Міністерство освіти і науки України
Криворізький національний університет
Кафедра моделювання та програмного забезпечення

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти бакалавра

зі спеціальності 121 – Інженерія програмного забезпечення

На тему: Розробка утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками ОС Windows

Засвідчую, що в цій кваліфікаційній роботі немає запозичень із праць інших авторів без відповідних посилань.
Студент гр. ІПЗ–21-2
_____/ Р.О. Холод /

Керівник кваліфікаційної роботи _____/ Д. В. Швець /

Завідувач кафедри _____/ А. М. Стрюк /

Кривий Ріг
2025

Криворізький національний університет

Факультет: Інформаційних технологій

Кафедра: Моделювання та програмного забезпечення

Ступінь вищої освіти: бакалавр

Спеціальність: 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:

Зав. кафедри

_____ А. М. Стрюк

«____» _____ 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу

студенту групи ІПЗ–21-2 Холоду Роману Олександровичу

1. Тема: «Розробка утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками ОС Windows» затверджена наказом по КНУ № 200с від «10» квітня 2025 р.
2. Термін подання студентом закінченої роботи: «30» травня 2025 р.
3. Вихідні дані по роботі: розроблені утиліти мають забезпечити реалізацію блокування реклами при роботі в операційній системі Windows.
4. Зміст пояснювальної записки (перелік питань, що їх треба розробити): провести аналіз існуючих на ринку аналогічних програмних продуктів, обґрунтувати функціонал розроблюваної системи, створити програмне забезпечення, здійснити тестування розробленого додатку.
5. Перелік ілюстративного матеріалу: функціональна схема, блок–схема алгоритму, зображення екранних форм додатку.

Календарний план:

№	Найменування етапів кваліфікаційної роботи	Термін виконання етапів роботи
1	Розгляд літературних джерел та пошук інтернет-ресурсів з заданої тематики	06.01.25 – 21.01.25
2	Аналіз існуючих методів вирішення проблеми	22.01.25 – 06.02.25
3	Формулювання актуальності роботи і постановка завдань	07.02.25 – 18.02.25
4	Оформлення матеріалів першого розділу роботи	19.02.25 – 07.03.25
5	Створення функціональної системи та алгоритму додатку	08.03.25 – 18.03.25
6	Оформлення матеріалів другого розділу роботи	19.04.25 – 07.04.25
7	Розробка баз даних, інтерфейсу програмного забезпечення, програмних модулів	08.04.25 – 01.05.25
8	Оформлення додатків	02.05.25 – 07.05.25
9	Тестування розробленої програми	08.05.25 – 15.05.25
10	Оформлення пояснювальної записки	16.05.25 – 29.05.25

Дата видачі завдання: «05» січня 2025 р.

Студент: _____ / Р. О. Холод /

Керівник роботи: _____ / Д. В. Швець /

РЕФЕРАТ

РЕКЛАМА, ФІЛЬТРАЦІЯ, УТИЛІТА, СЕРФІНГ, HOSTS, DNS, WINDOWS.

Пояснювальна записка: 57 с., 17 рис., 2 дод., 25 джерел.

Мета кваліфікаційної роботи: розробка утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками операційної системи Windows.

Об’єкт проектування: утиліта для фільтрації реклами при веб-серфінгу та роботі з додатками операційної системи Windows.

У теоретичній частині роботи виконано аналіз існуючих на сьогодні аналогічних програмних рішень на ринку. Зазначені сильні та слабкі сторони існуючих програмних продуктів. Обґрунтовані актуальність роботи, мета та сформульовані завдання для розробки зазначеної системи.

У практичній частині кваліфікаційної роботи реалізовано функціональну схему розроблюваного продукту та алгоритм його роботи. Розроблено інтерфейс програмного продукту, програмну логіку роботи додатку. Проведено тестування розробленого програмного забезпечення.

Розроблена утиліта для фільтрації реклами при веб-серфінгу та роботі з додатками операційної системи Windows може бути корисна як для досвідчених користувачів, які бажають реалізовувати контроль над мережевими підключеннями, так і для тих, хто просто хоче заблокувати рекламу та інший небажаний вміст.

ABSTRACT

ADVERTISING, FILTERING, UTILITY, SURFING, HOSTS, DNS, WINDOWS.

Explanatory note: 57 p., 17 fig., 2 app., 25 references.

The aim of the qualifying work: development of a utility for filtering ads while surfing the web and working with Windows applications.

Design object: a utility for filtering ads while surfing the web and working with Windows applications.

In the theoretical part of the work, an analysis of today's similar software decisions in the market have executed. The strengths and weaknesses of existing software products have listed. The urgency of work, the purpose, and the objectives for developing the specified system have formulated.

The functional scheme of the developed product and its algorithm has realized in the practical part of the qualification work. The interface of the software product, the program logic of the application have developed. The developed software has tested.

The developed utility for filtering ads while surfing the web and working with Windows applications can be useful both for advanced users who want to exercise control over network connections and for those who simply want to block ads and other unwanted content.

ЗМІСТ

ВСТУП

Сьогодні реклама стала невід'ємною частиною повсякденного досвіду користувача при роботі з комп'ютером. Вона супроводжує людину під час веб-серфінгу, використання мобільних пристроїв, а також настільних додатків у середовищі операційних систем настільних комп'ютерів. Багато компаній інтегрують рекламні оголошення у свої продукти з метою монетизації, проте надмірна кількість такої реклами часто має нав'язливий характер, негативно впливає на продуктивність системи, уповільнює завантаження сторінок і додатків, а також іноді створює загрозу безпеці за рахунок можливих зловмисних посилань або фішингових елементів.

Проблема наявності надлишкової реклами викликає потребу в ефективних методах її блокування. Серед найпоширеніших підходів можна виокремити використання розширень для браузерів, фільтрацію на рівні мережі та зміну DNS-серверів. Кожен з цих методів має свої переваги та недоліки.

З урахуванням постійного зростання обсягів реклами, постає нагайна потреба у створенні програмного засобу, який автоматизує процес фільтрації реклами в операційних системах. Такий інструмент дозволить користувачам зменшити обсяг небажаної інформації, підвищити комфорт роботи за комп'ютером, а також посприяти безпеці при взаємодії з мережевими ресурсами. Розробка подібної утиліти є актуальним завданням для фахівця у сфері програмного забезпечення та може зекономити велику кількість часу для її користувачів.

Кваліфікаційна робота містить вступ, три основних розділи, висновки, список використаних літературних та електроних джерел і додатки. У дослідженні розглядається проблема стрімкого розповсюдження інтернет-реклами та актуальні методи її блокування, аналізуються існуючі програмні засоби фільтрації, описується процес розробки утиліти для автоматизованого блокування рекламних джерел в операційній системі Windows, а також

наводяться результати тестування розробленого програмного забезпечення та приклади його використання в реальних умовах. Запропонована програма може знайти застосування у широкому колі користувачів незалежно від їх рівня підготовки, та дозволить зменшити використання трафіку та завантаженість мережі, а також допоможе зконцентруватися на виконанні потрібних задач без відволікання на нав'язливі рекламні повідомлення.

1 ОГЛЯД ПРОБЛЕМИ НАЯВНОСТІ ІНТЕРНЕТ-РЕКЛАМИ ТА ШЛЯХІВ ЇЇ БЛОКУВАННЯ В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS

1.1 Актуальність питання блокування реклами в операційній системі Windows

Користувачі щодня взаємодіють з великою кількістю контенту через різні засоби комунікації. Реклама стала постійним супутником цього процесу. Операційна система Windows, яка є найбільш поширеною серед настільних ОС у світі, не є винятком — реклама може з'являтися не лише у веб-браузерах, але й у додатках, системних інтерфейсах (наприклад, у меню «Пуск» або на екрані блокування), а також у вигляді нав'язливих спливаючих вікон, повідомлень та банерів.

Реклама, яка завантажується з зовнішніх серверів, може становити загрозу для безпеки та стабільності роботи комп'ютера. У багатьох випадках така реклама не є просто графічним зображенням чи текстовим оголошенням — вона може містити шкідливі скрипти, які виконуються у фоновому режимі без відома користувача. Ці скрипти можуть збирати особисту інформацію, історію переглядів, натискання клавіш, дані про встановлені програми або апаратне забезпечення, що створює серйозні ризики порушення конфіденційності та витоку даних. Така прихована активність називається телеметрією, і хоча іноді вона використовується в легальних цілях (наприклад, для аналітики), у руках недобросовісних розробників або зловмисників вона може стати інструментом шпигунства чи соціальної інженерії.

Крім загроз безпеці, реклама суттєво впливає на продуктивність системи. Кожен рекламний блок — це додатковий запит до сервера, завантаження зображення, відео або JavaScript-компонентів. У великій кількості такі елементи споживають значні обсяги оперативної пам'яті та процесорного часу. Це призводить до уповільнення роботи як окремих

додатків, так і всієї операційної системи загалом. На комп'ютерах із застарілим або слабким апаратним забезпеченням це може проявлятися у вигляді затримок при завантаженні сторінок, зниження чутливості інтерфейсу, зависань або збоїв у роботі.

