

Міністерство освіти і науки України

Луцький національний технічний університет

(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій

(повне найменування факультету)

Кафедра комп'ютерної інженерії та безпеки

(повне найменування кафедри)

**КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»**

**МЕРЕЖЕВЕ СХОВИЩЕ НА ОСНОВІ RASPBERRY PI
RASPBERRY PI-BASED NETWORK STORAGE**

спеціальність 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія

(назва освітньої програми)

Виконав: здобувач вищої освіти
групи KI-41
Прокопенко Віталій Сергійович

(підпис)

Керівник:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 06 » червня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних та інформаційних технологій

Кафедра комп'ютерної інженерії та безпеки

Ступінь вищої освіти: бакалавр

Галузь знань: 12 Інформаційні технології

Спеціальність: 123 Комп'ютерна інженерія

Освітня програма: «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри

доц. Тарас ТЕРЛЕЦЬКИЙ

« 10 » 01 2025 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Прокопенку Віталію Сергійовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Мережеве сховище на основі Raspberry Pi*

Керівник роботи *к.т.н., доцент Лавренчук Світлана Василівна*

затверджені наказом закладу вищої освіти від «04» січня 2025 року № 11/01-02

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 10.06.2025р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):

Вступ

Аналіз предметної області та наявних рішень

Вибір апаратної та програмної бази для мережевого сховища

Проектування та тестування мережевого сховища

Висновки

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
<i>Аналіз проблеми за темою роботи та постановка завдань дослідження</i>	<i>Лавренчук С.В., доцент</i>		
<i>Вибір апаратної та програмної бази для мережевого сховища</i>	<i>Лавренчук С.В., доцент</i>		
<i>Проектування та тестування мережевого сховища</i>	<i>Лавренчук С.В., доцент</i>		
<i>Нормоконтроль</i>	<i>Багнюк Н.В., доцент</i>		
<i>Гарант ОП</i>	<i>Лавренчук С.В., доцент</i>		
<i>Показник запозичень тексту</i>		_____%	
<i>Академічна доброчесність</i>	<i>Міскевич О.І., ст. викладач</i>		

7. Дата видачі завдання 10.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	<i>Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень</i>	до 10.02.2025 р.	Виконано
2.	<i>Вибір апаратної та програмної бази для проекту</i>	до 02.03.2025 р.	Виконано
3.	<i>Проектування та тестування системи моніторингу</i>	до 02.04.2025 р.	Виконано
4.	<i>Висновки та пропозиції</i>	до 10.04.2025 р.	Виконано
5.	<i>Формування списку використаних джерел</i>	до 15.04.2025 р.	Виконано
6.	<i>Формування додатків</i>	до 02.05.2025 р.	Виконано
7.	<i>Оформлення ілюстративного матеріалу</i>	до 10.05.2025 р.	Виконано
8.	<i>Представлення остаточного варіанту кваліфікаційної роботи керівникові</i>	до 15.05.2025 р.	Виконано
9.	<i>Нормоконтроль</i>	до 30.05.2025 р.	Виконано
10.	<i>Інструментальна перевірка на академічний плагіат</i>	до 03.06.2025 р.	Виконано
11.	<i>Здача кваліфікаційної роботи та всіх супровідних документів на кафедру</i>	до 11.06.2025 р.	Виконано

Здобувач вищої освіти

(підпис)

Прокопенко В.С.

(прізвище, ініціали)

Керівник кваліфікаційної роботи

(підпис)

Лавренчук С.В.

(прізвище, ініціали)

АНОТАЦІЯ

Прокопенко В.С. Мережеве сховище на основі Raspberry Pi. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, додатку.

Перший розділ присвячено огляду предметної області, тут обґрунтовано актуальність обраної теми, розглянуто можливості використання мережевих сховищ та Raspberry Pi, проаналізовані вже існуючі рішення реалізації проекту.

В другому розділі здійснено вибір та обґрунтування засобів розробки. Розглянуто будову Raspberry Pi, його компоненти, види дисків для зберігання даних, різниця між форматами зберігання даних. Виконано дослідження мережевих технологій для доступу до пристрою через інтернет, та локальну мережу.

Третій розділ присвячено проектуванню пристрою, налаштування Raspberry Pi, налаштування локальної мережі і подальше відкриття доступу в інтернет, також описані подальші можливості вдосконалення пристрою.

Ключові слова: мережеве сховище, NAS, Raspberry Pi.

ANNOTATION

Prokopenko V. Raspberry Pi-based network storage. Manuscript.

Qualification work for bachelor's degree in Computer Engineering, specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

The qualification work consists of an introduction, three chapters, conclusions, a list of references, and an appendix.

The first section is devoted to an overview of the subject area, it substantiates the relevance of the chosen topic, considers the possibilities of using network storage and Raspberry Pi, analyzes existing solutions for the project.

In the second section, we select and justify the development tools. The structure of the Raspberry Pi, its components, types of disks for data storage, and the difference between data storage formats are considered. A study of network technologies for accessing the device via the Internet and a local network is performed.

The third section is devoted to the design of the device, setting up the Raspberry Pi, setting up a local network and further opening access to the Internet, and further opportunities for improving the device are also described.

Keywords: network storage, NAS, Raspberry Pi.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА НАЯВНИХ РІШЕНЬ	10
1.1 Мережеве сховище (NAS).....	10
1.2 Raspberry Pi як платформа для побудови мережевих сховищ	14
1.3 Переваги використання Raspberry Pi як бази для мережевого сховища	16
1.4 Безпека мережевих сховищ на базі одноплатних комп'ютерів	17
РОЗДІЛ 2 ВИБІР АПАРАТНОЇ ТА ПРОГРАМНОЇ БАЗИ ДЛЯ МЕРЕЖЕВОГО СХОВИЩА.....	20
2.1 Обґрунтування вибору апаратної платформи.....	20
2.2 Вибір та обґрунтування накопичувачів для зберігання даних.....	21
2.3 Вибір операційної системи та базового програмного забезпечення	23
2.4 Мережеві технології та протоколи доступу.....	24
2.5 Додаткові сервіси та їх інтеграція	25
РОЗДІЛ 3 ПРОЕКТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖЕВОГО СХОВИЩА.....	27
3.1 Підготовка апаратної платформи та початкове встановлення.....	27
3.1.1 Підготовка Raspberry Pi та периферійних пристроїв	27
3.1.2 Встановлення Raspberry Pi OS.....	28
3.1.3 Конфігурація статичної IP адреси	29
3.2 Встановлення та налаштування Proxmox VE	30
3.2.1 Підготовка системи до встановлення Proxmox VE	31
3.2.2 Налаштування мережевих інтерфейсів	31
3.2.3 Встановлення Proxmox VE	32
3.3 Розгортання Pi-hole в LXC контейнері.....	33
3.4 Конфігурація ZFS файлової системи	35
3.5 Встановлення та налаштування OpenMediaVault.....	36
3.5.1 Створення віртуальної машини для OpenMediaVault	36
3.5.2 Встановлення та налаштування OpenMediaVault.....	37

	7
ВИСНОВКИ	41
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ	43
ДОДАТКИ	45

ВСТУП

Актуальність теми дослідження. У сучасному світі зростання обсягів цифрової інформації та потреба в надійному, доступному та економічно ефективному зберіганні даних стають все більш важливими проблемами як для індивідуальних користувачів, так і для малих підприємств. Традиційні рішення для мережевого зберігання даних часто характеризуються високою вартістю та складністю налаштування, що робить їх недоступними для широкого кола користувачів. У цьому контексті використання одно платних комп'ютерів Raspberry Pi для створення мережевих сховищ представляє інноваційний підхід, що дозволяє поєднати доступність, енергоефективність та функціональність. Актуальність дослідження зумовлена необхідністю розробки економічно вигідних альтернатив дорогим комерційним NAS-системам та зростаючою популярністю IoT пристроїв у домашніх та корпоративних мережах.

Стан вивченості проблеми. Проблематика створення мережевих сховищ даних досліджувалася багатьма вченими та практиками. Сучасні дослідження в галузі домашніх NAS-систем та IoT-пристроїв представлені в роботах провідних технологічних компаній та відкритих спільнот розробників. Однак комплексні дослідження, що поєднують питання продуктивності, безпеки та економічної ефективності мережевих сховищ на базі Raspberry Pi, залишаються недостатньо вивченими та потребують подальшого дослідження.

Мета роботи – розробка та дослідження ефективного мережевого сховища даних на основі мікро комп'ютера Raspberry Pi з оцінкою його продуктивності, надійності та практичної застосовності.

Завдання роботи. Розглянути сучасні підходи до організації мережевих сховищ даних та проаналізувати переваги і недоліки існуючих рішень. Дослідити технічні характеристики та можливості платформи Raspberry Pi для застосування в якості основи мережевого сховища. Спроектувати та реалізувати мережеве сховище на базі Raspberry Pi з необхідними функціональними можливостями.

Об'єкт дослідження – мережеві сховища даних та одноплатні комп'ютерні системи як основа для їх реалізації в умовах домашнього та малого офісного використання.

Предмет дослідження – процес проектування, розробки та оптимізації мережевого сховища даних на основі платформи Raspberry Pi, включаючи аспекти продуктивності, надійності та користувацького досвіду.

Методи дослідження. У процесі виконання роботи використовувалися емпіричні методи дослідження: експериментальне тестування продуктивності, спостереження за функціонуванням системи, порівняльний аналіз різних конфігурацій та вимірювання ключових параметрів системи. Серед методів теоретичного пізнання застосовувалися: системний підхід для комплексного аналізу архітектури мережевого сховища, моделювання для прогнозування поведінки системи під різними навантаженнями. Використовувалися також загально логічні методи: аналіз та синтез при дослідженні компонентів системи, узагальнення для формулювання висновків, дедукція для виведення практичних рекомендацій.

Інформаційна база дослідження включає: технічну документацію Raspberry Pi Foundation; специфікації мережевих протоколів та файлових систем; результати тестування, опубліковані в спеціалізованих технічних виданнях та на платформах Stack Overflow, GitHub, матеріали конференцій з embedded систем та IoT-технологій; монографічні дослідження з розподілених систем та мережевих технологій; статистичні дані про використання домашніх NAS-систем з аналітичних платформ.

Матеріали кваліфікаційної роботи обговорювалися на міжнародній науково-практичній конференції молодих вчених та студентів «Програмне та апаратне забезпечення в інформаційних технологіях» [16], яка відбулася 6 травня 2025 року в місті Луцьку. За результатами дослідження опубліковано тези [17] (додаток А).

РОЗДІЛ 1

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА НАЯВНИХ РІШЕНЬ

1.1 Мережеве сховище (NAS)

Мережеве сховище або NAS (Network Attached Storage) [1] – це пристрій який дозволяє користувачам зберігати та обмінюватись файлами через мережу, наприклад домашню або офісну мережу. Будь-яка комп'ютерна мережа має взаємопов'язані комп'ютери сервери та клієнтські комп'ютери, які надсилають запити до серверів. Пристрої NAS – це сервери, які виконують лише функції зберігання даних і спільного доступу до файлів. Вони забезпечують швидке, безпечне та надійне зберігання даних у приватних мережах.

За призначенням мережеві сховища поділяються на домашні, офісні та корпоративні рішення. Домашні NAS призначені для персонального використання, зберігання мультимедійних файлів та резервного копіювання. Офісні системи орієнтовані на малі та середні підприємства, забезпечуючи централізоване зберігання робочих документів. Корпоративні рішення характеризуються високою продуктивністю, масштабованістю та розширеними функціями безпеки.

За архітектурою розрізняють одно блочні та модульні NAS-системи. Одно блочні системи містять всі компоненти в єдиному корпусі, що забезпечує простоту налаштування та обслуговування. Модульні системи дозволяють нарощувати функціональність шляхом додавання окремих модулів.

