси інтернет-шлюзу MikroTik (Рис 3.14):

– Відкривається меню IP;
– Вибирається Routes;
– У вікні натискається кнопку Add (плюсик);
– У новому вікні в полі Gateway: прописується IP адреса шлюзу;
– Натискається кнопку OK для збереження налаштувань.

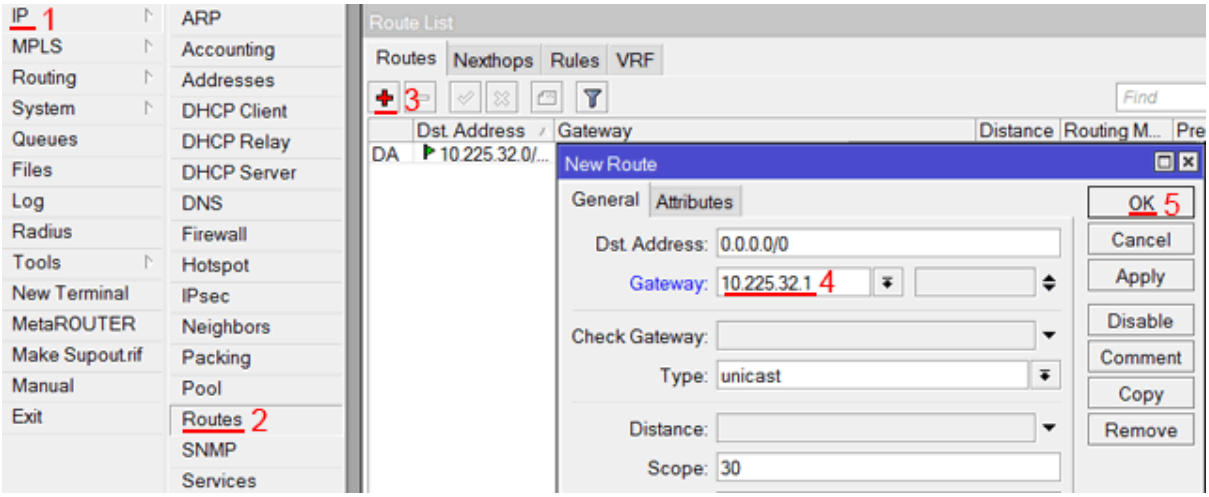

Рисунок 3.14 — Налаштування адреси інтернет-шлюзу

Додавання адрес DNS-серверів (Рис 3.15) MikroTik:

- Відкривається меню IP;
- Вибирається DNS;
- У вікні натискається кнопку Settings;
- У новому вікні в полі Servers: прописується IP адреса пріоритетного DNS сервера;
- Натискається кнопку "вниз" (чорний трикутник), щоб додати ще одне поле для введення;
- У новому полі прописується IP адреса альтернативного DNS сервера;
- Ставиться галочку Allow Remote Requests;
- Натискається кнопку OK для збереження налаштувань.

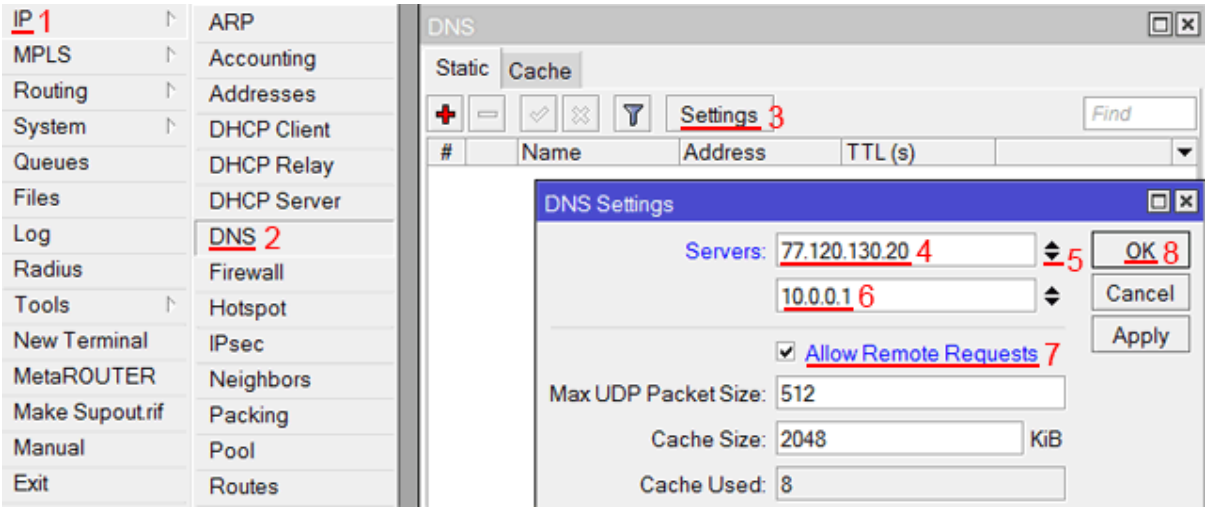

Рисунок 3.15 — налаштування DNS-серверів

– Налаштування клієнтського з’єднання PPPoE(Рис 3.16):
  – Зліва вибирається меню PPP;
  – Натискається кнопку Add (плюсик);
  – Вибирається PPPoE Client.

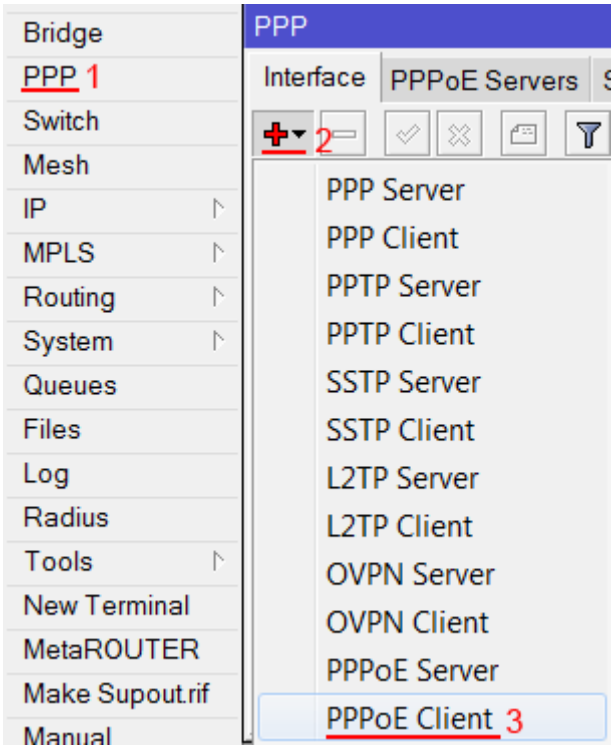

Рисунок 3.16 — Налаштування клієнтського з’єднання PPPoE

– Налаштування параметрів PPPoE з'єднання(Рис 3.17) MikroTik:
  – В полі Name вказується ім'я з'єднання;
  – У списку Interfaces вибирається перший WAN порт ether1, який підключений до провайдера.

