Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки, факультет радіоелектроніки та телекомунікацій
(повне найменування інституту, факультету)

Кафедра «Захисту інформації»
(повне найменування кафедри)

Пояснювальна записка

до магістерської роботи

магістр
(ступінь вищої освіти)

на тему Аналіз та побудова програмно-апаратної безпеки серверів для віддаленого доступу

Виконав: студент 2 курсу, групи РТ-811м
Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних систем

Локаєнко В.О.
(прізвище та ініціали)

Керівник Воскобойник В.О.
(прізвище та ініціали)

Рецензент Паршина О.А.
(прізвище та ініціали)

2022

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Інститут, факультет ІПРЕ, ФРЕТ
Кафедра захисту інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
Завідувач кафедри Воскобойник В.О.,
канд. техн. наук, доц.
«19» 12 2022 року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТА

Локаєнко Віталія Олександровича
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Аналіз та побудова програмно-апаратної безпеки серверів для віддаленого доступу
керівник проекту (роботи) Воскобойник Володимир Олександрович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від 08 листопада 2022 року № 371
2. Строк подання студентом проекту (роботи) 15 грудня 2022 р.
3. Вихідні дані до проекту (роботи) Несанкціонований доступ за допомогою hydra, бази даних, сервери готові до налаштування, роутери Microtik.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз проблеми та постановка завдань; дослідження баз даних; вибір програмних та апаратних засобів; налаштування програм; використання віддаленого доступу; перевірка працездатності сервера та роутерів Mikrotik; та отримання результатів аналізу.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Презентація

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основні розділи	Воскобойник В.О., доцент	01.09.2022	
Нормоконтроль	Корольков Р.Ю., ст. викладач		

7. Дата видачі завдання "_01_" _09_____2022 року._____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Прим.
1	Складання та затвердження ТЗ	01.09—10.09	Викон.
2	Підбір літератури	11.09—17.09	Викон.
3	Аналіз предметної області.	18.09—20.09	Викон.
4	Аналіз існуючих баз даних та різниці між ними	21.09—01.10	Викон.
5	Вибір програмних налаштувань	02.10—04.10	Викон.
6	Аналіз роботи Raid	05.10—12.10	Викон.
7	Аналіз системи MicroTik	13.10—18.10	Викон.
8	Аналіз процедури активації Rds	19.10—03.11	Викон.
9	Розробка параметрів налаштування для подальношого використання сервера	04.11—26.11	Викон.
10	Оформлення пояснювальної записки	27.11—8.12	Викон.
11	Оформлення графічної частини	8.12—10.12	Викон.

Студент _____ Локаєнко В.О.
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ Воскобойник В.О.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

ПЗ: 79 сторінка, 90 рисунків, 5 таблиць, 13 джерел.

БРУТФОРС, БАЗИ ДАНИХ, СУБД, СЕРВЕР, BIOS, HYDRA,HYPER-V, MIKROTIK, RAID, RDP, RDS, SQL, SQLITE,WINDOWS.

Мета магістерської роботи – проведення аналізу та побудова програмно-апаратної безпеки серверів для віддаленого доступу а також для забезпечення їх працездатності та автономності.

У роботі проводиться аналіз баз даних з метою визначення кола конкретних задач. В ході виконання роботи запропоновано покрокове установлення та налаштування операційної системи для задач інформаційної безпеки. Також приводиться план налаштування роутеру який має властну операційну систему, та розписується відкривання певних портів для доступу між серверами та віртуальними машинами. Після цього у роутер вписуються правила фаерволу для захисту від брутфорс атак на адреса та на порт. Для перевірки захисту зроблена атака на сервер за допомогою брутфорсу.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 6
ВСТУП 7
1 СЕРВЕРИ ТА БАЗИ ДАНИХ 8
1.1 Класифікація серверів та їх характеристики 8
1.2 Бази даних та СУБД 11
1.2.1 Реляційні СУБД 14
1.3 Актуальні реляційні бази 17
2 ПРОГРАМНЕ НАЛАШТУВАННЯ СЕРВЕРА ДЛЯ ВИКОРИСТАННЯ 23
2.1 Класифікація Raid для серверів 24
2.2 Створення та налагодження Raid 29
2.3 Установка Windows Server 2016 33
2.4 Налаштування ОС перед використанням. 36
2.5 Технологія віртуалізації Hyper-V 41
2.6 Налагодження Rds для Windows Server 45
3 ВИКОРИСТАННЯ МЕРЕЖІ РОУТЕРІВ MICROTIK ДЛЯ НАЛАШТУВАННЯ ВІДДАЛЕНОГО ДОСТУПУ 50
3.1 Налаштування роутерів для внутрішньої та зовнішньої мережі. 53
3.2 Створення ім'я хоста для зовнішнього підключення. 54
3.3 Налаштування зовнішніх та внутрішніх портів. 56
4 АНАЛІЗ І ЗАБЕЗПЕЧЕННЯ ПАРАМЕТРІВ БЕЗПЕКИ 62
4.1 Параметри зберігання баз даних. 62
4.2 Використання двох варіантів захисту від брутфорсу. 72
Висновок 77
Перелік посилань 78

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БД – Бази даних

ОС – операційна система

СУБД – Системи управління базами даних

BIOS – Basic input/output system (базова система введення-виведення)

DNS – Domain Name System (система доменних імен)

DHCP– Dynamic Host Configuration Protocol (протокол динамічної конфігурації вузла)

IP – Internet Protocol (міжмережевий протокол)

NAT – Network Address Translation (перетворення мережевих адрес)

RAID – Redundant Array of Independent Disks (надлишковий масив незалежних дисків)

RDP – Remote Desktop Protocol (Протокол віддаленого робочого стола)

TCP – Transmission Control Protocol (протокол управління передачею)

UDP – User Datagram Protocol (протокол призначених для користувача датаграм)

ВСТУП

Актуальність дослідження. Необхідність захисту інформації у сучасному світі займають дуже важливе місце у будь-якій сфері. Разом з цим зростає число інформаційних атак зловмисників та важливішою стає потреба у захисті інформації, що передається та обробляється у мережі. Необхідність захисту віддаленого сервера з використанням сучасних технічних та програмних засобів покликана знизити ризик втрати, обмеживши зовнішній доступ до БД.

Необхідність провести аналіз щодо програмно-апаратної частини серверів, обумовлена побудовою варіанта при якому в разі порушення стабільності допоможе мінімізувати шкоду як для сервера, так і для баз даних.

Використання програмних методів обмеження доступу дозволяє краще налаштувати авторизацію користувачів, які будуть підключатися до різних віртуальних машин. Також за допомогою роутерів виконається прокидання портів, яке допоможе заплутати зловмисників та ускладнить завдання з пошуком потрібного зовнішнього порту. Щодо самих користувачів будуть застосовані налаштування обмеження доступу до певних папок, це повинно знизити ризик розкрадання та спроб використовувати неправомірні дані самими користувачами.

У роботі розглядається налаштування сервера, використання Raid, створення середовищ безпеки за допомогою сервера та його функції Hyper-V, захист від збоїв та резервне копіювання, апаратний захист від різкого вимкнення енергії.

1 СЕРВЕРИ ТА БАЗИ ДАНИХ

1.1 Класифікація серверів

Сервер – це спеціальна модель комп'ютера, яка створена для постійного навантаження та безперервної роботи. Основна його відмінність від персонального комп'ютера це безперервне використання ресурсів, що дозволяє використовувати його для зберігання та обробки інформації, галузі розробки або передачі даних. Варто відзначити гнучкість операційних систем, програм та Bios які налаштовані на продуктивну роботу з серверами, дозволяючи змінювати налаштування до дрібниць, забезпечуючи тим самим безперебійне підключення до пристрою та стабільність роботи.

Рисунок 1.1 – Параметри вибору серверу

Крім вирішення описаних вище завдань, метою організації сервера є: підвищення безпеки пристрою, зменшення витрат, збільшення безпеки зберігання документів та важливої інформації, резервне копіювання даних.

Рисунок 1.2 – Різновиди користування серверами

При організації сервера необхідно визначиться для яких завдань налаштовується сервер і яка його межа. Апаратні комплекси розраховуються з поточного навантаження на сервер завдяки цьому визначається скільки потрібно користувачів та завдань для сервера [5].

Програмна частина, визначає розподіл функціоналу та стабільність сервера. Вибір програмного забезпечення обґрунтований тим що задачі які буде повинен виконувати сервер та на який апаратній платформі він буде виконуватись . Рекомендується брати програмні засоби які зарекомендував сам виробник операційної системи [5].

```
Имя узла:                          SERVER
Название ОС:                       Майкрософт Windows Server 2016 Standard
Версия ОС:                         10.0.14393 Н/Д построение 14393
Изготовитель ОС:                   Microsoft Corporation
Параметры ОС:                      Изолированный сервер
Построение ОС:                     Multiprocessor Free
Зарегистрированный владелец:       Пользователь Windows
Зарегистрированная организация:
Код продукта:
Дата установки:
Время загрузки системы:
Изготовитель системы:              HP
Модель системы:                    ProLiant DL180 G6
Тип системы:                       x64-based PC
Процессор(ы):                      Число процессоров - 2.
                                   [01]: Intel64 Family 6 Model 44 Stepping 2 GenuineIntel ~2000 МГц
                                   [02]: Intel64 Family 6 Model 44 Stepping 2 GenuineIntel ~1600 МГц
Версия BIOS:                       HP O20, 15.06.2011
Папка Windows:                     C:\Windows
Системная папка:                   C:\Windows\system32
Устройство загрузки:               \Device\HarddiskVolume1
Язык системы:                      ru;Русский
Язык ввода:                        ru;Русский
Часовой пояс:                      (UTC+02:00) Вильнюс, Киев, Рига, София, Таллин, Хельсинки
Полный объем физической памяти:    65 527 МБ
Доступная физическая память:       41 626 МБ
Виртуальная память: Макс. размер:  75 255 МБ
Виртуальная память: Доступна:      51 153 МБ
Виртуальная память: Используется:  24 102 МБ
```

Рисунок 1.3 – Характеристики першого серверу

```
Имя узла:                          ROYAL
Название ОС:                       Майкрософт Windows Server 2016 Standard
Версия ОС:                         10.0.14393 Н/Д построение 14393
Изготовитель ОС:                   Microsoft Corporation
Параметры ОС:                      Изолированный сервер
Построение ОС:                     Multiprocessor Free
Зарегистрированный владелец:       Пользователь Windows
Зарегистрированная организация:
Код продукта:
Дата установки:
Время загрузки системы:
Изготовитель системы:              ASUSTeK COMPUTER INC.
Модель системы:                    P10S-I Series
Тип системы:                       x64-based PC
Процессор(ы):                      Число процессоров - 1.
                                   [01]: Intel64 Family 6 Model 94 Stepping 3 GenuineIntel ~800 МГц
Версия BIOS:                       American Megatrends Inc. 4301, 31.01.2018
Папка Windows:                     C:\Windows
Системная папка:                   C:\Windows\system32
Устройство загрузки:               \Device\HarddiskVolume1
Язык системы:                      ru;Русский
Язык ввода:                        ru;Русский
Часовой пояс:                      (UTC+02:00) Вильнюс, Киев, Рига, София, Таллин, Хельсинки
Полный объем физической памяти:    16 316 МБ
Доступная физическая память:       3 812 МБ
Виртуальная память: Макс. размер:  18 748 МБ
Виртуальная память: Доступна:      5 602 МБ
Виртуальная память: Используется:  13 146 МБ
```

Рисунок 1.4 – Характеристики другого серверу

У цій роботі сервера будуть використовуватися як серверні бази даних, і до кожного сервера буде проведено локальне підключення мережі, перевірка на встановлені внутрішні IP-адреси, а також застосовані норми безпеки самого сервера, баз даних, архівації та активація ліцензії RDP.

1.2 Бази даних та СУБД

У наш час інформація набуває статусу ресурсу завдяки розвитку інформаційного суспільства, але й у цього є зворотний бік медалі, тому що потрібно все більше необхідності зберігання великих обсягів інформації. Також постає відкрите питання про складність використання технології, яка здатна: організовувати, систематизувати, зберігати, оновлювати, редагувати, структурувати, обробляти інформацію.

Оптимальними й доступними є технології баз даних - БД. Бази даних дозволяють створювати структуровані масиви даних, які будуть зберігатися й управляються із застосуванням комп'ютерних технологій, які також використовуються для створення та функціонування даних.

Бази даних (БД) - це спеціальний набір даних, який зберігається у системі. Управління самою базою бере СУБД система управління базами даних, завдання якої забезпечення та контроль даними [7].

Реляційна база даних (БД) – є організованим набором даних, який здійснює за допомогою набору таблиць, що складається зі стовпців та рядків. У цих таблицях зберігається інформація, яка занесена до бази даних [6]. Ідентифікація рядка в таблиці відбувається з допомогою первинного ключа, а зв'язок між іншими таблицями дозволяє здійснювати зовнішній ключ. Основна мета такої бази це усунення надмірності бази даних, завдяки ключу можно упорядкувати БД для інформації

Таблиця 1.1– Функції та призначення БД

Функція	**Призначення**
Зберігання певних даних	У БД зберігаються: особиста інформація, транзакції, тексти, логи, документи, паролі. В електронному форматі доступ до певних даних можна отримати через Адміністратора, або посади яка має дозвіл надавати доступ.
Змінити дані	Щоб забезпечити максимальний захист даних, для зміни видаються певні дозволи, які дозволяють редагувати частину бази даних, або повністю залежно від повноважень.
Управління метаданими	Інформація зберігається з метаданими або метатегами, завдяки яким підтримується порядок у базі даних та дозволяє використовувати функцію пошуку. Дозволи регулюються за допомогою метаданих.
Безпека даних	Доступ до бази даних може здійснюватися за допомогою аутентифікації, яка запитує пароль та ім'я користувача. Це необхідно для запобігання доступу неуповноважених осіб до інформації, наприклад, яка може нашкодити системі.
Цілісність даних	Функція цілісності включає в себе перевірку бази даних перед оновленням або видаленням. Також встановлюються тригери для перевірки записів, наприклад, опорних таблиць.

Продовження Таблиці 1.1

Функція	Призначення
Розрахована на багато користувачів функція	Ця функція дозволяє використовувати базу даних через додаток n-му кількості користувачів.
Оптимізовані запити	Оптимізація бази даних завжди стоїть на першому місці через продуктивність та навантаження. Чим краще оптимізована база, тим швидше будуть зчитуватися запити.
Тригери та процедури	Типові процеси, які зберігаються в СУБД. Збережені процедури дозволяють підвищити продуктивність додатків.
Прозорість системи	Прозорість системи актуальна, особливо у розподілених моделях класифікації БД.

Найчастіше БД створюється для зберігання та доступу до даних, які будуть регулярно використовуватися в робочих цілях, а також забезпечення контролю доступу за інформацією. Наприклад, в електронних базах зберігаються логіни та шифруються паролі, особисті дані користувачів і навіть електронні валюти тощо.

Залежно від зміни бази даних її тип відносять за класифікацією БД до статичного чи динамічного. Функції статичних БД: Дозволяють лише читання даних, крім модифікації. Застосовуються для біографій та історичних фактів або сценаріїв, до яких можна звертатися для дослідження, без зміни змісту. Вони безпечні та прості у використанні під час підключення до мережі.

Функції динамічних БД: Вони мають поняття самоврядування. Можуть бути пов'язані з динамічними мережами. Ця структурна асоціація дозволяє зберігати та оновлювати інформацію бази даних. Використовує HTML як

мову зв'язку між мережею та динамічною БД. Найбільш використовуються мови для створення динамічних мереж, пов'язаних з BBDD: Perl, CGI, PHP, JSP та ASP.

Основними СУБД, які працюють з динамічними вебсторінками, є PostgresQL, MySQL, Oracle та Microsoft SQL. Для того, щоб зрозуміти, які існують варіанти класифікації БД, що використовуються у науковому та освітньому середовищі, розглядають: бібліографічні; документальні; спеціалізовані; довідники.

Рисунок 1.5 – Класифікація баз даних

1.2.1 Реляційні СУБД

Основне завдання СУБД – це оптимізація, зчитування та запис даних. SQL (мова структурованих запитів) та MQL (мова запитів MongoDB) – це

приклади мов запитів, призначених для різних структур даних. SQL (Structured Query Language) – це спеціальна структурована мова запитів для роботи з реляційними БД та СУБД. За допомогою SQL можна формувати запит і направляти його в базу. Авжеж, база даних розуміє запит і обробляє необхідну інформацію. MQL (Metaweb Query Language) – це API для створення програмованих запитів до Freebase. MQL дозволяє включати інформацію з бази даних Freebase в різні програми та вебсайти. На додаток до забезпечення синтаксису, системи управління БД зазвичай надають мережеву точку доступу для підключення до бази даних та видачі команд.

Рисунок 1.6 – Основні функції СУБД

Рисунок 1.7 – Компоненти сучасної СУБД

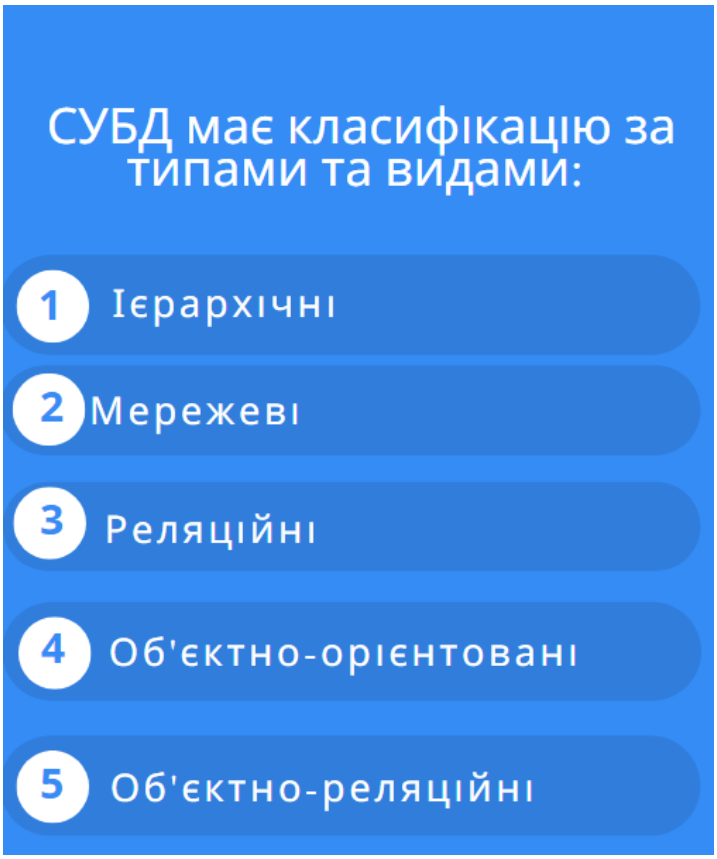


Рисунок 1.8 – Класифікація СУБД

Натомість об'єктно-реляційна СУБД дозволяє завантажувати код, призначений для обробки «нетипових» даних[2].

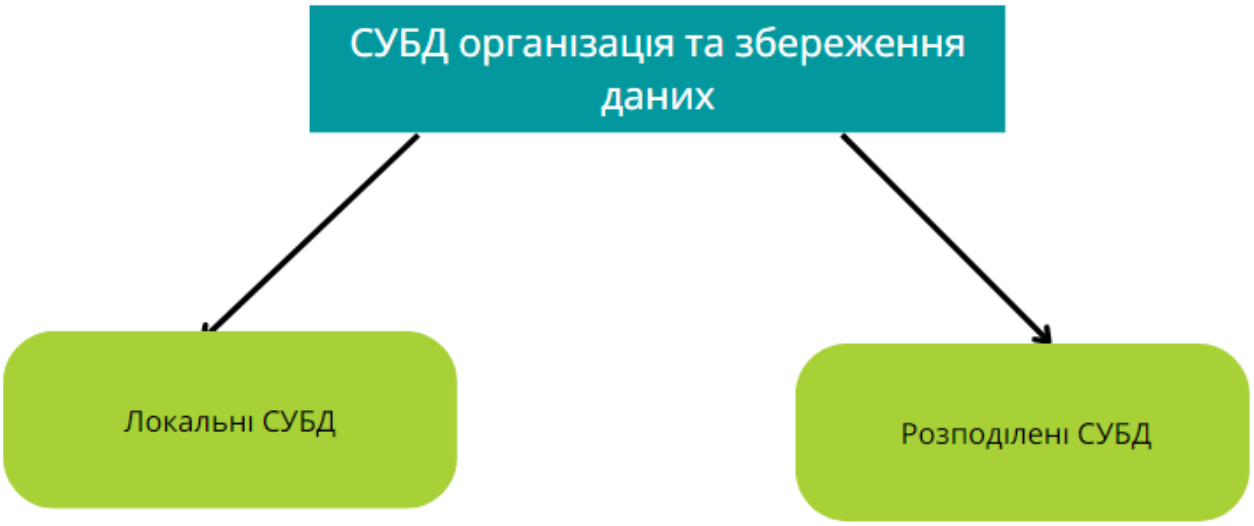


Рисунок 1.9 – Збереження та організація даних СУБД

1.3 Актуальні реляційні бази

СУБД може зберігати та організовувати дані за допомогою двох варіантів: локально та розподілено. Локально це означає, що на одному пристрої будуть розподілені всі частини системи управління базою даних. Авжеж, розподілено дозволяє розміщувати частини СУБД на 2-х і більше пристроях [7].

Доступ до БД здійснюється за допомогою СУБД, що вбудовується, клієнт-серверного, файлу-серверного. Наприклад, файл-серверний дозволяє отримувати доступ завдяки лише локальній мережі, але через це відбувається навантаження всієї локальної мережі [7]. Також оновлення відбуваються завдяки файловим блокуванням.

Клієнт-серверний варіант вимагає існування сервера для СУБД внаслідок, що споживає великі обчислювальні ресурси, особливо оперативну

пам'ять. Позитивною стороною цього методу є низьке завантаження для клієнтських апаратів, мережі та розподіл доступу між безліччю користувачів.

СУБД, що вбудовується, має більше швидкості при читанні та запису в порівнянні з клієнт-серверним варіантом, тому що зберігає велику кількість інформації на одному пристрої і не вимагають установки самого сервера [7]. Доступ здійснюється через особливість СУБД або мову SQL.

SQLite - це одна з найлегших релятивних СУБД більшість функцій якої є безплатним. Працює вона методом файл-сервер суть якого є оновлення шляхом блокування файлів. Завдяки цьому відбувається низьке навантаження на ЦП, що робить цю базу актуальною для використання, наприклад, телеграм бота.

Таблиця 1.2.– Переваги і недоліки SQLite

Переваги	**Недоліки**
Не вимагає багато ресурсів для встановлення бази даних та роботи.	Підтримка лише чотирьох типів даних: INTEGER - відповідає за цілі числа; REAL - відповідає за дробові числа; TEXT - відповідає за символи або інакше текст; BLOB - відповідає за двійкові дані.
Відсутність тривалого налаштування програми, додаткові компоненти встановлюються рідко.	Не підтримується функція збережених процедур, яка необхідна забезпечення бази даних, що дозволяє замість постійного запиту посилатися процедуру.
Безкоштовність СУБД.	Неможливість створити користувача для керування правами доступу до даних.
Висока швидкість обробки простих операцій.	Відсутність додаткових параметрів для підвищення продуктивності.

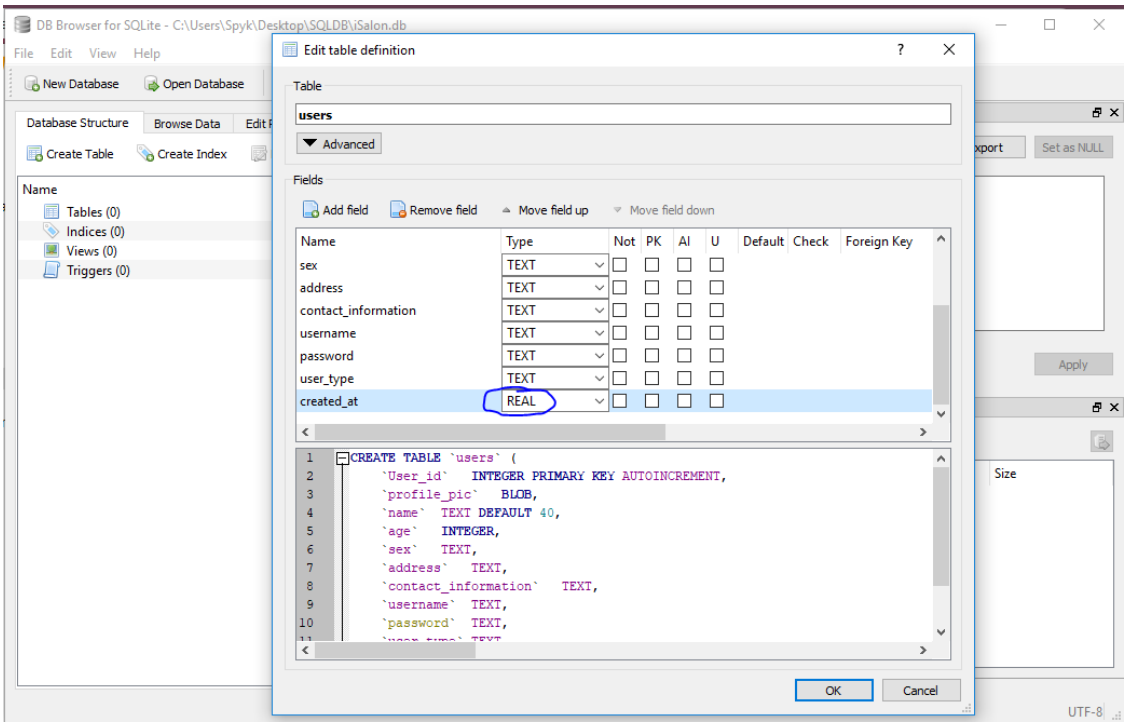


Рисунок 1.10 –Приклад роботи з інтерфейсом SQLite

MySQL - це популярна реляційна система управління базами даних, яка налаштована на роботу з сайтами та вебдодатками. Розвитку цієї СУБД допомагають плагіни, популярність та простота.

Таблиця 1.3– Переваги і недоліки MySQL

Переваги	**Недоліки**
Вбудовані функції безпеки даних.	Дуже рідкісні оновлення через безкоштовність програми.
Наявність плагінів, які спрощують роботу з БД.	Обмежений набір можливостей SQL для роботи з БД.
Універсальність. Завдяки досвіду роботи з MySQL можна запросто вивчати інші СУБД	Проблема роботи з дуже величезними базами. Інструментарій MySQL не встигає обробляти запити тощо.
Безкоштовність СУБД.	Налаштування функцій, які використовуються в інших СУБД.
Поширеність. Поточна СУБД є для 3-х типів систем Linux, MacOS та Windows.	Відсутність додаткових параметрів для підвищення продуктивності.

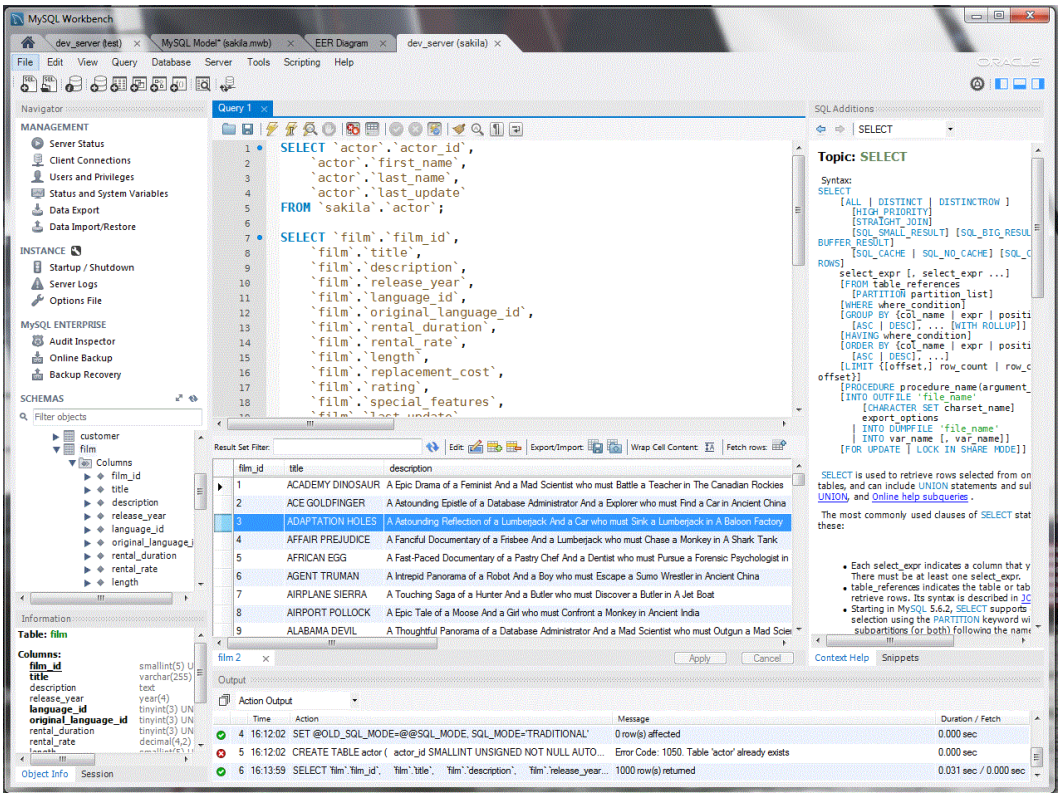


Рисунок 1.11 –Приклад роботи з інтерфейсом MySQL

PostgreSQL це СУБД, яка застосовується за типом клієнт-сервер, її особливістю є архітектура, яка будує розподілену систему для клієнта та сервера. Ця функція називається паралельний доступ, наприклад коли виконується транзакція розповсюдження інформації починається після її завершення. На жаль у нас час реалізація PostgreSQL під великим питанням, більшість вибирає Microsoft SQL Server із-за зручності застосування, але PostgreSQL має великий потенціал завдяки ретельного налаштування. Також цю СУБД використовують у різних сферах, наприклад наукова сфера де проводяться дослідження, та обробка величезних даних кожен день. Спеціальній компонент Postgre GIS, допомагає у роботі з географічними даними.

