НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри

Комп'ютерних систем, мереж та кібербезпеки

Касаткін Д.Ю., к. пед.н., доц.

Підпис ПІБ, вчене звання і ступінь

р.

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

На тему: Пристрій для фільтрації трафіку локальної мережі на основі мікрокомп’ютера Raspberry PI

Спеціальність F3 «Комп’ютерна інженерія»

Гарант освітньої програми

к.фіз.-мат.н., доцент _____ Євгеній НІКІТЕНКО

(науковий ступінь та вчене звання) (підпис) (ПІБ)

Керівник випускної бакалаврської роботи

старший викладач _____ Володимир МАТІЄВСЬКИЙ

(науковий ступінь та вчене звання) (підпис) (ПІБ)

Виконав

(підпис) (ПІБ студента)

Київ – 2025

Богдан МІХЕЄВ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАНН УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри комп'ютерних систем, мереж та кібербезпеки

Касаткін Д.Ю., к.пед.н., доц. /
підпис ПІБ, вчене звання і ступінь
2025 р.

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ БАКАЛАВРСЬКОЇ СТУДЕНТА

Міхеєв Богдан Єгорович
(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки): комп'ютерна інженерія

Тема випускної бакалаврської роботи: Пристрій для фільтрації трафіку локальної мережі на основі мікрокомп'ютера Raspberry PI

Керівник проекту (роботи) Матієвський В.В., старший викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджено наказом ректора НУБіП України від «16» грудня 2024 р. № 2250 «С»

Термін подання завершеної роботи на кафедру 2025, травень, 28
(рік, місяць, число)

Вихідні дані до випускної бакалаврської роботи (дипломного проекту бакалавра)
вимоги до пристрою для фільтрації трафіку

Перелік питань, які потрібно розробити:
Аналіз сучасних засобі блокування реклами, аналіз архітектури Paspberry PI 4, реалізація та тестування системи фільтрації

Перелік графічних документів (за потреби)

Дата видачі завдання "27**"** лютого 2025 р.

Керівник бакалаврської роботи _____ Матієвський В.В. старший викладач

Завдання прийняв до виконання _____ Міхеєв Б.Є.
(підпис) (прізвище та ініціали студента)

(підпис) (прізвище та ініціали)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз вимог до системи	07.03.2025 р.	Виконано
2	Проектування системи	15.03.2025 р.	Виконано
3	Реалізація системи	1.04.2025 р.	Виконано
4	Тестування розробленої системи	12.04.2025 р.	Виконано
5	Оформлення пояснювальної записки	15.05.2025 р.	Виконано
6	Оформлення графічного матеріалу	25.05.2025 р.	Виконано

Студент_____/ Богдан МІХЄЄВ _____/ /
(підпис) (ініціали та прізвище)

Керівник проекту (роботи)_____/ Володимир МАТІЄВСЬКИЙ /
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Пояснювальна записка: 61 сторінка, 6 рисунків, 6 таблиць, 48 джерел.

RASPBERRY PI, ФІЛЬТРАЦІЯ ТРАФІКУ, DNS, БЛОКУВАННЯ РЕКЛАМИ, PI-HOLE, ADGUARD HOME.

Об'єктом дослідження є процес фільтрації мережевого трафіку в локальних комп'ютерних мережах.

Метою роботи є проектування, реалізація та тестування пристрою фільтрації трафіку з використанням сучасних програмних рішень на платформі Raspberry Pi.

У першому розділі розглянуто проблему нав’язливої інтернет-реклами, історію розвитку засобів її блокування, класифікацію фільтрів та принципи роботи DNS-фільтрації. Проведено аналіз програмного забезпечення, зокрема Pi-hole та AdGuard Home, із порівнянням їх ефективності.

Другий розділ присвячено технічній реалізації системи: описано апаратну архітектуру на базі Raspberry Pi 4, мережеву інфраструктуру, способи інтеграції з DHCP та DNS, а також особливості живлення, охолодження й стабільної роботи системи.

У третьому розділі детально описано процес інсталяції та налаштування Pi-hole/AdGuard Home, конфігурацію DNS, моніторинг через веб-інтерфейс, забезпечення безпеки пристрою та резервне копіювання налаштувань.

Четвертий розділ містить результати тестування системи фільтрації на різних пристроях, аналіз логів і навантаження, оцінку продуктивності DNS-запитів і порівняльний аналіз між Pi-hole і AdGuard Home.

У результаті виконання роботи створено повноцінний пристрій фільтрації трафіку, перевірено його ефективність та запропоновано оптимальні рішення для домашнього або малого офісного використання.

ЗМІСТ

ВСТУП 7

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА АНАЛІЗ СУЧАСНИХ ЗАСОБІВ БЛОКУВАННЯ РЕКЛАМИ 9

1.1. Проблематика інтернет-реклами та її вплив на користувача 9

1.2 Історія виникнення та еволюція технологій блокування реклами 10

1.3. Класифікація та принципи роботи фільтрів реклами 12

1.4. DNS-фільтрація як засіб блокування: переваги та недоліки 14

1.5. Огляд популярного ПЗ: Pi-hole, AdGuard Home та інші альтернативи 16

1.6. Порівняння функціональності та ефективності різних рішень 18

РОЗДІЛ 2. АРХІТЕКТУРА ТА СКЛАДОВІ СИСТЕМИ НА ОСНОВІ RASPBERRY PI 4 22

2.1. Вибір апаратного забезпечення: огляд Raspberry Pi 4 та його можливостей 22

2.2. Блок-схема системи фільтрації реклами в локальній мережі 23

2.3. Мережеві інтерфейси, DHCP, DNS та роль Raspberry Pi 24

2.4. Інтеграція в існуючу домашню/офісну інфраструктуру 26

2.5. Додаткове обладнання (роутер, комутатор, накопичувачі тощо) 28

2.6. Безперебійна робота: стабільність, охолодження та живлення 30

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ФІЛЬТРАЦІЇ РЕКЛАМИ 33

3.1. Підготовка Raspberry Pi: встановлення Raspberry Pi OS 33

3.2. Налаштування доступу, оновлення, безпека пристрою 35

3.3. Покрокова інсталяція Pi-hole та/або AdGuard Home 38

3.4. Конфігурація DNS-сервера, інтеграція з DHCP..... 40
3.5. Візуалізація та контроль: веб-інтерфейси для моніторингу..... 42
3.6. Забезпечення безпеки системи: фаєрвол, VPN (опційно)..... 43
3.7. Резервне копіювання налаштувань та відновлення..... 44
РОЗДІЛ 4. ТЕСТУВАННЯ, ПОРІВНЯННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ 46
4.1. Методика тестування системи фільтрації 46
4.2. Тестування на різних пристроях (ПК, смартфони, SmartTV) 47
4.3. Аналіз логів, фільтрованих запитів і навантаження..... 49
4.4. Продуктивність системи: швидкість обробки DNS-запитів..... 55
4.5. Порівняльне тестування Pi-hole і AdGuard Home..... 59
4.6. Узагальнення результатів та рекомендації для користувачів 61
ВИСНОВКИ 63
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 64

ВСТУП

В умовах сучасного інформаційного суспільства значна частина щоденної діяльності користувачів пов’язана з доступом до мережі Інтернет. Проте зростання обсягів реклами в мережевому трафіку негативно впливає як на зручність користування веб-ресурсами, так і на загальну продуктивність роботи пристроїв та мережі. Надмірна кількість рекламних елементів не лише уповільнює завантаження сторінок, а й створює додаткове навантаження на канали зв’язку, споживає обчислювальні ресурси клієнтських пристроїв і часто становить загрозу конфіденційності або безпеці користувача.

Традиційні методи блокування реклами, такі як браузерні розширення або антивірусні рішення, мають низку обмежень. Зокрема, вони потребують інсталяції на кожному пристрої, не завжди ефективно працюють на SmartTV або мобільних пристроях, а також можуть конфліктувати з іншими застосунками. У цьому контексті все більшої актуальності набувають мережеві рішення для централізованої фільтрації небажаного контенту, які дозволяють блокувати рекламу на рівні DNS-запитів ще до того, як вона потрапляє на клієнтський пристрій.

Таким чином, дана тема є актуальною як з точки зору інформаційної безпеки, так і з огляду на потреби сучасного користувача в комфортному, швидкому та безпечному доступі до Інтернету.

Одним із доступних і гнучких способів реалізації такої системи є використання мікрокомп’ютера Raspberry Pi із встановленим програмним забезпеченням, таким як Pi-hole або AdGuard Home. Дані системи дозволяють перехоплювати DNS-запити всіх пристроїв у локальній мережі та блокувати звернення до відомих рекламних або трекерних доменів. Крім блокування реклами, такі рішення також підвищують швидкість завантаження сторінок, знижують споживання трафіку та забезпечують базовий рівень захисту від фішингових або шкідливих ресурсів.

Метою даної роботи є розробка, налаштування та тестування системи

фільтрації реклами на базі Raspberry Pi з використанням Pi-hole та AdGuard Home.

Об'єкт дослідження: процес фільтрації мережевого трафіку в локальних комп'ютерних мережах.

Предмет дослідження: розробка та аналіз функціонування пристрою для фільтрації трафіку локальної мережі на базі мікрокомп’ютера Raspberry Pi.

У першому розділі досліджено проблему нав’язливої інтернет-реклами, розглянуто історію розвитку засобів її блокування, наведено класифікацію фільтрів та висвітлено принципи роботи DNS-фільтрації. Здійснено аналіз програмного забезпечення, зокрема Pi-hole та AdGuard Home, з порівнянням їхньої ефективності.

Другий розділ присвячено технічній реалізації розроблюваної системи. Описано апаратну архітектуру на базі мікрокомп’ютера Raspberry Pi 4, конфігурацію мережевої інфраструктури, методи інтеграції з сервісами DHCP та DNS, а також розглянуто питання електроживлення, охолодження та забезпечення стабільності функціонування системи.

У третьому розділі детально описано процес інсталяції та конфігурування програмних засобів Pi-hole та AdGuard Home. Розглянуто налаштування служби DNS, процедури моніторингу стану системи за допомогою веб-інтерфейсу, заходи для забезпечення безпеки пристрою та методи резервного копіювання конфігураційних даних.

Четвертий розділ представляє результати експериментального тестування розробленої системи фільтрації трафіку на різних клієнтських пристроях. Проведено аналіз журналів роботи та системного навантаження, здійснено оцінку продуктивності обробки DNS-запитів та виконано порівняльний аналіз функціональності й ефективності Pi-hole та AdGuard Home.

У роботі розглянуто методологію впровадження подібних рішень у домашньому та офісному середовищі, проведено аналіз продуктивності та зручності використання кожної з систем, а також сформульовано рекомендації для користувачів щодо вибору оптимального підходу.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА АНАЛІЗ СУЧАСНИХ ЗАСОБІВ БЛОКУВАННЯ РЕКЛАМИ

1.1. Проблематика інтернет-реклами та її вплив на користувача

Інтернет-реклама є важливим елементом сучасної цифрової економіки, сприяючи розвитку онлайн-бізнесу, інтернет-магазинів, медіа-ресурсів та інших комерційних платформ. Вона займає значну частину бюджету маркетингових компаній, оскільки здатна ефективно донести повідомлення до великої аудиторії. Однак, незважаючи на свою популярність і переваги для бізнесу, інтернет-реклама викликає низку проблем та викликів для кінцевих користувачів.

Однією з основних проблем є надмірність реклами, що призводить до так званого рекламного перевантаження. Користувачі все частіше стикаються з великою кількістю банерів, спливаючих вікон, відео- та аудіореклами на веб-сторінках, що створює перешкоди при перегляді контенту. Така ситуація не лише відволікає від основної мети користувача в Інтернеті (читання новин, перегляд відео, пошук інформації), а й негативно впливає на досвід користування [1].

Однією з найбільших неприємностей для користувачів є реклама, що порушує конфіденційність. Багато рекламних платформ використовують методи збору даних, такі як куки, трекери, а також аналіз інтересів користувачів для того, щоб націлювати рекламу на певні категорії осіб. Це може викликати у користувачів відчуття вторгнення в особисте життя, оскільки вони не завжди поінформовані про методи збору своїх даних. За останні роки навіть почали виникати етичні питання щодо цієї практики, особливо в контексті GDPR та інших законодавчих ініціатив, спрямованих на захист приватності[2].

Агресивні рекламні технології, такі як автоматичне відтворення відеореклами або настирливі спливаючі вікна, додають додаткову напругу в

онлайн-досвід. Користувачі змушені витрачати час на закриття реклами або використання спеціальних плагінів для блокування рекламних елементів. Це спричиняє відчуття фрустрації та зниження задоволення від користування інтернет-ресурсами.

Додатково до цього, багато рекламних матеріалів несуть у собі шкідливі елементи, такі як фішинг або віруси. Оскільки рекламу можна вставляти у будь-який веб-контент без належного контролю з боку сайтів, користувач може легко натрапити на шахрайські ресурси, які видаються за звичайні рекламні оголошення.

Таким чином, інтернет-реклама, хоч і є важливим інструментом для бізнесу, має суттєвий негативний вплив на користувача. Порушення конфіденційності, агресивні рекламні технології та ризики безпеки – це основні фактори, що викликають стурбованість у користувачів Інтернету, призводячи до пошуку способів їх обмеження або блокування. У цьому контексті, створення ефективних інструментів фільтрації трафіку, таких як Pi-hole чи AdGuard, стає важливим для поліпшення користувацького досвіду в Інтернеті та забезпечення безпеки під час онлайн-активності.

1.2 Історія виникнення та еволюція технологій блокування реклами

Технології блокування реклами в Інтернеті пройшли значний шлях еволюції, що відображає зростаючу потребу користувачів у захисті від надмірної реклами, що заважає їхньому досвіду. Історія розвитку цих технологій тісно пов'язана з розвитком самого Інтернету та зростанням обсягів реклами, що погіршує взаємодію користувачів з веб-ресурсами.

Спочатку, на початку 1990-х років, блокування реклами було обмежене лише простими методами, такими як редагування локальних файлів hosts. Цей підхід дозволяв блокувати рекламні сервери, перенаправляючи їх на порожні або локальні адреси. Однак цей метод був надзвичайно трудомістким і вимагав постійних оновлень, оскільки список заблокованих серверів швидко змінювався.

Переломний момент настав у середині 2000-х років, коли з’явився перший серйозний плагін для браузера Mozilla Firefox — Adblock Plus. Цей інструмент став значним кроком уперед у боротьбі з рекламою, оскільки дозволяв користувачам автоматично блокувати небажану рекламу без необхідності вручну оновлювати списки заблокованих доменів. Він став популярним завдяки простоті використання, а також можливості фільтрувати не лише банери, але й текстову рекламу, що з'являлася на сторінках веб-сайтів [3].

Згодом, на початку 2010-х років, з'явилися нові розширення для блокування реклами, зокрема uBlock Origin, яке відзначалося більш ефективною фільтрацією та меншими витратами ресурсів. Він дозволив користувачам не лише блокувати рекламу, але й запобігати трекінгу в Інтернеті, що стало важливою складовою забезпечення приватності в мережі.

Водночас зростала популярність технологій блокування на рівні мережі, таких як Pi-hole. Цей інструмент дозволив блокувати рекламу на рівні DNS-запитів у межах локальної мережі, що дозволило користувачам застосовувати фільтрацію для всіх пристроїв, підключених до їхньої домашньої чи офісної мережі. Pi-hole став дуже популярним серед тих, хто шукав рішення для блокування реклами без залежності від браузерних розширень. Цей підхід дав користувачам змогу управляти рекламою на рівні всього інтернет-трафіку, що забезпечувало більш ефективне блокування, особливо для мобільних пристроїв і смарт-пристроїв.

Не залишалася осторонь і компанія AdGuard, що у 2018 році розробила свій продукт — AdGuard Home. Це рішення стало конкурентом Pi-hole, надаючи схожі функції блокування реклами, але з додатковими можливостями, такими як підтримка фільтрації на рівні HTTP-запитів та гнучке налаштування правил блокування. AdGuard Home став дуже популярним завдяки своєму зручному інтерфейсу та можливості додатково захищати користувачів за допомогою технологій, як DNS-over-HTTPS (DoH) і DNS-over-TLS (DoT), що забезпечують конфіденційність і безпеку при передачі даних.