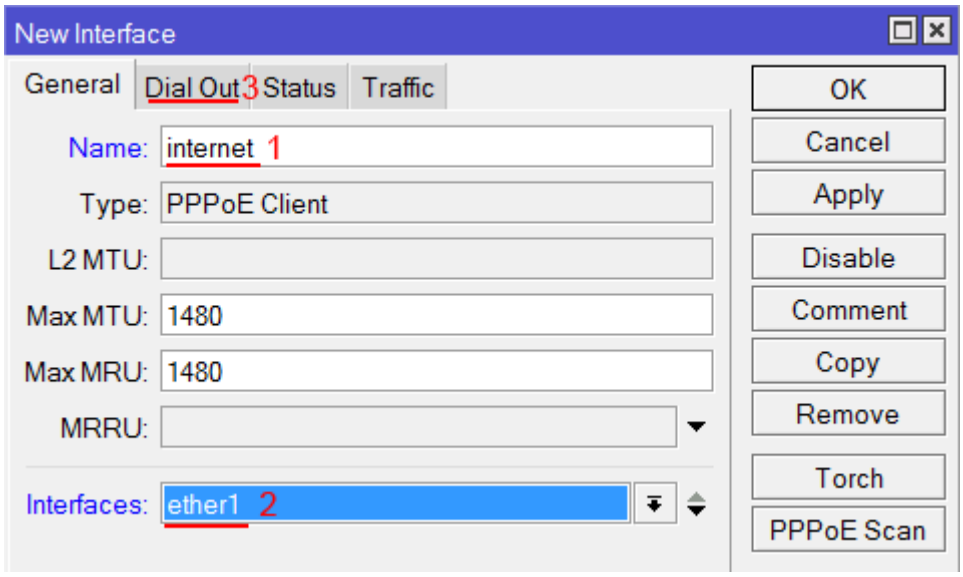

Рисунок 3.17 — Налаштування параметрів PPPoE з'єднання

– Переходиться на вкладку Dial Out(Рис 2.18);
– В полі User вказується ім'я користувача;
– В поле Password вводиться пароль;
– Ставиться галочку Use Peer DNS;
– Натискається кнопку OK.

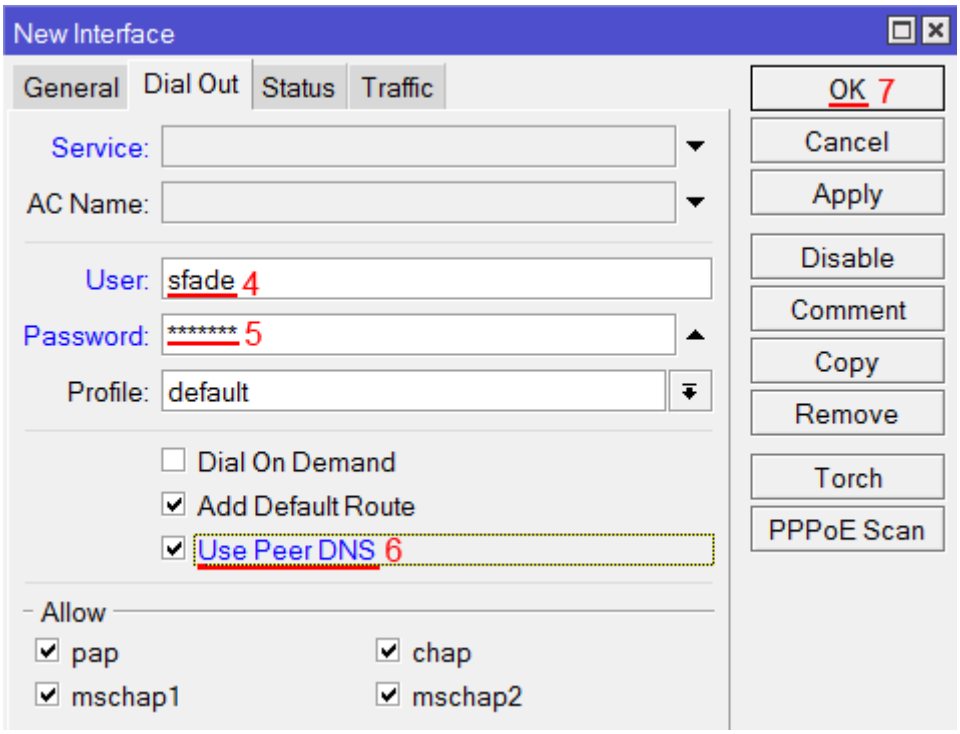

Рисунок 3.18 — Вкладка DiaL Out

3.7 Налаштування локальної мережі MikroTik

– Об'єднання Wi-Fi і дротових інтерфейсів в локальну мережу

Щоб комп'ютери, підключені до роутера по кабелю і по Wi-Fi, один одного «бачили», необхідно об'єднати бездротової і провідні інтерфейси MikroTik.

Створення об'єднання bridge-local (міст) (Рис 3.19):

– Відкривається меню Bridge;

– Натискається кнопку Add (плюсик);
– В поле Name прописується ім'я об'єднання bridge-local;
– Натискається кнопку OK.