Основні протоколи доступу до мережевих сховищ:

– SMB/CIFS (Server Message Block/Common Internet File System) є найпоширенішим стандартом для доступу до файлів у Windows-мережах, забезпечуючи прозору інтеграцію з операційною системою та підтримку функції автентифікації користувачів;

– NFS (Network File System) призначений переважно для Unix/Linux систем, характеризується високою продуктивністю та ефективним використанням мережевих ресурсів, особливо у гомогенних Linux середовищах;

– FTP (File Transfer Protocol) надає універсальний доступ до файлів через стандартний протокол, підтримується практично всіма операційними системами, але має обмежені можливості щодо безпеки у базовому варіанті;

– WebDAV (Web Distributed Authoring and Versioning) дозволяє доступ до файлів через HTTP/HTTPS протокол, забезпечуючи можливість роботи через веб-браузер та спрощений доступ через мережу Інтернет.

1.2 Аналіз сучасного ринку мережевих сховищ

На ринку вже давно є присутні готові збірки мережевих сховищ готових до використання, які представляють собою комплексні рішення для організації централізованого зберігання даних. Ці пристрої набули широкого поширення завдяки простоті налаштування, надійності роботи. Сучасні готові NAS-рішення поєднують у собі апаратну частину, оптимізовану для безперервної роботи, та спеціалізовані операційні системи з інтуїтивними веб-інтерфейсами, що дозволяє користувачам без глибоких технічних знань легко налаштовувати та керувати власною мережевою інфраструктурою. Розглянемо декілька з них

Synology DiskStation (рис. 1.1) є одним з лідерів ринку завдяки інтуїтивній операційній системі DSM (DiskStation Manager), яка надає зручний веб-інтерфейс та широкий спектр додатків. Пристрої Synology відзначаються високою надійністю, регулярними оновленнями безпеки та потужними функціями синхронізації даних. Вартість початкових моделей становить від 8-12 тис. грн.

QNAP Systems (рис. 1.2) позиціонується як рішення для професіонального використання, пропонуючи високопродуктивні системи з підтримкою віртуалізації та контейнерів. Операційна система QTS характеризується багатофункціональністю, але може бути складнішою для початківців. Цінова категорія варіюється від 10 тис. грн. до декількох десятків тисяч гривень залежно від конфігурації.



Рисунок 1.1 – Мережеве сховище Synology DS224+ [2]



Рисунок 1.2 – Мережеве сховище QNAP TS-216G [3]

Western Digital My Cloud (рис. 1.3) орієнтована на споживчий ринок, пропонуючи прості у використанні пристрої за доступними цінами. Однак функціональність таких систем обмежена базовими функціями зберігання та синхронізації.



Рисунок 1.3 – Мережеве сховище WD My Cloud Home [4]

Відкриті програмні рішення для створення NAS:

– OpenMediaVault базується на Debian Linux і призначена спеціально для створення NAS-систем. Система надає веб інтерфейс для управління, підтримує різноманітні файлові системи та протоколи доступу. Головною перевагою є безкоштовність та можливість встановлення на будь-яке сумісне обладнання;

– TrueNAS (колишня FreeNAS) ґрунтується на FreeBSD та файловій системі ZFS, що забезпечує високий рівень цілісності даних та продуктивності. Рішення підходить для професійного використання, але вимагає більш глибоких знань для налаштування;

– Nextcloud являє собою платформу для хмарного зберігання з відкритим кодом, що може працювати як самостійне рішення або доповнювати існуючі NAS системи функціями синхронізації та співпраці.

За функціональністю комерційні рішення зазвичай пропонують більш відполіровані інтерфейси та розширені можливості, але самостійні рішення надають повний контроль над системою та можливість налаштування під специфічні потреби.

Основними недоліками комерційних рішень є висока вартість, обмежена можливість налаштувань та залежність від виробника щодо оновлень та підтримки. Готові системи часто включають функції, які не потрібні домашнім користувачам, але впливають на вартість.

Відкриті рішення, хоча і безкоштовні, вимагають значних технічних знань для налаштування та обслуговування, що може бути перешкодою для звичайних користувачів. Крім того, відсутність офіційної технічної підтримки може ускладнити вирішення проблем.

1.2 Raspberry Pi як платформа для побудови мережевих сховищ

Розглянемо декілька Raspberry Pi плат та виділемо різницю між ними.

Raspberry Pi 4 Model B (рис. 1.4) оснащена 64-рибітним чотири ядерним ARM Cortex-A72 процесором з частотою 1,8 ГГц, до 8 ГБ RAM, двома портами USB 3.0, гігабітним Ethernet. Ці характеристики роблять Pi 4 придатною для використання як легкий сервер.

Raspberry Pi 5 (рис. 1.5), випущена у 2023 році, демонструє значне покращення продуктивності завдяки новому чипу BCM2712 та збільшенню частоти процесора до 2,4 ГГц. Додано підтримку PCIe, що розширює можливості підключення швидких накопичувачів.

Порівняно з попередніми поколіннями, сучасні моделі показують покращення продуктивності процесора в 2-3 рази та значне зростання пропускної здатності мережевого інтерфейсу.

Основними перевагами є низька вартість (від 3 тис. грн залежно від моделі), мінімальне енергоспоживання (5-10 Вт), компактні розміри та тиха

робота. Платформа підтримує різноманітні операційні системи на базі Linux, що забезпечує гнучкість налаштування.

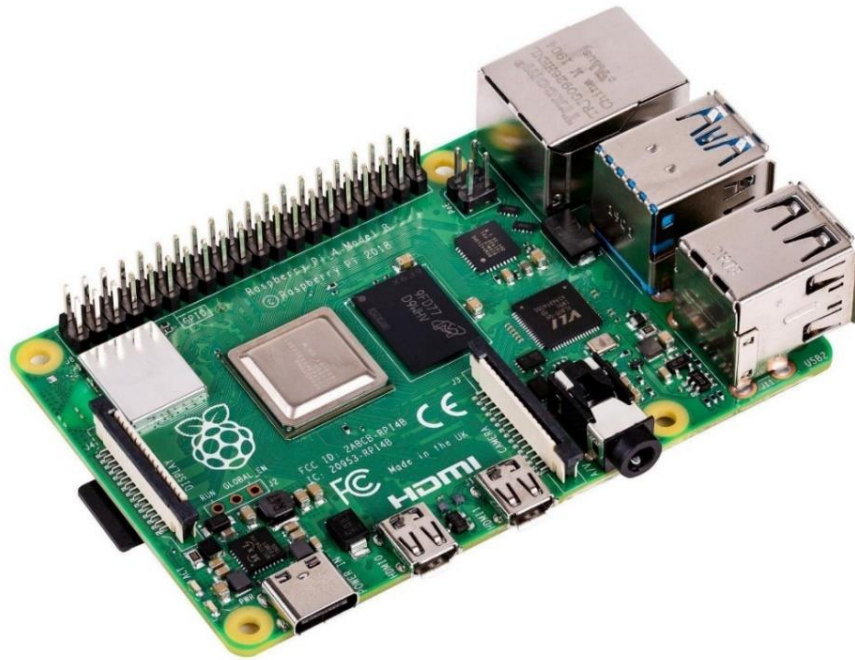


Рисунок 1.4 – Raspberry Pi 4 Model B [5]

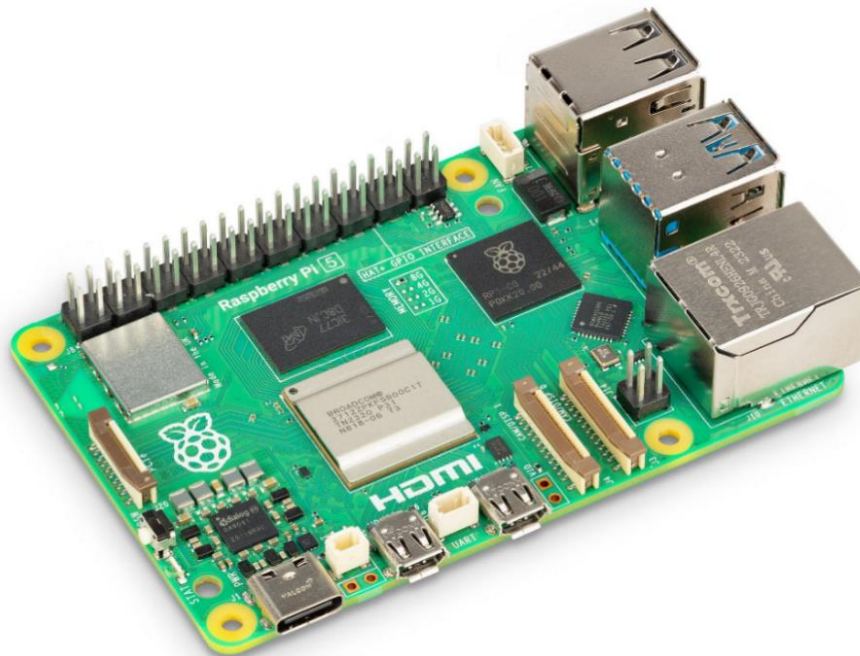


Рисунок 1.5 – Raspberry Pi 5 [6]

Серед обмежень слід відзначити відносно низьку продуктивність процесора порівняно з x86-системами, обмежену кількість портів для підключення дисків та залежність від якості карти пам'яті microSD. Продуктивність мережевого інтерфейсу може стати вузьким місцем під час інтенсивного використання.

1.3 Переваги використання Raspberry Pi як бази для мережевого сховища

Найбільшою перевагою створення власного мережевого сховища окрім меншої вартості для збирання такого пристрою – це можливість розширення технологій і програм що встановлені і використовуються на ньому. Розглянемо приклади програм що можна використовувати на такому пристрої.

Pi-hole являє собою DNS сервер з функцією блокування реклами на рівні мережі, який може працювати паралельно з NAS функціями на тому самому Raspberry Pi. Система перехоплює DNS запити та блокує домени, відомі як джерела реклами та шкідливого контенту, забезпечуючи захист всіх пристроїв у локальній мережі.

Інтеграція Pi-hole з мережевим сховищем дозволяє створити комплексне рішення для домашньої мережі, що поєднує функції зберігання даних та підвищення безпеки інтернет серфінгу. Додатковими перевагами є покращення швидкості завантаження веб сторінок та економія трафіку.

Docker дозволяє розгортати додаткові сервіси у вигляді контейнерів, забезпечуючи ізоляцію та спрощуючи управління. На Raspberry Pi можна одночасно запускати контейнери з NAS сервісами, медіа серверами, системами моніторингу та іншими додатками.

Proxmox VE, хоча і менш поширений на ARM-архітектурі, надає можливості віртуалізації для розділення ресурсів між різними сервісами. Це особливо корисно для тестування різних конфігурацій NAS або ізоляції критично важливих сервісів.

Plex Media Server може перетворити мережеве сховище на повноцінний медіа-центр з можливостями транскодування та стримінгу контенту на різні пристрої. Raspberry Pi 4 та новіші моделі забезпечують достатню продуктивність для відтворення відео контенту та обмеженого транскодування.

Jellyfin, як відкрита альтернатива Plex, надає аналогічні можливості без обмежень комерційної версії. Обидва рішення можуть інтегруватися з NAS системою для автоматичного сканування та каталогізації медіа-файлів.

Інтеграція рішень для резервного копіювання, таких як Duplicati або BorgBackup, дозволяє автоматизувати процес створення резервних копій даних з комп'ютерів мережі. Ці системи можуть працювати за розкладом та підтримують інкрементальне копіювання для економії простору.

Syncthing забезпечує децентралізовану синхронізацію файлів між пристроями без використання хмарних сервісів, що підвищує приватність та контроль над даними.