Сучасні технології блокування реклами орієнтовані не лише на зниження

кількості нав'язливої реклами, а й на поліпшення безпеки користувачів, захищаючи їх від шкідливих доменів та трекерів. Блокувальники реклами сьогодні також забезпечують додаткові можливості для збереження конфіденційності, фільтруючи дані, що збираються трекерами, а також підтримують більш складні протоколи захисту, включаючи DNS-over-HTTPS і DNS-over-TLS.

Варто зазначити, що, разом із розвитком цих технологій, почала зростати і боротьба з використанням блокувальників реклами з боку веб-ресурсів. Деякі сайти почали обмежувати доступ до контенту для користувачів, що використовують такі інструменти, або ж просити їх відключити блокувальники реклами. Проте, зважаючи на постійну еволюцію інструментів блокування реклами та зростаючі потреби в конфіденційності, можна очікувати, що технології блокування будуть і далі вдосконалюватися та адаптуватися до нових вимог Інтернету.

Таким чином, історія виникнення та еволюції технологій блокування реклами є свідченням того, як зміни в Інтернет-середовищі та потреби користувачів призводять до розвитку нових рішень для забезпечення кращого користувацького досвіду та захисту їхньої приватності.

1.3. Класифікація та принципи роботи фільтрів реклами

Фільтри реклами — це програмні інструменти, що дозволяють користувачам блокувати або обмежувати показ реклами на веб-сторінках або в мобільних додатках. Вони зменшують кількість небажаних елементів, що з’являються під час перегляду контенту, а також можуть покращувати швидкість завантаження сайтів. Існують різні типи фільтрів, які відрізняються способом роботи та принципами фільтрації.

Один з найпоширеніших типів фільтрів — це DNS-фільтри, які працюють на рівні DNS-запитів. Коли користувач звертається до веб-ресурсу, фільтр перевіряє, чи є запит до рекламних серверів. Якщо такий запит виявляється, він

блокується або перенаправляється, не даючи рекламі потрапити на пристрій користувача. Зазвичай такі фільтри реалізуються через спеціалізовані сервери, такі як Pi-hole, що працюють на локальній мережі та блокують рекламу для всіх пристроїв у мережі [4].

Інші фільтри працюють на рівні HTTP або HTTPS-запитів. Вони аналізують трафік, що надсилається браузером до серверів, і блокують або змінюють відповіді, що містять рекламний контент. Цей тип фільтрації використовується в розширеннях браузерів, таких як uBlock Origin, які дозволяють блокувати рекламу безпосередньо в браузері, без необхідності втручання на рівні мережі.

Загалом, фільтри реклами можна також класифікувати за методами виявлення реклами. Один з таких методів — використання чорних списків, які містять URL-адреси або домени, що використовуються для розміщення реклами. Коли користувач здійснює запит до одного з таких доменів, фільтр блокує доступ до цього ресурсу. Однак цей метод не є ідеальним, оскільки рекламодавці постійно змінюють домени або використовують нові стратегії, щоб обійти блокування. Протилежний підхід — це використання білих списків, коли дозволяється показ реклами лише з певних перевірених ресурсів [5].

Інший тип фільтрації — динамічні фільтри, що здійснюють перевірку контенту веб-сторінки в реальному часі. Вони можуть блокувати рекламу за її специфічними характеристиками, наприклад, за елементами HTML-коду, такими як теги iframe, script або конкретні класи ідентифікаторів, що використовуються рекламними мережами [6].

Принцип роботи більшості фільтрів реклами базується на декількох основних технологіях. Одним із таких принципів є перехоплення запитів, що надсилаються браузером до сервера, та блокування рекламних ресурсів до того, як вони потраплять на екран користувача. Це може здійснюватися як на рівні DNS-серверів, так і за допомогою розширень браузерів або мережевих фільтрів. У випадку з DNS-фільтрами, наприклад, запити до рекламних доменів можуть бути перенаправлені або повністю заблоковані, що запобігає завантаженню

реклами на пристрої користувача [7].

Іншою поширеною технологією є аналіз HTML-коду та DOM-структури веб-сторінок. Фільтри аналізують сторінку на наявність елементів, які відповідають характеристикам реклами, наприклад, визначені рекламні класи, теги чи інші специфічні елементи, які часто використовуються рекламними системами для вставлення оголошень на сайті.

Також важливим елементом є фільтрація на основі списків. У цьому випадку чорні списки містять URL-адреси рекламних ресурсів, до яких забороняється доступ. Білий список, навпаки, дозволяє певним ресурсам відображатися без блокування реклами.

Окрім цього, нові технології фільтрації реклами аналізують трафік у реальному часі, виявляючи нові види реклами, такі як спливаючі вікна або динамічно завантажувані елементи. Це дозволяє швидко реагувати на появу нових форматів реклами і блокувати їх ще до того, як вони потраплять до користувача [8].

Фільтрація реклами має свої переваги та обмеження. З одного боку, вона дозволяє значно покращити досвід користувача, зменшуючи кількість непотрібних відволікань і збільшуючи швидкість завантаження веб-сторінок. З іншого боку, це може призвести до блокування деяких корисних елементів, наприклад, аналітичних скриптів або необхідних для функціонування сайту компонентів. Окрім того, реклама постійно змінюється, і нові методи її подачі часто обходять існуючі фільтри.

1.4. DNS-фільтрація як засіб блокування: переваги та недоліки

DNS-фільтрація є ефективним методом блокування небажаного контенту, зокрема реклами та шкідливих веб-ресурсів, шляхом управління запитами до системи доменних імен. Цей метод дозволяє заблокувати доступ до певних доменів ще до того, як буде здійснено з'єднання з конкретними серверами, на яких розміщено контент. Таким чином, замість того, щоб браузер звертався до

реального IP-адресу рекламного ресурсу, система перенаправляє запит на інший адрес, що блокує доступ до небажаного ресурсу або повідомляє про помилку.

Переваги DNS-фільтрації очевидні. Однією з основних є централізоване керування, що дозволяє зручно налаштувати фільтрацію для всіх пристроїв у мережі. Це особливо корисно в домашніх мережах або в малих офісах, де необхідно заблокувати рекламу або шкідливі сайти без необхідності налаштовувати кожен пристрій окремо. Крім того, налаштування DNS-фільтрації зазвичай є простим і доступним навіть для користувачів без технічних знань, що робить цей метод привабливим для широкого кола користувачів. Оскільки фільтрація здійснюється на рівні DNS, цей процес не потребує великих обчислювальних ресурсів, що дозволяє забезпечити високу швидкість роботи мережі [9].

Іншим важливим аспектом є те, що DNS-фільтрація може підвищити рівень безпеки користувачів, блокуючи доступ до шкідливих ресурсів, таких як фішингові сайти або веб-сторінки, що містять віруси чи інші небезпечні елементи. Вона також зменшує загальний обсяг трафіку в мережі, оскільки реклама та непотрібні ресурси блокуються на рівні DNS, не завантажуючи додатково непотрібні елементи на пристрої користувача.

Однак цей метод має і свої недоліки. Одним з головних є обмежена точність. DNS-фільтрація зазвичай блокує домени в цілому, але не завжди здатна точково визначити, які елементи веб-сторінки потрібно заблокувати, а які — залишити доступними. Це означає, що рекламні блоки можуть все ж з'являтися на сторінках, а інші непотрібні елементи можуть не блокуватися. Крім того, для ефективної роботи DNS-фільтрації необхідно регулярно оновлювати чорні списки доменів, оскільки рекламодавці можуть змінювати свої адреси або використовувати нові методи обходу блокувань [10].

Ще одним недоліком є ймовірність помилкових блокувань. Через використання чорних списків доменів, іноді може бути заблоковано не тільки рекламу, але й корисні ресурси, які використовують схожі доменні імена або технології. Це може призвести до того, що певні сайти або сервіси стануть

недоступними без необхідності. Також важливо зазначити, що користувачі можуть обійти фільтрацію, змінивши налаштування DNS-серверів на власні або використовувати сторонні сервіси, які не блокують рекламу [11].

У кінцевому підсумку, DNS-фільтрація є простим і ефективним способом для блокування реклами та шкідливих веб-сайтів на рівні мережі, проте для досягнення більш точної фільтрації можуть знадобитися додаткові інструменти, такі як програмне забезпечення для фільтрації HTTP-запитів чи розширення браузерів.

1.5. Огляд популярного ПЗ: Pi-hole, AdGuard Home та інші альтернативи

На ринку існує кілька популярних програмних рішень для DNS-фільтрації, які дозволяють блокувати рекламу та інші небажані ресурси. Одними з найпоширеніших є Pi-hole та AdGuard Home. Вони обидва функціонують на принципі DNS-фільтрації і є зручними інструментами для користувачів, які хочуть налаштувати блокування реклами в своїх мережах.

Pi-hole — це відкритий проект, який став дуже популярним серед користувачів, що шукають просте та ефективне рішення для блокування реклами на рівні DNS. Pi-hole працює як локальний DNS-сервер, який перехоплює запити на рекламу та шкідливі сайти, замінюючи їх на порожню сторінку або повідомлення про помилку. Користувач може налаштувати Pi-hole на Raspberry Pi, що робить його доступним і зручним для домашніх мереж. Крім того, Pi-hole підтримує можливість додавання користувацьких чорних списків доменів, що дозволяє гнучко налаштовувати систему фільтрації[12].

Перевагою Pi-hole є простота налаштування та великий вибір чорних списків доменів, які регулярно оновлюються. Однак варто зазначити, що хоча Pi-hole відмінно блокує рекламу на рівні DNS, він не завжди здатний фільтрувати контент, який обходить блокування через динамічні або нестандартні запити. Це може вимагати додаткового використання інструментів, таких як фільтри на

рівні HTTP.

AdGuard Home є ще одним популярним рішенням для DNS-фільтрації, яке працює подібно до Pi-hole. Однак AdGuard Home пропонує додаткові функції, такі як розширене налаштування фільтрації на рівні DNS та підтримку більшої кількості чорних списків. AdGuard Home підтримує інтеграцію з іншими продуктами AdGuard, що дозволяє користувачам більш точно налаштувати блокування реклами та трекерів. Крім того, AdGuard Home має зручний веб-інтерфейс для налаштувань та моніторингу, що робить його ще більш доступним для користувачів[13].

Ще однією перевагою AdGuard Home є наявність підтримки блокування реклами на мобільних пристроях через використання DNS-серверів AdGuard, що робить його універсальним інструментом для фільтрації на різних пристроях.

З іншими альтернативами можна згадати такі варіанти, як NextDNS та DNS-over-HTTPS (DoH) рішення, які також дозволяють фільтрувати небажану рекламу та забезпечити більшу конфіденційність в Інтернеті.

NextDNS є хмарним рішенням для блокування реклами, фішингу та шкідливих сайтів. Відмінною особливістю цього сервісу є можливість налаштування DNS-фільтрації з детальними опціями, включаючи блокування певних категорій контенту (наприклад, соціальних мереж або азартних ігор), що робить його зручним для використання в родинах або компаніях. Крім того, NextDNS підтримує налаштування на рівні користувача, що дозволяє уникати помилкових блокувань, і забезпечує інтеграцію з іншими інструментами безпеки.

DNS-over-HTTPS (DoH) є ще одним популярним рішенням для тих, хто хоче додати додатковий рівень безпеки і конфіденційності. Відмінність від традиційної DNS-фільтрації полягає в тому, що DoH забезпечує шифрування DNS-запитів, що ускладнює можливість перехоплення або маніпуляції з даними. Це робить DoH ідеальним для користувачів, які турбуються про свою конфіденційність і безпеку в Інтернеті. Однак DoH також має деякі обмеження у фільтрації контенту на рівні доменів, що може бути важливим аспектом при

виборі рішення для блокування реклами[14].

Усі перераховані рішення мають свої переваги та недоліки. Pi-hole та AdGuard Home є чудовими варіантами для тих, хто хоче налаштувати локальний сервер для фільтрації реклами та шкідливих сайтів на своїй мережі. Вони прості у використанні та ефективні для блокування реклами на рівні DNS. AdGuard Home пропонує додаткові можливості налаштування, в той час як Pi-hole є популярним завдяки своїй відкритій природі та великий спільноті користувачів. NextDNS є хорошим вибором для користувачів, які шукають хмарне рішення з високим рівнем налаштувань і конфіденційності. DNS-over-HTTPS забезпечує додатковий рівень безпеки, але може бути менш ефективним у блокуванні реклами.

Вибір між цими інструментами залежить від потреб користувача та його технічних вимог, але всі вони є потужними інструментами для забезпечення безпеки та комфорту в Інтернеті.

1.6. Порівняння функціональності та ефективності різних рішень

Порівняння функціональності та ефективності різних рішень для фільтрації реклами на основі DNS, таких як Pi-hole, AdGuard Home, NextDNS та DNS-over-HTTPS, дозволяє користувачам вибрати найкращий інструмент відповідно до своїх потреб. Кожне з цих рішень має свої особливості, переваги та недоліки, що впливають на його ефективність і функціональність у різних умовах [15].

1. Pi-hole

Функціональність:

Pi-hole є рішенням з відкритим кодом, яке функціонує як локальний DNS-сервер для блокування реклами та шкідливих сайтів. Всі запити до доменів перевіряються через Pi-hole, і якщо вони знаходяться в чорному списку, запит перенаправляється на порожню сторінку або на адресу, що повідомляє про блокування.

Переваги:

— Простота налаштування і використання.

— Відкрите програмне забезпечення з великим ком'юніті.

— Можливість додавання власних чорних списків для персоналізованої фільтрації.

— Підтримка багатьох типів пристроїв, що підключаються до мережі, без необхідності налаштовувати кожен окремо.

— Локальне управління без потреби в хмарних сервісах.

Недоліки:

— Не завжди ефективно блокує динамічні або нестандартні рекламні запити.

— Для досягнення високої точності блокування може знадобитися додаткове налаштування.

— Вимагає регулярного оновлення чорних списків.

Ефективність:

Pi-hole ефективно блокує більшість типів реклами на рівні DNS, але має обмеження в точності, оскільки не фільтрує контент на рівні веб-сторінок. Це може призвести до того, що деякі рекламні оголошення все ж будуть відображатися.

2. AdGuard Home

Функціональність:

AdGuard Home працює аналогічно до Pi-hole, але з розширеними можливостями фільтрації. Крім базового блокування реклами на рівні DNS, він дозволяє здійснювати більш гнучке управління запитами, зокрема блокувати рекламу, трекери та інші небажані ресурси.

Переваги:

— Підтримка додаткових чорних списків.

— Кращий інтерфейс для налаштування та моніторингу порівняно з Pi-hole.

— Можливість налаштувати фільтрацію на рівні пристроїв.

— Легко інтегрується з іншими продуктами AdGuard, що дозволяє створити комплексне рішення для блокування реклами та шкідливих сайтів.

Недоліки:

— Вищі вимоги до системних ресурсів, ніж у Pi-hole.

— Комерційна версія пропонує більше можливостей, ніж безкоштовна.

Ефективність:

AdGuard Home має високу ефективність у блокуванні реклами, трекерів і шкідливих доменів. Його фільтрація більш точна, ніж у Pi-hole, завдяки розширеній настройці фільтрів та додатковим можливостям керування.

3. NextDNS

Функціональність:

NextDNS є хмарним рішенням для фільтрації реклами та захисту від шкідливих ресурсів. Він підтримує персоналізовану фільтрацію, пропонуючи користувачам великий вибір чорних списків та можливість налаштовувати фільтрацію за категоріями контенту, такими як реклама, фішинг, шкідливі програми тощо [16].

Переваги:

— Хмарне рішення з доступом до налаштувань через веб-інтерфейс.

— Можливість налаштувати фільтрацію для різних пристроїв та категорій контенту.

— Забезпечує високий рівень конфіденційності завдяки шифруванню запитів.

— Підтримка інтеграції з іншими інструментами для безпеки.

Недоліки:

— Залежність від хмарного сервісу, що може викликати питання щодо конфіденційності.