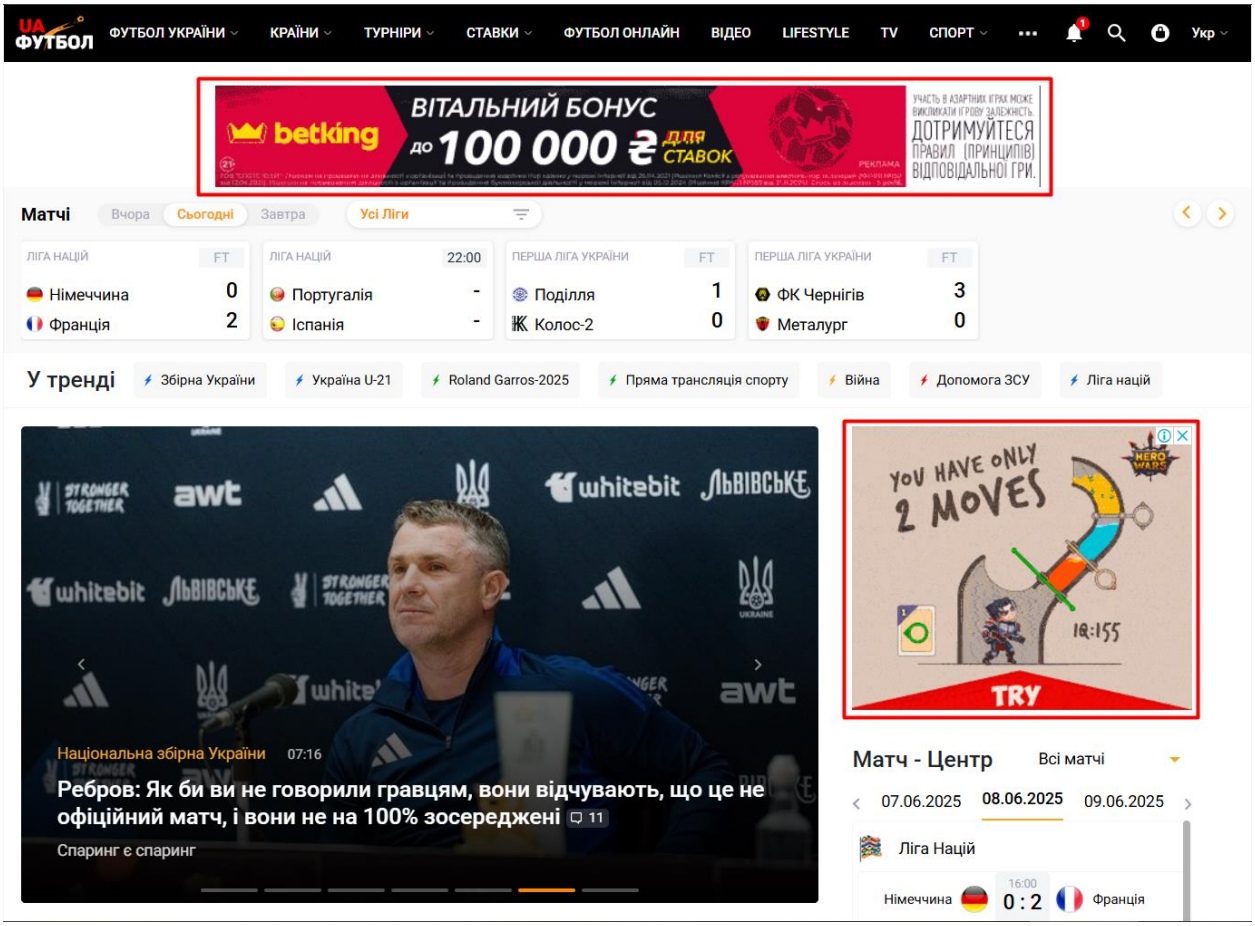

Рисунок 1.1 – Рекламні вставки на одному з популярних спортивних порталів

Крім того, постійне завантаження рекламного контенту призводить до суттєвого збільшення мережевого трафіку. Для користувачів із обмеженим тарифом на передачу даних, наприклад у сільських районах або при використанні мобільного інтернету, це може означати перевитрату трафіку, додаткові витрати або зниження швидкості з'єднання після досягнення ліміту. Таким чином, реклама не тільки нав'язує небажаний контент, але й впливає на вартість та якість інтернет-доступу для кінцевого користувача.

У сукупності ці фактори роблять проблему нав’язливої реклами в середовищі Windows актуальною та такою, що потребує ефективних і системних рішень для її подолання.

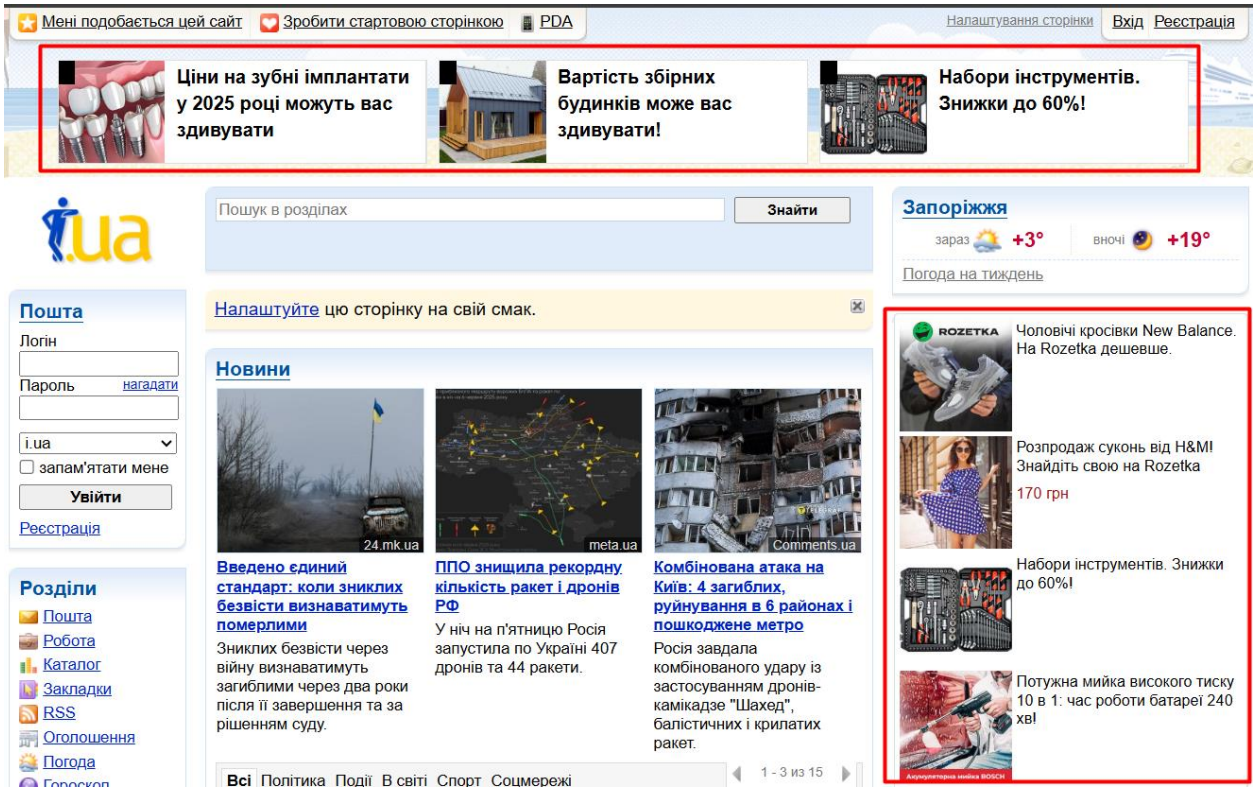

Рисунок 1.2 – Рекламні вставки на одному з поштових порталів

Попри наявність численних засобів блокування реклами, вони охоплюють лише вузький спектр застосувань і не вирішують проблему реклами на рівні всієї системи. Саме тому виникає необхідність у системних рішеннях, які забезпечують глобальну фільтрацію небажаного контенту незалежно від того, яке програмне забезпечення його генерує.

Зважаючи на вищезазначене, розробка утиліти для централізованого блокування реклами в середовищі Windows є актуальним і практично значущим завданням, яке дозволяє підвищити безпеку, комфорт та продуктивність користувацької роботи з комп’ютером.

1.2 Шляхи блокування реклами в операційній системі Windows

У боротьбі з нав'язливою рекламою в операційній системі Windows користувачам доступна низка методів, які відрізняються за рівнем впливу на систему, ефективністю та складністю реалізації. Вибір конкретного способу залежить від технічних знань користувача, цілей блокування (веб-реклама, системна або реклама в додатках), а також від потреб у централізованому або локальному керуванні процесом фільтрації.

Найпоширенішим підходом до блокування реклами є використання розширень для веб-браузерів. Такі розширення, як AdBlock [1], uBlock Origin [2], Ghostery [3] та інші, дозволяють ефективно фільтрувати контент на веб-сайтах, блокуючи завантаження рекламних елементів, спливаючих вікон, трекерів та аналітичних скриптів.

Розглянемо детальніше розширення AdBlock.

AdBlock [1] є одним із найпоширеніших розширень для веб-браузерів, яке забезпечує ефективне та швидке блокування реклами в Інтернеті. Його основний принцип функціонування ґрунтується на використанні так званих фільтраційних списків, що містять набір правил для виявлення і блокування елементів веб-сторінок, пов'язаних із рекламою. Під час завантаження сайту AdBlock аналізує його вміст і перешкоджає завантаженню тих елементів, які відповідають ознакам рекламного чи трекерного контенту. Завдяки цьому користувач бачить очищену від банерів, відеореклами та спливаючих вікон сторінку, що суттєво підвищує зручність веб-серфінгу.

Популярність AdBlock пояснюється простотою встановлення, автоматичною роботою без потреби у складному налаштуванні та зручним інтерфейсом для внесення змін або винятків. Розширення дозволяє блокувати рекламу практично на будь-якому сайті, у тому числі в соціальних мережах і на деяких відеоплатформах. При цьому воно забезпечує певний рівень конфіденційності, адже здатне фільтрувати й елементи, що відповідають за збір даних про користувача.