Налаштування VPN-сервера (WireGuard або OpenVPN) на тому самому Raspberry Pi дозволяє безпечно підключатися до домашньої мережі та отримувати доступ до NAS з будь-якої точки світу. Це рішення забезпечує шифрування трафіку та приховує справжню IP адресу користувача.

WireGuard, завдяки простоті налаштування та високій продуктивності, стає все більш популярним вибором для домашніх VPN серверів.

1.4 Безпека мережевих сховищ на базі одноплатних комп'ютерів

Домашні NAS системи стикаються з різноманітними загрозами безпеки, включаючи несанкціонований доступ через слабкі паролі, експлойти не виправлених вразливостей операційної системи, атаки типу «людина посередині» у незахищених мережах та фізичний доступ до пристрою.

Особливу увагу заслуговують атаки на SSH-сервіс, спроби брутфорс атак на веб-інтерфейс управління та потенційні вразливості у встановленому програмному забезпеченні. Raspberry Pi, як популярна платформа, може стати

мішенню автоматизованих атак, спрямованих на пристрої з типовими налаштуваннями.

Базова система безпеки має включати заміну стандартних паролів на складні унікальні комбінації, налаштування різних рівнів доступу для користувачів та груп, використання ключів SSH замість паролів для адміністративного доступу.

Додаткові методи захисту включають двофакторну аутентифікацію для веб-інтерфейсу, обмеження доступу за IP адресами, налаштування автоматичного блокування після невдалих спроб входу та регулярну ротацію паролів для критично важливих облікових записів.

Додаткові заходи включають налаштування мережевої сегментації для ізоляції NAS від інших пристроїв, використання фаєрволу для обмеження відкритих портів та регулярне оновлення системи для закриття відомих вразливостей.

Системи моніторингу дозволяють виявляти підозрілу активність в режимі реального часу. Налаштування системних логів для відстеження спроб входу, файлових операцій та мережевої активності допомагає ідентифікувати потенційні інциденти безпеки.

Інструменти типу Fail2ban можуть автоматично блокувати IP адреси після повторних невдалих спроб автентифікації, а системи сповіщень можуть інформувати адміністратора про критичні події через email або push-повідомлення.

Проведений аналіз предметної області демонструє актуальність розробки мережевого сховища на базі Raspberry Pi як економічно ефективною альтернативи комерційним NAS рішенням. Сучасні моделі Raspberry Pi 4/5 забезпечують достатню продуктивність [7] для домашнього використання при значно нижчій вартості та енергоспоживанні.

Огляд існуючих рішень виявив основні недоліки комерційних систем – високу вартість та надмірну складність, тоді як відкриті рішення вимагають

значних технічних знань. Raspberry Pi – це базоване рішення може поєднати доступність, функціональність та можливість підлаштовувати пристрій під себе.

Аналіз додаткових сервісів показав можливість створення комплексної домашньої IT-інфраструктури на базі одного пристрою, включаючи DNS сервер, VPN, медіа-сервер та системи резервного копіювання. Визначені вимоги до системи та технічні обмеження платформи створюють основу для подальшого проектування та реалізації мережевого сховища.

РОЗДІЛ 2

ВИБІР АПАРАТНОЇ ТА ПРОГРАМНОЇ БАЗИ ДЛЯ МЕРЕЖЕВОГО СХОВИЩА

2.1 Обґрунтування вибору апаратної платформи

Для реалізації проекту була обрана Raspberry Pi 5 з 8 ГБ RAM як найсучасніша модель з максимальними можливостями для NAS пристрою. 64-бітний чотири ядерний ARM процесор з частотою 2,4 ГГц забезпечує значне покращення продуктивності порівняно з попередніми поколіннями, особливо в задачах, що вимагають інтенсивних обчислень.

Ключовою перевагою Raspberry Pi 5 є наявність PCIe 2.0 слоту, що дозволяє підключати високошвидкісні SSD накопичувачі напряму до системної шини. Це забезпечує пропускну здатність до 5 ГБ/с, що у 4-5 разів перевищує можливості USB 3.0 інтерфейсу. Гігабітний Ethernet контролер тепер підключений напряму до SoC, що усуває обмеження пропускну здатності попередніх моделей.

Енергоспоживання Pi 5 становить 8-12 Вт під навантаженням, що вимагає більш ефективного охолодження. Робоча температура може досягати 85 °C, тому активне охолодження є обов'язковим для стабільної роботи під постійним навантаженням NAS системи.

Система охолодження для Raspberry Pi 5 є критично важливою через підвищене тепловиділення нового процесора. В даному проекті використовується активний охолоджувач з алюмінієвим радіатором та 30 мм вентилятором (рис. 2.1), підключеним до 4-ох пінового роз'єму для PWM управління швидкістю обертання. Це забезпечує автоматичне регулювання охолодження в залежності від температури та зменшує шум в нічний час.

Для системних файлів Raspberry Pi 5 використовується microSD карта з мінімальним об'ємом 128 ГБ для розміщення Proxmox VE та базових системних компонентів.

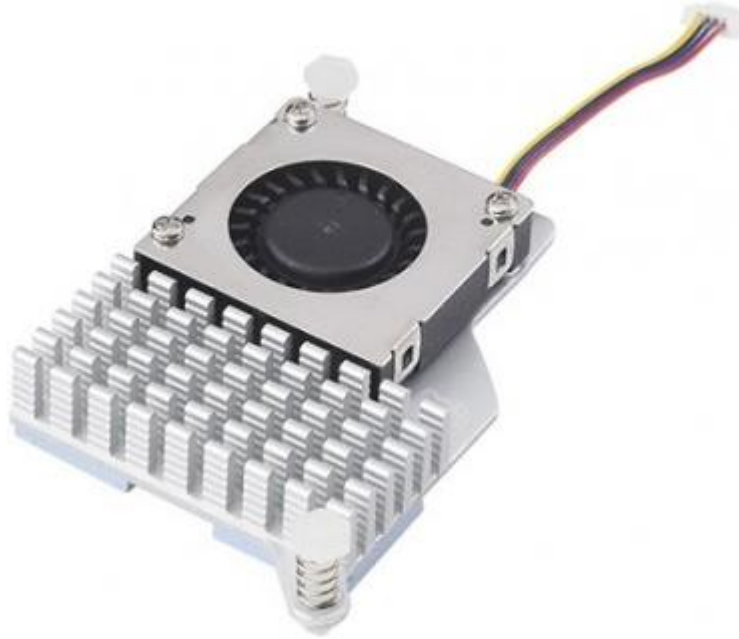


Рисунок 2.1 – Активний охолоджувач для Raspberry Pi 5 [8]

2.2 Вибір та обґрунтування накопичувачів для зберігання даних

SATA розширювач для M.2 SSD (рис. 2.2) є основним рішенням для зберігання користувацьких даних у даному проекті. Підключення через PCIe 2.0 слот забезпечує пропускну здатність до 5 ГБ/с, що значно перевищує можливості USB-інтерфейсу. Розширювач підтримує два M.2 NVMe SSD диски типорозміру 2280, що дозволяє створити RAID-масив або розділити диски за призначенням.

Альтернативні варіанти включають USB 3.0 накопичувачі (HDD та SSD) з пропускну здатністю до 400-500 МБ/с, що може бути достатньо для домашнього використання. USB-SATA адаптери [9] дозволяють підключити стандартні 2,5 та 3,5 диски, але обмежують швидкість інтерфейсом USB. Мережеві накопичувачі (iSCSI, NFS) можуть використовуватися для розширення дискового простору, але додають затримки мережі.

M.2 NVMe SSD диски забезпечують найвищу продуктивність з швидкістю послідовного читання до 3-7 тис. МБ/с та низькими затримками доступу. Для

NAS системи рекомендуються диски з 3D NAND пам'яттю та розширеною гарантією.

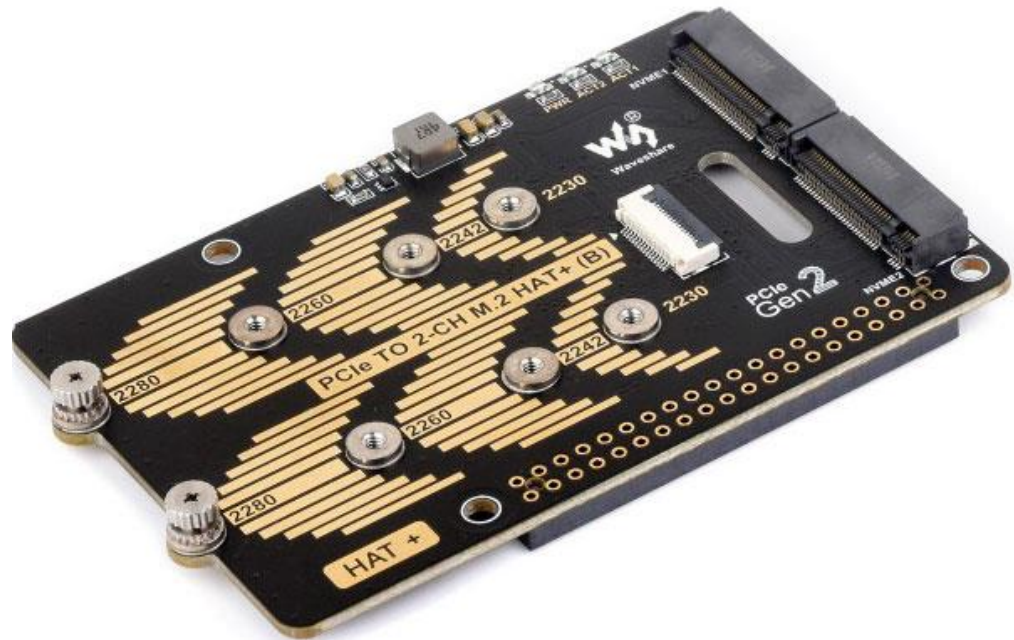


Рисунок 2.2 – SATA розширювач для M.2 SSD [9]

ZFS (Zettabyte File System) обрана як основна файлова система для проекту завдяки унікальним можливостям забезпечення цілісності даних, снапшотів та вбудованої підтримки RAID. ZFS використовує copy-on-write механізм, що забезпечує консистентність даних навіть при раптових відключеннях живлення. Система автоматично виявляє та виправляє помилки читання через перевірку всіх блоків даних.

Переваги ZFS включають вбудовану компресію (LZ4, GZIP), що може зменшити займаний простір на 20-40 %, де дуплікацію однакових блоків даних, миттєві бекапи для резервного копіювання та можливість створення зашифрованих datasets. Система підтримує різні рівні RAID (Mirror, RAIDZ1/2/3) без необхідності апаратного RAID контролера.

Порівняно з традиційними файловими системами, ext4 забезпечує високу продуктивність та стабільність, але не має розширених функцій ZFS. NTFS підходить для сумісності з Windows, але в Linux середовищі працює через додаткові драйвери з можливими обмеженнями продуктивності. Btrfs надає деякі функції ZFS, але має менш зрілу реалізацію та може бути менш стабільною під навантаженням.

Планування структури зберігання даних має враховувати різні типи контенту та їх особливості доступу. Документи та фотографії вимагають надійного зберігання з регулярним резервним копіюванням, відео-контент потребує великого об'єму та високої швидкості читання.

Для типової домашньої мережі з 3-4 користувачами рекомендується планувати 2-4 ТБ для основного зберігання плюс 25-50 % додатково для резервних копій. Швидкість послідовного читання повинна становити не менше 80-100 МБ/с для комфортної роботи з великими файлами. Для цього проекту був використаний SSD накопичувач розміром 512 GB.