Таблиця 1.4 – Переваги і недоліки PostgreSQL

Переваги	Недоліки
Велика підтримка спільноти.	Робити реплікацію складніше.
Обробка величезної кількості даних.	Не найвища швидкість обробки даних.
Має підтримку ACID, тобто. атомарність, узгодженість, ізоляція, довговічність.	Величезне використання оперативної пам'яті.
Функція зберігання різних типів мережевих адрес.	Не просте встановлення програми.
Поширеність. Поточна СУБД є для 3-х типів систем Linux, MacOS та Windows.	Необхідність навчання роботи із СУБД. Ця програма не для недосвідчених адміністраторів.

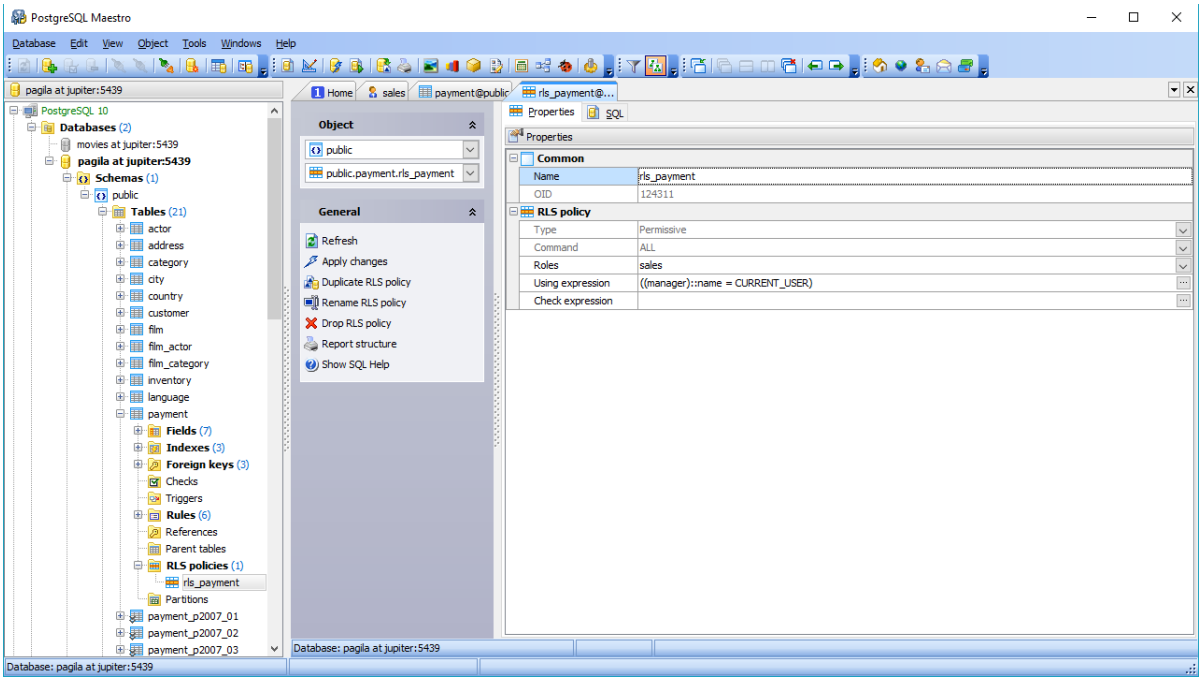


Рисунок 1.12 –Приклад роботи з інтерфейсом PostgreSQL

Microsoft SQL Server – ця СУБД розроблена компанією Microsoft. Програма доступу в кількох версіях зі своїми відмінностями працює тільки на операційній системі Windows. Являється одною с найпопулярніших прогам для баз даних.

Таблиця 1.5– Переваги і недоліки Microsoft SQL Server

Переваги	Недоліки
Можливість використовувати пошук за допомогою ключових індексів, а також словами чи текстом.	Працює тільки на операційній системі Windows.
Висока продуктивність та обробка величезної кількості запитів.	Не найвища швидкість обробки даних.
Можливість здійснювати запити, використовуючи тільки англійську мову.	Величезне використання оперативної пам'яті.
Оптимізоване адміністрування та автоматизовані завдання.	Не просте встановлення програми.
Інтеграція з іншими продуктами Microsoft.	Необхідність навчання роботи із СУБД. Ця програма не для недосвідчених адміністраторів.

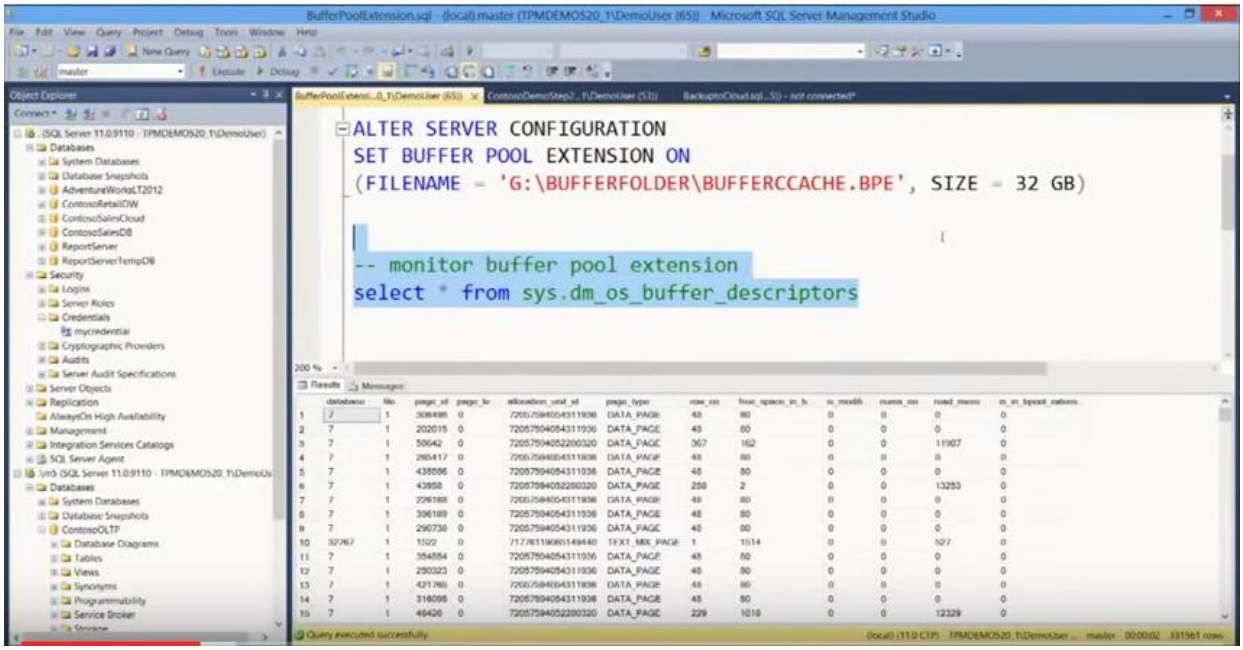


Рисунок 1.13 –Приклад роботи з інтерфейсом Microsoft SQL Server

2 ПРОГРАМНЕ НАЛАШТУВАННЯ СЕРВЕРА ДЛЯ ВИКОРИСТАННЯ

Перш ніж почати використовувати сервер, його потрібно програмно налаштувати й підготувати. Для початку необхідно створити та налаштувати Raid через біос, потім на нього встановити нашу операційну систему, а також налаштувати систему під потреби сервера та встановити програми. Сервер необхідно підтримувати, що означає оновлення програмного забезпечення, резервне копіювання, контроль доступу до мережевих ресурсів, розподіл жорстких дисків. Створення Hyper-V для роботи та безпеки інформації. В даному етапі після налаштування Raid обов'язково потрібно налаштувати віддалене підключення до сервера і на прикладі в сервер я покажу як відбувається налаштування та активація. Після цього оновлюємо драйвера для нашого пристрою, щоб переконатися в стабільності та працездатності. З налаштуванням сервера під завдання нам допоможе диспетчер серверів.

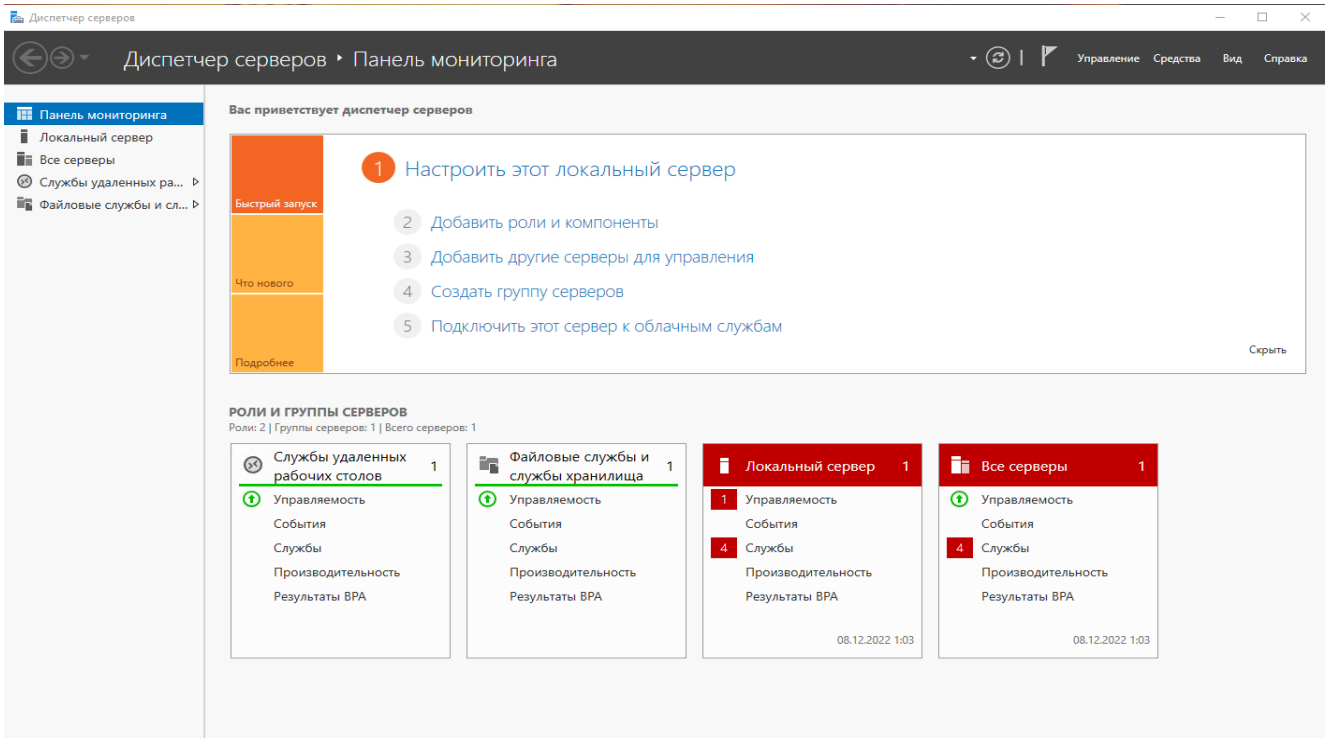


Рисунок 2.1 – Диспетчер серверів

2.1 Класифікація Raid для серверів

Спершу нам потрібно створити та налаштувати Raid основне завдання якого – захист та оптимізація використання даних. Як тільки ця дія буде закінчена, починається встановлення зазначеної операційної системи.

Raid - це технологія створення масивів при промощі кількох дисків суть якого сприйматиметься як один диск. Його також використовують як варіант мінімізування втрат даних за рахунок своєї стійкості до відмови, також деякі Raid використовують дозволяють прискорити диски [14]. У наш час використовується таки типи Raid :

Raid0, Raid1, Raid10, Raid1E, Raid5, Raid5EE, Raid6, Raid50, Raid60.

Raid 0 у разі використовується технологія розподілу на два диска, де дані пишуться спочатку однією диск, потім другий. Безперечна перевага даного Raid у продуктивності, а також чудовій швидкості передачі даних [8]. На жаль, при пошкодженні одного з пристроїв інформація стає пошкодженною.

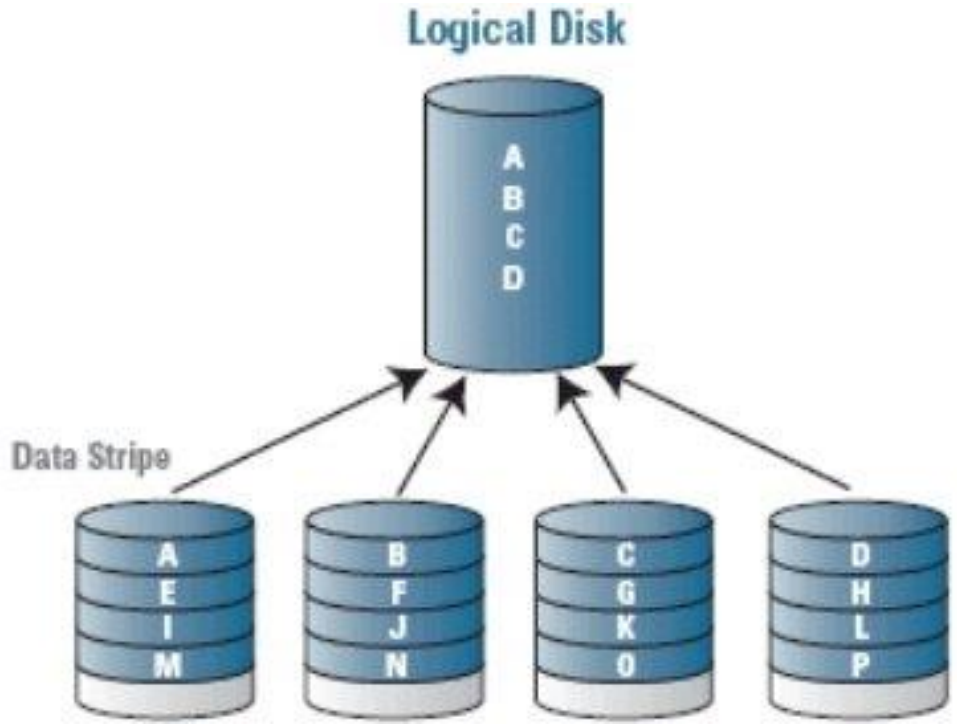


Рисунок 2.2 – Як працює Raid 0

Raid1 його також називають Mirror. Відмінність цього режиму від минулого, що він зосереджений на мінімізації збитків у разі втрати даних. Тобто, якщо один з його дисків має пошкодження, які заважають йому працювати, то робота буде продовжуватися з іншим диском, який в оптимальному стані. Для його створення жертвується розміром диска вдвічі.

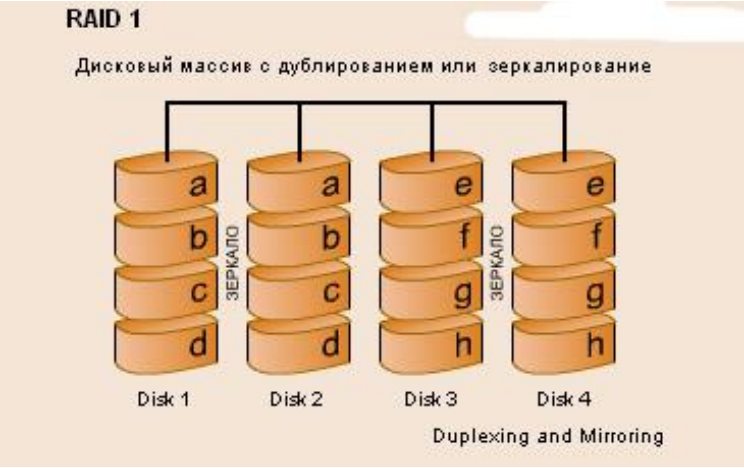


Рисунок 2.3 – Використання методу Raid 1

Raid10 є одним з доступних варіантів для підвищення стабільності та підвищення швидкості. Тому що він використовує технології Raid0 та Raid1 мінімальне використання 4 диски [8].

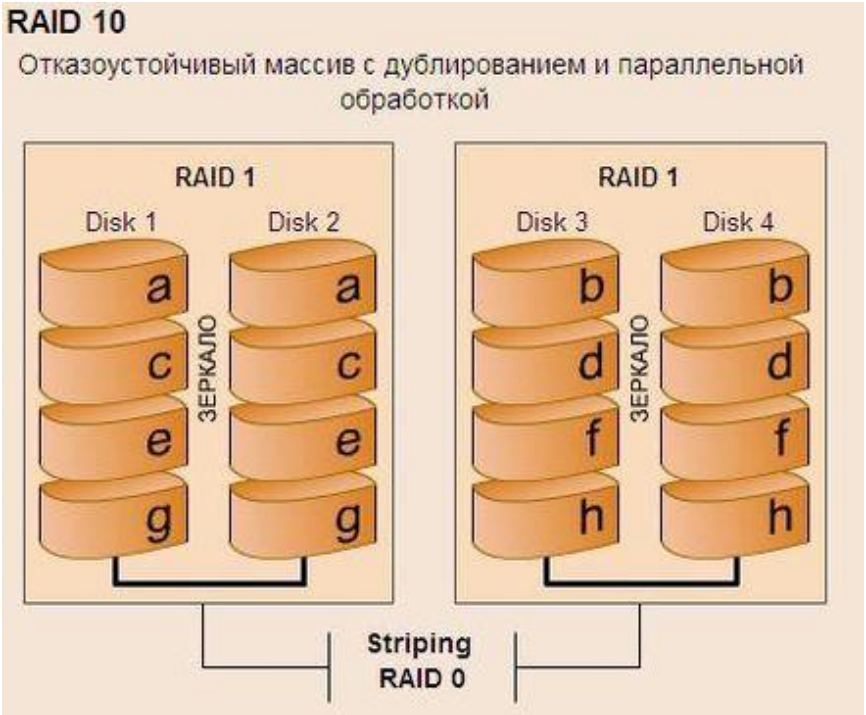


Рисунок 2.4 – Використання Raid10

Raid 1E - дуже своєрідний метод оскільки він вимагає три диски для запису даних, та був пише копію однією з них. Повторює Raid 10 за функціоналом.

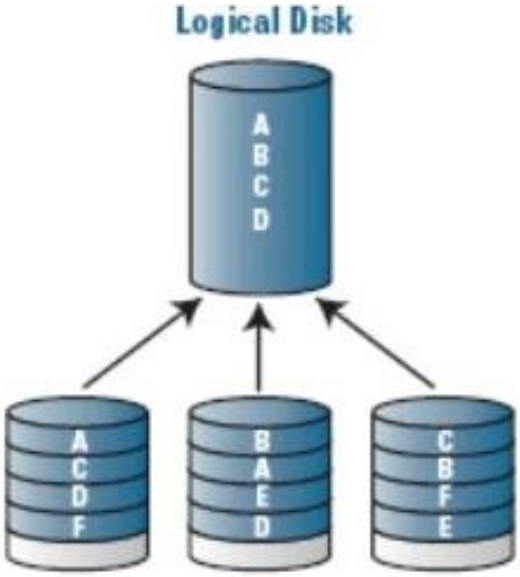


Рисунок 2.5 – Приклад роботи Raid 1E

Raid 5 - використовує розподіл інформації між усіма дисками по секторах, що дозволяє йому працювати далі, якщо трапиться неполадка з диском. Однак відновлювати інформацію через його розподіл досить складне завдання [8]. Переваги висока швидкість читання та запис даних.

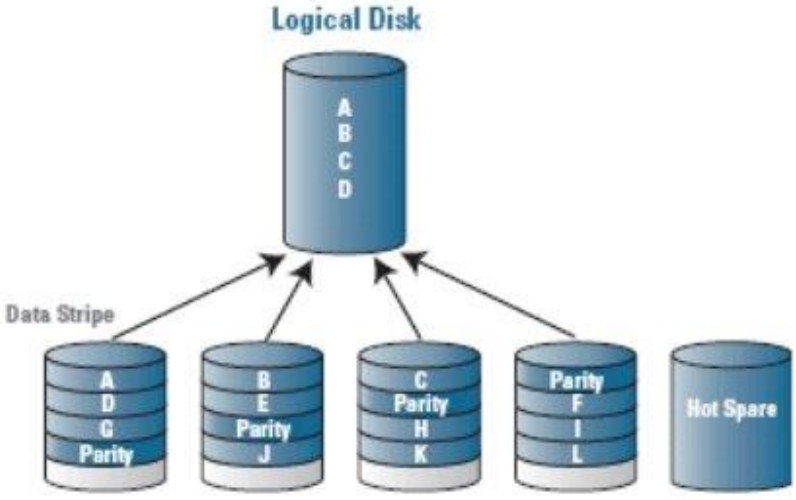


Рисунок 2.6 – Приклад роботи Raid 5

Raid 5EE - використовує функціональність Raid 5, але з парними дисками, що дозволяє включати чергування блоками і бітами. Це дозволяє використовувати відновлення системи набагато швидше.

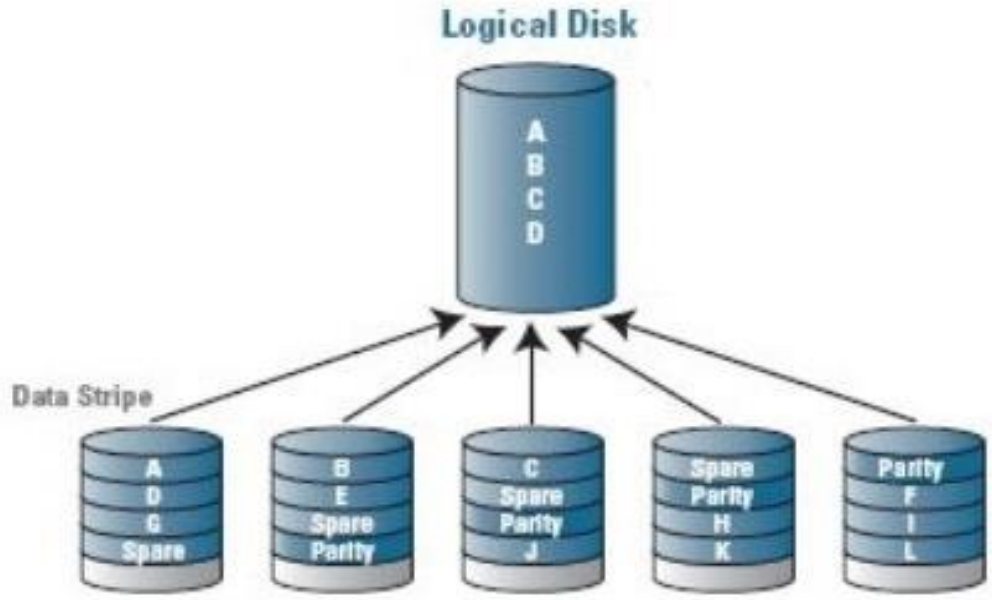


Рисунок 2.7 – Використання Raid 5EE

Raid 6 - використовує чотири диски які застосовують 2 схеми парності, що дозволяє мати стійкість до відмови у двох дисків. Недоліком є незмінна швидкість запису.

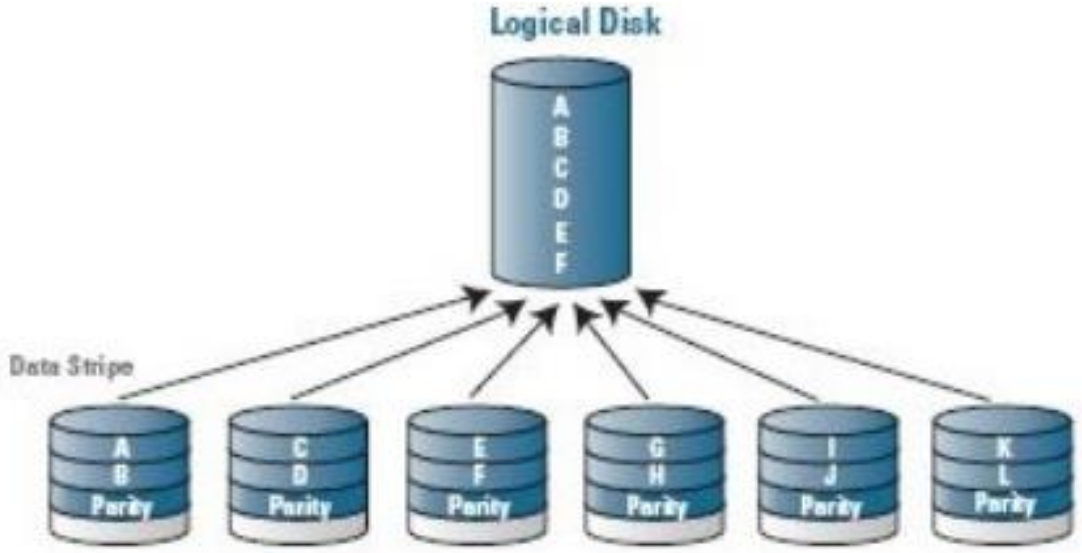


Рисунок 2.8 – Використання методу Raid 6

Raid 50 - це масив який комбінує Raid5 і Raid0, Завдяки цьому Raid5 має не таку низьку швидкість запису даних. Основний недолік що місткість масиву зменшується вже на два диски. Також, він переносить лише відмову одного диску без втрати даних. Кількість дисків для створення такого масиву потребує 6 штук.

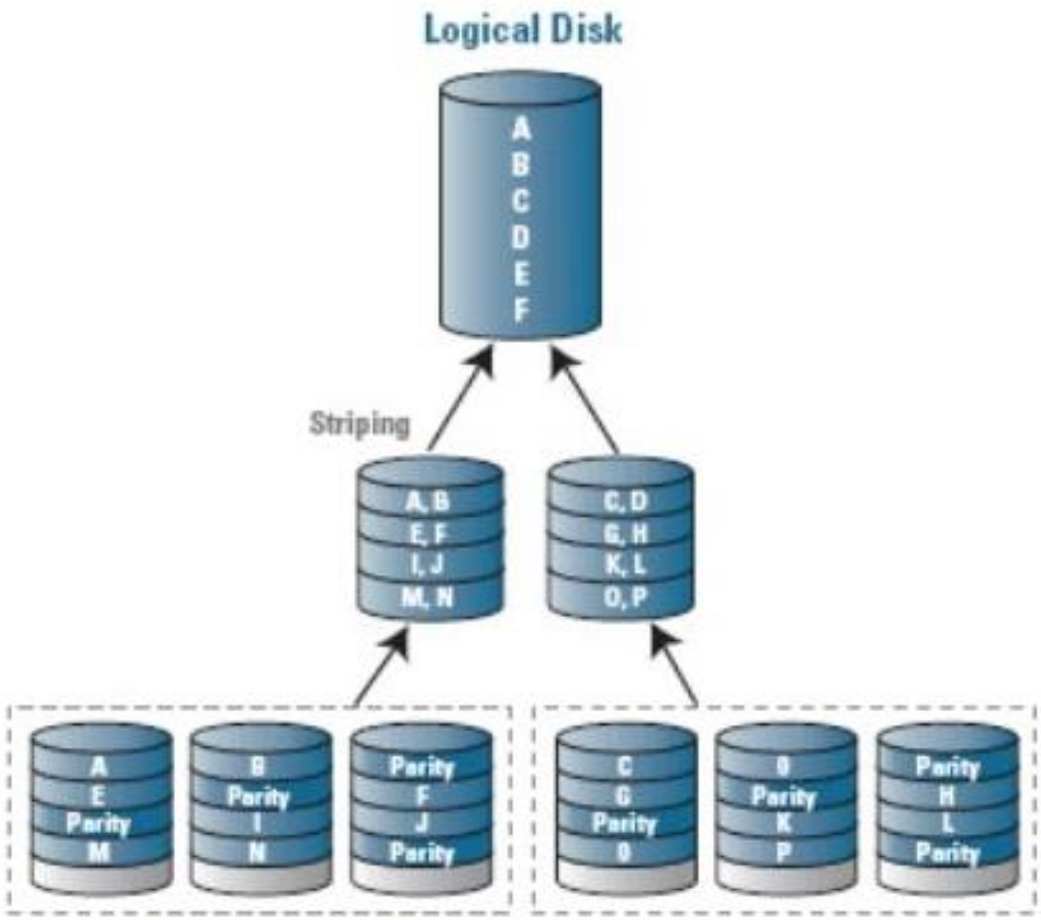


Рисунок 2.9 – Приклад роботи Raid 50

Raid 60 - не дуже поширена технологія, але вона має кілька переваг, наприклад відсутність затримок та запису. Незважаючи на невисокий запис даних Raid 60 має високу швидкість роботи з даними та підвищену відмовостійкість. Має всі плюси Raid 6, тому зберігання даних у цьому варіанті надійніше.