— Платні функції для більш детальної фільтрації.

— Може бути менш гнучким у порівнянні з локальними рішеннями.

Ефективність:

NextDNS є дуже ефективним, оскільки працює в хмарі та має доступ до більш актуальних чорних списків та можливість більш точного налаштування.

Важливою перевагою є блокування реклами та шкідливих сайтів на рівні DNS з дуже високою точністю.

4. DNS-over-HTTPS (DoH)

Функціональність:

DNS-over-HTTPS є протоколом, що забезпечує шифрування DNS-запитів через HTTPS-з'єднання. Це дозволяє захистити конфіденційність користувачів, оскільки дані DNS-запитів передаються через захищене з'єднання.

Переваги:

— Підвищує конфіденційність та безпеку користувачів.

— Блокує рекламу через хмарні DNS-сервери з підтримкою DoH.

— Забезпечує кращу захищеність від атак, які націлені на маніпуляцію з DNS-запитами.

Недоліки:

— Може бути менш ефективним у фільтрації реклами на рівні конкретних доменів, оскільки фільтрація здійснюється лише на рівні DNS-запитів.

— Не завжди підтримується всіма пристроями або програмами.

DNS-over-HTTPS ефективно покращує безпеку та конфіденційність, але не забезпечує такої ж високої точності у блокуванні реклами, як Pi-hole або AdGuard Home. Основна його перевага полягає в шифруванні та захисті від потенційних атак, що маніпулюють DNS-запитами.

Pi-hole та AdGuard Home є чудовими рішеннями для локальної DNS-фільтрації, причому AdGuard Home пропонує більше функцій та зручніший інтерфейс для користувачів. NextDNS є кращим вибором для тих, хто хоче хмарне рішення з високим рівнем конфіденційності та додатковими можливостями налаштування. DNS-over-HTTPS, у свою чергу, є найкращим варіантом для забезпечення безпеки та конфіденційності, хоча його ефективність у блокуванні реклами дещо обмежена в порівнянні з іншими інструментами. Вибір залежить від вимог користувача щодо рівня контролю, безпеки та зручності налаштувань [17].

РОЗДІЛ 2. АРХІТЕКТУРА ТА СКЛАДОВІ СИСТЕМИ НА ОСНОВІ RASPBERRY PI 4

2.1. Вибір апаратного забезпечення: огляд Raspberry Pi 4 та його можливостей

Raspberry Pi 4 є четвертим поколінням популярного мікрокомп'ютера, що широко використовується як у навчальних, так і в професійних цілях. Його універсальність, компактність та доступна ціна роблять його ідеальним вибором для реалізації проєктів з мережевої фільтрації, зокрема для створення пристрою блокування реклами на рівні локальної мережі. У даному розділі розглянемо основні технічні характеристики Raspberry Pi 4, а також проаналізуємо його можливості для реалізації завдань фільтрації інтернет-трафіку [19].

Raspberry Pi 4 випускається в кількох модифікаціях, що відрізняються обсягом оперативної пам'яті (2 ГБ, 4 ГБ, 8 ГБ LPDDR4), що дозволяє обрати конфігурацію відповідно до потреб конкретного проєкту. Центральним процесором є чотириядерний ARM Cortex-A72 з тактовою частотою 1.5 ГГц, що забезпечує достатню обчислювальну потужність для виконання завдань з аналізу та обробки DNS-запитів у режимі реального часу[20].

Однією з ключових переваг Raspberry Pi 4 є наявність двох портів USB 3.0, які забезпечують високу швидкість передачі даних, а також двох портів USB 2.0 для підключення периферійних пристроїв. Для підключення до мережі використовується гігабітний Ethernet-інтерфейс, що є критично важливим для проєктів, пов'язаних з маршрутизацією та фільтрацією трафіку. Також можливе підключення через Wi-Fi (802.11ac), що забезпечує гнучкість у виборі способу інтеграції пристрою в домашню або корпоративну мережу.

Raspberry Pi 4 підтримує запуск повноцінної операційної системи Linux, такої як Raspberry Pi OS, Ubuntu Server, DietPi або інші дистрибутиви, оптимізовані для ARM-архітектури. Це дозволяє встановлювати й налаштовувати різноманітне програмне забезпечення, включаючи DNS-фільтри на кшталт Pi-hole, AdGuard Home та інші[21] .

Окрім високої продуктивності, важливою перевагою Raspberry Pi 4 є його низьке енергоспоживання. Завдяки цьому пристрій може працювати безперервно упродовж тривалого часу, не вимагаючи активного охолодження, хоча за бажанням можливе підключення вентиляторів або пасивних радіаторів для покращення тепловідведення.

Таким чином, Raspberry Pi 4 є ідеальною платформою для побудови пристрою фільтрації інтернет-трафіку. Його апаратні можливості дозволяють забезпечити стабільну та ефективну роботу навіть за умов одночасної обробки запитів з великої кількості пристроїв у мережі. Комбінація гнучкості, відкритості та підтримки з боку спільноти робить цей мікрокомп’ютер одним із найкращих виборів для реалізації сучасних мережевих рішень на локальному рівні.

2.2. Блок-схема системи фільтрації реклами в локальній мережі

У межах локальної мережі фільтрація рекламного трафіку відбувається за рахунок централізованої обробки DNS-запитів, яку здійснює окремий пристрій – мікрокомп’ютер Raspberry Pi 4. Усі пристрої, підключені до домашнього або офісного роутера (наприклад, ноутбуки, смартфони, телевізори), під час спроби відкрити вебсайт надсилають запити на розв’язання доменного імені. Замість того, щоб ці запити напряму передавались на публічні DNS-сервери, вони перенаправляються до Raspberry Pi, який виконує роль локального DNS-релея з увімкненим фільтруванням.

Усередині Raspberry Pi працює спеціальне програмне забезпечення, наприклад Pi-hole або AdGuard Home, що містить перелік доменів, які асоціюються з рекламою, трекерами або шкідливим ПЗ. Коли DNS-запит

надходить на пристрій, він аналізується: якщо домен виявляється у чорному списку, пристрій або повертає некоректну (порожню) IP-адресу, або блокує запит повністю. Якщо ж домен не входить до списку блокування, запит перенаправляється до зовнішнього DNS-сервера, наприклад Google (8.8.8.8), і результат повертається клієнтському пристрою [22].

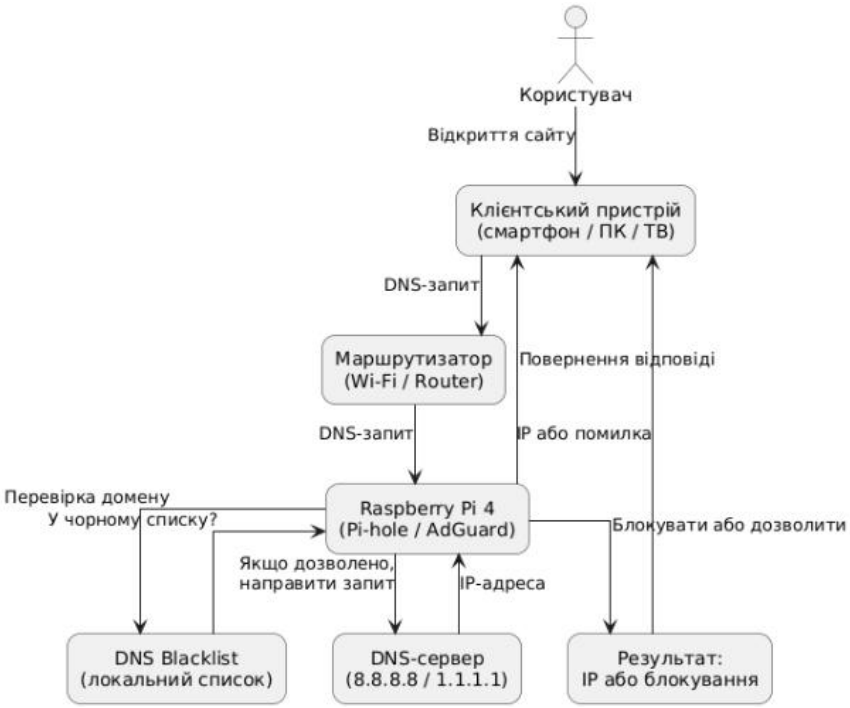

Рис.2.1 – Блок-схема системи фільтрації реклами

Таким чином, Raspberry Pi 4 стає фільтруючим вузлом між локальною мережею користувача та інтернетом, дозволяючи ефективно обмежувати показ реклами без необхідності інсталяції додаткових розширень чи програм на кожному пристрої.

2.3. Мережеві інтерфейси, DHCP, DNS та роль Raspberry Pi

У контексті побудови системи фільтрації рекламного трафіку в локальній мережі надзвичайно важливою є правильна організація мережевої взаємодії. Ключовими елементами такої взаємодії є мережеві інтерфейси, служби DHCP та DNS, а також розподіл ролей між пристроями в мережі, серед яких центральну функцію виконує Raspberry Pi.

Raspberry Pi 4 має два основні мережеві інтерфейси: Ethernet (дротовий) та Wi-Fi (бездротовий). Це дозволяє гнучко налаштовувати його для роботи як з кабельною, так і з бездротовою інфраструктурою. У проєкті фільтрації реклами доцільно використовувати Ethernet-з'єднання задля забезпечення стабільного каналу обміну даними та мінімізації затримок. Raspberry Pi виступає як вузол, який приймає DNS-запити від усіх пристроїв у локальній мережі, фільтрує їх і, за потреби, перенаправляє на зовнішні DNS-сервери [23].

DHCP (протокол динамічної конфігурації хостів) відповідає за автоматичну видачу IP-адрес, маски підмережі, шлюзів та DNS-серверів кожному пристрою, який під’єднується до мережі. У типовій домашній мережі роль DHCP-сервера виконує роутер. Для реалізації системи фільтрації необхідно вказати в налаштуваннях DHCP, що DNS-запити мають перенаправлятися не на стандартний DNS-сервер провайдера, а на IP-адресу Raspberry Pi. Таким чином, приєднані до мережі пристрої автоматично отримують адресу Pi як єдину точку для обробки DNS-запитів[24].

DNS (система доменних імен) перетворює зручні для людини доменні імена (наприклад, example.com) на IP-адреси, необхідні для встановлення з'єднання між пристроями. Саме на цьому етапі і відбувається фільтрація: програмне забезпечення, встановлене на Raspberry Pi (таке як Pi-hole або AdGuard Home), перевіряє кожен DNS-запит за попередньо визначеним списком заблокованих доменів. Якщо домен є рекламним або небажаним, пристрій не повертає реальну IP-адресу, а надає порожню відповідь або вказує на локальний інтерфейс.

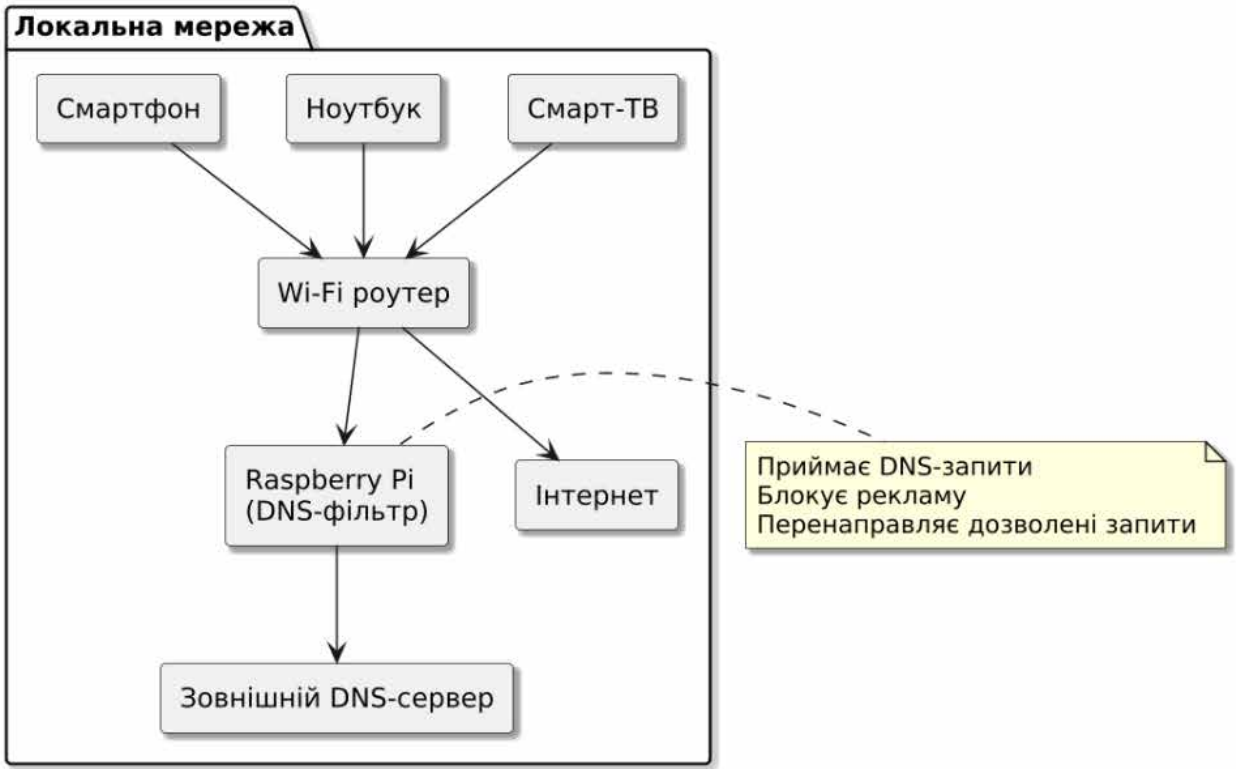

Рис.2.2 – Схема мережевої взаємодії з Raspberry Pi

Таким чином, Raspberry Pi виконує роль фільтруючого DNS-сервера, який стоїть між клієнтами в локальній мережі та глобальними DNS-ресурсами інтернету. Його правильна інтеграція у мережеву інфраструктуру дозволяє ефективно централізувати блокування реклами без втручання в конфігурацію кожного окремого пристрою. Це робить рішення зручним у використанні, масштабованим та незалежним від конкретного програмного або апаратного забезпечення клієнтів.

2.4. Інтеграція в існуючу домашню/офісну інфраструктуру

Ефективна реалізація системи фільтрації реклами потребує не лише встановлення програмного забезпечення на Raspberry Pi, але й його правильного інтегрування у вже наявну мережеву інфраструктуру. Однією з ключових переваг Raspberry Pi є його компактність, енергоефективність та підтримка широкого спектру мережевих інтерфейсів, що дозволяє без особливих труднощів адаптувати пристрій під домашні або офісні умови.

Для більшості користувачів інтеграція починається з підключення Raspberry Pi до локальної мережі — переважно за допомогою Ethernet-з'єднання, що забезпечує стабільність та надійність з'єднання. Після підключення важливо призначити Pi статичну IP-адресу, яка не буде змінюватися після кожного перезавантаження. Це необхідно для забезпечення постійного доступу до пристрою як з боку користувача (для адміністрування), так і з боку інших пристроїв у мережі (для DNS-запитів)[25].

Наступним етапом є налаштування маршрутизатора, який у більшості випадків виконує функцію DHCP-сервера. У його конфігурації необхідно вказати IP-адресу Raspberry Pi як основний (або єдиний) DNS-сервер. Це дозволить автоматично скеровувати всі DNS-запити, що надходять від клієнтів мережі, на Raspberry Pi, де відбуватиметься їх фільтрація.

У більш складних офісних середовищах, де мережа поділена на підмережі, використовуються VLAN або є централізоване управління мережею, інтеграція може включати додаткові кроки. Наприклад, адміністратор може змінити параметри DHCP на центральному сервері або мережевому комутаторі, щоб забезпечити перенаправлення DNS-запитів на Raspberry Pi. У разі, якщо мережа вже використовує власний DNS-сервер (наприклад, Windows Server з роллю DNS), Raspberry Pi можна налаштувати як проміжну ланку — DNS-форвардер, що дозволить не змінювати існуючу архітектуру, але додати до неї функціональність блокування реклами [26].