2.3 Вибір операційної системи та базового програмного забезпечення

Proxmox Virtual Environment (VE) була обрана як основна платформа віртуалізації для проекту. Proxmox VE являє собою відкриту платформу віртуалізації на базі Debian, що поєднує KVM для повної віртуалізації та LXC для контейнерів. Система надає потужний веб інтерфейс для управління віртуальними машинами, контейнерами, мережами та сховищами даних.

Переваги Proxmox включають централізоване управління всіма сервісами через єдиний інтерфейс, можливість живої міграції віртуальних машин, вбудовану підтримку кластеризації та автоматичне резервне копіювання. Система підтримує різні типи сховищ, включаючи ZFS, що робить її ідеальним вибором для даного проекту.

Proxmox VE була обрана як основна платформа для проекту через її унікальні можливості централізованого управління інфраструктурою. Система

дозволяє розгортати різні NAS рішення у вигляді віртуальних машин або LXC контейнерів, забезпечуючи ізоляцію сервісів та спрощуючи експериментування з різними конфігураціями.

Критерії оцінки включали можливість ефективного використання ZFS на рівні сервера (Proxmox підтримує ZFS), централізоване управління ресурсами та сервісами через веб інтерфейс, можливість швидкого відновлення системи через бекапи віртуальних машин та docker контейнерів. Споживання оперативної пам'яті Proxmox становить приблизно 1 ГБ RAM, залишаючи достатньо ресурсів для віртуальних сервісів.

Додатковими перевагами є вбудована система резервного копіювання Proxmox Backup Server, підтримка кластеризації для майбутнього розширення системи та велика спільнота користувачів з детальною документацією. Система також дозволяє легко мігрувати сервіси між різними конфігураціями без переналаштування базової ОС.

Альтернативні рішення типу прямого встановлення NAS систем на голі залізо обмежують гнучкість та ускладнюють тестування нових функцій, тоді як Proxmox дозволяє паралельно запускати декілька NAS-рішень для порівняння їх можливостей.

2.4 Мережеві технології та протоколи доступу

Конфігурація мережевих інтерфейсів здійснюється через Network Manager для динамічного отримання IP адреси або через статичне призначення для стабільної роботи сервера. Рекомендується використання статичної IP адреси з діапазону локальної мережі (наприклад, 192.168.0.100) для спрощення доступу клієнтів.

Wi-Fi інтерфейс налаштовується як резервний канал зв'язку або для початкового налаштування системи без доступу до Ethernet. Використання 5 ГГц діапазону забезпечує кращу продуктивність, але вимагає близького розташування до роутера через меншу дальність дії сигналу.

Firewall налаштовується через `ufw` (Uncomplicated Firewall) з дозволом лише необхідних портів: 22 (SSH), 445 (SMB), 2049 (NFS), 21 (FTP), 80/443 (HTTP/HTTPS). Додатково обмежується доступ SSH лише з локальної мережі та налаштовується `fail2ban` для автоматичного блокування після невдалих спроб входу.

WireGuard VPN налаштовується для безпечного віддаленого доступу до NAS з мобільних пристроїв та з офісу. Генеруються унікальні ключі для кожного клієнта з можливістю швидкого відкликання доступу. Конфігурація включає маршрутизацію лише трафіку до локальної мережі для збереження пропускну здатності інтернет-каналу.

SSL/TLS сертифікати генеруються через Let's Encrypt для HTTPS доступу до веб інтерфейсу або створюються само підписані для внутрішнього використання. Налаштовується автоматичне оновлення сертифікатів та перенаправлення HTTP трафіку на HTTPS.

2.5 Додаткові сервіси та їх інтеграція

Pi-hole розгортається як окремий LXC контейнер в Proxmox VE для забезпечення ізоляції та легкості управління. Контейнер налаштовується з виділеними ресурсами (512 МБ RAM, 1 CPU) та статичною IP адресою в локальній мережі. Така конфігурація дозволяє Pi-hole функціонувати незалежно від основних NAS сервісів та забезпечує можливість швидкого відновлення через бекапи.

Архітектура Pi-hole включає `dnsmasq` як основний DNS сервер з підтримкою кешування, `lighttpd` веб сервер для інтерфейсу адміністрування та SQLite базу даних для зберігання налаштувань та статистики. Система налаштовується як основний DNS сервер для всієї локальної мережі через DHCP налаштування роутера або можна налаштувати вручну для ПК підключеної до мережі в якій знаходиться Raspberry Pi.

Інтеграція з мережевою інфраструктурою включає налаштування Pi-hole як upstream DNS для локальних доменів (.local, .lan) та використання зовнішніх DNS серверів (Cloudflare 1.1.1.1, Google 8.8.8.8) для публічних доменів. Налаштовується conditional forwarding для коректного відображення локальних адрес у статистиці.

Списки блокування включають регулярно оновлюванні фільтри: StevenBlack's Unified Hosts List (реклама та шкідливі домени), AdGuard, DNS фільтер, EasyList та регіональні фільтри для україномовного контенту. Система автоматично оновлює списки щотижня та підтримує власні чорні та білі списки для тонкого налаштування фільтрації.

РОЗДІЛ 3

ПРОЕКТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖЕВОГО СХОВИЩА

3.1 Підготовка апаратної платформи та початкове встановлення

Для початку необхідно зібрати наш пристрій і встановити базову операційну систему на якій буде базуватись все наступне налаштування мережевого сховища.

3.1.1 Підготовка Raspberry Pi та периферійних пристроїв

Перед початком встановлення програмного забезпечення необхідно підготувати апаратну платформу. Були придбані всі компоненти потрібні для проекту, а саме:

- Raspberry Pi 5 (8 GB RAM);
- активне охолодження;
- адаптер PCIe to 2 x M.2 HAT+;
- microSD 128 GB;
- SSD 512GB.

В результаті отримали вже готовий для налаштування пристрій (рис. 3.1).



Рисунок 3.1 – Зібраний Raspberry Pi пристрій

3.1.2 Встановлення Raspberry Pi OS

Встановлення операційної системи виконується з використанням офіційного інструменту «Raspberry Pi Imager». Обирається «Raspberry Pi OS Lite (64-bit)» як базова система без графічного інтерфейсу для оптимального використання ресурсів.

Процес встановлення включає завантаження та запуск Raspberry Pi Imager на комп'ютері, вибір образу «Raspberry Pi OS Lite (64-bit)» з офіційного репозиторію та вибір цільового диску як носія для встановлення (рис. 3.2). В розширених налаштуваннях конфігуруються початкові параметри: увімкнення SSH доступу з налаштуванням автентифікації за ключами, створення користувача з безпечним паролем, налаштування WiFi мережі за потреби та встановлення часового поясу Europe/Київ.

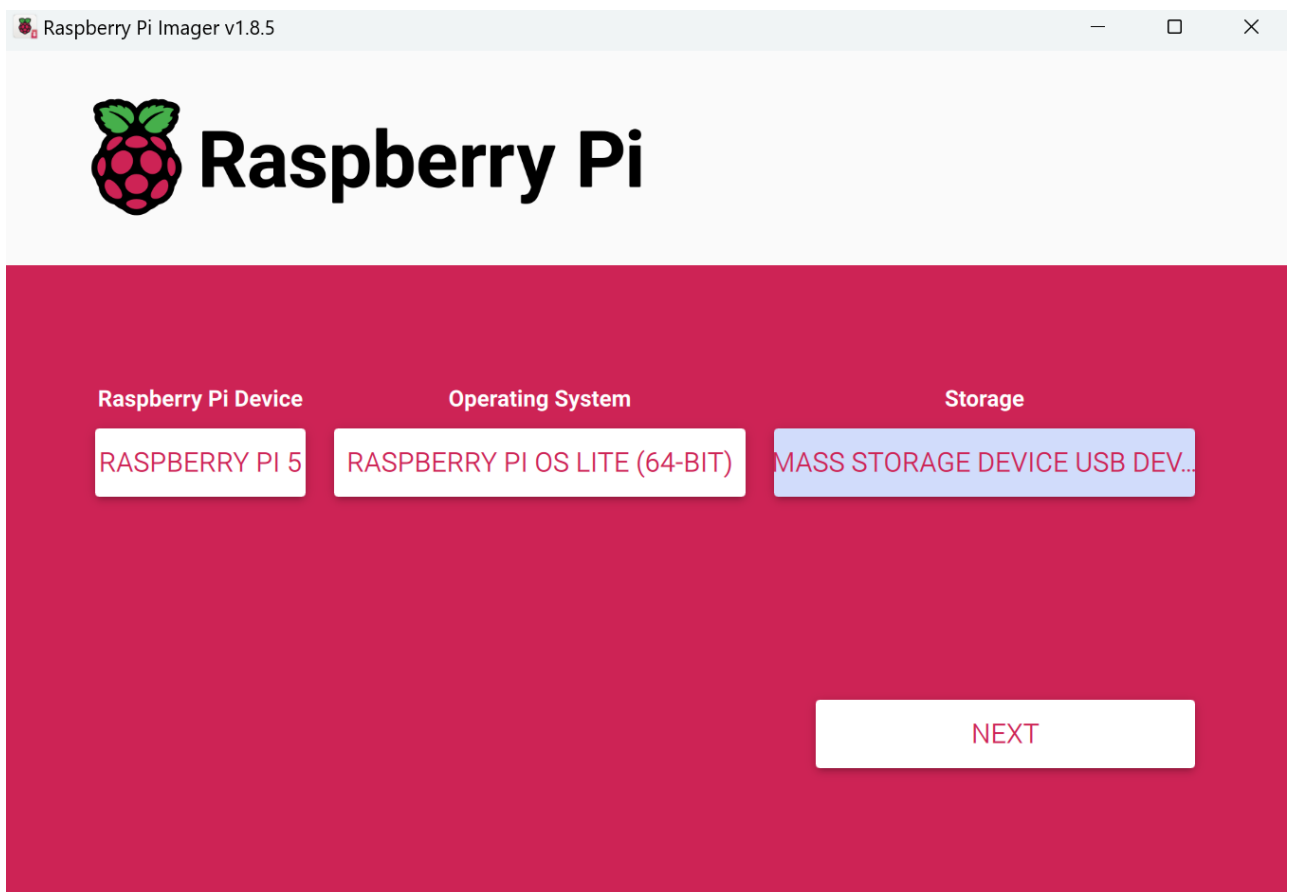


Рисунок 3.2 – Базові налаштування Raspberry Pi Imager

Після завершення запису образу на диск, система готова до першого запуску. Перший запуск супроводжується автоматичним розширенням файлової системи на весь доступний обсяг диску та виконанням початкових налаштувань безпеки.

3.1.3 Конфігурація статичної IP адреси

Перед налаштуванням статичної IP адреси [10] необхідно проаналізувати поточну мережеву конфігурацію системи. Виконується збір інформації про мережевий інтерфейс, шлюз за замовчуванням та DNS сервери.

Для отримання інформації про поточний шлюз виконується команда «`ip r | grep default`» (рис. 3.3).

```
vinvit@vrpi:~ $ ip r | grep default
default via 192.168.0.1 dev eth0 proto dhcp src 192.168.0.90 metric 100
vinvit@vrpi:~ $
```

Рисунок 3.3 – Результат виконання команди «`ip r`»

В результаті виконання даної команди ми отримуємо такі дані:

- адреса роутера: 192.168.0.1;
- адреса Raspberry Pi: 192.168.0.90.

Для забезпечення стабільного мережевого підключення та передбачуваності доступу до сервісів налаштовується статична IP адреса. Використовується метод конфігурації через графічний інтерфейс Network Manager, потрапити до якого можна за допомогою команди «`nmtui`» (рис. 3.4).

В інтерфейсі перейшовши до налаштування інтернет з'єднання потрібно ввести наші нові налаштування. В поле «Addresses» вводимо нову статичну ip адресу «192.168.0.100», в поле «Gateway» адресу роутера, в «DNS servers» заповнюємо адресами DNS серверів Cloudflare і Google.