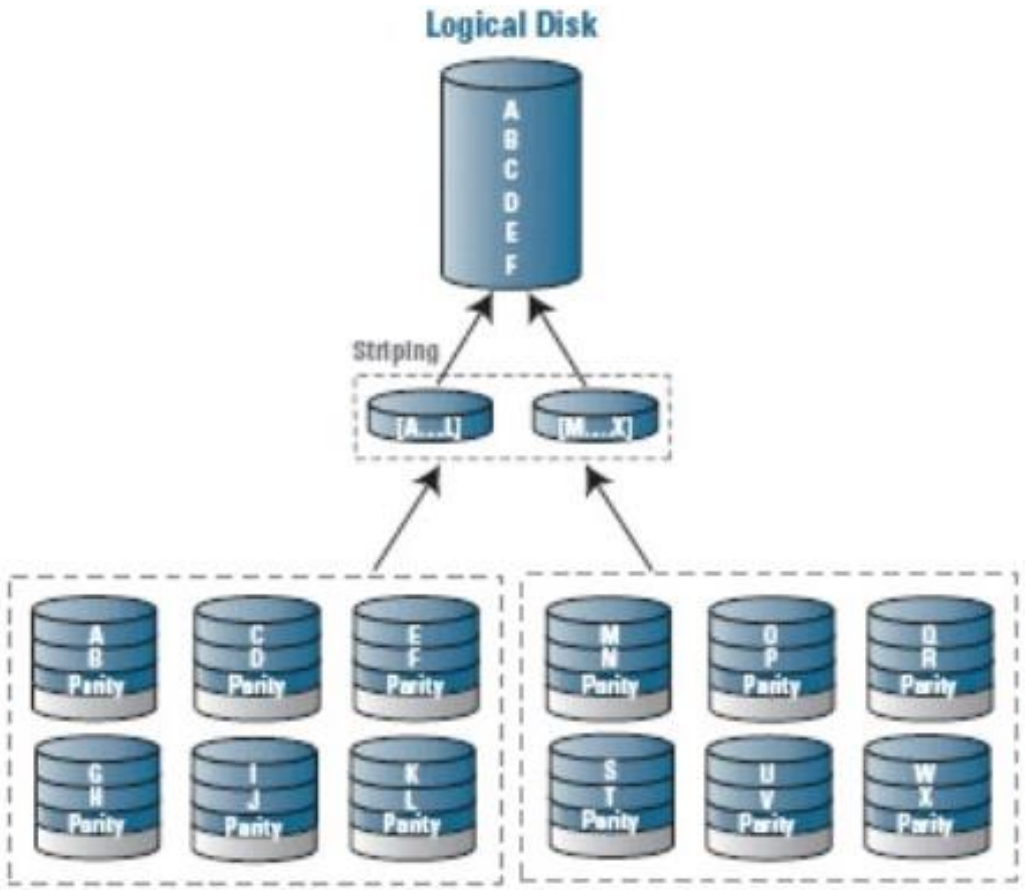


Рисунок 2.10 – Використання методу Raid 6

2.2 Налаштування та створення Raid

Використовуємо BIOS серверу для створення та налаштування Raid1 як приклад. Для початку включимо функцію, яка знаходиться в BIOS сервері. Після того, як був зроблений вхід у біос вибираємо Advanced, опція AHCI Capable SATA Controler. Вибираємо RaidMode. Щоб зберегти зміни натискаємо клавішу F10, після цього Yes. Щоб застосувати установки, використовується перезавантаження пристрою [14]. Дана функція BIOS знаходиться у кожній платі від популярних виробників, але вони мають власні обмеження щодо типу Raid, тому не кожна материнська плата підтримує усі Raid, цім відрізняються звичайні плати від серверних.

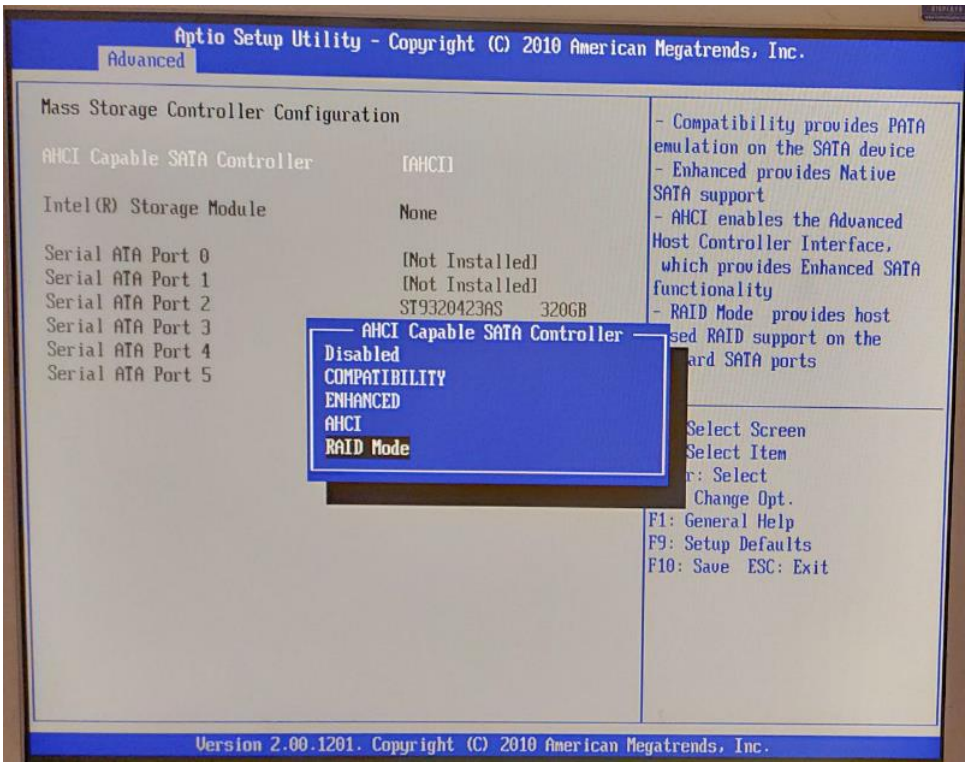


Рисунок 2.11 – Опція Raid Mode

Тепер потрібно зайти в меню Raid, натискаємо на клавіатурі комбінацію клавіш Ctrl+E та меню відкривається.

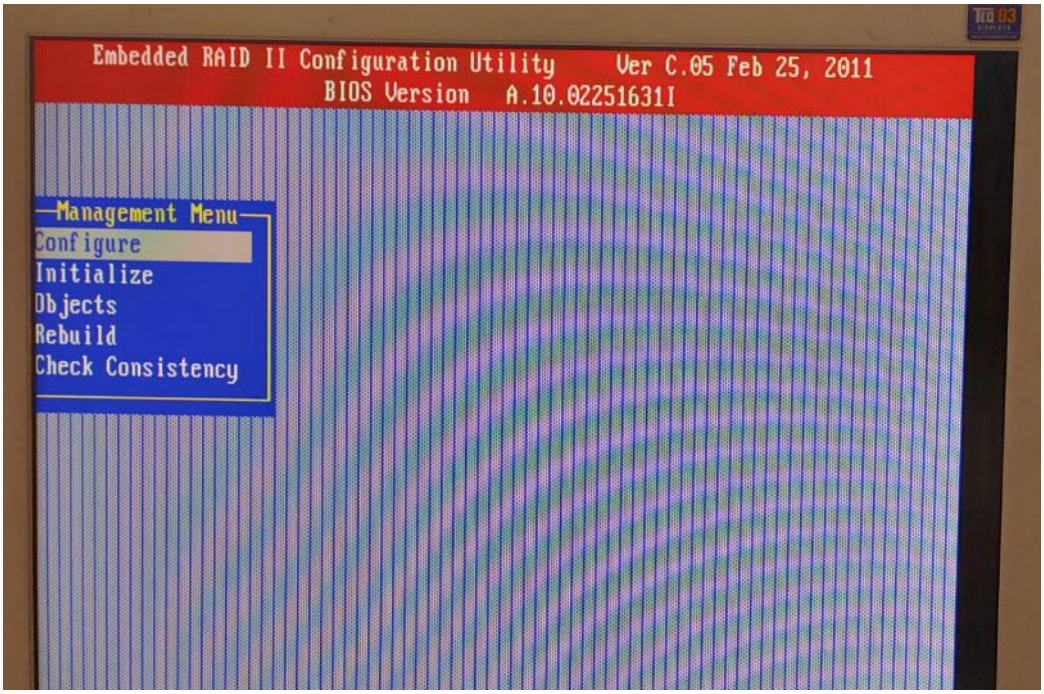


Рисунок 2.12 – Меню Raid

Далі вибираємо Configure та нажимаємо на вибір New Configuration.

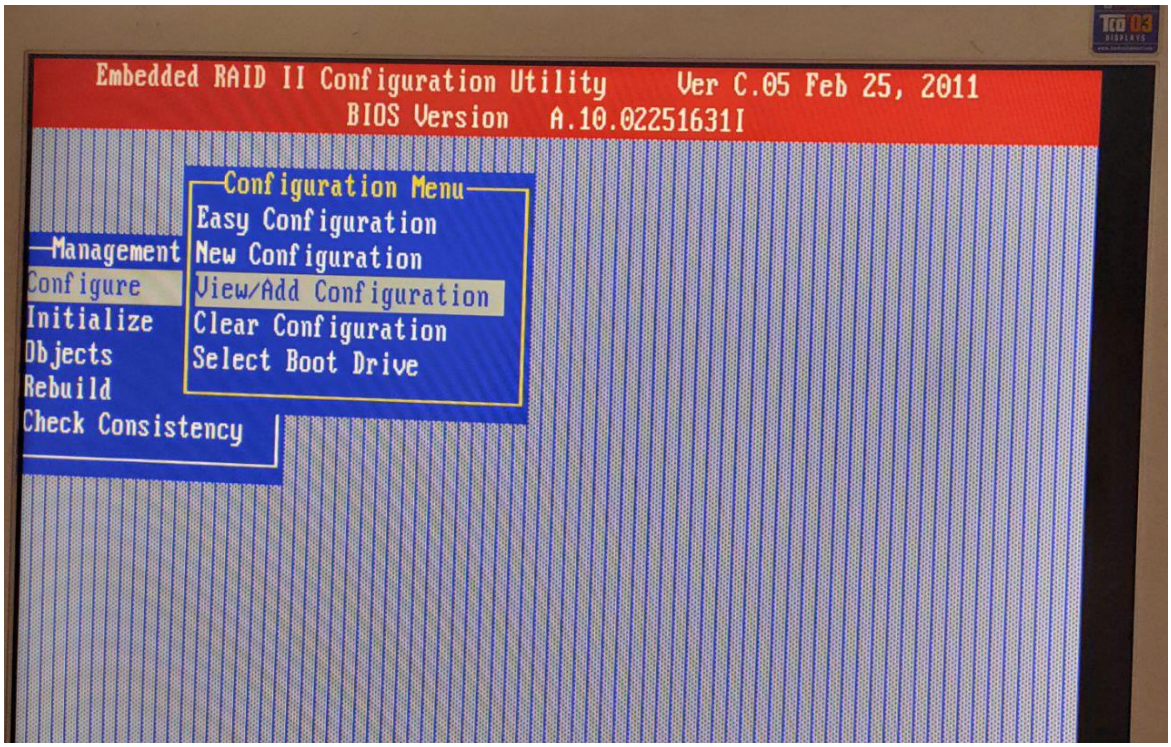


Рисунок 2.13 – Створення Raid масиву

Помічаємо диски з яких буде створюватися Raid1.

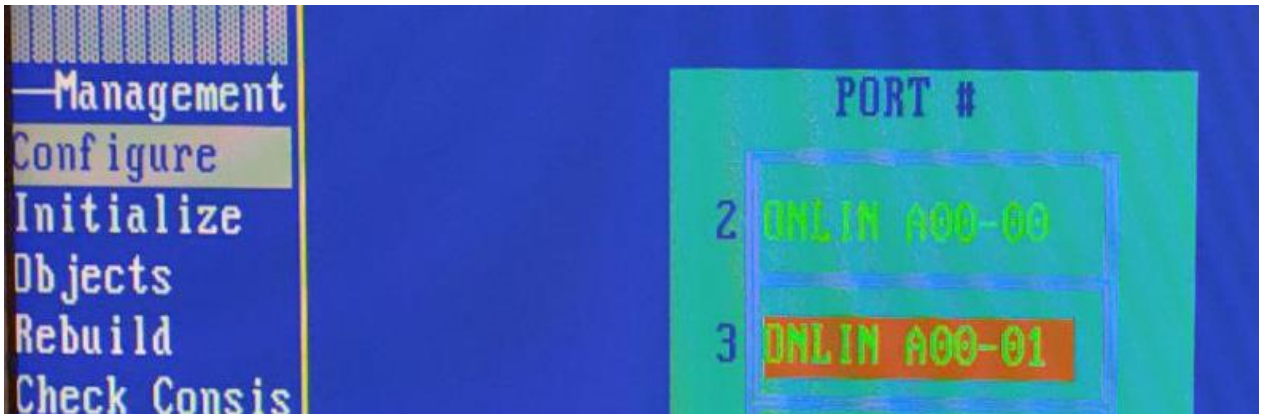


Рисунок 2.14 – Вибір дисків для використання

Вибираємо створення Raid1, інтерфейс показує нам характеристики диска, який вийде шляхом створення масиву [8].

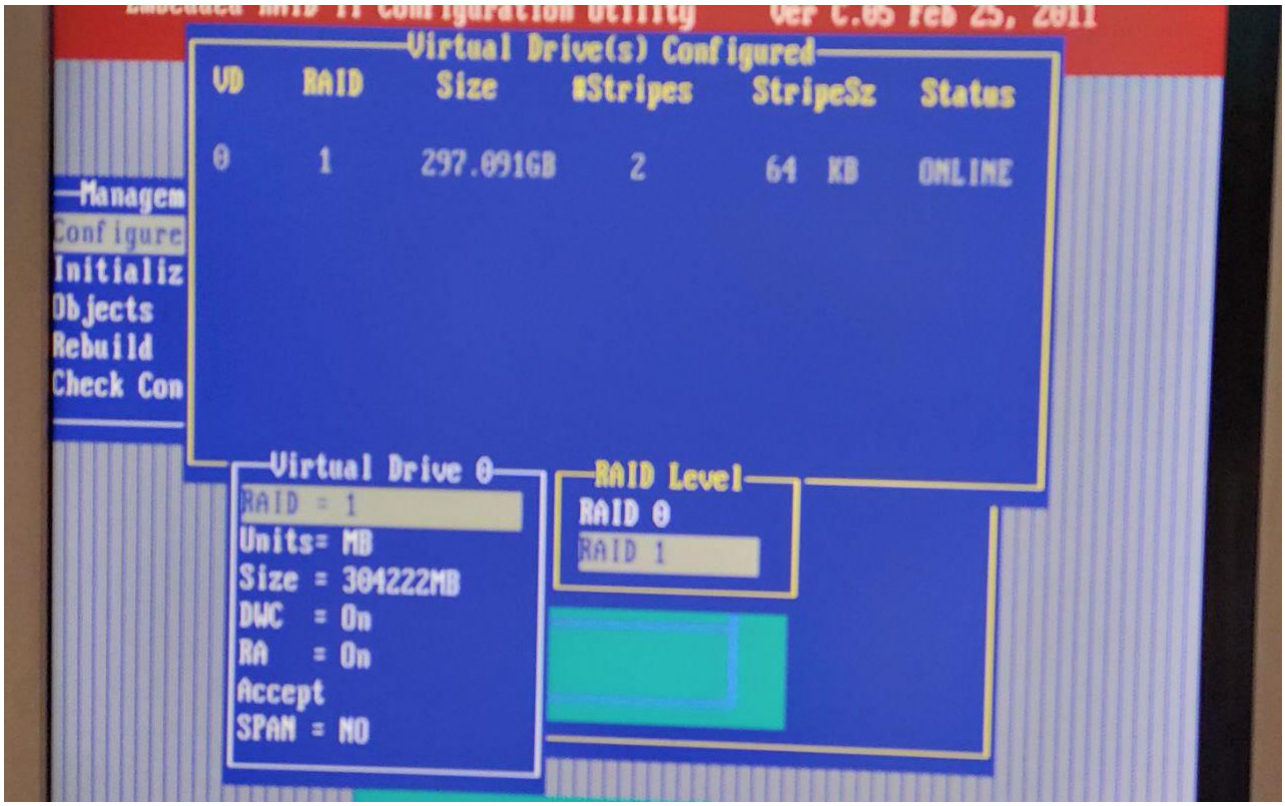


Рисунок 2.15 – Вибір масива Raid1

Останній крок перед створенням Raid1 коли ми отримуємо повідомлення про те, що вся інформація, яка знаходиться на цих дисках, буде остаточно стерта, це варто враховувати, якщо беруться диски на яких вже є дані.

Рисунок 2.16 – Підтвердження для стирання даних

Після остаточного застосування наш пристрій перезавантажується, потім в етапі завантаження видно, що Raid1 визначився і тепер використовується.

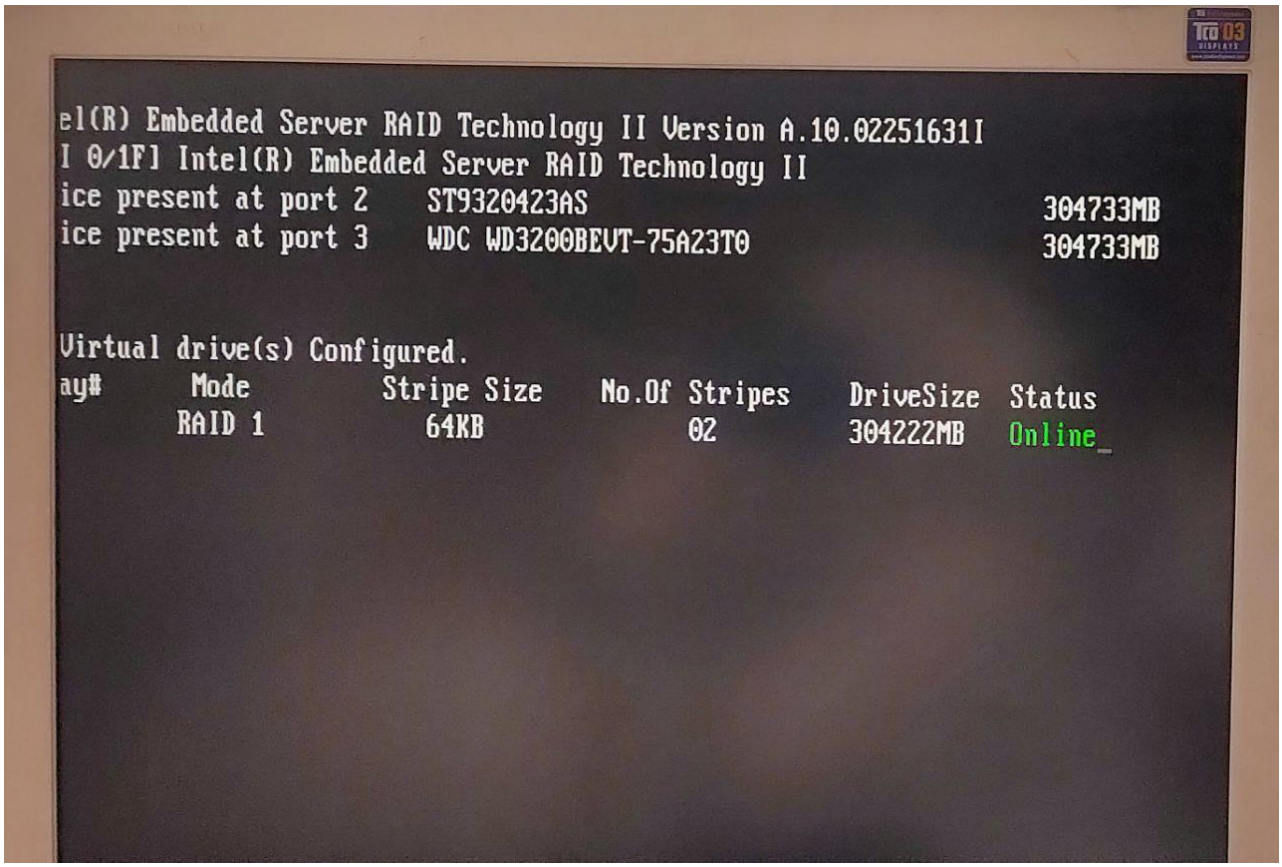


Рисунок 2.17 – Raid1

2.3 Установка Windows Server 2016

Вибираємо вже перевірену часом ОС - Windows Server 2016 для зберігання і використання даних у Hyper-V. Основною перевагою стала підтримка та забезпечення віртуалізації. Система має дуже простий і зручний інтерфейс, оптимізація процесів адміністрування і т.д.

У даній дипломній роботі використовуємо сервер з метою створення віртуалізації та отримання доступу до віртуальних робочих столів. Необхідна функція для використання Intel Virtualization Technology, вона включається до BIOS. Тільки після цього можна використовувати Hyper-V.

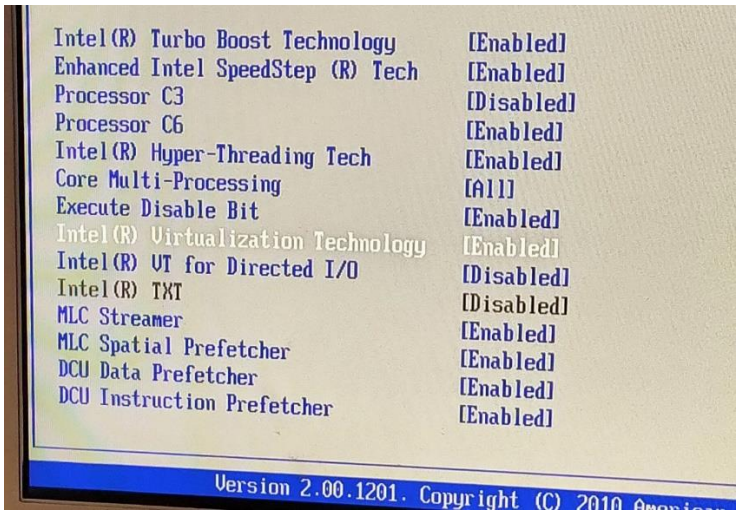


Рисунок 2.18 – Intel Virtualization Technology

Для початку завантажимо образ операційної системи на носій, наприклад флешку. Після цього в BIOS вибираємо щоб наш накопичувач завантажувався першим. Обираємо такі параметри як : мова, формат часу і грошових одиниць, розкладка клавіатури [14].

Версії Windows Server випускаються с графічною оболонкою та без неї. Що б не втрачати часу, вибираємо установку з графічною оболонкою.

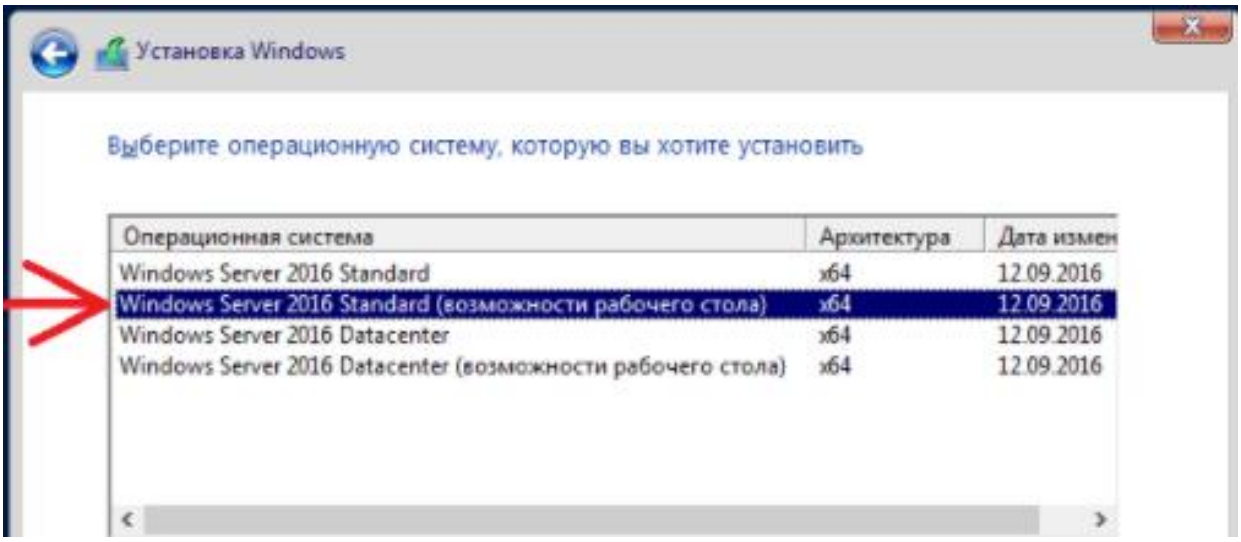


Рисунок 2.19 – Вибір установки з графічною оболонкою

Вибираємо диск, на який будемо встановлювати систему. Натискаємо створити розділ і очікуємо кінця установки.

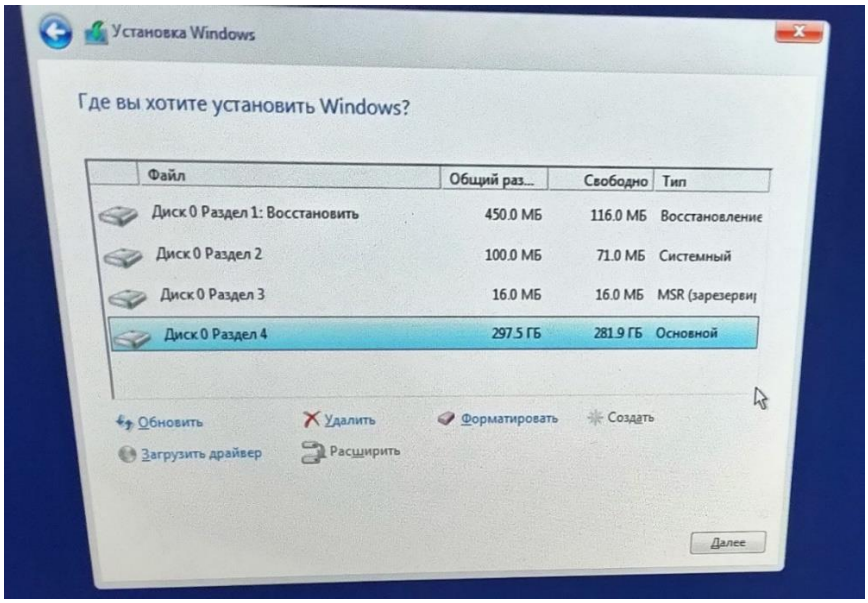


Рисунок 2.20 – Розмітка накопичувача

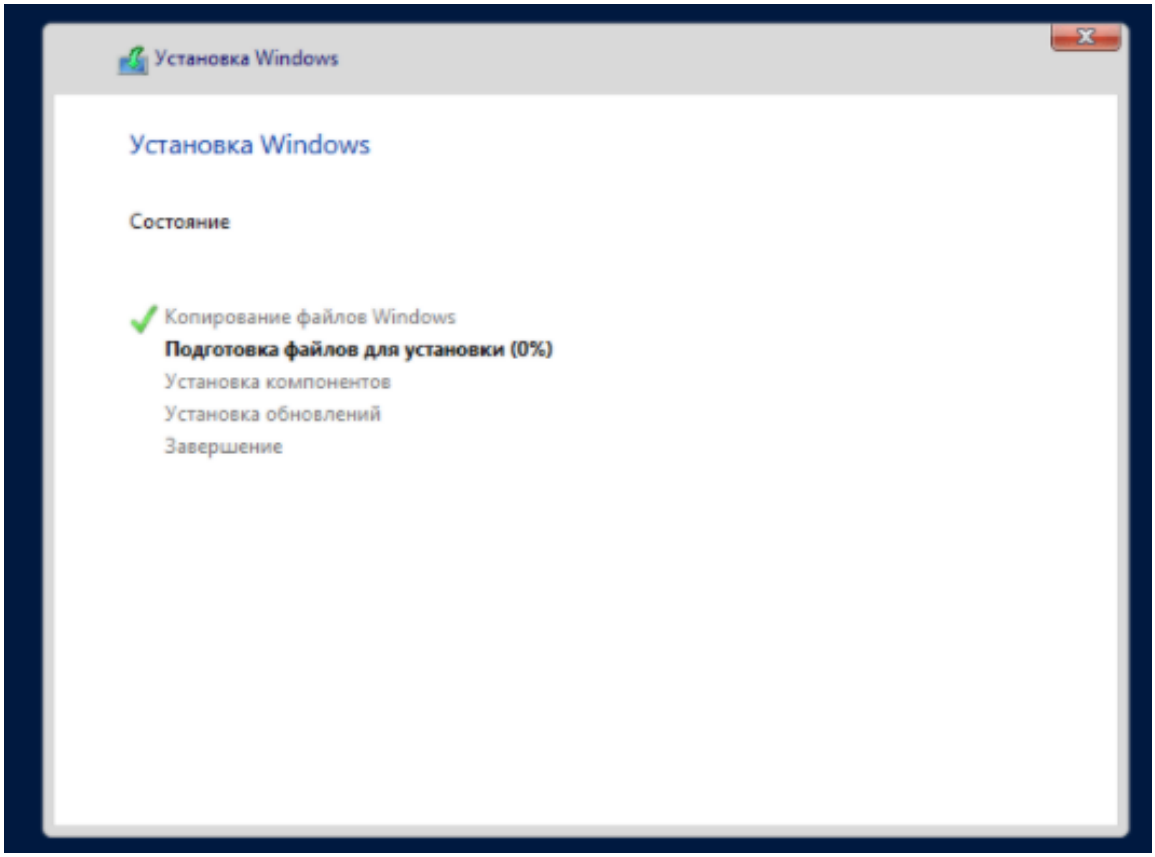


Рисунок 2.21 – очікування завершення установки ОС

2.4 Налаштування ОС перед використанням.

У цій дипломній роботі буде розглянуто базове налаштування Windows Server 2016 для роботи, потім налаштування параметрів підключення віддаленого робочого столу. Підготовка та налаштування до використання технології віртуалізації Hyper-V також буде розглянуто альтернативний варіант налаштування сервера через скрипт Sconfig, який запускається через PowerShell . Після цього буде розподіл прав, встановлення програм і т.д [14].

Після того як ми запустили систему, перше, що нам потрібно зробити це оновити драйвера. Для цього переходимо в параметри => оновлення та безпека => натискаємо перевірити оновлення. Після цього встановлюємо ті чекаємо, також перезавантажуємо систему коли все буде встановлено.