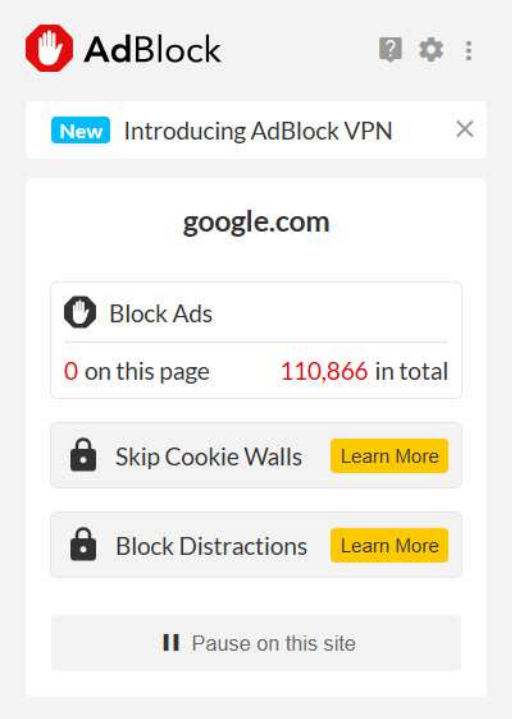

Рисунок 1.3 – AdBlock

Однак, останнім часом великі платформи, наприклад YouTube, вдаються до активної протидії блокувальникам, виводячи повідомлення про неможливість перегляду відео або змінюючи спосіб подачі реклами так, щоб вона обходила фільтрацію. Також деякі користувачі критикують AdBlock за наявність політики "допустимої реклами", яка дозволяє частині рекламодавців залишати ненав’язливу рекламу активною, що, з точки зору багатьох, суперечить ідеї повного блокування.

Ще одним схожим рішенням є uBlock Origin [2], що являє собою розширення для веб-браузерів, яке призначене для блокування небажаного вмісту. На відміну від аналогів, воно орієнтується не лише на кінцевий ефект, а й на ефективність використання системних ресурсів, що робить його привабливим для користувачів із застарілими або слабкими пристроями. Архітектура uBlock Origin побудована таким чином, щоб мінімізувати споживання оперативної пам’яті та процесорного часу навіть при великій кількості активних фільтраційних правил.

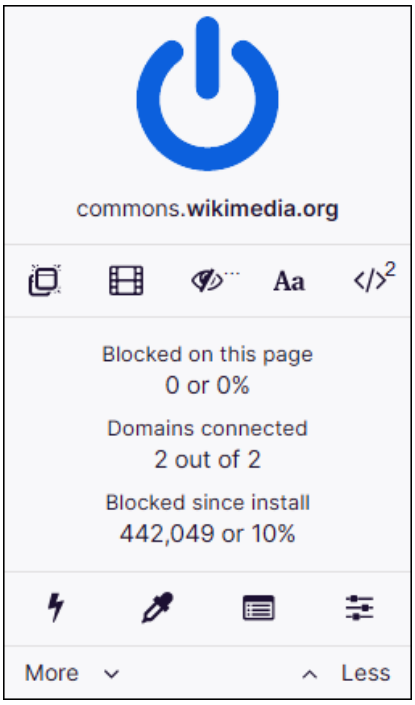

Рисунок 1.4 – uBlock Origin

Розробка цього інструменту з самого початку орієнтувалася на прозорість, відкритий код та відсутність будь-якої комерційної моделі, що виключає можливість платної "допустимої реклами" та співпраці з рекламодавцями. uBlock Origin дозволяє гнучко керувати як готовими фільтраційними списками, так і створювати власні правила, враховуючи індивідуальні потреби користувача. Він підтримує великий вибір джерел фільтрації, зокрема списки для блокування реклами, аналітики, трекінгу, фішингових сайтів і потенційно небезпечного програмного забезпечення.

Однією з позитивних сторін uBlock Origin є його глибока інтеграція в механізм аналізу DOM-структури сторінки, що дозволяє блокувати окремі елементи ще до їх завантаження або взаємодії з браузером. Це забезпечує високий рівень захисту від прихованих скриптів і мережевих викликів, які використовуються для збору телеметрії чи створення цифрових відбитків користувача. З іншого погляду, uBlock Origin часто розглядають не лише як блокувальник реклами, а як базовий компонент безпеки при роботі в мережі.

В той же час, uBlock Origin демонструє глибший рівень фільтрації і є більш технічно вивіреним, ніж більшість аналогів. Його можливості цінують просунуті користувачі, які прагнуть контролювати онлайн-трафік, формуючи власні правила доступу до контенту. Завдяки відкритості, відсутності комерційного впливу та технічній досконалості uBlock Origin сьогодні вважається непоганим рішеням для блокування небажаного контенту в браузері.

Попри високу ефективність у блокуванні реклами під час веб-серфінгу, як AdGuard, так і uBlock Origin мають суттєве обмеження — їх дія зосереджена виключно в межах браузера. Це означає, що реклама, яка з'являється в системному інтерфейсі Windows або в десктопних застосунках, залишається поза сферою їх впливу. Обидва інструменти не здатні забезпечити повноцінний системний захист від рекламного контенту. Окрім того, сучасні вебсайти дедалі частіше використовують динамічне завантаження реклами, що дозволяє частково обходити правила фільтрації та знижує ефективність браузерних рішень.

Ще одним методом є застосування спеціалізованого програмного забезпечення для фільтрації мережевого трафіку. До таких програм належать локальні проксі-сервери, фаєрволи або мережеві фільтратори, що аналізують вхідні та вихідні запити, дозволяючи блокувати рекламу ще до її завантаження. Приклади таких рішень – NextDNS [4], Pi-hole [5]. Ці засоби забезпечують системну фільтрацію, однак потребують глибших технічних знань для налаштування, іноді потребують встановлення сертифікатів для перехоплення HTTPS-запитів або створення додаткових мережевих маршрутів. Розглянемо їх детальніше.

NextDNS [4] представляє собою хмарне рішення для блокування реклами, і небажаного контенту, яке працює на рівні DNS-запитів. Його головна особливість полягає в тому, що замість локального встановлення фільтрів на пристрої чи в браузері, фільтрація відбувається через хмарний

DNS-сервер, що дозволяє захищати весь трафік незалежно від застосунків або операційної системи.

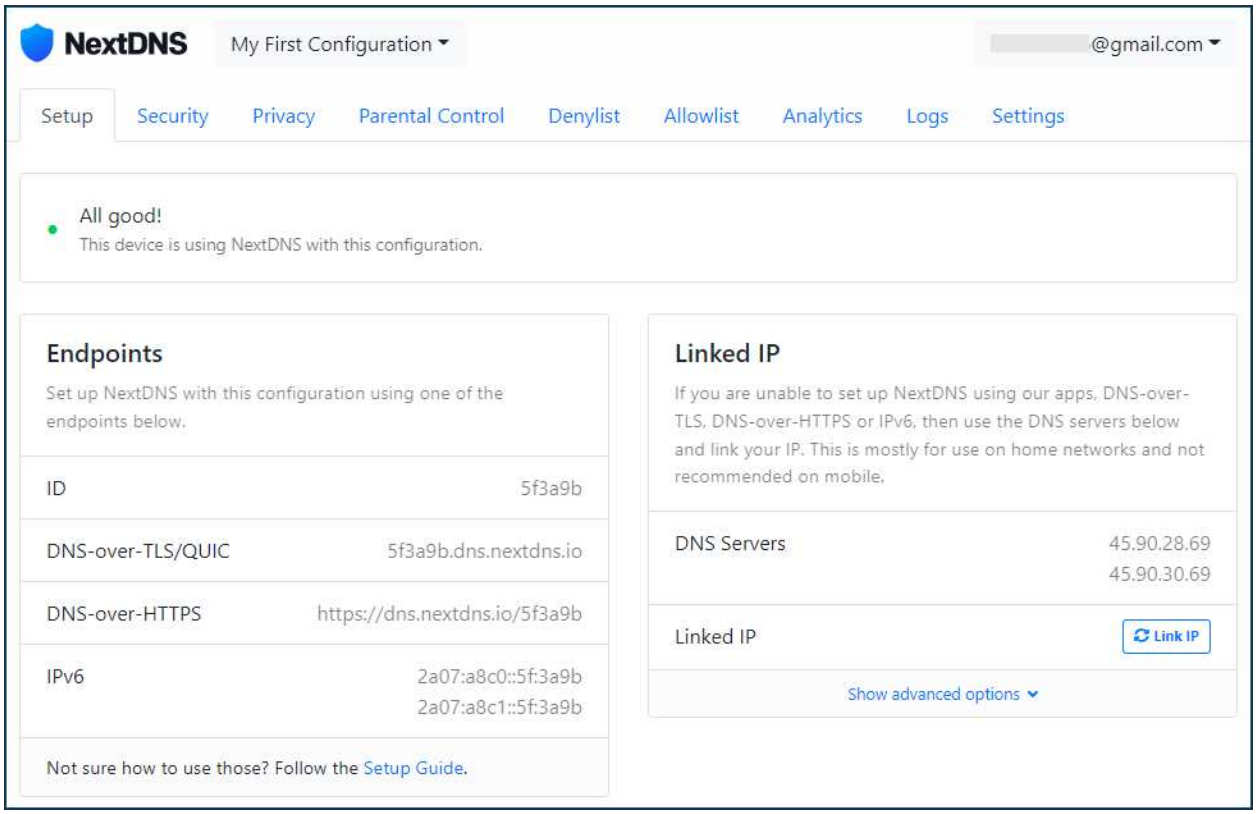

Рисунок 1.5 – NextDNS

Користувач реєструється на сайті NextDNS і отримує унікальний DNS-профіль. Далі необхідно вказати відповідні DNS-адреси у налаштуваннях мережі пристрою, маршрутизатора або використовувати офіційні додатки для відповідної операційної системи. Після цього весь DNS-трафік спрямовується через сервери додатку, де проходить фільтрацію відповідно до вибраних правил.