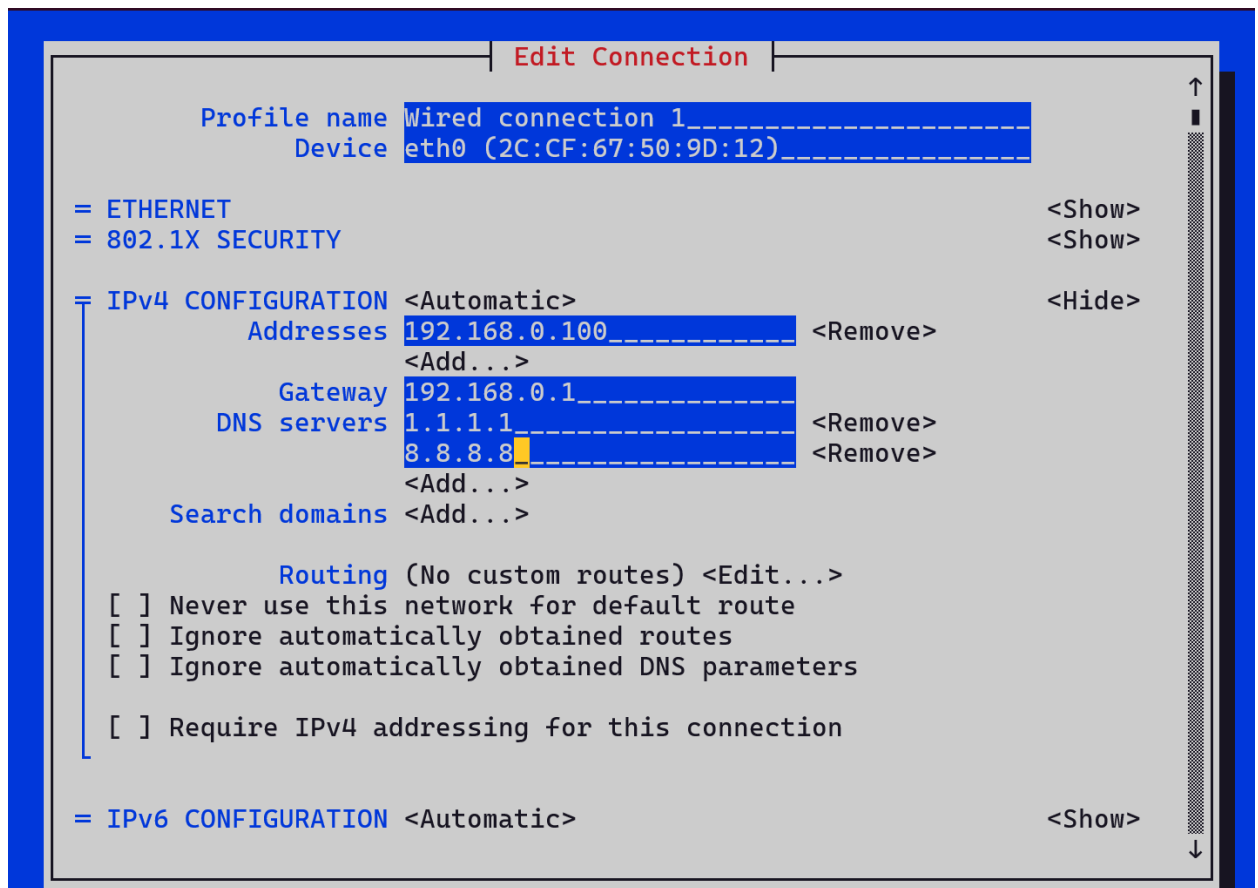


Рисунок 3.4 – Налаштування інтернет підключення

Для застосування змін потрібно перезавантажити пристрій командою «`sudo reboot`». В результаті таких налаштувань наш пристрій отримав статичну ір адресу в поточній мережі а саме 192.168.0.100. Перевірити це можна повторно використавши команду «`ip r | grep default`».

Після налаштування статичної IP адрису пристрою в локальній мережі можна приступати до встановлення Proxmox VE та налаштування інших систем для мережевого сховища.

3.2 Встановлення та налаштування Proxmox VE

Proxmox VE буде основною системою через яку буде відбуватись налаштування всіх сервісів на Raspberry Pi, необхідних для роботи мережевого сховища. Перед початком роботи над наступними кроками потрібно переконатись що він встановлений і налаштований вірно.

3.2.1 Підготовка системи до встановлення Proxmox VE

Перед встановленням Proxmox VE [11] необхідно підготувати операційну систему, оновити пакети та налаштувати репозиторії. Цей етап критично важливий для забезпечення стабільної роботи гіпервізора.

Оновлення системних пакетів здійснюється послідовним виконанням команд «update» і «upgrade» пакетного менеджера apt. Також встановлюються необхідні утиліти curl, wget та gpg.

Proxmox вимагає коректного налаштування системного імені хосту та його розв'язування через локальну IP адресу. Це налаштування виконується в системному файлі «hosts» заміною стандартного запису на конфігурацію, що включає локальну IP адресу та ім'я хосту (лістинг 3.1).

Лістинг 3.1 – Налаштування системного імені хосту

127.0.0.1	localhost
::1	localhost ip6-localhost ip6-loopback
ff02::1	ip6-allnodes
ff02::2	ip6-allrouters.1
192.168.1.100	vrpi
127.0.0.1	vrpi

кінець лістингу 3.1

3.2.2 Налаштування мережевих інтерфейсів

Наступним кроком буде створення нового мережевого інтерфейсу, який буде виступати мостом між з'єднанням «eth0» і віртуальними машинами Proxmox. Дане налаштування відбувається в файлі «/etc/network/interfaces» (лістинг 3.2). В цьому файлі ми прописуємо нове з'єднання «vmbri0», в ньому так само як в нашому «eth0» підключення прописуємо address (раніше заданий статичний ip) і gateway (ip роутера) що нам вже відомі.

Щоб ці зміни застосувались нам знову потрібно перезапустити пристрій.

