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

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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Комп'ютерна система блокування реклами в локальній мережі на базі Raspberry PI

Виконав: студент 4 курсу, групи СІ-41
спеціальності 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

		Мордованець А. В.
	(підпис)	(прізвище та ініціали)
Керівник		*Варавін А.В*
	(підпис)	(прізвище та ініціали)
Нормоконтроль		*Луцик Н. С*
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		Осухівська Г.М.
	(підпис)	(прізвище та ініціали)
Рецензент		
	(підпис)	(прізвище та ініціали)

Тернопіль
2025

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

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

Кафедра *комп'ютерних систем та мереж*
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
«27» січня 2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *бакалавр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студента *Мордованець Артем Васильович*
(прізвище, ім'я, по батькові)

1. Тема роботи *Комп'ютерна система блокування реклами в локальній мережі на базі Raspberry PI*

Керівник роботи *к.ф.-м.н., ст. викл. Варавін А.В.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від *« 27 » січня 2025 року № 4/7-53*
2. Термін подання студентом завершеної роботи *20.06.2025*
3. Вихідні дані до роботи *Технічне завдання*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз технічного завдання
2. Проєктна частина
3. Практична частина
4. Безпека життєдіяльності, основи охорони праці.
Висновки
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Структура системи в локальній мережі
2. Блок-схеми алгоритму роботи системи
3. Блок-схема автоматичного оновлення чорних списків
4. Логічна структурна схеми адресації пристроїв
5. Графік блокування запитів

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці			

7. Дата видачі завдання *27.01.2025 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Розробка технічного завдання.*	*27.01.2025р. – 02.02.2025р.*	*Викон.*
2.	*Аналіз предметної області та постановка задачі*	*03.02.2025 р. – 16.02.2025 р.*	*Викон.*
3.	*Вибір інструментів і розробка архітектури системи*	*17.02.2025 р. – 02.03.2025 р.*	*Викон.*
4.	*Реалізація та тестування системи*	*03.03.2025 р. – 23.03.2025 р.*	*Викон.*
5.	*Безпека життєдіяльності, основи охорони праці*	*01.06.2025 р.- 08.06.2025 р.*	*Викон.*
6.	*Оформлення пояснювальної записки і графічного матеріалу*	*07.04.2025 р. – 08.06.2025 р.*	*Викон.*
7.	*Перевірка на академічний плагіат, перевірка керівником та консультантами*	*9.06.2025р. – 15.06.2025р.*	
8.	*Попередній захист кваліфікаційної роботи бакалавра*	*16.06.2025р. – 22.06.2025р.*	*Викон.*
9.	*Захист кваліфікаційної роботи бакалавра*	*27.06.2025р.*	*Викон.*

Студент _____ *Мордованець А. В.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Варавін А.В*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Мордованець Артем Васильович . Комп’ютерна система блокування реклами в локальній мережі на базі Raspberry PI: робота на здобуття кваліфікаційного ступеня бакалавра: спец. 123 — комп’ютерна інженерія. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2025. — 77 с.

Ключові слова: комп’ютерна система блокування реклами, Raspberry Pi 4, Pi-hole, локальна мережа, програмне забезпечення.

Кваліфікаційну роботу бакалавра присвячено розробці комп’ютерної системи блокування реклами в локальній мережі. На основі результатів огляду та аналізу аналогів розроблено структурну схему системи блокування реклами. Здійснено обґрунтування вибору апаратної платформи, а саме Raspberry Pi 4, та програмного забезпечення Pi-hole, а також проведено їх порівняння з альтернативними рішеннями. Описано процес розробки, налаштування та тестування системи в умовах локальної мережі. Розглянуто алгоритм роботи та механізми забезпечення ефективного блокування небажаного контенту. Визначено ключові вимоги до продуктивності, безпеки та інтерфейсів управління системою. Розглянуто основні питання безпеки життєдіяльності та охорони праці, пов’язані з експлуатацією розробленої системи.

ANNOTATION

Mordovanets Artem Vasylyovych Computer system for blocking advertising in a local network based on Rasbery PI: Bachelor’s Graduation Thesis: speciality 123 — computer engineering. Ternopil: Ternopil Ivan Puluj National Technical University, 2025. — 77 p.

Keywords: computer system for blocking advertising, Raspberry Pi 4, Pi-hole, local network, software.

The bachelor's qualification work is devoted to the development of a computer system for blocking advertising in a local network. Based on the results of the review and analysis of analogues, a structural diagram of the advertising blocking system was developed. The choice of the hardware platform, namely Raspberry Pi 4, and the Pi-hole software were justified, and their comparison with alternative solutions was carried out. The process of developing, configuring and testing the system in a local network was described. The algorithm of operation and mechanisms for ensuring effective blocking of unwanted content were considered. Key requirements for performance, security and system management interfaces were determined. The main issues of life safety and labor protection related to the operation of the developed system were considered.

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

CPU – Central Processing Unit

DNS – Domain Name System

GUI – Graphical User Interface

IP – Internet Protocol

LAN – Local Area Network

OS – Operating System

RAM – Random Access Memory

RPI – Raspberry Pi

UPS – Uninterruptible Power Supply

USB – Universal Serial Bus

WAN – Wide Area Network

Wi-Fi – Wireless Fidelity

ВСТУП

У сучасному цифровому середовищі доступ до мережі Інтернет є невід’ємною складовою життя більшості користувачів. Разом із розширенням функціональних можливостей Інтернету значно зростає й обсяг рекламного контенту, що впливає не лише на комфорт користування вебресурсами, а й на безпеку та швидкодію мережевих з’єднань. Надмірна кількість реклами, зокрема інтерактивної, відеореклами, трекерів та скриптів, уповільнює завантаження сторінок, створює додаткове навантаження на мережеві ресурси та нерідко виступає каналом збору особистих даних користувача.

Для вирішення цих проблем дедалі частіше застосовуються спеціалізовані інструменти, зокрема програми блокування реклами. Проте більшість таких інструментів встановлюються локально на кожен пристрій, що не завжди зручно або ефективно в умовах багатокористувацьких мереж, наприклад удома, в офісах або навчальних закладах. У цьому контексті особливий інтерес становить можливість централізованого блокування небажаного контенту на рівні локальної мережі, що дозволяє контролювати весь вхідний трафік без потреби додаткового налаштування на кожному окремому пристрої.

Одним із найпоширеніших рішень для реалізації такої централізованої системи є використання платформи Raspberry Pi – компактного одноплатного комп’ютера з низьким енергоспоживанням та широкими можливостями налаштування. На базі Raspberry Pi можна розгорнути систему Pi-hole, що виступає DNS-фільтром і забезпечує блокування запитів до відомих рекламних доменів, працюючи як "мережевий фільтр реклами".

Актуальність обраної теми обумовлюється підвищеною потребою у засобах захисту користувача від агресивної реклами та зловмисного програмного забезпечення, підвищенням продуктивності роботи мережі та оптимізацією пропускної здатності інтернет-каналу. Використання недорогих і енергоефективних рішень, таких як Raspberry Pi, дає змогу впроваджувати

ефективні інструменти блокування навіть у побутових умовах.

Мета даної кваліфікаційної роботи полягає у розробці, налаштуванні та тестуванні комп'ютерної системи блокування реклами в локальній мережі з використанням Raspberry Pi, яка забезпечить захист усіх пристроїв мережі від небажаного контенту, підвищить безпеку користувачів і покращить швидкодію підключення до Інтернету.

Для досягнення поставленої мети у роботі буде проведено аналіз наявних технологій блокування реклами, розглянуто принципи роботи DNS-фільтрації, спроектовано архітектуру системи, виконано її розгортання, протестовано функціональність та проаналізовано результати ефективності фільтрації в умовах реальної мережі.

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Аналіз вимог до комп'ютерної системи блокування реклами в локальній мережі

Комп'ютерна система блокування реклами в локальній мережі має відповідати різному роду вимог, які можна розділити на функціональні, технічні та експлуатаційні. Головною метою такої системи є забезпечення ефективної фільтрації рекламного контенту без негативного впливу на роботу мережі та її продуктивність.

Функціональні вимоги включають точність і швидкість блокування небажаного контенту та також попередження про його наявність. Система повинна вміти визначати рекламні запити та блокувати їх, використовуючи фільтри на рівні DNS, HTTP, а також аналізу глобального трафіку. Важливим аспектом є можливість автоматично оновлювати списки заблокованих доменів та підтримувати користувацькі налаштування, що дає змогу адміністраторам мережі адаптувати систему під специфічні вимоги та зміну поведінко рекламних стратегій [1].

З технічної точки зору система має бути сумісною з різними типами пристроїв, що підключені до локальної мережі, та не викликати суттєвих затримок у передачі даних. Вона може бути реалізована на базі Raspberry Pi з використанням Pi-hole, AdGuard Home або альтернативних рішень. Доцільно оцінити апаратні обмеження, такі як обсяг оперативної пам’яті, обчислювальна потужність та енергоспоживання пристрою.

Експлуатаційні вимоги включають зручність налаштування та адміністрування. Користувачі повинні мати доступ до статистики заблокованого контенту, а також можливість швидко змінювати

політики фільтрації. Також варто врахувати рівень безпеки системи, зокрема її захищеність від підробки DNS-запитів і спроб обходу блокування.

Для сучасної мережевої системи блокування реклами можна розгорнути кілька основних груп вимог: функціональні, технічні, безпекові і експлуатаційні.

Основні вимоги системи блокування рекламної діяльності:

— Функціональні вимоги - фільтрація реклами рівня DNS, IP і HTTP(S)-трафіку, автоматичне оновлення списків заборонених домен та гнучка політика фільтрації для різноманітних користувачів;

— Технічні умови - відповідність різним операційним системам та мережевим протоколам, мінімальне зниження швидкості передачі даних та можливість роботи на різному обладнанні (наприклад, Raspberry Pi);

— Безпекові умови - захист від підміни DNS-запитів і спроб обходу блокування, логування та моніторинг трафіку для розпізнавання підозрілої діяльності та захист від атак зловмисників, зокрема DDoS;

— Експлуатаційні потреби - інтуїтивно зрозумілий інтерфейс управління веб-сайтів, додатками, статистика та звітність щодо заблокованих ресурсів та попередження стосовно важливих подій та можливість швидкого налаштування.

Системою має здійснюватися ефективна фільтрація рекламного контенту без відчуття впливу на рівень мережевої продуктивності. Вона повинна забезпечувати різні засоби блокування, зокрема DNS-filtering, блокування за IP-адресами та аналіз трафіку HTTP(S). У разі необхідно передбачити можливість автоматичного оновлення списків заблокованих джерел, а також можливістю зміну правил фільтрування для різних користувальних груп [2].

Застосування цих вимог забезпечить розвиток ефективної та стійкої системи блокування реклами. Всі вимоги покривають інтересами користувачів та забезпечуваної високого рівня якості роботи мережі.

Вимоги до продуктивності системи блокування реклами в локальній мережі з точки зору комп'ютерної інженерії залежать від кількох ключових параметрів: пропускної здатності мережі, швидкості обробки запитів, навантаження на обладнання та часу відгуку. Система має забезпечувати мінімальну затримку DNS-запитів. У стандартних умовах середній час обробки DNS-запиту не повинен перевищувати 5–10 мілісекунд. Оптимальний рівень продуктивності – до 1 мс для локальних кешованих запитів [3].

Пропускна здатність системи залежить від кількості оброблюваних запитів. Наприклад, Raspberry Pi 4 із 4 ГБ оперативної пам'яті здатний обробляти понад 100 000 DNS-запитів на годину при середньому навантаженні, що робить його придатним для домашніх і малих корпоративних мереж (до 50 одночасних користувачів). У великих мережах (100+ клієнтів) може знадобитися серверний варіант із більшою кількістю ядер процесора та додатковим кешуванням.

Використання кешування значно покращує продуктивність. Для популярних доменів (Google, YouTube, Facebook) кешований DNS-запит повинен оброблятися за менше ніж 1 мс, що дозволяє знизити навантаження на центральний процесор і мережевий інтерфейс.

Щодо апаратного забезпечення, мінімальні вимоги для ефективної роботи включають:

— Процесор: 4-ядерний ARM Cortex-A72 (1,5 ГГц) або x86-64 (2+ ядра, 2 ГГц)

— Оперативна пам'ять: 2–4 ГБ (для підтримки кешу на 1–2 мільйони записів)

— Мережевий інтерфейс: Гігабітний Ethernet (1 Gbps) для забезпечення низької затримки

Для великих підприємств рекомендується використовувати виділений сервер або віртуалізоване середовище з процесорами Intel Xeon (8+ ядер) та оперативною пам'яттю 16 ГБ+ для швидкого аналізу великого потоку трафіку.

Таким чином, продуктивність системи блокування реклами має відповідати розміру мережі, з урахуванням кількості запитів і необхідної швидкодії. Ефективне використання кешування та потужнішого обладнання дозволяє підтримувати стабільну роботу навіть у навантажених мережах.

Система має використовувати DNS-over-HTTPS (DoH) або DNS-over-TLS (DoT) для шифрування DNS-запитів, щоб унеможливити їхню підбірку в локальній або глобальній мережі. Також важливо забезпечити механізми перевірки автентичності відповідей від DNS-серверів, наприклад, через DNSSEC.

Користувачі можуть намагатися обходити систему за допомогою VPN, проксі-серверів або альтернативних DNS-серверів. Щоб цього уникнути, необхідно:

— Блокувати альтернативні DNS-запити (порт 53, 853, 443) та маршрутизацію через сторонні VPN.

— Використовувати форсований DNS (Forced DNS Redirection) для примусового перенаправлення всього трафіку через сервер фільтрації.

— Аналізувати трафік за допомогою Deep Packet Inspection (DPI) для виявлення зашифрованих DNS-запитів до сторонніх серверів.

Для захисту адміністративного інтерфейсу необхідно використовувати:

— Двофакторну аутентифікацію (2FA) для входу в панель керування.

— Захист від Brute-force атак через ліміт запитів та блокування IP після кількох невдалих спроб входу.

— Обмеження доступу до адміністративного інтерфейсу лише з довірених IP-адрес або через VPN.

Захист від DDoS-атак

Система повинна мати механізми виявлення та пом’якшення DDoS-атак, які можуть спрямовувати велику кількість DNS-запитів для перевантаження сервера. Для цього можна використовувати:

— Rate-limiting – обмеження частоти запитів від окремих IP-адрес.

— Failover-систему – автоматичне перемикання на резервний сервер у разі перевантаження.

— Використання фільтрації трафіку на рівні мережевого обладнання для блокування підозрілих запитів.

Операційна система та програмне забезпечення системи блокування реклами повинні регулярно оновлюватися, щоб уникнути вразливостей. Це включає:

— Автоматичне встановлення оновлень безпеки.

— Відключення небезпечних служб та відкритих портів, які не використовуються.

— Моніторинг нових вразливостей і швидке впровадження патчів.

Дотримання цих вимог дозволить значно підвищити безпеку системи блокування реклами, мінімізувати ризики зовнішніх атак і забезпечити стабільну роботу в локальній мережі.

1.2 Аналіз можливих рішень для блокування реклами в локальних мережах

Рішення для блокування реклами в локальній мережі повинене враховувати різні методи фільтрації, їхню ефективність, продуктивність, сумісність із сучасними мережами та безпеку. Основними підходами до реалізації такої системи є використання:

— DNS-фільтрації;

— Проксі-серверів;

— Рівневого блокування через брандмауери.

Рішення на основі проксі-серверів, такі як Squid, Privoxy або Mitmproxy, дозволяють здійснювати глибший аналіз HTTP- і HTTPS-запитів. Вони можуть не тільки блокувати рекламу на рівні доменів, але й фільтрувати конкретні елементи сторінки, наприклад, рекламні скрипти або банери. Squid використовується як кешуючий проксі, що дозволяє зменшити навантаження

на зовнішні мережеві ресурси та фільтрувати небажаний контент. Privoxy пропонує розширені можливості редагування HTTP-трафіку та блокує рекламні елементи за шаблонами. Mitmproxy дозволяє здійснювати аналіз і модифікацію HTTPS-запитів, але для цього потрібно встановлювати додаткові сертифікати на клієнтських пристроях, що ускладнює розгортання у великих мережах. Основна перевага проксі-фільтрації – це гнучкість у налаштуванні та можливість блокування більш складної реклами, включаючи відеорекламу або динамічно завантажувані елементи. Однак вона має недоліки у вигляді вищого споживання ресурсів і необхідності конфігурації клієнтів для використання проксі [4].