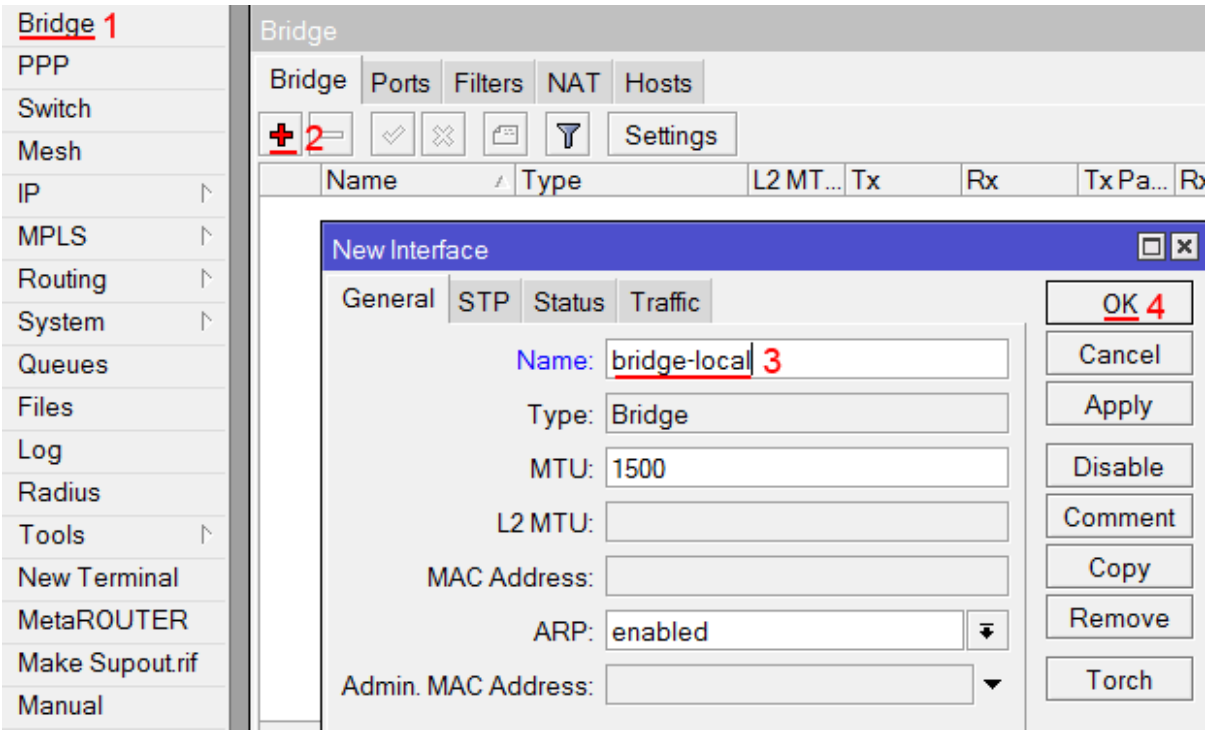

Рисунок 3.19 — об'єднання bridge-local

– Додавання в об'єднання провідні ethetnet порти(Рис 2.19) 2-5:
  – Переходиться на вкладку Ports;
  – Натискається кнопку Add (плюсик);
  – У списку Interface вибираається ethernet порт ether2;
  – У списку Bridge вибирається ім'я об'єднання bridge-local;
  – Натискається кнопку OK;
  – Повторюється цей цикл дій з портами ether3, ether4, ether5.

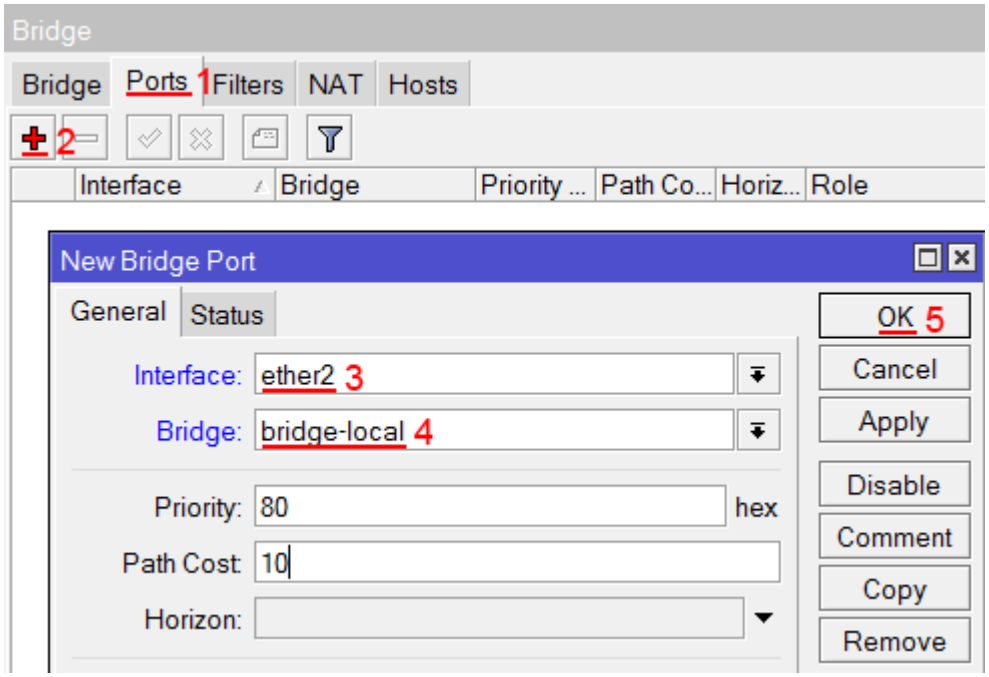

Рисунок 3.19 — Додавання в об'єднання провідні ethetnet порти

– Додавання в об'єднання Wi-Fi інтерфейс(Рис 3.20):
  – Переходиться на вкладку Ports;
  – Натискається кнопку Add (плюсик);
  – У списку Interface вибирається бездротової інтерфейс wlan1;
  – У списку Bridge вибирається ім'я об'єднання bridge-local;
  – Натискається кнопку OK.

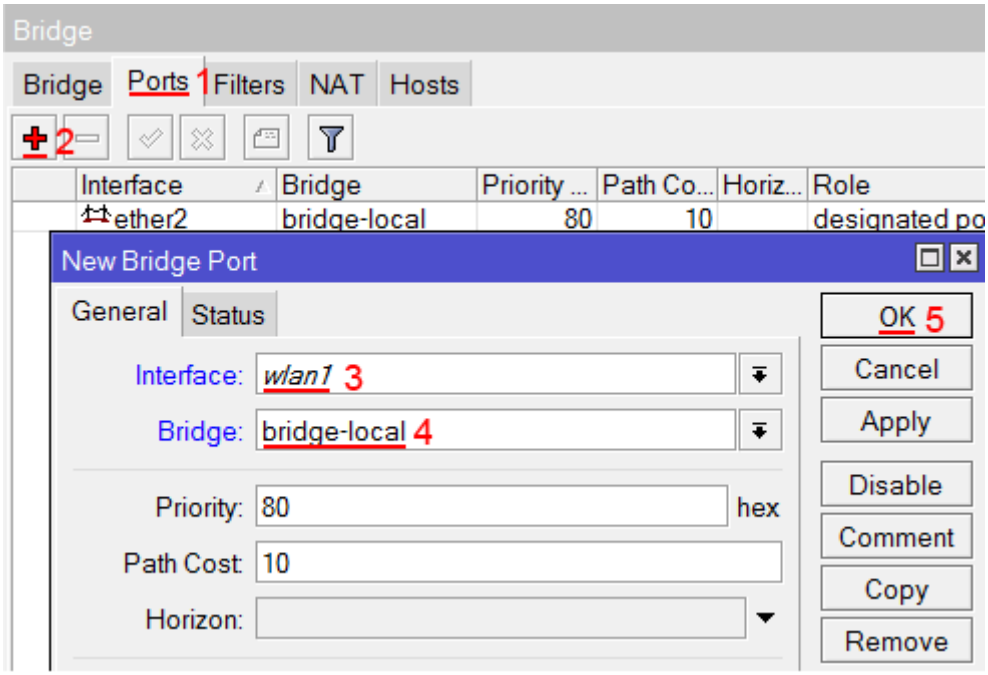

Рисунок 3.20 — Додавання в об'єднання Wi-Fi інтерфейс

– Призначення IP адреси локальної мережі

Налаштування IP адреси локальної мережі MikroTik(3.21):

– Відкривається меню IP;
– Вибирається Addresses;
– Натискається кнопку Add (плюсик);
– В поле Address вводиться адресу і маску локальної мережі, наприклад 192.168.88.1/24;
– У списку Interface вибирається bridge-local;
– Натискається кнопку OK.