Лістинг 3.2 – Налаштування мережевих інтерфейсів

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet manual

auto vmbro0
iface vmbro0 inet manual
    address 192.168.0.100
    gateway 192.168.0.1
    netmask 255.255.255.0
    bridge-ports eth0
    bridge-stp off
    bridge-fd 0
```

кінець лістингу 3.2

3.2.3 Встановлення Proxmox VE

Встановлення основних пакетів Proxmox здійснюється командою «install» для встановлення пакетів: proxmox-ve, postfix, open-iscsi, pve-edk2-firmware-aarch64. Попередньо в пакетний менеджер потрібно додати репозиторій що містить ці пакети. Їх можна знайти в документації на офіційному сайті Proxmox.

Під час встановлення буде запропоновано налаштувати Postfix, де рекомендується обрати «Local only» для локального використання та залишити системне ім'я за замовчуванням. Після завершення встановлення необхідно знову перезавантажити пристрій для застосування змін і запуску Proxmox.

Після перезавантаження Proxmox стає доступним через веб-інтерфейс за адресою «192.168.0.100:8006» (рис. 3.5). Для входу використовуються наступні параметри: Ім'я користувача: root, та Пароль для root користувача встановлений в Raspberry Pi OS.

В боковій панелі можна побачити список пристроїв та дисків що підключені і можуть налаштовуватись через Proxmox VE. Так до прикладу вибравши пристрій «vbr1», що є нашим Raspberry Pi можна відкрити «Summary» для перегляду статистики використання та навантаження нашого пристрою.

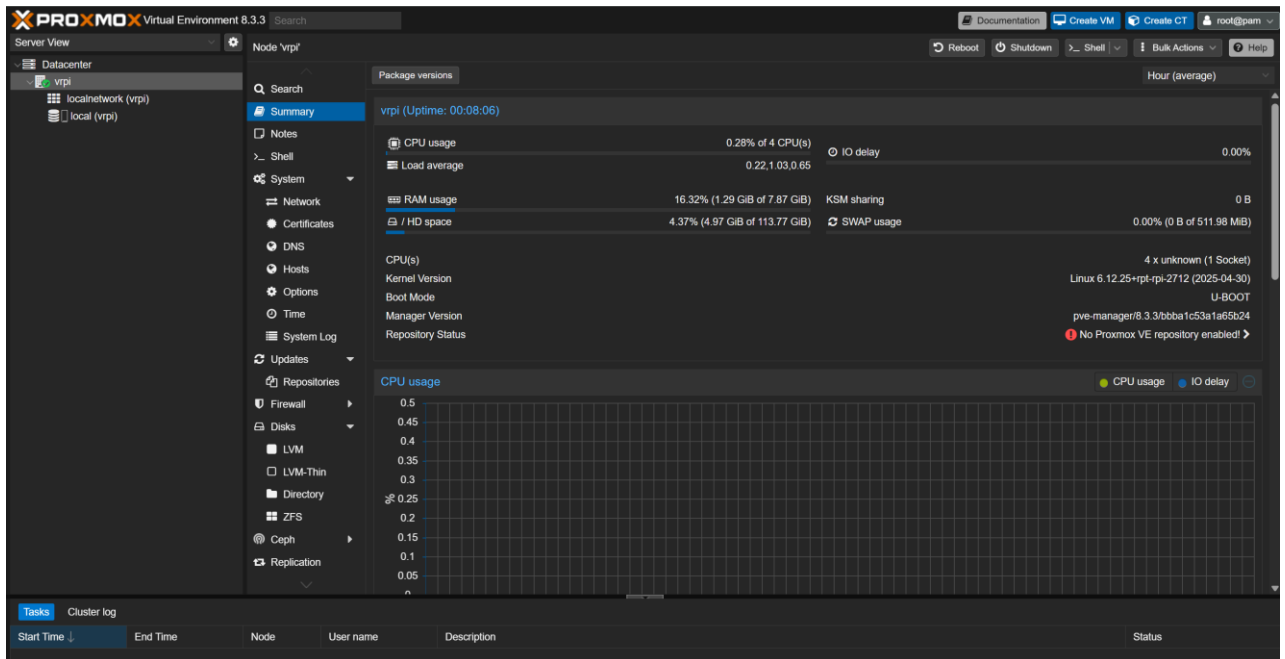


Рисунок 3.5 – Веб інтерфейс Прохтох

3.3 Розгортання Pi-hole в LXC контейнері

Створення нового LXC контейнера для Pi-hole виконується в веб інтерфейсі Прохтох [12]. Використовується шаблон Ubuntu 20.04 як стабільна база для DNS сервера. Параметри контейнера включають CT ID: 100, Hostname: pihole, режим Unprivileged container, розмір диску 4 GB, 1 ядро процесора, 512 MB оперативної пам'яті, мережа vmbr0 зі статичною IP 192.168.0.101/24, шлюз 192.168.0.1 та автозапуск при завантаженні системи (рис. 3.6). Як шаблон для LXC контейнера був використаний «Ubuntu 20.04» попередньо завантажений до Прохтох «CT Templates». Тут важливо зазначити що потрібен саме «arm64» контейнер інші види (x64, x86_64, AMD) не будуть працювати через не сумісність з процесором Raspberry Pi.

Після створення контейнера виконується його запуск та початкове налаштування. Вхід до консолі контейнера здійснюється через Прохтох або SSH за адресою 192.168.0.101.

Завантаження та запуск офіційного інсталяційного скрипта Pi-hole здійснюється командою «wget -O basic-install.sh https://install.pi-hole.net | sudo

bash basic-install.s». Під час встановлення система запропонує низку налаштувань: вибір мережевого інтерфейсу, налаштування DNS серверів (1.1.1.1, 8.8.8.8) встановлення веб інтерфейсу, встановлення веб сервера lighttpd, увімкнення логування запитів та встановлення рівня приватності «Show everything».

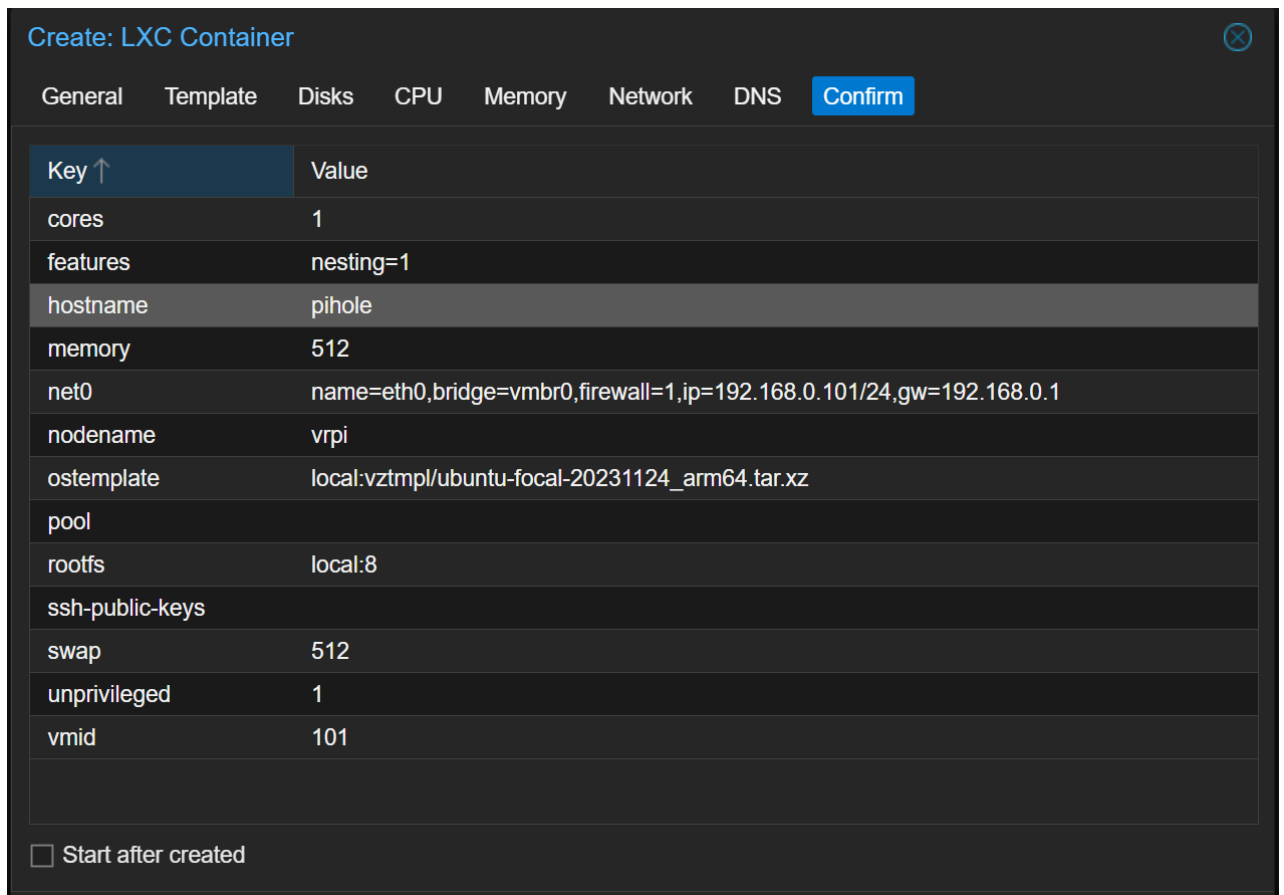


Рисунок 3.6 – Налаштування контейнера для Pi-hole

Після встановлення ми можемо отримати доступ до веб інтерфейсу Pi-hole за перейшовши за адресою «192.168.0.101:80/admin» в браузері. З цього інтерфейсу можна переглядати налаштування Pi-hole, додавати нові адреси через налаштування локальних DNS записів. Блокувати трафік, та переглядати статистику використання трафіку [13].

Щоб розпочати використовувати Pi-hole добавимо його ip адресу як основий DNS сервер в налаштуваннях підключення до Wi-fi на іншому пристрої

в мережі. Відразу після цього можна побачити як Pi-hole розпочав роботу (рис. 3.7).

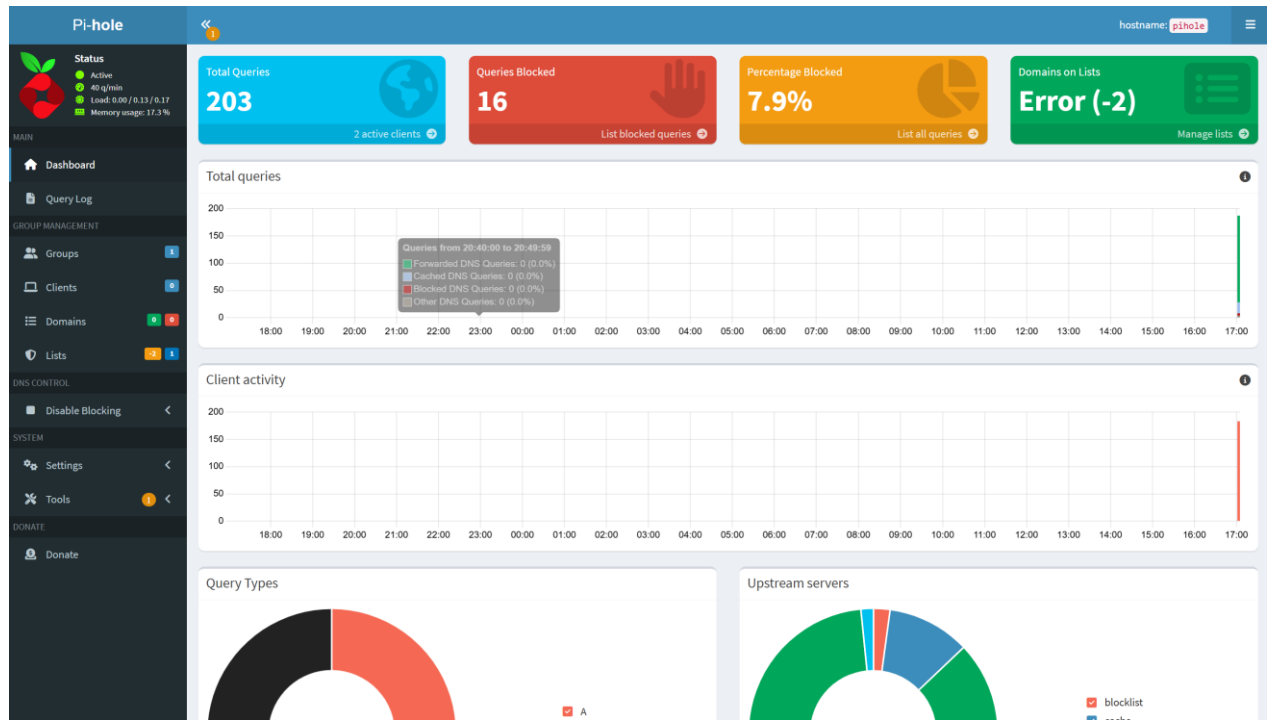


Рисунок 3.7 – Веб інтерфейс Pi-hole

3.4 Конфігурація ZFS файлової системи

ZFS [14] надає розширені можливості для управління даними, включаючи snapshots, compression та перевірку цілісності. Конфігурація виконується для SSD диску 512 GB.

Для початку роби з ZFS потрібно встановити пакет `zfsutils-linux` на хості Proxmox яким виступає Raspberry Pi OS. Визначення доступних дисків здійснюється командами «`lsblk`» (рис. 3.8) та «`fdisk-l`» для аналізу структури підключених накопичувачів.

Створення ZFS пулу з одного диску виконується командою «`zpool create storage /dev/nvme0n1-f`». Увімкнення compression для економії місця здійснюється командою «`zfs set compression=lz4 storage`». Додатково налаштовуються параметри оптимізації: вимкнення `atime` командою «`zfs set atime=off storage`», увімкнення `relatime` командою «`zfs set relatime=on storage`».

Створення окремих файлових систем для різних типів даних включає наступні команди: для користувацьких даних «zfs create storage/user_data» та для резервних копій «zfs create storage/backups» (рис. 3.9).

Додавання ZFS пулу до Proxmox як сховища даних здійснюється через веб інтерфейс в розділі «Datacenter» – «Storage» – «Add» – «ZFS» з параметрами: ID встановлюється як zfs-storage, ZFS Pool вказується як storage, а Content включає Container та Disk image.

```
vinvit@vrpi:~ $ lsblk
NAME                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
mmcblk0             179:0    0 116.1G  0 disk
├─mmcblk0p1         179:1    0   512M  0 part /boot/firmware
└─mmcblk0p2         179:2    0 115.6G  0 part /
nvme0n1             259:0    0 476.9G  0 disk
└─nvme0n1p1        259:1    0 476.9G  0 part
vinvit@vrpi:~ $
```

Рисунок 3.8 – Результат виконання команди «lsblk»