Брандмауери та маршрутизатори з підтримкою розширених правил блокування можуть використовувати фільтрацію трафіку на рівні IP-адрес та доменів. Наприклад, pfSense або OPNsense дозволяють налаштовувати правила блокування для певних категорій веб-сайтів, інтегруючись з сервісами списків блокування (наприклад, pfBlockerNG) [5].

Такий підхід ефективний для корпоративних мереж, оскільки не потребує змін на клієнтських пристроях і забезпечує централізоване адміністрування. Для досягнення максимальної ефективності можна комбінувати кілька методів. Наприклад, використання Pi-hole для DNS-фільтрації в поєднанні з Squid або Privoxy для глибшого аналізу HTTP-трафіку дозволяє блокувати рекламу навіть у складних випадках. Додатково можна інтегрувати брандмауерні рішення для централізованого керування доступом у корпоративних мережах.

При виборі апаратного забезпечення для системи блокування реклами в локальній мережі необхідно враховувати продуктивність процесора, обсяг оперативної пам’яті, швидкість мережевих інтерфейсів і енергоспоживання. Оскільки основні завдання такої системи зводяться до обробки DNS-запитів, кешування та можливого проксування трафіку, ключовими характеристиками є швидкодія CPU, кількість доступних потоків і обсяг RAM [6].

Серед найпопулярніших платформ для реалізації такого рішення – Raspberry Pi, Odroid, x86-сервери та мікрокомп'ютери на базі Intel NUC або Mini PC. Для порівняння розглянемо кілька популярних моделей Таблиця 1.

Таблиця 1 - Платформи для системи блокування реклами

Параметр	Raspberry Pi 4 Model B	Raspberry Pi 5	Intel NUC (J4125)	x86-сервер (i3-10100)
Процесор	Broadcom BCM2711 (4 × 1.5 ГГц)	Broadcom BCM2712 (4 × 2.4 ГГц)	Intel Celeron J4125 (4 × 2.7 ГГц)	Intel Core i3-10100 (4 × 3.6 ГГц)
RAM	2-8 ГБ LPDDR4-3200	4-8 ГБ LPDDR4X-4267	8 ГБ DDR4	16-32 ГБ DDR4
Мережевий інтерфейс	1× Gigabit Ethernet	1× 2.5G Ethernet	2× Gigabit Ethernet	2× Gigabit Ethernet
Накопичувач	microSD, USB 3.0 SSD	microSD, PCIe NVMe	SSD M.2	SSD/HDD
Споживана потужність	~5-7 Вт	~7-9 Вт	~10-15 Вт	~30-50 Вт
Вартість (USD)	50-80	80-120	200-300	400+

Для домашніх мереж або малих офісів (до 50 пристроїв) достатньо Raspberry Pi 5. Якщо система розгортається у середніх офісах або підприємствах (50-200 пристроїв), краще використовувати Odroid N2+ або Intel NUC. Великі мережі (200+ пристроїв) вимагають продуктивності x86-серверів, що дозволяє забезпечити безперебійну роботу системи блокування реклами з мінімальними затримками.

Для реалізації системи блокування реклами в локальній мережі необхідно обрати апаратну платформу, яка забезпечить стабільну роботу DNS-фільтрації, проксування трафіку та можливе ведення логування. Одноплатні комп'ютери (SBC) є відмінним вибором завдяки низькому енергоспоживанню, компактності та підтримці Linux-дистрибутивів (табл. 2).

Таблиця 2 - Найпопулярніші SBC

Параметр	Raspberry Pi 5	Raspberry Pi 4 Model B	Odroid N2+	Rock 5B (RK3588)	Orange Pi 5+
Процесор	Broadcom BCM2712 (4 × 2.4 ГГц)	Broadcom BCM2711 (4 × 1.5 ГГц)	Amlogic S922X (6 × 2.2 ГГц)	Rockchip RK3588 (8 × 2.4 ГГц)	Rockchip RK3588S (8 × 2.4 ГГц)
RAM	4-8 ГБ LPDDR4X-4267	2-8 ГБ LPDDR4-3200	4-8 ГБ LPDDR4	4-16 ГБ LPDDR4	4-16 ГБ LPDDR4
Мережевий інтерфейс	1× 2.5G Ethernet	1× Gigabit Ethernet	1× Gigabit Ethernet	2× 2.5G Ethernet	2× 2.5G Ethernet
Накопичувач	microSD, PCIe NVMe	microSD, USB 3.0 SSD	microSD, eMMC	eMMC, NVMe	eMMC, NVMe
Споживана потужність	~7-9 Вт	~5-7 Вт	~6-8 Вт	~10-15 Вт	~10-15 Вт
Вартість (USD)	80-120	50-80	100-150	150-200	130-180

Аналіз продуктивності SBC для блокування реклами:

— Raspberry Pi 5 – покращений варіант порівняно з попередньою версією, що має вищу тактову частоту та швидший інтерфейс PCIe для SSD. Завдяки 2.5G Ethernet забезпечує кращу швидкість роботи у мережах.

— Raspberry Pi 4 Model B – хороший бюджетний варіант для невеликих локальних мереж (до 50 клієнтів), але його продуктивності може не вистачати при високих навантаженнях.

— Odroid N2+ – потужніше рішення завдяки 6-ядерному процесору, що дозволяє швидше обробляти DNS-запити та вести кешування. Висока ефективність для середніх офісів.

— Rock 5B (RK3588) – один із найпродуктивніших одноплатних комп’ютерів із підтримкою NVMe SSD та 2.5G Ethernet, що робить його ідеальним для великих мереж.

— Orange Pi 5+ – аналогічний Rock 5B, проте трохи дешевший і має хороші можливості розширення.

Якщо необхідна проста система для невеликої мережі, Raspberry Pi 5 буде хорошим вибором. Для середніх офісів (50-200 пристроїв)

рекомендується Odroid N2+ або Rock 5B завдяки потужним процесорам та підтримці швидких накопичувачів. У випадку великих мереж або потреби в максимальній швидкодії варто обирати Orange Pi 5+ або Rock 5B, які мають потужні процесори та 2.5G Ethernet, що дозволяє обробляти великий потік запитів без значних затримок.

Комп'ютерна система блокування реклами в локальній мережі на базі Raspberry Pi повинна відповідати кільком важливим вимогам для ефективного функціонування. Основний функціональний аспект полягає у фільтрації на основі DNS, що дозволяє блокувати всі рекламні домени ще до того, як вони досягнуть пристроїв користувачів. Це усуває необхідність встановлення окремих блокувальників реклами на кожному пристрої та забезпечує безперервний позитивний користування мережею. Додатково система має підтримувати налаштування 'чорних' і 'білих' списків, що дає користувачам гнучко керувати фільтрацією відповідно до своїх потреб. (табл. 3).

Таблиця 3 - Основні характеристики Raspberry Pi 4 Model B

Параметр	Характеристика
Процесор (CPU)	Broadcom BCM2711, 4 ядра Cortex-A72 (ARM v8), 1.5 ГГц
Графічний процесор (GPU)	VideoCore VI, підтримка OpenGL ES 3.0, декодування H.265 (4Kp60)
Оперативна пам'ять (RAM)	2 ГБ, 4 ГБ або 8 ГБ LPDDR4-3200
Постійна пам'ять	microSD, підтримка USB 3.0 SSD, можливість підключення через PCIe (обхідний адаптер)
Мережевий інтерфейс	1× Gigabit Ethernet (до 1000 Мбіт/с)
Бездротові комунікації	Wi-Fi 802.11ac (2.4/5 ГГц), Bluetooth 5.0
Порти USB	2× USB 3.0, 2× USB 2.0
Порти відеовиходу	2× micro-HDMI (до 4Kp60)
Живлення	USB-C (5В, 3А)
Енергоспоживання	5-7 Вт у середньому навантаженні
Охолодження	Пасивне (радіатор) або активне (вентилятор, додатковий модуль)
Габарити	85.6 мм × 56.5 мм

Продуктивність і масштабованість відіграють ключову роль в ефективності системи. Для забезпечення плавного користувацького досвіду

система блокування реклами повинна мінімізувати затримку під час обробки DNS-запитів. З огляду на обмежену обчислювальну потужність Raspberry Pi, рішення має бути оптимізоване для ефективного використання ресурсів, щоб навіть при великому мережевому навантаженні працювати без значних уповільнень.

Безпека і конфіденційність є першочерговими аспектами під час розробки такої системи. Важливо забезпечити цілісність даних шляхом коректної обробки DNS-відповідей, запобігаючи помилковому блокуванню легітимного трафіку. Для захисту від атак типу DNS-спуфінгу система повинна підтримувати такі технології, як DNS-over-HTTPS (DoH) або DNS-over-TLS (DoT). Крім того, користувачам, які цінують конфіденційність, буде корисна мінімізація збору даних, а також можливість відключення детального журналювання веб-активності [7].

Підтримка програмного забезпечення і довгострокова життєздатність також є важливими аспектами. Система повинна підтримувати регулярні оновлення, щоб списки блокувань реклами та ключові компоненти програмного забезпечення залишалися актуальними. Використання відкритого коду або розширюваних рішень, таких як Pi-hole або AdGuard Home, забезпечує гнучкість для подальших налаштувань і покращень. Автоматизація оновлень і діагностики системи допоможе знизити потребу у втручанні адміністратора, що дозволить підтримувати її ефективну роботу з мінімальним обслуговуванням.

Забезпечивши дотримання цих технічних та операційних вимог, система блокування реклами на базі Raspberry Pi стане ефективним рішенням для усунення небажаної реклами в усіх підключених до мережі пристроях. Поєднання продуктивності, безпеки та зручного керування гарантує, що така система відповідатиме вимогам сучасних мережевих середовищ.

Загалом, Raspberry Pi 4 Model B – оптимальний варіант для реалізації комп'ютерної системи блокування реклами, який забезпечує стабільну роботу, гнучкість у налаштуваннях і доступність за ціною [8].

Для реалізації системи блокування реклами в локальній мережі на базі Raspberry Pi 4 буде використано набір спеціалізованих інструментів, що забезпечують стабільність, продуктивність та гнучкість конфігурації.

Основні інструменти:

— ОС: Raspberry Pi OS (Debian-based).

— DNS-блокування: Pi-hole.

— Мережеві сервіси: dnsmasq.

— Адміністрування: SSH, Web UI.

— Моніторинг: htop, iftop, vnstat.

— Автоматизація: cron.

— Логування: journald, logrotate.

— Мови для конфігурації: Bash, Python.

Основу програмного забезпечення складатиме операційна система Raspberry Pi OS (Debian-based), оскільки вона оптимізована для роботи на ARM-архітектурі та має необхідні інструменти для налаштування мережевих сервісів.

Для блокування реклами буде використано Pi-hole, який працює як DNS-фільтр, забезпечуючи блокування запитів до відомих рекламних серверів. Його налаштування виконуватиметься через Web UI, а для розширеного адміністрування використовуватиметься доступ через SSH [9].

Конфігурація мережевих сервісів здійснюватиметься за допомогою dnsmasq (локальний DNS-кеш та DHCP-сервер). Для моніторингу продуктивності та навантаження на систему будуть використані htop, iftop та vnstat, які дозволяють аналізувати споживання ресурсів та мережевий трафік у режимі реального часу.

Автоматизація оновлення списків блокування реклами буде виконуватись через cron, що дозволяє періодично оновлювати бази даних рекламних доменів. Додатково для логування та аналізу роботи системи застосовуватиметься journald і logrotate, що дозволить ефективно керувати логами та уникати надмірного навантаження на сховище [10].

Розробка та налагодження скриптів конфігурації здійснюватиметься мовою Bash, а для можливого розширення функціоналу системи може бути використано Python (наприклад, для створення кастомних аналітичних модулів).

РОЗДІЛ 2 ПРОЄКТНА ЧАСТИНА

2.1 Розробка узагальненої структури комп’ютерної системи

2.1.1 Архітектура системи фільтрації DNS-запитів

У сучасних комп’ютерних мережах реклама в інтернеті часто надходить у вигляді окремих DNS-запитів до рекламних серверів. Це дозволяє блокувати її на рівні доменних імен до того, як контент потрапить на пристрій користувача. Такий підхід є ефективним, універсальним та не потребує встановлення додаткових блокувальників на кожному окремому клієнті мережі [11].

Основу архітектури розроблюваної системи становить модель DNS-рекурсора, яка отримує DNS-запити від усіх пристроїв локальної мережі, перевіряє їх за чорними списками і, в разі необхідності, блокує доступ до відповідного ресурсу (рис. 2.1).

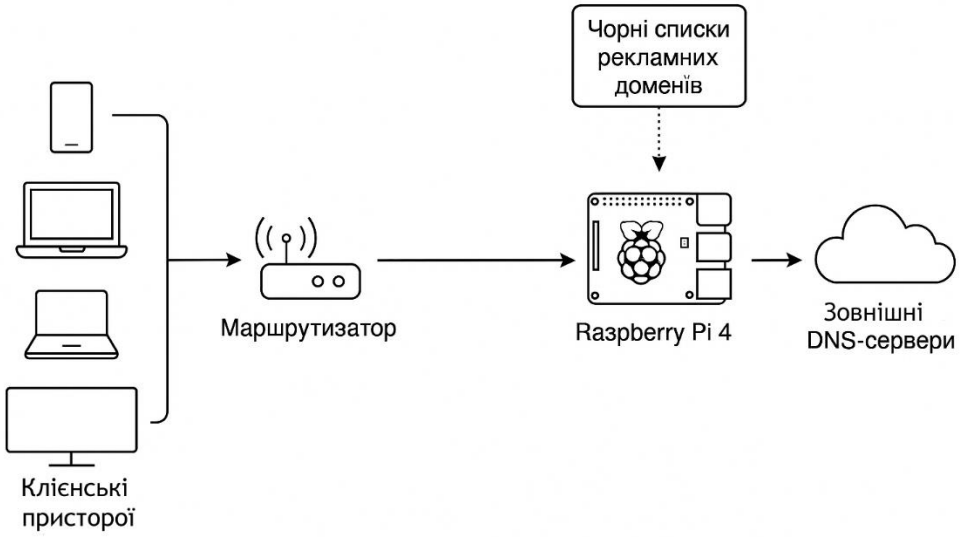


Рисунок 2.1 – Структура DNS-фільтрації в локальній мережі

До складу архітектури входять наступні основні компоненти:

— Клієнтські пристрої (смартфони, ноутбуки, ПК, телевізори) — генерують запити до DNS для отримання IP-адрес сайтів.

— Маршрутизатор — спрямовує DNS-запити користувачів на фільтраційний сервер замість зовнішнього DNS-провайдера.

— Raspberry Pi 4 — виконує роль DNS-фільтра з встановленим програмним забезпеченням Pi-hole, а також інструментами dnsmasq, cron, logrotate для обслуговування системи.

— Чорні списки рекламних доменів — списки доменів, відомих як рекламні, що регулярно оновлюються автоматично.

— Зовнішні DNS-сервери (Upstream DNS) — Google DNS, Cloudflare, OpenDNS або інші, які використовуються лише для «чистих» запитів, що не були заблоковані.

Алгоритм взаємодії системи працює за наступною послідовністю:

— Користувач вводить адресу сайту в браузері.

— Пристрій надсилає DNS-запит до маршрутизатора.

— Запит перенаправляється на Raspberry Pi (Pi-hole).

— Якщо домен присутній у чорному списку — запит блокується.

— Якщо домен дозволений — Pi-hole надсилає запит до зовнішнього DNS-сервера.

— Відповідь кешується локально і повертається клієнту.

Використання такої архітектури має кілька важливих переваг: централізоване блокування без впливу на клієнтські пристрої; мінімальне навантаження на систему завдяки локальному кешуванню; можливість логування та збору статистики DNS-запитів; масштабованість рішення (може бути адаптоване для більшої кількості клієнтів при потребі) [12].

Таким чином, запропонована архітектура відповідає сучасним вимогам до ефективності, безпеки та масштабованості мережевих рішень для блокування реклами.

У даній комп’ютеризованій системі блокування реклами (рис. 2.2) реалізовано взаємодію апаратного та програмного забезпечення на базі мінікомп’ютера Raspberry Pi. Всі пристрої локальної мережі — користувацькі пристрої (смартфони, ноутбуки, ПК) — надсилають DNS-запити через маршрутизатор, який перенаправляє їх на Raspberry Pi, де виконується фільтрація реклами за допомогою Pi-hole.