Функціонал NextDNS дозволяє не тільки блокувати рекламу, але й здійснювати фільтрацію трекерів, контроль часу доступу до ресурсів, а також аналіз DNS-запитів у реальному часі. Також можна створювати власні блокувальні списки або використовувати популярні публічні списки, наприклад EasyList [6], OISD [7] тощо. Важливо, що обробка запитів

здійснюється швидко завдяки глобальній мережі серверів компанії, що забезпечує низьку затримку і успішну роботу.

Крім фільтрації, сервіс має функції захисту від фішингу та зловмисного програмного забезпечення, виявлення запитів від трекерів, які часто використовуються в телеметрії Windows, і навіть здатен запобігати передачі даних до серверів Google, Facebook, Amazon та інших компаній, якщо це налаштовано в профілі.

Ще одним схожим рішенням є Pi-hole [5]. Це локальне мережеве рішення для блокування реклами та трекерів, яке також функціонує як DNS-сервер, що фільтрує небажані запити ще до того, як вони потрапляють до користувацьких пристроїв.

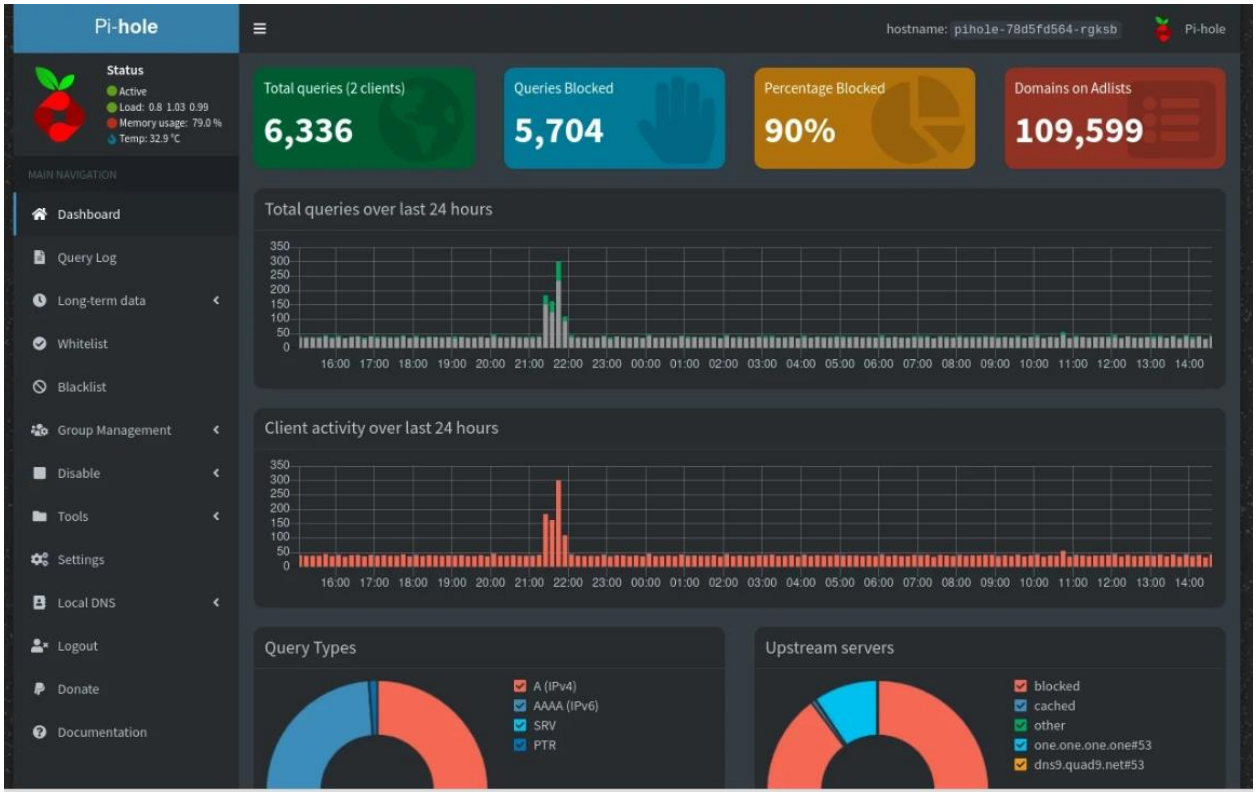

Рисунок 1.6 – Pi-hole

Його принцип роботи полягає в перенаправленні запитів до відомих рекламних і аналітичних доменів у "порожнечу", фактично запобігаючи завантаженню рекламного контенту в браузерах, програмах і мобільних

аплікаціях. Це дає змогу здійснювати фільтрацію на рівні всієї мережі, охоплюючи всі пристрої — від комп’ютерів до "розумних" телевізорів чи IoT-пристроїв.

Встановлення Pi-hole зазвичай відбувається на одноплатному комп’ютері, наприклад Raspberry Pi [8], або на будь-якому іншому пристрої в локальній мережі, який постійно працює. Після цього достатньо переналаштувати DNS на маршрутизаторі або вручну на окремих пристроях, щоб трафік почав проходити через Pi-hole. Завдяки централізованому підходу він дозволяє забезпечити контроль над DNS-запитами всередині локальної мережі та ефективно блокувати сторонній контент незалежно від платформи або програмного середовища.

Інтерфейс Pi-hole надає непогані аналітичні можливості — користувач може в режимі реального часу спостерігати за кількістю DNS-запитів, їх джерелами, а також бачити, які домени було заблоковано. Це корисно для моніторингу активності в мережі, виявлення підозрілих джерел або обмеження доступу до небажаного вмісту. Користувач може вручну додавати або виключати списки блокування, створювати власні правила, а також інтегрувати додаткові механізми захисту — наприклад, бази даних зі шкідливими доменами.

На відміну від хмарних сервісів, Pi-hole повністю контролюється користувачем і не потребує зовнішніх серверів або сторонніх акаунтів. Це робить його привабливим з погляду конфіденційності, оскільки всі DNS-запити обробляються локально й не передаються у зовнішні системи. Завдяки відкритому коду та активній спільноті, можливості Pi-hole час від часу розширюються: його можна поєднувати з DHCP-сервером, VPN або інтегрувати у складніші інфраструктури домашньої мережі.

Коментуючи описаний підхід захисту, варто зазначити, що робота NextDNS залежить від зовнішньої хмарної інфраструктури, тому всі DNS-запити передаються через сторонні сервери, що може викликати сумніви у

користувачів, які надають перевагу повному локальному контролю над даними.

Цієї вади позбавлений Pi-hole, але його головна слабкість полягає у необхідності ручного налаштування та адміністрування, що є очевидно складним для недосвідчених користувачів. До того ж система вимагає постійно увімкненого пристрою в локальній мережі, що створює додаткове навантаження на енергоспоживання або потребує придбання окремого обладнання.

Крім того, Pi-hole не фільтрує трафік, що проходить поза DNS (наприклад, у разі жорстко прописаних IP-адрес або DNS-over-HTTPS [9]), а отже, не гарантує повне блокування реклами в усіх сценаріях. Для обходу таких обмежень часто потрібна складніша конфігурація або інтеграція з іншими інструментами, як-от локальні фаєрволи чи VPN-сервіси.

На рівні операційної системи Windows одним із найбільш доступних і водночас ефективних способів є використання системного файлу *hosts* [10]. Цей текстовий файл, розташований зазвичай за шляхом *C:\Windows\System32\drivers\etc\hosts*, відповідає за локальну відповідність доменних імен конкретним IP-адресам до того, як система звернеться до зовнішнього DNS-сервера.

Принцип дії полягає у тому, що будь-який запит до зазначеного у файлі домену автоматично перенаправляється на вказану IP-адресу. Якщо, наприклад, у файлі вказано, що *ads.example.com* відповідає IP *0.0.0.0*, то при спробі доступу до цього ресурсу комп’ютер миттєво отримає "порожню" відповідь, оскільки ця адреса не відповідає жодному реальному серверу. У результаті рекламний вміст або трекер просто не зможе завантажитися.

Цей метод має низку переваг: він не потребує встановлення стороннього програмного забезпечення, працює на системному рівні незалежно від браузера чи інших програм і забезпечує високий рівень продуктивності, оскільки не вимагає додаткових обчислювальних ресурсів. Файл *hosts* може бути наповнений як вручну, так і за допомогою автоматизованих скриптів або

утиліт, які регулярно оновлюють список рекламних і небажаних доменів із публічних джерел.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

Рисунок 1.7 – Вміст файлу *hosts* в операційній системі Windows

Такий підхід ефективно блокує багато відомих рекламних серверів і аналітичних платформ, а також може бути корисним для обмеження доступу до окремих сайтів у навчальному чи корпоративному середовищі.

Також треба зазначити, що при цьому блокування відбувається у всіх програмах, незалежно від типу з’єднання або застосунку, і не потребує встановлення стороннього програмного забезпечення. Основною перевагою цього методу є простота, стабільність, відсутність навантаження на систему та високий рівень сумісності з будь-якими типами інтернет-з’єднання. Однак ручне редагування *hosts* може бути незручним, а його ефективність залежить від актуальності списку заблокованих доменів.