```
vinvit@vrpi:~ $ zfs list
NAME                USED   AVAIL   REFER  MOUNTPOINT
storage             170K   461G    24K    /storage
storage/backups     24K    461G    24K    /storage/backups
storage/user_data   24K    461G    24K    /storage/user_data
vinvit@vrpi:~ $
```

Рисунок 3.9 – Список створених файлових систем

3.5 Встановлення та налаштування OpenMediaVault

Тепер можна приступити до встановлення інтерфейсу для керування зберіганням файлів. Як систему для керування файлами будемо використовувати OpenMediaVault.

3.5.1 Створення віртуальної машини для OpenMediaVault

Створення нової віртуальної машини в Proxmox для OpenMediaVault виконується з наступними параметрами: VM ID 101, Name «openmediavault»,

CPU 2 cores, Memory 2048 MB, Hard Disk 32 GB на ZFS пулі, та CD/DVD з ISO образом OpenMediaVault (рис. 3.10).

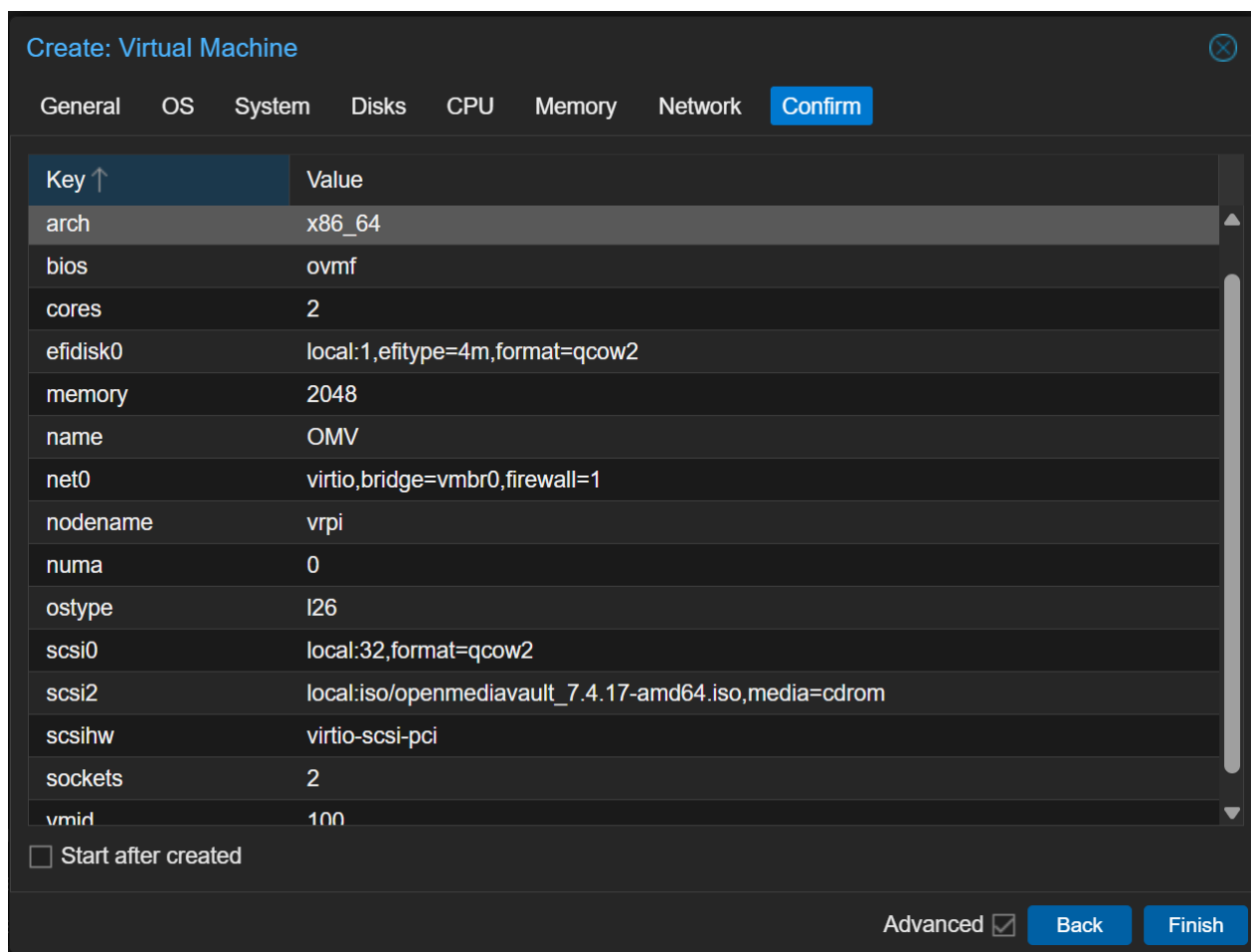


Рисунок 3.10 – Налаштування віртуальної машини OpenMediaVault

3.5.2 Встановлення та налаштування OpenMediaVault

Завантаження ISO образу OpenMediaVault 6 здійснюється з офіційного сайту та завантажується в Proxmox. Стандартне встановлення виконується через графічний інсталятор (рис. 3.11) з вибором мови English, розмітки системного диску «Guided – use entire disk», створення користувача root та налаштування мережі зі статичною IP 192.168.1.102.

Доступ до веб інтерфейсу OpenMediaVault здійснюється за адресою «openmediavault.local» з використанням стандартних доступів: ім'я користувача «admin» та пароль «openmediavault» (рис. 3.12).

Додавання додаткового віртуального диску для даних виконується в Proxmox шляхом додавання нового диску до VM (наприклад, 400 GB з ZFS пулу) [15]. В OMV через розділ Storage → Disks виявляється новий диск, після чого в «Storage» – «File Systems» створюється ext4 файлова система та виконується монтування файлової системи.

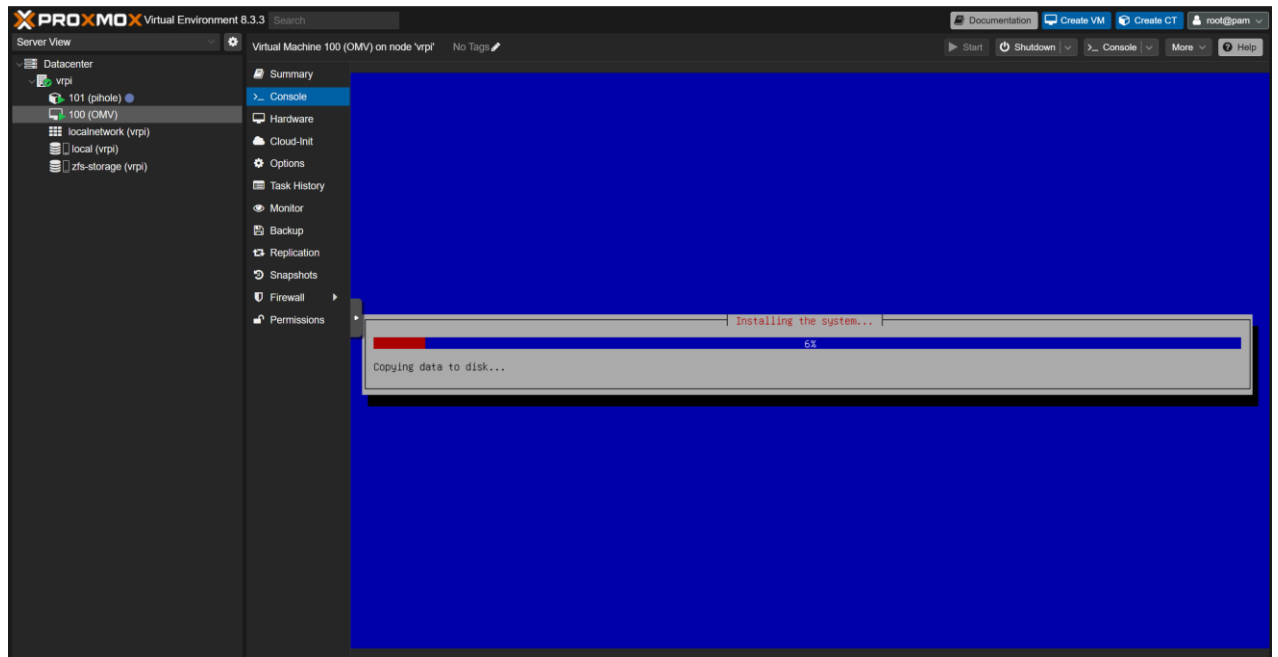


Рисунок 3.11 – Процес встановлення OpenMediaVault

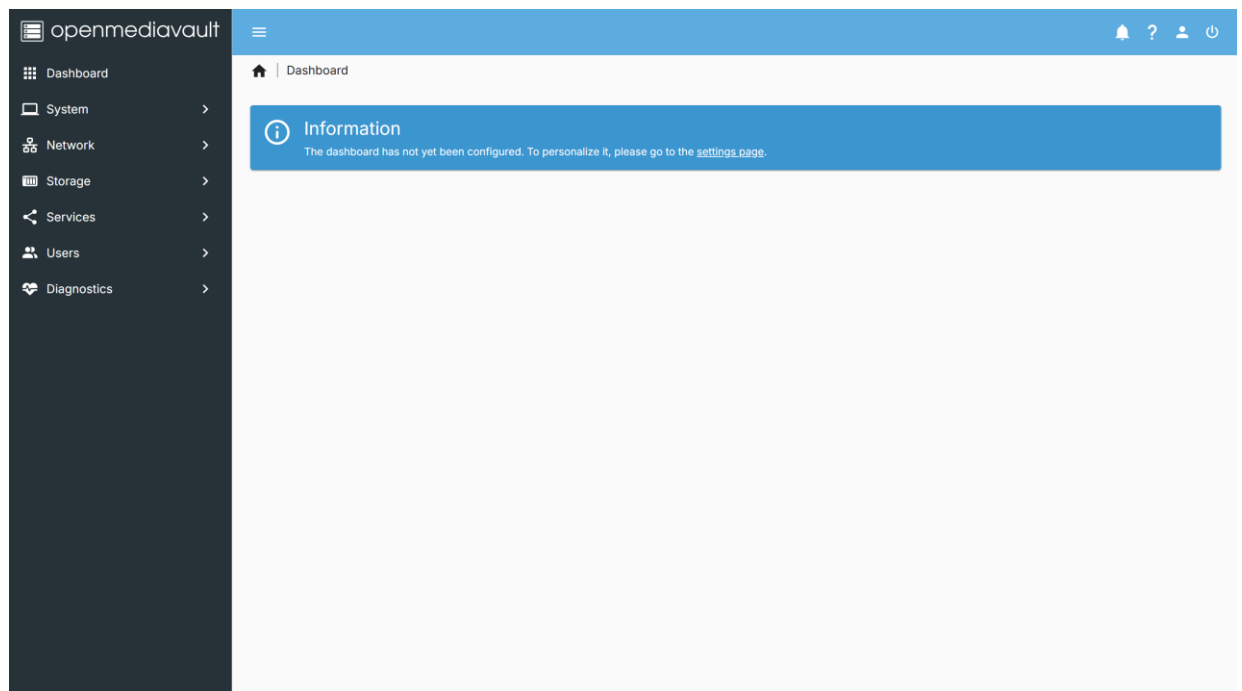


Рисунок 3.12 – Веб інтерфейс OpenMediaVault

Після монтування потрібно створи публічну папку яку зможуть використовувати інші користувачі та плагіни.

Далі можна встановлювати додаткові плагіни для роботи з OpenMediaVault.

Встановити плагіни можна через інтерфейс «System» – «Plugins», тут потрібно вибирати які саме плагіни потрібно встановити і натиснути кнопку для інсталяції. Для доступу до файлової системи через браузер потрібно встановити «File Browser». Після встановлення в конфігураціях плагіна (рис. 3.13) потрібно задати порт за яким він буде працювати, та публічну папку створену в OpenMediaVault. Після застосування змін переходимо за новим посиланням «openmediavault.local:3670», де знаходиться новий веб інтерфейс (рис. 3.14) звідки вже можна завантажувати та переглядати файли з нашого Raspberry Pi пристрою.

Також даний плагін підтримує функцію спільного користування файлами (File Sharing), можна розповсюдити файл або папку за допомогою посилання, або створити окремого користувача, що буде мати доступ до усіх файлів.

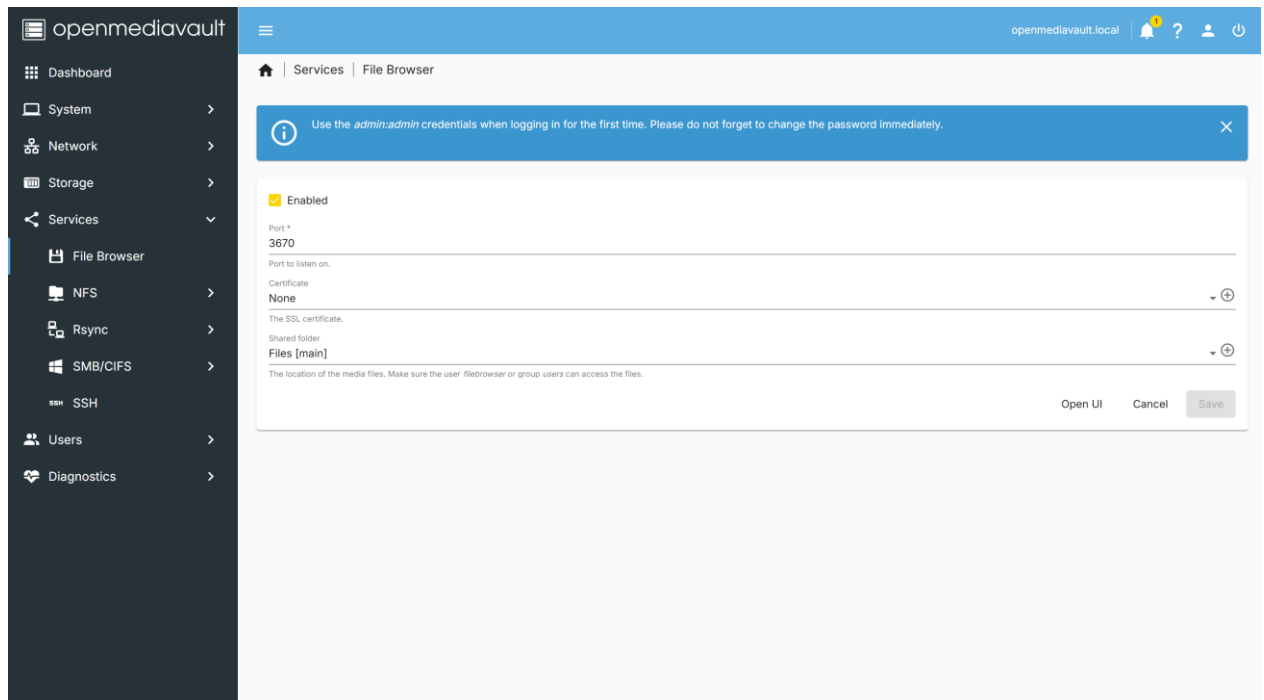


Рисунок 3.13 – Налаштування плагіна «File Browser»

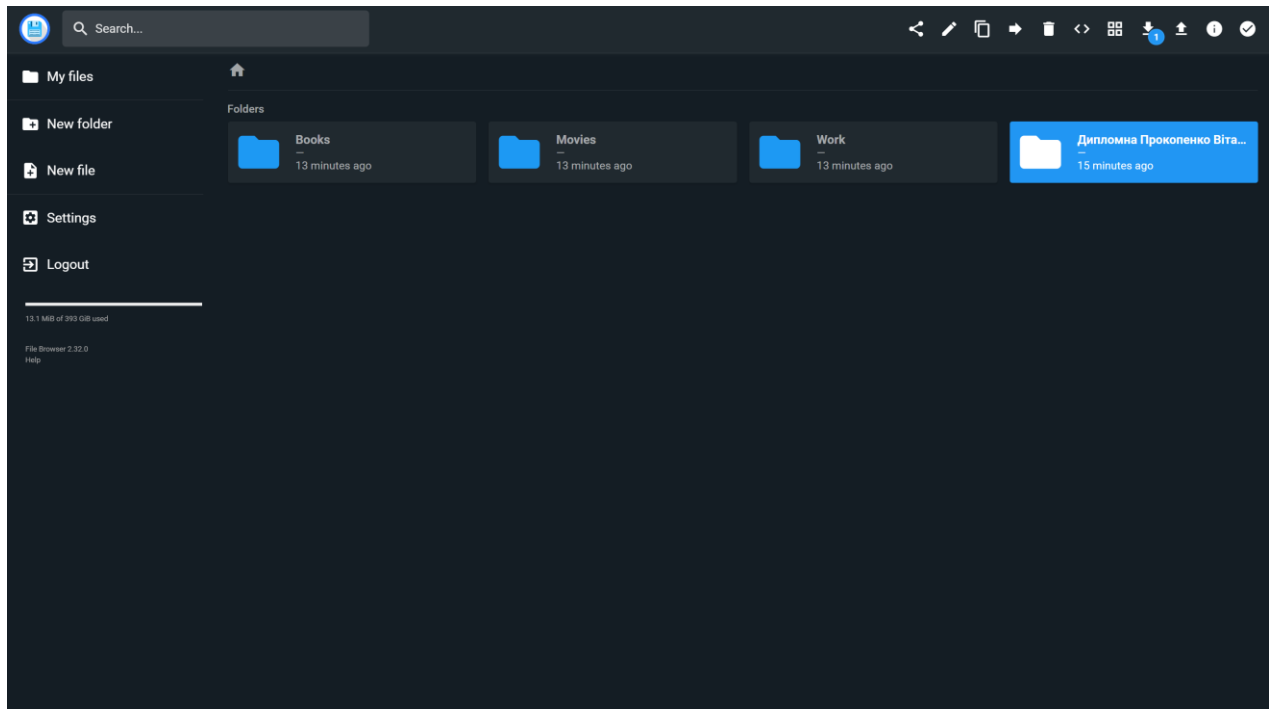


Рисунок 3.14 – Веб інтерфейс «File Browser»

Також варто зазначити що це не єдиний функціонал OpenMediaVault, для нього є десятки якщо не сотні створених розширень, що додають багато можливостей роботи з файлами та файловою системою пристрою. До прикладу можливо розповсюдити файли за допомогою NFS, Samba, відкрити доступ через FTP чи SSH сервіси. Все це супроводжується гнучкою системою керування користувачами, групами користувачів та правилами доступу для них.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи була успішно розроблена та реалізована система мережевого сховища даних на основі одноплатного комп'ютера Raspberry Pi 5, що підтверджує актуальність обраного напрямку дослідження та ефективність запропонованого підходу.

Виконання поставлених завдань. Аналіз сучасних підходів до організації мережевих сховищ показав, що традиційні комерційні NAS-рішення характеризуються високою вартістю (від 8-12 тис. грн. за базові моделі) та надмірною функціональністю для домашнього використання. Відкриті програмні рішення, хоча і безкоштовні, вимагають значних технічних знань для налаштування та обслуговування. Дослідження технічних характеристик платформи Raspberry Pi 5 виявило її придатність для створення мережевого сховища завдяки 64-бітному чотириядерному ARM Cortex-A72 процесору з частотою 2,4 ГГц, до 8 ГБ RAM, наявності PCIe 2.0 слоту для високошвидкісних накопичувачів та енергоспоживанню 8-12 Вт, що у 3-5 разів менше від традиційних серверних рішень. Проектування та реалізація мережевого сховища включила використання Proxmox VE як платформи віртуалізації, ZFS файлової системи для забезпечення цілісності даних та OpenMediaVault як веб інтерфейсу управління. Додатково було інтегровано Pi-hole для забезпечення мережевої безпеки, що демонструє можливість створення комплексної домашньої IT інфраструктури на базі одного пристрою.