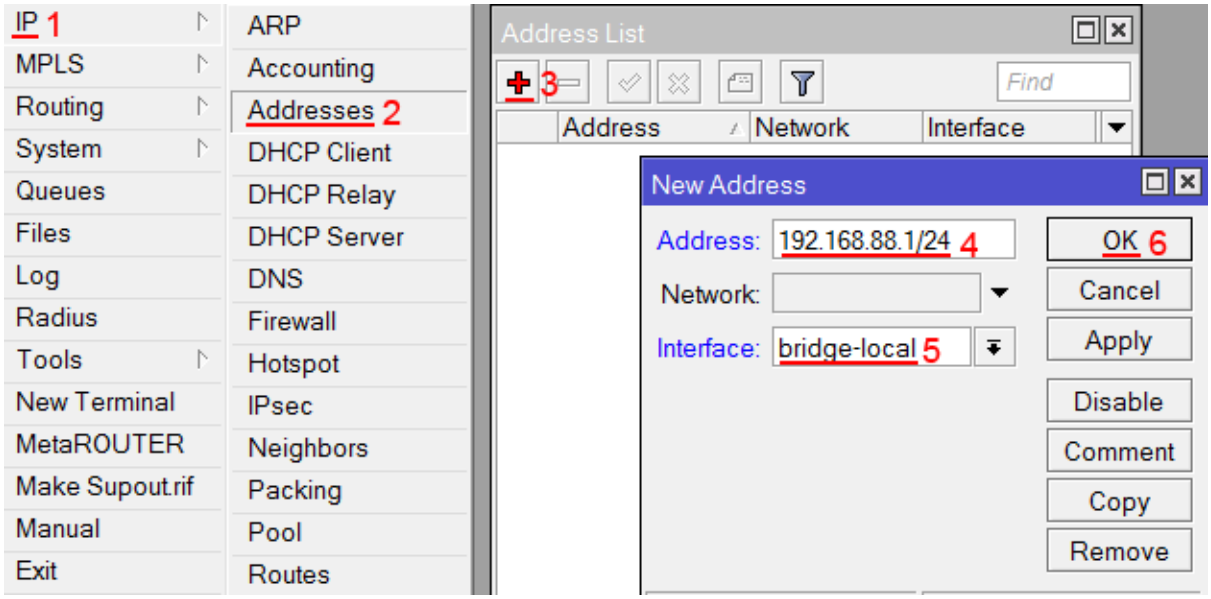

Рисунок 3.21 — Налаштування IP адреси локальної мережі MikroTik

– Налаштування DHCP сервера

Щоб комп'ютери, підключені до роутера, отримували мережеві настройки автоматично, налаштовується DHCP сервер(Рис 3.22) MikroTik:

– Відкривається меню IP;

– Вибирається DHCP Server;

– Натискається кнопку DHCP Setup.

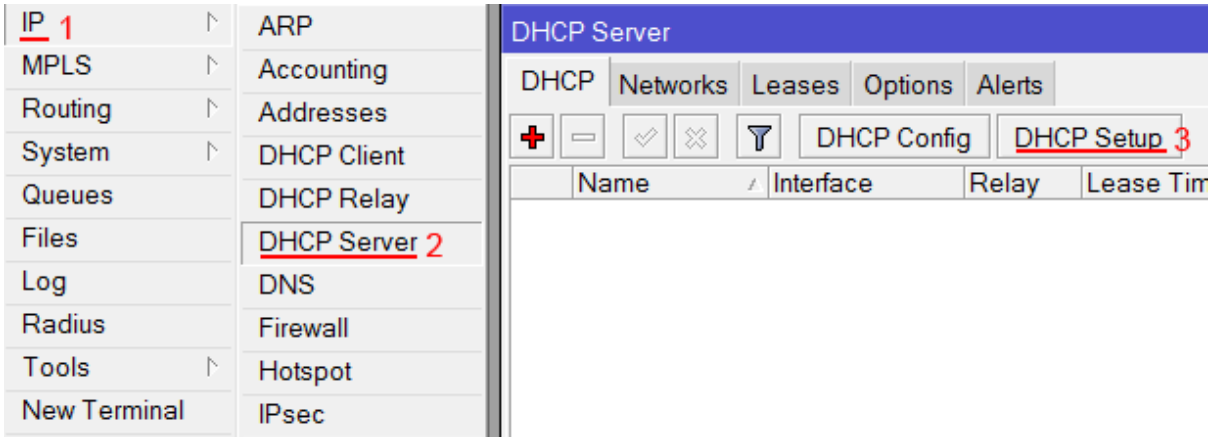

Рисунок 3.22 — налаштування DHCP сервер MikroTik

– У списку DHCP Server Interface вибирається bridge-local(Рис 3.23);
– Натискається кнопку Next;

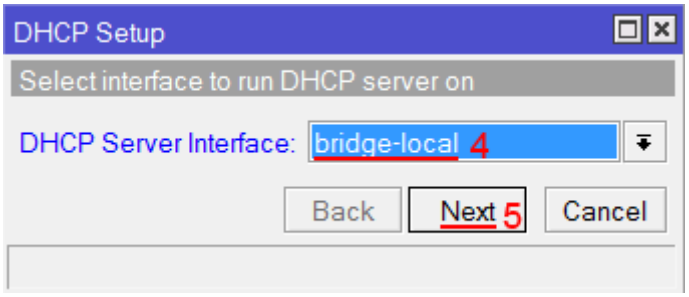

Рисунок 3.23 — bridge-local

– У цьому вікні(Рис 3.24) вибирається мережу для DHCP. Залишається без змін і натискається кнопку Next;
–

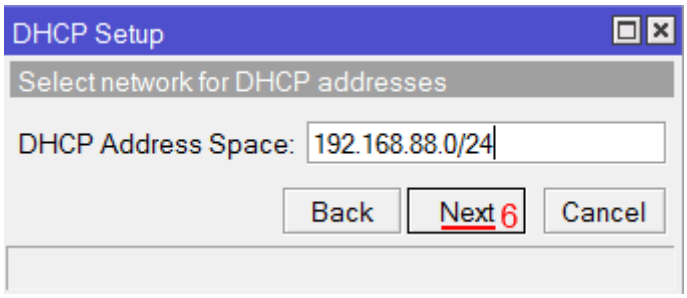

Рисунок 3.24 — Мережа для DHCP

– У наступному вікні (Рис 3.25) вказується адреса шлюзу. Натискається кнопку Next;