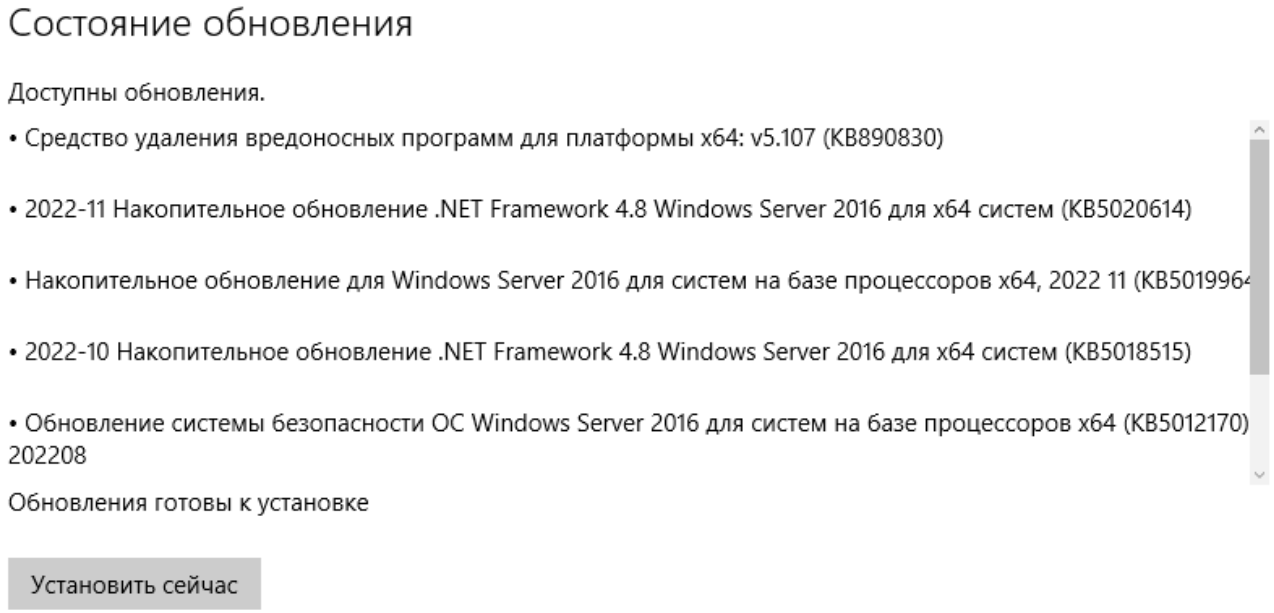


Рисунок 2.22 – Перевірка системи на оновлення

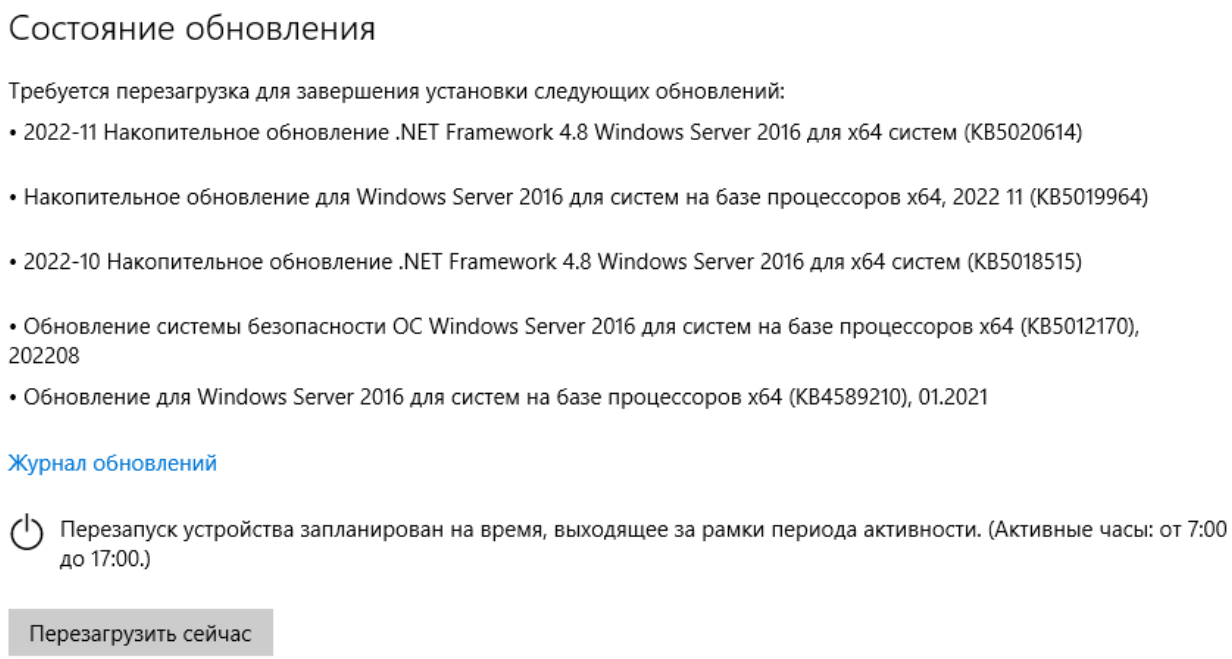


Рисунок 2.23 – Встановлення оновлення

Для роботи з нашим сервером с початку потрібно задати ім'я і робочу групу. Для цього заходимо в властивості системи => змінити параметри => змінити. Після зміни інформації потрібно перезавантажитися.

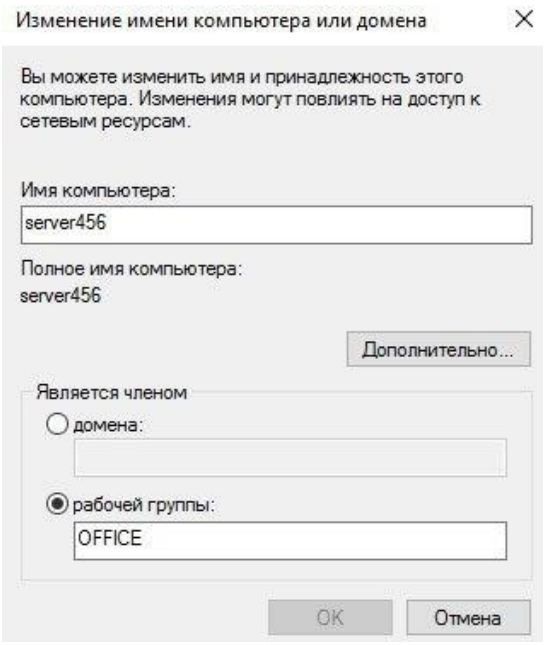


Рисунок 2.24 – Задавання імені та робочої групи

Далі нам потрібно добавити ролі і компоненти для подальшого налаштування сервера.

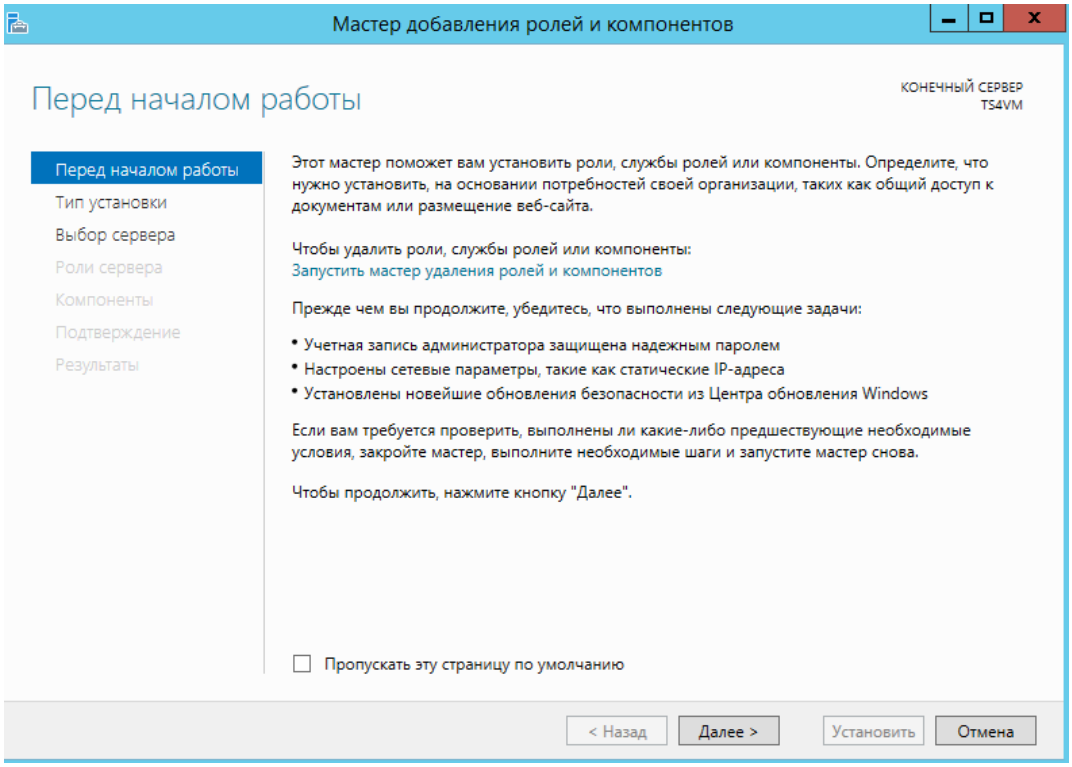


Рисунок 2.25 – Ролі та компоненти

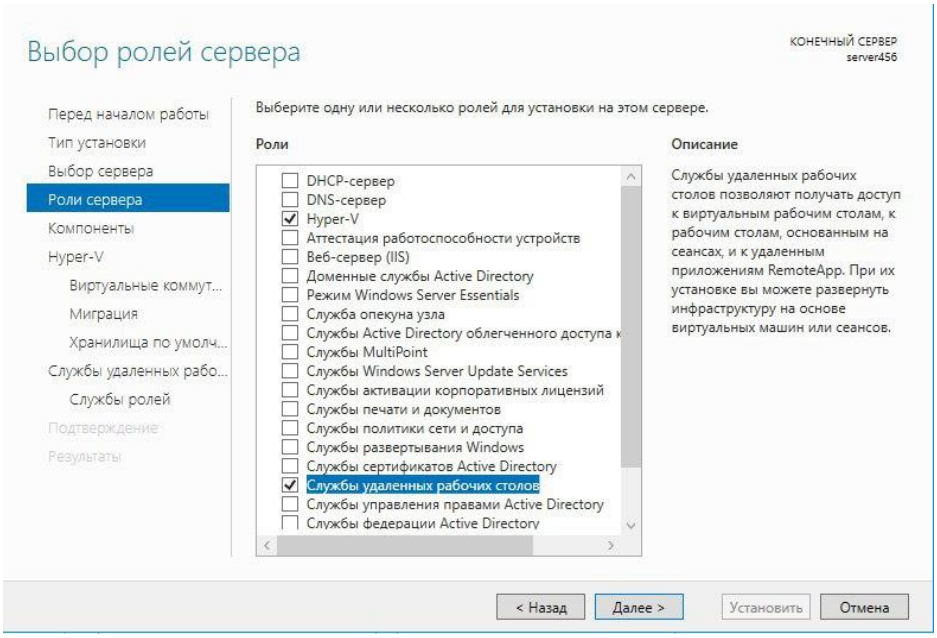


Рисунок 2.26 – Вибір ролей

Для забезпечення захисту інформації включаємо функцію міграція

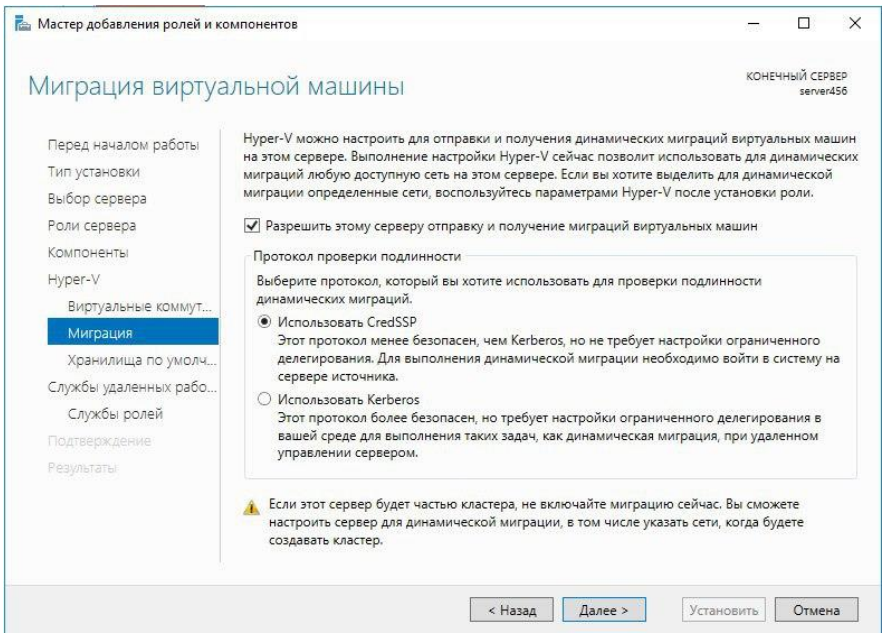


Рисунок 2.27 - Міграція з використанням протоколу CredSSP

Вибираємо ролі для установки служби віддалених робочих столів. Служба ліцензування управляє ліцензіями необхідними для підключення до сервера вузла сеансів віддалених робочих столів. Вузол віддалених робочих столів дозволяє розміщувати на сервері віддалені програми RemoteApp і т.д.

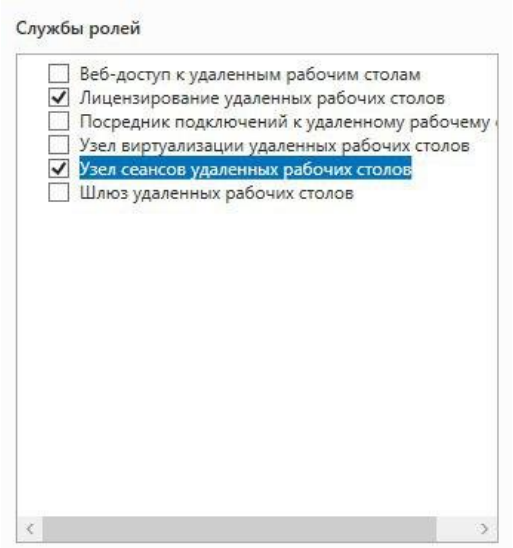


Рисунок 2.28 – Ролі служби віддалених робочих столів

Тепер налаштування сервера за допомогою скрипту Sconfig. Він дозволяє: змінювати ім'я комп'ютера, включати РДП, встановити оновлення, додати домен та адміністратора, налаштувати дату та час, а також вимкнути або перезавантажити комп'ютер. Цей варіант підходить для адміністраторів які мають опит. Попри на те, що все виконується через командний рядок, інтерфейс дуже зрозумілий. Використовується нумерація для потрібних пунктів і все, що потрібно зробити, вибрати цифру в меню та виконати налаштування.

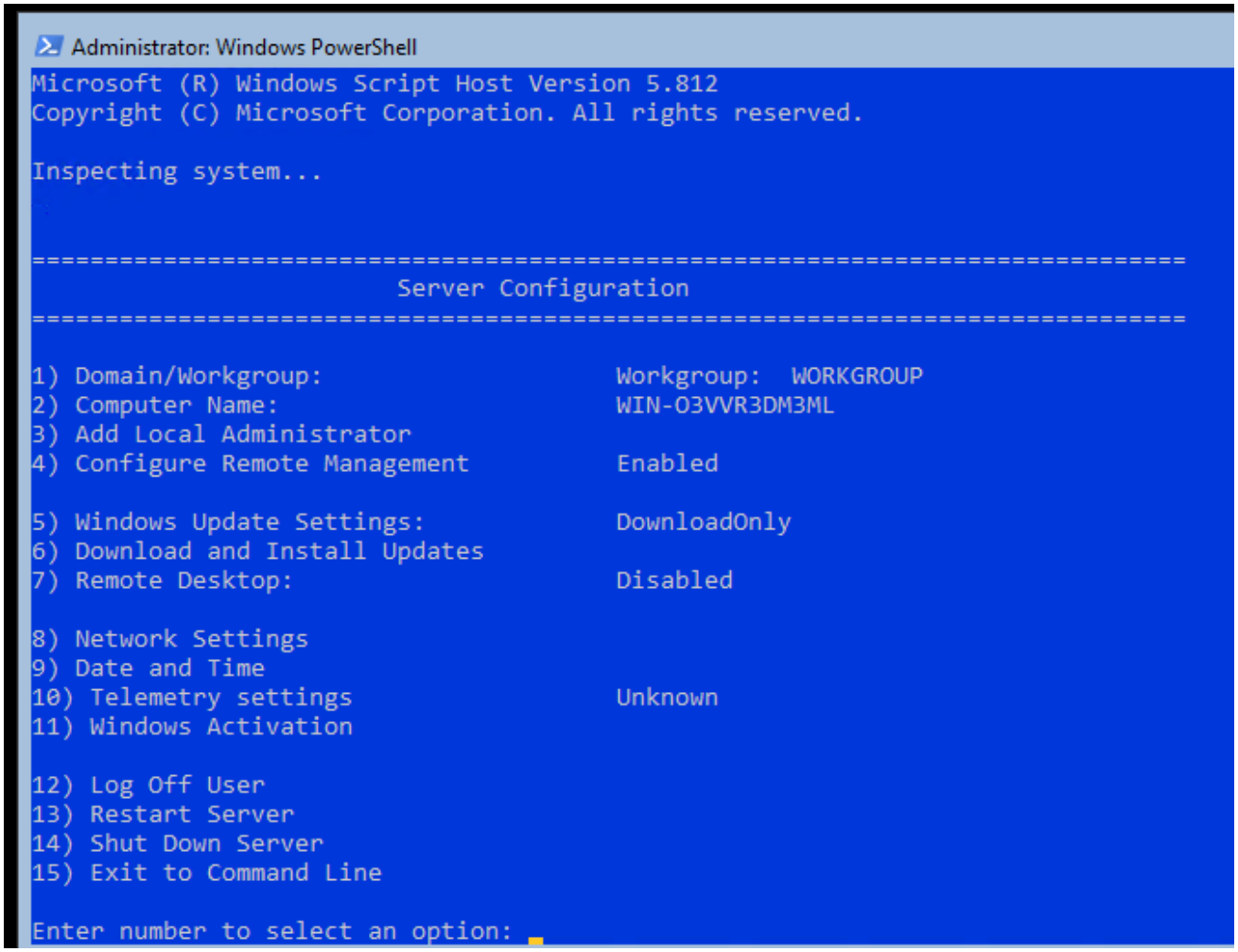


Рисунок 2.29 – Sconfig

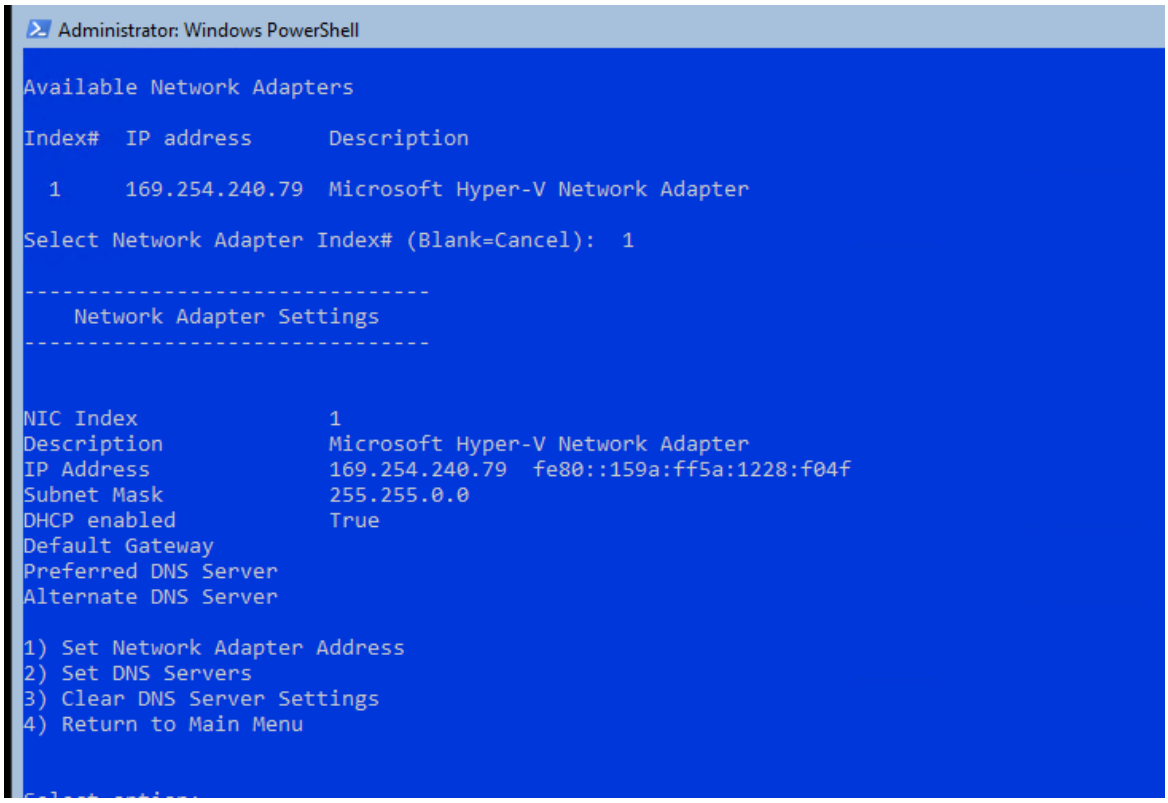


Рисунок 2.30 – Sconfig налаштування

2.5 Технологія віртуалізації Hyper-V

Hyper-V використовує віртуалізацію операційних систем, котра може бути використовуватись не тільки для Windows. При завантаженні системи Hyper-V створюється маленький програмний компонент вага якого не менше 1 Мбайт, його називають гіпервізором [14].

Функція гіпервізору полягає в тому, що він працює між апаратними компонентами фізичного сервера і «базової» операційною системою. Гіпервизор безпосередньо контактує з апаратними компонентами сервера і завжди завантажується до запуска операційної системи. Зазвичай його визначають як мініопераційну систему, яка забезпечує віртуалізацію інших операційних систем [9].

Для того що б використовувати віртуалізацію на основі гипервизора, процесор системи зобов'язаний підтримувати технологію, звану апаратною

підтримкою віртуалізації, перед установкою Hyper-V я вмикав її в BIOS. Гіпервизор виконує найважливіші завдання, такі як управління пам'яттю, і забезпечує захисну ізоляцію базової операційної системи від віртуальних.

Основні задачі гіпервізора це управління пам'яттю та забезпечення захисної базової ізоляції операційної системи від віртуальних. Для зниження ризику витоку усіх данних, Hyper-V використовують як повноцінні операційні системи для роботи і зберігання бази даних, якщо вірус або зловмисник отримає несанкціонований доступ до одної з систем, він не отримає повний контроль над всім сервером [14].

Для забезпечення даних в віртуальній машині рекомендується зробити контрольні точки. Існують стандартні контрольні точки та робочі. Стандартні створюють моментальний знімок віртуальної машини і стану її пам'яті. Робочі створюють резервну копію віртуальної машини на рівні даних, завдяки службі копіювання томів, зроблено це з метою перенесення віртуальної машини на інший пристрій без проблем [9].

Створення віртуальної машини завдяки диспетчеру Hyper-V

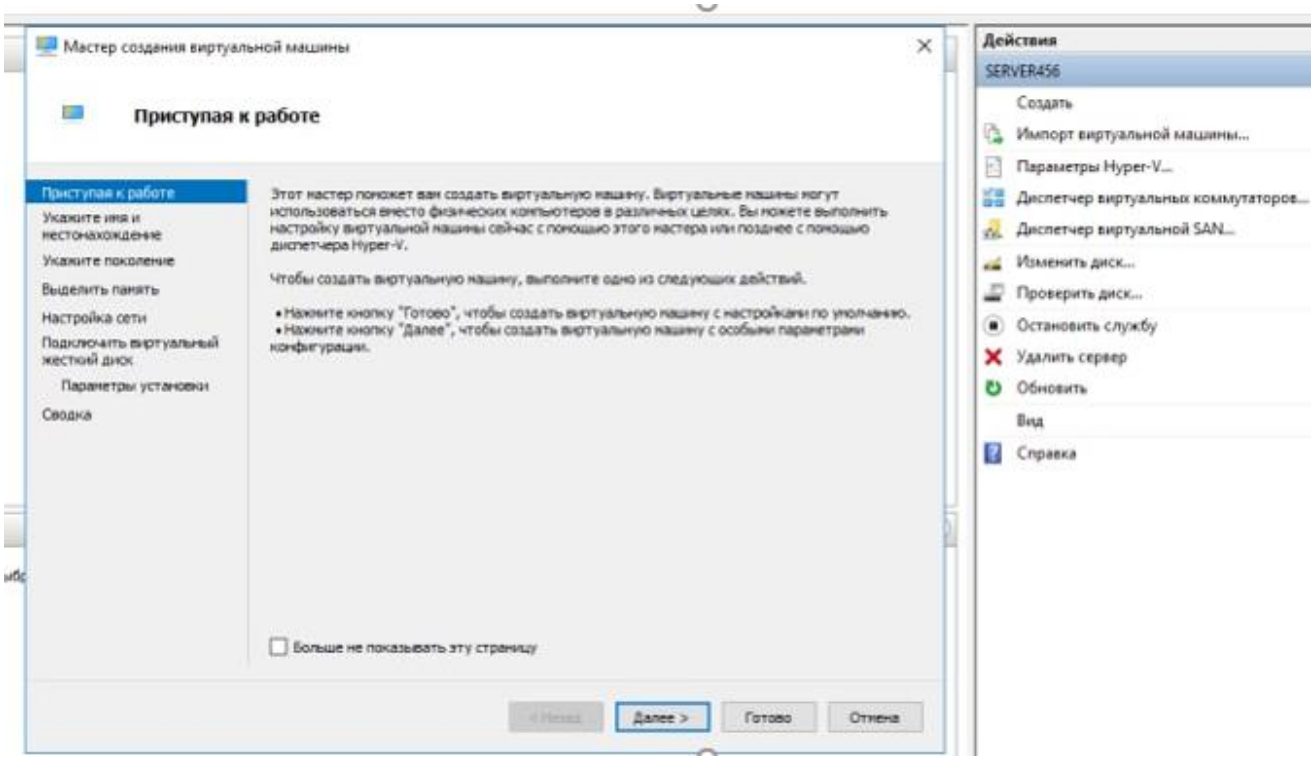


Рисунок 2.31 – Початок створення віртуалізації

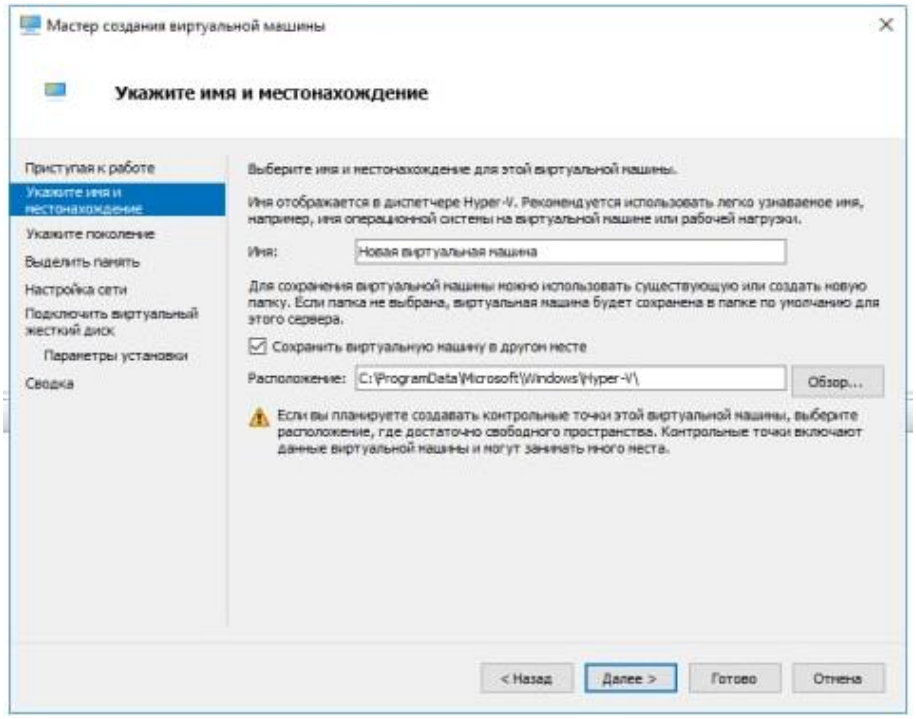


Рисунок 2.32 – Використання контрольних точок

Тепер регулювання параметрами які можна кастомізувати під потреби операційної системи