Досягнення мети дослідження. Розроблене мережеве сховище забезпечує економічну ефективність з загальною вартістю рішення приблизно 5-7 тис. грн, що у 2-3 рази менше від комерційних аналогів. Продуктивність системи характеризується пропускною здатністю до 5 ГБ/с через PCIe інтерфейс, що забезпечує достатню швидкість для домашнього використання. Надійність гарантується використанням ZFS файлової системи з вбудованою перевіркою цілісності та можливістю створення снапшотів. Гнучкість рішення проявляється

у можливості розширення функціональності через додаткові сервіси та контейнеризацію.

Практична застосовність. Реалізоване рішення підходить для домашніх користувачів, які потребують централізованого зберігання мультимедійних файлів, малих офісів з обмеженим бюджетом на ІТ інфраструктуру, освітніх цілей для вивчення мережевих технологій та систем зберігання даних, а також для прототипування більших корпоративних рішень.

Наукова новизна. Робота демонструє комплексний підхід до використання одноплатних комп'ютерів у якості основи для мережевої інфраструктури, поєднуючи функції NAS, DNS сервера та системи віртуалізації в єдиному енергоефективному рішенні. Використання ZFS на ARM архітектурі та інтеграція Pi-hole з Proxmox VE представляють інноваційний підхід до побудови домашніх ІТ систем.

Перспективи подальшого розвитку. Подальше вдосконалення системи може включати інтеграцію додаткових сервісів (VPN сервер, медіа центр, система моніторингу), розширення до кластерної конфігурації з використанням декількох Raspberry Pi, імплементацію автоматизованого резервного копіювання в хмарні сховища та розробку мобільного додатку для управління системою.

Результати роботи підтверджують гіпотезу про можливість створення ефективного та економічно вигідного мережевого сховища на базі одноплатного комп'ютера Raspberry Pi, що робить сучасні технології зберігання даних доступними для широкого кола користувачів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is NAS Storage? – Network–Attached Storage Explained – AWS. Amazon Web Services, Inc. URL: <https://aws.amazon.com/what-is/nas/> (дата звернення: 15.02.2025).
2. Synology DS224+ – Мережеве сховище Intel Celeron J4125 4 ядра 2x3,5"/2,5" DDR4 1GbE. Comtrade – постачальник мережевого обладнання. URL: <https://comtrade.ua/ua/synology-ds224/> (дата звернення: 20.02.2025).
3. QNAP TS-216G – Мережеве сховище, десктопне, ARM Cortex A55, 4 ядра, 4ГБ. Comtrade – постачальник мережевого обладнання. URL: <https://comtrade.ua/ua/qnap-ts-216g/> (дата звернення: 21.02.2025).
4. NAS-сервер WD My Cloud Home 2TB. Comtrade – постачальник мережевого обладнання. URL: <https://comtrade.ua/ua/nas-server-wd-my-cloud-home-2tb/> (дата звернення: 22.02.2025).
5. Купити Мікрокомп'ютер Raspberry Pi 4 Model B 8GB - evo.net.ua. Інтернет магазин мікрокомп'ютерів та аксесуарів. URL: <https://evo.net.ua/mikrokomputer-raspberry-pi-4-model-b-8gb/> (дата звернення: 24.03.2025).
6. Мікрокомп'ютер Raspberry Pi 5 Board 8GB. Інтернет магазин мікрокомп'ютерів та аксесуарів. URL: <https://evo.net.ua/mikrokompiuter-raspberry-pi-5-board-8gb> (дата звернення: 25.03.2025).
7. Garth A. Gibson, Rodney Van Meter Using a Raspberry Pi as a Network-Attached Storage Device: Performance and Limitations. ACMSE 2025: Proceedings of the 2025 ACM Southeast Conference, 8 травня 2025 р. м. Луцьк, 2025. С. 67-77.
8. Кулер Waveshare для Raspberry Pi 5 активний: ціна, опис, характеристики. RC-НОББУ. URL: <https://rc-hobby.com.ua/bortovi-komputeri/wvs-25939/> (дата звернення: 05.04.2025).
9. Адаптер PCIe to 2 x M.2 NAT+ для Raspberry Pi 5 сумісний з NVME розміром 2280/2260/2242/2230 купити в Києві та Україні. Arduino в Україні. URL:

<https://arduino.ua/prod7354-adapter-pcie-to-2-h-m-2-hat-dlya-raspberry-pi-5-symisnii-z-nvme-rozmirom-2280226022422230> (дата звернення: 06.04.2025).

10. How to setup a raspberry pi static IP address. Pi My Life Up. URL: <https://pimylifeup.com/raspberry-pi-static-ip-address/> (дата звернення: 10.04.2025).

11. Installing proxmox on the raspberry pi. Pi My Life Up. URL: <https://pimylifeup.com/raspberry-pi-proxmox/> (дата звернення: 11.04.2025).

12. Proxmox VE Administration Guide. Proxmox VE. URL: <https://pve.proxmox.com/pve-docs/pve-admin-guide.html> (дата звернення: 13.04.2025).

13. Delimarsky D. The Beauty Of Having A Pi-hole Den Delimarsky. Den Delimarsky - Principal Product Engineer, Tinkerer, Nerd, Trail Explorer. URL: <https://den.dev/blog/pihole/> (дата звернення: 14.04.2025).

14. Kirvan P., Sliwa C. What Is ZFS? | Definition from TechTarget. Search Storage. URL: <https://www.techtarget.com/searchstorage/definition/ZFS> (дата звернення: 20.04.2025).

15. ZFS on Linux – Proxmox VE. Proxmox VE. URL: https://pve.proxmox.com/wiki/ZFS_on_Linux (дата звернення: 21.04.2025).

16. Міжнародна науково-практична конференція молодих вчених та студентів «Програмне та апаратне забезпечення в інформаційних технологіях». URL: <https://conference.net.ua/> (дата звернення: 19.05.2025).

17. Прокопенко В., Лавренчук С. Віртуалізація сервісів на NAS системі з використанням Raspberry Pi 5 та Proxmox. *Програмне та апаратне забезпечення в інформаційних технологіях*: матеріали Міжнар. Науково- практ. конф., м. Луцьк, 6 травня 2025 р. м. Луцьк, 2025. С. 164-166.