МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

АПАРАТНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ

Виконав: студент групи 2К-21
Спеціальності 123 Комп’ютерна інженерія
Матвій ЯЦЕНКО
Керівник:
Маргарита МЕДОЛИЗ

Черкаси 2025

АНОТАЦІЯ

У кваліфікаційній роботі розглядається розробка бюджетної системи мережевої безпеки для малих комп'ютерних мереж на базі одноплатного мікрокомп'ютера Raspberry Pi. Актуальність дослідження зумовлена зростанням кіберзагроз та потребою у доступних, ефективних рішеннях для малого бізнесу та домашніх користувачів. Основну увагу приділено поєднанню функціоналу фаєрвола та системи виявлення/запобігання вторгненням Snort 3. У роботі проведено теоретичний аналіз загроз, апаратних засобів захисту та огляд сучасних рішень для малих мереж. Експериментальна частина охоплює моделювання мережі у Packet Tracer, розгортання захисної системи у середовищі VirtualBox та конфігурування компонентів безпеки на базі Kali Linux. Робота демонструє можливість створення ефективної та економічно доцільної захисної системи, придатної для практичного застосування у реальних умовах.

ABSTRACT

This qualification work explores the development of a budget-friendly network security system for small-scale computer networks using a single-board microcomputer. Raspberry Pi. The relevance of the research lies in the growing number of cyber threats and the demand for accessible, efficient solutions for small businesses and home users. The focus is on combining the functionality of a firewall and an intrusion detection/prevention system Snort 3. The theoretical section analyzes network threats, hardware security tools, and existing solutions for small networks. The practical part includes network modeling in Packet Tracer, system deployment in VirtualBox, and configuration of security components based on Kali Linux. The work demonstrates the feasibility of creating a cost-effective and functional security solution suitable for real-world applications.

ЗМІСТ

ВСТУП

Невпинний процес діджиталізації охоплює дедалі ширше коло аспектів людського буття, трансформуючи економіку, суспільне життя та повсякденні процеси. Глобальна торгівля, електронна комерція, фінансові системи, енергетика, охорона здоров'я та телекомунікації – усі ці сфери сьогодні критично залежать від надійності та безпеки мережевих технологій. Можливість миттєвого доступу до інформації, дистанційне керування складними системами, проведення високотехнологічних операцій та автоматизація рутинних завдань значно підвищують ефективність та відкривають нові горизонти для розвитку.

Однак, разом із безперечними перевагами, стрімкий розвиток цифрових технологій та зростаюча залежність від них породжують і нові масштабні виклики. Кіберзагрози перетворилися на одну з ключових проблем сучасності, здатною призвести як до локальних інцидентів на кшталт витоку даних чи порушення роботи окремих сервісів, так і до глобальних наслідків, включаючи економічні кризи, параліч критичної інфраструктури та навіть загрози національній безпеці. У цьому контексті питання забезпечення надійної кібербезпеки набуває стратегічного значення.

Важливу роль у побудові ешелонованої системи захисту відіграють апаратні засоби. Їхня здатність обробляти значні обсяги трафіку в реальному часі, висока продуктивність, надійність та відносна незалежність від вразливостей програмного забезпечення роблять їх ефективним інструментом протидії складним кібератакам. Апаратні рішення забезпечують стабільність роботи мережевої інфраструктури та безперервність функціонування критично важливих систем, що є особливо актуальним для організацій, які висувають найвищі вимоги до рівня безпеки.

Проте, вартість професійних апаратних комплексів захисту часто є надто високою для невеликих організацій, малого бізнесу чи домашніх мереж, які

також потребують ефективного захисту, також варто розуміти що професійне обладнання є складним у адмініструванні, для роботи з яким потрібно бути компетентним та мати професійні навички. Це створює попит на доступні, гнучкі та водночас надійні рішення.

Метою даної дипломної роботи є: розробка та дослідження бюджетного рішення для захисту невеликої комп'ютерної мережі на базі одноплатного мікрокомп'ютера Raspberry Pi. Запропонована система виконуватиме функції мережевого екрану (фаєрвола) та системи виявлення/запобігання вторгненням (IDS/IPS). Основна увага приділяється створенню функціональної, економічно ефективної та адаптивної системи безпеки, здатної забезпечити належний рівень захисту для мереж з обмеженими ресурсами, без необхідності інвестування у дороге професійне обладнання.

Основні завдання дослідження:

- Аналіз можливостей Raspberry Pi як апаратної платформи для реалізації функцій мережевої безпеки.
- Оцінка програмної складової для створення фаєрволу та IDS/IPS системи (Uncomplicated Firewall та Snort3)
- Розробка архітектури мережевого захисту з використанням Raspberry Pi.
- Робота з Linux та робота з терміналом.
- Налаштування обладнання та введення правил.
- Моделювання роботи системи у віртуальному середовищі VirtualBox.
- Тестування функціональності рішення в емуляторі мережевих топологій Cisco Packet Tracer.
- Оцінка продуктивності та ефективності запропонованого рішення.

Об’єкт дослідження: системи мережевої безпеки для інфраструктур малого масштабу, зокрема малих офісів та домашніх мереж.

Предмет дослідження: дослідження ефективності та аналіз функціональних можливостей одноплатного комп’ютера Raspberry Pi як апаратної платформи для створення бюджетного рішення мережевої безпеки, що включає фаєрвол та систему виявлення/запобігання вторгнень (IDS/IPS), робота з Linux та терміналом.

РОЗДІЛ І
ТЕОРЕТИЧНІ ОСНОВИ МЕРЕЖЕВОЇ БЕЗПЕКИ

1.1 Загрози інформаційній безпеці в комп’ютерних мережах

Інформаційна безпека –це стан захищеності систем передавання, опрацювання та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність даних.

Конфіденційність –забезпечення доступу до даних на основі розподілу прав доступу, захист від несанкціонованого ознайомлення.

Невпинний процес діджиталізації охоплює дедалі ширше коло аспектів людського буття. Це явище, безперечно, несе в собі значні переваги: підвищується ефективність робочих процесів, спрощується доступ до інформації та послуг, а впровадження автоматизованих систем у небезпечних галузях мінімізує ризики для життя. Разом з тим, стрімкий розвиток цифрових технологій ставить перед нами й нові складні завдання, зокрема у сфері захисту персональних даних, протидії кіберзлочинності та забезпечення рівного доступу до переваг цифрового світу для всіх верств населення.

Сучасні комп'ютерні мережі постійно піддаються впливу різноманітних загроз, які можуть призвести до витоку конфіденційних даних, фінансових втрат або повного припинення роботи систем. Ці загрози можна структурувати за такими основними категоріями:

Зовнішні загрози: Кібератаки зовнішніх суб'єктів (хакерські групи, кіберзлочинці), вірусні та шкідливі програми (трояни, черв'яки), фішингові атаки та соціальна інженерія, атаки типу "відмова в обслуговуванні" (DDoS), сканування мережі та експлуатація вразливостей.

Внутрішні загрози: Навмисні або випадкові дії персоналу, зловживання повноваженнями, використання неавторизованих пристроїв, несанкціоноване копіювання даних.

Технічні загрози: Апаратні збої та відмови обладнання, вразливості програмного забезпечення, нестабільність електроживлення, втрата даних через збій системи

Фізичні загрози: Крадіжка обладнання, Пошкодження інфраструктури, несанкціонований фізичний доступ, стихійні лиха.

1.2 Сучасні апаратні засоби захисту інформації

Фаєрвол, міжмережевий екран, мережевий екран, брандмауер – це базовий елемент захисту ІТ –інфраструктури, серверів, додатків та інформації від несанкціонованого доступу та інших зовнішніх загроз. Програмно – апаратний комплекс аналізує цифровий трафік і фільтрує пакети даних відповідно до встановлених адміністратором параметрів, блокує небажаний контент, і, таким чином, посилює рівень безпеки мережевої інфраструктури. Міжмережевий екран може бути реалізований як самостійне програмне забезпечення, фізичне обладнання, а також в якості додаткового елементу операційної системи. Його основне призначення – гарантування безпеки даних, збереження їх цілісності та конфіденційності. На Рисунку 1.2.1 зображено схему по якій фаєрвол монтується у мережу.

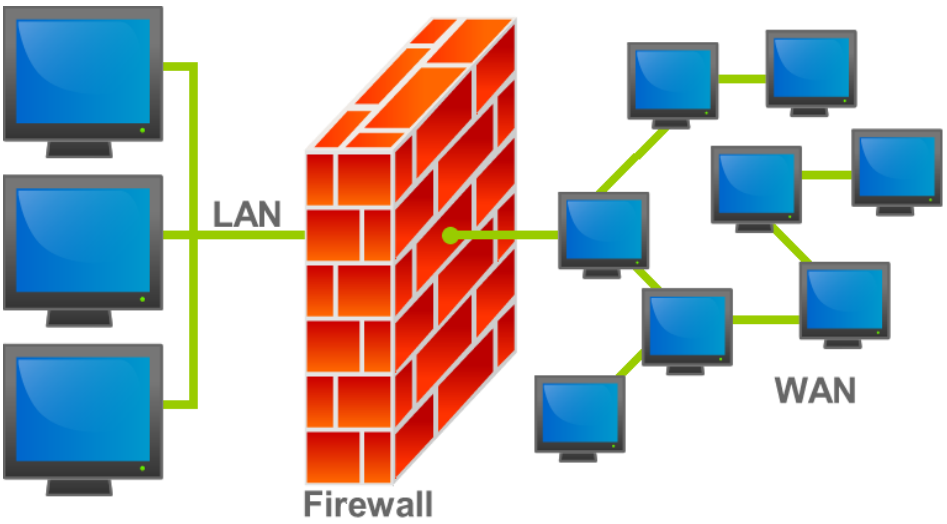

Рисунок 1.2.1 – Схема монтажу фаєрволоа у мережу

Фаєрвол забезпечує захист від таких загроз як

- Несанкціонований доступу до мережі,
- Атаки типу DDoS,
- Віруси та шкідливе ПЗ,
- Спуфінг IP –адрес,
- Витік даних,
- Фішинг,
- Внутрішні загрози.