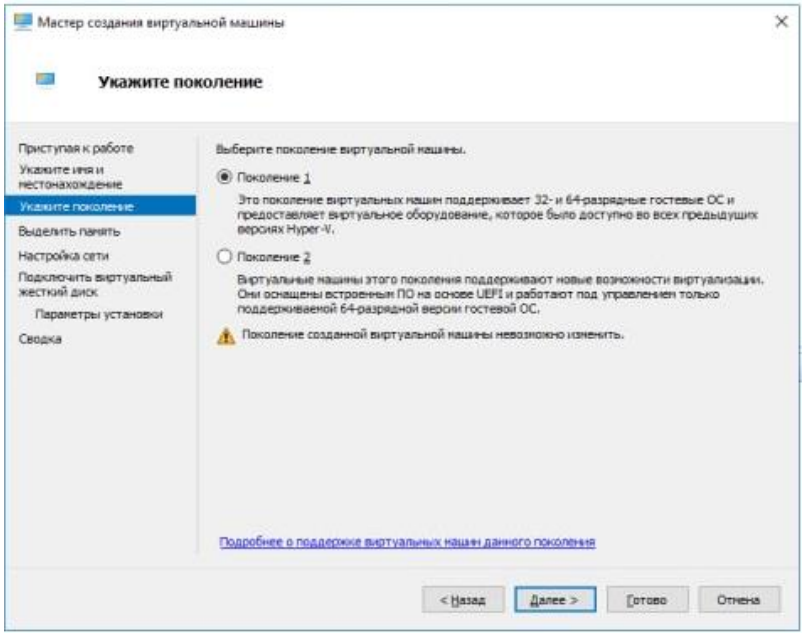


Рисунок 2.33 – Вибір покоління для ОС

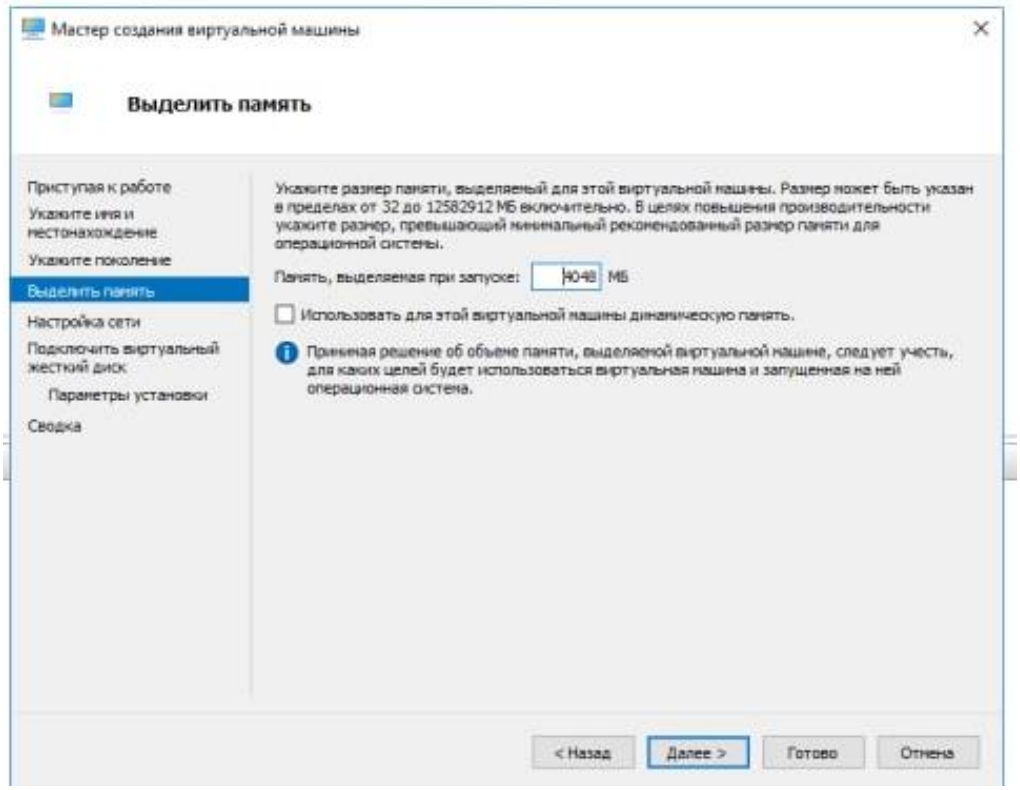


Рисунок 2.34 – Виділення пам'яті для ОС

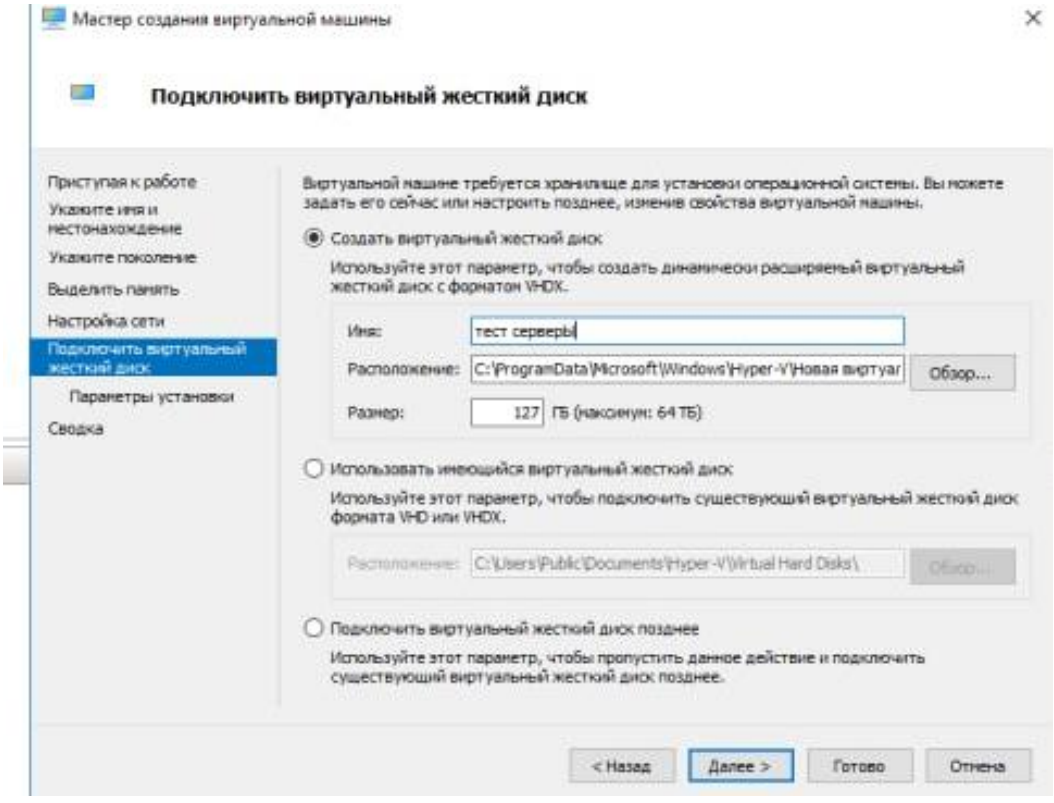


Рисунок 2.35 – Створення віртуального диску та вибір розташування

2.6 Налаштування Rds для Windows Server

Після встановлення віддалених робочих столів необхідно налаштувати та активувати ліцензію. Це особливість Windows Server, яка дозволяє користуватися віддаленим робочим столом кільком користувачам одночасно. У звичайній операційній системі за віддаленим робочим столом до пристрою може під'єднатися лише один користувач, тобто якщо перший користувач зайде на один обліковий запис, тоді при вході другого користувача на інший обліковий запис, з'єднання з першим сеансом буде закінчено. Операційні системи Windows Server розраховані на масову роботу незалежно від кількості користувачів та пристроїв.

Ліцензування віддалених робочих столів RDL (Remote Desktop Licensing) - дозволяє використовувати 2 типи ліцензії: на пристрій та на користувача. Спочатку після встановлення віддаленого робочого столу вам не потрібна ліцензія для використання, видається термін 120 днів для пробного періоду, після якого можливість використання RDS зникає до покупки ліцензії [10].

Відкриваємо диспетчер ліцензування віддалених робочих столів, він знаходиться в диспетчері серверів=> Засоби =>RDS.

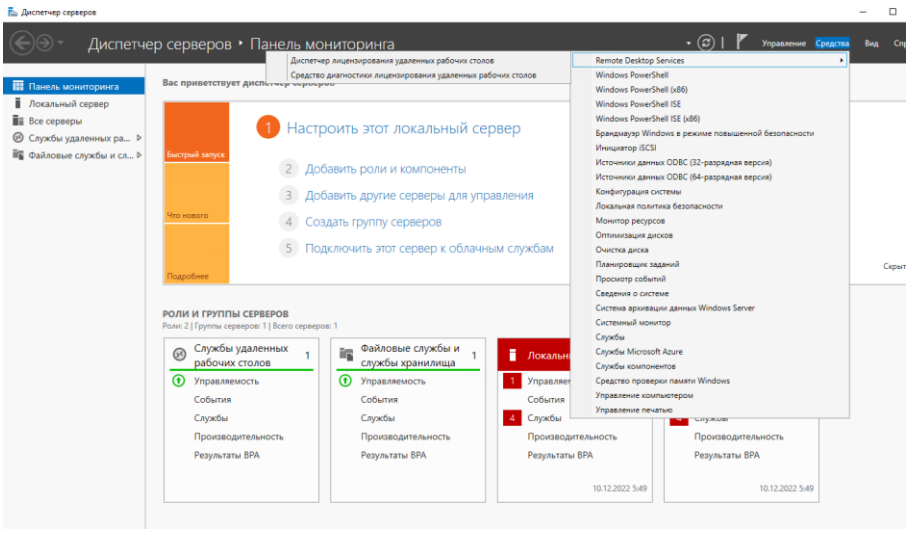


Рисунок 2.36 – Пошук диспетчера віддалених робочих столів

Натискаємо правою кнопкою миші на ім’я серверу та запускаємо активацію.

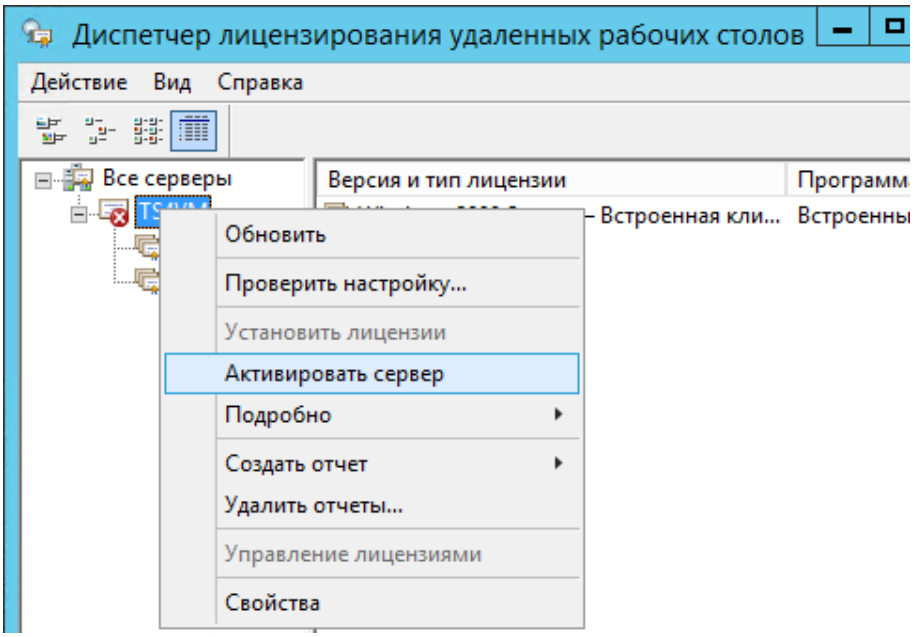


Рисунок 2.37 – Активація ліцензування

Для активації перш за все необхідно зареєструватися вказати на кого поширюється ліцензія та організацію яка буде її використовувати.

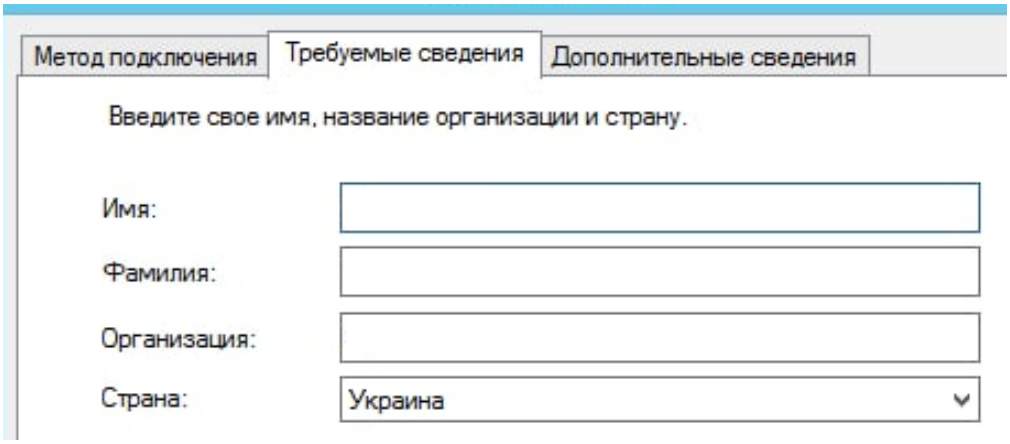


Рисунок 2.38 – Контактні дані

Після вказівки даних вам буде видано код операції для продовження активації. Його потрібно ввести через сайт для видачі коду ліцензування, який вказаний нижче полем.

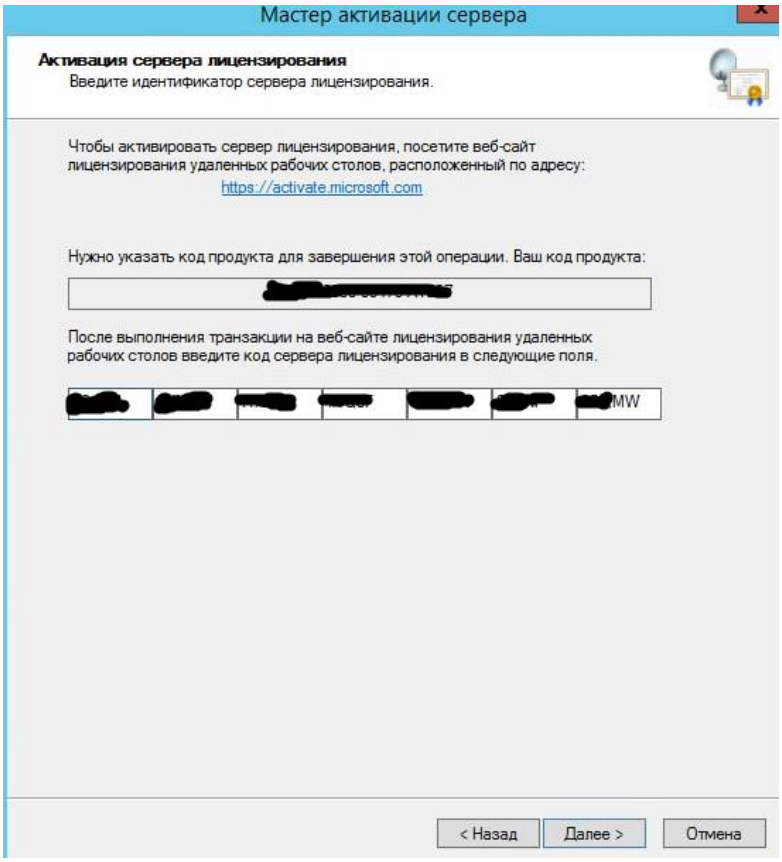


Рисунок 2.39 – Код сервера ліцензування

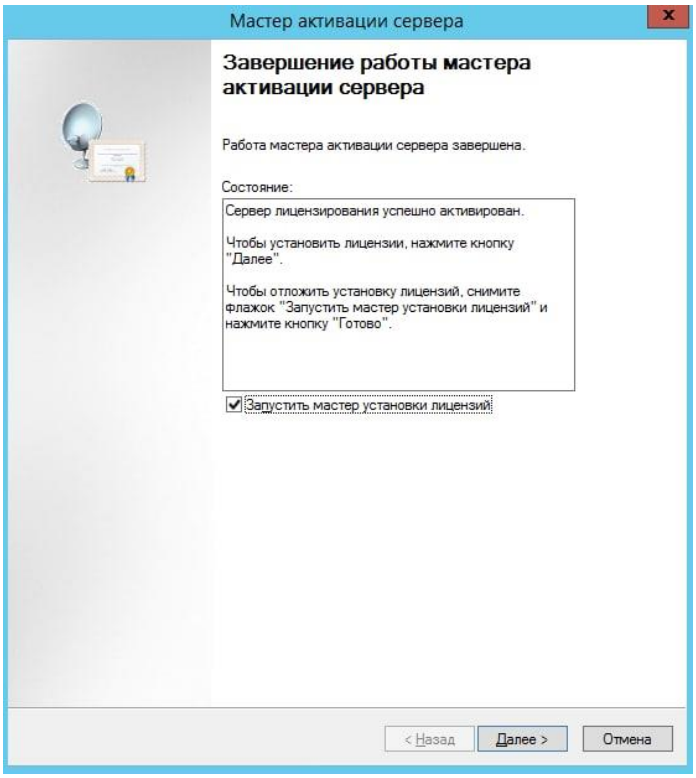


Рисунок 2.40 – Завершення активації

Тепер переходимо до ліцензій їх всього два типи: на пристрій (Per Device CAL) та користувача (Per User CAL). PDC ліцензія видається пристрою, який підключається кілька разів, але у цього є свій мінус. Якщо у вас мала кількість ліцензій, наприклад 15, то під'єднатися можуть лише 15 пристроїв яким видана постійна ліцензія. Тобто з іншого пристрою при нестачі кількості ліцензій, ви не зможете зайти на сервер за допомогою підключення RDS. Використання ліцензії на користувача дозволяє підключатися з будь-якої кількості пристроїв, але сама ліцензія прив'язана до облікового запису. Такий варіант варіативніший і практичніший, тому він поширений [10].

Вводимо наш код ліцензування, та вибираємо тип ліцензії та угоду, в такому випадку це ліцензія на користувачів, та угода Enterprise. Далі вводимо код пакета ліцензійних ключів.

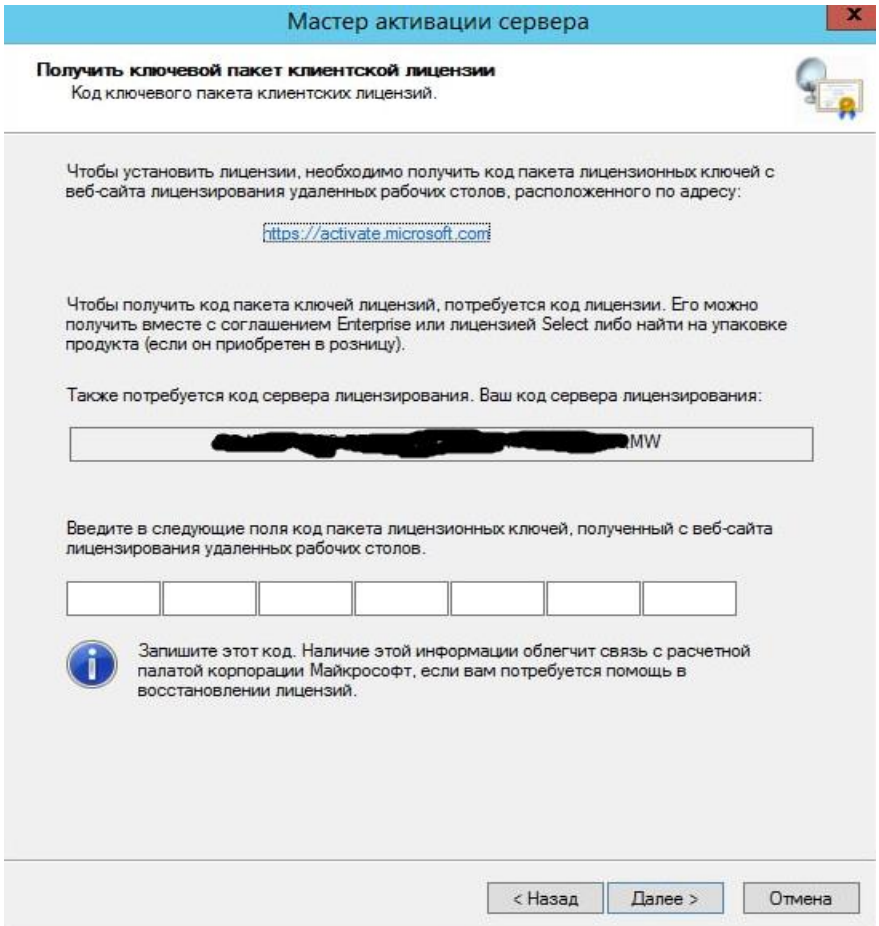


Рисунок 2.41 – Код пакета ліцензійних ключів

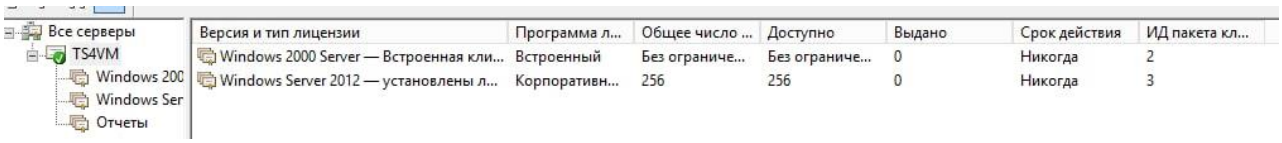


Рисунок 2.42 – Активація успішна

Заходимо у засіб діагностики ліцензування робочих столів, ця програма перевіряє підключення RDS та виводить інформацію про ліцензію.

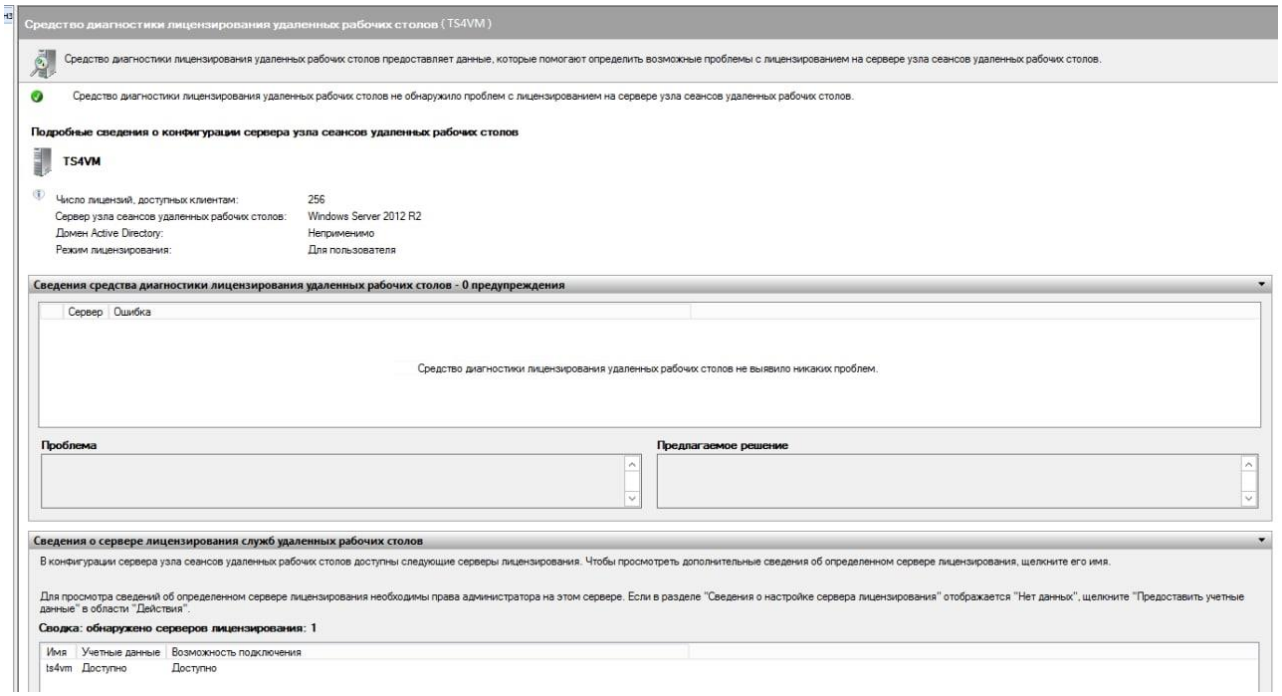


Рисунок 2.43 – Результат перевірки підключення RDS

3 ВИКОРИСТАННЯ МЕРЕЖІ РОУТЕРІВ MICROTIK ДЛЯ НАЛАШТУВАННЯ ВІДДАЛЕНОГО ДОСТУПУ

У роботі використовуються роутери фірми Mikrotik. Основна перевага – це власна операційна система RouterOS, яка дозволяє налаштовувати пристрої в залежності від вимог. Для початку буде зроблено базове налаштування обох роутерів, потім відкриття певних портів для забезпечення віддаленого підключення.

В інтерфейсі RouterOS є два режими налаштувань Quick set (Швидкий набір) WebFig (повноцінна версія). Швидкий набір дозволяє ввести всю необхідну інформацію для роботи пристрою. Повноцінна версія дозволяє налаштовувати максимально точно кожен крок.

Для початкового налаштування потрібно увімкнути роутер та приєднатися до внутрішньої мережі пристрою. З'єднання можна зробити через браузер або через спеціальну програму Winbox. Потім необхідно ввести IP-адресу 192.168.88.1 - це базова адреса підключення до автентифікації користувача. Як і у всіх роутерах ім'я користувача admin пароля немає.

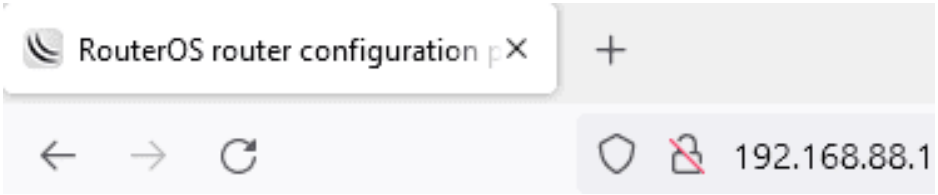


Рисунок 3.1 – Вид отримання IP-адресу

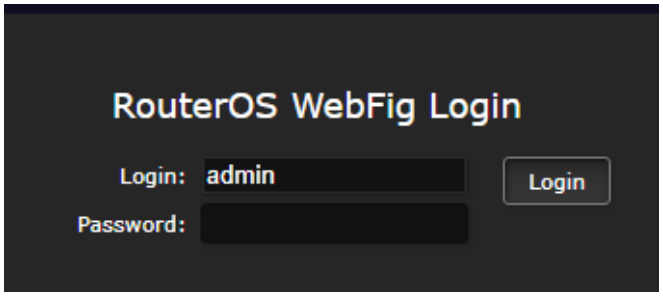


Рисунок 3.2 – Проведення автентифікації

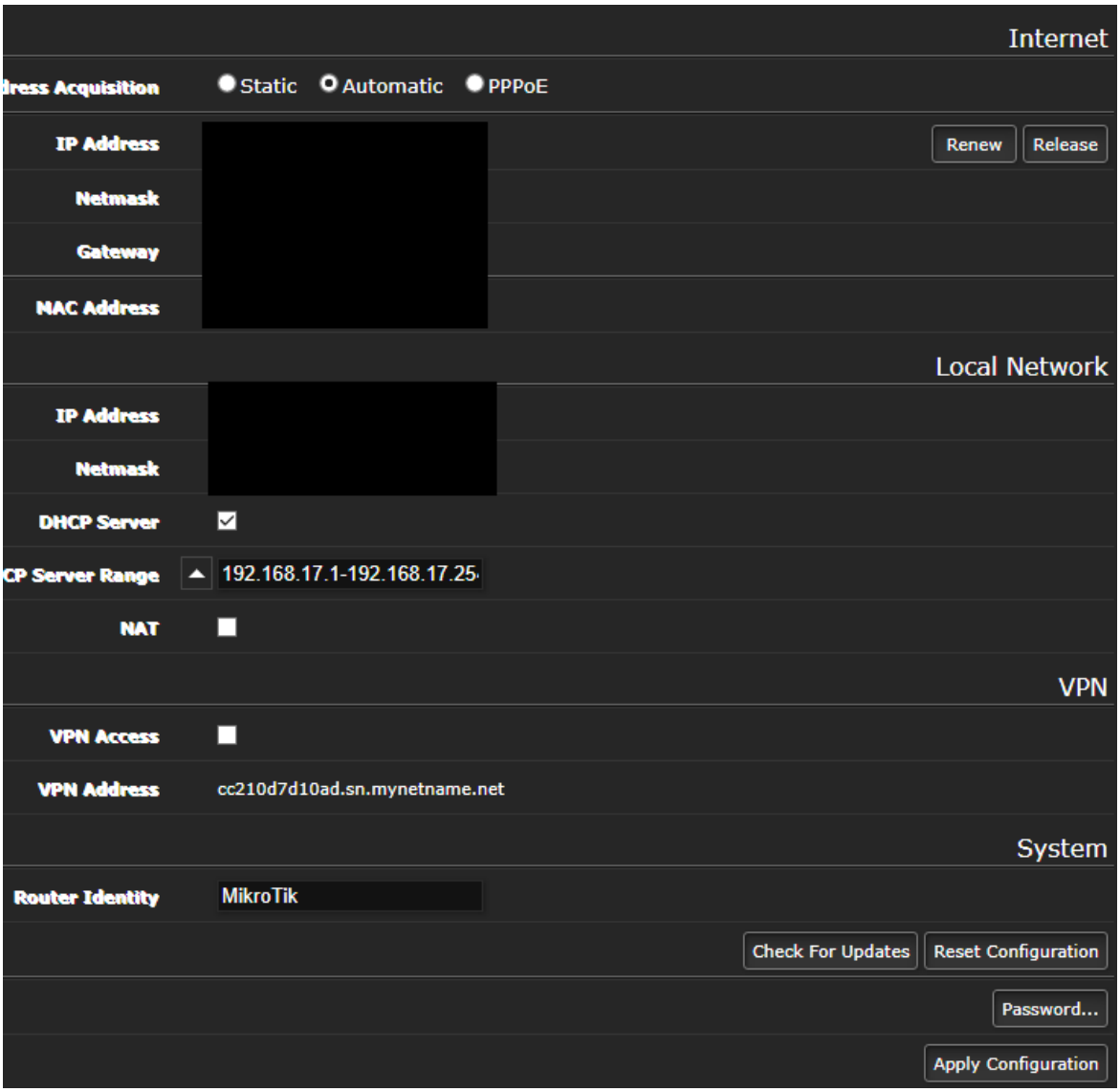


Рисунок 3.3 – Інтерфейс Quick Set

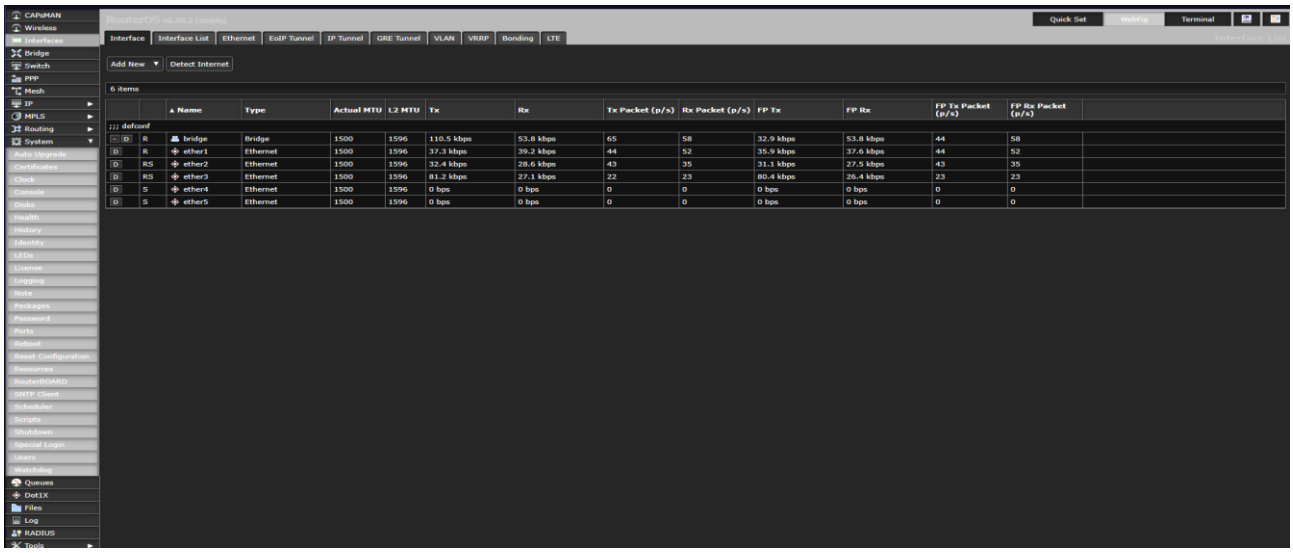


Рисунок 3.4 – Вид Інтерфейсу WebFig

Для забезпечення безпеки змінимо пароль роутера. Відкриваємо меню Quick Set та вибираємо Password, вводимо новий пароль з підтвердженням, нажимаємо Apply=>Ok .