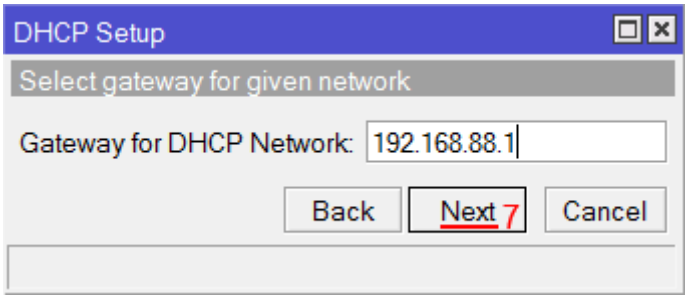

Рисунок 3.25 — Адреса шлюзу

– У цьому вікні(Рис 3.26) прописується діапазон IP адрес, які роздаватиме DHCP сервер. Натискається кнопку Next;

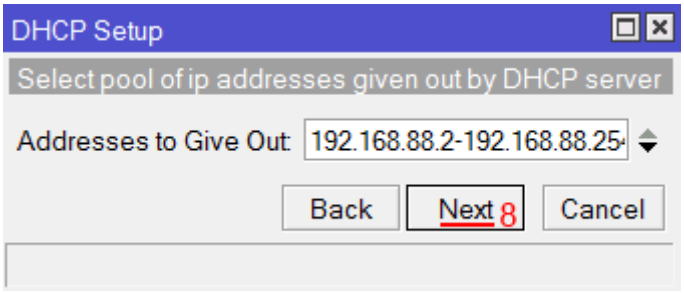

Рисунок 3.26 — Діапазон IP адрес

– Далі вводяться адреси DNS серверів(Рис 3.27). Натискається кнопку Next;

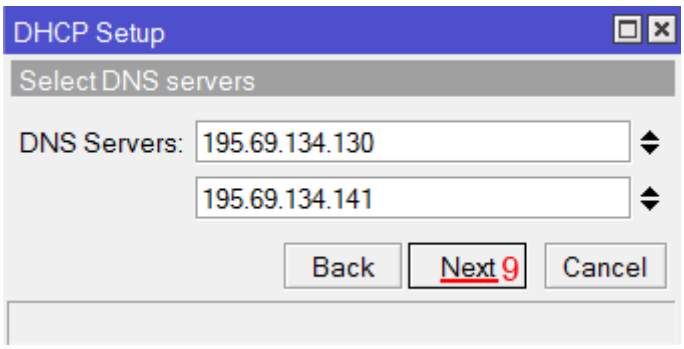

Рисунок 3.27 — Адреси DNS серверів

– Тут задається час резервування IP адрес(Рис 3.28). Натискається кнопку Next:

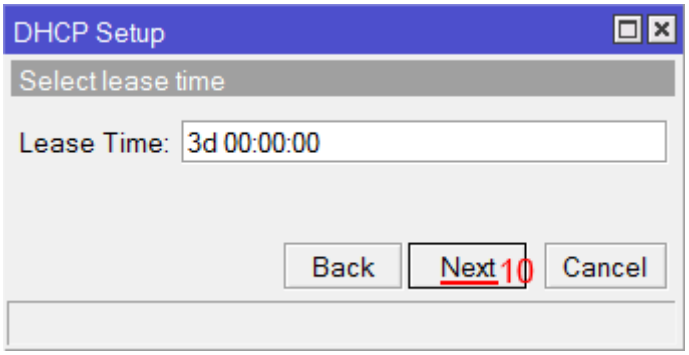

Рисунок 3.28 — Час резервування IP адрес

– Налаштування DHCP сервера успішно завершено (Рис 3.29). Натискається кнопку OK.

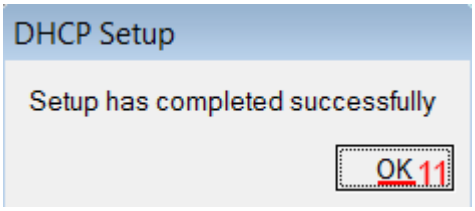

Рисунок. 3.29 — Налаштування DHCP сервера успішно завершено

3.8 Налаштування Wi-Fi точки доступу MikroTik

Спочатку необхідно включити Wi-Fi модуль (Рис 3.30):

– Відкривається меню Wireless;

– Вибирається Wi-Fi інтерфейс wlan1;

– Натискається кнопку Enable (синя галочка).

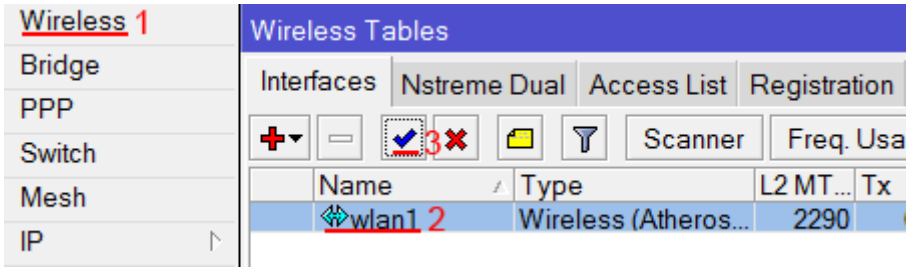

Рисунок 3.30 — Wi-Fi модуль

Створення пароля для підключення до точки доступу MikroTik(Рис 3.31):

- Відкривається вкладку Security Profiles;
- Натискається кнопку Add (плюсик);
- У новому вікні в полі Name: вказується ім'я профілю безпеки;
- Для кращої безпеки залишається тільки реєстрація по протоколу WPA2 PSK;
- В полі WPA2 Pre-Shared Key вводиться пароль для доступу до Wi-Fi точки;
- Для збереження налаштувань натискається кнопку OK.