Таблиця 1.2.1 – Захист фаєрволу.

Тип Загрози	Захист Фаєрволу	Детальніше про дію фаєрволу
1	2	3
Спроби несанкціонованого проникнення ззовні	Так	Фаєрволи успішно блокують "непроханих гостей", які намагаються підключитися до вашої мережі чи комп'ютерів, контролюючи, які "двері" (порти) та "шляхи" (протоколи) для них відкриті.
Базовий захист від деяких шкідливих програм	Частково	Фаєрвол може розпізнати та заблокувати доступ до відомих адрес в інтернеті, з яких поширюються певні віруси чи трояни. Однак він не "заглядає всередину" файлів, щоб перевірити їх на шкідливий вміст.

Продовження таблиці 1.2.1

1	2	3
Перевантаження системи (DoS/DDoS –атаки)	Частково	Сучасніші фаєрволи (NGFW) та спеціалізовані системи можуть розпізнавати та фільтрувати лавину шкідливого трафіку, спрямовану на виведення вашої системи з ладу. Проте надзвичайно потужні атаки можуть здолати і сам фаєрвол.
Вивідування відкритих портів (сканування)	Так	Фаєрволи допомагають приховати інформацію про відкриті порти вашої системи або сигналізують про спроби їх виявлення, що ускладнює зловмисникам пошук слабких місць.
Спроби зламу системи	Частково	Просунуті фаєрволи з функцією запобігання вторгненням (IPS) здатні виявляти та блокувати відомі методи атак. Але їх ефективність прямо залежить від того, наскільки свіжими є їхні знання про нові загрози.
Обман з метою виманювання даних (фішинг)	Ні	Фаєрволи зазвичай не аналізують зміст електронних листів чи веб –сторінок на предмет шахрайства. Тут потрібна ваша уважність та спеціальні антифішингові інструменти.
Віруси, завантажені власноруч	Ні	Якщо ви самі завантажили заражений файл або перейшли за небезпечним посиланням, фаєрвол навряд чи допоможе, адже для нього цей трафік може виглядати як звичайний. У таких випадках потрібен антивірус.
Атаки через зашифровані канали (HTTPS)	Частково/Ні	Звичайні фаєрволи "не бачать" крізь шифрування. Деякі новітні фаєрволи (NGFW) можуть перевіряти такий трафік, але це вимагає значних ресурсів та може порушувати питання приватності.
Загрози зсередини мережі	Ні	Фаєрволи орієнтовані на захист від атак ззовні. Вони не контролюють дії співробітників чи інших авторизованих користувачів, які можуть діяти зловмисно або через необережність. Для цього потрібні інші інструменти (системи моніторингу, політики доступу).
Психологічні маніпуляції (соціальна інженерія)	Ні	Фаєрвол безсилий проти обману, спрямованого на вас як користувача, з метою отримання паролів чи іншої цінної інформації. Найкращий захист тут – ваша обізнаність та критичне мислення.
Абсолютно нові, невідомі загрози (Zero –Day)	Ні/Частково	Фаєрволи, що покладаються на відомі "портрети" загроз, не встигають за новітніми атаками. Деякі NGFW з аналізом поведінки можуть запідозрити щось неладне, але це не гарантує 100% захисту.
Людський фактор: помилки в налаштуванні	Ні	Неправильно налаштований фаєрвол (наприклад, зі слабкими правилами) може бути не тільки марним, але й сам стати джерелом проблем безпеки.
Фізичне викрадення пристроїв	Ні	Фаєрвол – це програма або пристрій для захисту даних у мережі, він не вбереже комп'ютери чи сервери від фізичної крадіжки.
Атаки на веб – сайти та веб – додатки	Частково/Ні	Класичні мережеві фаєрволи часто не здатні ефективно протистояти атакам, націленим на слабкі місця веб – додатків (наприклад, SQL –ін'єкції). Для цього існують спеціальні фаєрволи для веб –додатків (WAF).

Системи виявлення та запобігання вторгненням (IDS/IPS) є важливими елементами забезпечення інформаційної безпеки, призначеними для виявлення та нейтралізації несанкціонованого доступу до комп'ютерних мереж. Вони можуть реалізовуватись як у програмному, так і в апаратному вигляді, забезпечуючи оперативне виявлення загроз та запобігання можливим атакам. Серед основних функцій таких систем –інформування фахівців з інформаційної безпеки про спроби здійснення хакерських атак, впровадження шкідливого програмного забезпечення, автоматичне припинення з'єднань із потенційно небезпечними джерелами, а також динамічне налаштування мережевого екрану з метою блокування доступу до корпоративної інформації, як зображено на Рисунку 1.2.2.

Попри функціональні подібності до фаєрволів, системи IDS/IPS відрізняються більш складним та гнучким механізмом дії. Якщо фаєрволи здійснюють фільтрацію трафіку на основі заздалегідь визначених правил, то IDS/IPS –системи аналізують мережеву активність з урахуванням поведінкових шаблонів і сигнатур відомих атак. Це дозволяє виявляти навіть ті загрози, які можуть обійти класичний набір правил фаєрвола, тим самим значно підвищуючи рівень захисту мережевої інфраструктури.

Система виявлення вторгнень (IDS) –це засіб контролю, який здійснює моніторинг мережевої або системної активності з метою виявлення ознак несанкціонованого доступу або спроб несанкціонованого управління інформаційними ресурсами.

Система запобігання вторгненням (IPS), у свою чергу, є розширеним функціоналом IDS і виконує не лише виявлення, але й активне блокування шкідливих дій у реальному часі. Таким чином, IPS забезпечує не лише фіксацію інцидентів, а й автоматичне реагування на них, що дозволяє ефективно нейтралізувати загрози ще на етапі їх виникнення.

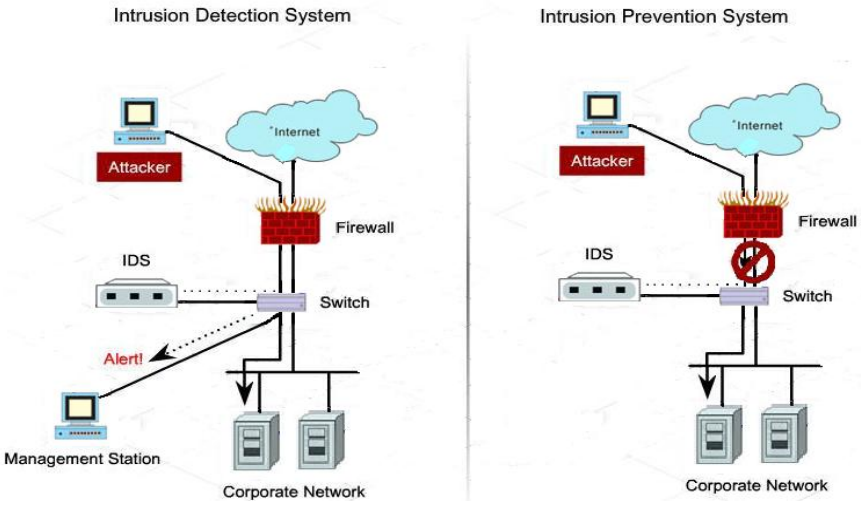

Рисунок 1.2.2 –схема роботи роботи IPS / IDS систем

Таблиця 1.2.2 – Різниця між IDS та IPS

Критерій	IDS (Система виявлення вторгнень)	IPS (Система запобігання вторгнень)
Основна функція	Моніторить мережевий трафік та виявляє аномалії	Активно блокує підозрілий трафік на основі правил
Режим роботи	Пасивний (лише попередження)	Активний (автоматичне втручання)
Місце в мережі	Копіює трафік (наприклад, через SPAN –порт)	Розташовується на шляху трафіку (inline)
Типи загроз	Виявляє: DDoS, сканування портів, SQL –ін'єкції	Блокує: атаки на рівні мережі/додатків, експлойти Zero –day
Плюси	– Не впливає на продуктивність мережі – Детальний аналіз трафіку	– Запобігає атакам у реальному часі – Зменшує навантаження на SOC
Мінуси	– Не зупиняє атаки – Ризик пропуску загроз через затримки аналізу	– Може викликати false –positive (блокування легального трафіку) – Вимагає тонкого налаштування
Технології	– Сигнатурний аналіз – Аналіз аномалій (ML) – Snort, Suricata	– Глибинний аналіз пакетів (DPI) – Інтеграція з SIEM – Cisco Firepower, Palo Alto IPS
Використання	Для моніторингу та аудиту безпеки	Для активного захисту критичних систем
Приклад роботи	Зафіксувала сканування портів → надсилає alert адміну	Виявила SQL –ін'єкцію → миттєво блокує з’єднання

1.3 Огляд існуючих рішень для захисту малих мереж

Хмарні рішення безпеки (Security as a Service – SECaaS / SASE): на сьогоднішній день малі підприємства все частіше прибігають до хмарних сервісів безпеки, які пропонують комплексний захист "як послугу", зменшуючи потребу у локальному обладнанні та експертизі що полегшує адміністрування мережі.

Конкретні рішення:

Cloudflare One: Пропонує комплексний SASE –підхід. Cloudflare Gateway включає функції безпечного веб –шлюзу, фільтрації DNS, DLP та базовий IPS/IDS. Cloudflare Access є ZTNA –рішенням для безпечного доступу до внутрішніх ресурсів без VPN. Безкоштовний план Cloudflare надає базовий захист від DDoS, CDN та SSL, що є відмінним рішення для невеликих мереж.

Zscaler Internet Access (ZIA): Лідер ринку SASE, який надає повний спектр хмарних сервісів безпеки, включаючи SWG, Cloud Firewall, IPS, Sandbox, DLP. Чудово підходить для зростаючого малого бізнесу.