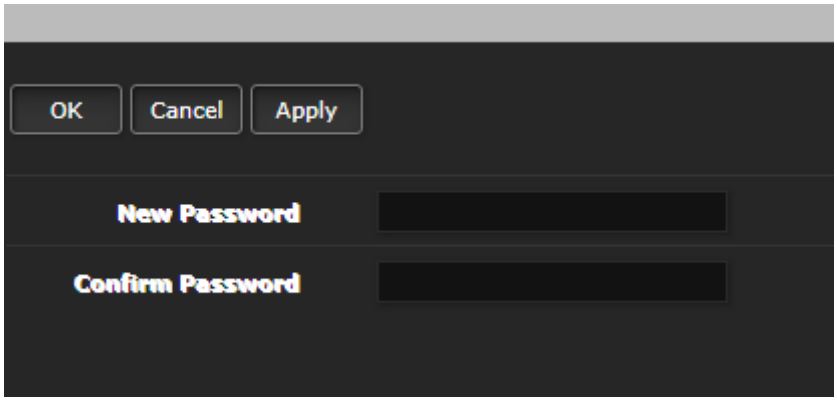


Рисунок 3.5– Quick Set зміна паролю

Для зміни паролю у WebFig потрібно відкрити System Users та вибрати необхідного, також можливо змінити права доступу, відключити, або додати користувача.

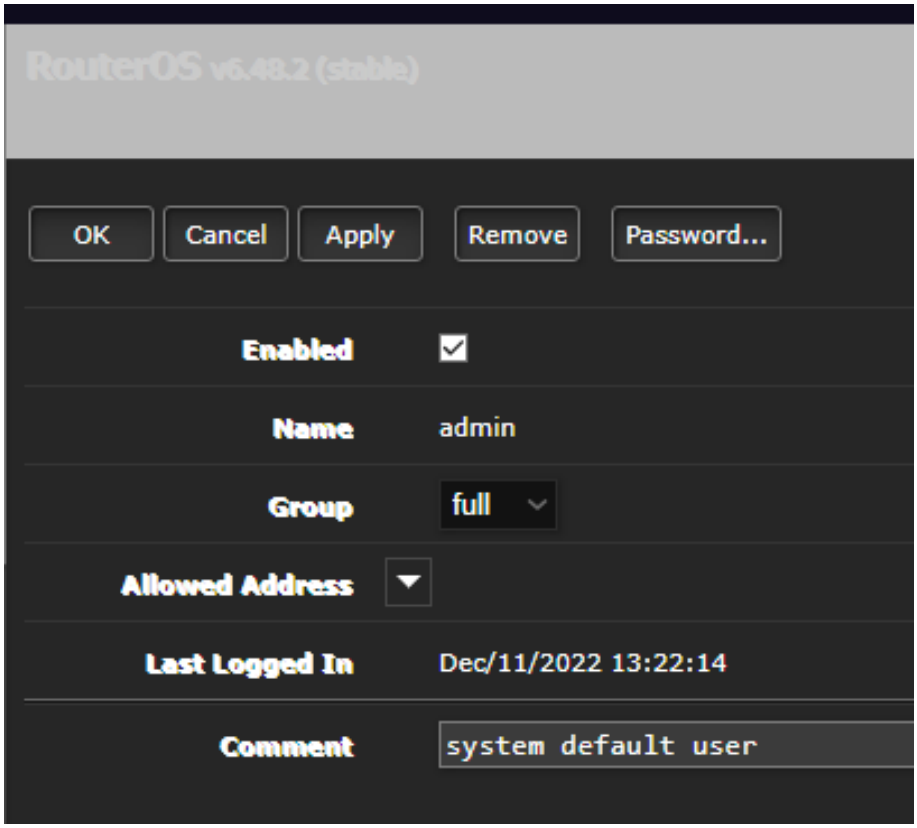


Рисунок 3.6 – WebFig зміна паролю та доступу

3.1 Налаштування роутерів для внутрішньої та зовнішньої мережі

Використовуємо конфігурацію Quick Set для налаштування зовнішньої мережі. Щоб використовувати віддалене підключення за допомогою програми РДП, нам необхідний статичний інтернет. Статичний інтернет це окрема послуга провайдера який видає вам IP-адресу в оренду, цю адресу ніхто не може використовувати крім арендатора [11]. Тому такі адреси необхідні підключення віддаленого робочого стола. Тоді як динамічна адреса постійно змінюється при відключенні пристрою. У першій вкладці ми налаштовуємо зовнішню мережу, прописуємо статичну адресу, маску мережі та мережевий шлюз.

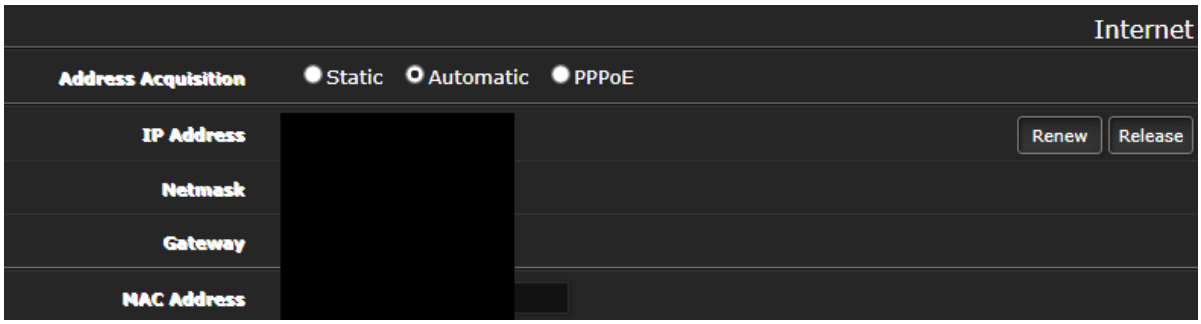


Рисунок 3.7 – Налаштування зовнішньої мережі першого роутера

Далі налаштуємо нашу внутрішню мережу першого роутера, за допомогою якої ми налаштуємо другий роутер.

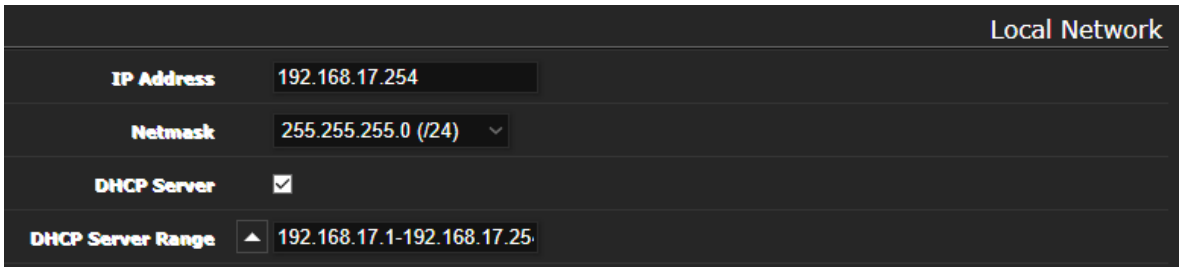


Рисунок 3.8 – Налаштування внутрішньої мережі першого роутера

Тепер зайдемо в налаштування другого роутера і вкажемо зовнішній і внутрішній адресу, до якого будуть переадресовуватися наші запити на підключення віддаленого доступу.

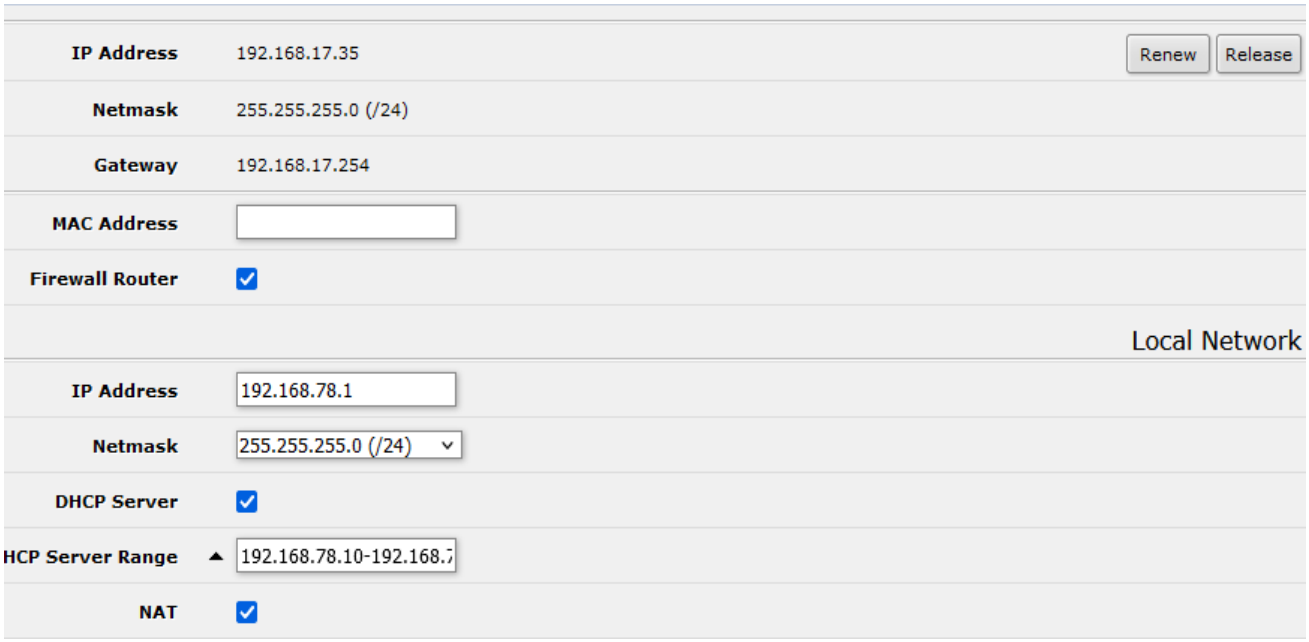


Рисунок 3.9 – Налаштування зовнішньої і внутрішньої адреси другого роутеру

3.2 Створення ім'я хоста для зовнішнього підключення

Використовуємо нашу статичну IP-адресу, щоб вказати hostname для підключення. Hostname завжди буде унікальним, це робиться для ідентифікації сервера, тому що за великої кількості серверів можна заплутатися. Також необхідно для виконання звернення до сервера на ім'я (віддалений доступ, авторизація на сервері, виконання віддалених команд). Для доступу до сервера на ім'я необхідно щоб це ім'я перетворювалося на IP-адресу з боку адресанта. Працює це якщо локальний DNS сервер адресанта перетворює hostname адресата. Використовуємо сайт noip.com. Для цього потрібно зареєструватися на сайті, потрібно мати електрона пошту та задати пароль.

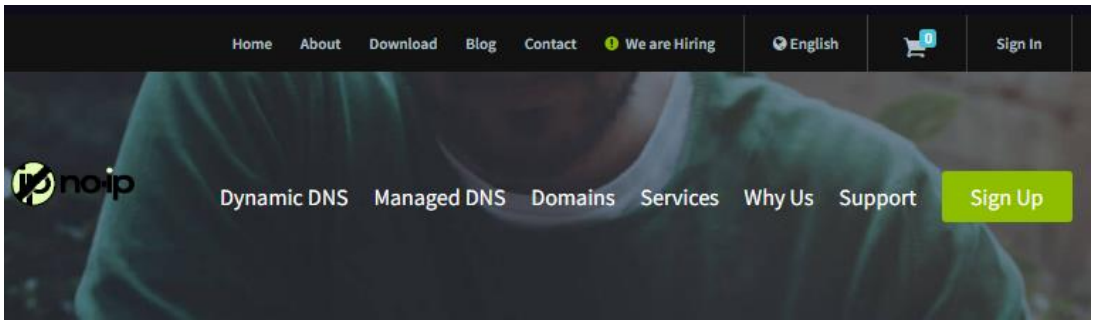


Рисунок 3.10 – Сайт noip.com

Після реєстрації на сайті, натискаємо створити hostname. З'являється інтерфейс де ми вказуємо свої дані, вибираємо домен і тип запису DNS Host(A) для адреси IPv4.

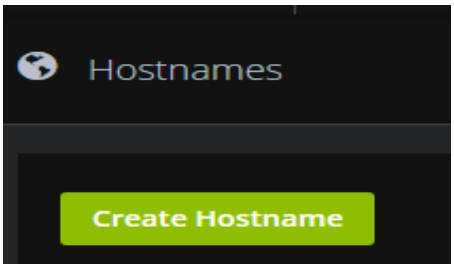


Рисунок 3.11 – Створення hostname

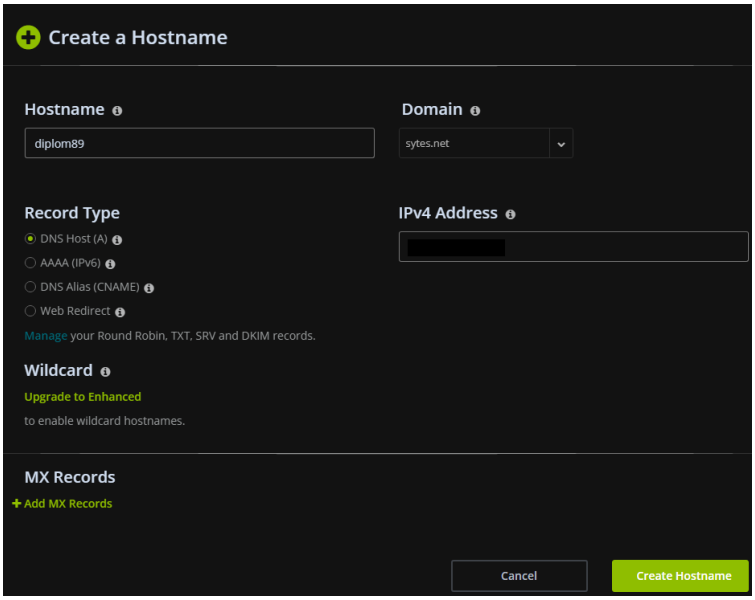


Рисунок 3.12 – Налаштування hostname

3.3 Налаштування зовнішніх та внутрішніх портів

Для надання віддаленого доступу до сервера необхідно вказати певні порти маршрутизатора. У зовнішній мережі всі пристрої мають ту саму IP-адресу, але перенаправлення до пристроїв відбувається завдяки внутрішнім і зовнішнім портам. У цій роботі використовується прокидання портів на системі Mikrotik RouterOS. Для початку надається топологія мережі, потім прокидання портів. Використовується програма Cisco Packet Tracer Student.

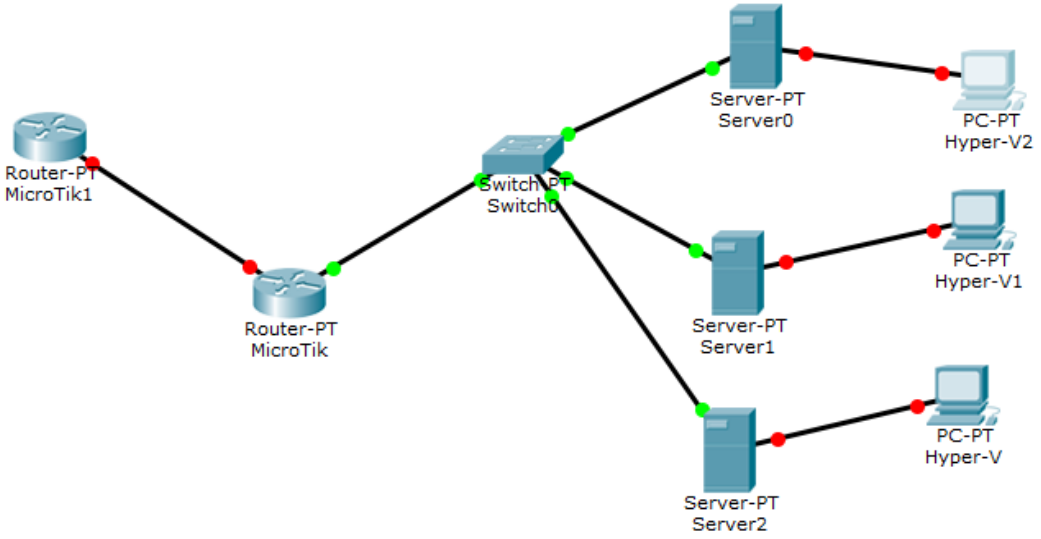


Рисунок 3.13 – Топологія мережі

NAT - це технологія, задача якої перетворити IP-адреси в зовнішні та навпаки. Перетворення NAT допомагають сховати топологію внутрішньої мережі від зовнішніх користувачів, також ускладнює несанкціонований доступ до ресурсів мережі. Організуємо NAT за допомогою IP => Firewall, створюємо правило. Завдяки функції NAT відкриваються порти, котрі потім використовуються для пересилання вхідних даних користувачів.

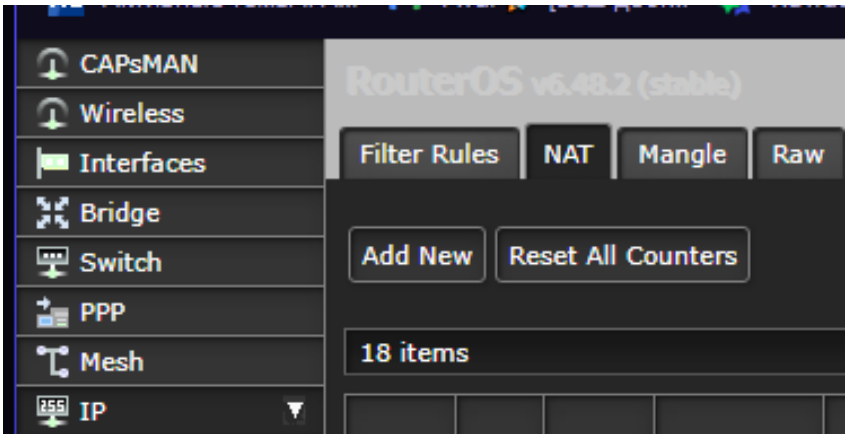


Рисунок 3.14 – Вид NAT-перетворення

Також потрібно налаштувати локальну мережу сервера та віртуальної машини Hyper-V для того, щоб використовувати віддалене підключення і визначати до якого пристрою йде підключення. Спочатку відкриємо параметри сервера виберемо мережу та інтернет, центр управління мережами та загальним доступом. Після цього заходимо на підключення інтернету => властивості => TCP/IPv4. Вказуємо основний шлюз, IP-адреса не зарезервований і маску, і виставляємо DNS-сервер [9].

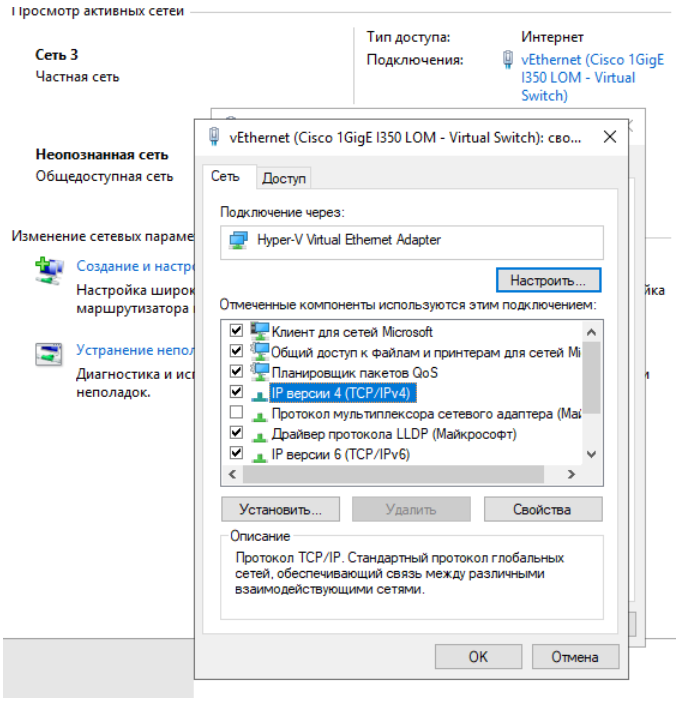


Рисунок 3.15– Вибір налаштування локальної мережі

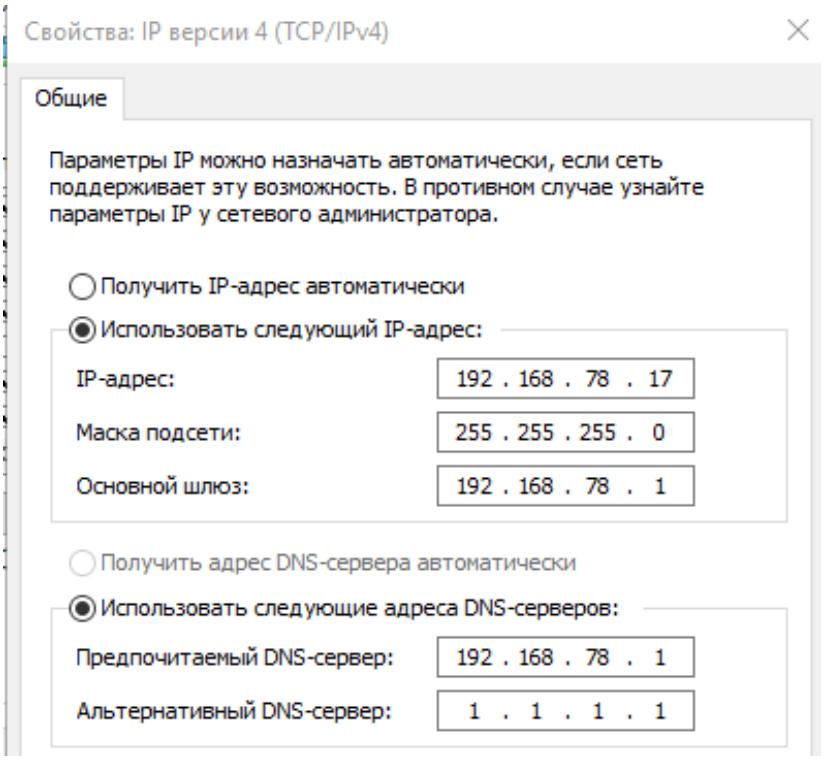


Рисунок 3.16– Налаштування локальної мережі серверу

Повторюємо такі ж дії, але у віртуальній машині.

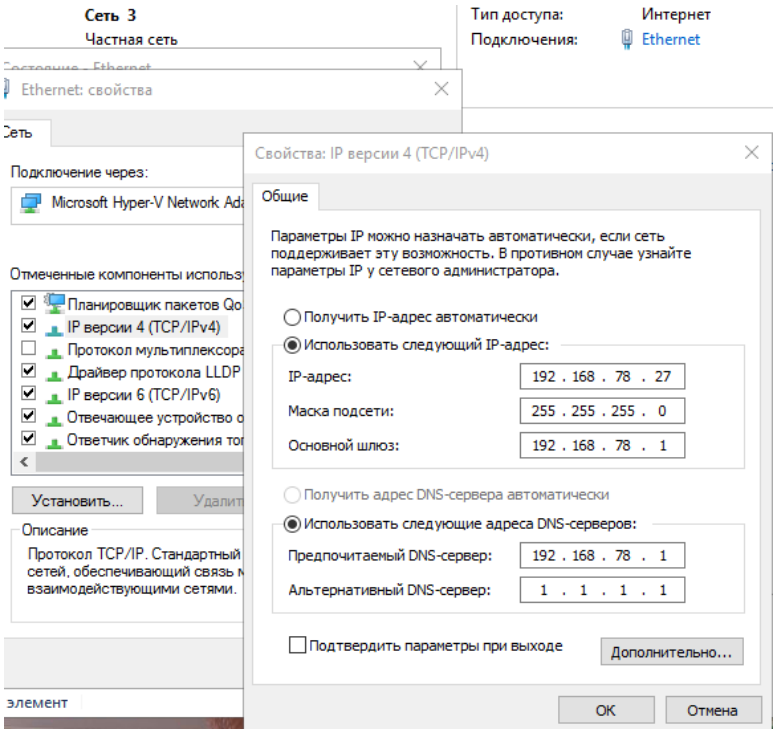


Рисунок 3.17– Налаштування локальної мережі у віртуальній машині

У Mikrotik є альтернатива діям, зазначеним вище. Якщо залишити автоматичне отримання IP-адреса в системі, то при перезавантаженні пристрою адреса може змінитися, для цього його зазвичай прописують як було зазначено вище [10]. Але Mikrotik дозволяє у своїй системі RouterOS запам'ятати вказаний автоматичний IP-адресу. Таким чином адреса теж буде закріплена за пристроєм, але вже в системі роутера. Для цього потрібно перейти до WebFig IP => DHCP Server => Leases. Ця функція корисна ще тим, що може запам'ятати різні пристрої, підключені до цієї мережі, наприклад роутери або андроїд приставку. Ця функція зазвичай не використовується, але для різноманітності может бути застосована на багатьох пристроях.

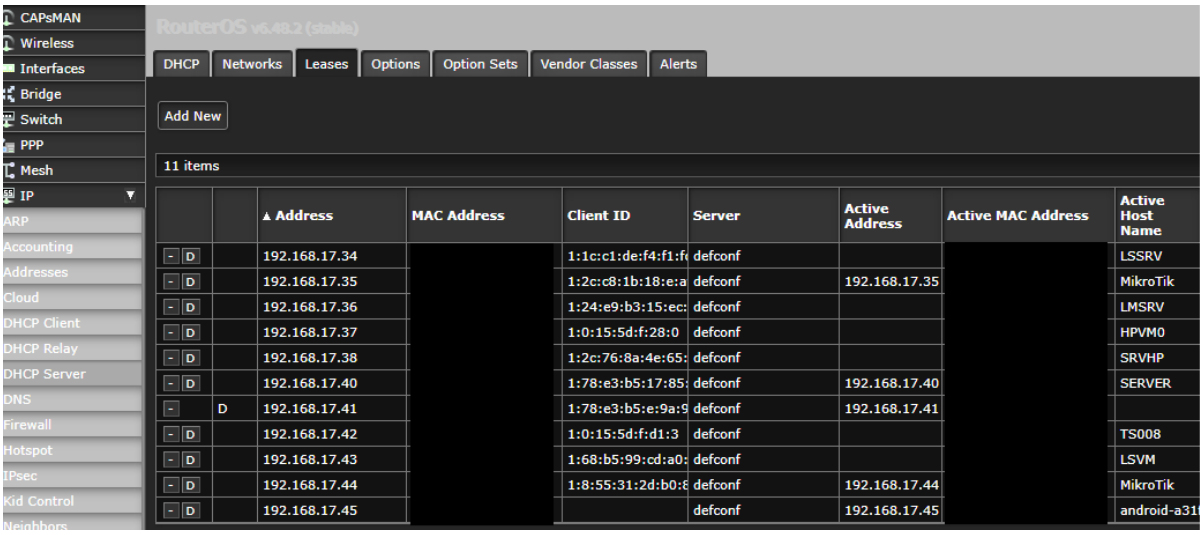


Рисунок 3.18– Використання Leases

У вікні інтерфейсу, що відкрилося, вибираємо напрямок потоку даних, в даному випадку це із зовнішньої мережі у внутрішню dstnat. Далі вказуємо протокол tcp і вказуємо Dst. Port номер зовнішнього порту маршрутизатора. Операція дозволить отримувати дані на порт і переадресовуватиме на внутрішній мережу. Далі вказуємо вхідний інтерфейс, наприклад ether1.

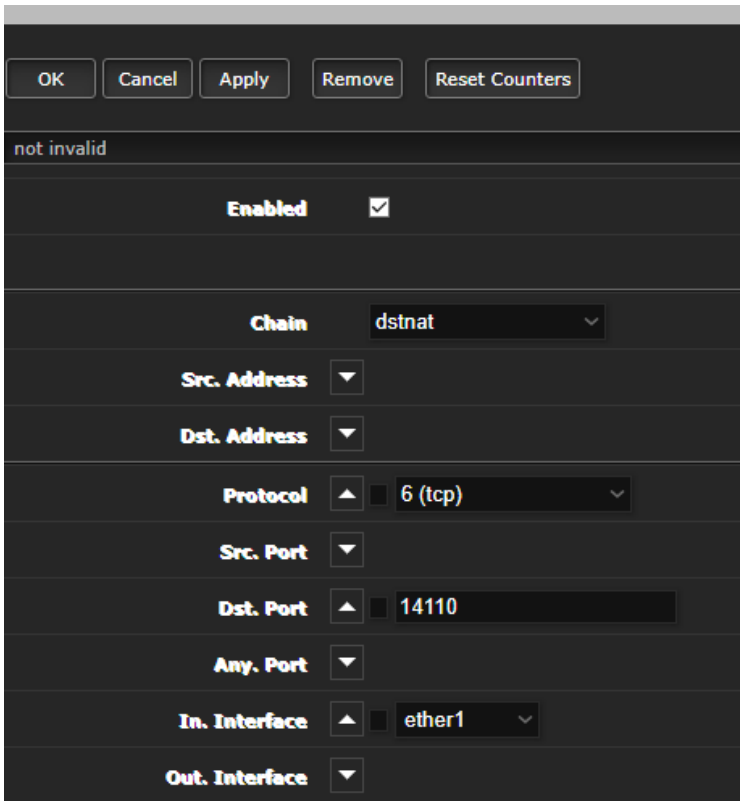


Рисунок 3.19– Створення зовнішнього порту

Нижче в інтерфейсі є Action, в якому ми прописуємо подальші дії. Такі як перенаправлення даних із зовнішньої мережі на локальну dst-nat. Прописуємо IP-адресу другого роутера і порт яким передаються дані.