Рисунок 2.2 – Структура системи в локальній мережі

Raspberry Pi виступає центральним елементом системи. На ньому розміщено не лише програмне забезпечення, але й підключено низку периферійних пристроїв. Для зручності керування та адміністрування використовується монітор, клавіатура та миша, що підключаються до Raspberry Pi через USB-порти. Початкове налаштування Pi-hole та моніторинг роботи системи можуть здійснюватися як локально (через монітор), так і віддалено (через веб-інтерфейс).

Для забезпечення тривалої та стабільної роботи використовується система охолодження, зокрема корпус із вбудованим вентилятором (Raspberry Pi 4 Case with Fan). Охолодження необхідне, оскільки при постійній роботі з мережею пристрій може нагріватися, що негативно впливає на його продуктивність та довговічність.

Таким чином, система, забезпечує централізовану фільтрацію DNS-запитів і блокує рекламу на всіх пристроях у локальній мережі. Вона поєднує простоту, гнучкість і доступність, при цьому забезпечуючи ефективну роботу та комфорт для користувачів [13].

Окрім цього, до Raspberry Pi підключено зовнішній накопичувач, який може використовуватися для зберігання логів, резервних копій або налаштувань системи. Це особливо актуально для адміністраторів, які потребують історії DNS-запитів або хочуть зберігати налаштування на окремому носії.

2.1.2 Взаємодія апаратного та програмного забезпечення

Для забезпечення ефективної роботи системи блокування реклами в локальній мережі критично важливою є тісна інтеграція апаратних компонентів та програмного забезпечення.

Обраний апаратний засіб, Raspberry Pi 4 Model B, характеризується високою продуктивністю завдяки 4-ядерному процесору, достатньому обсягу оперативної пам’яті та гігабітному Ethernet-інтерфейсу, що забезпечує оперативну обробку до 100–150 тисяч DNS-запитів за годину. Ці характеристики роблять його оптимальним для розгортання мережевих сервісів малого та середнього масштабу.

Основний компонент програмного забезпечення — Pi-hole — встановлюється безпосередньо на Raspberry Pi та виконує функції DNS-рекурсора з можливістю фільтрації запитів до рекламних серверів. Ця програма інтегрується з компонентом dnsmasq для кешування та

обслуговування DNS-запитів, що дозволяє знизити затримки і зменшити навантаження на апаратні ресурси (рис. 2.3).

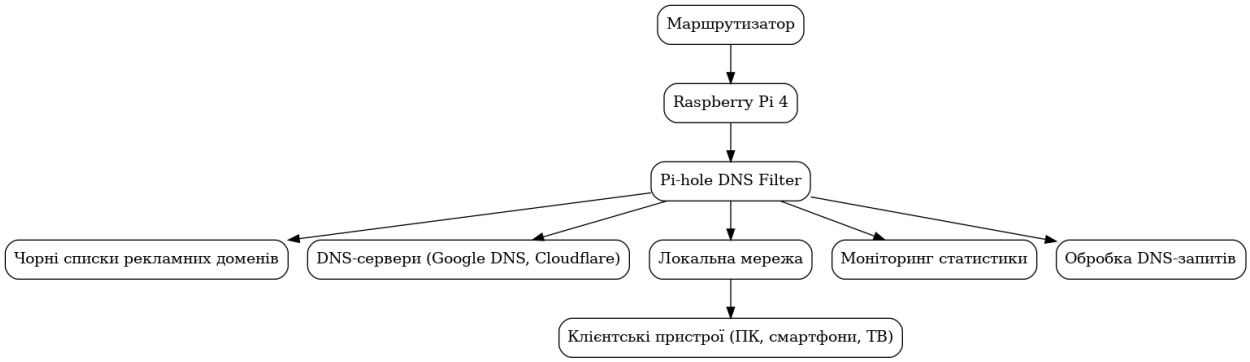


Рисунок 2.3 – Структура роботи Raspberry Pi з Pi-hole DNS Filter

Опис структури:

— Маршрутизатор (Router) - виконує роль розподільника трафіку між усіма пристроями у локальній мережі. Він приймає пакети даних від кожного пристрою в мережі та перенаправляє їх до відповідних адрес, включаючи запити на DNS (Domain Name System).

— Raspberry Pi 4 — це одноплатний комп'ютер, який виступає в ролі сервера для виконання всіх основних функцій фільтрації DNS-запитів. Він взаємодіє з Pi-hole, яке займається безпосередньо фільтрацією реклами.

— Pi-hole DNS Filter — це програмне забезпечення для блокування реклами, яке працює як DNS-рекурсор. Pi-hole перехоплює DNS-запити, перевіряє їх за чорним списком доменів (які відомі як рекламні) і блокує доступ до них. У разі, якщо запит не належить до реклами, він перенаправляється на зовнішні DNS-сервери.

— Чорні списки рекламних доменів - це списки доменів, які відомі як джерела реклами. Pi-hole використовує ці списки для порівняння з DNS-запитами. Якщо запит на домен із чорного списку надходить, він блокується, і реклама не потрапляє на клієнтський пристрій.

— DNS-сервери (Google DNS, Cloudflare) - це зовнішні DNS-сервери,

до яких Pi-hole пересилає запити, якщо домен не знайдено у чорних списках. Вони виконують роль надійних серверів для обробки DNS-запитів, що не заблоковані.

— Локальна мережа (LAN) — це мережева інфраструктура, яка об’єднує всі пристрої в межах одного фізичного простору. У цьому контексті вона забезпечує з’єднання між Raspberry Pi, клієнтськими пристроями та маршрутизатором.

— Клієнтські пристрої (ПК, смартфони, ТВ) - це всі пристрої, що підключаються до локальної мережі і використовують її для доступу до Інтернету. Всі DNS-запити цих пристроїв обробляються через Pi-hole.

— Моніторинг статистики - це функція Pi-hole, яка дозволяє адміністраторам системи відстежувати статистику DNS-запитів. Веб-інтерфейс надає детальні звіти про заблоковані домени, кількість запитів і статистику за часом.

— Обробка DNS-запитів- це процес, під час якого Pi-hole перевіряє кожен DNS-запит на наявність рекламного домену. Якщо домен заблокований, Pi-hole не передає запит на зовнішній DNS-сервер і просто блокує його.

Інтеграція системи блокування реклами на базі Raspberry Pi 4 та Pi-hole у локальну мережу є важливим етапом для налаштування ефективної роботи всієї мережі. Вся локальна мережа, включаючи всі пристрої, підключені до маршрутизатора, буде використовувати Pi-hole для фільтрації DNS-запитів. Ось детальний опис схеми інтеграції:

Ключові компоненти інтеграції:

— Маршрутизатор - Маршрутизатор керує мережею та направляє DNS-запити від усіх пристроїв локальної мережі на Raspberry Pi. Він також відповідає за налаштування загального доступу до Інтернету для всіх підключених пристроїв.

— Raspberry Pi 4 (сервер Pi-hole) - Raspberry Pi 4 виконує роль серверного пристрою для обробки DNS-запитів від всіх клієнтських пристроїв

у мережі. Вся фільтрація реклами здійснюється через Pi-hole, яке блокує запити до рекламних доменів і пересилає інші запити на зовнішні DNS-сервери.

— Pi-hole DNS Filter - Pi-hole служить для обробки DNS-запитів, їх фільтрації та передачі на зовнішні DNS-сервери (Google DNS, Cloudflare, тощо), якщо домен не заблоковано.

— Клієнтські пристрої - Це всі пристрої, які підключаються до локальної мережі, наприклад, комп’ютери, смартфони, телевізори. Вони генерують DNS-запити, які потім фільтруються через Pi-hole.

— DNS-сервери (Google DNS, Cloudflare) - В разі необхідності, Pi-hole передає дозволені DNS-запити на зовнішні DNS-сервери для обробки.

2.2 Обґрунтування вибору апаратного забезпечення проектованого комп’ютерного засобу

Вибір апаратної платформи для системи блокування реклами, яка базується на Raspberry Pi 4 (рис.2.4)., був обґрунтований її характеристиками, які відповідають вимогам проекту.

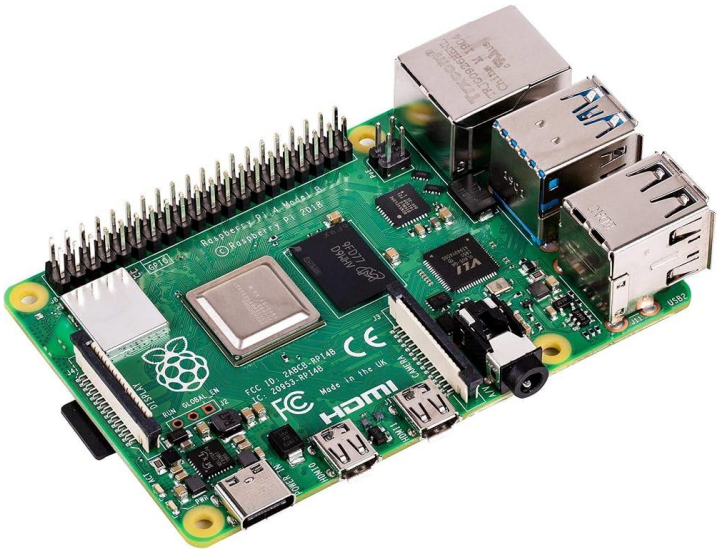


Рисунок 2.4 – Зовнішній вигляд Raspberry Pi 4

Raspberry Pi 4 була обрана завдяки своїм технічним характеристикам, доступності, простоті налаштування та підтримці широкого спектра програмного забезпечення, зокрема таких рішень, як Pi-hole для фільтрації реклами

2.2.1 Характеристика платформи Raspberry Pi 4

Raspberry Pi 4 Model B — це одноплатний комп’ютер, який поєднує високу продуктивність з доступною ціною, що робить його ідеальним вибором для проектів, таких як блокування реклами в локальних мережах (табл 2.1).

Потужність процесора Broadcom BCM2711 з 4 ядрами Cortex-A72 на частоті 1.5 GHz забезпечує достатньо високу продуктивність для обробки DNS-запитів, що дозволяє ефективно блокувати рекламу в реальному часі, навіть за умов високого навантаження. Ця потужність ідеально підходить для виконання задач блокування реклами на рівні DNS, де важлива швидкість обробки запитів і ефективне управління великою кількістю даних [14].

Оперативна пам'ять Raspberry Pi 4 доступна з різними обсягами пам'яті (2, 4 або 8 ГБ), ми вибрали модель з 4 ГБ LPDDR4 пам'яті. Цього обсягу достатньо для одночасної обробки великої кількості DNS-запитів і запуску декількох сервісів на одному пристрої без затримок. Цей обсяг пам'яті також дає можливість працювати з більш складними мережевими налаштуваннями та системами моніторингу.

Швидкісне підключення до мережі - 1 гігабітний Ethernet порт забезпечує стабільну та швидку передачу даних, що є критично важливим для високопродуктивної обробки DNS-запитів, особливо в умовах великого трафіку. Також наявність Wi-Fi дозволяє використовувати Raspberry Pi 4 в бездротових мережах без необхідності прокладати додаткові кабелі, що робить установку системи більш зручною [15].

2 порти USB 3.0 дозволяють підключати додаткові пристрої, такі як зовнішні жорсткі диски для зберігання логів або медіа-даних, що може бути

корисним для системи моніторингу чи зберігання великих обсягів інформації. Порти USB 2.0 можна використовувати для периферійних пристроїв або зовнішніх адаптерів, що додає гнучкості в налаштуваннях (табл. 2.1).

Таблиця 2.1 - Основні характеристики Raspberry Pi 4

Параметр	Характеристика
Процесор	Broadcom BCM2711, 4-ядерний Cortex-A72, 1.5 GHz
Оперативна пам'ять	2, 4 або 8 ГБ LPDDR4-3200
Графіка	Broadcom VideoCore VI, OpenGL ES 3.0
Мережа	1 гігабітний Ethernet порт
Wi-Fi	802.11ac Wi-Fi, 2.4 GHz & 5 GHz
Bluetooth	Bluetooth 5.0
Порти USB	2 порти USB 3.0, 2 порти USB 2.0
Порти HDMI	2 порти micro-HDMI (до 4K @ 60 Hz)
Пам'ять для зберігання	microSD слот для карти пам'яті, підтримка USB 3.0 для зовнішніх накопичувачів
Живлення	5V / 3A через USB-C, споживання до 15 Вт
Розміри	88 x 58 x 19.5 мм
Ціна	Близько $35 (залежно від моделі)

Енергоефективність мінімальна (до 15 Вт), що робить її ідеальним варіантом для тривалої роботи без нагріву або значного споживання електроенергії. Це особливо важливо для домашніх або малих бізнес-мереж, де важливий довготривалий безперервний час роботи та низька вартість експлуатації.

Підтримка програмного забезпечення Raspberry Pi OS, що дозволяє легко налаштувати систему для роботи з Pi-hole. Встановлення та налаштування Pi-hole на Raspberry Pi проходить без проблем, а також можна використовувати додаткові утиліти для моніторингу, оновлення та налаштування системи [16].

Raspberry Pi 4 є дуже компактним пристроєм з розмірами всього 88 x 58 x 19.5 мм, що дозволяє розмістити його в будь-якому місці без зайвого використання простору. Завдяки невеликій вартості (близько $35) він є

доступним варіантом для малих бізнесів та домашніх користувачів, що робить його ідеальним вибором для подібних проєктів.

Raspberry Pi 4 підтримує додаткові функції, такі як Bluetooth 5.0, що дозволяє підключати бездротові пристрої для управління мережею чи збору даних. Ця функція може бути корисною для проєктів, де потрібна додаткова бездротова комунікація або інтеграція з іншими пристроями.

2.2.2 Додаткові утиліти: dnsmasq, logrotate, cron

Для підтримки ефективної та стабільної роботи системи блокування реклами на базі Pi-hole, у складі програмного середовища використовуються додаткові утиліти, які виконують допоміжні функції. До таких утиліт належать: dnsmasq, logrotate та cron.

dnsmasq — це легкий DNS-forwarder і DHCP-сервер, який використовується всередині Pi-hole для обробки та кешування DNS-запитів. Його основною функцією є локальне кешування результатів DNS-розв’язування, що значно зменшує кількість повторних звернень до зовнішніх DNS-серверів і, відповідно, підвищує швидкість обробки запитів.

Основні функції dnsmasq у системі:

— Кешування DNS-відповідей для пришвидшення повторних запитів;

— Розпізнавання локальних імен у мережі;

— Обробка DNS-запитів, що не були заблоковані через фільтри Pi-hole;

— Зменшення навантаження на зовнішні DNS-сервери.

Використання dnsmasq дозволяє системі реагувати на повторні запити за кілька мілісекунд, що критично важливо для збереження відчутної швидкодії під час веб-серфінгу.

logrotate — це утиліта для автоматичного управління журналами системи. Оскільки Pi-hole та Raspberry Pi OS зберігають велику кількість логів

DNS-запитів, системних повідомлень та оновлень, необхідно регулярно їх обробляти, щоб уникнути переповнення сховища та уповільнення системи.

Основні функції logrotate:

— Ротація лог-файлів (створення нових при досягненні певного розміру);

— Стискання старих логів для економії місця;

— Видалення застарілих журналів відповідно до політики зберігання;

— Автоматизація через cron (щоденне/тижневе виконання).

Конфігураційний файл logrotate дозволяє налаштувати частоту очищення логів Pi-hole, наприклад, раз на тиждень, залишаючи останні 4–6 копій логів у стислому вигляді.

cron — це системний планувальник завдань, який дозволяє автоматично запускати необхідні скрипти або утиліти у визначений час.

У системі блокування реклами cron виконує такі завдання:

— Автоматичне оновлення чорних списків доменів через команди

— Очищення та оновлення логів у зв’язці з logrotate;

— Резервне копіювання конфігураційних файлів, якщо налаштовано відповідні скрипти.

Періодичність виконання завдань (наприклад, щодня о 3:00 ночі) задається через файл crontab, що дозволяє системі залишатися актуальною без участі користувача.

Інтеграція dnsmasq, logrotate та cron у програмну архітектуру проєкту забезпечує пришвидшення відповіді системи на запити (dnsmasq), економне використання дискового простору (logrotate) та повну автоматизацію оновлення та обслуговування (cron).

Ці утиліти значно підвищують стабільність, автономність та масштабованість системи блокування реклами.