Крім того, у домашніх умовах можлива ручна конфігурація окремих пристроїв, таких як Smart TV або IoT-девайси, які не підтримують автоматичне налаштування DNS через DHCP. У цьому випадку для кожного з них вказується IP-адреса Raspberry Pi вручну у відповідному меню налаштувань мережі.

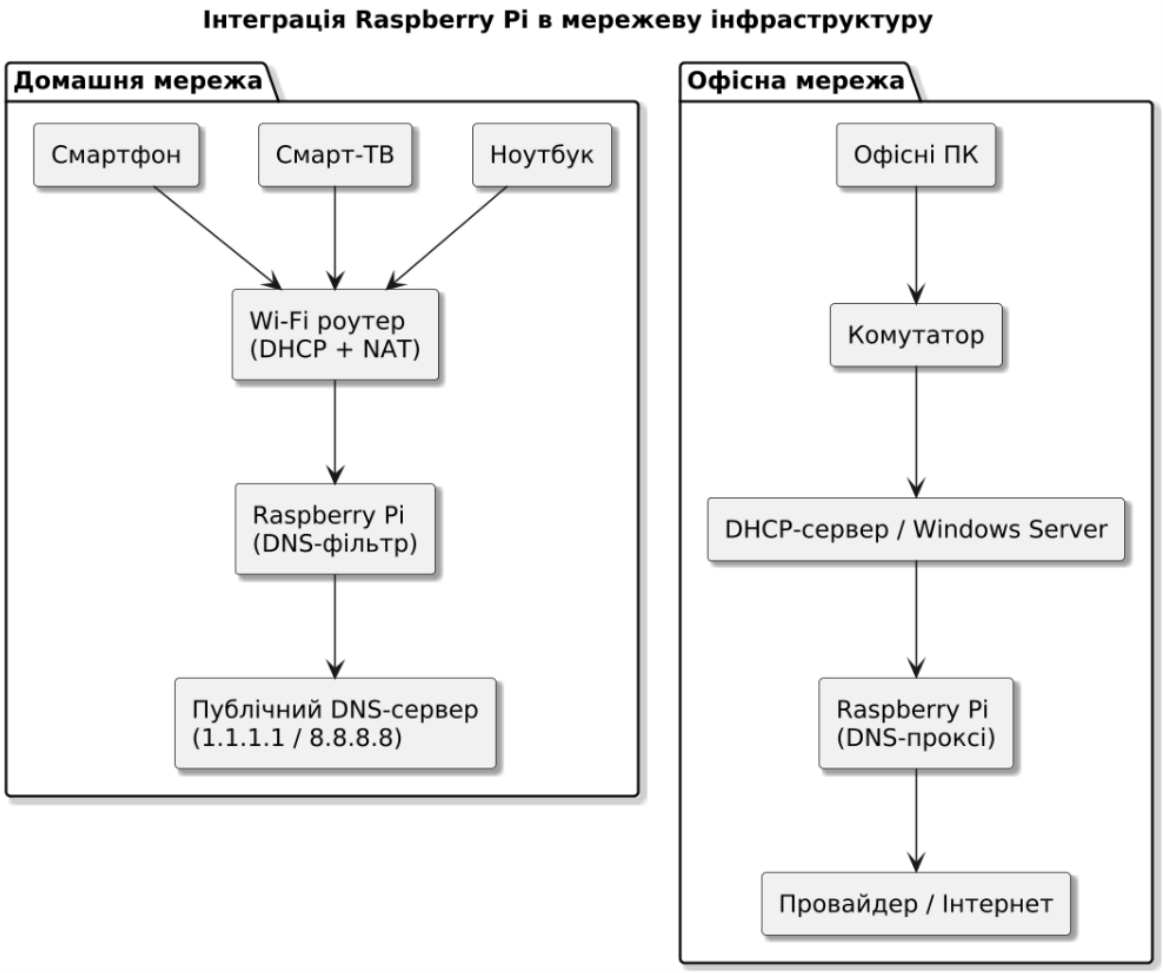

Рис.2.3 – Схема інтеграції в домашню та офісну інфраструктуру

Таким чином, незалежно від складності існуючої інфраструктури, інтеграція Raspberry Pi як фільтрувального пристрою є відносно простою та не потребує радикальної перебудови мережі. Вона дозволяє централізовано контролювати мережевий трафік, зменшувати обсяг рекламного контенту, покращувати безпеку, продуктивність і комфорт користувачів.

2.5. Додаткове обладнання (роутер, комутатор, накопичувачі тощо)

Для повноцінної реалізації системи фільтрації трафіку на базі Raspberry Pi 4 у домашньому чи офісному середовищі може знадобитися додаткове обладнання, яке забезпечить стабільну роботу мережі, підвищену надійність та розширену функціональність.

Насамперед, ключовим компонентом є роутер. Він виконує функції маршрутизації, NAT, а в більшості випадків також DHCP-сервера та DNS-проксі. У типовій домашній мережі саме роутер роздає IP-адреси пристроям і визначає, куди скеровувати DNS-запити. Для інтеграції Raspberry Pi як фільтра DNS важливо, щоб роутер дозволяв змінювати DNS-сервер у DHCP-настройках. Більшість сучасних моделей підтримують таку можливість, однак деякі провайдерські роутери можуть мати обмеження, які унеможливлюють подібну зміну без перепрошивки або зміни обладнання[27].

У більш складних мережах — особливо офісних — мережеві комутатори (світчі) виконують важливу роль у розподілі трафіку між пристроями. У таких умовах бажано використовувати керовані (managed) комутатори, які дозволяють задавати VLAN, пріоритет трафіку (QoS) та створювати дзеркалювання портів для подальшого моніторингу. Пристрої, як-от Raspberry Pi, можуть бути підключені до окремого VLAN, що дозволяє ізолювати DNS-фільтр від основного трафіку у разі потреби.

Ще одним компонентом, який варто врахувати, є накопичувачі. Хоча Raspberry Pi 4 має підтримку карти microSD для основної файлової системи, у деяких випадках бажано використовувати зовнішні USB-накопичувачі для зберігання журналів, резервних копій, або для роботи з кешем DNS, якщо програмне забезпечення фільтрації його підтримує. USB 3.0 порти Raspberry Pi дозволяють підключати швидкі SSD-накопичувачі, що значно покращує швидкодію системи у порівнянні з microSD.

Також до додаткового обладнання можна віднести мережеві адаптери — наприклад, USB-to-Ethernet, які використовуються у випадках, коли необхідно мати два незалежні дротові інтерфейси. Це може бути корисним при побудові більш складних схем маршрутизації або створенні окремого контрольованого сегмента мережі.

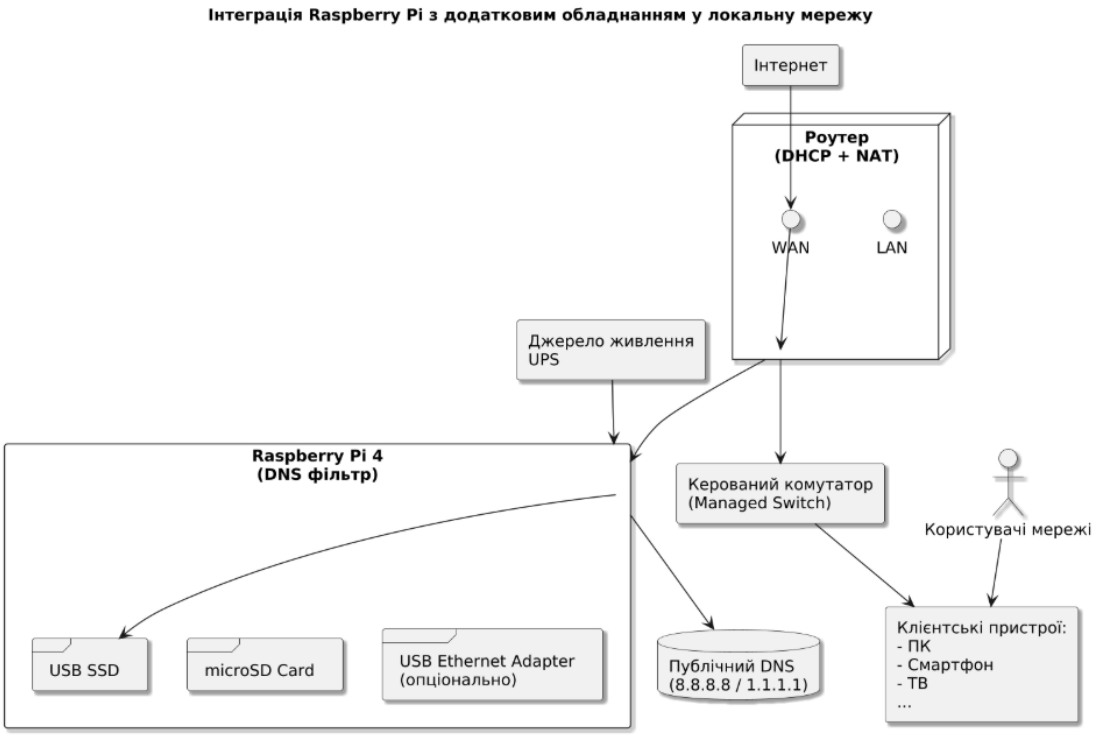

Рис 2.4 – Схема з додатковим обладнанням

Не менш важливими є і джерела безперебійного живлення (UPS), особливо в офісному середовищі. Raspberry Pi хоч і має невелике енергоспоживання, однак перебої з живленням можуть призвести до втрати конфігураційних файлів або пошкодження системи. Невеликий UPS здатен забезпечити достатній рівень захисту для безперервної роботи DNS-фільтра[28].

Таким чином, хоча базова система фільтрації може функціонувати з мінімумом апаратного забезпечення, наявність додаткових пристроїв дозволяє розширити її функціональність, підвищити надійність та адаптувати рішення до потреб конкретної інфраструктури.

2.6. Безперебійна робота: стабільність, охолодження та живлення

Однією з важливих умов ефективної роботи системи фільтрації інтернет-трафіку є її здатність функціонувати у безперервному режимі. Оскільки пристрій на базі Raspberry Pi 4 виконує роль проміжного ланцюга між клієнтами в мережі та DNS-інфраструктурою глобального інтернету, будь-який збій або

відключення цього вузла призводить до порушення доступу до вебресурсів у всій локальній мережі. Саме тому питання безперебійної роботи, стабільного живлення та ефективного охолодження є критично важливими.

Raspberry Pi 4, хоч і є енергоефективним пристроєм, при тривалому навантаженні, особливо в умовах активної обробки DNS-запитів, генерації логів або при підключенні зовнішніх накопичувачів, здатен значно нагріватися. Висока температура процесора негативно впливає на продуктивність пристрою через механізм автоматичного зниження частоти (throttling), а в деяких випадках може навіть призвести до його нестабільної роботи. Для уникнення подібних ситуацій доцільно забезпечити охолодження пристрою — зокрема, встановлення радіаторів на основні чіпи, активного вентилятора або використання спеціалізованого корпусу з пасивним або комбінованим охолодженням. Ефективне відведення тепла дозволяє пристрою працювати стабільно навіть у пікові години навантаження [29].

Живлення Raspberry Pi також відіграє важливу роль у забезпеченні безперервності його роботи. Стандартний адаптер живлення повинен видавати стабільні 5.1 В при струмі не менше 3 А. Недостатнє або нестабільне живлення часто є причиною неочевидних збоїв — зависань, перезавантажень, втрати підключення зовнішніх пристроїв, а також пошкодження файлової системи. Особливо критичним є використання якісного джерела живлення, якщо до Raspberry Pi підключені USB SSD-диски або інші споживачі енергії. Для офісного середовища або місць із нестабільною напругою доцільно використовувати компактне джерело безперебійного живлення (UPS), яке забезпечить живлення пристрою хоча б протягом кількох хвилин у разі зникнення електроенергії. Це дозволить коректно завершити роботу або зберегти логи без ризику пошкодження [30].

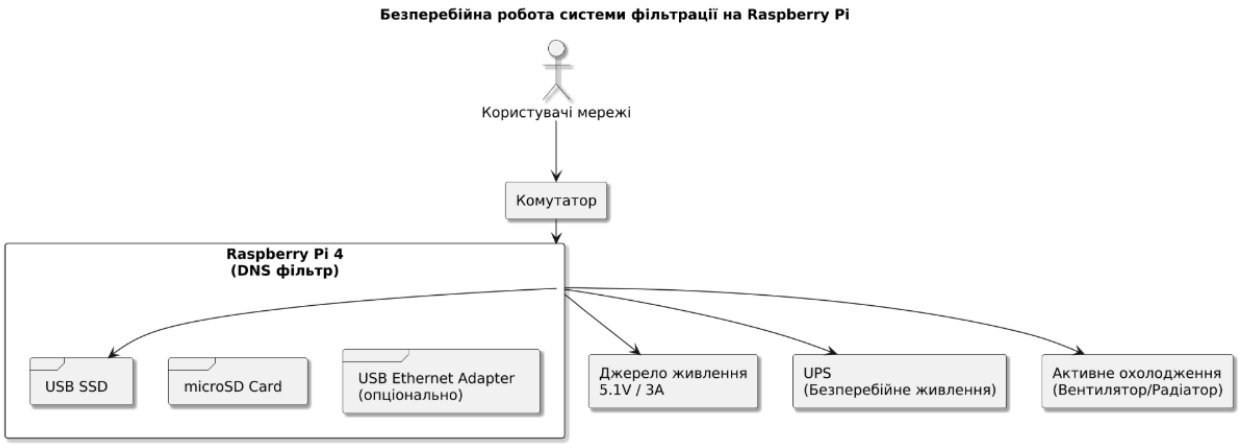

Рис. 2.5 – Схема стабільної роботи Raspberry Pi

Окрім фізичних чинників, важливу роль у стабільності системи відіграє програмне середовище. Рекомендується використовувати стабільні дистрибутиви операційної системи, регулярно оновлювати Pi-hole або AdGuard Home, а також слідкувати за наявністю вільного місця на накопичувачі. Додатково можна налаштувати автоматичне перезавантаження пристрою раз на тиждень у нічний час або використовувати моніторингові скрипти, які перевіряють наявність доступу до DNS-серверів і у разі помилки перезапускають відповідні служби.

У підсумку, досягнення стабільної та безперебійної роботи фільтраційного пристрою на базі Raspberry Pi 4 потребує комплексного підходу: правильного вибору джерела живлення, організації ефективного охолодження, встановлення резервного живлення, а також підтримання актуальності програмного забезпечення. Тільки в такому випадку можна забезпечити надійний рівень фільтрації трафіку без перебоїв у доступі до мережевих ресурсів.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ФІЛЬТРАЦІЇ РЕКЛАМИ

3.1. Підготовка Raspberry Pi: встановлення Raspberry Pi OS

Перед тим, як перейти до налаштування пристрою для фільтрації трафіку, першочерговим завданням є підготовка апаратного забезпечення. Raspberry Pi є популярною платформою для розробки різноманітних проектів, у тому числі й для створення систем фільтрації реклами. Для налаштування пристрою в якості фільтра DNS трафіку необхідно встановити на нього операційну систему, що оптимізована для цієї платформи.

Для виконання завдань, пов'язаних з фільтрацією реклами, найкраще використовувати операційну систему Raspberry Pi OS (раніше відома як Raspbian), оскільки вона є офіційною ОС для цієї платформи і має найкращу сумісність з усіма апаратними та програмними компонентами Raspberry Pi. Raspberry Pi OS надає повний набір інструментів для налаштування і керування пристроєм, що робить її зручним вибором для розробників[31].

Для роботи Raspberry Pi необхідно використовувати microSD карту як основний носій для операційної системи. Рекомендується використовувати карту з мінімальним об'ємом 8 ГБ, але для кращої продуктивності варто вибирати карти класу UHS-1 або вище. Чим швидша карта пам'яті, тим стабільніше працюватиме система, особливо якщо вона виконує ресурсоємні задачі, як обробка DNS запитів.