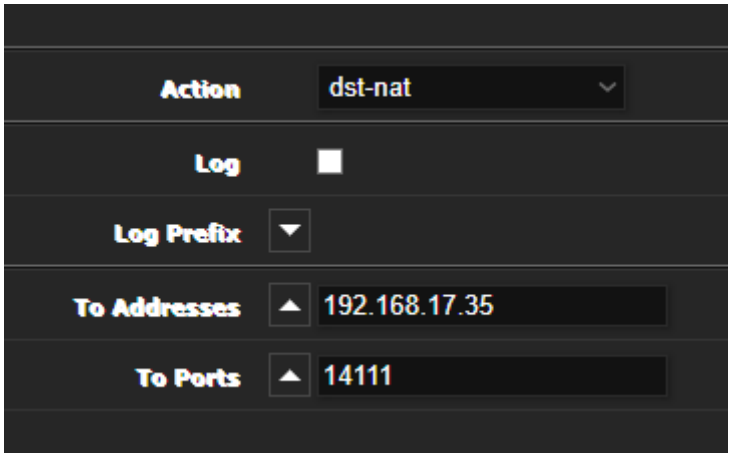


Рисунок 3.20– Переадресація даних

Тепер переходимо до другого роутера прописуємо такі ж налаштування, за винятком порту. Необхідно вказати порт, який використовували у вкладці

Action. Таким чином йде перекидання даних з одного порту на інший що забезпечує безпеку якщо зовнішній порт виявлять та будуть використовувати брутфорс атаку.

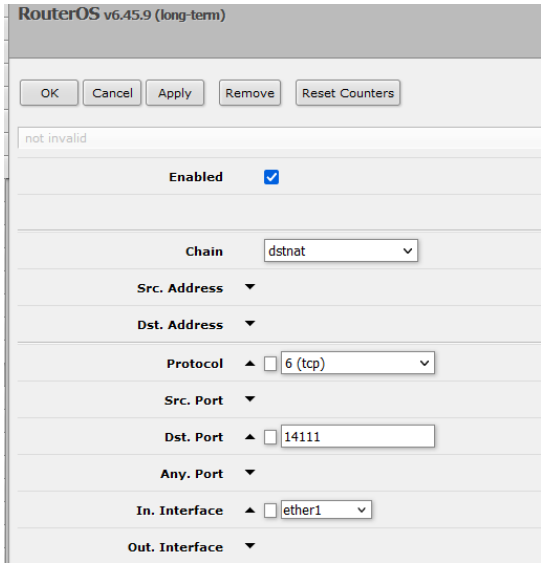


Рисунок 3.21– Створення зовнішнього порту локальної мережі другого роутера

Далі використовуємо Action, але тепер вказуємо локальний іп нашої віртуальної машини і порт який за замовчуванням 3389.

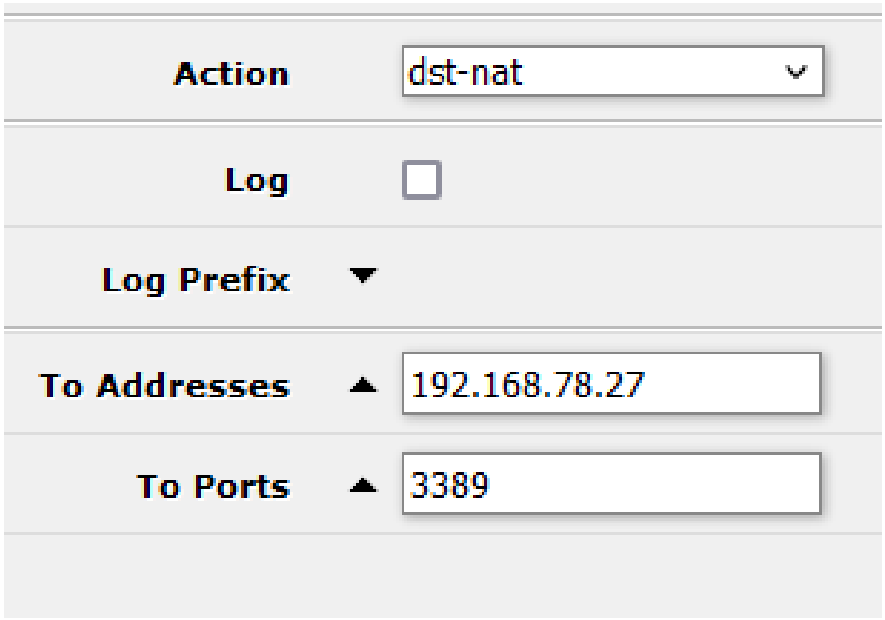


Рисунок 3.22– Остаточне завершення

4 АНАЛІЗ ТА ПОРІВНЯННЯ ПАРАМЕТРІВ БЕЗПЕКИ БАЗ ДАНИХ ТА СЕРВЕРІВ

В наш час використання баз даних стало буденністю, завдяки їм обробляти безліч даних за невеликий час стало реальністю. Але тепер постало питання збереження інформації, яка може бути продана, або використана зловмисниками з корисливою метою. Сервера є оптимальним варіантом для зберігання інформації: завдяки спеціальної архітектури комплектуючих, серверної операційної системи, програм для роботи з реляційними БД. Завдання цієї роботи знизити ризики до мінімуму, забезпечити захист та доступ до даних. На основі цього буде зроблено аналіз всіляких ризиків, які можуть статися при віддаленому доступі. Також буде розглянуто можливість архівації баз даних та збереження бекапів на інший пристрій або файлообмінник.

Весь обмін даних відбувається через віддалений доступ тому варто подбати про права користувачів та захист від брутфорс атак методом додавання підозрілих адресу у чорний список. Ця реалізація буде доступна завдяки RouterOS і точному настроюванню фаєрволу. Потім буде порівняння рекомендованого варіанта налаштування фаєрволу від Mikrotik, із запропонованим.

Останнім часом необхідність стабільної електромережі зросла, тому необхідно забезпечити зниження ризиків втрати даних через різке відключення живлення.

4.1 Параметри зберігання баз даних

Використання баз даних організаціями стало необхідністю зростання інформаційних технологій, як така структура зберігання інформації змінювалася протягом самої історії. Тепер більша частина інформації зберігається на пристрої, а не на портативних носіях інформації, розвиток технологій дозволило працювати з величезною кількістю інформації, тому

необхідність у базах даних зросла. На жаль, також зріс попит на торгівлю інформацією, крадіжкою або навіть фальсифікацією. Тому необхідно забезпечити бази даних контролю доступу до інформації. Деякі бази не можуть створити окремих користувачів, тому використовують шифрування.

Найпоширеніші атаки на реляційні основи це використання SQL-коду. Цей процес заражає структуру БД і дозволяє поступово отримувати доступом до всієї інформації у базі. Такий тип загрози називають SQL ін'єкціями, вони бувають у числових параметрах та рядковому.

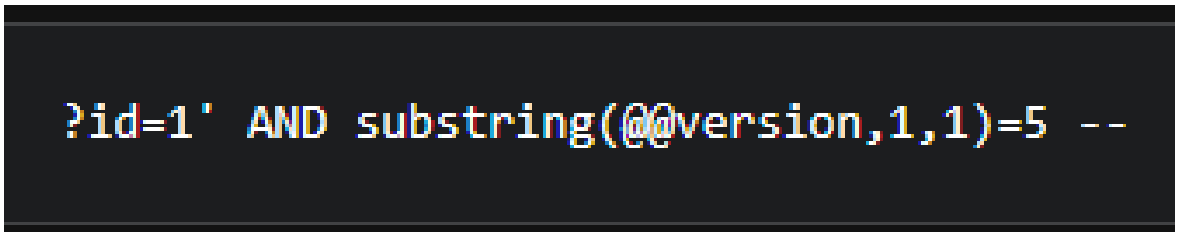


Рисунок 4.1– Використання ін'єкції

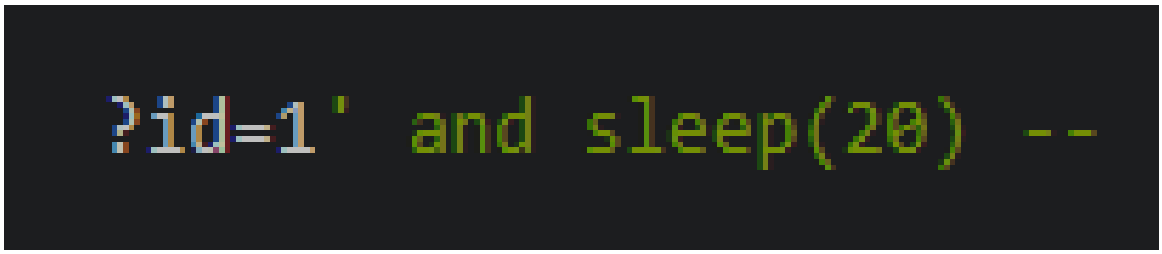


Рисунок 4.2– Приклад ін'єкції, яка викликає затримку відповіді бази даних

Однією із найчастіших прикладів уразливості є людський чинник. Причини завжди бувають різні, коли стосуються витоку інформації. Для зниження ймовірності допустити виток інформації використовується обмеження прав користувачів, зі зміною пароля через певний час. Таким чином мінімізується можлива шкода він користувачів.

Ще одна вразливість, яка зустрічається це вразливість резервних копій. Така помилка часто зустрічається якщо файлова база, а резервна копія

лежить десь у звичайній папці. У такому разі зловмиснику не важко вкрасти базу і проаналізувати її захист, а потім дістати необхідну інформацію.

Ознайомившись із цією інформацією було проаналізовано та зроблено висновок щодо забезпечення доступу та архівації БД. Далі будуть розглянуті приклади використання релятивних баз та стандартних файлових. Щоб уникнути витоку інформації, будуть використані різні методи в залежності від БД.

Виберемо приклад файл-серверної бази SQLite. У цьому випадку є невелика база, але SQLite не має можливості створювати користувачів і налаштовувати доступ до бази. Тому первним рішенням буде використання шифрування за допомогою SQLCipher.

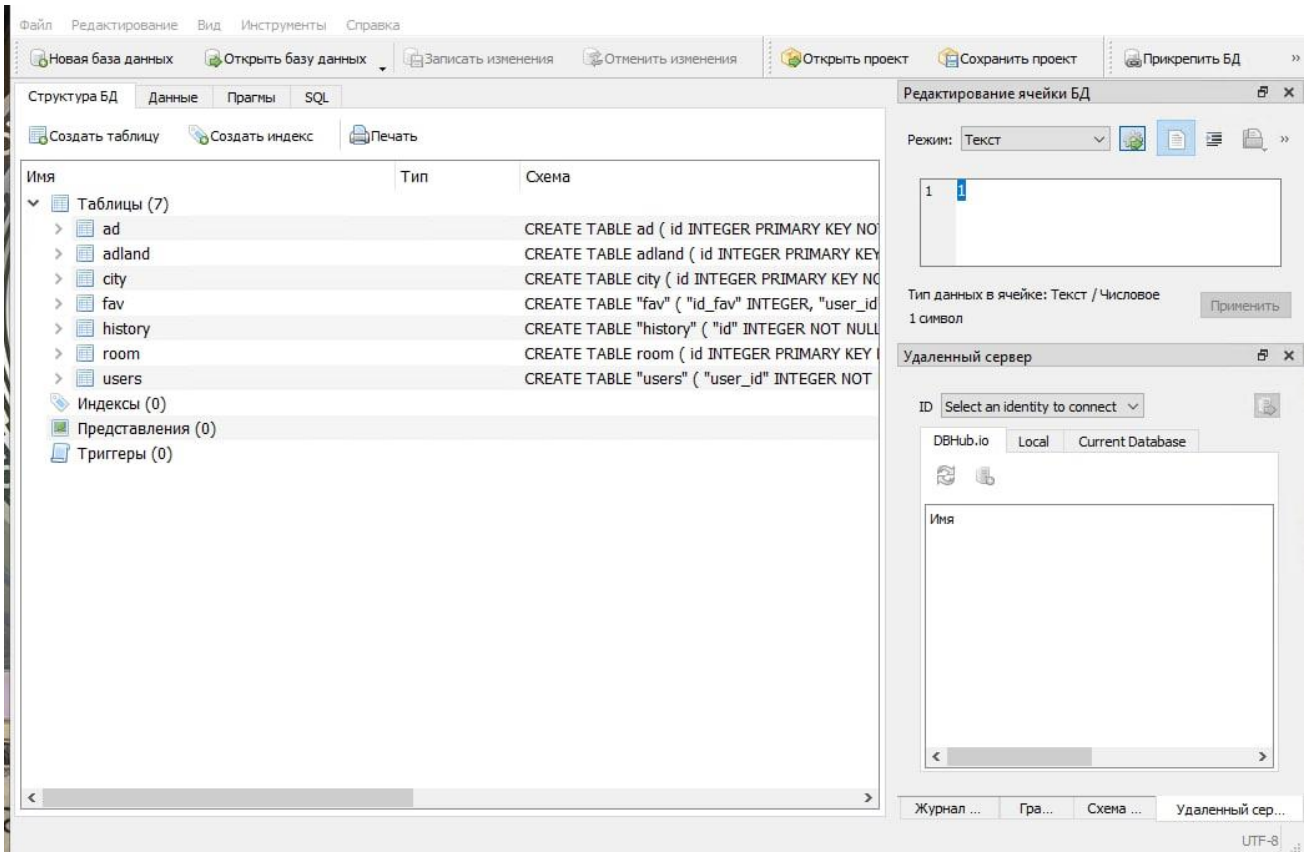


Рисунок 4.3– SQLite БД

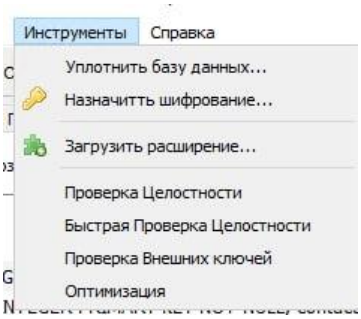


Рисунок 4.4– Шифрування

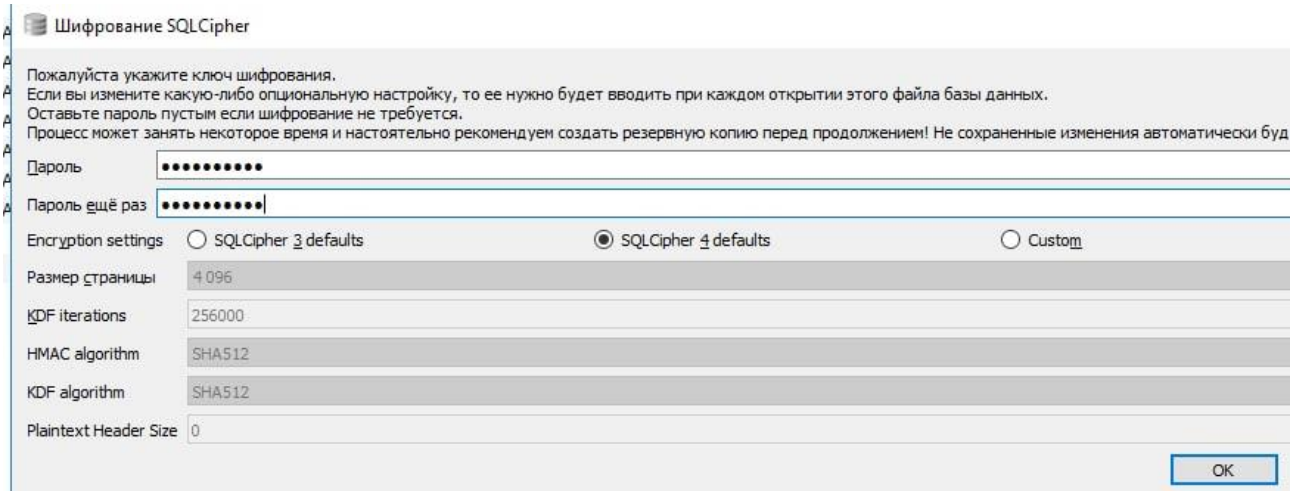


Рисунок 4.5– Вибір шифрування та вказівки параметрів

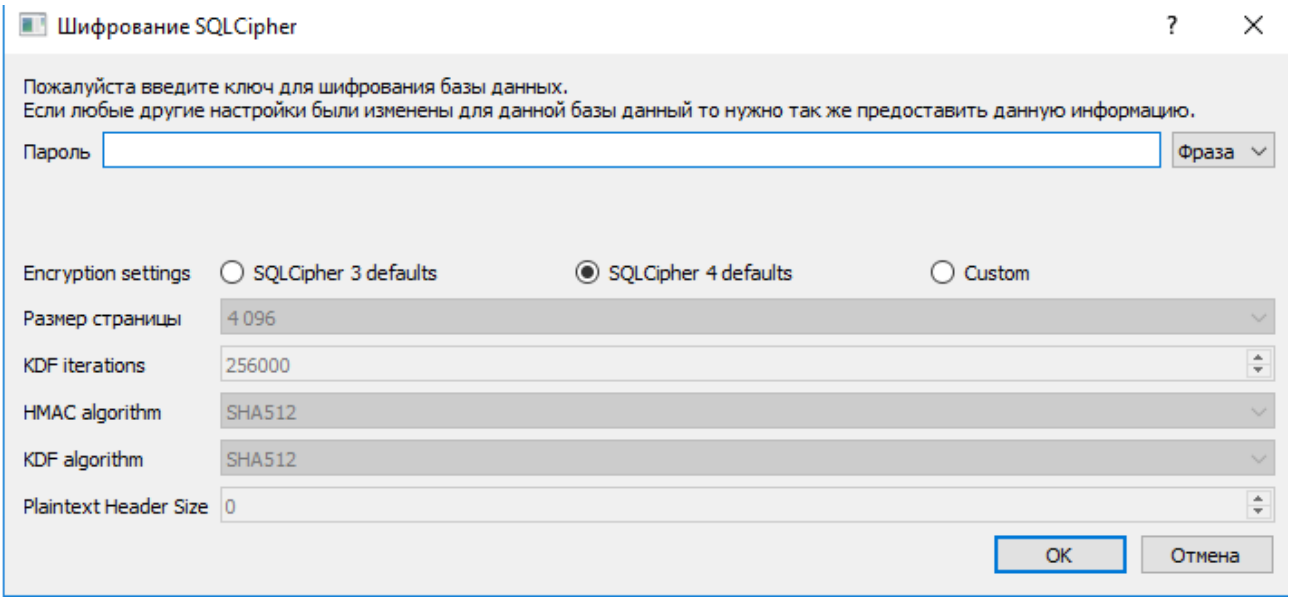


Рисунок 4.6– Перевірка паролю

Для збереження нашої бази, яка знаходиться у файлі, ми використовуємо права доступу адміністратора і приховуємо цей файл у папці з правами адміністратора, або використовуємо файлообмінник. Таким чином, ми можемо зберігати бекапи наших баз або самі бази даних. Також можна налаштувати архівацію за таймером.

Тепер використовуємо варіативнішу програму з базою даних 1С. Ця програма може зберігати свою БД у файловому варіанті та клієнт-серверному.

Файловий варіант пропонується за замовчуванням під час встановлення бази даних. Його недоліки: Частина файлу БД може бути заблокована для інших користувачів через зміни бази у відкритому доступі в провіднику. Приховати базу в спеціальну папку не вийде, тому що інші користувачі, які не мають доступу до цієї папки, не зможуть використовувати 1с. База легко повністю копіюється без зайвих засобів архівації та знімків. За підсумком файловий варіант 1С є небезпечним і рекомендується використовувати його за наявності Адміністратора сервера.

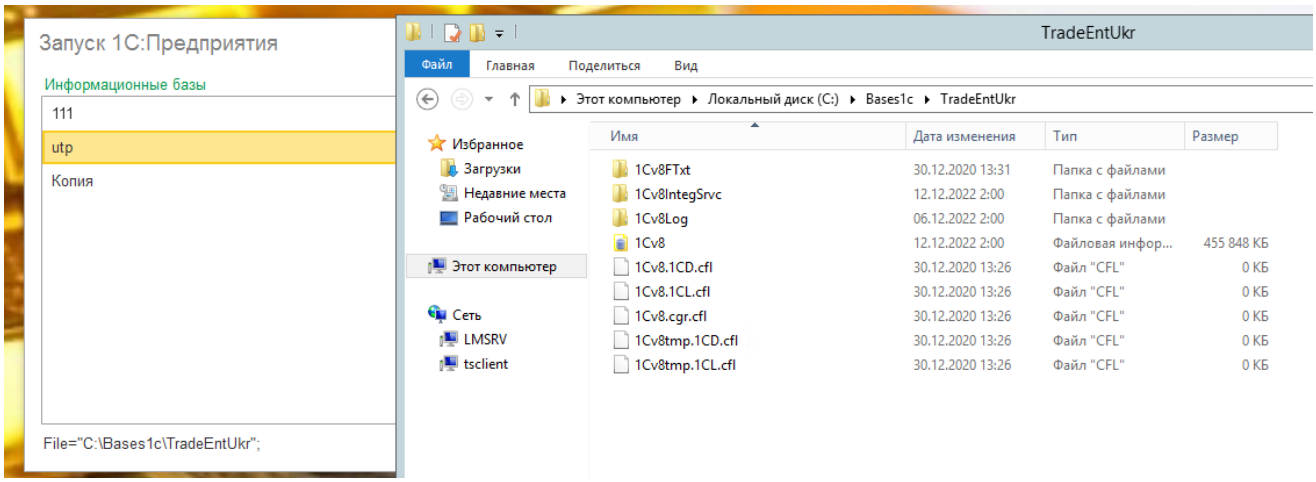


Рисунок 4.7– Приклад файлової 1С БД

Для бекапа передбачена функція розвантаження бази, вона знаходиться у конфігурації.

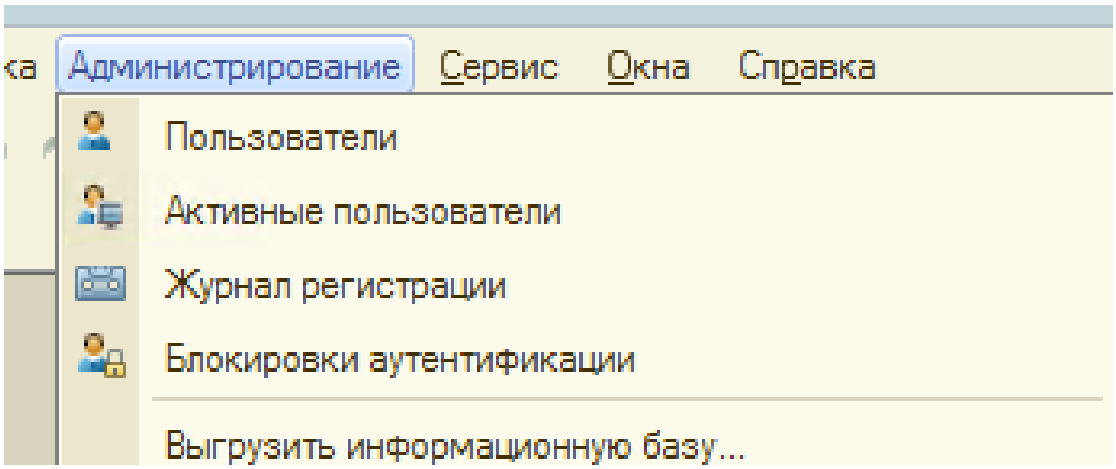


Рисунок 4.8– Бекап 1С

Але є програма яка автоматизує цей процес і називається вона Effector Saver. Можна поставити розклад виконання бекапа та вказати потрібну папку.

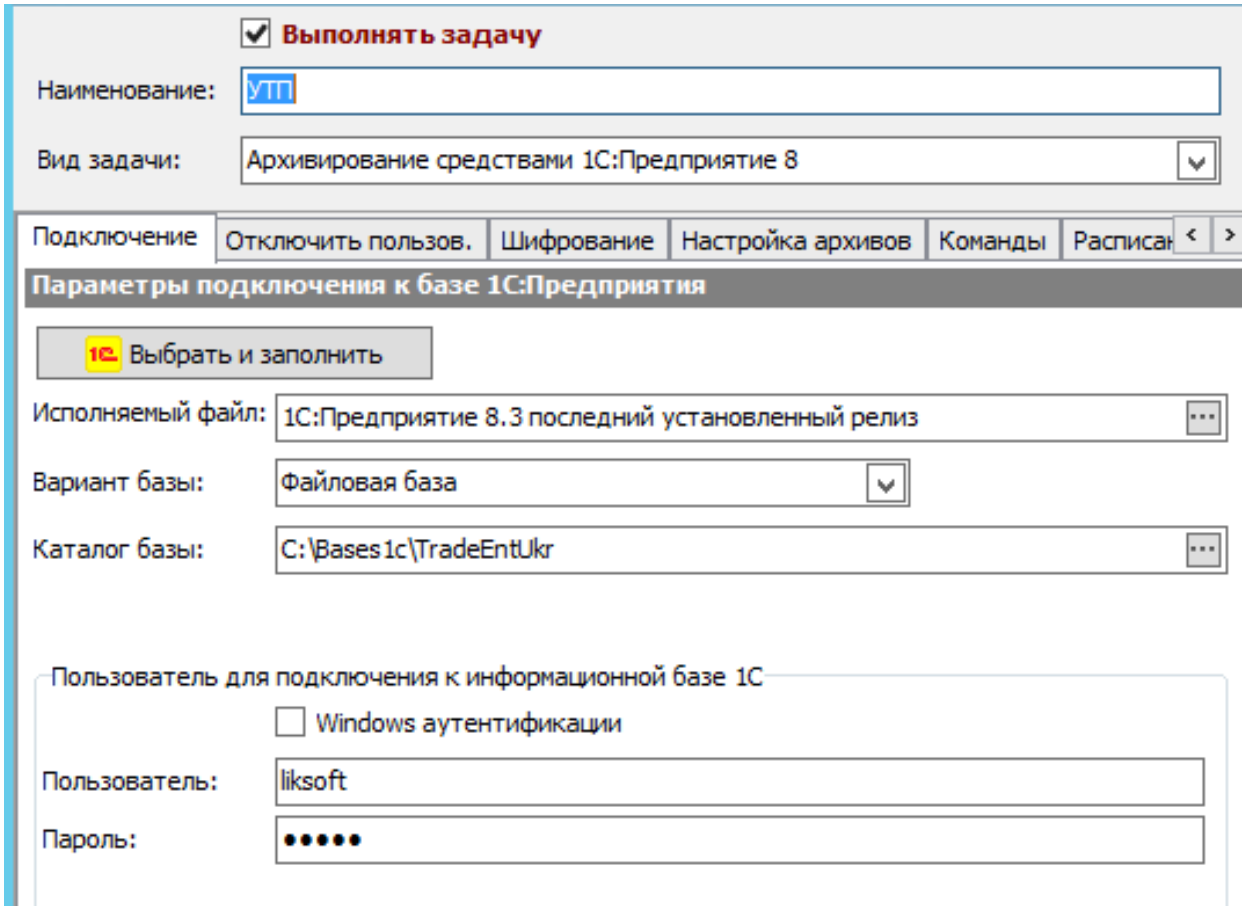


Рисунок 4.9– Інтерфейс програми

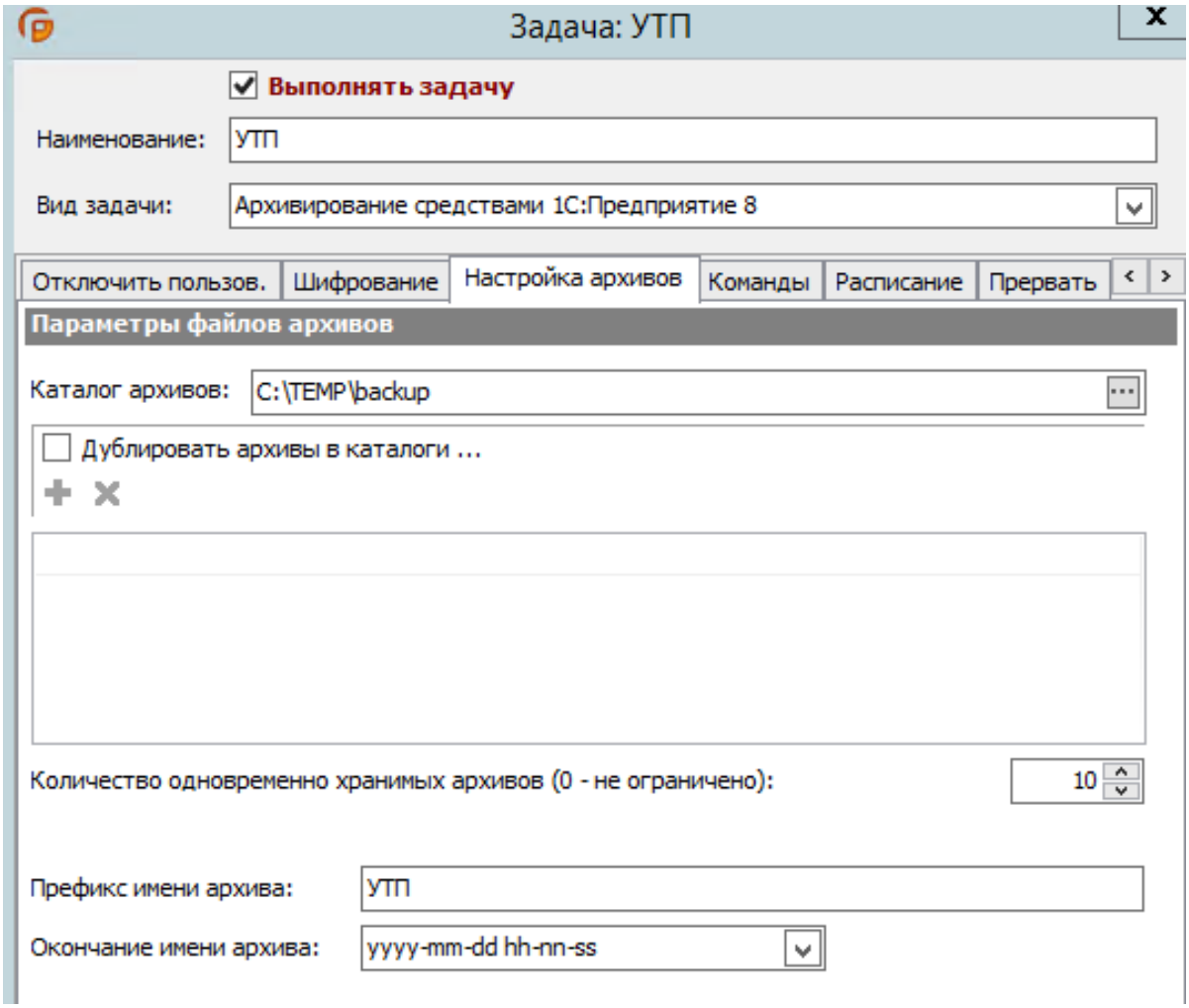


Рисунок 4.10– Налаштування архіву

Клієнт-серверний варіант дозволяє працювати користувачам без перешкод із базою даних. Робоча система розбивається на три частини: сервер БД, клієнтський додаток, кластер серверів 1С. Кластер розподіляє запити до потрібних файлів у БД, а клієнтський додаток це програма користувача, яка не використовує ресурси пристрою. Натомість усі ресурси використовує сервер, тому ресурсомісткі завдання ідеально підходять для такого варіанту. Отримати доступ до бази безпосередньо з файловим варіантом не вийде, тому що сама база має пароль і вимагає права доступу адміністратора в 1С. Також клієнтський додаток та БД можуть знаходитися на різних пристроях, що виключає ймовірність несанкціонований доступу. Як реляційна СУБД

використовувалася MS SQL Server, вона є найбільш оптимізованою і гнучкою під такі завдання.