Cisco Umbrella: Хмарний DNS –рівневий захист, який блокує шкідливі домени, фішингові сайти та колбек –запити від шкідливого ПЗ. Просто впроваджується та ефективний для первинного фільтрування загроз.

SASE (Secure Access Service Edge, "прикордонний сервіс безпечного доступу") – це компонент архітектури з нульовою довірою, що захищає мережеві елементи всередині та поза традиційним периметром мережі.

DLP –технологія запобігання витоку конфіденційної інформації з інформаційної системи DLP –системи будуються на аналізі потоків даних, які перетинають периметр інформаційної системи, що захищається. При виявлені в цьому потоці конфіденційної інформації передача повідомлень (пакета, потоку, сесії) блокується.

ZTNA (Zero Trust Network Access) – це технологія, що дає більш безпечний та точний контроль доступу до корпоративних ресурсів, як в

локальних мережах, так і в хмарах. Згідно з принципом Zero Trust, ZTNA ніколи не довіряє і завжди перевіряє, незалежно від того, де знаходиться користувач або пристрій.

Міжмережевий екран наступного покоління (NGFW, Next –Generation Firewall) –це пристрій або програмне забезпечення, що є еволюцією традиційних фаєрволів. Якщо традиційні фаєрволи здебільшого орієнтувалися на фільтрацію трафіку на основі IP –адрес, портів та протоколів, на мережевому та транспортному рівнях моделі OSI (2 –4 рівні), то NGFW працюють набагато глибше, аналізуючи трафік аж до рівня додатків (рівень 7).

Це означає, що NGFW не просто перевіряє, звідки і куди йде трафік, а й вміст трафіку, який додаток його використовує і хто є користувачем. Завдяки цій глибокій інспекції, NGFW здатні виявляти та блокувати набагато складніші та приховані загрози, які традиційні міжмережеві екрани не здатні зупинити.

Ознака	Традиційний міжмережевий екран (Stateful Firewall)	Міжмережевий екран наступного покоління (NGFW)
Рівень роботи (OSI)	Рівень 2 –4 (Мережевий, Транспортний)	Рівень 2 –7 (Від мережевого до рівня додатків)
Що аналізує	IP –адреси, порти, протоколи, стан з'єднання	IP –адреси, порти, протоколи, додаток, користувач, вміст, контекст
Аналіз вмісту пакетів	Ні (тільки заголовки)	Так (Deep Packet Inspection – DPI)
Виявлення загроз	Базове (заблокувати порт/IP)	Розширене (IPS, Sandboxing, Threat Intelligence)
Контроль додатків	Ні (лише за портами)	Так (застосування політик до конкретних додатків)
Захист від DDoS	Базовий	Розширений
Інспекція SSL/TLS	Ні	Так
Інтеграція з Ідентичністю	Ні	Так (Active Directory, LDAP)
Вартість	Дешевше	Дорожче (але економічно вигідніше у довгостроковій перспективі)
Складність управління	Простіше	Складніше (але надає більше контролю)

Хоча NGFW можуть бути дорожчими за традиційні міжмережеві екрани, їхні переваги для малого бізнесу значні:

1. Комплексний захист: Замість придбання та управління кількома окремими рішеннями (фаєрвол, IPS, фільтр вмісту, VPN –шлюз), NGFW об'єднує їх в одному пристрої. Це спрощує управління, знижує витрати на ліцензії та зменшує ймовірність "прогалин" у безпеці між різними продуктами.

2. Захист від сучасних загроз: Малий бізнес так само вразливий до фішингу, програм –вимагачів та атак нульового дня, як і великі корпорації. NGFW надає необхідний рівень захисту від цих складних загроз.

3. Контроль та видимість: Можливість бачити, які додатки використовуються, хто їх використовує та який трафік генерується, дозволяє краще керувати пропускною здатністю та застосовувати політики безпеки.

4. Віддалений доступ: Вбудовані можливості VPN дозволяють працівникам безпечно підключатися до мережі з будь –якого місця, що є особливо актуальним у сучасному гібридному робочому середовищі.

5. Відповідність нормативним вимогам: Для деяких галузей або типів даних (наприклад, фінансові, медичні) NGFW допомагає дотримуватися регуляторних вимог безпеки.

Провідні виробники NGFW:

Palo Alto Networks: Вважається одним з лідерів ринку, відомий своїми інноваціями та високим рівнем безпеки.

Fortinet: Дуже популярний вибір завдяки широкому функціоналу, високій продуктивності та конкурентній ціні (особливо молодші моделі для SMB).

Check Point: Один з піонерів у сфері міжмережевих екранів, пропонує надійні рішення з широким набором функцій.

Cisco (Firepower Next –Generation Firewall): Пропонує інтегровані рішення з екосистемою Cisco.

Sophos: Пропонує NGFW, які легко інтегруються з іншими продуктами Sophos (наприклад, Intercept X для кінцевих точок).

SonicWall: Відомі своєю глибокою перевіркою пакетів та ефективним захистом від загроз.

WatchGuard: Пропонують широкий спектр рішень для малого та середнього бізнесу, з акцентом на простоту використання та комплексний захист.

РОЗДІЛ ІІ
RASPBERRY PI ЯК ОСНОВА ДЛЯ СИСТЕМИ ЗАХИСТУ

2.1 Raspberry Pi, характеристики та можливості платформи

Raspberry Pi –це сімейство одноплатних мікрокомп’ютерів, розроблених британським фондом Raspberry Pi Foundation насамперед для освітніх цілей. Однак завдяки своїй доступності, компактності, низькому енергоспоживанню, широким технічним можливостям та прийнятній ціні, ці пристрої здобули велику популярність серед ентузіастів, розробників, інженерів, а також у сфері прототипування та навіть у комерційних продуктах. На рисунку 2.1.1 зображено один з представників даного сімейства одноплатних комп’ютерів.

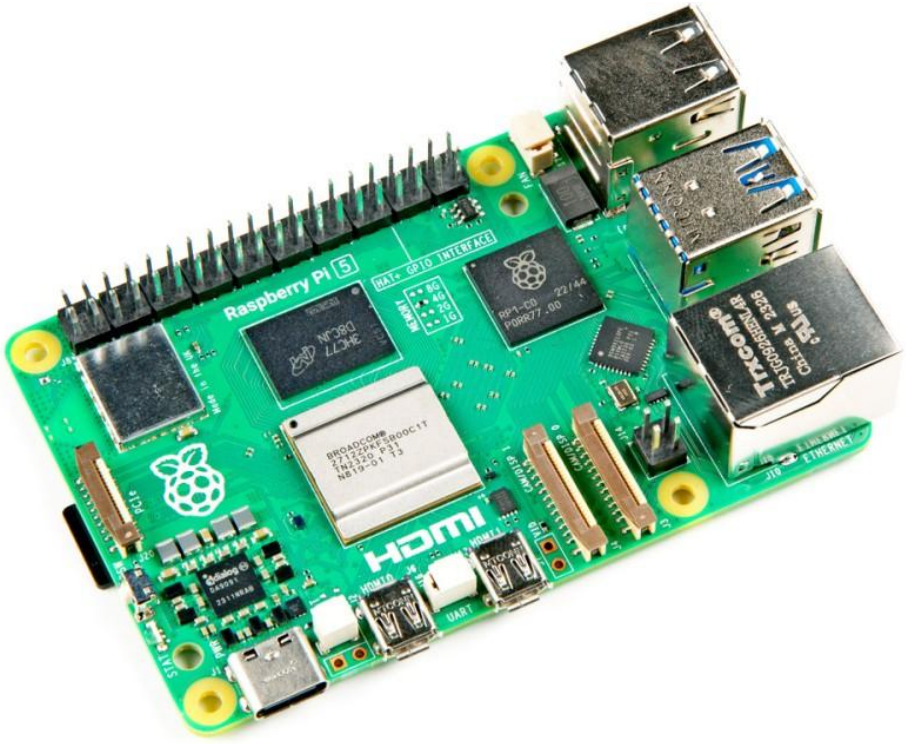

Рисунок 2.1.1 –одноплатний комп’ютер Raspberry Pi 5

Одноплатний комп'ютер (SBC) – це повноцінний комп'ютер, побудований на одній друкованій платі. На ній розміщуються всі основні компоненти, необхідні для роботи комп'ютера: центральний процесор, оперативна пам'ять, порти введення та виведення, а також слот для карт пам'яті для зберігання операційної системи та даних.

Ключові особливості платформи Raspberry Pi:

Розмір та ціна: Raspberry Pi зазвичай має розмір кредитної картки (або навіть менше, як у випадку Raspberry Pi Zero) і коштує від кількох доларів до приблизно $100 за найпотужніші моделі. Ця доступність є однією з головних причин його популярності.

Повноцінний комп'ютер: Незважаючи на розмір, Raspberry Pi –це повноцінний комп'ютер, який може запускати повноцінні операційні системи (переважно на базі Linux, такі як Raspberry Pi OS, Ubuntu, а також спеціалізовані ОС для медіацентрів чи для запуску ретро –ігор).

Наявність актуальних портів: Одноплатні комп’ютери Raspberry Pi мають різноманітні порти які на сьогоднішній день є актуальними, і це дає змогу значно збільшити вже й так широкий функціонал одноплатного комп’ютера.

Робота з повноцінними ОС: По при свої розміри Raspberry Pi підтримують роботу з повноцінними ОС найчастіше це дистрибутиви на базі ядра Linux, але й зустрічаються екземпляри які працюють і з Microsoft Windows 10.

Енергоефективність: Raspberry Pi споживає невелику кількість електроенергії навіть під піковимим навантаженнями, тому Raspberry Pi ідеально підходить для реалізації пристроїв які будуть працювати цілодобово або автономно від акумулятора.