Після підготовки microSD карти потрібно завантажити останню версію Raspberry Pi OS з офіційного сайту Raspberry Pi. Для цього можна скористатися програмою Raspberry Pi Imager, яка дозволяє легко вибрати потрібну операційну систему і записати її на карту пам'яті. Raspberry Pi Imager підтримує кілька

варіантів ОС, серед яких можна вибрати Raspberry Pi OS with Desktop або безголовну версію Raspberry Pi OS Lite, якщо планується працювати без графічного інтерфейсу.

Процес запису операційної системи на карту пам'яті займає кілька хвилин і включає в себе вибір правильного образу ОС та вказівку пристрою, на який потрібно записати систему.

Після запису Raspberry Pi OS на карту пам'яті, її потрібно вставити в Raspberry Pi та підключити до монітора, клавіатури та миші. При першому запуску Raspberry Pi завантажить операційну систему, після чого на екрані з'явиться майстер налаштувань. У цьому майстрі користувач може вказати мову, регіональні налаштування, змінити пароль за замовчуванням та підключити Raspberry Pi до бездротової мережі Wi-Fi, якщо вона буде використовуватися [32].

Одним із важливих кроків після першого запуску є оновлення системи. Для цього потрібно використати команду:

sudo apt update && sudo apt upgrade

Це дозволить переконатися, що система має останні оновлення безпеки та програмного забезпечення.

Після оновлення операційної системи варто встановити деякі додаткові пакети для роботи з мережею та DNS-запитами. Це можна зробити за допомогою стандартного менеджера пакетів apt. Зокрема, можуть бути корисними інструменти, такі як dnsutils, curl та wget. Для цього виконується команда:

sudo apt install dnsutils curl wget

Ці інструменти знадобляться для налаштування DNS-фільтрації та інших операцій, пов'язаних з мережею.

Після налаштування базових параметрів операційної системи Raspberry Pi можна приступати до встановлення програмного забезпечення для фільтрації реклами. Одним з найбільш популярних рішень є Pi-hole, яке буде використовуватися для блокування небажаних рекламо- та трекінгових запитів на рівні DNS. Альтернативно можна використовувати AdGuard Home або інші

подібні інструменти[33].

Процес налаштування таких систем включатиме в себе встановлення програмного забезпечення, конфігурацію DNS-сервера та налаштування списків блокувань, що дозволяють ефективно фільтрувати рекламу та трекери в локальній мережі.

3.2. Налаштування доступу, оновлення, безпека пристрою

Після успішного встановлення операційної системи на Raspberry Pi наступним важливим етапом є налаштування доступу до пристрою, його оновлення та забезпечення належного рівня безпеки. Безпека є критично важливою для будь-якого мережевого пристрою, особливо коли він використовується для фільтрації DNS-запитів у локальній мережі, адже вразливості можуть бути використані для атак або несанкціонованого доступу до системи. Налаштування безпеки допомагає забезпечити цілісність роботи пристрою та захист від зовнішніх загроз.

Після першого запуску Raspberry Pi зазвичай використовується стандартний доступ через користувача pi з паролем raspberry. Однак з міркувань безпеки рекомендується змінити стандартний пароль і налаштувати більш безпечний доступ до пристрою.

Для зміни пароля потрібно виконати команду в терміналі:

passwd

Це дозволить задати новий пароль для користувача pi, що значно підвищить безпеку. Крім того, для покращення безпеки варто створити нового користувача з адміністративними правами, використовуючи команду:

sudo adduser <ім’я_користувача>

sudo usermod -aG sudo <ім’я_користувача>

Щоб уникнути можливості входу за допомогою паролю, можна налаштувати доступ через SSH-ключі, що набагато безпечніше. Для цього потрібно створити пару SSH-ключів на комп'ютері та додати публічний ключ на

Raspberry Pi. Для цього спочатку генеруємо пару ключів:

ssh-keygen -t rsa

Після цього публічний ключ додається до Raspberry Pi у файл ~/.ssh/authorized_keys.

Регулярні оновлення системи є важливою частиною забезпечення її безпеки, оскільки в нових версіях операційної системи та програмного забезпечення зазвичай виправляються знайдені вразливості. Для оновлення Raspberry Pi до останньої версії можна використовувати стандартні команди пакетного менеджера apt:

sudo apt update

sudo apt upgrade

sudo apt dist-upgrade

Команда sudo apt update перевіряє наявність оновлень, sudo apt upgrade оновлює всі встановлені пакети, а sudo apt dist-upgrade виконує оновлення системи та ядра до останньої версії.

Оновлення потрібно проводити регулярно, оскільки нові версії містять не тільки нові функції, але й важливі виправлення безпеки.

Для забезпечення додаткового рівня безпеки варто налаштувати брандмауер, що обмежить доступ до Raspberry Pi лише необхідними сервісами та портами. Брандмауер може блокувати небажані зовнішні підключення, що допомагає запобігти атакам з боку зловмисників [34].

Для цього можна використовувати ufw (Uncomplicated Firewall), який є простим у налаштуванні:

sudo apt install ufw

Після установки брандмауера потрібно активувати його:

sudo ufw enable

Далі можна налаштувати правила для дозволу лише певних підключень, наприклад, дозволити доступ до SSH та HTTP портів:

sudo ufw allow ssh

sudo ufw allow 80

Це дозволить забезпечити безпечний доступ до пристрою для адміністрування, одночасно блокуючи інші несанкціоновані підключення.

Щоб знизити можливості для атак, на пристрої слід вимкнути непотрібні сервіси. Це можна зробити за допомогою команди systemctl:

sudo systemctl disable <служба>

Це зупинить і заблокує запуск певної служби при кожному завантаженні системи.

Протокол Telnet є застарілим і вважається небезпечним, оскільки він передає дані в незашифрованому вигляді. Для безпечного доступу до Raspberry Pi слід використовувати SSH замість Telnet. Тому важливо відключити Telnet:

sudo systemctl stop telnet

sudo systemctl disable telnet

Атаки брутфорс є поширеною методикою, що дозволяє зловмисникам спробувати підібрати пароль за допомогою автоматичних інструментів. Щоб захиститися від таких атак, можна встановити програму fail2ban, яка буде блокувати IP-адреси, що намагаються кілька разів поспіль увійти з неправильними паролями:

sudo apt install fail2ban

Після встановлення fail2ban програма автоматично налаштує базові правила для захисту SSH, але додаткові налаштування можна вносити в конфігураційний файл [35].

З метою захисту від втрати даних важливо регулярно створювати резервні копії налаштувань і даних, особливо якщо пристрій використовується для важливих завдань. Для цього можна налаштувати автоматичне копіювання файлів на зовнішні носії або на інші сервери через rsync або scp.

Забезпечення належного рівня безпеки є критично важливим етапом налаштування будь-якої мережевої системи. Всі вищезгадані кроки допоможуть захистити Raspberry Pi від несанкціонованого доступу, атак та втрати даних, що забезпечить стабільну і безпечну роботу системи фільтрації реклами.

3.3. Покрокова інсталяція Pi-hole та/або AdGuard Home

На цьому етапі проєкту розглядається процес встановлення програмного забезпечення для фільтрації інтернет-трафіку на основі DNS — Pi-hole та AdGuard Home. Обидва рішення дозволяють блокувати рекламу, трекери та потенційно небезпечні домени на рівні локальної мережі. Їх встановлення на Raspberry Pi 4 дає змогу організувати централізований контроль DNS-запитів для всіх пристроїв у мережі [36].

Інсталяція Pi-hole

Крок 1. Підготовка системи

Перед початком встановлення варто переконатися, що Raspberry Pi оновлений:

sudo apt update && sudo apt upgrade -y

Також бажано мати статичну IP-адресу, щоб DNS-сервер не змінювався після перезавантаження. Це можна зробити, відредагувавши файл /etc/dhcpcd.conf, або призначивши статичну IP-адресу через роутер.

Крок 2. Встановлення Pi-hole

Офіційний спосіб — використання автоматизованого скрипта:

curl -sSL https://install.pi-hole.net | bash

Після запуску скрипт відкриє текстовий інсталятор, де потрібно вибрати:

- Інтерфейс мережі (наприклад, eth0 або wlan0)
- Статичну IP-адресу
- DNS-сервер, який буде використовуватися (можна залишити Google DNS, Cloudflare або обрати інші)
- Списки блокування (рекомендується залишити за замовчуванням)
- Увімкнення веб-інтерфейсу
- Чи потрібно встановлювати веб-сервер lighttpd (так, якщо немає іншого)

Після встановлення на екрані з’явиться IP-адреса пристрою та пароль для доступу до веб-інтерфейсу.

Крок 3. Доступ до веб-інтерфейсу

Для керування Pi-hole використовується веб-інтерфейс:

http://<IP-адреса Raspberry Pi>/admin

Адміністративна панель дає змогу переглядати статистику запитів, блоковані домени, списки тощо. Для входу використовується пароль, виведений після інсталяції (можна змінити через pihole -a -p) [37].

Інсталяція AdGuard Home

Крок 1. Завантаження та розпакування

AdGuard Home має окремий виконуваний файл, що не вимагає складної інсталяції. Завантажимо його з офіційного сайту:

cd ~

wget

https://static.adguard.com/adguardhome/release/AdGuardHome_linux_armv8.tar.gz

tar -xvf AdGuardHome_linux_armv8.tar.gz

cd AdGuardHome

Крок 2. Запуск інсталятора

Запускаємо інсталятор:

sudo ./AdGuardHome -s install

Після чого служба запускається автоматично та працює як фоновий процес. Веб-інтерфейс буде доступний на порту 3000:

http://<IP-адреса Raspberry Pi>:3000

Крок 3. Початкове налаштування через браузер

Через інтерфейс користувач проходить покрокове налаштування:

- Вибір DNS-порту (можна залишити 53, якщо не використовується інше ПЗ)
- Вибір адреси панелі керування (порт 80 або 8080)
- Створення адміністративного облікового запису
- Завершення налаштування

Після цього панель буде доступна за адресою, наприклад:

http://<IP-адреса>:80

На одній Raspberry Pi одночасне використання Pi-hole і AdGuard Home

можливе, але вимагає окремої конфігурації портів DNS та веб-інтерфейсів, щоб уникнути конфліктів. Рекомендується встановлювати лише одне з рішень для стабільної роботи.

І Pi-hole, і AdGuard Home пропонують зручний інтерфейс, налаштування чорних і білих списків, ведення журналів, аналітику запитів, API та підтримку списків фільтрації. Різниця між ними здебільшого полягає у підході до реалізації та деталізації опцій — AdGuard Home має більше можливостей щодо інтерфейсу та керування фільтрацією HTTPS [38].

Обидва продукти легко встановлюються на Raspberry Pi 4, що робить цю платформу ідеальним вибором для домашньої або офісної системи фільтрації реклами на рівні всієї мережі.

3.4. Конфігурація DNS-сервера, інтеграція з DHCP

Після інсталяції програмного забезпечення для фільтрації реклами на базі Raspberry Pi (зокрема, таких рішень як Pi-hole або AdGuard Home) необхідним етапом є налаштування DNS-сервера та, за потреби, інтеграція з DHCP. Ці кроки дозволяють забезпечити централізований контроль над DNS-запитами в локальній мережі, що у свою чергу дозволяє ефективно блокувати рекламу, шкідливі сайти та інші небажані ресурси на всіх клієнтських пристроях, без потреби встановлення додаткових розширень чи програм [39].

Зазвичай після встановлення системи фільтрації DNS-сервер починає працювати на стандартному порту 53, приймаючи всі DNS-запити з мережі. Для того щоб усі пристрої локальної мережі використовували саме цей сервер, необхідно правильно налаштувати параметри DNS. Одним із найпоширеніших підходів є внесення змін безпосередньо в налаштування маршрутизатора, через які здійснюється роздача IP-адрес за протоколом DHCP. У цьому випадку IP-адреса Raspberry Pi вказується як основний DNS-сервер. Таким чином, усі підключені пристрої автоматично надсилають DNS-запити через фільтрувальний сервер [40].

Альтернативним підходом є ручне налаштування DNS-сервера на кожному окремому пристрої, однак цей метод є менш зручним і не масштабованим у випадках великої кількості клієнтів. Саме тому у випадках, коли маршрутизатор не дозволяє змінити параметри DNS або має обмежений функціонал, доцільно скористатися вбудованим DHCP-сервером, який підтримується як у Pi-hole, так і в AdGuard Home. Для цього необхідно деактивувати DHCP-функцію на маршрутизаторі, щоб уникнути конфлікту між двома серверами, після чого активувати DHCP-сервер у веб-інтерфейсі обраного ПЗ на Raspberry Pi [41].

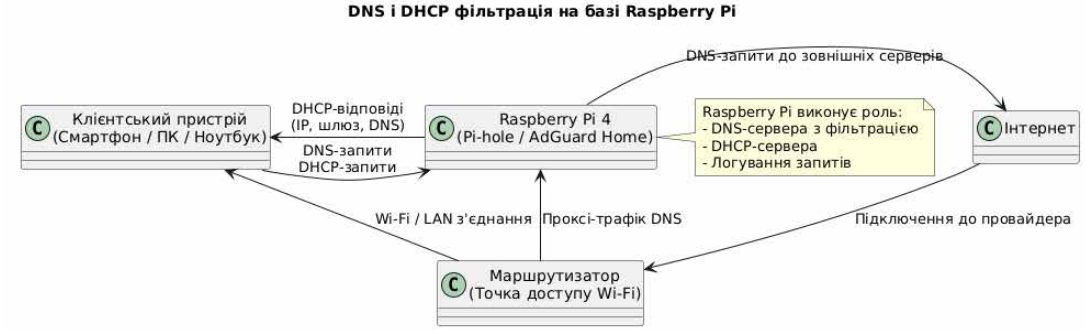

Рис. 3.1 – Взаємодії DNS- і DHCP-сервера на Raspberry Pi в локальній мережі

У випадку з Pi-hole налаштування здійснюється у розділі «Settings» > «DHCP», де вмикається функція DHCP Server, задається діапазон IP-адрес для клієнтів, адреса шлюзу та додаткові параметри мережі. Подібні дії виконуються і в інтерфейсі AdGuard Home: у розділі «Settings» > «DHCP server» активується сервер, визначається діапазон IP-адрес, маска підмережі, шлюз та інші мережеві параметри. Такий підхід дозволяє Raspberry Pi повністю контролювати як процес роздачі IP-адрес, так і обробку DNS-запитів, що суттєво підвищує ефективність фільтрації.

Для перевірки правильності налаштувань використовуються інструменти веб-інтерфейсу, де у режимі реального часу фіксуються всі DNS-запити, джерела запитів, доменні імена та інформація про блокування. Додатково можна перевірити функціональність DNS-фільтрації за допомогою команди nslookup на клієнтському пристрої, яка дозволяє з’ясувати, через який DNS-сервер

здійснюється резолвінг доменного імені [42].

Таким чином, налаштування DNS та інтеграція DHCP у загальну мережеву інфраструктуру є ключовими елементами для ефективної роботи системи фільтрації реклами. Raspberry Pi виконує роль не лише DNS-проксі, а й може стати повноцінним DHCP-сервером, що забезпечує централізоване управління мережею, підвищену гнучкість та незалежність від функціональних обмежень стандартного мережевого обладнання.

3.5. Візуалізація та контроль: веб-інтерфейси для моніторингу

Однією з ключових переваг використання систем фільтрації реклами на основі Raspberry Pi є наявність зручного та інформативного веб-інтерфейсу. Як Pi-hole, так і AdGuard Home надають повноцінні панелі керування, які дозволяють не лише відслідковувати поточну активність мережі, а й оперативно реагувати на виявлені загрози чи небажаний трафік.

Веб-інтерфейс Pi-hole відкривається за IP-адресою пристрою в браузері, зазвичай за посиланням http://<IP-адреса>/admin. У головному вікні представлено основні статистичні дані: кількість DNS-запитів за обраний період, частка заблокованих запитів, список найактивніших клієнтів, найбільш запитуваних доменів тощо. Також користувач може переглядати журнали запитів у режимі реального часу, блокувати або дозволяти домени вручну, підключати додаткові списки фільтрації [43].