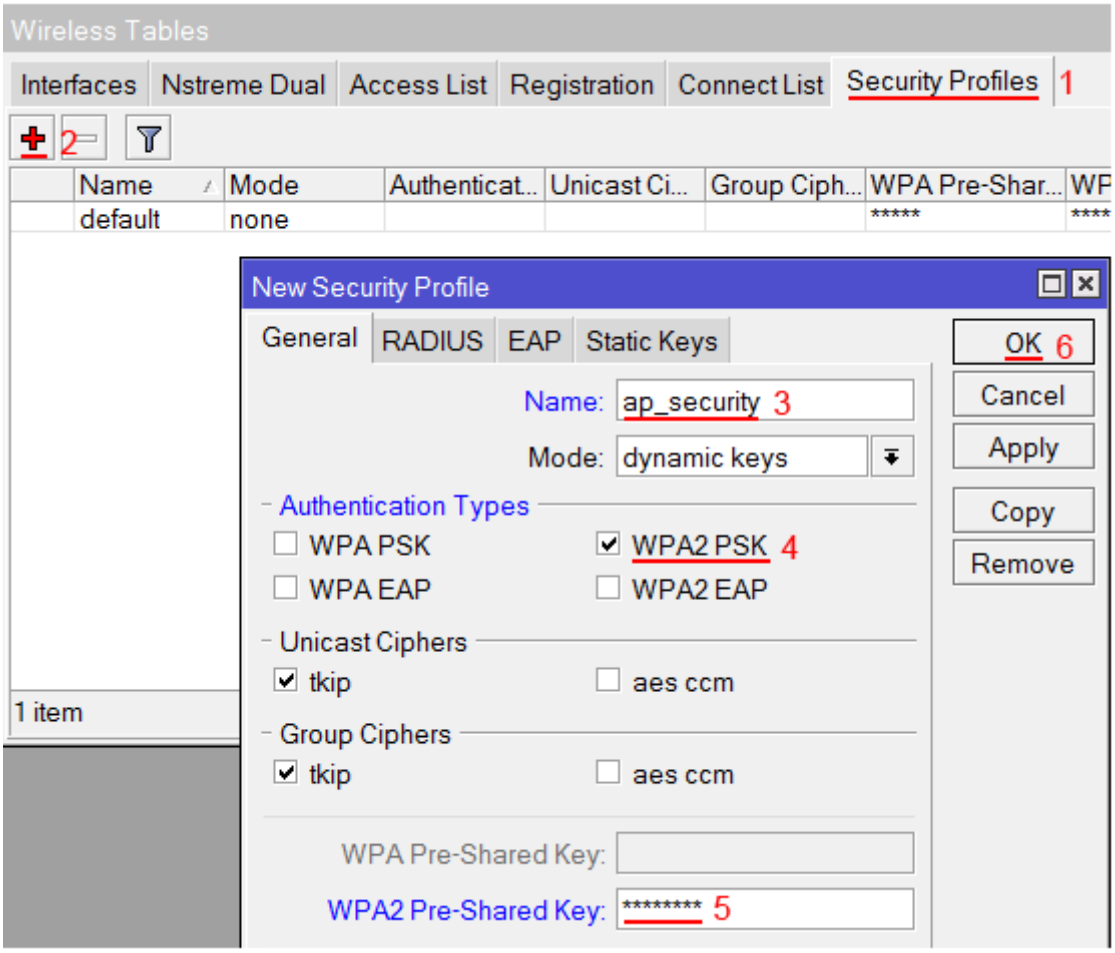

Рисунок 3.31 — Створення пароля

Налаштування параметрів Wi-Fi точки MikroTik(Рис 3.32):

– Відкривається вкладку Interfaces;
– Робиться подвійний клік кнопкою миші на Wi-Fi інтерфейсі wlan1, щоб зайти в його налаштування;
– Переходиться на вкладку Wireless;
– У списку Mode: вибирається режим роботи ap bridge (точка доступу в режимі моста);
– У списку Band: вибирається в яких стандартах буде працювати Wi-Fi точка, вибрано B / G / N;
– В поле SSID: прописується ім'я точки доступу;
– У списку Security Profile вибирається ім'я профілю безпеки, в якому створено пароль для доступу до Wi-Fi точки;
– Натискається кнопку OK для збереження налаштувань.

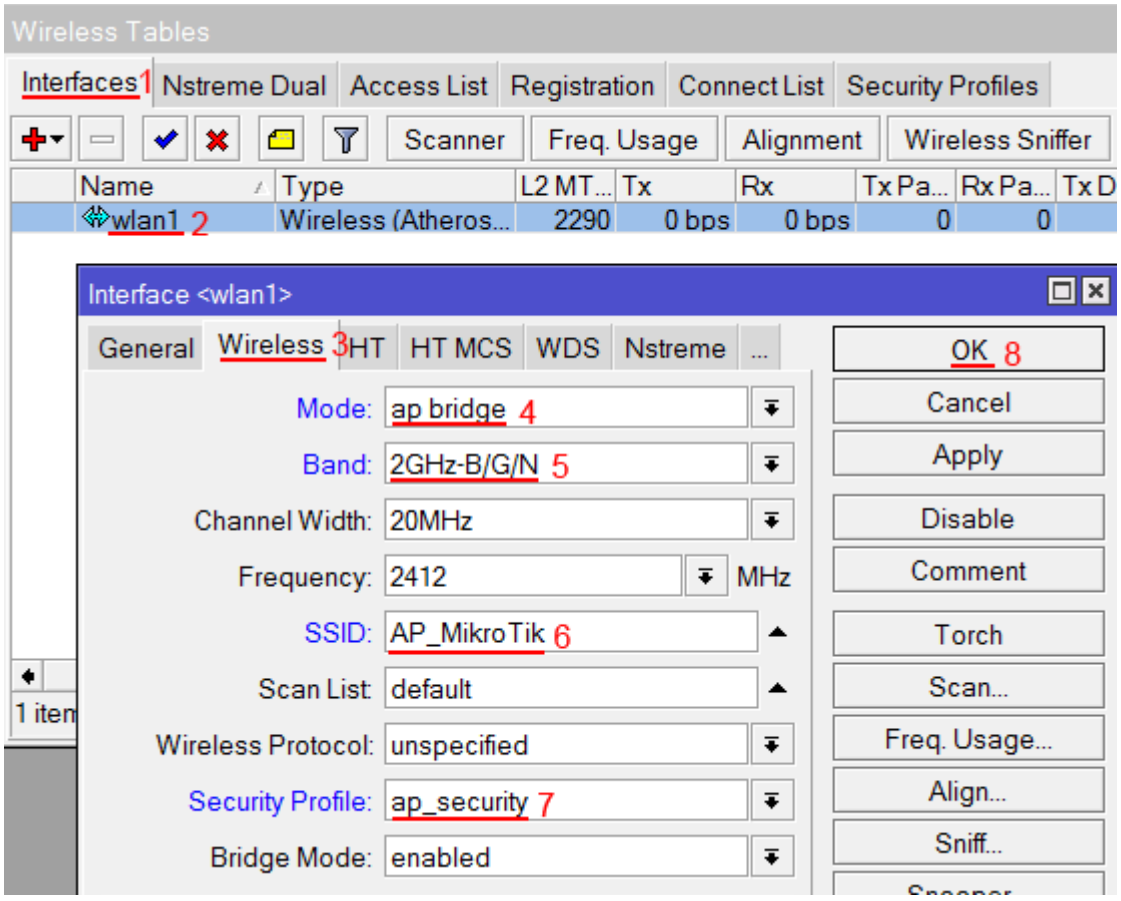

Рисунок 3.32 — Налаштування параметрів Wi-Fi точки

3.9 Налаштування Firewall і NAT

Щоб комп'ютери отримували доступ до інтернету, необхідно налаштувати Firewall і NAT на марштрутизаторі MikroTik.

Для цього використовується меню New Terminal, щоб ввести необхідні команди.