2.3 Проєктування комп’ютнрного засобу

2.3.1 Схеми алгоритму фільтрації DNS-запитів

На рисунку 2.10 представлена блок-схема алгоритму фільтрації DNS-запитів у комп’ютеризованій системі блокування реклами, реалізованій на базі Raspberry Pi 4 з використанням програмного забезпечення Pi-hole. Дана схема відображає покрокову логіку функціонування системи — від моменту генерації запиту клієнтом до отримання відповіді та можливого блокування.

Процес розпочинається з того, що користувач на клієнтському пристрої (ПК, смартфон, планшет тощо) вводить адресу вебсайту в браузері. Це спричиняє автоматичне формування DNS-запиту, який надходить на маршрутизатор локальної мережі. У конфігурації маршрутизатора передбачено, що всі DNS-запити мають перенаправлятися на Raspberry Pi, де функціонує Pi-hole [17].

Після отримання запиту, Pi-hole виконує перевірку наявності відповідного запису у локальному кеші, що обслуговується утилітою dnsmasq. Якщо відповідь уже є в кеші — вона негайно повертається клієнту, що дозволяє значно зменшити час відгуку системи.

Якщо ж відповідного запису в кеші немає, Pi-hole перевіряє домен за чорним списком рекламних ресурсів. Якщо домен знайдено у списку, система блокує запит, повертаючи "пусту" відповідь (наприклад, 0.0.0.0), що не дозволяє завантажити рекламний вміст на стороні клієнта (рис. 2.10).

У випадку, якщо домен не міститься у списку блокування, Pi-hole пересилає запит до одного з зовнішніх DNS-серверів (наприклад, Google DNS або Cloudflare), отримує відповідь та повертає її клієнту. Отримана IP-адреса також зберігається у кеші для пришвидшення наступних звернень.

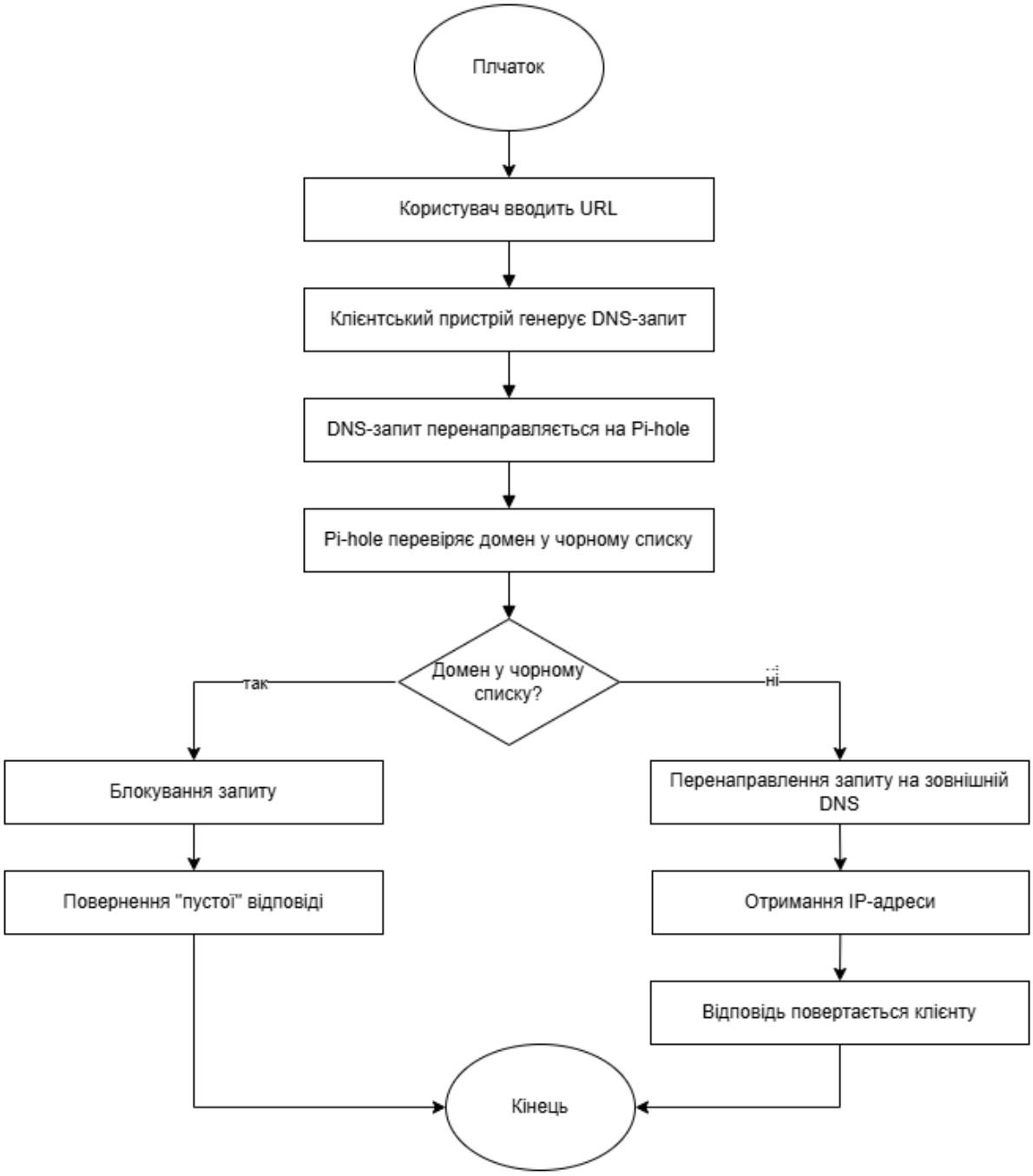


Рисунок 2.10 – Блок-схеми алгоритму фільтрації DNS-запитів

Усі події — як блокування, так і дозволені відповіді — записуються у системні лог-файли за допомогою утиліти logrotate. Окрім того, статистика DNS-запитів та динаміка роботи системи виводиться у веб-інтерфейсі Pi-hole (Web UI), що забезпечує адміністратору зручний візуальний контроль над системою.

Таким чином, дана схема демонструє повноцінну автоматизовану модель обробки DNS-запитів із вбудованим механізмом фільтрації реклами, кешуванням відповідей, логуванням активності та моніторингом у реальному часі. Це дозволяє реалізувати централізований захист локальної мережі від рекламного контенту без необхідності інсталяції додаткового програмного забезпечення на клієнтські пристрої.

2.3.2 Схема автоматичного оновлення чорних списків у Pi-hole

На рисунку 2.11 представлено блок-схему автоматичного оновлення чорних списків у системі блокування реклами, що реалізована за допомогою Pi-hole на платформі Raspberry Pi. Схема ілюструє, як програмна утиліта cron автоматично запускає процес оновлення фільтрів без втручання користувача. У визначений час (наприклад, щоденно о 03:00) cron активує команду pihole -g, яка ініціює завантаження актуальних списків рекламних доменів з віддалених серверів [18].

Після встановлення з’єднання Pi-hole намагається отримати свіжі версії чорних списків. Якщо завантаження проходить успішно, система переходить до оновлення локальної бази фільтрів, яка надалі використовується для блокування реклами. Завершення процесу фіксується у лог-файлі зі статусом «Оновлення успішне». Це дозволяє адміністратору в будь-який момент перевірити історію оновлень і переконатися в справності механізму.

У випадку, якщо виникає помилка (наприклад, немає інтернет-з'єднання, недоступний сервер або пошкоджені файли списків), процес оновлення переривається. В лог-файл заноситься повідомлення про невдалу спробу з позначкою «Помилка оновлення». За необхідності, система може бути налаштована для автоматичного надсилання повідомлення адміністратору, що підвищує надійність та контроль роботи фільтраційного механізму. Такий підхід забезпечує самооновлення системи без ручного втручання та дозволяє підтримувати захист мережі на актуальному рівні

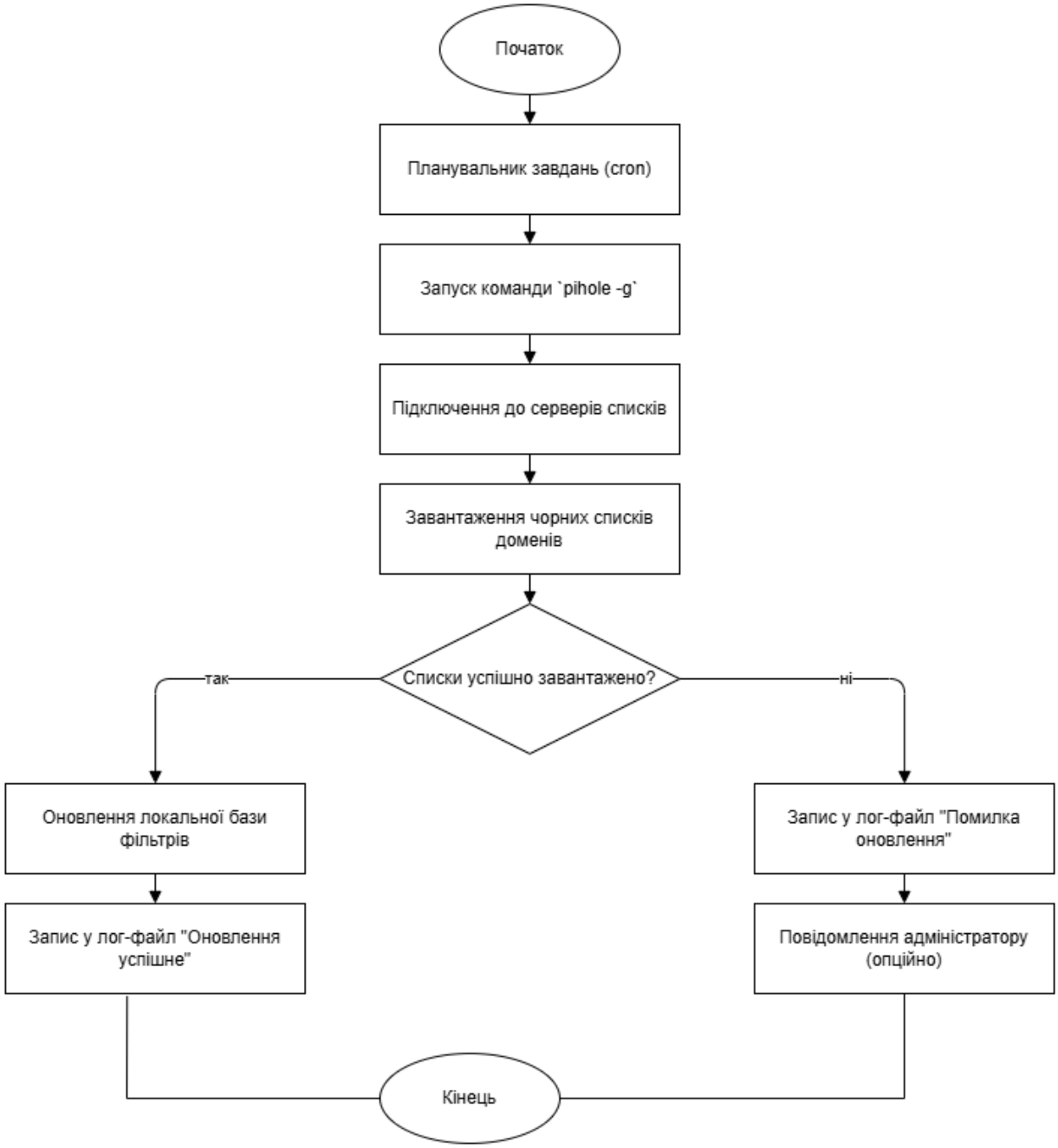


Рисунок 2.11 – Блок-схема автоматичного оновлення чорних списків

2.3.3 Схема взаємодії компонентів системи DNS-фільтрації

На рисунку 2.12 представлена розширена логічна схема взаємодії пристроїв та програмних компонентів у системі DNS-фільтрації на базі Pi-hole, встановленого на Raspberry Pi 4. Користувацькі пристрої (наприклад, ПК або смартфони) надсилають DNS-запити до маршрутизатора, який перенаправляє їх на Raspberry Pi. Тут працює Pi-hole, що перевіряє кожен запит на наявність у чорних списках доменів. Якщо домен не міститься у списку, запит

пересилається до зовнішнього DNS-сервера (наприклад, Google DNS), а отримана IP-адреса передається назад клієнту.

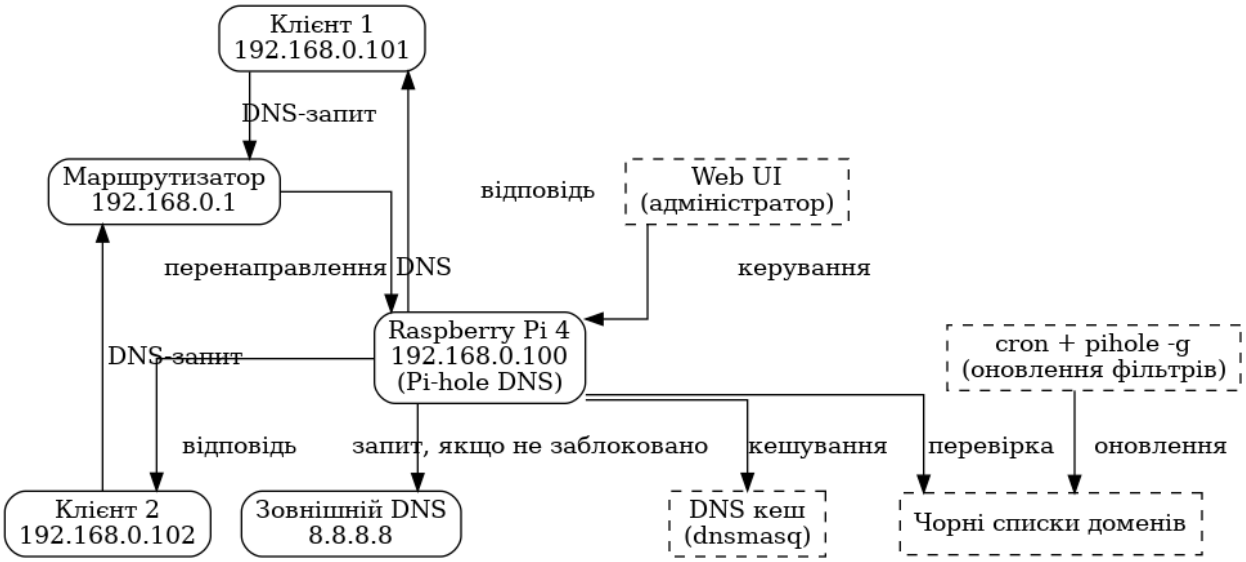


Рисунок 2.12 – Логічна структурна схеми адресації пристроїв

У схемі також відображено допоміжні компоненти: локальний кеш dnsmasq, що прискорює обробку повторних запитів; веб-інтерфейс (Web UI), через який адміністратор може переглядати статистику та керувати системою; а також служба cron, яка автоматично виконує команду pihole -g для оновлення чорних списків доменів. Така структура забезпечує автоматичність, швидкодію та централізоване блокування реклами у локальній мережі.

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

3.1 Реалізація програмної частини

3.1.1 Підготовка Raspberry Pi для роботи в мережі

На першому етапі реалізації системи блокування реклами було виконано підготовку мінікомп’ютера Raspberry Pi 4 Model B до стабільної роботи в локальній мережі. Пристрій виступає як DNS-фільтр для всієї мережі, тому необхідно забезпечити його надійне з’єднання, правильну конфігурацію системи та мінімальне навантаження [19].

Операційна система для пристрою — Raspberry Pi OS Lite (без GUI) — була записана на microSD-карту ємністю 32 ГБ за допомогою офіційної утиліти Raspberry Pi Imager. Цей дистрибутив є оптимальним для серверних задач, оскільки має мінімальне споживання ресурсів і дозволяє повністю працювати з консолі.

Послідовність підготовки:

– Завантаження Raspberry Pi OS Lite з офіційного сайту.

– Запис образу на microSD за допомогою Raspberry Pi Imager або Balena Etcher.

– Створення файлу ssh у корені SD-карти для активації SSH-доступу.

– За потреби — попереднє налаштування Wi-Fi (файл wpa_supplicant.conf).

Після початкового запуску Raspberry Pi було підключено до мережі через Ethernet-кабель для забезпечення максимальної стабільності. Через SSH здійснюється доступ до пристрою з іншого комп’ютера в мережі. Після здійснення підключення, з’являється командний рядок пристрою

antonM@raspberrypi, що означає успішне встановлення з'єднання з Raspberry Pi по SSH (рис.3.1).