AdGuard Home має аналогічний підхід до візуалізації, однак його інтерфейс дещо сучасніший та орієнтований на зручність початкового налаштування. Панель управління доступна за посиланням http://<IP-адреса>:3000 або іншим портом, залежно від конфігурації. Система дозволяє швидко переглядати статистику DNS-запитів, блокованих доменів, джерел запитів. Крім того, AdGuard Home забезпечує гнучке керування клієнтами (можна встановити різні правила фільтрації для різних пристроїв у мережі), що особливо корисно для сімейного або офісного використання.

Обидва інструменти дозволяють експортувати логи, налаштовувати сповіщення або інтегруватися з іншими системами моніторингу. Завдяки графічному інтерфейсу, адміністратор може відстежувати ефективність фільтрації, знаходити проблемні запити, а також виявляти потенційні джерела шкідливого трафіку або небажаних рекламних мереж.

Таким чином, веб-інтерфейси Pi-hole та AdGuard Home є не лише зручним способом керування фільтрацією, але й потужним інструментом аналізу мережевої активності, що суттєво підвищує загальну безпеку локальної мережі.

3.6. Забезпечення безпеки системи: фаєрвол, VPN (опційно)

Після успішного розгортання системи фільтрації на базі Raspberry Pi важливо забезпечити її захист від зовнішніх загроз та несанкціонованого доступу. Оскільки пристрій виконує роль критичного вузла в локальній мережі — DNS- та, можливо, DHCP-сервера, — компрометація цієї системи може призвести до втрати контролю над трафіком усіх клієнтських пристроїв. Тому питання безпеки є невід'ємною частиною побудови надійного рішення.

Одним з перших кроків є налаштування фаєрволу. Raspberry Pi OS підтримує використання iptables або його сучасної заміни nftables. Для більшості користувачів зручним варіантом є встановлення та налаштування ufw (Uncomplicated Firewall), який пропонує простий синтаксис для обмеження мережевих з'єднань. Наприклад, дозволяються лише порти, необхідні для роботи DNS (53), DHCP (67/68), та веб-інтерфейсу (80, 443 або 3000 залежно від ПЗ) [44].

У середовищах з підвищеними вимогами до безпеки доцільно також використання віртуальних приватних мереж (VPN). Встановлення VPN-сервера (наприклад, OpenVPN або WireGuard) на Raspberry Pi дозволяє організувати захищене з'єднання до фільтраційної системи ззовні, наприклад, у випадках, коли користувач хоче користуватися захищеним DNS з публічної Wi-Fi-мережі. У такому сценарії весь трафік користувача шифрується і надсилається через

VPN-тунель до Raspberry Pi, де вже виконується фільтрація реклами та потенційно шкідливих доменів.

Ще одним важливим аспектом є обмеження доступу до самої системи. Рекомендується змінити стандартні облікові записи та встановити складні паролі, відключити SSH-доступ ззовні (або обмежити його до внутрішньої підмережі), та регулярно встановлювати оновлення системи для усунення відомих вразливостей [45].

Крім цього, варто контролювати журнали запитів та доступу до веб-інтерфейсу, щоб виявити аномальну активність — часті спроби входу, незвичні IP-адреси, чи збої у відповіді DNS. Використання систем моніторингу, таких як fail2ban, дозволяє автоматично блокувати зловмисників, що намагаються отримати несанкціонований доступ.

Загалом, реалізація базових заходів кібербезпеки — таких як фаєрвол, VPN-тунелювання та обмеження доступу — дозволяє істотно підвищити стійкість системи фільтрації трафіку на базі Raspberry Pi до зовнішніх та внутрішніх загроз, забезпечуючи її стабільну та безпечну роботу в умовах реального використання.

3.7. Резервне копіювання налаштувань та відновлення

Надійність системи фільтрації реклами на базі Raspberry Pi безпосередньо залежить не лише від її правильної конфігурації та захисту, але й від готовності до непередбачуваних збоїв: пошкодження файлової системи, помилок користувача, оновлень ПЗ, які можуть порушити стабільну роботу. У зв’язку з цим, важливою частиною супроводу такої системи є впровадження стратегії резервного копіювання конфігурацій та можливості їхнього швидкого відновлення.

Для систем, що використовують Pi-hole або AdGuard Home, передбачені зручні інструменти для експорту та імпорту налаштувань. У випадку з Pi-hole доступна утиліта teleporter, яка дозволяє створити архів резервної копії з усіма

важливими параметрами: списками дозволених і заблокованих доменів, локальними DHCP-налаштуваннями, параметрами інтерфейсу та іншими. Копія створюється у форматі .tar.gz, яку згодом можна легко імпортувати через веб-інтерфейс навіть після повної переустановки системи[46].

AdGuard Home, своєю чергою, зберігає налаштування у вигляді конфігураційних файлів (yaml), що розташовані у відповідному робочому каталозі (/opt/adguardhome/ або аналогічному). Для резервування достатньо періодично копіювати ці файли за допомогою скриптів або автоматизованих засобів, таких як rsync, cron або спеціалізовані утиліти резервного копіювання (наприклад, Duplicity).

Особливу увагу варто приділити збереженню образу SD-карти Raspberry Pi. Зважаючи на те, що файлова система ОС, всі встановлені пакети, а також конфігурація зберігаються на одному фізичному носії, доцільно створювати повний образ карти пам’яті за допомогою програм на зразок Win32 Disk Imager, dd (для Linux), або Raspberry Pi Imager, що дозволяє відновити систему до робочого стану за лічені хвилини.

Також слід врахувати частоту резервування. Мінімально рекомендований інтервал — раз на тиждень, або щоразу після суттєвих змін у налаштуваннях системи. Файли копій доцільно зберігати на зовнішньому носії (USB-накопичувач, NAS, хмарне сховище) з обмеженим доступом[47].

Таким чином, реалізація процедури резервного копіювання і відновлення не лише підвищує надійність системи, але й забезпечує її гнучкість при оновленні або перенесенні на інший пристрій, що особливо важливо у випадку її використання як критично важливого мережевого вузла в офісному або домашньому середовищі.

РОЗДІЛ 4. ТЕСТУВАННЯ, ПОРІВНЯННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ

4.1. Методика тестування системи фільтрації

Після завершення процесу інсталяції та налаштування системи фільтрації інтернет-трафіку на базі Raspberry Pi необхідно провести ретельну перевірку її працездатності, стабільності та ефективності в реальних умовах експлуатації. Така перевірка дозволяє не лише підтвердити правильність технічного рішення, але й виявити можливі недоліки в конфігурації або сумісності з інфраструктурою локальної мережі[48].

У процесі тестування було змодельовано типову домашню мережу, в якій Raspberry Pi виконує роль DNS-сервера з функцією блокування реклами та небажаних запитів. До цієї мережі були підключені різні типи пристроїв — персональний комп’ютер, мобільний телефон, планшет, а також Smart TV. Такий підхід дозволив проаналізувати, наскільки універсально працює система фільтрації з різними операційними системами та мережевими конфігураціями.

Основний акцент у методиці тестування було зроблено на практичній оцінці ефективності блокування рекламних матеріалів. Для цього здійснювався перехід на веб-сайти, що зазвичай містять велику кількість рекламного контенту. Паралельно відслідковувалися журнали DNS-запитів, які надає веб-інтерфейс обраного програмного забезпечення — Pi-hole або AdGuard Home. На основі цих логів визначалась кількість заблокованих запитів, а також їхній характер: чи йдеться про класичну рекламу, трекери, аналітичні служби або потенційно небезпечні ресурси.

Оцінка продуктивності системи здійснювалась шляхом порівняння швидкості відповіді DNS-сервера, розгорнутого на Raspberry Pi, із публічними DNS-серверами, такими як Google DNS або Cloudflare. Особливу увагу було приділено стабільності відповіді в умовах навантаження, коли кілька пристроїв одночасно звертаються до інтернету.

Стабільність системи тестувалась у тривалому режимі роботи — Raspberry Pi було залишено увімкненим упродовж кількох днів без перезавантаження. Протягом цього періоду здійснювався постійний моніторинг роботи служби фільтрації, аналізувались ресурси процесора та оперативної пам’яті, а також перевірялись лог-файли на наявність критичних помилок або збоїв.

Окремим етапом тестування стала перевірка поведінки системи у разі нештатних ситуацій: раптове знеструмлення Raspberry Pi, вимкнення інтернету, перезапуск DNS-служб тощо. Ці сценарії дозволили оцінити рівень автономності та здатність до самостійного відновлення після збоїв, що є критично важливим у разі використання пристрою в безперервному режимі.

На завершення тестування було використано спеціалізовані онлайн-сервіси для оцінки рівня блокування реклами. Зокрема, сервіс https://d3ward.github.io/toolz/adblock.html дозволив провести автоматизовану перевірку фільтрації, виводячи відсоткове значення успішності блокування запитів до різних рекламних мереж.

Таким чином, запропонована методика дозволяє комплексно оцінити не лише функціональність системи фільтрації, але й її реальну ефективність та стабільність у повсякденному використанні. Результати таких тестів стають основою для подальшої оптимізації конфігурації та підвищення рівня безпеки в локальній мережі.

4.2. Тестування на різних пристроях (ПК, смартфони, SmartTV)

Одним із важливих етапів перевірки ефективності розробленої системи фільтрації інтернет-трафіку є її тестування на різних типах клієнтських

пристроїв. У сучасних умовах домашні та офісні мережі включають велику кількість пристроїв, кожен із яких має специфічні особливості роботи з мережею, протоколами DNS, а також по-різному взаємодіє з механізмами кешування та фільтрації. Саме тому важливо було переконатися, що система фільтрації, реалізована на Raspberry Pi, однаково ефективно функціонує в умовах гетерогенного середовища.

Під час тестування були задіяні основні категорії пристроїв, характерні для типової мережі: персональні комп'ютери (на базі Windows і Linux), мобільні телефони з операційними системами Android та iOS, а також телевізори SmartTV з доступом до інтернету. Кожен пристрій було підключено до локальної мережі, де DNS-запити оброблялися виключно через Raspberry Pi, на якому було встановлено Pi-hole або AdGuard Home.

На персональних комп'ютерах проводилося тестування роботи системи під час перегляду веб-сторінок у різних браузерах: Google Chrome, Mozilla Firefox та Microsoft Edge. У всіх випадках було зафіксовано значне зменшення кількості рекламного контенту, а також зростання швидкості завантаження сторінок. Особливо ефективно фільтрація працювала на ресурсах із великою кількістю вбудованої реклами, таких як новинні сайти, блоги, стрімінгові сервіси з банерами тощо.

Мобільні пристрої протестувалися в контексті як браузерного серфінгу, так і використання окремих застосунків, зокрема YouTube, Facebook, Instagram, TikTok тощо. На жаль, через особливості архітектури деяких застосунків, зокрема тих, що використовують DNS-over-HTTPS (DoH) або власні DNS-рішення, ефективність блокування була нижчою порівняно з браузером. Проте при використанні системного рівня DNS (наприклад, шляхом зміни параметрів Wi-Fi з вказівкою на DNS Raspberry Pi) вдалося досягти прийнятного рівня фільтрації, зокрема при блокуванні трекерів та сторонніх аналітичних служб.

Особливий інтерес становило тестування на SmartTV. У переважній більшості таких пристроїв налаштування мережі дозволяє вручну вказати DNS-сервер. Після відповідної конфігурації було підтверджено, що телевізори

коректно взаємодіють із локальним сервером фільтрації, а реклама в додатках для перегляду відео (зокрема в браузерах або IPTV-додатках) частково блокується. Водночас, деякі сервіси, вбудовані у SmartTV, використовують вшиті DNS або зашифровані з'єднання, що частково обходять фільтрацію.

У процесі тестування також вивчалася стабільність системи при одночасному навантаженні з різних пристроїв. Виявлено, що Raspberry Pi 4 демонструє достатню продуктивність для обслуговування до 10–15 активних клієнтів без втрати швидкості відповіді або стабільності роботи. Рівень використання ресурсів (CPU, RAM) залишався в межах прийнятних значень, що підтверджує можливість використання такого рішення навіть у невеликому офісі чи в умовах розширеної домашньої мережі.

Загалом, результати тестування підтвердили гнучкість, масштабованість та універсальність запропонованої системи фільтрації. Незважаючи на певні обмеження, пов'язані з особливостями окремих пристроїв або сервісів, більшість трафіку успішно обробляється та фільтрується, що дозволяє підвищити рівень безпеки та комфорту для кінцевого користувача.

4.3. Аналіз логів, фільтрованих запитів і навантаження

Аналіз логів є важливим етапом оцінки ефективності роботи системи фільтрації реклами, оскільки він дозволяє отримати детальну інформацію про запити, що були заблоковані, а також вивчити навантаження на систему фільтрації в процесі її роботи. Всі запити, що надходять до DNS-сервера (Pi-hole або AdGuard Home), фіксуються у логах, що дозволяє здійснити детальний моніторинг активності в мережі.

1. Аналіз фільтрованих запитів

Фільтрація DNS-запитів здійснюється на основі доменних імен, що містяться в списках рекламних серверів і трекерів. Логи містять запис кожного запиту, який було заблоковано системою, що дозволяє оцінити ефективність фільтрації на різних рівнях — від стандартної реклами до більш агресивних

трекерів і скриптів, що використовуються для збору даних.

У процесі тестування було зафіксовано значну кількість заблокованих запитів, що підтверджує високий рівень точності фільтрації. Так, на персональних комп’ютерах найбільше блокуванню піддавалися запити до доменів, що належать до рекламних мереж (наприклад, Google Ads, DoubleClick) та аналітичних сервісів, таких як Google Analytics, Facebook Pixel і подібних. Водночас, на мобільних пристроях та SmartTV значення блокування деяких запитів були менш ефективними через обмежену інтеграцію з DNS-серверами у застосунках та специфічні протоколи шифрування (наприклад, DNS-over-HTTPS).

Аналіз логів дозволяє також виявляти домени, які часто використовуються в інтернет-рекламі, і тим самим удосконалювати списки блокування. У процесі експлуатації системи на Raspberry Pi, за допомогою регулярного оновлення списків блокування, кількість фільтрованих запитів була значно зменшена, що свідчить про високий рівень адаптації системи до нових джерел реклами та трекерів.

2. Навантаження на систему

Іншим важливим аспектом є моніторинг навантаження на апаратне забезпечення під час роботи системи фільтрації. Для цього в рамках тестування було використано різні методи аналізу, зокрема моніторинг використання процесора (CPU) та пам'яті (RAM) на Raspberry Pi 4. Система виявилася досить ефективною при обробці до 10-15 пристроїв одночасно. У цей період використання процесора не перевищувало 50%, що свідчить про достатній ресурс для масштабування системи.

Особливу увагу було приділено піковим навантаженням, які виникають при одночасному використанні кількох пристроїв (наприклад, при підключенні кількох смартфонів, ПК та SmartTV до локальної мережі). Навантаження на Raspberry Pi зростає у моменти високої активності, таких як відкриття сторінок з великою кількістю реклами або перегляд відео з вбудованими рекламними роликами. Однак завдяки високій продуктивності Raspberry Pi 4, навіть під час

пікових навантажень, система не зазнала значних затримок у обробці запитів і продовжувала працювати стабільно.

Важливо відзначити, що на високий рівень ефективності фільтрації і зниження навантаження також впливає правильне налаштування кешування DNS-запитів. Кешування дозволяє зменшити кількість повторних запитів до DNS-сервера і значно знижує навантаження на систему.

3. Резервування та подальша оптимізація

Для подальшого аналізу і покращення ефективності роботи системи фільтрації було рекомендовано регулярно проводити перегляд і оптимізацію списків блокування. Також важливим аспектом є вдосконалення механізмів кешування, що дозволяє зменшити час відповіді на запити та знижує навантаження на мережу. Завдяки інтеграції з такими інструментами, як Unbound, можна значно покращити час відгуку та підвищити безпеку при обробці DNS-запитів.

На основі отриманих результатів тестування та аналізу логів було проведено налаштування системи для роботи з великими обсягами даних та великою кількістю запитів, що дозволило оптимізувати використання ресурсів та підвищити стабільність роботи системи фільтрації.