Налаштування NAT виконується командами поданими в лістингу 3.1:

Лістинг 3.1 — Налаштування NAT:

```
ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```

Для захисту самого маршрутизатора були використані команди, подані в лістингу 3.2:

Лістинг 3.2 — Захист маршрутизатора:

```
ip firewall filter add action=accept chain=input disabled=no protocol=icmp
```

Дана команда дозволяє пропускати вхідні пакети з протоколом icmp.

```
ip firewall filter add action=accept chain=input connection-state=established disabled=no in-interface=ether1
```

Ця команда дозволяє пакети які перебувають в встановленому з’єднанні з маршрутизатором.

```
ip firewall filter add action=accept chain=input connection-state=related disabled=no in-interface=ether1
```

Подана вище команда дозволяє приймати пакети з встановленим раніше з’єднанням.

Для захисту внутрішньої мережі були використані команди, подані в лістингу 3.3:

Лістинг 3.3 — Захист LAN-мережі.

```
ip firewall filter add action=jump chain=forward disabled=no in-interface=ether1 jump-target=customer
ip firewall filter add action=accept chain=customer connection-state=established disabled=no
ip firewall filter add action=accept chain=customer connection-state=related disabled=no
ip firewall filter add action=drop chain=customer disabled=no
```

Даний набір команд визначає, що всі всі пакети, що попали в таблицю forward будуть перенаправлені в таблицю customer, а в даній таблиці встановлюються правила приймати тільки пакети із встановленим з'єднанням, а інші видаляти. Тобто Ніхто не може встановити з'єднання в середину custom, лише пакети-custom можуть створювати з'єднання.

Також потрібно визначити типи інтерфейсів для кожного порту, команди подані в лістингу 3.4:

Лістинг 3.4 — типи інтерфейсів.