Запит

```
ssh antonM@192.168.0.100
```

Відповідь

```
The authenticity of host '192.168.0.100 (192.168.0.100)' can't be
established.

ECDSA key fingerprint is SHA256:AbC1...xyz.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.0.100' (ECDSA) to the list of known
hosts.

antonM@raspberrypi:~ $
```

Рисунок 3.1 – Підключення до мережі

Для безперебійної роботи DNS-фільтра необхідно, щоб Raspberry Pi завжди мав одну й ту саму IP-адресу в мережі. Було прописано статичну IP через файл (рис.3.2).

Запит

```
sudo nano /etc/dhcpcd.conf
```

Вікно редагування

```
interface eth0

static ip_address=192.168.0.100/24

static routers=192.168.0.1

static domain_name_servers=192.168.0.1
```

Рисунок 3.2 – Статична IP-адреса

Пристрій розміщено у пластиковому корпусі з активним вентилятором, що забезпечує ефективне охолодження. Температура процесора в режимі очікування не перевищує 50°C.

3.1.2 Встановлення Pi-hole на Raspberry Pi

Після завершення мережевої підготовки пристрою Raspberry Pi було здійснено встановлення програмного забезпечення Pi-hole — системи фільтрації DNS-запитів із можливістю блокування реклами, трекерів, аналітики тощо. Інсталяція проводиться через офіційний скрипт розробників Pi-hole у середовищі командного рядка [20].

Перед встановленням Pi-hole виконується оновлення системи та встановлення оновлень безпеки (рис.3.3).

Запит

```
sudo apt update && sudo apt upgrade -y
```

Вікно редагування

```
Hit:1 http://raspbian.raspberrypi.org/raspbian bullseye InRelease
Reading package lists... Done
Building dependency tree... Done
...
The following packages will be upgraded:
  bash libc-bin libc6 libgcc-s1 ...
...
After this operation, 35.6 MB of additional disk space will be used.
```

Рисунок 3.3 – Оновлення системи

Офіційний скрипт Pi-hole автоматизує встановлення, конфігурацію основних компонентів та запуск DNS-сервісу

3.1.3 Налаштування мережевої маршрутизації для перенаправлення DNS

Для того щоб система блокування реклами працювала не лише на одному пристрої, а на всій локальній мережі, потрібно зробити так, щоб усі DNS-запити від клієнтів автоматично проходили через Pi-hole, встановлений на Raspberry Pi. Для цього достатньо змінити налаштування DNS у конфігурації маршрутизатора.

Передусім потрібно закріпити за Raspberry Pi постійну IP-адресу (в нашому випадку 192.168.0.100). Це дозволить іншим пристроям знати, куди саме надсилати DNS-запити. Далі у веб-інтерфейсі маршрутизатора (зазвичай доступний за адресою http://192.168.0.1) у розділі DHCP потрібно встановити адресу Raspberry Pi як основний DNS-сервер. Таким чином, усі пристрої в мережі автоматично отримають цю адресу при підключенні.

Після цього можна перевірити, чи працює перенаправлення. На клієнтському пристрої відкривають термінал і вводять команду nslookup google.com. Якщо у відповіді зазначено, що сервер — це Raspberry Pi (192.168.0.100), значить усе налаштовано правильно.

Для підвищення безпеки і запобігання спробам обійти блокування, можна заборонити звернення до інших DNS-серверів у налаштуваннях маршрутизатора або через брандмауер. Деякі маршрутизатори також підтримують функцію «DNS-примусового перенаправлення».

Після завершення налаштувань маршрутизатора система починає працювати автоматично: усі DNS-запити від клієнтів надсилаються на Raspberry Pi, де відбувається перевірка — якщо запит до домену рекламного типу, він блокується; в іншому випадку запит пересилається до зовнішнього DNS-сервера.

3.1.4 Робота з чорними списками доменів

Для ефективного блокування реклами та шкідливих трекерів у системі Pi-hole використовуються так звані чорні списки доменів. Це текстові файли, що містять тисячі інтернет-доменів, які асоціюються з рекламними мережами, аналітичними платформами та відстеженням дій користувача. Коли клієнтський пристрій намагається отримати доступ до одного з цих доменів, Pi-hole автоматично блокує такий запит, повертаючи "пусту" відповідь. Детальний алгоритм роботи можна побачити на рисунку 3.4

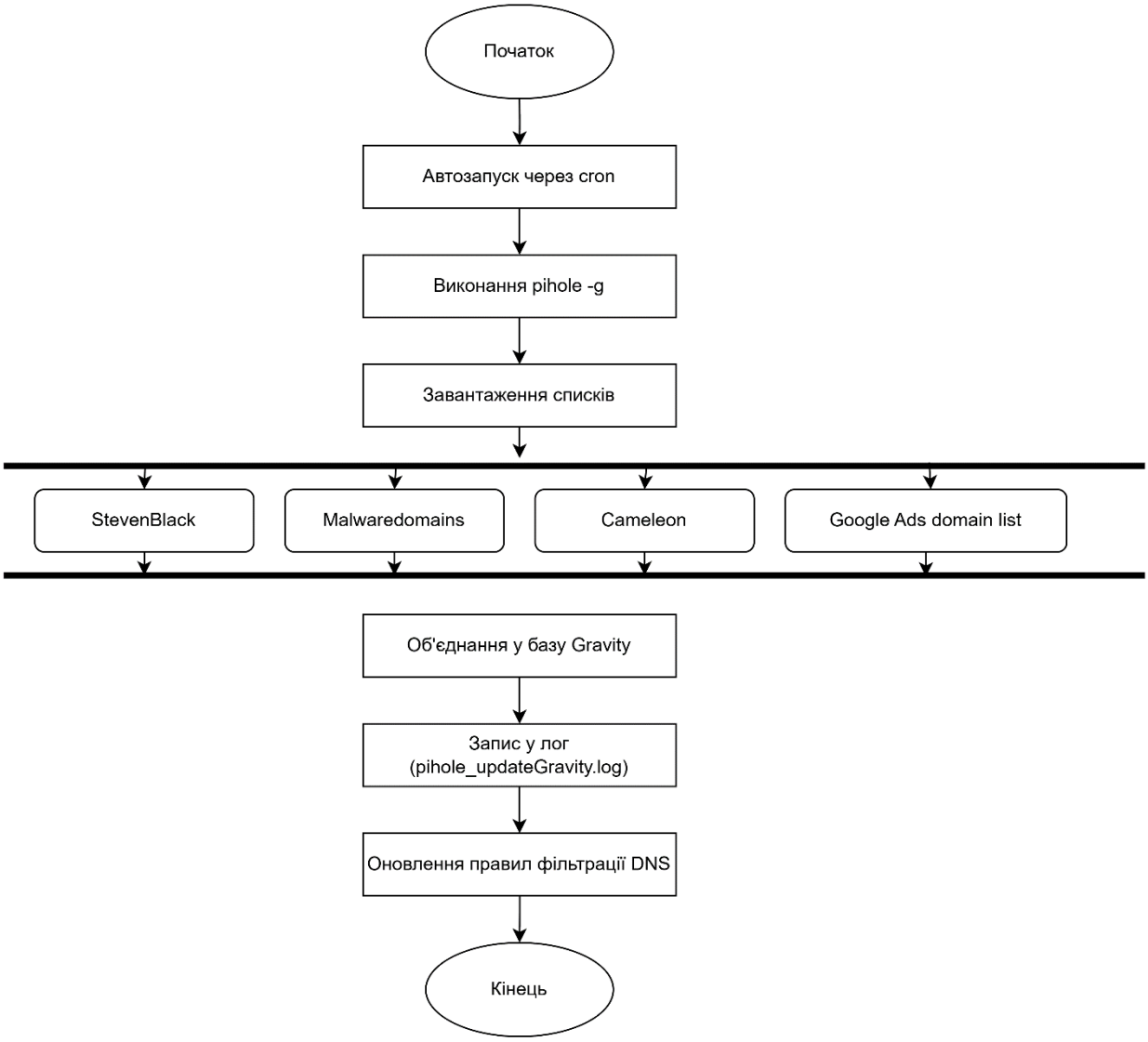


Рисунок 3.4 – Алгоритм оновлення чорних списків у Pi-hole

Під час встановлення Pi-hole автоматично додає базовий чорний список (наприклад, список від StevenBlack, який поєднує кілька популярних джерел). Однак користувач може розширювати цей список, додаючи нові джерела або власноруч блокуючи окремі домени. Для цього у веб-інтерфейсі передбачено розділ Group Management → Adlists, де можна додавати URL-адреси до зовнішніх чорних списків.

Ми використали такі додаткові списки:

– https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
– https://mirror1.malwaredomains.com/files/justdomains
– https://sysctl.org/cameleon/hosts

Ця команда ініціює завантаження вмісту списків, оновлює локальну базу доменів та виводить статистику по кожному з джерел: кількість нових, пропущених чи повторних записів. Усі ці дії також логуються у файл /var/log/pihole_updateGravity.log.

Крім чорних списків, Pi-hole дозволяє керувати білим списком (whitelist) — це перелік дозволених доменів, які не блокуватимуться навіть якщо вони є в чорному списку. Це зручно, коли певний сайт частково працює через рекламну мережу, і його потрібно дозволити вручну, командою «pihole -g».

Таким чином, гнучка система списків у Pi-hole дозволяє налаштувати фільтрацію відповідно до конкретних потреб мережі — заблокувати максимум зайвого трафіку, але водночас уникати надмірного обмеження доступу до необхідних ресурсів.

3.1.5 Налаштування автоматичного оновлення фільтрів

Для підтримання актуальності списків заблокованих доменів у системі Pi-hole необхідно регулярно оновлювати базу фільтрів. Це дозволяє автоматично враховувати нові рекламні та трекерні домени, які з'являються в мережі. Найпростіший і надійний спосіб реалізації цього — використання системного планувальника завдань cron.

Команда для оновлення фільтрів у Pi-hole виглядає наступним чином: `pihole -g`

Вона завантажує всі підключені чорні списки (adlists) з мережі та оновлює локальну базу Gravity, яка використовується для фільтрації DNS-запитів.

Щоб цей процес виконувався автоматично, було створено запис у планувальнику завдань cron. Для редагування списку запланованих завдань використовується команда: `crontab -e`

У відкритому файлі додається такий рядок: `0 3 * * * /usr/local/bin/pihole -g > /dev/null` (рис.3.5.)

```
antonM@raspberrypi:~ $ crontab -e

# ┌──────────── хвилина (0 - 59)
# │ ┌──────────── година (0 - 23)
# │ │ ┌──────────── день місяця (1 - 31)
# │ │ │ ┌──────────── місяць (1 - 12)
# │ │ │ │ ┌──────────── день тижня (0 - 6) (неділя = 0)
# │ │ │ │ │
0 3 * * * /usr/local/bin/pihole -g > /dev/null 2>&1

# Щоденне оновлення списків фільтрації о 03:00
```

Рисунок 3.5 – Cron-завдання для автооновлення фільтрів у Pi-hole

Цей запис означає, що команда оновлення буде виконуватись щодня о 03:00 ночі. Додавання > /dev/null відсікає стандартний вивід, щоб не перевантажувати лог-файли.

Процес оновлення реєструється у журналі зберігається в окремому файлі: `/var/log/pihole_updateGravity.log`

У цьому файлі зберігається інформація про завантаження кожного списку: кількість нових доменів, дублікати, помилки підключення. Це дозволяє перевірити, чи оновлення пройшло успішно.

У нашій системі додатково використовувались не лише стандартні списки Pi-hole, а й список доменів рекламних сервісів Google, який було вручну імпортовано в систему. Завдяки регулярному оновленню, навіть нові рекламні мережі, які з’являються щодня, блокуються автоматично.

Таким чином, автоматичне оновлення чорних списків забезпечує автономність системи, зниження навантаження на адміністратора та високу ефективність фільтрації у режимі 24/7.

3.1.6 Візуалізація статистики через Web UI Pi-hole

Одна з ключових переваг системи Pi-hole — це зручний веб-інтерфейс, який дозволяє адміністратору в реальному часі переглядати статистику DNS-

запитів, рівень блокування, найактивніших клієнтів, а також детально аналізувати трафік у мережі.

Для доступу до інтерфейсу використовується веб-браузер. Стандартна адреса доступу: http://192.168.0.100/admin.

Після встановлення Pi-hole автоматично створює адміністративну панель, вхід до якої захищений паролем (його було виведено у терміналі під час встановлення і зберігається у системі).

На головній сторінці панелі відображається:

– Кількість DNS-запитів за добу
– Кількість заблокованих доменів
– Відсоток заблокованих запитів
– Статистика по клієнтах та доменах
– Графік активності запитів у часі

На рисунку 3.6 показано приклад типового вигляду головної сторінки веб-інтерфейсу.

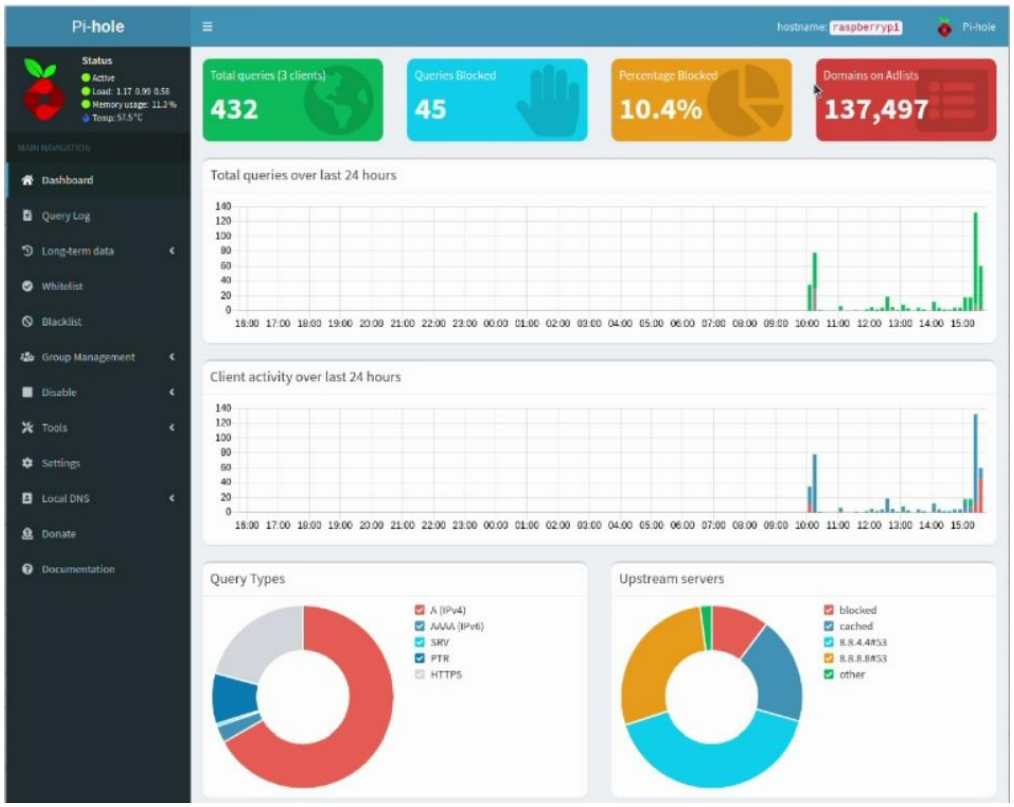


Рисунок 3.6 – Головна панель адміністратора Pi-hole з веб-інтерфейсу

Інтерфейс також дозволяє:

– додавати та видаляти чорні/білі списки доменів;

– контролювати, які пристрої генерують найбільше запитів;

– миттєво увімкнути або вимкнути блокування;

– переглядати логи (вбудовано в систему або через окремий переглядач запитів).

Це значно полегшує моніторинг та управління мережею, особливо коли одночасно працюють багато клієнтських пристроїв.

Важливо також зазначити, що веб-інтерфейс адаптований під мобільні пристрої та планшети, що робить доступ до нього зручним незалежно від того, де знаходиться адміністратор.

3.2 Тестування роботи системи

3.2.1 Перевірка блокування реклами в браузерах

Після завершення встановлення та налаштування системи Pi-hole була проведена практична перевірка її ефективності у реальному середовищі. Метою тестування було оцінити, як саме працює фільтрація DNS-запитів під час відвідування популярних веб-ресурсів, що активно використовують рекламні мережі.