Raspberry Pi 5 який має такі характеристики:

1. Процесор:

Модель: Broadcom BCM2712

Архітектура CPU: 64 –розрядний чотириядерний процесор Arm Cortex – A76 (ARM v8)

Тактова частота: 2.4 ГГц

Кеш: 512 КБ кешу L2 на ядро, 2 МБ спільного кешу L3.

Додатково: Підтримка Cryptographic Extension (апаратне прискорення AES), що важливо для шифрування/розшифрування даних (наприклад, для VPN, SSL/TLS інспекції).

2. Графічний процесор (GPU):

Модель: VideoCore VII

Частота: 800 МГц

Підтримка: OpenGL ES 3.1, Vulkan 1.2

Відеодекодер: 4Kp60 HEVC (High Efficiency Video Coding)

Відеовивід: Подвійний вихід micro –HDMI з підтримкою 4Kp60 (4K при 60 кадрах/с) та HDR.

3. Оперативна пам'ять (RAM):

Тип: LPDDR4X –4267 SDRAM

Доступні об'єми: 2 ГБ, 4 ГБ, 8 Гб та 16 ГБ

4. Мережеві можливості:

Ethernet: Gigabit Ethernet (10/100/1000 Мбіт/с) з підтримкою PoE+ (Power over Ethernet Plus) – вимагає окремого PoE+ HAT.

Wi –Fi: Дводіапазонний 802.11ac Wi –Fi (2.4 ГГц та 5 ГГц).

Bluetooth: Bluetooth 5.0 з підтримкою BLE (Bluetooth Low Energy).

5. Порти та інтерфейси:

2 порти USB 3.0 (зі швидкістю 5 Гбіт/с, підтримують одночасну повну пропускну здатність).

2 порти USB 2.0.

micro –HDMI: 2 порти для виводу відео.

GPIO: Стандартний 40 –контактний роз'єм GPIO Raspberry Pi для підключення зовнішніх електронних компонентів.

MIPI: Подвійні 4 –канальні трансівери MIPI CSI/DSI (Camera Serial Interface / Display Serial Interface) – дозволяють підключати дві камери, два дисплеї або одну камеру + один дисплей.

PCIe: 1x PCIe 2.0 інтерфейс (x1) – це нова і дуже важлива особливість. Дозволяє підключати швидкісну периферію, таку як NVMe SSD через HAT (Hardware Attached on Top) або інші адаптери, що значно покращує швидкість зберігання даних.Слот для карти пам'яті: microSD (з підтримкою високошвидкісного режиму SDR104, що подвоює швидкість порівняно з Pi 4).

Роз'єм вентилятора: Для підключення активної системи охолодження (рекомендовано для інтенсивних навантажень).

Годинник реального часу (RTC): Вбудований RTC з роз'ємом для резервного акумулятора, що дозволяє зберігати точний час навіть без живлення.

Кнопка живлення: Фізична кнопка ввімкнення/вимкнення на платі.

UART header: Роз'єм UART для налагодження та доступу до консолі.

6. Живлення:

Порт: USB –C (з підтримкою Power Delivery).

Вимоги: 5 В / 5 А (рекомендовано використовувати офіційний блок живлення або якісний блок живлення з підтримкою Power Delivery, щоб уникнути проблем зі стабільністю).

7. Розміри плати:

Стандартний форм –фактор Raspberry Pi: 85 мм × 56 мм. Детальніше зображено на кресленнях (Рисунок 2.1.2, Рисунок 2.1.3)

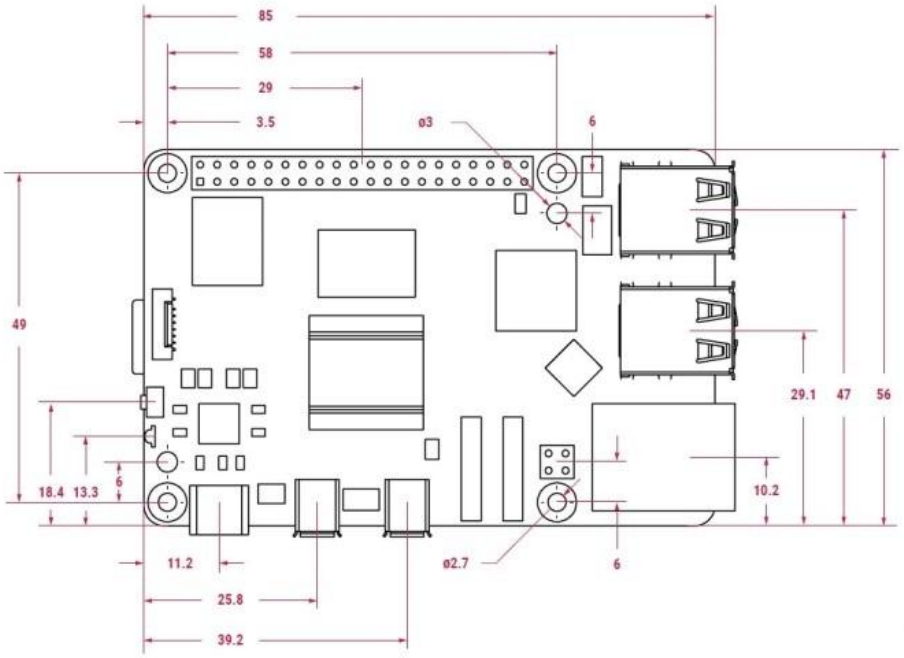

Рисунок 2.1.2 – креслення Raspberry Pi 5 (вид зверху)

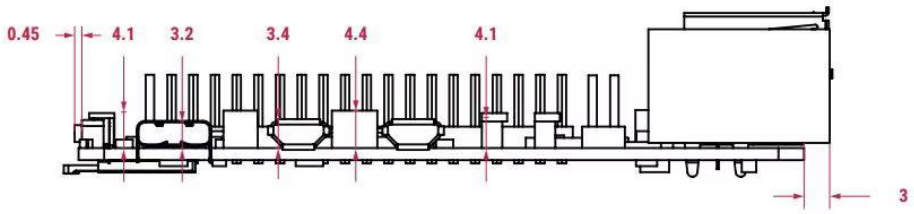

Рисунок 2.1.3 – креслення Raspberry Pi 5 (вид збоку)

2.2 Вибір програмного забезпечення

Програмна складова базуватиметься на операційній системі Linux конкретніше дистрибутив Kali linux на який буде встановлено вище описані програми, Uncomplicated Firewall (UFW) та Snort3.

Kali linux – Це дистрибутив на базі Debian, створений та підтримуваний компанією Offensive Security. Його основна відмінність від інших дистрибутивів полягає в тому, що він поставляється з тисячами попередньо встановлених інструментів, спеціально розроблених для:

- Тестування на проникнення (пентестінгу): Процес імітації кібератаки на систему, мережу або веб –додаток для виявлення вразливостей.

- Аудиту безпеки: Оцінка безпеки інформаційних систем.
- Цифрової криміналістики (Digital Forensics): Збір, аналіз та відновлення цифрових доказів.
- Реверс –інжинірингу: Аналіз програмного забезпечення для розуміння його функціонування.

Для реалізації фаєрвола я використав Uncomplicated Firewall (UFW) – зручне програмне забезпечення для керування міжмережевим екраном Netfilter вбудованим в ядро Linux. Ціль цієї програми упростити користуванням таких утиліт як iptables та nftables, без необхідності заглиблюватися в складну синтаксичну структуру цих утиліт.

Ключові особливості та переваги UFW:

- UFW розроблений так, щоб бути максимально інтуїтивно зрозумілим. Замість складних команд iptables з безліччю параметрів, UFW пропонує прості, читабельні команди. Наприклад, щоб дозволити SSH –трафік, замість довгої команди iptables, в термінал вписується sudo ufw allow ssh або sudo ufw allow 22/tcp.
- Він ідеально підходить для початківців або для тих, хто шукає швидке та ефективне рішення для базового захисту сервера чи робочої станції.
- UFW однаково ефективно керує правилами як для IPv4, так і для IPv6.
- UFW дозволяє або забороняє трафік для конкретних портів.
- UFW має вбудовану підтримку для "профілів додатків" (application profiles). Можна дозволити трафік для певного сервісу (наприклад, sudo ufw allow "OpenSSH"), і UFW автоматично визначить потрібні порти.
- Можна дозволяти або забороняти підключення з конкретних IP – адрес або цілих підмереж.
- Правила можуть бути застосовані до конкретних мережевих інтерфейсів.

- UFW може обмежувати кількість з'єднань з певного IP –адреси до певного порту за певний період часу.
- UFW може вести логування подій фаєрволу, що допомагає відстежувати спроби доступу та виявляти потенційні загрози. Рівень деталізації логів можна налаштовувати.
- UFW інтегрований з системою Linux, що означає, що правила фаєрволу автоматично застосовуються при кожному завантаженні системи.

Netfilter –це фреймворк вбудований в ядро Linux, він надає механізм для перехоплення та обробки мережевих пакетів на різних етапах його проходження через мережевий стек ядра. Є основою для реалізації функції фаєрволу, NAT (Network Address Translation), QoS (Quality of Service) та багатьох інших мережевих можливостей у Linux.

А от для реалізації IDS/IPS систем я використав програмне забезпечення Snort3 – це вільне програмне забезпечення системи виявлення та запобігання атак, яке комбінує в собі методи зіставлення по сигнатурам, засоби для інспекції протоколів і механізми для виявлення аномалій.

Сигнатура атаки – це характерні ознаки атаки або вірусу, що допомагають виявити віруси, експлоїти та загрози для подальшого їх усунення.

Головні переваги Snort3:

Вища продуктивність завдяки багатопоточності, Snort 3 ефективно використовує всі ядра процесора, забезпечуючи значно кращу пропускну здатність та швидкість обробки трафіку порівняно з попередніми версіями.

Його модульна архітектура дозволяє легко додавати нові функції через плагіни та адаптувати систему під конкретні потреби.

Використання Lua для конфігураційних файлів робить налаштування більш гнучким, читабельним та легким для автоматизації.