Не дивлячись на це, *hosts*-файл залишається простим, стабільним і перевіреним засобом базової фільтрації, особливо ефективним у поєднанні з іншими методами.

1.3 Оцінка результатів аналізу методів блокування рекламного трафіку та розглянутих програмних рішень

У процесі огляду підходів до блокування реклами в операційній системі Windows було проаналізовано як браузерні розширення, так і системні рішення, зокрема хмарні DNS-сервіси й локальні фільтрувальні інструменти. Кожен із методів має свої особливості і сферу застосування, однак жоден із них не є універсальним без певних компромісів щодо зручності або продуктивності.

На цьому тлі використання системного файлу *hosts* виділяється як простий та ефективний спосіб глобального блокування рекламних доменів. Цей метод не потребує постійної фонової роботи сервісів, не передає дані третім сторонам і працює на базовому рівні операційної системи. Його головна перевага полягає швидкодії, простоті налаштування та повному контролі з боку користувача.

Таким чином, використання *hosts*-файлу є оптимальним вибором для тих, хто прагне до системної фільтрації без зайвих ускладнень. У зв’язку з цим автоматизація процесу його наповнення через проектовану утиліту доцільною й практично необхідною для забезпечення комфортного та безпечного користування комп’ютером.

2 ПРОЕКТУВАННЯ УТИЛІТИ ДЛЯ ФІЛЬТРАЦІЇ РЕКЛАМИ ПРИ ВЕБ-СЕРФІНГУ ТА РОБОТІ З ДОДАТКАМИ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS

2.1 Короткі відомості щодо файлу hosts

Файл *hosts* у Windows є одним із найстаріших та найпростіших інструментів управління мережею на рівні операційної системи. Його основне призначення — ручне або автоматизоване встановлення відповідностей між доменними іменами та IP-адресами до того, як ці запити будуть передані до зовнішнього DNS-сервера.

Таким чином, файл *hosts* фактично дозволяє локально керувати маршрутизацією інтернет-запитів.

Синтаксис записів у цьому файлі доволі простий: кожен рядок містить IP-адресу та доменне ім’я, розділені пробілом або табуляцією. Наприклад:

```
0.0.0.0 ads.example.com
127.0.0.1 telemetry.service.net
```

Ці записи означають, що при зверненні до зазначених доменів операційна система спробує встановити з’єднання із вказаними IP-адресами, які, у випадку 0.0.0.0 або 127.0.0.1, фактично не ведуть до реального ресурсу, що робить завантаження реклами неможливим.

В той же час варто зазначити, що використання адреси 0.0.0.0 є кращим за 127.0.0.1 при блокуванні, оскільки остання може спричинити зайві локальні з’єднання, які хоч і не досягають зовнішнього сервера, але створюють трафік до локального інтерфейсу.

Крім того, один IP-адрес може бути пов'язаний з кількома доменами через пробіл. Система ігнорує порожні рядки, тому для зручності можна структурувати файл групами записів.

```
0.0.0.0 ad1.com ad2.com ad3.net
```

Коментарі починаються з символу # і можуть розміщуватись як на окремому рядку, так і в кінці службового запису.

```
# Приклад коментаря
0.0.0.0 example.com # Блокування домену
```

Файл *hosts* у Windows є системним, тому для його редагування потрібні права адміністратора. Це означає, що користувач повинен запускати текстовий редактор (наприклад, Блокнот) від імені адміністратора, інакше зберегти зміни буде неможливо. Така вимога забезпечує базовий рівень захисту від несанкціонованих змін з боку шкідливого програмного забезпечення або скриптів.

Отже, у контексті теми блокування реклами файл *hosts* є зручним майданчиком для реалізації централізованої фільтрації небажаного трафіку. Розуміння синтаксису його заповнення дозволить перейти до проектування і розробки програмних засобів для фільтрації трафіка. Але спочатку доцільно провести огляд наявних постачальників даних, що пропонують систематизовані списки рекламних доменів.

2.2 Вибір постачальника даних стосовно рекламних доменів

Як зазначалося вище, блокування реклами через модифікацію системного *hosts*-файлу полягає у перенаправленні відомих рекламних, трекерних чи шкідливих доменів на неіснуючі в межах глобальної мережі IP-адреси (0.0.0.0 або 127.0.0.1). Існує кілька відомих проєктів зі списками таких доменів. Серед безкоштовних найбільш комплексним є StevenBlack’s Unified Hosts [11] – він «консолідує» кілька авторитетних *hosts*-файлів в один [12]. Наразі базовий список StevenBlack містить близько 190 тисяч доменів і регулярно оновлюється [11]. Цей файл забезпечує блокування реклами, трекерів та джерел розповсюдження шкідливого програмного забезпечення, а також дозволяє додавати чи виключати окремі категорії – наприклад, є переліки хостів для блокування фейкових новин або соцмереж.

Усі конфігурації StevenBlack сумісні з усіма популярними на сьогоднішній день операційними системами і працюють шляхом інтеграції в системний файл *hosts*. Оновлення можна отримувати автоматично – проєкт розміщений на GitHub [13], тому можна підключати файл як джерело блокувальника (наприклад, через відповідні скрипти чи апаратні рішення на кшталт розглянутого в першому розділі Pi-hole). Завдяки відносно великому обсягу і різнобічному охопленню цей список дає високий рівень фільтрації небажаного контенту при відносно оптимальному розмірі файлу.

На рисунку 2.1 наведено динаміку зміни кількості доменів для фільтрації в переліку StevenBlack [14].

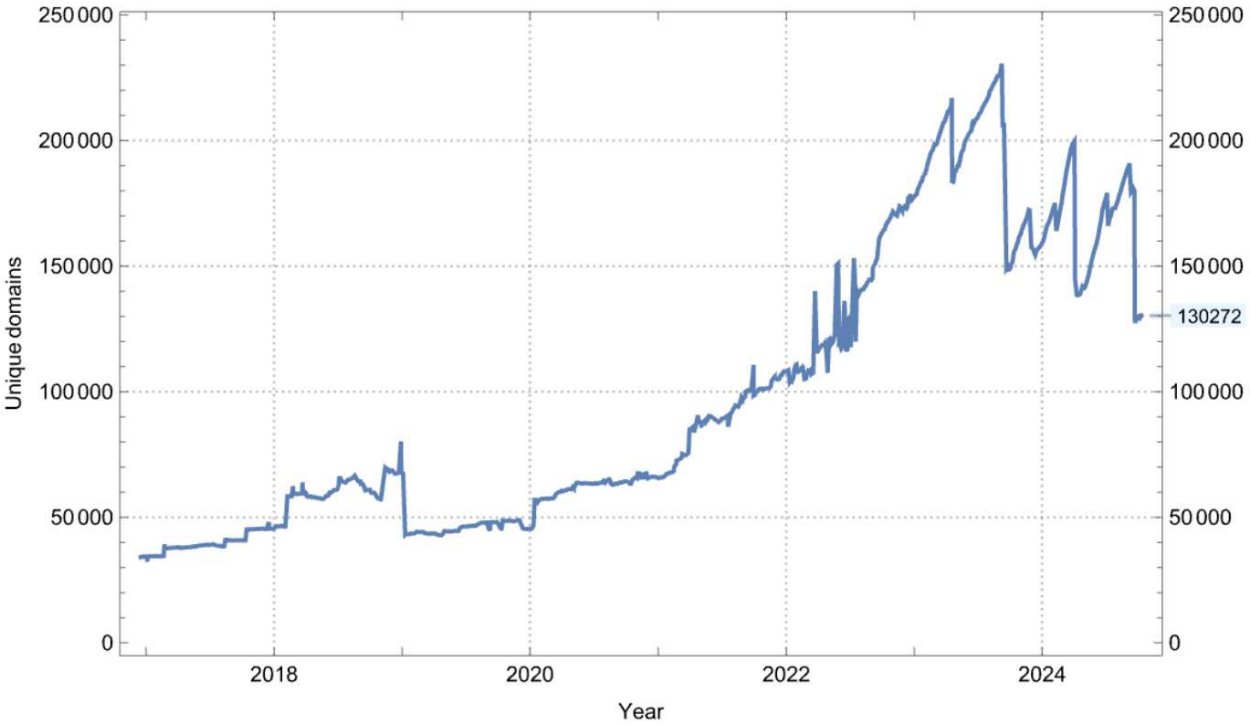

Рисунок 2.1 – Динаміка зміни кількості доменів для фільтрації в переліку StevenBlack

Ще один крупний проєкт – Energized Protection [15], який пропонує декілька варіантів hosts-файлів різного ступеня агресивності фільтрації. Наприклад, варіанти «Adware» та «Malware» охоплюють чотири та п’ять

сотень тисяч доменів відповідно [16,17], а об'єднаний список хостів з усіх категорій налічує понад один мільйон унікальних доменів [18].

Списки Energized також регулярно оновлюються волонтерами, їх можна завантажити з GitHub або дзеркал, щоб синхронізувати через DNS-сервери чи скрипти. Як і у випадку з StevenBlack, ці файли не залежать від ОС – будь-який пристрій, здатний використовувати власний *hosts* або DNS-фільтр, може застосувати їх. Велика кількість записів забезпечує широке покриття реклами, трекерів та шкідливих ресурсів, але водночас вимагає трохи більше ресурсів через встановлення великого файлу *hosts*.

Для мобільних пристроїв під Android поширені більш компактні рішення. Зокрема, AdAway [19] (і його стандартний *hosts*) охоплює головним чином популярні мобільні рекламні домени. За оцінкою спільноти, дефолтний AdAway-файл містить близько 8,8 тис. записів, що займають приблизно третину мегабайту [20].