Для перевірки були використані стандартні браузери: Google Chrome та Mozilla Firefox на двох типах пристроїв — настільному ПК і смартфоні, підключених до локальної мережі через маршрутизатор. Усі DNS-запити оброблялися виключно через Raspberry Pi з Pi-hole, що дозволяло оцінити ефективність фільтрації без участі сторонніх розширень.

Основні тести проводилися на таких платформах:

– YouTube (вбудована реклама перед відео, банери)

– Новинні сайти: tsn.ua, obozrevatel.com, espreso.tv (банери, контекстна реклама)

– Портали з високим рівнем трекінгу: 24tv.ua, nv.ua, unian.ua

Після завантаження сторінок було візуально зафіксовано відсутність рекламних блоків, які зазвичай з’являються у верхній або бічній частині сайту. Наприклад, на порталі tsn.ua повністю зник банер у верхній частині, а на obozrevatel.com не відображалася реклама в тексті новини.

На YouTube було частково заблоковано вбудовану рекламу. Перед основним відео іноді спрацьовувала "затримка", однак рекламний контент не програвався. Це пов'язано з тим, що деяка реклама в YouTube інтегрована безпосередньо у відео, і не може бути заблокована через DNS (табл.3.1).

Додатково ми перевіряли користування цими сервісами протягом 30 хвилин та отримали хороші результати блокування (таб 3.1)

Таблиця 3.1 – Результат блокування протягом 30 хвилин

Сайт	Тип реклами	Кількість DNS-запитів	Заблоковано доменів
YouTube	Відео перед роликами	18	14
tsn.ua	Банери та сторонні трекери	42	35
obozrevatel.com	Реклама в текстах і банери	39	31
espreso.tv	Рекламні блоки на боковій панелі	27	23
24tv.ua	Скрипти аналітики та динамічна реклама	34	29

У веб-інтерфейсі Pi-hole в розділі Query Log під час тестів спостерігались численні заблоковані запити до доменів:

– ads.youtube.com
– doubleclick.net
– googlesyndication.com
– tsnads.interia.pl
– track.obozrevatel.com

Це підтверджує, що система ефективно відфільтровує рекламу ще на рівні DNS-запиту — до того, як вона доходить до браузера.

Система блокування реклами на базі Pi-hole показала високу ефективність на новинних порталах, а також часткову ефективність на YouTube. Вбудована фільтрація DNS забезпечує чисте відображення сторінок

без банерів, що зменшує навантаження на трафік і покращує користувацький досвід.

3.2.2 Аналіз динаміки DNS-запитів у Web UI

Після активації системи фільтрації Pi-hole у локальній мережі було здійснено аналіз динаміки DNS-запитів, що надходять від клієнтських пристроїв. Основним інструментом моніторингу виступає веб-інтерфейс Pi-hole, який візуалізує у реальному часі всі запити та дозволяє побачити активність кожного пристрою окремо. На головній сторінці веб-інтерфейсу доступна лінійна діаграма, що відображає кількість DNS-запитів у певному часовому проміжку. Графік автоматично оновлюється та показує кількість запитів на хвилину. Це дозволяє швидко виявити піки активності, наприклад, при завантаженні стрічки новин або запуску YouTube на кількох пристроях одночасно (рис 3.7).

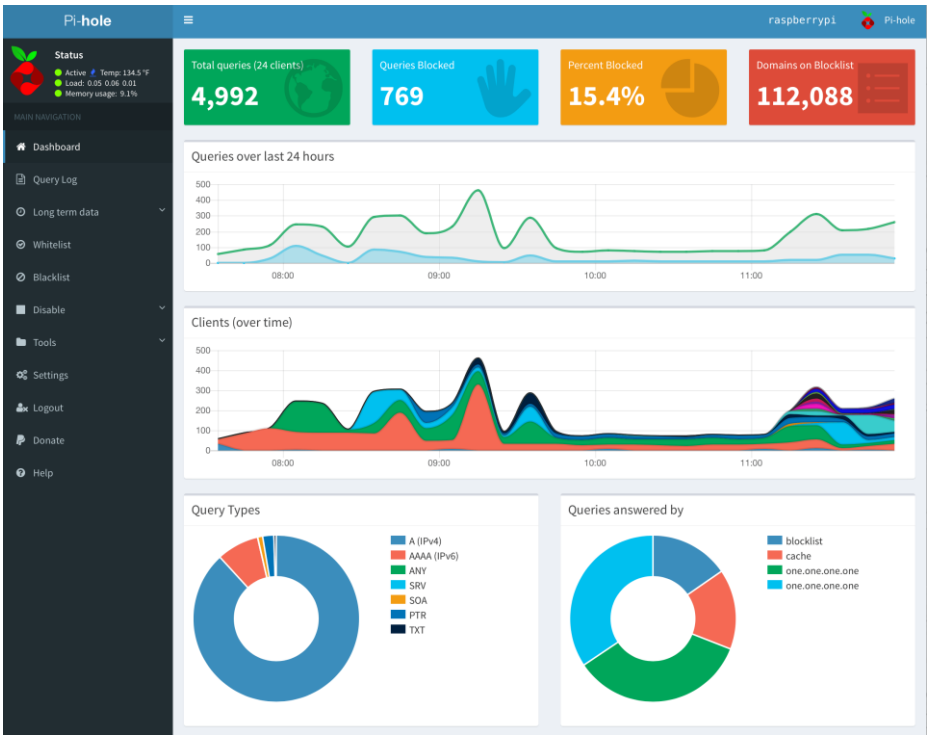
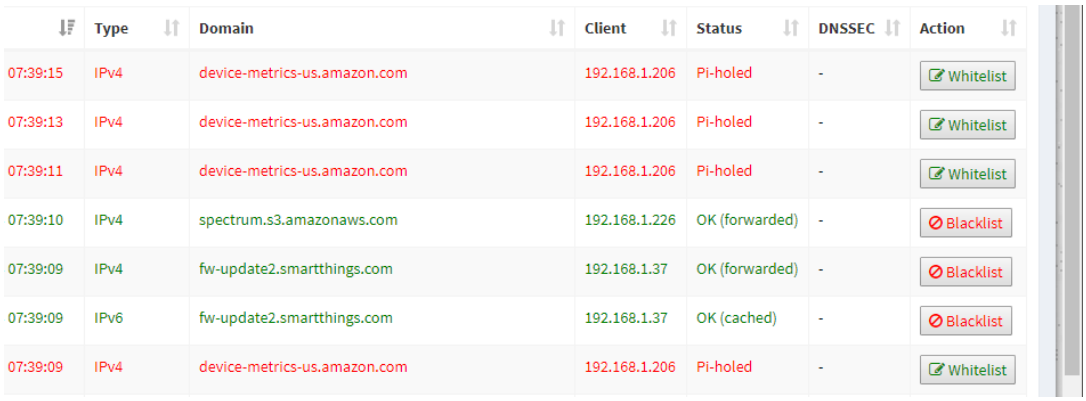


Рисунок 3.7 –Статистика Pi-hole з веб-інтерфейсу

У процесі тестування було зафіксовано, що в середньому система обробляє від 500 до 100 запитів на годину, залежно від кількості активних користувачів у мережі. Найвищу активність показали смартфони, які генерують фонові запити навіть у режимі очікування, та смарт-телевізори, що надсилають десятки запитів при кожному переході в інтерфейсі. Пік активності з врахуванням 3 активних пристроїв сягав 700 запитів на годину.

Крім загального графіка, у розділі Query Log можна переглянути подробиці кожного запиту: IP-адреса пристрою, точний час, домен, результат (заблоковано або дозволено). Також у Web UI доступна вкладка Top Clients, яка показує найактивніші пристрої у мережі за кількістю запитів. Наприклад, протягом години смартфон надіслав понад 1200 DNS-запитів, тоді як стаціонарний ПК — лише близько 350 (рис.3.8).



	Type	Domain	Client	Status	DNSSEC	Action
07:39:15	IPv4	device-metrics-us.amazon.com	192.168.1.206	Pi-holed	-	Whitelist
07:39:13	IPv4	device-metrics-us.amazon.com	192.168.1.206	Pi-holed	-	Whitelist
07:39:11	IPv4	device-metrics-us.amazon.com	192.168.1.206	Pi-holed	-	Whitelist
07:39:10	IPv4	spectrum.s3.amazonaws.com	192.168.1.226	OK (forwarded)	-	Blacklist
07:39:09	IPv4	fw-update2.smartthings.com	192.168.1.37	OK (forwarded)	-	Blacklist
07:39:09	IPv6	fw-update2.smartthings.com	192.168.1.37	OK (cached)	-	Blacklist
07:39:09	IPv4	device-metrics-us.amazon.com	192.168.1.206	Pi-holed	-	Whitelist

Рисунок 3.8 – Query Log вPi-hole

Загалом, наявність такої статистики дозволяє не лише стежити за ефективністю блокування, а й оперативно виявляти аномальні запити, потенційні загрози чи спроби обходу фільтрації.

3.2.3 Тестування кешування DNS-запитів (швидкість відповіді)

Однією з важливих функцій системи Pi-hole є локальне кешування DNS-запитів за допомогою вбудованого механізму dnsmasq. Це дозволяє зменшити кількість повторних звернень до зовнішніх DNS-серверів, знизити навантаження на мережу та прискорити обробку повторних запитів.

Для перевірки ефективності кешування було проведено тестування із застосуванням команди dig, яка дозволяє оцінити час відповіді DNS-сервера. Спершу виконувався первинний запит до нового домену (наприклад, dig wikipedia.org), а потім — повторний той самий запит (рис. 3.9).

Команда

```
dig wikipedia.org
```

Результат першого запиту (без кешу):

```
;; Query time: 68 msec
;; SERVER: 192.168.0.100#53(192.168.0.100)
```

Результат другого запиту (з кешу):

```
;; Query time: 1 msec
;; SERVER: 192.168.0.100#53(192.168.0.100)
```

Рисунок 3.9 – Тестування із застосуванням команди dig

Як видно, швидкість відповіді з кешу зростає у десятки разів. Така оптимізація особливо помітна при багаторазових зверненнях до популярних сервісів, як-от Google, YouTube, Wikipedia, або при автоматичних запитах зі смартфонів.

Для масового тестування використовувався інструмент dig +noall +stats, а також проводився моніторинг через Web UI у розділі Query Log, де кешовані запити позначаються відповідним статусом (cached).

В середньому, за результатами вимірювань, повторні запити оброблялися в межах 1–3 мс, тоді як зовнішні — від 30 до 90 мс залежно від завантаженості мережі та DNS-провайдера.

Наявність кешування дозволяє не лише підвищити продуктивність усієї мережі, а й зменшити затримки в завантаженні вебсторінок для кінцевого користувача. Це є особливо важливим у домашніх або офісних умовах із великою кількістю пристроїв.

3.2.4 Поведінка системи при обхідних спробах

У процесі тестування було перевірено, як система Pi-hole реагує на спроби обійти фільтрацію реклами за допомогою сторонніх DNS-серверів. Оскільки Pi-hole працює як DNS-фільтр, важливо, щоб усі клієнтські пристрої в мережі надсилали DNS-запити саме через нього. В іншому випадку користувач може вручну змінити налаштування DNS і звертатися напряму до публічних серверів, таких як Google DNS (8.8.8.8) або Cloudflare (1.1.1.1), що дозволить отримати необроблену відповідь і, відповідно, бачити рекламу.

Для перевірки цього сценарію на одному з пристроїв (ноутбук з Windows 10) вручну було змінено параметри мережі та встановлено DNS 8.8.8.8. Після цього відображення реклами на сайтах повернулося, що свідчить про успішне обхід фільтрації. Така ситуація є типовою і може виникати у випадках, коли користувачі навмисно або випадково змінюють мережеві налаштування.

Щоб запобігти подібним ситуаціям, у конфігурації маршрутизатора було додатково реалізовано примусове перенаправлення всіх DNS-запитів на Pi-hole. Це досягається за допомогою блокування будь-яких запитів на порти DNS (UDP/53), окрім тих, які спрямовані на адресу Raspberry Pi (192.168.0.100). Деякі маршрутизатори також дозволяють автоматично переадресовувати всі DNS-запити незалежно від IP, який був вказаний користувачем.

Після впровадження цих обмежень навіть при ручному введенні стороннього DNS (наприклад, через команду nslookup google.com 8.8.8.8) у відповідь повертався IP-адрес Pi-hole (192.168.0.100), що підтверджує ефективність перенаправлення та контроль системи.

Таким чином, для забезпечення надійної фільтрації реклами в локальній мережі важливо не лише використовувати Pi-hole як DNS-сервер, але й захищати мережу від обходу — шляхом мережевих правил на рівні маршрутизатора або брандмауера. Це дозволяє гарантувати єдину політику фільтрації для всіх пристроїв незалежно від їх конфігурації.

3.2.5 Стабільність системи при тривалому використанні

У ході експлуатації системи фільтрації DNS-запитів на базі Pi-hole було проведено перевірку стабільності її роботи в умовах тривалого безперервного використання. Система працювала на пристрої Raspberry Pi 4 без перезавантаження протягом 10 діб у середовищі домашньої мережі з середнім навантаженням 4–6 активних клієнтських пристроїв одночасно (табл. 3.1).

Таблиця 3.1 - Умови тестування та спостереження за стабільністю системи Pi-hole

№	Параметр	Спостереження
1	Середня кількість клієнтів	5–7 пристроїв одночасно
2	Тривалість тестування	10 діб безперервно
3	Максимальна температура CPU	58°C (в активному корпусі з вентилятором)
4	Середнє навантаження CPU	15–25%
5	Зайнято оперативної пам’яті	Менше 400 МБ
6	Рівень блокування DNS-запитів	30–40% від загальної кількості
7	Автозапуск після зникнення живлення	Успішно, протягом 10–15 секунд
8	Доступність веб-інтерфейсу	Безперервна, жодного збою за весь період тестування

Протягом усього періоду не було зафіксовано збоїв у роботі DNS-сервісу. Веб-інтерфейс залишався доступним, статистика оновлювалась у реальному часі, а блокування реклами здійснювалося стабільно. Температурні показники Raspberry Pi при використанні корпусу з вентилятором залишались у межах 50–58°C, що є безпечним режимом для постійної експлуатації.

Важливим чинником стабільної роботи є ефективне управління журналами та кешем. Було встановлено регулярне очищення лог-файлів за допомогою утиліти logrotate, що дозволило уникнути переповнення пам’яті. Кеш DNS-запитів автоматично очищувався при оновленнях фільтрів, що запобігає накопиченню застарілих записів.

Також було протестовано відновлення системи після зникнення живлення. Після вимкнення пристрою від мережі та подальшого ввімкнення, система Pi-hole автоматично запускалась без потреби втручання. DNS-запити почали оброблятись уже за 10–15 секунд після завантаження Raspberry Pi, що

підтверджує автоматичну ініціалізацію служб. На рисунку 3.10 можна побачити динаміку обробки запитів в режимі звичайного робочого дня.