Покращені механізми інспекції та підтримка порто –незалежних правил дозволяють виявляти загрози, незалежно від використовуваних портів.

Швидкий запуск, можливість інкрементального перезавантаження правил та зручніший моніторинг роблять Snort 3 ефективнішим та простішим в управлінні.

РОЗДІЛ ІІІ
ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ

3.1 Апаратна складова системи захисту

Система захисту була емульована в середовищі VirtualBox, топологія мережі змодельована в середовищі Packet Tracer, ці середовища здатні в повній мірі продемонструвати як працювати з операційною системою Linux, програмним забезпеченням Snort та UFW, як працює комп'ютерна мережа та як об'єднувати пристрої в мережу.

Для реалізації системи захисту крім Raspberry Pi 5 необхідно також мати накопичувач, який необхідний для встановлення операційної системи та програмного забезпечення, можна використати як карту пам'яті типу MicroSD так і накопичувач типу NVMe M2 (через слот PCI Express). Необхідно використовувати об'ємом не менше 32Гб та Class 10 (для MicroSD).

Система активного охолодження необхідна для забезпечення стабільної температури під навантаженнями. Та для збільшення надійності та довговічності системи. На рисунку 3.1.1 зображено один з варіантів системи активного охолодження Raspberry Pi 5 Active Cooler –офіційне рішення від Raspberry Pi Foundation та креслення рисунок 3.1.2

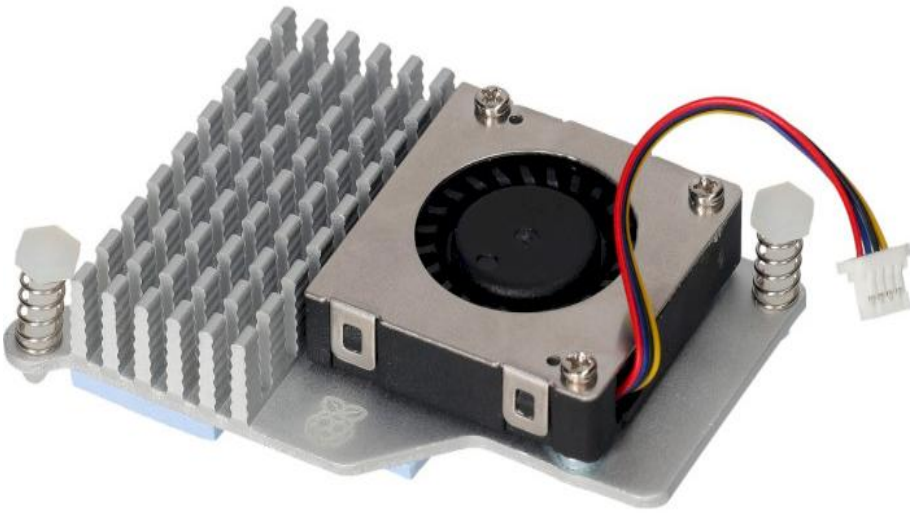

Рисунок 3.1.1 –Raspberry Pi 5 Active Cooler

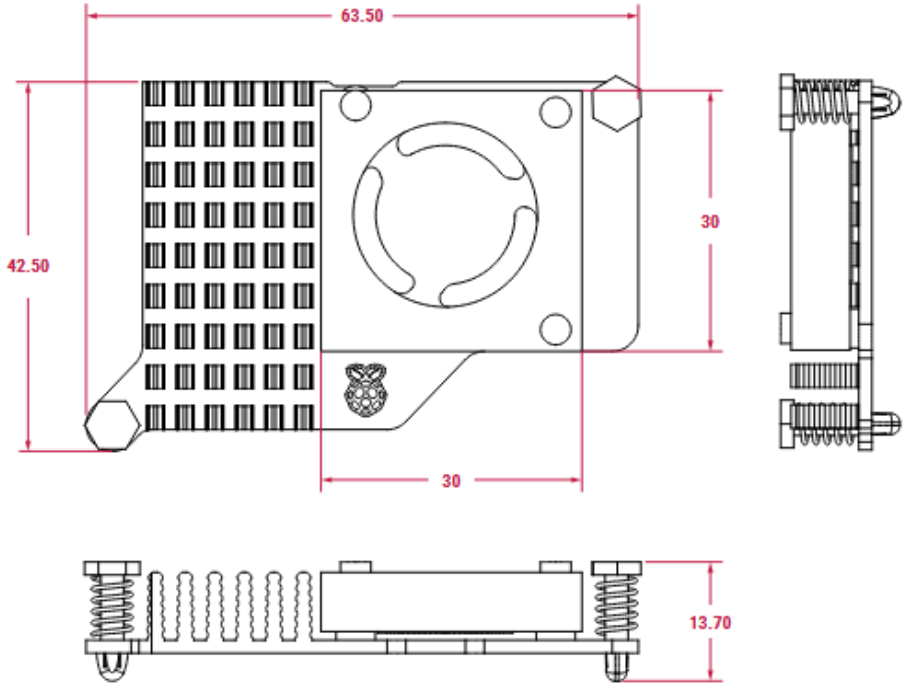

Рисунок 3.1.2 –креслення системи охолодження

Корпус Raspberry Pi 5 використовується для захисту системи від фізичних загроз, покращення системи охолодження та для зручного монтажу системи в необхідне місце. Його можна купити окремо а можна й реалізувати самостійно при наявності відповідного інструменту та матеріалів (зручніше

всього за допомогою 3d принтера та пластику типу ASA). На рисунку 3.1.3 зображено Raspberry Pi 5 Case, офіційне рішення від Raspberry Pi Foundation.

Блок живлення –необхідний для правильної і безперебійної подачі електроенергії у систему захисту, вимоги до блоку живлення:

Вхідна напруга : 100–240 В змінного струму.

Вихідна напруга : 5,1 В, 5 А; 9В, 3А; 12 В, 2,25 А; 15 В, 1,8 А.

Роз’єм: USB –C

Патч-Корд – Необхідний для під’єднання системи захисту до комп'ютерної мережі, краще використовувати 8-жильний мідний кабель такий кабель забезпечить краще з’єднання, якісніший сигал, довговічність та високу пропускну здатність, що грає велику роль в ефективності системи захисту та ефективності мережі загалом.

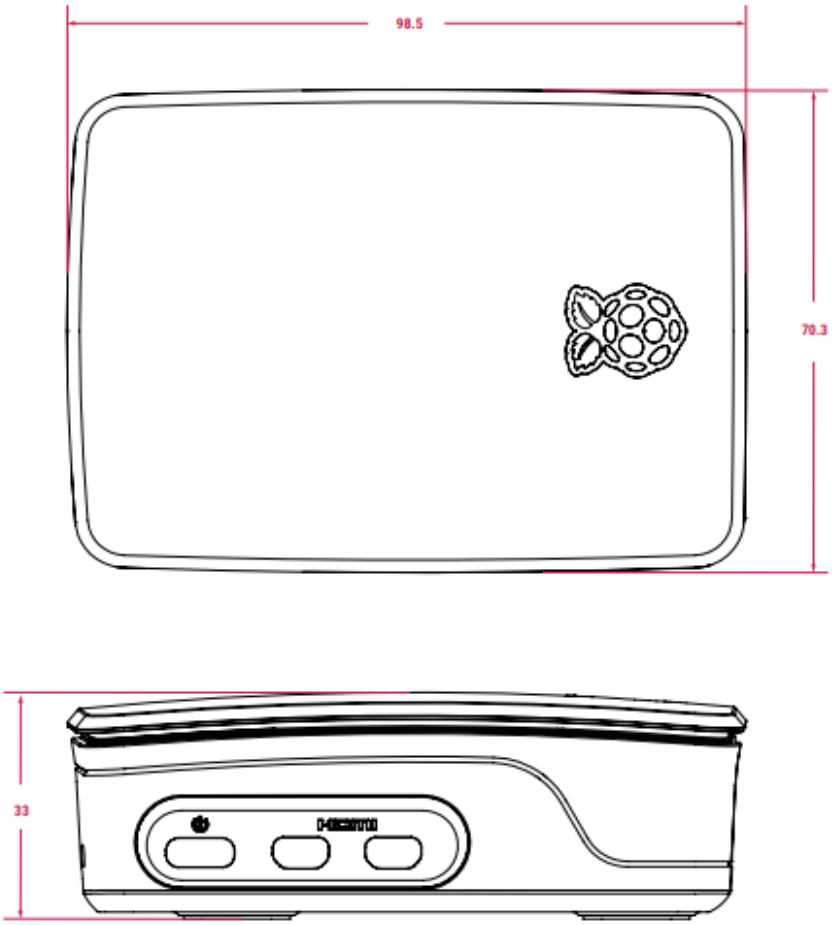

рисунок 3.1.3 – корпус Raspberry 5 Case

Пристрої вводу та виводу – монітор, клавіатура та комп’ютерна миша використовуватимуться при першому налаштувані та конфігурації системи захисту, в подальшому можна використовувати SSH (Secure Shell) – для доступу до командного рядка або VNC (Virtual Network Computing) – для графічного інтерфейсу. Без фізичного втручання в систему захисту.

У рамках реалізації проєкту система захисту розміщується у мережевій інфраструктурі, організованій за топологією типу «зірка». Така топологія передбачає централізовану структуру, в якій усі периферійні вузли підключені до одного центрального комутаційного елемента (рисунок 3.1.4). Розміщення засобів захисту в центральному вузлі дозволяє здійснювати повноцінний контроль та аналіз усього вхідного і вихідного трафіку, що проходить через мережу. Це забезпечує підвищений рівень інформаційної безпеки, оскільки дозволяє централізовано виявляти, реєструвати та блокувати потенційні загрози до того, як вони досягнуть кінцевих пристроїв користувачів.