Він оновлюється досить часто та інтегрується безпосередньо в сам додаток AdAway [21], проте не має спеціальних розширень (тобто підтримує лише блокування основної реклами/аналітики). Порівняно з попередніми списками його обсяг достатньо невеликий, тому і захист реалізується менш всеохопний.

Схожий за задумом достатньо старий проект Dan Pollock's hosts [22] налічує близько 15 тисяч доменів і також регулярно оновлюється [23]. Він призначений для загального блокування реклами та трекерів, але застарів у порівнянні з сучасними рішеннями через меншу базу доменів.

Іншим цікавим варіантом є GoodbyeAds [24] – кураторський *hosts*-файл, орієнтований на мобільні додатки (але сумісний з будь-якою платформою). Він займає менше 5 мегабайт і застосовується для блокування реклами, шкідливих та трекерних доменів. Список регулярно оновлюється автором, який підтримує дзеркало з заголовком Last-Modified для автоматичної синхронізації. Як і AdAway, цей список фокусується насамперед на рекламі та аналітичних скриптах, та не містить розширених модулів на кшталт

соціальних мереж. Завдяки своєму розміру він не створює значного навантаження, але при цьому за замовчуванням неповністю охоплює «широкі» категорії контенту.

Комерційні рішення, своєю чергою, найчастіше базуються на DNS-фільтрації і не пропонують відкритих *hosts*-файлів. Наприклад, сервіси NextDNS або CleanBrowsing [25] блокують рекламу на своєму рівні, використовуючи готові списки EasyList/EasyPrivacy чи власні фільтри, але не розповсюджують звичайних списків для *hosts*-файлів. Теоретично більшість згаданих *hosts*-списків можна імпортувати в DNS-фільтр. Однак на практиці платних *hosts*-стримів мало – частіше такі сервіси пропонують платні підписки на фільтри в інших форматах

Отже, серед усіх порівняних рішень особливу увагу заслуговує проєкт StevenBlack. Він об'єднує кілька популярних *hosts*-файлів (AdAway, Malwaredomains, DanPollock тощо) в один з усуненням дублікатів, що дозволяє одразу блокувати рекламу, трекери, шкідливі та потенційно небажані сайти. Їх список регулярно оновлюється і доступний для широкого загалу операційних систем. Водночас архітектура StevenBlack модульна: користувач може обрати базовий блок та при потребі підключити додаткові набори доменів. За рахунок цього StevenBlack поєднує у собі зручність користування і потужні інструменти фільтрації, при тому що завантажується база доменів у вигляді одного текстового файла. Такий компроміс між обсягом та різноманітністю блокування робить StevenBlack одним із найефективніших *hosts*-ресурсів для блокування реклами в порівнянні з іншими проаналізованими рішеннями.

2.3 Функціональна схема утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками ОС Windows

На рисунку 2.2 наведено функціональну схему утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками операційної системи Windows.

Наведемо детальний опис розробленої функціональної схеми.

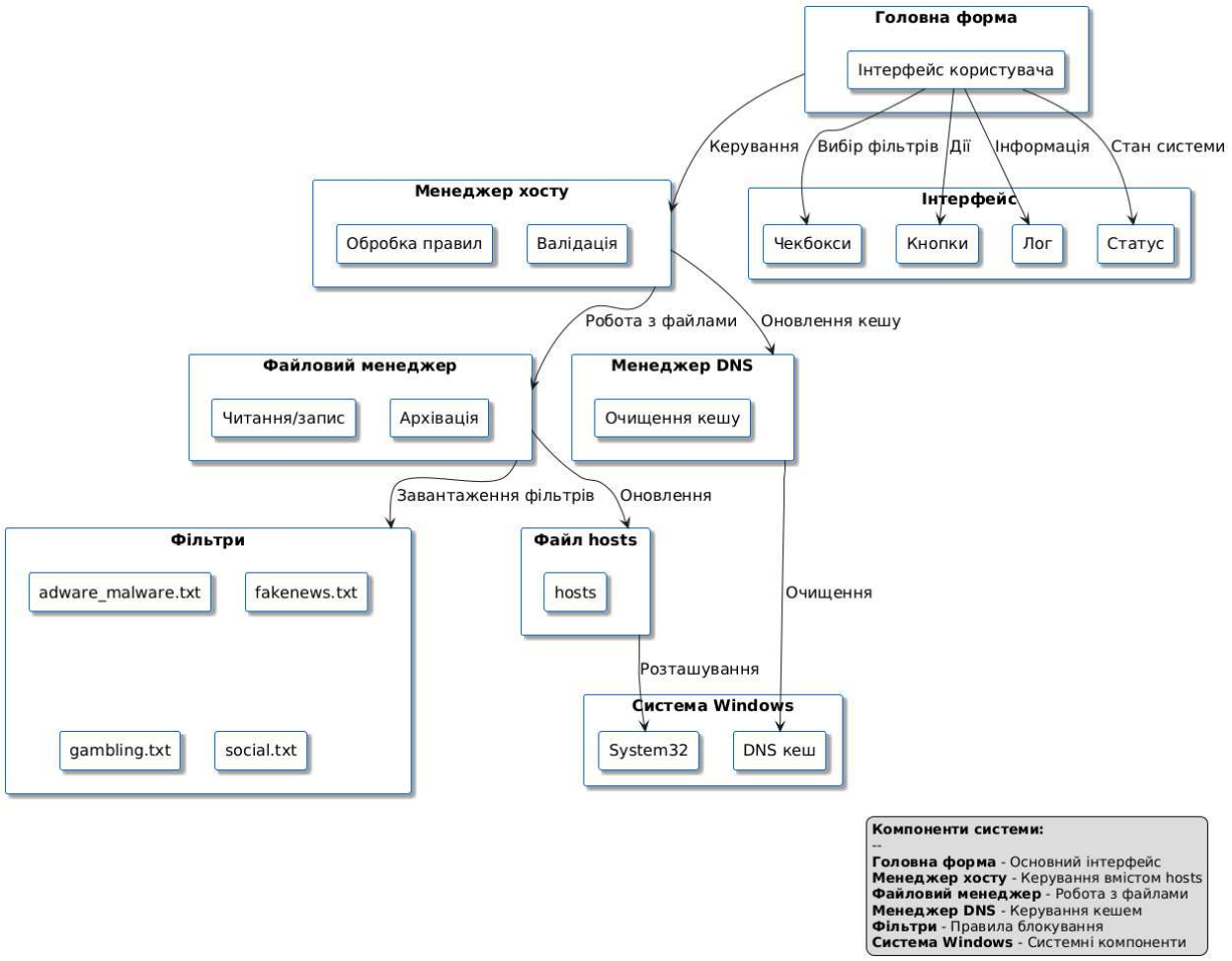

Рисунок 2.2 – Функціональна схема утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками ОС Windows

Головна форма забезпечує взаємодію з користувачем через зрозумілий та ергономічний інтерфейс. Вона відповідає за відображення стану системи та обробку дій користувача, передаючи відповідні команди іншим компонентам.

Менеджер хосту виконує основоположну роль у роботі програми, керуючи вмістом системного файлу *hosts*. Він забезпечує валідацію вхідних даних та обробку правил блокування, перевіряючи їхню коректність перед застосуванням. Цей компонент також відповідає за синхронізацію з іншими частинами системи.

Файловий менеджер забезпечує роботу відповідно з файловою системою. Він відповідає за читання та запис даних, а також створення

резервних копій. Цей компонент забезпечує цілісність даних при оновленні файлу *hosts* та керує сховищем фільтрів.

Менеджер DNS виконує функції з очищення кешу DNS після внесення змін у файл *hosts*. Це забезпечує негайне застосування нових правил блокування без необхідності перезавантаження системи.

Файл *hosts* представлений як окремий об'єкт, що відображає його засадничий статус у системі. Він містить правила перенаправлення мережевих адрес та є основним об'єктом маніпуляцій програми.

Фільтри представлені у вигляді окремого блоку, що містить набори правил для блокування різних категорій вмісту. Кожен фільтр відповідає за певний тип блокування та може бути активований або деактивований користувачем.

Система Windows показана як зовнішнє середовище, з яким взаємодіє програма. Вона включає системні компоненти, такі як каталог System32 та DNS кеш, які є невід'ємною частиною роботи програми.

Інтерфейс користувача деталізовано через набір елементів керування, включаючи чекбокси для вибору фільтрів та кнопки для виконання дій.

Взаємодія між компонентами відбувається за визначеною схемою: користувач взаємодіє з інтерфейсом, який передає команди менеджеру хосту; останній координує роботу файлового менеджера та менеджера DNS для забезпечення коректного оновлення системних налаштувань.

2.3 Алгоритм функціонування утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками ОС Windows

На рисунку 2.3 наведено блок-схему алгоритма функціонування утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками операційної системи Windows. Програма починає свою роботу з перевірки наявності прав адміністратора, що є обов'язковою умовою для коректного функціонування, оскільки робота з системним файлом *hosts* вимагає підвищених привілеїв.