```
ip upnp interfaces add disabled=no interface=ether1 type=external
ip upnp interfaces add disabled=no interface=ether2 type=internal
ip upnp interfaces add disabled=no interface=ether3 type=internal
ip upnp interfaces add disabled=no interface=ether4 type=internal
ip upnp interfaces add disabled=no interface=ether5 type=internal
ip upnp interfaces add disabled=no interface=bridge-local type=internal
```

4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при кровотечах

Будь – яка кровотеча є небезпечною для людини: зменшення кількості крові, що циркулює, зумовлює [2] порушення діяльності серця і недостатнє постачання кисню до життєво важливих органів (мозок, печінка, нирки, легені).

· Залежно від того, яка судина кровоточить, розрізняють:

- капілярну;
- венозну;
- артеріальну кровотечі.

При зовнішній капілярній кровотечі кров виділяється рівномірно зі всієї рани; при венозній кровотечі – витікає рівномірним струменем, має темно – вишневе забарвлення (якщо пошкоджено крупну вену, струмінь крові може пульсувати у ритмі диханню); при артеріальній кровотечі кров має яскраво – червоний колір, б'є сильним уривистим струменем (фонтаном), викиди крові відповідають ритму серцевих скорочень.

Насамперед необхідно подбати про запобігання зараженню хворобами, які передаються через кров, та вдягнути одноразові стерильні гумові рукавички. Щоб встановити джерело кровотечі, слід оголити рану потерпілого, знявши чи розірвавши одяг.

На поверхню рани накласти стерильну пов'язку або чисту тканину (носовичок, рушник тощо) і притиснути [8,10] пальцями чи долонею. Натискати слід рівномірно, тоді кровотеча зупиниться впродовж 10 хвилин. Якщо цього не сталося, можливо, ви натискаєте недостатньо сильно, чи не в тому місці. Спробуйте натискати сильніше, охоплюючи більшу поверхню рани.

Не бажано тиснути на рану, якщо у ній є фрагменти кісток, сторонні предмети тощо. У такому разі для зупинки кровотечі слід використовувати кільцеву подушечку. Зробити таку подушечку можна з вузького бинта, шматка тканини тощо. Насамперед слід зробити петлю, обмотавши тканину декілька разів навколо пальців. Потім вільний кінець тканини обмотати навколо петлі, поки не утвориться кільце.

При кровотечі через поранення [8-11] руки чи ноги слід підняти пошкоджену кінцівку, щоб зменшити прилив крові. Утримуючи підняте положення кінцівки, слід продовжувати натискати на рану.

Після зупинки кровотечі накласти на рану щільну пов'язку та перебинтувати вище і нижче місця поранення. Не варто перебинтовувати занадто міцно, щоб не порушити кровообіг. Перевірити кровообіг можна за допомогою тесту наповнення капілярів. У нормальному стані, при піднятті кінцівки чи натисканні на нігтьове ложе шкіра блідне. Опускаючи кінцівку чи припиняючи натиск на нігтьове ложе, шкіра набуває попереднього забарвлення впродовж 2 – 3 секунд.

Кровотечу необхідно зупинити негайно, наклавши джгут, турнікет чи щільну пов'язку, щоб попередити її раптове, неконтрольоване поновлення.

Терміново викликати швидку медичну допомогу.

При сильних артеріальних кровотечах, джгута чи щільної пов'язки зазвичай недостатньо. Щоб попередити швидку крововтрату, слід натиснути на точки притиснення артерій – плечову (на внутрішній поверхні плеча) і стегнову. Ці точки розміщено у місцях, де артерії проходять близько до шкірних покривів і їх можна притиснути до кістки.

Місце кровотечі: кисть і передпліччя.

Дії: руку максимально зігнути у ліктьовому суглобі до плеча і зафіксувати джгутом або ременем.

·Місце кровотечі: гомілка і нижня третина стегна.

Дії: ногу максимально зігнути у колінному суглобі, підняти гомілку до стегна і зафіксувати, підклавши м'який валик у підколінну ямку.

· Місце кровотечі: верхня третина стегна і пахвина.

Дії: ногу максимально зігнути у тазостегновому та колінному суглобах, притиснути до тулуба та зафіксувати ременем через поперек.

· Місце кровотечі: підключична ділянка.

Дії: випрямлені руки слід максимально завести за спину і стягнути у ліктьових суглобах.

Окрім наявного гумового джгута, можна використовувати турнікети або широкі еластичні матеріали (широкий ремінь, складений у декілька шарів бинт, тканину, одяг). Не [11] можна використовувати мотузки, дроти, вузькі ремені.

Джгут накладають вище рани і якомога ближче до неї (але не на суглоб). Під джгут слід підкласти хустку, рушник чи будь-яку іншу тканину.

Джгут слід затягнути до моменту зупинки кровотечі з рани і зникнення пульсу нижче рани. Правильність накладання джгута визначають за припиненням кровотечі. Якщо джгут затягнено слабо і здавлені тільки вени, кровотеча продовжуватиметься, а шкірні покриви набудуть ціанотичного забарвлення.

Джгут надійно закріплюють та записують час його накладання (найкраще написати ці дані на шкірі потерпілого).

Джгут на кінцівці має залишатися не більше двох годин влітку і однієї години взимку. У холодну пору року перетягнуту кінцівку утеплюють, наприклад, за допомогою одягу.

Кінцівку з накладеним джгутом слід іммобілізувати. Варто постійно слідкувати, щоб постраждалий не зняв джгут чи щільну пов’язку.

4.2 Аналіз потенційних шкідливостей на дільниці. Заходи щодо їх зниженню

Шкідливі виробничі фактори — фактори середовища і трудового процесу, які можуть викликати [10-11] професійну патологію, тимчасове або стійке зниження працездатності, підвищити частоту соматичних та інфекційних захворювань, призвести до порушення здоров'я потомства.

Небезпечні та шкідливі виробничі фактори, по природі дії, підрозділяються на наступні групи:

- фізичні;
- хімічні;
- біологічні;
- психофізіологічні.

На підприємстві є наступні фактори:

- підвищена вологість повітря;
- підвищений рівень електромагнітних випромінювань;
- недолік природного світла;
- монотонність праці;

Прийнято рішення про проведення заходів щодо зниження шкідливого впливу даних факторів на працівників що працюють з інформаційно-комунікаційною мережею організації.

Для зниження вологості приміщення виконується регулярне провітрювання в теплу пору року та використання обігрівачів в холодну пору року. Також додатково встановлено вологопоглинач, який «всмоктує» зайву вологу, фільтрує повітря, а потім повертає сухе в кімнату. У прилад

встановлено спеціальні регулятори вологості, завдяки яким повітря в приміщенні не пересушується, а тільки позбавляється від зайвої вологи.

Для боротьби з підвищеним рівнем електромагнітних випромінювань, було проведено аналіз випромінювання та екранування приміщення. Екранування високочастотних полів ґрунтується на двох основних фізичних властивостях – відбиванні і поглинанні електромагнітних хвиль при переході з одного середовища в інше. Обидва ці ефекти знижують енергію електромагнітної хвилі, що пройшла за екран. Найчастіше в якості матеріалу [11] екрану використовується провідник. Екрануючі матеріали (крім екрануючих фарб) містять в своєму складі металеві волокна (мідні, срібні чи сталеві), що утворюють сітку. Саме ця сітка і служить захисним екраном.

Природне освітлення має важливе фізіолого-гігієнічне значення для працюючих. Воно позитивно впливає на органи зору, стимулює фізіологічні процеси, підвищує обмін речовин та покращує розвиток організму в цілому. Сонячне випромінювання зігріває та знезаражує повітря, очищуючи його від збудників багатьох хвороб (наприклад, вірусу грипу). Окрім того, природне світло має і психологічну дію, створюючи в приміщенні для працівників відчуття безпосереднього зв'язку з довкіллям.

Для компенсації недоліку природного світла, було встановлене додаткове штучне освітлення та збільшено тривалість перерви. Також було рекомендовано працівникам проводити більшість часу виділеного на відпочинок на вулиці.

Для зміни статичної сидячої роботи за комп’ютером було введено додаткові перерви під час яких виконуються фізичні навантаження, а також було введено регулярне чергування статичної роботи за комп’ютером та роботи з клієнтами поза офісом.

ВИСНОВКИ

Кожне підприємство та організація володіє технічними активами, завдяки яким здійснює свою підприємницьку діяльність. Для послідовної роботи та забезпечення бізнес процесів практично усюди потрібен доступ до мереж Інтернет. На основі цього виникає завдання у забезпеченні захисту мережі від стороннього доступу та витоку інформації.

В ході виконання роботи було здійснено детальний аналіз організації та за його результатами був зроблено висновок, що наявне апаратне забезпечення не володіє належним функціоналом, не забезпечується потрібний рівень безпеки, виявлено вразливості щодо несанкціонованого доступу. В кваліфікаційній роботі також було проведено аналіз інтернет-загроз, особливу увагу було звернено на загрози бездротових мереж, досліджено вразливості словникови паролів, міжмережевого екрану, та роутерів D-Link, які і використовуються в організації.

Врахувавши аналіз діючого апаратного забезпечення та виявлених вразливостей було обрано роутер MikroTik, що вирішує проблему вразливостей та забезпечує достатній рівень захисту. Оновлене апаратне забезпечення є стійким до раніше виявлених вразливостей та здатне ефективно справлятись з поставленими завданнями в рамках інформаційно-комунікаційної мережі ТзОВ “Центр сервісного обслуговування, завдяки системі Nat та Firewall.

Четвертий розділ присвячений основним питанням безпеки життєдіяльності: допомозі про кровотечах та загроз на дільниці.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Настройка роутера MikroTik [Електронний ресурс] – Режим доступу до ресурсу: https://www.technotrade.com.ua/Articles/mikrotik_router_setup.php. - (дата звертання: 04.04.2021).
2. Перша долікарська допомога при кровотечі [Електронний ресурс] – Режим доступу до ресурсу: http://dnz416.edu.kh.ua/poradi_likarya/pamyatki/persha_dolikarsjka_dopomoga_pri_krovotechi/ (дата звертання: 15.05.2021).
3. Електромагнітне випромінювання та здоров'я [Електронний ресурс] – Режим доступу до ресурсу: uk.wikipedia.org/wiki/Електромагнітне_випромінювання_та_здоров%27я#Поради,_як_вберегтися_від_ЕМЗ (дата звертання: 20.05.2021)
4. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. – М.: Интернет-университет информационных технологий ИНТУИТ.ру, 2008. – 207 с.
5. Литвинов В. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі // Математичні машини і системи, № 1, С. 31- 40, 2018. [Електронний ресурс]. Режим доступу: URL: https:// cyberleninka.ru/article/v/analiz-sistem-ta-metodiv-viyavlennya-nesanktsionovanihvtorgnen-u-kompyuternimerezhi (дата звертання: 03.05.2021).
6. Сєвєрінов О.В., Хрєнов А.Г. Аналіз сучасних систем виявлення вторгнень // Системи обробки інформації. — 2014. — № 6(122). – С. 100-124.
7. Як захистити веб-додатки: основні поради, інструменти, корисні посилання [Електронний ресурс] : Exo. Поринь у світ – Режим доступа: https://echo.lviv.ua/dev/6231 - (дата звертання: 20.05.2021).
8. Бєрковський В. В., Безсонов О. С. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему // Системи управління, навігації та

зв'язку. - 2017. - Вип. 3. - С. 57-62. - Режим доступу: http://nbuv.gov.ua/UJRN/suntz_2017_3_17 - (дата звертання: 26.05.2021).

9. Толок А.О. Крюковська О.А. Безпека життєдіяльності: Навч. посібник. – 2011. – 215 с.
10. Агєєв Є .Я. Основи охорони праці: Навчально-методичний посібник для самостійної роботи по вивченню дисципліни – Львів: «Новий Світ – 2000», 2009. – 404 с. 51
11. Основи охорони праці: Підручник.; 3-те видання, доповнене та перероблене / За ред. К. Н Ткачука. – К.: Основа, 2011. – 480 с.