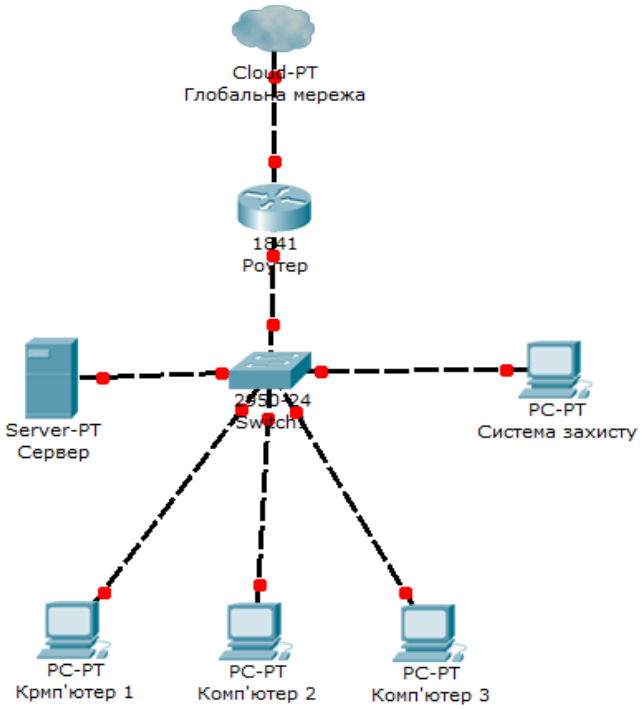

Рисунок 3.1.4 топологія мережі в якій розглядається система захисту

3.2 Налаштування системи захисту та встановлення програмного забезпечення

Перед початком роботи з Raspberry Pi 5 необхідно підготувати зовнішній накопичувач для подальшого встановлення операційної системи. Для цього слід скористатися офіційним програмним забезпеченням, яке доступне на веб –сайті Raspberry Pi Foundation за посиланням: https://www.raspberrypi.com/software. Зазначене програмне забезпечення забезпечує форматування накопичувача та запис на нього образу операційної системи.

Після завершення завантаження інсталяційного пакета його необхідно встановити згідно зі стандартною процедурою для відповідної операційної системи. Після завершення інсталяції відкривається інтерфейс програми, який надає користувачеві можливість обрати тип пристрою, операційну систему та цільовий накопичувач для запису образу (Рисунок 3.2.1).

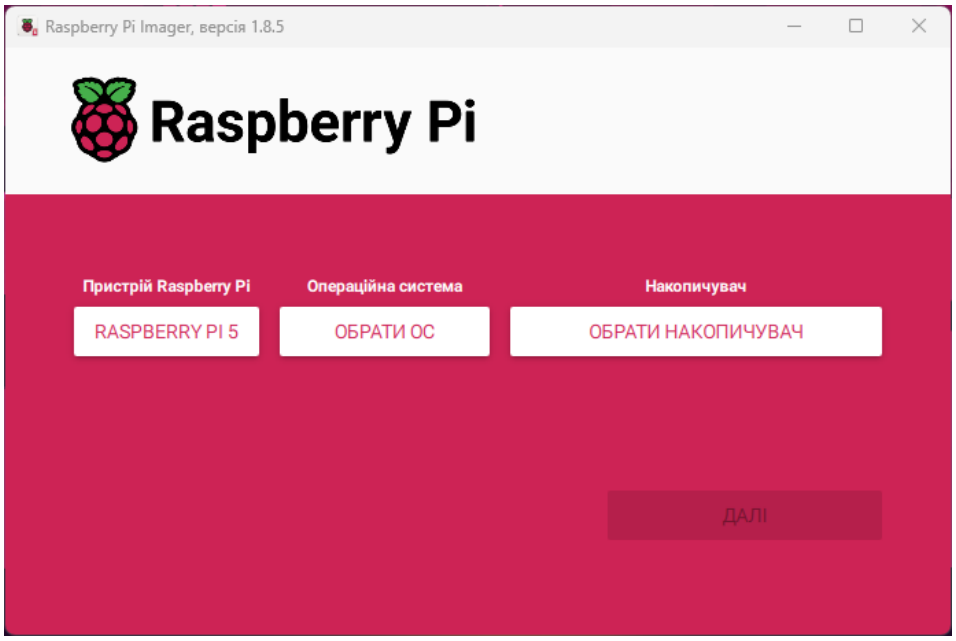

Рисунок 3.2.1 – вікно програми Raspberry Pi manager

Установка операційної системи Kali Linux майже не відрізняється від стандартного процесу установки будь –якої іншої операційної системи але варто звернути увагу на вибір оточення робочого столу (desktop environment)

(див. рисунок 3.2.2), варто вибрати Xfce тому що це оточення робочого столу споживає менше ресурсів ніж Gnome або KDE Plasma, що позитивно скажется на ефективності системи захисту.

Після того як операційну систему було успішно встановлено та налаштовано, необхідно перевірити наявність оновлень системи та встановити їх за необхідності, робиться це за допомогою команди sudo apt update – перевірка списку пакетів, та команди sudo apt upgrade – якщо є доступні оновлення то система почне їхню установку, прогрес установки буде показано у вікні терміналу.

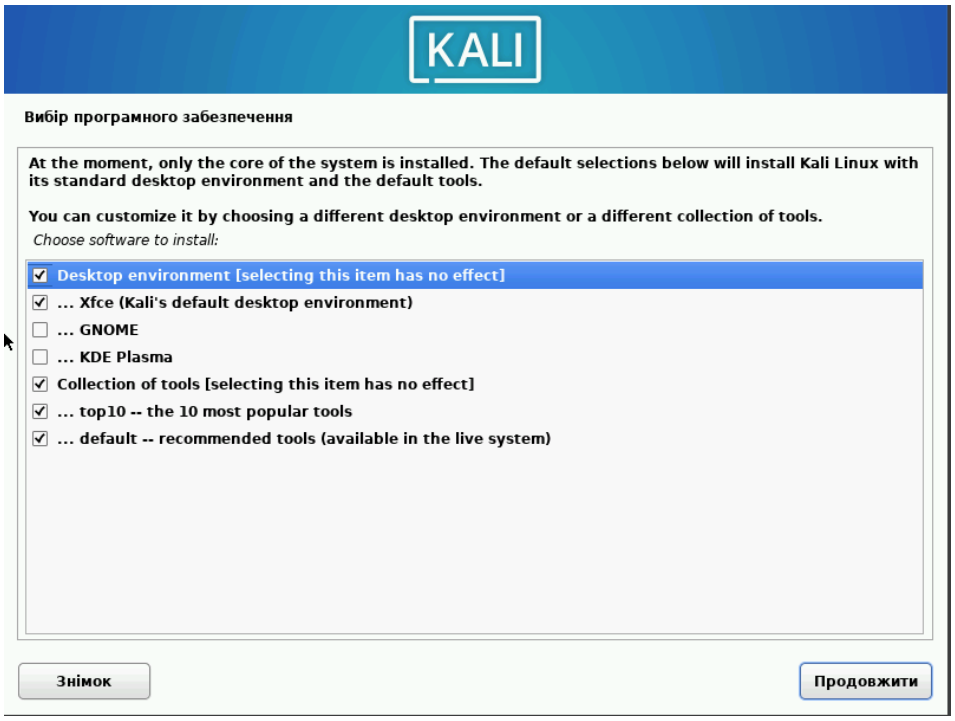

Рисунок 3.2.2 – меню вибору середовища робочого столу в інсталяторі Kali Linux

Після виконання підготовчих робіт необхідно встановити програмне забезпечення, почнемо з встановлення Snort3, для цього необхідно:

Відкрити термінал та ввести, sudo apt install snort –команда яка починає установку Snort3. Система спочатку вибирає та розпаковує різні пакети, від

яких залежить Snort, такі як snort –common, libstro, libfastjson4 та інші (Рисунок 3.2.3)

Після завершення інсталяції програмного забезпечення Snort3 доцільно здійснити перевірку його встановлення та коректності роботи. Для цього в терміналі виконується команда snort –V, яка виводить інформацію щодо поточного стану системи, версії встановленого програмного забезпечення, завантажених правил, а також можливих помилок або конфігураційних зауважень. Результати виконання цієї команди наведено на рисунку 3.2.4.

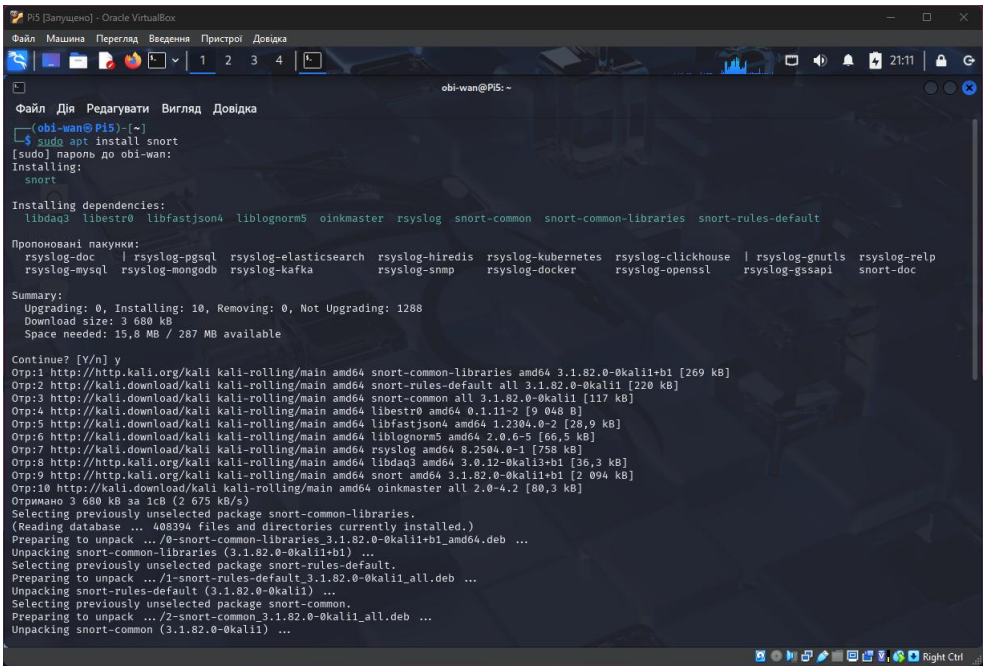

Рисунок 3.2.3 – процесс установки Snort за допомогою терміналу

Рисунок 3.2.4 – виведення інформації про стан програмного забезпечення Snort у термінал Linux

Перед тим, як переходити до конфігурації Snort, рекомендовано ознайомитися з деякими його важливими файлами та їх розташуванням.