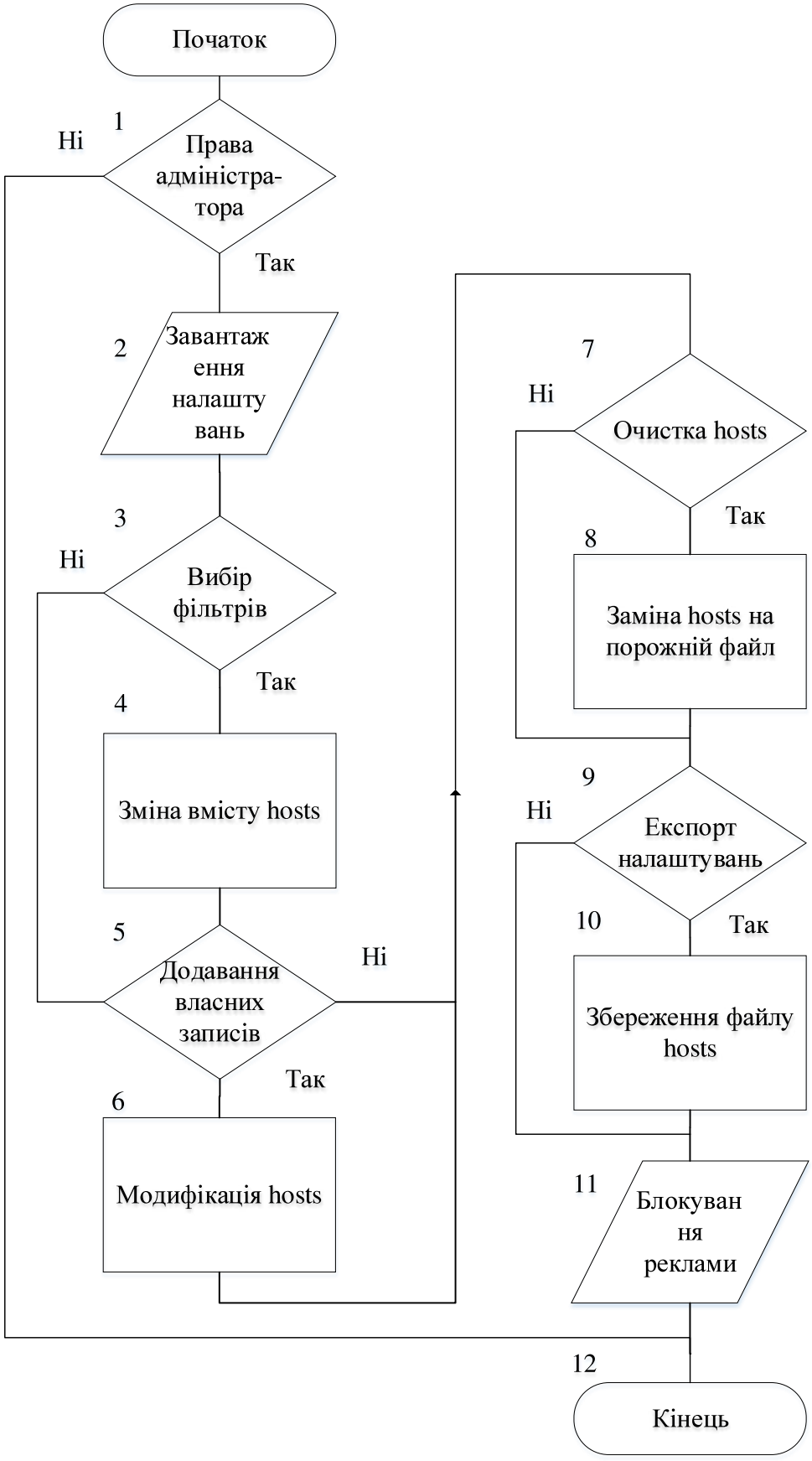

Рисунок 2.3 – Алгоритм роботи утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками операційної системи Windows

При успішній перевірці відбувається ініціалізація інтерфейсу користувача та завантаження збережених налаштувань.

На етапі ініціалізації програма перевіряє наявність необхідних файлів фільтрів. У разі їх відсутності створюються стандартні набори фільтрів для блокування реклами, шкідливого програмного забезпечення, фейкових новин, азартних ігор та соціальних мереж. Це забезпечує готовність програми до роботи відразу після встановлення.

Основний робочий цикл програми базується на очікуванні дій користувача. Користувач має можливість вибирати необхідні фільтри зі списку доступних. При натисканні кнопки застосування змін відбувається збір усіх вибраних фільтрів, після чого створюється нова версія файлу *hosts*, яка заміняє поточну.

Процес оновлення файлу *hosts* включає формування нового вмісту на основі вибраних фільтрів та спробу його запису. У разі успішного запису програма автоматично очищує кеш DNS для застосування змін. У разі виникнення помилок під час запису відбувається автоматичне відновлення з резервної копії, що запобігає втраті даних та забезпечує стабільність роботи операційної системи.

Додатково реалізовано функціонал експорту поточних налаштувань, що дозволяє зберігати конфігурацію для подальшого використання.

Перед завершенням роботи програма автоматично зберігає поточний стан налаштувань.

У разі відсутності необхідних прав адміністратора програма відображає відповідне повідомлення та завершує роботу, запобігаючи можливим проблемам із доступом до системних файлів.

Реалізований алгоритм забезпечує функціонал утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками операційної системи Windows, дозволяючи ефективно керувати блокуванням небажаного контенту через модифікацію файлу hosts. Використання резервних копій, автоматичного створення необхідних файлів та обробки помилок забезпечує

ефективну роботу програми. Зрозумілий та доступний інтерфейс утиліти у поєднанні з продуманим та детально описаним функціоналом робить зпроектовану програму ефективним та зручним інструментом для керування мережевими запитами на рівні операційної системи, та, як наслідок, фільтрації реклами.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ УТИЛІТИ ДЛЯ ФІЛЬТРАЦІЇ РЕКЛАМИ ПРИ ВЕБ-СЕРФІНГУ ТА РОБОТІ З ДОДАТКАМИ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS

3.1 Розгляд створеної утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками операційної системи Windows та кейсів її використання

Зовнішній вигляд головного вікна створеної програми для фільтрації реклами при веб-серфінгу та роботі з додатками наведено на рисунку 3.1.

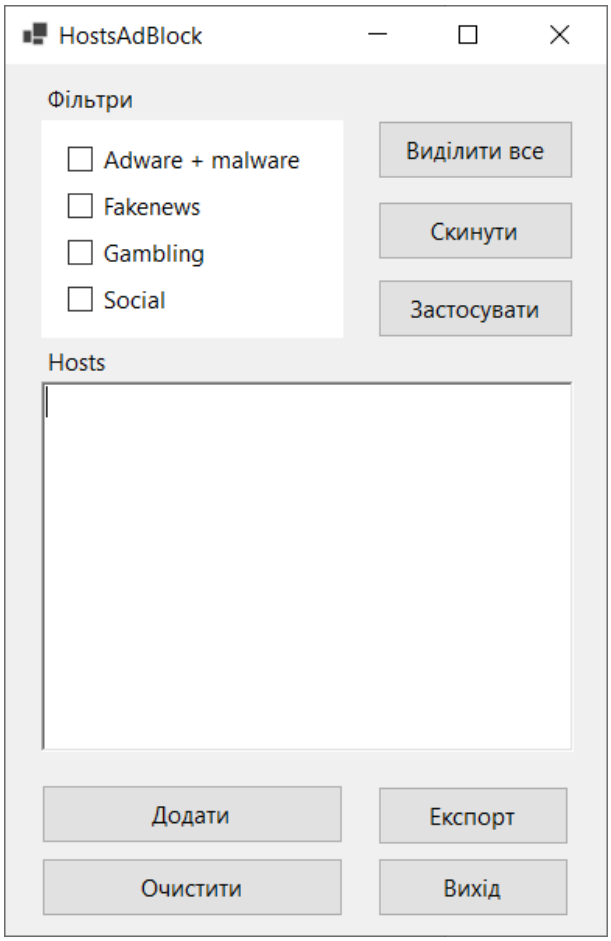

Рисунок 3.1 – Головне вікно створеної утиліти

Перед запуском утиліти необхідно впевнитися, що користувач має права адміністратора в операційній системі. В противному випадку буде показане

повідомлення про необхідність підвищення рівня доступу (рисунок 3.2). Запуск програми відбувається шляхом виконання подвійного кліку на виконуваному файлі HostsAdBlock.exe. При першому запуску створиться директорія DB у каталозі з програмою, де будуть зберігатися файли фільтрів.

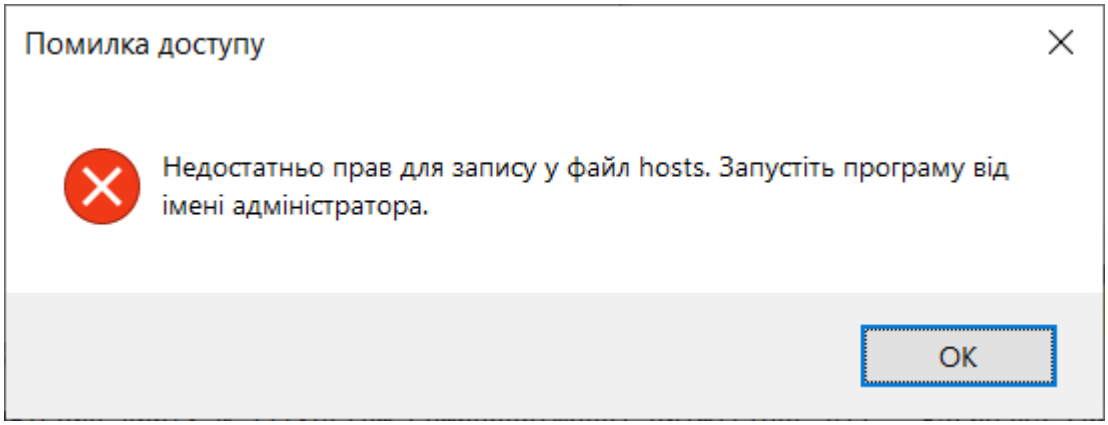

Рисунок 3.2 – Помилка доступу до файла *hosts* через відсутність адміністраторських прав в користувача

Головне вікно програми містить кілька основних елементів керування. У лівій частині зверху розташовано панель з чекбоксами для вибору категорій блокування. Права частина містить кнопки керування, трохи нижче представлено текстове поле для перегляду та редагування вмісту файлу *hosts*.