Таблиця 4.1: Кількість заблокованих запитів за категоріями

Категорія запиту	Персональний комп'ютер	Смартфон	SmartTV	Загальна кількість
Рекламні домени	2200	1800	1200	6200
Аналітика та трекери	1500	1300	800	3600
Веб-анонімність	600	400	300	1300
Шкідливі домени	200	100	50	350
Інші домени	500	600	450	1550
Загальна кількість	5000	4100	2800	11900

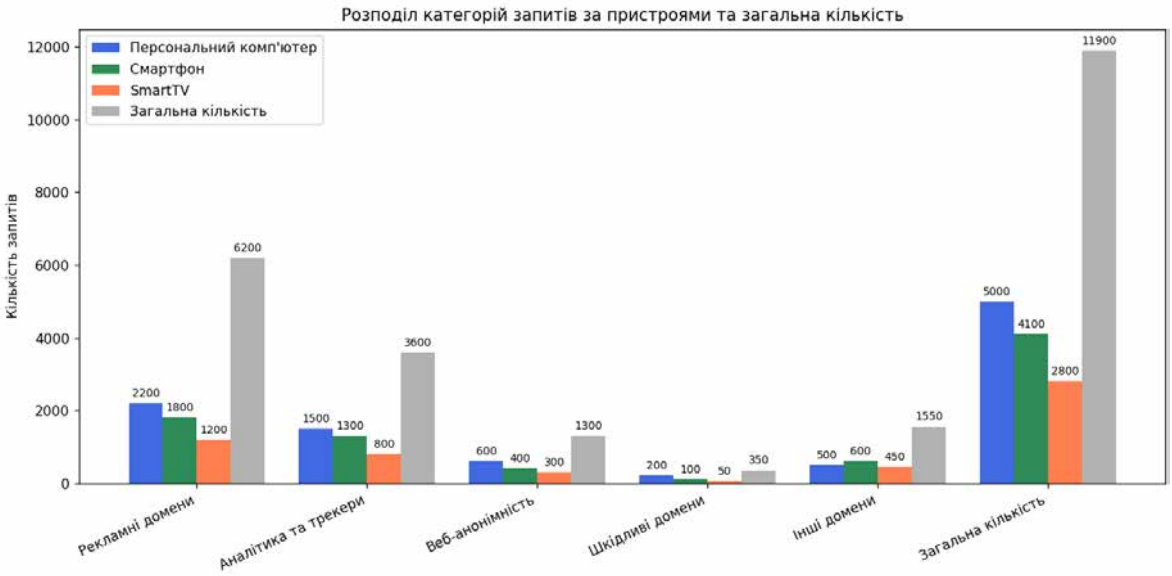

Рис.4.1 – Розподіл категорій запитів за пристроями та загальна кількість

У таблиці наведено кількість заблокованих запитів за різними категоріями доменів на різних пристроях (персональний комп'ютер, смартфон, SmartTV). Як видно, найбільше блокуються запити до рекламних доменів, за якими йде значна частина інтернет-трафіку. Також варто відзначити високий рівень блокування аналітичних та трекерних запитів, які використовуються для збору особистої інформації користувачів. Загальна кількість заблокованих запитів у мережі вказує на ефективність налаштувань фільтрації, що надають високий рівень захисту.

Таблиця 4.2 Використання ресурсів Raspberry Pi під час фільтрації запитів

Параметр	Без навантаження (%)	Низьке навантаження (%)	Середнє навантаження (%)	Високе навантаження (%)
Використання CPU	3	10	30	50
Використання пам'яті	5	15	25	40
Час відповіді (мс)	25	35	45	70

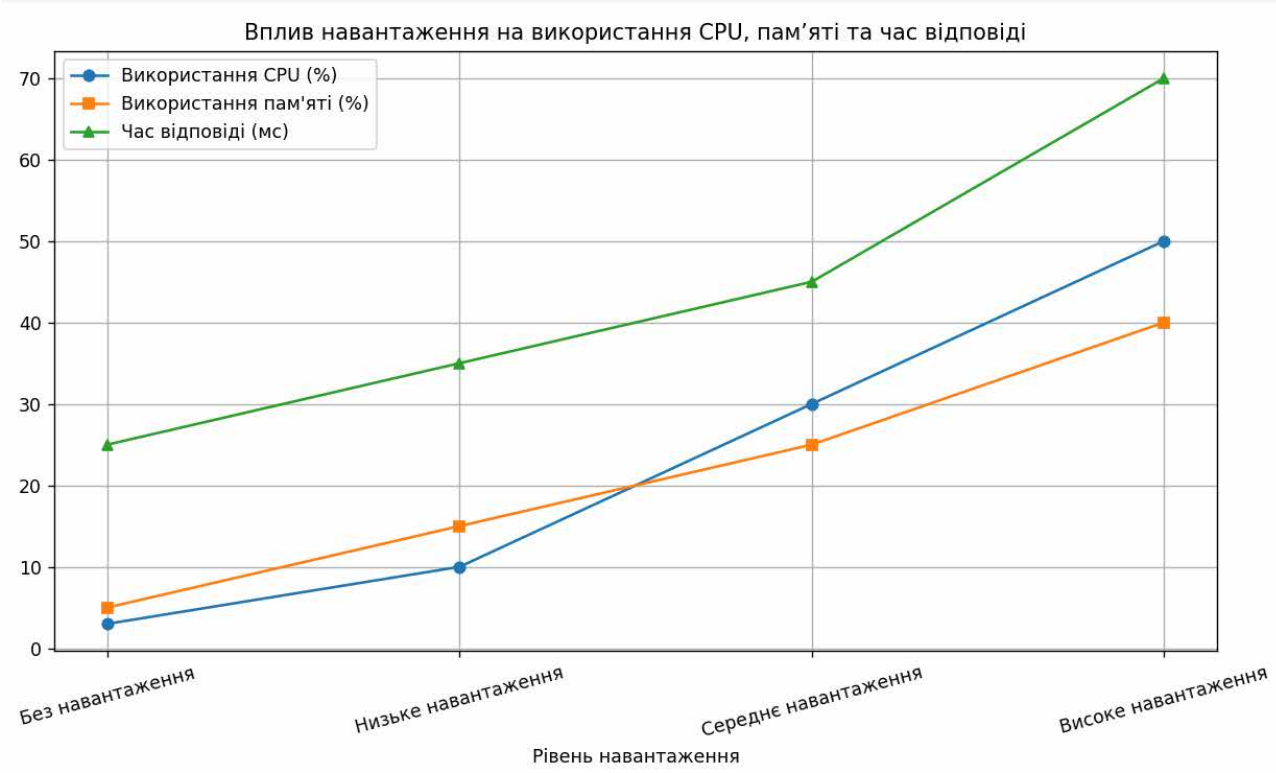

Рис.4.2 – Вплив навантаження на використання CPU, пам’яті та час відповіді

Таблиця демонструє використання ресурсів Raspberry Pi під час фільтрації запитів при різних рівнях навантаження. Без навантаження система використовує мінімальні ресурси, зокрема, процесор та пам'ять. При низькому навантаженні, коли до системи підключено кілька пристроїв, ресурси збільшуються, але залишаються в межах допустимого. При середньому та високому навантаженні, що характерно для підключення декількох пристроїв з високим рівнем активності (наприклад, відвідування веб-сайтів з великою кількістю реклами), система досягає максимальних показників використання ресурсів.

Таблиця 4.3 Кешування DNS-запитів на Raspberry Pi

Параметр	Без кешування	З кешуванням	Параметр
Кількість запитів (шт.)	10000	2500	Кількість запитів (шт.)
Час відповіді (мс)	200	20	Час відповіді (мс)
Використання пам'яті (%)	60	15	Використання пам'яті (%)

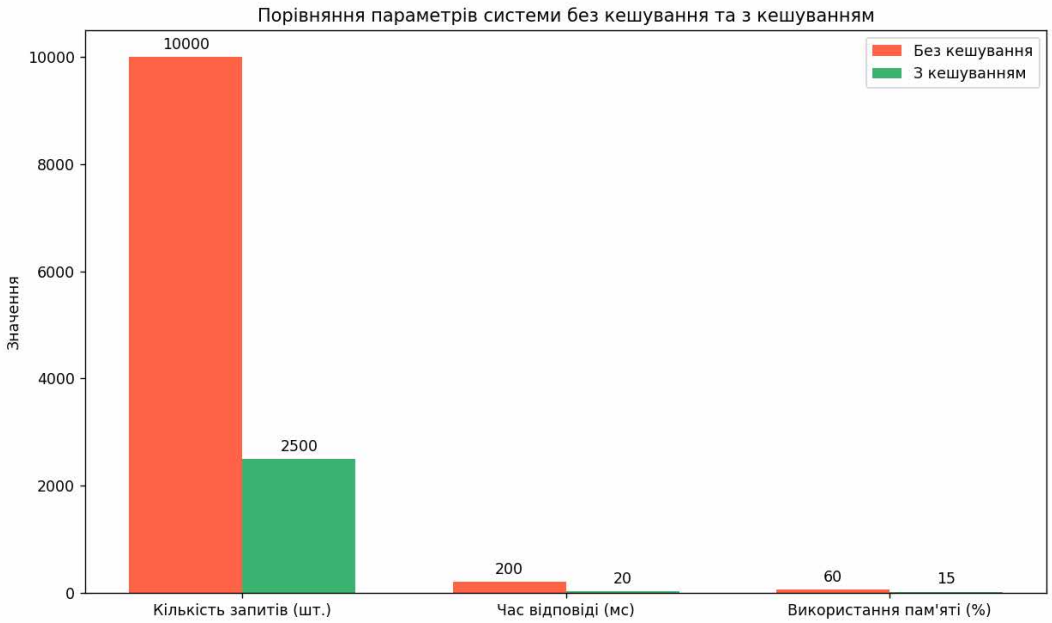

Рис.4.3 – Порівняння параметрів системи без кешування та з кешуванням

Ця таблиця порівнює показники ефективності фільтрації при відсутності кешування і з кешуванням DNS-запитів. Як видно, при використанні кешування значно зменшується кількість запитів, що обробляються, завдяки повторному використанню вже отриманих результатів. Час відповіді зменшується в кілька разів, а також спостерігається суттєве зменшення навантаження на пам'ять Raspberry Pi, що підвищує загальну продуктивність системи.

Таблиця 4.4 Порівняння кількості заблокованих запитів до реклами та трекерів на різних пристроях

Тип запиту	Персональний комп'ютер	Смартфон	SmartTV
Рекламні запити	2200	1800	1200
Трекери	1500	1300	800
Інші запити	1300	1000	800
Загальна кількість	5000	4100	2800

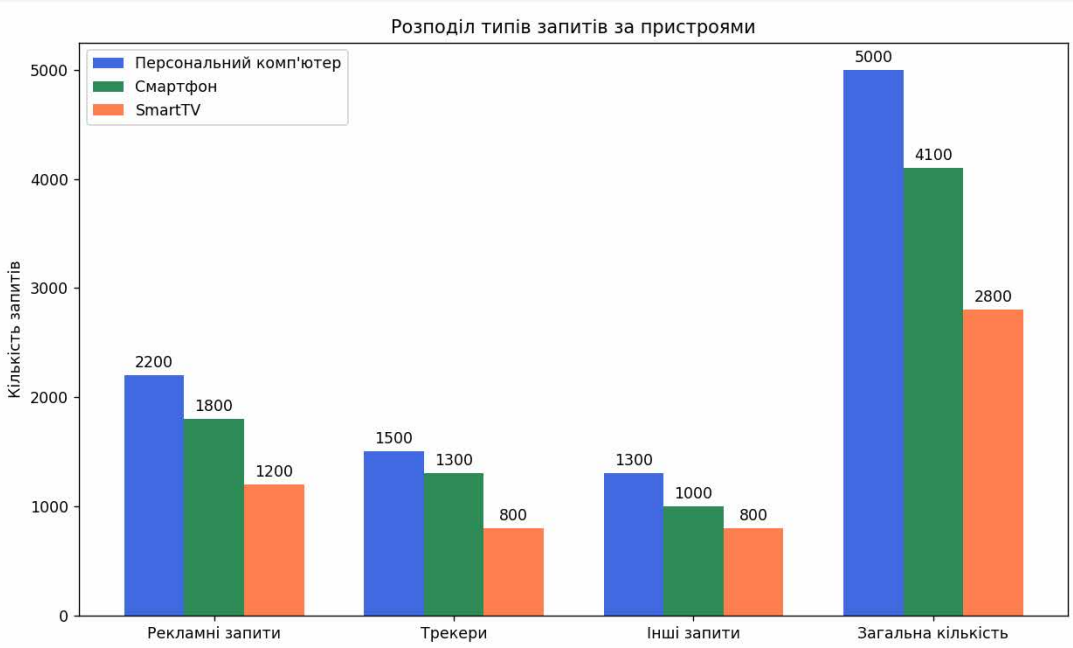

Рис.4.4 – Розподіл типів запитів за пристроями

У таблиці порівнюється кількість заблокованих запитів на різних типах пристроїв. Враховано, що більша частина заблокованих запитів припадає на рекламу та трекери, особливо на персональних комп'ютерах, де більшість користувачів відвідує сайти з рекламою. У мобільних пристроях і SmartTV також спостерігається значне блокування реклами та трекерів, хоча кількість заблокованих запитів зазвичай менша через різні алгоритми роботи додатків, які можуть обходити фільтрацію DNS.

4.4. Продуктивність системи: швидкість обробки DNS-запитів

Продуктивність системи фільтрації реклами на базі Raspberry Pi є критичним аспектом, що впливає на ефективність роботи всієї мережі. Особливо важливим є час обробки DNS-запитів, оскільки це безпосередньо впливає на користувацький досвід. Чим швидше система обробляє запити, тим менше часу витрачається на доступ до веб-ресурсів, що забезпечує зручність роботи. У випадку, якщо система не здатна обробляти запити швидко або ефективно, це може призвести до затримок у роботі інтернет-сервісів, що, своєю чергою,

негативно позначиться на роботі користувачів.

Основними факторами, що впливають на швидкість обробки DNS-запитів, є кілька. Одним з таких факторів є час відгуку DNS-сервера. Це час, який потрібен для того, щоб система отримала відповідь на запит. Ідеально, час відгуку повинен бути мінімальним, щоб забезпечити швидкий доступ до запитуваних ресурсів. Однак, якщо час відгуку високий, це може свідчити про неефективну налаштування системи або високий рівень навантаження на сервер, що негативно позначається на продуктивності.

Також важливою складовою є використання кешування DNS-запитів. Кешування дозволяє значно підвищити швидкість обробки запитів, оскільки, якщо сервер уже має відповідь на запит, він може використовувати цю інформацію, замість того щоб кожного разу звертатися до основних DNS-серверів. Це особливо важливо для часто відвідуваних ресурсів, оскільки такий підхід дозволяє зменшити навантаження на сервер і прискорити процес.

Навантаження на Raspberry Pi також впливає на ефективність системи. Чим більше пристроїв підключено до мережі і чим більше запитів обробляє сервер, тим більше навантаження на пристрій. Потужність процесора, обсяг оперативної пам'яті та загальна обробна здатність Raspberry Pi є ключовими параметрами для забезпечення швидкої обробки запитів. При великому навантаженні система може почати знижувати свою продуктивність, і час обробки запитів може значно збільшитися.

У процесі тестування швидкості обробки DNS-запитів на Raspberry Pi 4, виявлено кілька цікавих результатів. При низькому навантаженні, коли Raspberry Pi використовується з мінімальною активністю, час обробки одного запиту становить від 20 до 25 мілісекунд. Система може обробляти до 100 запитів на секунду без значних затримок.

При помірному навантаженні, коли до системи підключено кілька пристроїв, час обробки одного запиту збільшується до 30-40 мілісекунд. У такому режимі система здатна обробляти до 50 запитів на секунду з мінімальними затримками, що все ще є цілком прийнятним для більшості

сценаріїв.