У цьому варіанті програма 1С запущена на віртуальній машині, а сама БД знаходиться на сервері. Якщо допустити можливість зараження системи, сама база не постраждає, тому що користувачі працюватимуть через віртуальну машину. Таким чином, ми оптимізуємо роботу нашої бази завдяки виробничого СУБД MS SQL Server. Найбільшим недоліком є надмірне споживання оперативної пам'яті. У поточній ситуації 31 гігабайт оперативної пам'яті зайнято MS SQL Server.

Щоб використовувати СУБД, необхідно створити порожню базу в MS SQL Server. Спочатку відкриваємо програму адміністрування серверів 1С Підприємства, натискаємо на інформаційні бази створити. Після цього називаємо базу та ім'я, вказуємо як має називатися сервер баз даних для з'єднання з 1С, вибираємо тип СУБД. Також обов'язково потрібно ввести ім'я користувача MS SQL Server та вказати пароль.

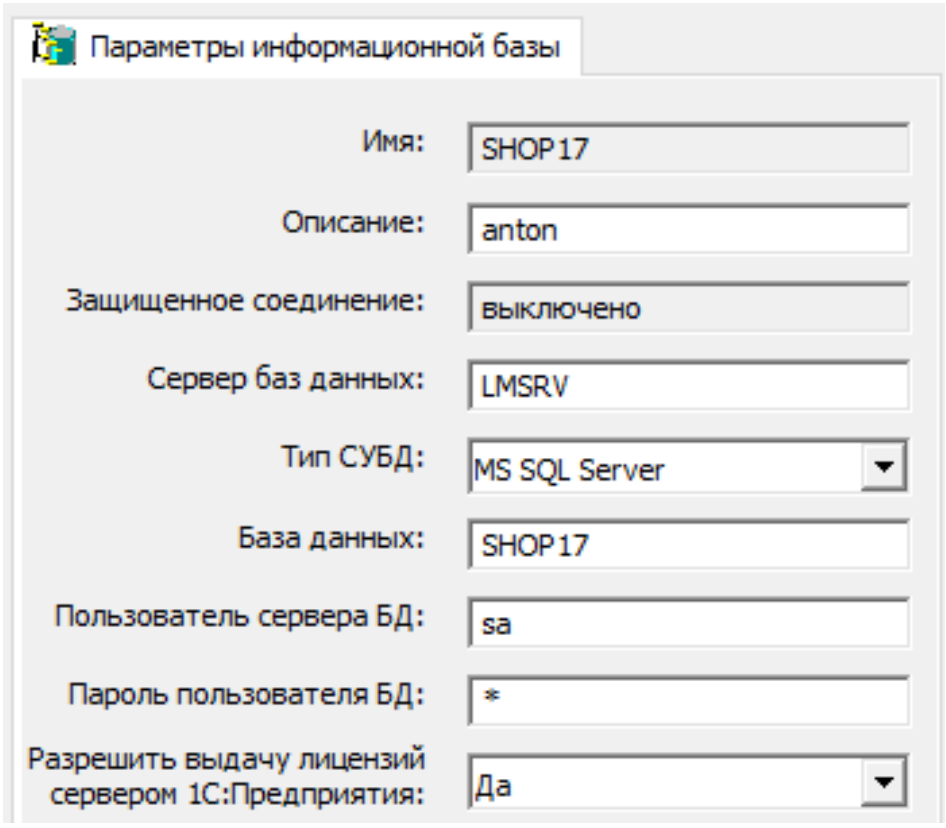


Рисунок 4.11– Створення клієнт-серверної 1С бази

Далі ми додаємо створену базу до програми. Після цього ми можемо взяти бекап БД і завантажити конфігуратором або створити нову базу під 1С.

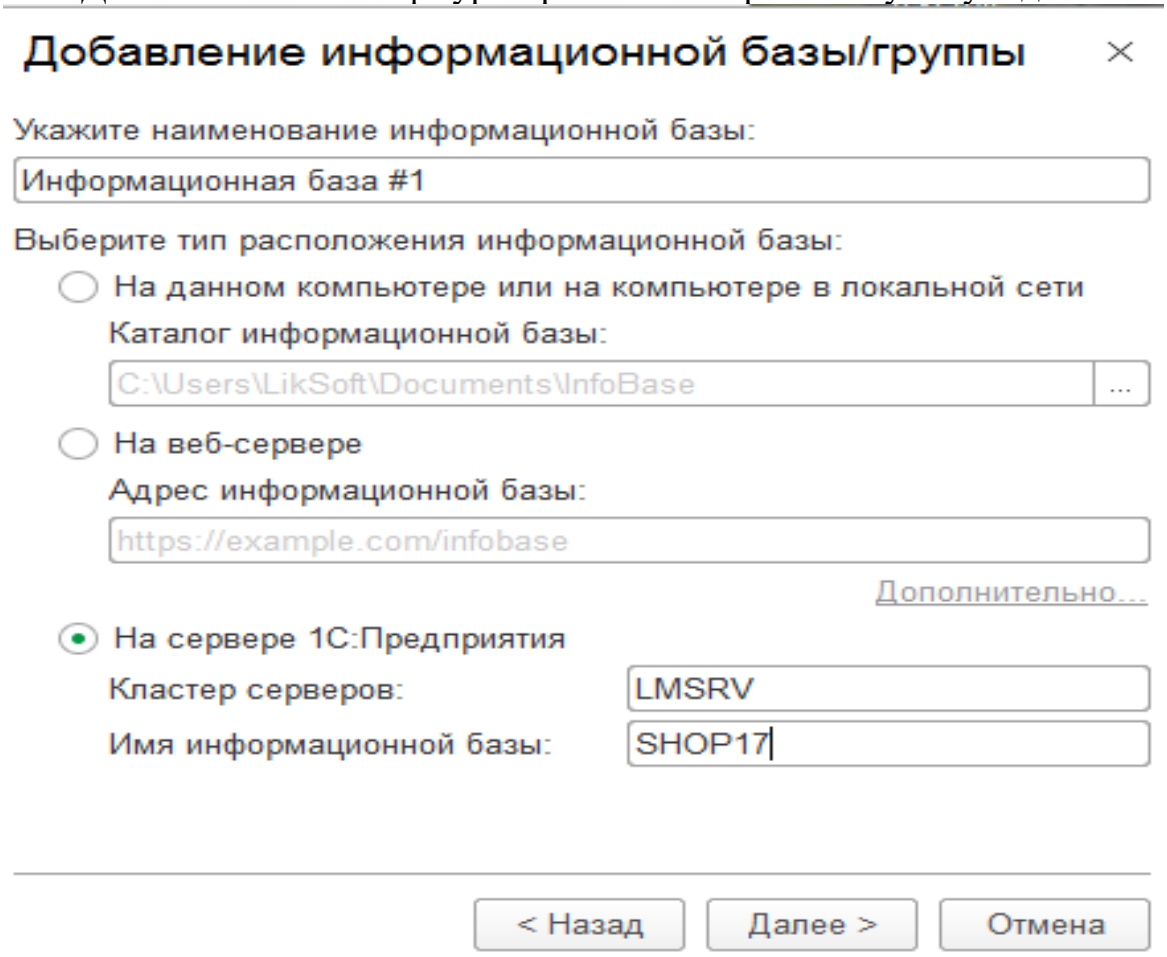


Рисунок 4.12– Додавання бази через програму

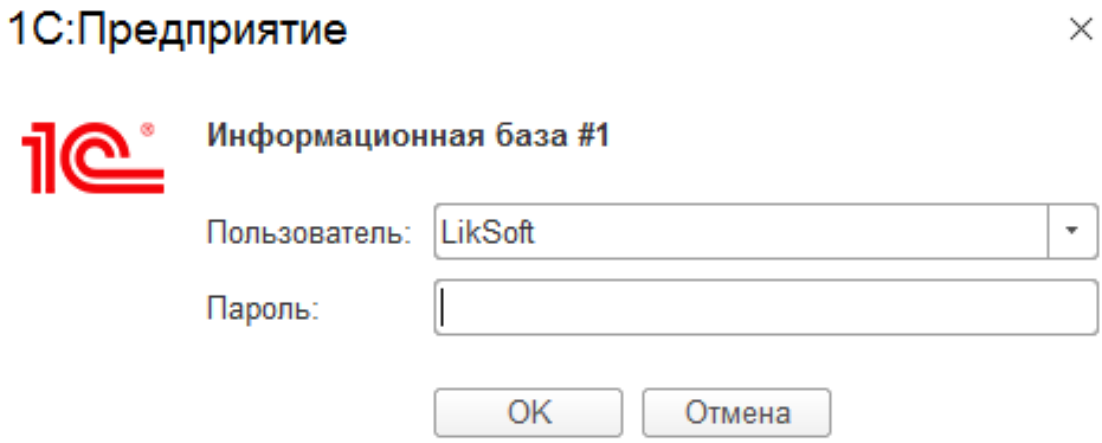


Рисунок 4.13– Перевірка

4.2 Використання двох варіантів захисту від брутфорсу

Оскільки вище було налаштування портів, щоб вони приймали дані із зовнішньої адреси, необхідно налаштувати роутер на захист від брутфорс атак. Звичайно потрібно налаштувати роутери так що б вони розрізняли користувача та бота, який використовує брутфорс. У разі віддаленого доступу брутфорс атаки можуть заважати з'єднанню та викликати перешкоди у мережі. Розглянемо 2 варіанти захисту та визначимо різницю між ними. Використовуватимемо консоль для зручності.

Почнемо з правила, яке буде блокувати IP-адреси, які запитують з'єднання більше 4-х разів за хвилину. У данному випадку використовую порт 22.

```
/ip firewall filter

add chain=input protocol=tcp dst-port=22 connection-state=new \
src-address-list=ssh_stage3 action=add-src-to-address-list address-list=blacklist \
address-list-timeout=10d comment="blacklist" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new \
src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3 \
address-list-timeout=1m comment="ssh-stage3" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new src-address-
list=ssh_stage1 \
action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m
comment="ssh-stage2" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new action=add-src-to-
address-list \
address-list=ssh_stage1 address-list-timeout=1m comment="" disabled=no
```

Рисунок 4.14 – Захист від brute-force атак для SSH

```
/ip firewall filter
add chain=input protocol=tcp dst-port=21 src-address-
list=ftp_blacklist action=drop comment="drop ftp brute forcers"
add chain=output action=accept protocol=tcp content="530 Login
incorrect" dst-limit=1/1m,9,dst-address/1m
add chain=output action=add-dst-to-address-list protocol=tcp
content="530 Login incorrect" address-list=ftp_blacklist address-list-
timeout=3h
```

Рисунок 4.15– Захист від brute-force атак для FTP

Створимо 3 правила за допомогою консолі, задача яких блокування підключення до роутера зі списків кожного ресурсу відповідно - dshield, spamhaus і blocklist.de. Для початку підключаємося к робочому MikroTik та записуємо у консоль наступне [11]:

```
/ ip firewall raw add chain=prerouting src-address-list="sbl dshield"
action=drop comment="sbl dshield"
ip firewall raw add chain=prerouting src-address-list="sbl spamhaus"
action=drop comment="sbl spamhaus"
ip firewall raw add chain=prerouting src-address-list="sbl blocklist.de"
action=drop comment="sbl blocklist.de"
```

Рисунок 4.16– Блокування підключень

Для поновлення актуальних списків необхідно налаштувати автоматичний завантажувач в роутері [11]. В поле On Event запишемо скрипт:

```
add chain=input protocol=tcp dst-port=2233 connection-state=new action=add-src-to-address-list address-list=ssh_round1 address-list-timeout=2m disabled=no
```

Рисунок 4.17– Ідентифікація підозрілого IP

Для імпорту списку в конфігурацію роутеру необхідно створити ще одну задачу. Це налаштування дозволить занести неподобаючі IP-адреси до вічного блеклісту, прописуємо:

```
add chain=input protocol=tcp dst-port=2233 src-address-list=ssh_blacklist action=drop comment="drop ssh brute forcers" disabled=no
```

Рисунок 4.18– Занесення навічно у блекліст

Рисунок 4.19 – Завдання на оновлення списків

Таким чином у нас буде оновлення даних щодо ip адрес зловмисників. Тепер використовуємо другий варіант налаштування. Робимо перше правило, яке блокуватиме будь-які підключення з чорного списку.

```
/ip firewall raw add action=drop chain=prerouting src-address-list=black-list
```

Рисунок 4.20 – Перше правило

Додаємо правильно яке буде додавати в чорний список black-list на добу всі адреси, які намагатимуться підключитися до tcp 3389

```
/ip firewall filter add action=add-src-to-address-list address-list=black-list address-list-timeout=1d
chain=input connection-state=new dst-port=3389 protocol=tcp
```

Рисунок 4.21 – Друге правило

Наступне правило підтримує раніше дозволені з'єднання з включеним fasttrack, правило нижче те ж саме, але без fasttrack. Друге правило дропає всі пакети зі статусом invalid (тобто ті, які роутер не зможе ідентифікувати по connection tracker'y). Останнє правило забороняє все, що прилетить на інтерфейс ether1 і не матиме стан dstnat'ed

```
/ip firewall filter add action=fasttrack-connection chain=forward
comment=fasttrack connection-state=established,related
/ip firewall filter add action=accept chain=forward comment="accept
established, related, untracked" connection-
state=established,related,untracked
/ip firewall filter add action=drop chain=forward comment="drop
invalid" connection-state=invalid
/ip firewall filter add action=drop chain=forward comment="drop all
from WAN not DSTNATed" connection-nat-state=!dstnat connection-
state=new in-interface=ether1
```

Рисунок 4.22– Набір правил

Для перевірки використовувалася брутфорс атака, щоб оцінити як працюють правила разом. Перед атакою було сформовано генератор списку паролів програмою Wordlists [12]. Використовувалася поширена програма hydra, система Kali Linux [13]. Брутфорс є одним з простих методів взлому сервера. Для цього використаємо програму hydra яка у відкритому доступі та має підтримку величезну кількість служб

```
-R відновити попередню перервану / обірвану сесію
-S виконати SSL з'єднання
-s ПОРТ якщо служба не на порту за замовчуванням, то можна задати порт тут
-l ЛОГІН або -L Фото з логіном (іменами), або завантажити кілька логінів з ФАЙЛА
-p ПАРОЛЬ або -P Фото з паролями для перебору, або завантажити кілька паролів з ФАЙЛА
-x МІНІМУМ: МАКСИМУМ: НАБОР_СІМВОЛОВ генерація паролів для брутфорса, наберіть "-x -h" для допомоги
-e nsr "n" - пробувати з порожнім паролем, "s" - логін в якості пароля і / або "r" - реверс облікових даних
-u зациклюватися на користувача, а не на паролі (ефективно! мається на увазі з використанням опції -x)
-C Файл формат де "логін: пароль" розділені двокрапкою, замість опції -L / -P
-M Файл список серверів для атак, одна запис на рядок, після двокрапки ':' можна задати порт
-o Файл записувати знайдені пари логін / пароль в Фото замість стандартного виводу
-f / -F вийти, коли пара логін / пароль підібрана (-M: -f для хоста, -F глобально)
-t ЗАВДАННЯ кількість запущених паралельно ЗАВДАНЬ (на хост, за замовчуванням: 16)
-w / -W ЧАС час очікування відповідей (32 секунди) / між сполуками на потік
-4 / -6 віддавати перевагу IPv4 (за замовчуванням) або IPv6 адреси
-v / -V / -d вербальний режим / показувати логін + пароль для кожної спроби / режим налагодження
-O використовувати старі SSL v2 і v3
-q не друкувати повідомлення про помилки з'єднання
-U докладні відомості про використання модуля
service служба для злому (дивіться список підтримуваних протоколів)
OPT деякі модулі служб підтримують додаткове введення (-U для довідки по модулю)
```

Рисунок 4.23– Список команд

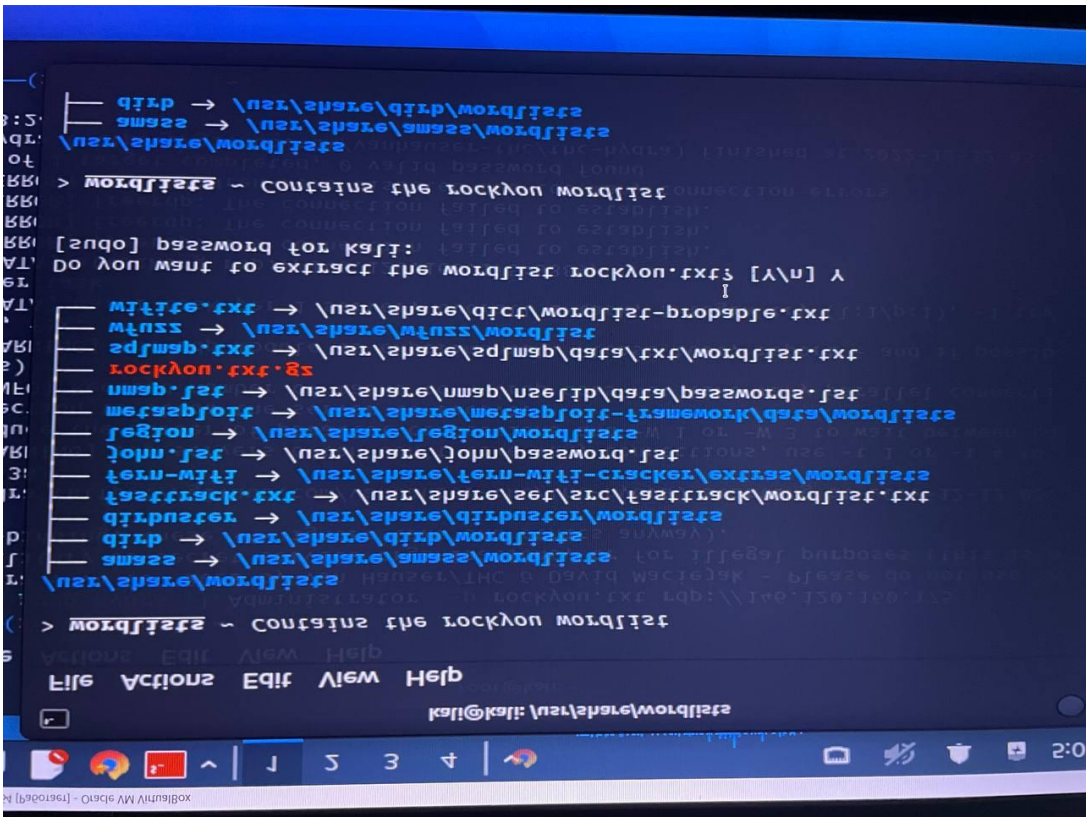


Рисунок 4.24 – Генерація списку паролів

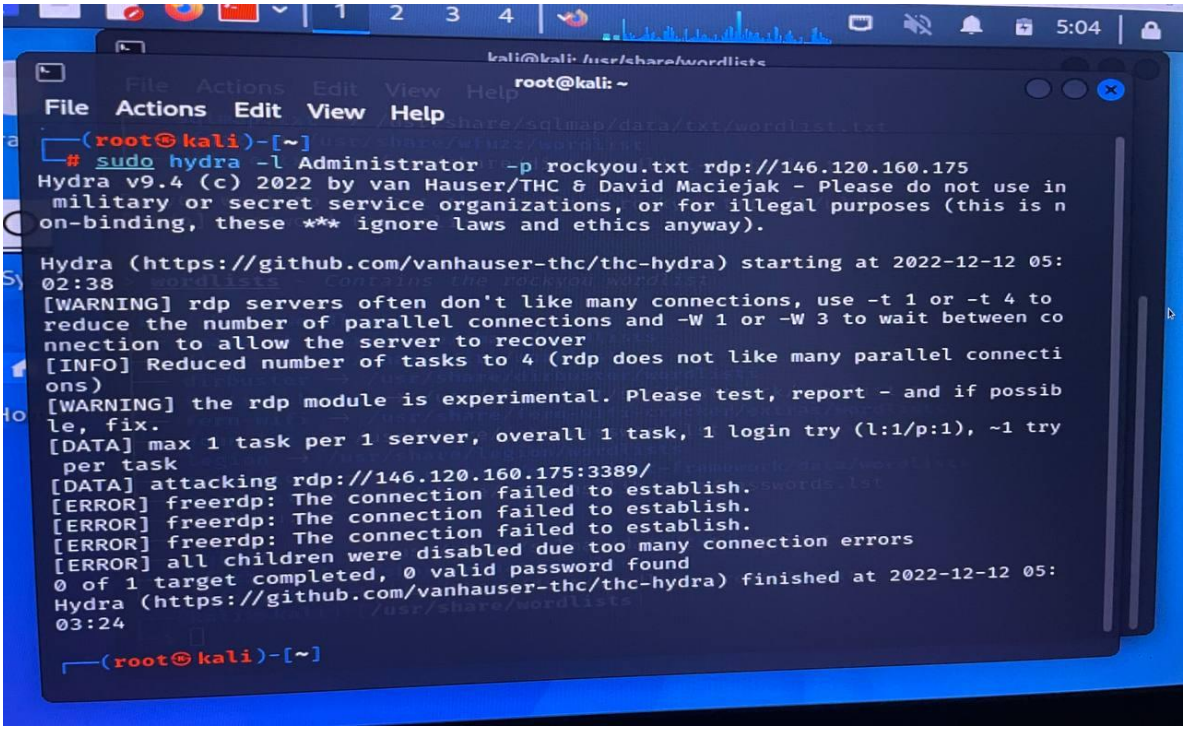
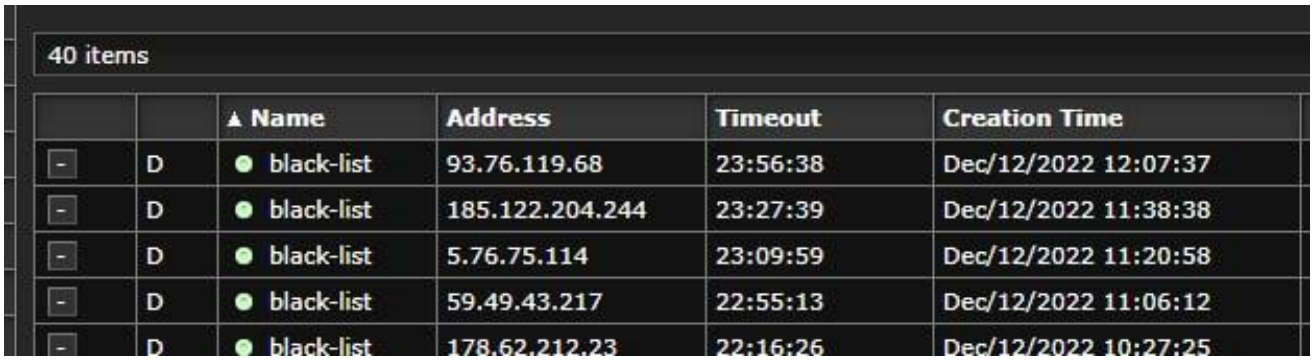


Рисунок 4.25 – Атака hydra

Рисунок 4.26 – IP-адреса з якої проводилася атака



40 items

		Name	Address	Timeout	Creation Time
-	D	black-list	93.76.119.68	23:56:38	Dec/12/2022 12:07:37
-	D	black-list	185.122.204.244	23:27:39	Dec/12/2022 11:38:38
-	D	black-list	5.76.75.114	23:09:59	Dec/12/2022 11:20:58
-	D	black-list	59.49.43.217	22:55:13	Dec/12/2022 11:06:12
-	D	black-list	178.62.212.23	22:16:26	Dec/12/2022 10:27:25

Рисунок 4.27 – Перевірка IP у блекліст

ВИСНОВОК

У роботі розглянуто питання аналізу та побудови параметрів безпеки сервера для віддаленого використання та розглянуті сучасні БД та СУБД. Для перевірки налаштувань з питань безпеки та стабільности, було проаналізовано та використано програмні засоби.

Для практичного використання у роботі запропоновано створення Raid1 який виконує функцію покращення стабільності, резерву даних, та збільшення швидкості накопичувачів. Виконана покрокова інструкція встановлювання Raid1 за допомогою BIOS серверу. Операційна система була вибрана Windows Server 2016, вона використовує віртуальні середовища, для того, щоб не впливати на саму операційну систему. Приділена увага налаштуванню роутера Mikrotik. Виконано прокидання портів, для користувачів сервера. Також завдяки цьому було мінімізовано атака брутфорсу на конкретний порт. Виконання брутфорс-атаки через RDP було також мінімізовано на сервері, завдяки налаштуванню правил на роутері. В роботі розкладено та доповнено використання баз даних, на прикладі програми 1С. Завдяки гнучкості програми вона була представлена у двох видах файл-сервер і кліент-сервер.

Для перевірки захисту на мережу, було використана спеціальна операційна система KaliLinux, яка має встановлену програму Hydra за допомогою якої виконується мережева атака брутфорс. Описані дії для налаштування роутера та відкриття портів дали результат, IP-адрес зловмистника був заблоковано, дуже швидко, можна перевірити завдяки блеклісту.

В цілому, в результаті виконання магістерської роботи, була досягнута поставлена мета у вигляді забезпечення стабільності, працездатності, захисту від брутфорс-атак та надійності зберігання баз даних, забезпечуючи цілісність, конфіденційність та доступність інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Положення про технічний захист інформації в Україні №1229/99 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1229/99#Text
2. Protect your business online [Електронний ресурс] – Режим доступу: https://www.nibusinessinfo.co.uk/content/server-security
3. Server Security [Електронний ресурс] – Режим доступу: https://www.speedster-it.com/server-security-explained-what-is-server-security/
4. 21 Server Security Tips to Secure Your Server [Електронний ресурс] – Режим доступу: https://phoenixnap.com/kb/server-security-tips
5. Основные виды серверов: назначение и особенности [Електронний ресурс] – Режим доступу: https://galtsystems.com/blog/start/osnovnye_vidy_serverov_naznachenie_i_osobennosti/
6. Що таке реляційна база даних? Електронний ресурс] – Режим доступу: https://aws.amazon.com/ru/relational-database/
7. Класифікація СУБД. Типи та види СУБД [Електронний ресурс] – Режим доступу: https://www.sqlhome.org.ua/klassifikaciya-tipy-vidy-subd/
8. RAID масив: види і процес створення. [Електронний ресурс] – Режим доступу: https://subcase.ru/uk/raid-1-opisanie-raid-massiv-vidy-i-process-sozdaniya-chto-takoe-raid-v.html
9. Установка и настройка Windows Hyper-V Server 2019 [Електронний ресурс] – Режим доступу: https://winitpro.ru/index.php/2019/08/07/nastrojka-free-windows-hyper-v-server/
10. Установка и активация сервера лицензирования RDS на Windows Server 2019/2016 [Електронний ресурс] – Режим доступу:

https://winitpro.ru/index.php/2017/11/21/ustanovka-i-aktivaciya-rds-license-na-windows-server-2016/

11. Умная защита от атак Mikrotik [Електронний ресурс] – Режим доступу: https://wiki.merionet.ru/seti/11/umnaya-zashhita-ot-atak-mikrotik/
12. Создание и нормализация словарей [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/pentestit/blog/337718/
13. Hydra [Електронний ресурс] – Режим доступу: https://kali.tools/?p=1847
14. Локаєнко В.О. Програмно-апаратний захист сервера: бакалаврська робота / В.О. Локаєнко – Запоріжжя: НУ «Запорізька політехніка», 2021. – 18-38 с.