Основний файл конфігурації Snort 3 використовує файл конфігурації на основі Lua замість традиційного текстового формату.

Розташування: /etc/snort/snort.lua

Каталог правил містить різні файли правил, які Snort використовує для виявлення підозрілої активності.

Розташування: /etc/snort/rules/

Виконуваний файл Snort має розташування: /etc/bin/snort

Це виконуваний файл для Snort 3.

За замовчуванням Snort 3 зберігає свої файли журналів та сповіщення в цьому каталозі.

Розташування: /var/log/snort/

Файл локальних правил містить перелік правил що до об’єму трафіку та сигнатур атак. В нього дозволяється додавати власні правила.

Розташування: /etc/snort/rules/local.rules

Файл політики за замовчуванням містить конфігурації за замовчуванням і може бути включений до основного файлу конфігурації.

Розташування: /etc/snort/snort_defaults.lua

Для перевірки первірити файлу конфігурації використовується команда sudo snort –c /etc/snort/snort.lua. Ключовою строкою серед масиву інформації про стан файлу конфігурації є повідомлення “Snort successfully validated the configuration (with 0 warnings).” Це означає, що з файл конфігурації є коректним і не містить ніяких помилок. Отже, можна продовжувати роботу далі.

3.3 Snort створення правил. Моніторинг вторгнень з допомогою користувацьких правил

Ефективність Snort для IDS/IPS систем значною мірою залежить від його правил. Ці правила визначають шаблони мережевого трафіку, які можуть вказувати на зловмисну активність. Snort пропонує кілька типів наборів правил:

- Правила спільноти (Community Rules) – безкоштовні, загальнодоступні правила, створені та підтримувані спільнотою Snort. Ці правила забезпечують надійну основу для виявлення поширених загроз.
- Зареєстровані правила (Registered Rules) – доступні безкоштовно після реєстрації. Ці правила більш актуальні, ніж правила спільноти, і оновлюються частіше.
- Правила за передплатою (Subscription Rules) – преміум –правила, доступні за платною підпискою. Вони пропонують найповніший та найновіший захист.

Для системи захисту на базі Raspberry Pi буде застосовано правила спільноти. Хоча вони не такі обширні, як правила за передплатою, вони все одно забезпечують достатній захист від багатьох поширених загроз.

Процедура досить проста і зрозуміла:

1. Відкривається термінал. В термінал вводиться команда wget https://www.snort.org/downloads/community/snort3 –community –rules.tar.gz.
2. Витягування файлу, для цього необхідно ввести в термінал tar -xvzf snort3 -community -rules.tar.gz.
3. Перенос файлів в каталог з правилами Snort. за допомогою команди sudo mv snort3 –community.rules /etc/snort/rules/.
4. Запуск Snort3 з правилами спільноти, ввівши в термінал sudo snort –c /etc/snort/snort.lua –R /etc/snort/rules/snort3 –community.rules та –i wlan0 –A alert_fast.

Ця конфігурація дозволяє Snort моніторити кожен пакет, що проходить через інтерфейс Wlan0. Щоб моніторити всю мережу, потрібно розгорнути Snort на машині, яка діє як мережевий шлюз.

3.4 Uncomplicated Firewall інсталяція та налаштування

Перед початком роботи потрібно відкрити термінал та перевірити наявність оновлень, встановлюємо їх за необхідності командою яку було оголошено раніше.

Першим кроком в терміналі потрібно ввести sudo apt –get install ufw, для встановлення програмного забезпечення.

Після установки програмного забезпечення потрібно перевірити його наявність на пристрої та коректність установки, робиться це за допомогою комнади sudo ufw status, після чого буде показано стан програмного забезпечення рисунок 3.4.1

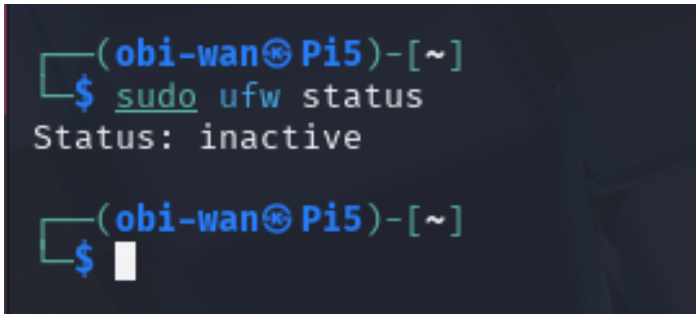

Рисунок 3.4.1 – Перевірка стану UFW

На цьому етапі очікується, що стан міжмережевого екрану UFW буде позначено як «неактивний», оскільки ще не було задано жодних правил фільтрації трафіку.

Для забезпечення належної роботи фаєрвола необхідно задати відповідні правила, які визначатимуть політику обробки вхідного та вихідного мережевого трафіку. За відсутності налаштувань система фільтрації не матиме інструкцій щодо того, які з'єднання вважати потенційно небезпечними або небажаними.

Введення базових правил дозволяє міжмережевому екрану автоматично блокувати несанкціоновані або підозрілі з’єднання ззовні, водночас зберігаючи можливість пристрою ініціювати безпечні вихідні з’єднання з іншими мережами. Таким чином досягається базовий рівень мережевої безпеки без порушення функціональності системи.

Для початку можна спробувати ввести sudo ufw default deny incoming sudo ufw default allow outgoing – ця команда забороняє будь –яке вхідне з'єднання до мережі рисунок 3.4.2.

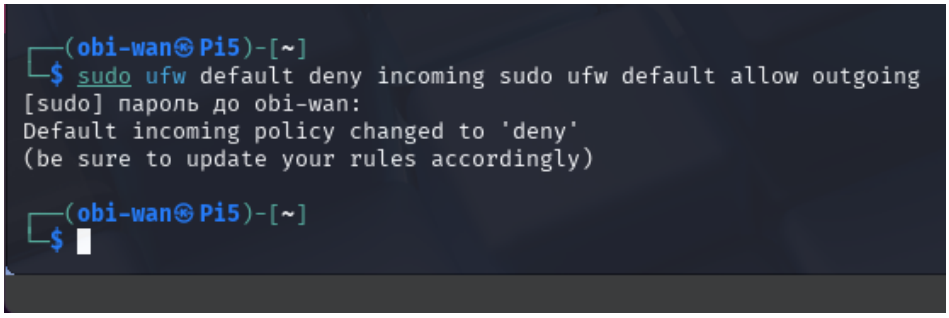

Рисунок 3.4.2 введення заборони на вхідне з’єднання

У подібній конфігурації, коли всі вхідні з’єднання за замовчуванням блокуються, доступ до веб –сервера, розміщеного в межах локальної мережі, стає неможливим для користувачів, які намагаються підключитися до нього ззовні, зокрема через глобальну мережу Інтернет.

Для забезпечення доступності веб –сервера ззовні необхідно явно дозволити вхідні з’єднання на відповідні мережеві порти, що використовуються для обробки запитів, для дозволу прийому трафіку на порті небхідно ввести в терміналі sudo ufw allow 80 sudo ufw allow 443 де 80 порт HTTP а 443 порт HTTPS, рисунок 3.4.3.

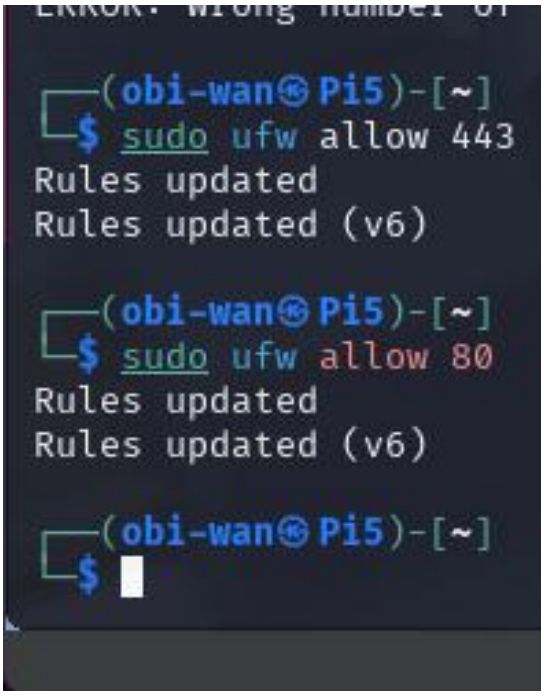

Рисунок 3.4.3. застосування правила до портів

Як видно на зображені рисунок 3.4.4 термінал сповістив нас про те що фаєрвол активовано і він буде вмикатися разом з системою.

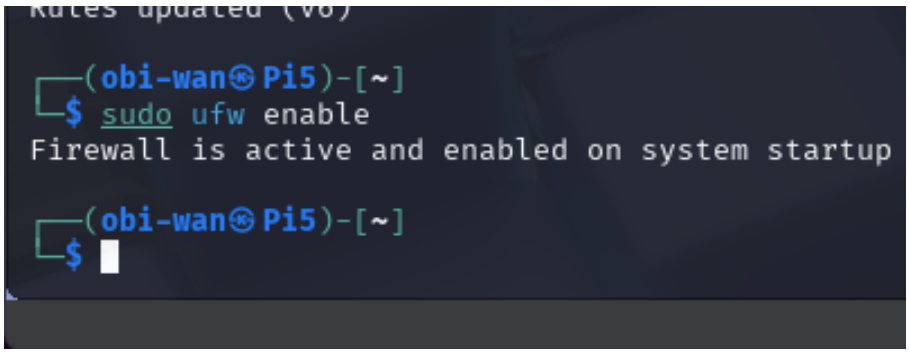

Рисунок 3.4.4 активація фаєрволу

Також можливо перевірити роботу фаєрвола і пересвідчитися чи правильно введено правила і чи виконує їх фаєрвол для цього необхідно ввести в термінал sudo ufw status, ця команда показує нам стан фаєрвола.