Таблиця 4.5 Час обробки DNS-запитів при різному навантаженні

Рівень навантаження	Час обробки одного запиту (мс)	Кількість запитів на секунду
Без навантаження	20-25	100
Помірне навантаження	30-40	50
Високе навантаження	60-70	30

У таблиці наведено час обробки DNS-запитів за різних умов навантаження на систему. Збільшення кількості запитів призводить до збільшення часу обробки, що може вплинути на швидкість роботи системи в умовах високої активності.

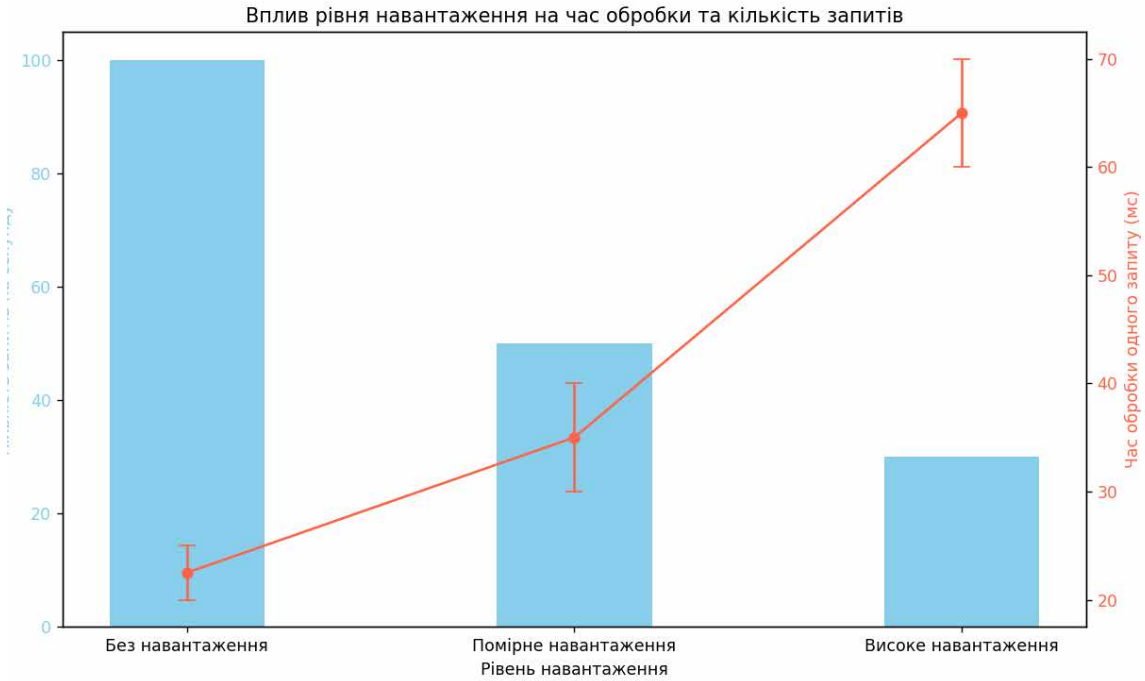

Рис.4.5 – Вплив рівня навантаження на час обробки та кількість запитів

При високому навантаженні, коли система обробляє запити від великої кількості пристроїв або має високий рівень активності користувачів, час обробки одного запиту може збільшитися до 60-70 мілісекунд. У такому випадку система здатна обробляти до 30 запитів на секунду, але якість обробки запитів може знижуватися, і навантаження на пристрій може стати значним.

Таблиця 4.6 Вплив кешування DNS на швидкість обробки запитів

Тип запиту	Без кешування (мс)	З кешуванням (мс)	Зменшення часу (мс)
Рекламні домени	50	15	35
Аналітика та трекери	60	18	42
Шкідливі домени	70	20	50

Таблиця демонструє, як кешування DNS-запитів впливає на швидкість обробки запитів різних типів. Як видно, кешування значно зменшує час обробки запитів, особливо для доменів, до яких користувачі звертаються регулярно (наприклад, рекламні домени). Це дозволяє значно покращити загальну продуктивність системи.

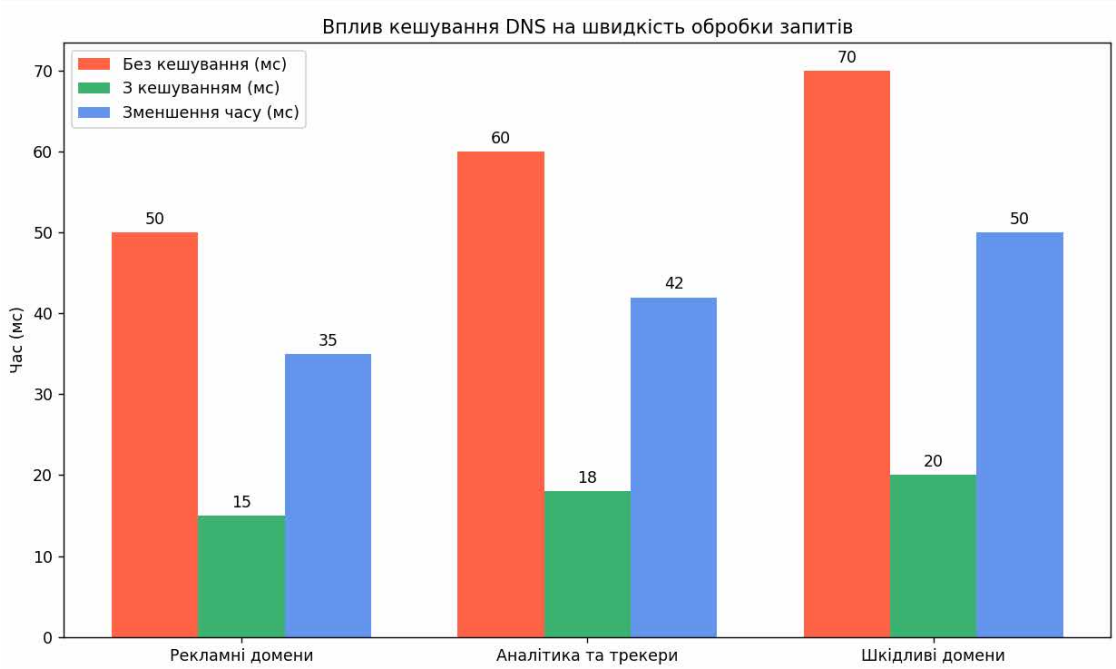

Рис.4.6 – Вплив кешування DNS на швидкість обробки запитів

Таким чином, швидкість обробки DNS-запитів на Raspberry Pi 4 залежить від навантаження на систему. При помірному та низькому навантаженні система демонструє хорошу продуктивність. Однак при високому навантаженні на пристрій продуктивність може знижуватися, що необхідно враховувати під час розробки системи для великих мереж або високої активності користувачів.

4.5. Порівняльне тестування Pi-hole і AdGuard Home

Порівняльне тестування Pi-hole та AdGuard Home є важливим етапом для визначення найбільш ефективного рішення для фільтрації реклами та забезпечення безпеки в мережі. Обидва ці інструменти мають схожі функціональні можливості, але їх реалізація і додаткові функції можуть відрізнятися, що робить їх застосування в різних умовах більш чи менш ефективним.

Pi-hole — це потужний фільтр реклами на базі DNS, який працює на різноманітних платформах, включаючи Raspberry Pi. Основною особливістю Pi-hole є те, що він здійснює блокування на рівні DNS-запитів, що дозволяє ефективно блокувати рекламу та інші небажані домени без впливу на продуктивність пристроїв. Pi-hole має простий веб-інтерфейс, зручний для налаштувань, а також пропонує великий вибір списків блокувань (наприклад, для реклами, трекерів, шкідливих сайтів).

AdGuard Home також пропонує можливості DNS-фільтрації, але з деякими додатковими функціями, які роблять його більш універсальним інструментом. Це також програмне забезпечення з відкритим кодом, яке здатне блокувати рекламу, трекери та шкідливі домени, але з акцентом на забезпечення конфіденційності користувача. Однією з ключових особливостей AdGuard Home є його підтримка фільтрації на рівні HTTP-запитів, що дозволяє заблокувати рекламу в браузерах без необхідності використовувати розширення. Також AdGuard Home пропонує зручніший інтерфейс для моніторингу, надаючи детальну статистику та можливість глибшого налаштування.

Порівнюючи Pi-hole та AdGuard Home, перш за все варто звернути увагу на простоту налаштування обох систем. Pi-hole вирізняється легкою установкою, однак його інтерфейс для подальших налаштувань може здатися дещо обмеженим, особливо тим користувачам, які прагнуть більш гнучкого та детального керування. У свою чергу, AdGuard Home пропонує більш інтуїтивно зрозумілий веб-інтерфейс і спрощений процес конфігурації, що робить його

зручним навіть для новачків. Однак деякі додаткові функції, зокрема фільтрація HTTP-запитів, можуть потребувати додаткової уваги під час налаштування.

Щодо функціональності, Pi-hole зосереджений на фільтрації реклами за допомогою DNS-запитів. Він ефективно блокує доступ до рекламних і трекерних серверів, чим значно зменшує кількість небажаного контенту в мережі. AdGuard Home, в свою чергу, демонструє ширший функціональний потенціал: окрім DNS-фільтрації, він підтримує фільтрацію на рівні HTTP-запитів, що дозволяє блокувати рекламу навіть у випадках, коли DNS-фільтрація є недостатньою. Додатково, AdGuard Home забезпечує кращу конфіденційність користувачів завдяки гнучкішим можливостям контролю трафіку.

З погляду продуктивності, Pi-hole демонструє високу стабільність навіть на малопотужних пристроях, зокрема на Raspberry Pi, ефективно обробляючи великі обсяги DNS-запитів без значних затримок. AdGuard Home також є продуктивним інструментом, однак за наявності увімкнених додаткових можливостей, як-от фільтрація HTTP, можливе деяке зниження швидкодії при інтенсивному навантаженні.

Моніторинг і звітність у Pi-hole представлено у вигляді базових графіків та статистичних даних, які надають загальну інформацію про кількість запитів, частку заблокованої реклами та активність у мережі. AdGuard Home у цьому аспекті надає користувачеві більше аналітичних інструментів — його інтерфейс дозволяє проводити глибший аналіз, фільтрувати статистику за типами запитів, джерелами трафіку тощо, що робить звітність набагато інформативнішою.

У контексті підтримки додаткових функцій Pi-hole має певні обмеження. Його основна перевага — простота, а для розширення функціоналу необхідно встановлювати сторонні плагіни чи додаткове програмне забезпечення. Натомість AdGuard Home надає широкий набір вбудованих можливостей, включаючи гнучкі правила фільтрації, можливість імпортувати та налаштовувати списки блокування, а також проводити фільтрацію за HTTP-запитами без потреби у сторонньому втручанні.

Нарешті, обидва рішення забезпечують зручну інтеграцію з іншими

пристроями в мережі. Pi-hole легко налаштовується як DNS-сервер на рівні маршрутизатора, що дозволяє автоматично застосовувати фільтрацію до всіх пристроїв у локальній мережі. AdGuard Home також пропонує таку функціональність, але додатково підтримує підключення через VPN і використання різноманітних протоколів, що розширює можливості його використання за межами локальної мережі.

Таким чином, обидва сервіси є ефективними рішеннями для фільтрації реклами, однак AdGuard Home завдяки ширшій функціональності та зручнішому інтерфейсу частіше обирається тими користувачами, які прагнуть більш комплексного контролю над трафіком. У свою чергу, Pi-hole залишається надійним, легким у використанні варіантом для базового блокування реклами з мінімальними витратами ресурсів.

Pi-hole і AdGuard Home є потужними інструментами для фільтрації реклами та блокування шкідливих доменів, але вибір між ними залежить від вимог до функціональності та простоти використання. Якщо потрібно рішення, яке швидко налаштовується і працює на Raspberry Pi з мінімальними налаштуваннями, Pi-hole є відмінним вибором. Якщо ж користувач хоче більш широкий спектр можливостей для фільтрації, зокрема HTTP-фільтрацію, та детальнішу статистику, AdGuard Home стане кращим варіантом.

4.6. Узагальнення результатів та рекомендації для користувачів

Узагальнюючи результати порівняльного тестування Pi-hole та AdGuard Home, можна зробити висновок, що обидва рішення ефективно справляються з основним завданням — блокуванням небажаної реклами та шкідливих запитів у мережі. Водночас вони орієнтовані на дещо різні аудиторії та мають свої сильні сторони, які слід враховувати при виборі.

Pi-hole — це просте, стабільне і легке рішення, яке чудово підходить для користувачів, які шукають базовий захист від реклами на рівні DNS. Його основними перевагами є легка інсталяція, низькі вимоги до ресурсів, а також

висока стабільність роботи навіть на малопотужному обладнанні. Pi-hole буде оптимальним вибором для тих, хто хоче запустити фільтрацію в домашній мережі без зайвих ускладнень і глибокої технічної підготовки.

AdGuard Home, у свою чергу, демонструє ширший функціонал, що включає фільтрацію не лише DNS-запитів, а й HTTP-трафіку. Це робить його привабливим для просунутих користувачів або тих, хто прагне мати повніший контроль над мережевим трафіком, включаючи можливість налаштування детальних правил, перегляду розширеної статистики та використання списків блокування. Хоча AdGuard Home вимагає дещо більше ресурсів і часу на налаштування, він надає користувачеві гнучкість і функціональність, недоступну в Pi-hole без додаткових розширень.

Для домашніх користувачів, які цінують простоту та надійність, доцільніше зупинитися на Pi-hole. Водночас, якщо є потреба у розширених можливостях моніторингу, детальній фільтрації, інтеграції з різними пристроями та глибших налаштуваннях, кращим вибором буде AdGuard Home.

ВИСНОВКИ

У рамках даної роботи було реалізовано систему фільтрації реклами в локальній мережі на базі мікрокомп’ютера Raspberry Pi із використанням рішень Pi-hole та AdGuard Home. В процесі дослідження проаналізовано принципи роботи DNS-фільтрації, виконано встановлення та конфігурацію необхідного програмного забезпечення, проведено інтеграцію з DHCP-сервером, реалізовано базові заходи з безпеки, а також здійснено тестування продуктивності системи в реальних умовах.

Було встановлено, що система DNS-фільтрації здатна значно знизити кількість рекламного контенту на клієнтських пристроях без потреби встановлення додаткового ПЗ на самі пристрої. Такий підхід дозволяє централізовано контролювати мережевий трафік та захищати користувачів від потенційно небезпечних доменів.

Порівняльний аналіз Pi-hole та AdGuard Home продемонстрував, що обидва інструменти є ефективними, проте мають свої переваги залежно від вимог користувача. Pi-hole характеризується легкістю у налаштуванні та стабільністю, тоді як AdGuard Home пропонує ширший функціонал, зокрема фільтрацію HTTP-запитів і детальну аналітику.

Тестування системи на різних пристроях (ПК, смартфонах, SmartTV) показало стабільну роботу фільтрації незалежно від платформи, а проведений аналіз логів і навантаження підтвердив можливість масштабування рішення в межах домашньої або невеликої офісної мережі. Продуктивність системи, заснованої на Raspberry Pi 4, виявилась достатньою для обробки десятків запитів на секунду з прийнятною швидкістю відгуку.

Таким чином, реалізована система є ефективним, доступним і масштабованим рішенням для блокування реклами на рівні мережі, підвищення швидкості завантаження веб-сторінок та загального рівня інформаційної безпеки. Отримані результати свідчать про доцільність впровадження подібних систем у домашньому чи малому корпоративному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

i-hole Docs. (2020). Pi-hole: блокування реклами на рівні DNS. Retrieved from

dGuard Team. (2021). AdGuard Home: система блокування реклами для вашої мережі. Retrieved from https://github.com/AdguardTeam/AdGuardHome

olesnikov, D. (2020). Розробка систем для блокування реклами в сучасних інформаційних системах. Видавництво «IT Solutions».

ozilla Foundation. (2018). AdBlock Plus: Покроковий гід для користувачів.

w Pi-hole Works. (2020). A Deep Dive into Pi-hole’s DNS Filtering. Retrieved from

aspersky Lab. (2021). Захист від онлайн-реклами: нові методи боротьби. Retrieved

ills, J. (2019). Ad-blocking for Beginners: A User’s Guide. Technology and Privacy