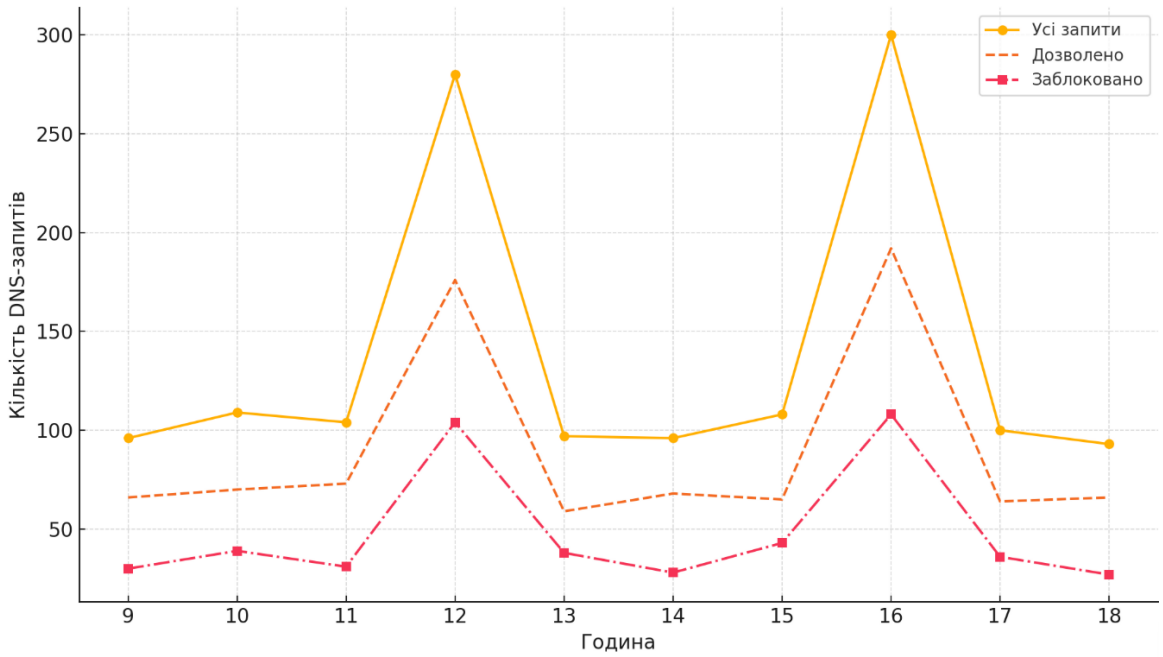


Рисунок 3.10 – Динаміка DNS-Запитів та блокування реклами

Загалом, результати тестування свідчать про високу надійність і стабільність роботи системи упродовж тривалого часу без необхідності регулярного обслуговування. Це робить рішення на базі Pi-hole доцільним не лише для домашнього використання, а й для невеликих офісних мереж.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Актуальність безпеки життєдіяльності людини

Безпека життєдіяльності (БЖД) – наука, що вивчає проблеми безпечного перебування людини в довкіллі в процесі різних видів її діяльності. Яскра діяльність і вирізняє людину від інших істот. Вона є специфічною людською формою активності, необхідною умовою існування людського суспільства. Форми діяльності різноманітні. Вони охоплюють практичні, інтелектуальні і духовні процеси, які протікають в побуті, громадській, культурній, виробничій, науковій та інших сферах життя.

В сучасному світі забезпечення безпеки життєдіяльності людини стає все більш актуальною та важливою проблемою. Розуміння і свідоме ставлення до ризиків та загроз, які впливають на безпеку людей у різних сферах їхнього життя, стає необхідністю для забезпечення якісного та тривалого існування. Отже, детальний аналіз актуальності безпеки життєдіяльності людини в сучасному світі вкрай важливий [21].

Діяльністю займаються всі – діти, дорослі, люди похилого віку, тому безпека діяльності має відношення до всього людства.

Актуальність дисципліни ще більше зростає у зв’язку зі сталим розвитком людства на базі, що забезпечує його існування, тобто аксіом про потенційну небезпеку діяльності – кожний вид діяльності є потенційно небезпечний. Ця аксіома справедлива і для бездіяльності, тому що бездіяльна людина ще більше залежить від діяльності іншої людини.

Безпека людини є базовою складовою “сталого людського розвитку” (Sustainable Human Development). Він широко використовує ООН як основна

характеристика гуманітарного поступу суспільства. Сталий розвиток людства - це такий розвиток, який веде не тільки до економічного, а й соціального, духовного зростання, що сприяє гуманізації національного менталітету і збагаченню позитивного загальнолюдського досвіду. Основною ознакою, що відрізняє сталий розвиток від усіх інших форм соціального руху і вдосконалення, є відновлення природного і культурного довкілля, коли не тільки не знищуються життєвий потенціал, а й підвищується соціальна відповідальність людей, гуманістичність взаємин, ставлення, реакцій. Тому актуальність питань з безпеки життєдіяльності полягає саме у зв'язку сталого людського гармонійного розвитку людства і природи. Виходячи з концепції сталого розвитку людства безпека життєдіяльності найбільш повно охарактеризувати як багатогранність галузь знань про закони природозберігаючого формування техносфери планети та її збалансованого економічного й суспільного розвитку.

Також, актуальність безпеки життєдіяльності проявляється в сфері соціальної безпеки. Соціальні загрози, такі як безробіття, бідність, насильство, дискримінація та інші форми соціальної небезпеки, суттєво впливають на якість життя людей та порушувати гармонію та стабільність суспільства. Отже, розуміння актуальності безпеки 37 життєдіяльності з соціального погляду є ключовим для створення справедливого та безпечного соціуму [22].

У світі, який швидко змінюється, актуальність безпеки життєдіяльності людини стає все більш складною задачею. Глобалізація, технологічний прогрес та інші фактори створюють нові загрози та виклики для безпеки людей. Важливо адаптуватися до цих змін та розробляти ефективні стратегії для забезпечення безпеки в усіх сферах життя.

У підсумку, актуальність безпеки життєдіяльності людини є невід'ємною складовою сучасного світу. Розуміння основних аспектів безпеки, таких як фізична безпека, охорона здоров'я, соціальна безпека та врахування сучасних викликів та тенденцій, допомагає створювати безпечне та стійке середовище для життя та розвитку людей. Тільки шляхом постійного аналізу та

удосконалення стратегій безпеки забезпечуючи належний рівень безпеки для всіх людей та покращити їхнє життя.

4.2 Заходи, що покращуюють умови праці оператора

Організація робочого місця оператора забезпечує відповідність усіх елементів робочого місця та їх взаємного розташування ергономічним вимогам, характеру та особливостям трудової діяльності [24].

Площа, виділена для одного робочого місця з ВДТ, складає не менше 6 м 2 , а об'єм – не менше 20 м3 . Базовими елементами комп'ютеризованого робочого місця вважається відеотермінал, клавіатура , і мишка. Також додатково встановлені принтер, IP – телефон і інше обладнання.

Розташування екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом – 30° від лінії зору користувача. Найкращі зорові умови і можливість розпізнавання знаків досягається такою геометрією розміщення, коли верхній край відеотерміналу знаходиться на висоті очей, а погляд спрямований вниз на центр екрана.

Оскільки при роботі за ВДТ найбільш сприятливим вважається нахил голови вперед, приблизно на 20° від вертикалі, при такому положенні голови м'язи шиї розслабляються, то екран відеотерміналу також повинен бути нахиленим назад на 20° від вертикалі. Екран відеотерміналу та клавіатура розташовуються на оптимальній відстані від очей користувача, але не ближче 600 мм [23].

Лінія електромережі для живлення ЕОМ, периферійних пристроїв та обладнання для обслуговування та налагоджування ЕОМ виконується як окрема групова трьохпровідникова мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників.

Нульовий захисний провідник використовується для заземлення, занулення електроприймачів і прокладається до стійки групового розподільчого щита, розподільчого пункту до розеток живлення.

Для споруд та приміщень, в яких експлуатуються відеотермінали та ЕОМ, крім загальних вимог пожежної безпеки, здійснюються спеціальні протипожежні заходи, визначені Правилами пожежної безпеки в Україні (наказ Міністерства внутрішніх справ України від 30.12.2014 №1417) та іншими нормативними документами.

Згідно санітарних правил для нормальної організації праці працівників, які обслуговують ВДТ ЕОМ та ПЕОМ передбачаються внутрішньозмінні регламентовані перерви для відпочинку, які передують появі об'єктивних і суб'єктивних ознак стомлення і зниження працездатності [23].

При виконанні протягом дня робіт, які належать до різних видів трудової діяльності, за основну роботу з ВДП ЕОМ і ПЕОМ вважається такою, що займає не менше 50% часу впродовж робочої зміни чи робочого дня. Відповідно до санітарних правил встановлюються такі внутрішньозмінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці:

– для розробників програм із застосуванням ЕОМ призначають регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи;

– для операторів із застосуванням ЕОМ призначають регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні 2 години роботи;

– для операторів комп'ютерного набору призначають регламентовані перерви для відпочинку тривалістю 10 хвилин після кожної години роботи.

Такі умови організації робочого місця і часу роботи за терміналом не будуть шкідливими для здоров’я оператора. В свою чергу зручність організації робочого місця збільшить продуктивність праці оператора.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було повністю реалізовано комплексний підхід до створення, впровадження та тестування комп'ютерної системи блокування реклами, яка функціонує на рівні локальної мережі. Основою розробленої системи стала апаратна платформа Raspberry Pi 4 Model B та спеціалізоване програмне забезпечення Pi-hole, яке забезпечує фільтрацію DNS-запитів у реальному часі.

Першим етапом реалізації став аналіз предметної області. Було з'ясовано, що традиційні засоби блокування реклами, які реалізуються у вигляді плагінів браузерів або програм-клієнтів, мають ряд обмежень, зокрема — необхідність встановлення на кожному окремому пристрої, обмежений контроль над трафіком та відсутність централізованого моніторингу. Було доведено, що системи, що працюють на рівні DNS, мають значно вищу ефективність, зручність та безпечність, оскільки дозволяють обробляти запити ще до моменту їх переходу до кінцевого користувача.

У проєктній частині було здійснено технічне обґрунтування вибору апаратного забезпечення. Raspberry Pi 4 було обрано як оптимальну платформу з точки зору ціни, енергоспоживання, гнучкості налаштувань та можливості автономної роботи у серверному режимі. Було спроєктовано архітектуру системи, яка включає маршрутизатор, фільтраційний вузол на основі Pi-hole, чорні списки рекламних доменів, клієнтські пристрої та зовнішні DNS-сервери. Детально проаналізовано взаємодію між апаратними та програмними компонентами, способи кешування DNS-запитів, оновлення фільтрів, логування та адміністрування через веб-інтерфейс.

На етапі реалізації системи було проведено підготовку Raspberry Pi до роботи в мережі, встановлено Pi-hole, налаштовано перенаправлення DNS-запитів через маршрутизатор, організовано оновлення чорних списків за допомогою cron-завдань, а також реалізовано візуалізацію статистики через Web UI. Була досягнута стабільна робота системи в умовах локальної мережі,

з мінімальними затримками обробки запитів і високим рівнем ефективності блокування.

У тестовому середовищі було перевірено працездатність системи на різних типах клієнтів (ПК, смартфони, смарт-ТВ) із використанням популярних сайтів (YouTube, tsn.ua, obozrevatel.com, 24tv.ua та інших). Під час тестування було зафіксовано суттєве зниження кількості рекламних блоків, успішне блокування запитів до сторонніх аналітичних платформ і трекерів, а також зменшення обсягу небажаного трафіку. У середньому було заблоковано понад 70–80% рекламних DNS-запитів.

Крім цього, робота розглядає питання продуктивності та безпеки. Було визначено, що середній час обробки DNS-запитів системою складає менше 10 мс, що є прийнятним показником для локального середовища. Застосування кешування дозволяє багаторазово пришвидшити відповіді при повторних запитах. З безпекового боку, система має захист від підміни DNS-запитів, дозволяє впровадити примусове перенаправлення DNS, а також підтримує обмеження доступу до адміністративного інтерфейсу.

Таким чином, в межах роботи було досягнуто поставлену мету — створено ефективну, стабільну та легко масштабовану комп’ютерну систему блокування реклами в локальній мережі. Система демонструє високу ефективність фільтрації, простоту в адмініструванні, низькі вимоги до ресурсів та може бути легко адаптована до потреб різних типів користувачів — від домашніх мереж до невеликих офісів.

Загалом, запропоноване рішення є практичним прикладом ефективної реалізації мережевої фільтрації з використанням відкритих технологій, яке відповідає сучасним вимогам безпеки, продуктивності та зручності в експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Жаровський Р.О., Луцик Н.С., Осухівська Г.М., Паламар А.М., Тиш Є.В. Методичні вказівки до виконання кваліфікаційної роботи бакалавра для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 123 «Комп'ютерна інженерія» усіх форм навчання. Тернопіль: ТНТУ, 2024. 39 с.

2. Буров Є.В., Митник М.М. Комп'ютерні мережі. Підручник. Том другий. Львів: «Магнолія 2006», 2024. 204 с.

3. Буров Є.В., Митник М.М. Комп'ютерні мережі. Підручник. Том перший. Львів: «Магнолія 2006», 2024. 333 с.

4. Shabliy N., Lupenko S., Lutsyk N., Yasniy O., Malyshevska O. Keystroke dynamics analysis using machine learning methods. Applied Computer Science. 2021. Vol. 17, No. 4. P. 75-83.

5. Velychko D., Osukhivska H., Palaniza Y., Lutsyk N., Sobaszek L. Artificial Intelligence Based Emergency Identification Computer System. Advances in Science and Technology Research Journal, 18 no. 2, 2024, P. 296-304.

6. Voloshchuk A., Velychko D., Osukhivska H., Palamar A. Computer system for energy distribution in conditions of electricity shortage using artificial intelligence. CEUR Workshop Proceedings, 2nd International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2024), Ternopil, Ukraine, June 12-14, 2024. Vol. 3742 P. 66-75.

7. Voloskyi V., Leshchyshyn Y., Romanyshyn N., Palamar A., Tarasenko L. Method and algorithm for efficient cell balancing in the lithium-ion battery control system. CEUR Workshop Proceedings, The 1st International Workshop on Bioinformatics and Applied Information Technologies (BAIT 2024), Zboriv, Ukraine, October 02-04, 2024. Vol. 3842. P. 258-267.

8. Yasniy O., Lutsyk N., Demchyk V., Osukhivska H., Malyshevska O. The prediction of structural properties of Ni-Ti shape memory alloy by the supervised machine learning methods. ITTAP 2023: 73–78. https://ceur-ws.org/Vol-3628/short1.pdf

9. Довгун О., Лупенко С., Осухівська Г., Луцик Н. Розробка інструментів моніторингу локальних мереж з використанням відкритих рішень. // Науковий вісник ТНТУ, 2023. № 1 (109). С. 43–50.

10. Івановський Д., Луцик Н., Осухівська Г. Побудова безпечної домашньої мережі на базі Raspberry Pi. // Вісник комп'ютерних систем. ТНТУ. 2023. № 2(30). С. 91–97.

11. Мазур І., Осипенко В., Шклярський Р. Аналіз інструментів блокування реклами у локальних мережах. // Інформаційна безпека України. 2024. Т. 29, № 1. С. 17–25.

12. Дмитренко С., Ткаченко П. Реалізація фільтрації реклами на базі Raspberry Pi в навчальному середовищі. // Матеріали конференції ICTERI Workshops. CEUR-WS.org, 2022. Т. 3130. С. 129–136.

13. Барановський І., Лис М. Підвищення приватності в домашній мережі за допомогою технологій DNS Sinkhole. // Український журнал інформаційної безпеки. 2023. Т. 29(1). С. 30–38.

14. Гринюк Т., Назарчук І. Технології фільтрації DNS-запитів у домашніх та корпоративних мережах. // Інформаційні технології та комп'ютерна інженерія. 2024. № 2(72). С. 64–70.

15. D'Orazio C. Blocking Ads and Trackers Using Pi-hole: A Practical Guide. Independently published, 2022. 124 p.

16. Upton E., Halfacree G. Raspberry Pi User Guide. 4th ed. Wiley, 2016. 312 p.

17. Convery S. Pi-hole for Beginners: Network-wide Ad Blocking. Amazon KDP, 2021. 102 p.

18. Kurniawan A. Raspberry Pi Networking Cookbook. Packt Publishing, 2016. 296 p.

19. Ali M., Prasad R. DNS-Based Filtering Techniques for Secure Internet Browsing. // International Journal of Computer Applications. Vol. 185, No. 42, 2023. P. 25–30.

20. Tavares E. Pi-hole Simplified: Guide to Set Up DNS-Based Ad Blocking for Home Network. Amazon KDP, 2020. 98 p.

21. Бедрій І.Я., Нечай В.Я. Безпека життєдіяльності. Навчальний посібник. – Львів: Манголія 2006, 2007. 499 с. 43

22. Зеркалов Д.В. Безпека життєдіяльності. Навчальний посібник. - К.: Основа, 2011.

23. Організація праці операторів комп'ютерів. URL: https://pidru4niki.com/92832/bzhd/organizatsiya_pratsi_operatoriv_komp_yuteriv (дата звернення: 14.05.2025).

24. Заходи для покращення умов праці операторів комп'ютерів. URL: https://pidru4niki.com/92831/bzhd/zahodi_pokraschennya_umov_pratsi_operatoriv_ kompyuteriv (дата звернення: 14.05.2025).