Рисунок 3.4.5 стан фаєрволу

Згідно із зображенням рисунок 3.4.5 правила введено правильно і вони виконуються.

ВИСНОВКИ

Дана кваліфікаційна робота мала на меті розробку та всебічне дослідження бюджетного рішення для забезпечення високого рівня мережевої безпеки малих комп'ютерних мереж шляхом інтеграції функціоналу міжмережевого екрану та системи виявлення/запобігання вторгненням. Всі поставлені завдання було успішно реалізовано, що дозволило отримати низку значущих науково-практичних результатів та підтвердити принципову можливість побудови ефективної системи захисту з мінімальними фінансовими витратами, використовуючи одноплатний мікрокомп'ютер Raspberry Pi як центральну апаратну платформу.

На початковому етапі дослідження було проведено ґрунтовний аналіз сучасних загроз інформаційній безпеці, що дозволило ідентифікувати ключові вектори атак, актуальні для малих мереж, а також визначити вимоги до засобів їхнього запобігання та виявлення. Огляд існуючих комерційних та програмних рішень для мережевого захисту підкреслив необхідність розробки доступної альтернативи, здатної забезпечити адекватний рівень безпеки без значних капіталовкладень. Саме цей аспект став рушійною силою для вибору Raspberry Pi як базової апаратної платформи.

Детальне вивчення характеристик та можливостей мікрокомп'ютера Raspberry Pi, зокрема моделі Raspberry Pi 5, підтвердило його повну відповідність поставленим задачам. Було встановлено, що високопродуктивний 64-бітний процесор ARM Cortex-A76, достатній обсяг оперативної пам'яті (4-8 ГБ LPDDR4X), наявність гігабітного Ethernet-порту та підтримка високошвидкісних бездротових з'єднань Wi-Fi 802.11ac надають цій платформі необхідну обчислювальну потужність та пропускну здатність для ефективної обробки мережевого трафіку. Додатковими перевагами стали компактність пристрою, його низьке енергоспоживання, що є критично важливим для цілодобової роботи, та загальна економічна доступність.

Вибір програмного забезпечення також був ретельно обґрунтований. В якості базової операційної системи обрано дистрибутив Kali Linux, який, будучи похідним від Debian, надає широкі можливості для конфігурації мережевих інтерфейсів, встановлення та керування необхідними сервісами, а також містить велику кількість попередньо встановлених інструментів для аналізу безпеки, що було корисним на етапі тестування та налагодження.

Для реалізації функціоналу міжмережевого екрану було обрано Uncomplicated Firewall (UFW). Його переваги полягають у простоті конфігурації та інтуїтивно зрозумілому синтаксисі команд, що значно спрощує керування правилами фільтрації трафіку в порівнянні з безпосереднім використанням iptables, зберігаючи при цьому всю потужність ядра Netfilter. Це дозволило ефективно налаштувати дозвіл та заборону з'єднань, захищаючи внутрішню мережу від несанкціонованого зовнішнього доступу та контролюючи вихідний трафік.

Центральним елементом системи виявлення та запобігання вторгненням стала система Snort3. Її архітектура, що характеризується високою продуктивністю завдяки багатопоточності та модульності, дозволяє здійснювати глибокий пакетний аналіз у реальному часі. Було реалізовано конфігурацію Snort3 для моніторингу мережевого трафіку, застосування сигнатурного аналізу для виявлення відомих типів атак та аномалій. Особлива увага приділялася розробці та впровадженню користувацьких правил для Snort3, що дозволило адаптувати систему до специфічних загроз, характерних для захищуваної мережі, та підвищити точність виявлення цільових атак. Можливість автоматичного генерування сповіщень та блокування підозрілої активності за фактом спрацьовування правил є ключовим аспектом проактивного захисту.

Проектування архітектури системи передбачало оптимальне розміщення Raspberry Pi у мережевій інфраструктурі та конфігурацію його мережевих інтерфейсів у режимі мосту або маршрутизатора, що забезпечує ефективну фільтрацію та моніторинг всього трафіку, що проходить через систему. Для

верифікації працездатності та ефективності розробленого рішення було проведено його моделювання у віртуальному середовищі VirtualBox, що дозволило відпрацювати сценарії розгортання та початкової конфігурації без ризику впливу на реальну мережу. Додатково, тестування функціональності було здійснено в симуляторі Cisco Packet Tracer, який надав можливість імітувати різноманітні сценарії мережевих атак (такі як сканування портів, спроби проникнення, відмова в обслуговуванні) та перевірити адекватність реакції системи. Отримані результати підтвердили, що запропоноване рішення на базі Raspberry Pi з інтегрованими UFW та Snort3 здатне ефективно виявляти та блокувати широкий спектр мережевих загроз, демонструючи високу надійність та відмовостійкість.

Отже, дане дослідження успішно демонструє, що Raspberry Pi є не лише життєздатним, але й економічно вигідним рішенням для створення надійної системи захисту малих комп'ютерних мереж. Розроблена система може слугувати повноцінною альтернативою значно дорожчим комерційним апаратним комплексам, забезпечуючи при цьому гнучкість налаштувань, можливість масштабування та високу адаптивність до специфічних потреб користувача. Економічна доцільність, поєднана з високим рівнем функціональності, робить дане рішення особливо привабливим для приватних користувачів, малого та середнього бізнесу, а також освітніх установ, які потребують ефективного захисту інформаційних ресурсів в умовах обмеженого бюджету.

Перспективи подальших досліджень та розвитку даного рішення включають розширення його функціоналу шляхом інтеграції додаткових модулів, таких як системи аналізу поведінки користувачів (UEBA), централізовані системи керування журналюванням (SIEM Lite) для агрегації та аналізу подій безпеки. Також вбачається необхідність розробки більш інтуїтивно зрозумілого графічного інтерфейсу користувача, що спростить процес конфігурації та моніторингу для неспеціалістів. Додатково, варто

дослідити можливості впровадження методів машинного навчання для виявлення нових, раніше невідомих загроз, а також розширення масштабованості рішення для потенційного застосування у більших корпоративних мережах та його інтеграції з хмарними сервісами безпеки, що дозволить підвищити рівень автоматизації та централізації управління безпекою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Connect, protect, and build everywhere Cloudflare : веб –сайт : URL: https://www.cloudflare.com (Дата звернення 15.01.2025).
2. 5 Steps to Zero Trust Network Access: Creating Your First USe Cases веб –сайт: URL: https://blackberry.bakotech.com/en/5 –steps –to –implementing – zero –trust –network –access (дата звернення 15.01.2025).
3. Leading Cloud Enterprise Security Provider for Zero Trust: веб –сайт: URL: https://www.zscaler.com (дата звернення 15.01.2025).
4. Cisco Umbrella | Leader in Cloud Cybersecurity and SASE Solutions : Веб –сайт: URL: https://umbrella.cisco.com (дата звернення 17.01.2025).
5. Cisco Firepower Next –Generation Firewall At –a –Glance – at – aglance –c45 –736624.pdf:URL: https://www.cisco.com/c/dam/global/en_uk/assets/pdfs/at –a –glance –c45 – 736624.pdf (дата звернення 17.01.2025).
6. Raspberry Pi Datasheets: веб –сайт: URL: https://datasheets. raspberrypi.com (Дата звернення 19.01.2025).
7. Raspberry Pi Ltd. Raspberry Pi 5 –Raspberry Pi Ltd: даташит, січень 2025 6 с. : raspberry –pi –5 –product –brief.pdf https://datasheets.raspberrypi.com/rpi5/ raspberry –pi –5 –product –brief.pdf (дата звернення 19.01.2025).
8. Raspberry Pi. Урок 3. Налаштування мережі: веб –сайт: URL: https://raspberry.com.ua/raspberry –pi –lesson –3/ (дата звернення 16.01.2025).
9. netfilter/iptables project homepage –The netfilter.org project: ваб –сайт: URL: https://netfilter.org (дата звернення 10.02.2025).
10. Case for Raspberry Pi 5 –Raspberry Pi ltd: даташит, травень 2024 8 с. :URL : https://datasheets.raspberrypi.com/case/case –for –raspberry –pi –5 –product –brief.pdf (дата звернення 22.04.2025).

11. Raspberry Pi OS – Raspberry Pi: веб –сайт: URL: https://www.raspberrypi. com/ software (дата звернення 23.02.2025).

12. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution: ваб –сайт: URL: https://www.kali.org (дата звернення 23.02.2025).

13. Базові команди в Linux для початківців – aCode: веб –сайт: URL https://acode.com.ua/basic –commands –linux (дата звернення 23.02.2025).

14. Build a Raspberry Pi IDS/IPS with Snort Tutorial: веб –сайт: URL: https://thesecmaster.com/blog/turn –your –raspberry –pi –as –a –ids –ips –box –and –hunt –for –potential –intrusions –on –your (дата звернення 30.04.2025)

15. Setting Up Raspberry Pi Firewall : 10 Steps – Instructables: веб –сайт: URL: https://www.instructables.com/Setting –Up –a –Raspberry –Pi –Firewall

16. raspberry –pi –5 –mechanical –drawing: веб –сайт URL: https://datasheets.raspberrypi.com/rpi5/raspberry –pi –5 –mechanical –drawing.pdf (дата звернення 20.04.2025).