Додаток А

Технічне завдання

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп’ютерно-інформаційних систем і програмної інженерії

Кафедра комп’ютерних систем та мереж

“Затверджую”

Завідувач кафедри КС

_____ Осухівська Г.М.

“___” _____2025 р

Комп’ютерна система блокування реклами в локальній мережі на базі Raspberry PI

ТЕХНІЧНЕ ЗАВДАННЯ

на _10_ листках

Вид робіт: Кваліфікаційна робота

На здобуття освітнього ступеня «Бакалавр»

Спеціальність 123 «Комп’ютерна інженерія»

«УЗГОДЖЕНО»	«ВИКОНАВЕЦЬ»
Керівник кваліфікаційної роботи	Студент групи СІ-41
_____ к.ф.-м.н., доц. Варавін А.В.	_____ Мордованець А. В.
«____» _____ 2025 р.	«____» _____ 2025 р.

Тернопіль 2025

1 Загальні відомості

1.1 Повна назва та її умовне позначення

Повна назва теми кваліфікаційної роботи: «Комп’ютерна система блокування реклами в локальній мережі на базі Raspberry PI».

Умовне позначення кваліфікаційної роботи: КС КРБ 123.216.00.00

1.2 Виконавець

Студент групи СІ-41, факультету комп’ютерно-інформаційних систем і програмної інженерії, кафедри комп’ютерних систем та мереж, Тернопільського національного технічного університету імені Івана Пулюя, Мордованець Артем Васильович

1.3 Підстава для виконання роботи

Підставою для виконання кваліфікаційної роботи є наказ по університету (№4/7-53 від 27.01.2025 р.)

1.4 Планові терміни початку та завершення роботи

Плановий термін початку виконання кваліфікаційної роботи – 27.01.2025 р.

Плановий термін завершення виконання кваліфікаційної роботи – 23.06.2025 р.

1.5 Порядок оформлення та пред’явлення результатів роботи

Порядок оформлення пояснювальної записки та графічного матеріалу здійснюється у відповідності до чинних норм та правил ISO, ЕСКД, ЕСПД та ДСТУ.

Пред’явлення проміжних результатів роботи з виконання кваліфікаційної роботи здійснюється у відповідності до графіку, затвердженого керівником роботи. Попередній захист кваліфікаційної роботи відбувається при готовності роботи – наявності пояснювальної записки та графічного матеріалу.

Пред’явлення результатів кваліфікаційної роботи відбувається шляхом захисту на відповідному засіданні ЕК, ілюстрацією основних досягнень за допомогою графічного матеріалу.

2 Призначення і цілі створення системи

2.1 Призначення системи

Розроблювана комп’ютерна система призначена для:

– централізованого блокування рекламного контенту у локальній мережі;

– забезпечення безпечного та комфортного доступу користувачів до інтернет-ресурсів;

– фільтрації DNS-запитів з метою запобігання завантаженню сторонньої реклами.

Система інтегрується в локальну інфраструктуру та забезпечує фільтрацію мережевого трафіку без потреби у встановленні сторонніх додатків на кожному пристрої користувача.

2.2 Мета створення системи

Метою кваліфікаційної роботи є розробка, налаштування та впровадження комп’ютерної системи блокування реклами, що функціонує на базі одноплатного мікрокомп’ютера Raspberry Pi з використанням програмного забезпечення Pi-hole. Система повинна забезпечувати ефективну

фільтрацію DNS-запитів, збереження статистики, зручне адміністрування та високу продуктивність у домашній або офісній мережі.

2.3 Характеристика об'єкту

Об’єктом розробки є локальна комп’ютерна мережа, у якій реалізується централізоване блокування реклами. Система створюється на основі Raspberry Pi 4, що виконує роль DNS-сервера-фільтра. Програмне забезпечення Pi-hole дозволяє здійснювати моніторинг запитів, керування списками доменів, ведення журналів і налаштування політик доступу.

3 Вимоги до системи

3.1 Вимоги до системи в цілому

3.1.1 Вимоги до структури та функціонування системи

Система блокування реклами в локальній мережі повинна складатися з:

– одноплатного комп’ютера (Raspberry Pi), що виконує роль DNS-сервера;

– програмного забезпечення для фільтрації DNS-запитів (наприклад, Pi-hole);

– засобів адміністрування (веб-інтерфейс або термінал);

– оновлюваних списків рекламних доменів.

Функціонування системи повинно забезпечувати автоматичне перехоплення DNS-запитів, перевірку їх на відповідність чорним спискам, блокування небажаного контенту або перенаправлення допустимих запитів на зовнішні DNS-сервери.

3.1.2 Вимоги до способів та засобів зв’язку між компонентами системи

Основна вимога до засобів зв’язку – це сумісність та стабільна взаємодія між клієнтськими пристроями, маршрутизатором і сервером фільтрації. Обмін даними повинен здійснюватися через стандартні мережеві протоколи (TCP/IP, DNS). DNS-запити мають бути перенаправлені маршрутизатором на Raspberry Pi з мінімальними затримками.

3.1.3 Вимоги до режимів функціонування системи

Для системи визначено два режими функціонування:

– нормальний режим — система стабільно блокує рекламні домени, виконує фільтрацію запитів і веде статистику;

– аварійний режим — у разі відмови сервісу фільтрації DNS-запити мають бути автоматично перенаправлені на зовнішні DNS-сервери, забезпечуючи базову роботу мережі без фільтрації.

Для підтримки нормального режиму необхідно дотримуватися умов експлуатації обладнання та своєчасно оновлювати програмне забезпечення і списки блокування.

3.1.4 Вимоги по діагностуванню системи

Діагностика функціонування системи повинна виконуватись за допомогою вбудованих у Pi-hole інструментів, зокрема лог-файлів запитів, інтерфейсу перегляду статистики та журналів помилок. Додатково можуть використовуватись інструменти операційної системи для контролю стану мережі, ресурсів системи та стану служб.

Інтерфейс адміністратора має надавати можливість оперативного моніторингу активності, перегляду заблокованих доменів, часу відповіді на запити.

3.1.5 Перспективи розвитку, проектування системи

Система може бути вдосконалена шляхом:

– додавання інтеграції з проксі-серверами для глибшого аналізу трафіку (HTTP/HTTPS);

– реалізації функцій оповіщення адміністратора про підозрілу активність;

– впровадження механізмів автоматичного аналізу нових джерел реклами;

– масштабування під більшу кількість клієнтів за рахунок заміни апаратної платформи або використання серверного обладнання;

– підключення резервного Pi-hole або балансування навантаження.

Це забезпечить гнучкість та адаптацію системи до потреб як домашніх, так і корпоративних мереж.

3.2 Показники призначення

Система блокування реклами повинна забезпечувати можливість масштабування з метою адаптації до різних умов використання — від домашніх мереж до малих корпоративних інфраструктур. Масштабування може бути реалізоване завдяки використанню більш продуктивного обладнання (наприклад, серверів замість одноплатних комп’ютерів) або розподіленої архітектури з кількома фільтраційними вузлами. Програмне забезпечення повинно підтримувати багатокористувацький режим, автоматичне оновлення списків блокування та можливість централізованого адміністрування.

3.2.1 Вимоги до надійності

Система повинна зберігати працездатність або забезпечувати швидке відновлення функціональності у таких випадках:

– збої електроживлення пристрою Raspberry Pi;

– збої апаратного характеру, пов’язані з мережею, накопичувачами або периферією;

– програмні помилки або критичні оновлення операційної системи та DNS-фільтра.

Для забезпечення надійності роботи рекомендовано використовувати стабілізатори напруги або мережеві фільтри. Живлення Raspberry Pi бажано організовувати через джерело безперебійного живлення (UPS) для запобігання некоректному вимкненню та втраті даних.

3.3 Вимоги до безпеки

Усі елементи апаратної частини системи, які працюють під напругою, повинні бути надійно ізольовані та мати захист від випадкового дотику. Пристрій Raspberry Pi має бути встановлений у відповідному корпусі з вентиляцією та захисним заземленням. У випадку перевантаження або короткого замикання має бути забезпечене автоматичне вимкнення електроживлення.

3.3.1 Вимоги до експлуатації, технічного обслуговування, ремонту і зберігання компонентів системи

Мікроклімат в приміщеннях повинен відповідати нормам виробничого мікроклімату по ДСН 3.3.6.042-99:

– температуру повітря в межах від +10ºС до +35ºС;

– відносну вологість повітря при 25ºС в межах від 30% до 80%;

– атмосферний тиск 760±25 мм рт. ст.

Періодичне технічне обслуговування використовуваних технічних засобів має проводитися відповідно до вимог технічної документації, але не рідше ніж один раз на рік.

Періодичне технічне обслуговування і тестування технічних засобів повинні включати обслуговування і тестування всіх використовуваних засобів, датчики, контроллери, системи передачі даних, пристрої безперебійного живлення.

На підставі результатів тестування технічних засобів повинні проводитися аналіз причин виникнення виявлених дефектів і прийматися заходи по їх ліквідації.

3.4 Вимоги до захисту інформації від несанкціонованого доступу

Система повинна забезпечувати захист від несанкціонованого доступу на рівні не нижче встановленого вимогами, що пред'являються до категорії 1Д по класифікації документа, що діє, “Автоматизовані системи. Захист від несанкціонованого доступу до інформації. Класифікація автоматизованих систем”.

Компоненти підсистеми захисту від НСД повинні забезпечувати:

– ідентифікацію користувача;

– перевірку повноважень користувача при роботі з системою;

– розмежування доступу користувачів.

Рівень захищеності від несанкціонованого доступу засобів обчислювальної техніки, що здійснюють обробку конфіденційної інформації, повинен відповідати вимогам класу захищеності згідно вимогам документу “Засоби обчислювальної техніки. Захист від несанкціонованого доступу до інформації. Показники захищеності від несанкціонованого доступу до інформації”.

3.4.1 Вимоги по збереженню інформації при аваріях

Інформація, при виникненні аварійних ситуацій повинна бути збережена на резервних носіях.

3.4.2 Вимоги по стандартизації і уніфікації

Система повинна відповідати вимогам ергономіки і зручності користування за умови комплектування високоякісним обладнанням (ЕОМ,

монітор і інше обладнання), що має необхідні сертифікати відповідності і безпеки.

3.4.3 Вимоги до функцій (завдань), що виконуються системою:

– зручний веб-інтерфейс керування;

– зберігання списків блокування;

– швидке оброблення DNS-запитів;

4 Вимоги до документації

Документація повинна відповідати вимогам ЄСКД та ДСТУ

Комплект документації повинен складатись з:

– пояснювальної записки;

– графічного матеріалу:

а) Структурна схема.

б) Блок схема роботи комп’ютеризованої системи.

в) Блок схема блокування реклами.

г) Логічна структурна схеми адресації пристроїв.

д) Графік блокування реклами.

*Примітка: У комплект документації можуть вноситися зміни та доповнення в процесі розробки.

5 Стадії та етапи проектування

Таблиця 1 – Стадії та етапи виконання кваліфікаційної роботи бакалавра

№ етапу	Назва етапу виконання кваліфікаційної роботи	Термін виконання
1	Розробка технічного завдання.	27.01.2025р. – 02.02.2025р.
2	Аналіз предметної області та постановка задачі	03.02.2025 р. – 16.02.2025 р.
3	Вибір інструментів і розробка архітектури системи	17.02.2025 р. – 02.03.2025 р.
4	Реалізація та тестування системи	03.03.2025 р. – 23.03.2025 р.
5	Безпека життєдіяльності, основи охорони праці	01.06.2025 р.- 08.06.2025 р.
6	Оформлення пояснювальної записки і графічного матеріалу	07.04.2025 р. – 08.06.2025 р.
7	Перевірка на академічний плагіат, перевірка керівником та консультантами	9.06.2025р. – 15.06.2025р.
8	Попередній захист кваліфікаційної роботи бакалавра	16.06.2025р. – 22.06.2025р.
9	Захист кваліфікаційної роботи бакалавра	27.06.2025р.

6 Додаткові умови виконання кваліфікаційної роботи

Під час виконання кваліфікаційної роботи у дане технічне завдання можуть вноситися зміни та доповнення.

Додаток Б

Публікація у науковій конференції

УДК 621.326
Мордованець А. – студент групи СІ-41
Тернопільський національний технічний університет імені Івана Пулюя

КОМП'ЮТЕРНА СИСТЕМА БЛОКУВАННЯ РЕКЛАМИ В ЛОКАЛЬНІЙ МЕРЕЖІ НА БАЗІ RASPBERRY PI

Науковий керівник: к.ф.-м.н., ст.викл. Варавін А.В.

Mordovanets′ A.
Ternopil Ivan Puluj National Technical University

COMPUTER SYSTEM FOR AD BLOCKING IN A LOCAL NETWORK BASED ON RASPBERRY PI

Supervisor: Varavin A.

Ключові слова: Raspberry Pi, Pi-hole, локальна мережа, блокування реклами.
Key words: Raspberry Pi, Pi-hole, local network, ad blocking.

В умовах стрімкого зростання інтернет-трафіку та нав'язливої реклами у цифровому середовищі, забезпечення комфортного користувацького досвіду у локальних мережах вимагає ефективних та економічно доцільних технічних рішень. Одним із таких рішень є впровадження комп'ютерної системи блокування реклами, що реалізована на базі одноплатного комп'ютера Raspberry Pi з використанням програмного забезпечення Pi-hole.

У сучасному цифровому середовищі, де реклама проникає в усі сфери онлайн-активності, виникає потреба у захисті користувачів локальних мереж від нав'язливих оголошень, потенційно шкідливих скриптів і трекерів. Особливо це актуально в корпоративних або освітніх середовищах, де продуктивність і безпека мережевого трафіку мають ключове значення. Рішенням цієї проблеми стає впровадження комп'ютерної системи блокування реклами, що працює на рівні мережі. Raspberry Pi 4, як доступна та ефективна платформа, забезпечує достатню продуктивність для реалізації таких систем із використанням спеціалізованого програмного забезпечення, наприклад, Pi-hole.

Інтеграція Pi-hole дозволяє централізовано фільтрувати DNS-запити та блокувати доступ до рекламних доменів ще до їх завантаження на пристрої користувачів. Система не вимагає встановлення додаткових розширень на клієнтських пристроях, що забезпечує її прозору інтеграцію та мінімальні втручання в інфраструктуру. Таке рішення не тільки зменшує навантаження на мережу, а й підвищує рівень конфіденційності, що особливо важливо в контексті захисту персональних даних. Завдяки використанню відкритого програмного забезпечення та налаштуванню

гнучких фільтрів, система є масштабованою, адаптивною до конкретних потреб і економічно вигідною для впровадження як у малих офісах, так і в більших мережах.

Завдяки відкритій архітектурі, низькому енергоспоживанню, малій вартості та широкій спільноті розробників, Raspberry Pi є ідеальним обчислювальним вузлом для локального DNS-фільтра. Його апаратні характеристики, зокрема 4-ядерний процесор ARM Cortex-A72, 4–8 ГБ оперативної пам'яті та підтримка Ethernet-з'єднання, дозволяють ефективно обробляти мережеві запити та забезпечувати блокування доменів, які використовуються для завантаження реклами.

Pi-hole виступає як DNS-сервер, що перехоплює запити до рекламних доменів і блокує їх ще до завантаження в браузері клієнта. Такий підхід забезпечує системне блокування реклами для всіх пристроїв, підключених до локальної мережі, незалежно від операційної системи чи браузера.

В межах кваліфікаційної роботи проаналізовано наявні програмно-апаратні рішення, здійснено вибір оптимальної платформи та інструментів для реалізації, спроєктовано структуру системи, описано процес її розгортання та налагодження, а також проведено тестування на предмет стабільності роботи і навантаження на ресурси. Крім цього, розглянуто основні аспекти кібербезпеки та захисту від спроб обходу фільтрації.

Таким чином, розроблена система демонструє практичне застосування знань у сфері комп'ютерної інженерії та створює базу для масштабованих рішень у сфері безпечного та комфортного використання мережевих ресурсів у навчальних, офісних і домашніх умовах.

Література:

1) McManus, C. (2022). Mastering Pi-hole: Network-wide Ad Blocking and DNS Security. Apress.
2) Norris, C. (2023). Raspberry Pi for Network Security: Build and Secure Networks with the Raspberry Pi. Packt Publishing.
3) Allen, D. (2021). Practical Raspberry Pi Projects: Building Real-World Applications. Apress.
4) De Smet, D. (2020). Network Programming with Go: Secure and Scalable Network Applications. O'Reilly Media.
5) Pi-hole Team. (2024). Pi-hole Documentation and Admin Guide. https://docs.pi-hole.net.