У блоці "Фільтри" користувач може обрати категорії, які бажає заблокувати (рисунок 3.3).

Рисунок 3.3 – Налаштування фільтрів

Доступні наступні типи блокувань: реклама та шкідливе програмне забезпечення, фейкові новини, азартні ігри та соціальні мережі. Користувачеві необхідно встановити прапорці біля потрібних категорій. Для зручності доцільно використати кнопки "Виділити все" для вибору всіх категорій або "Скинути" для скасування вибору.

Після вибору необхідних фільтрів треба натиснути кнопку "Застосувати". Програма створить резервну копію існуючого файлу *hosts*, після чого оновить його згідно з обраними налаштуваннями. Після успішного оновлення з'явиться повідомлення про успішне завершення операції (рисунок 3.4). При цьому текстове поле під зазначеною кнопкою оновиться та буде містити перелік заблокованих інтернет-джерел, які можна продивитися в повному обсязі з використанням вертикальної прокрутки.

Для застосування змін може знадобитися виконання перезавантаження операційної системи.

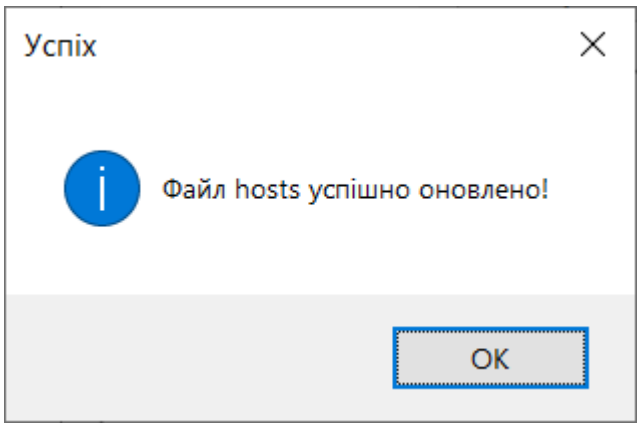

Рисунок 3.4 – Повідомлення про успішне оновлення файлу *hosts*

Якщо користувач хоче додати власні записи, йому необхідно скористатися великим текстовим полем у середній частині вікна. Він можете безпосередньо вносити зміни у вміст файлу *hosts*. Для збереження змін потрібно натиснути кнопку "Додати". При цьому треба мати на увазі, що неправильне форматування може призвести до проблем з мережевим

з'єднанням. Тому потрібно послуговуватися правилами форматування та оформлення переліку хостів, що наведені у розділі 2.1.

На рисунку 3.5 показано вид головного вікна після застосування певних змін до списку hosts.

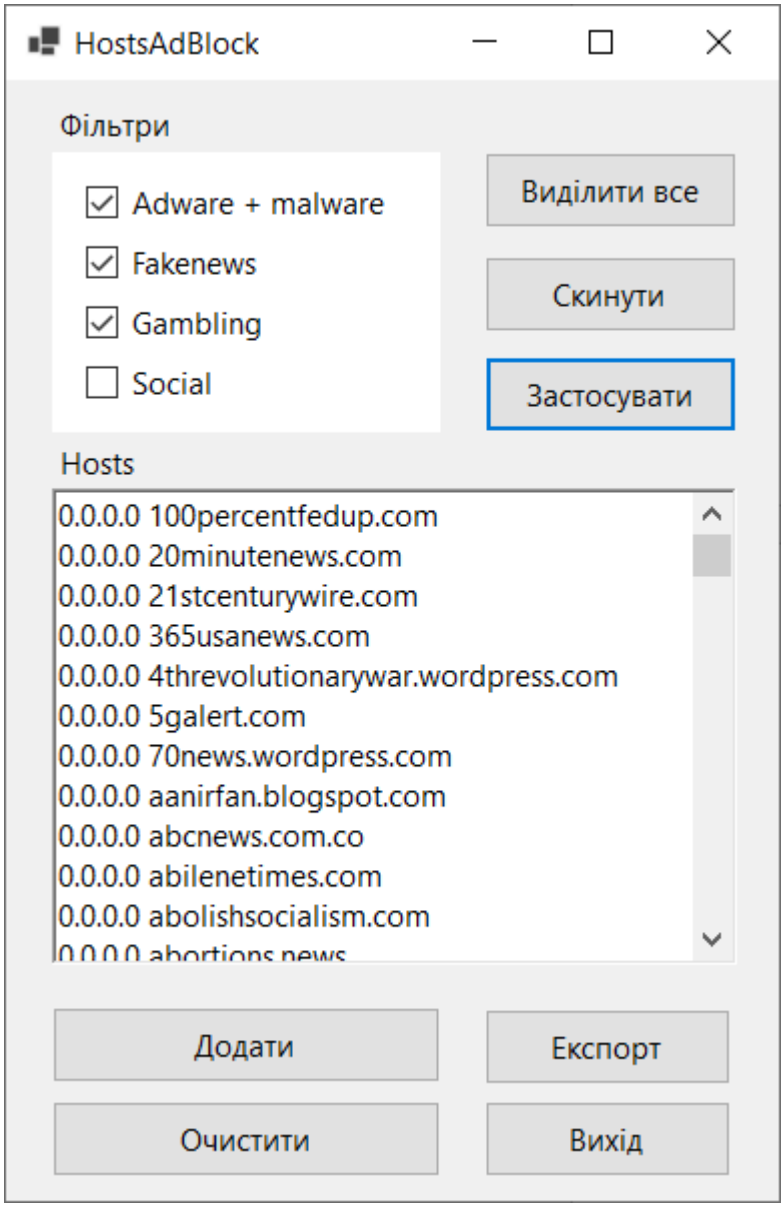

Рисунок 3.5 – Вигляд головного вікна програми вибору фільтрів та їх застосування

Також програма дозволяє експортувати поточний набір правил у зовнішній файл. Для цього потрібно натиснути кнопку "Експорт" та обрати місце для збереження файлу.

У разі виникнення проблем або при появі необхідності повернення до стандартних налаштувань, користувач може скористатися кнопкою "Очистити". Це відновить оригінальний вміст файлу *hosts*, видаливши всі додані правила. Перед виконанням цієї операції програма запитає підтвердження, показане на рисунку 3.6.

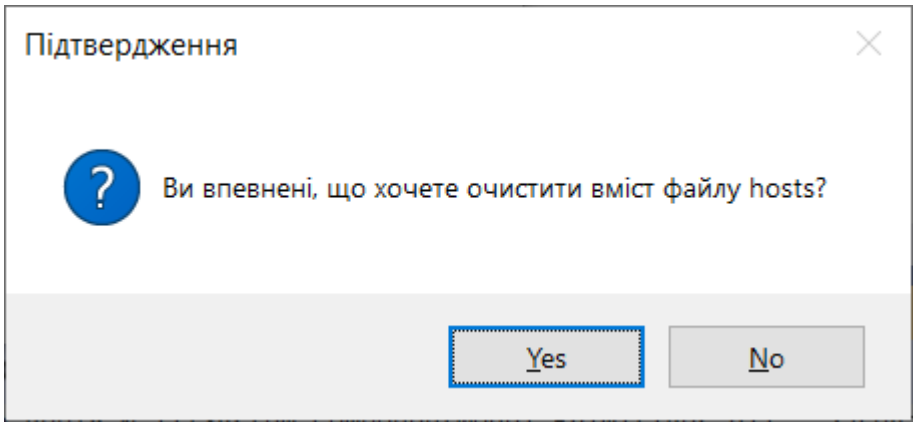

Рисунок 3.6 – Запит на очищення файлу hosts

Якщо не виникло ніяких проблем в ході цієї операції, користувачеві буде представлено повідомлення про успішне скидання вмісту файлу *hosts* до стандартного стану (рисунок 3.7).

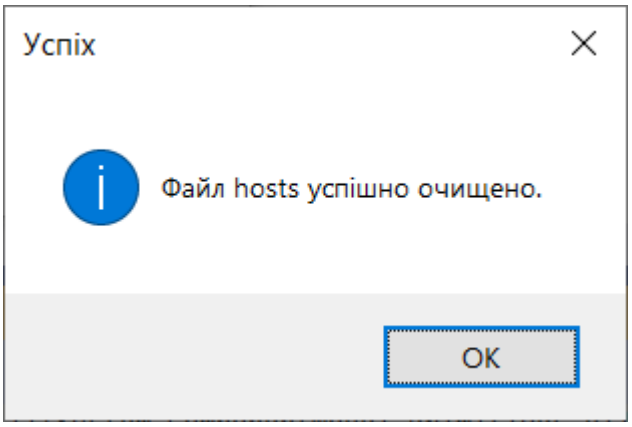

Рисунок 3.7 – Успішне очищення файлу hosts

Після завершення роботи з програмою користувач можете закрити її, натиснувши кнопку "Вихід" або використовуючи стандартний спосіб закриття

вікна. Усі зміни, внесені у файл *hosts*, залишаться дійсними до наступної зміни налаштувань.

Варто ще раз зауважити, що програма вимагає запуску з правами адміністратора для коректної роботи в разі необхідності зміни налаштувань в файлі *hosts*. Також рекомендується створювати резервні копії файлу *hosts* перед внесенням змін. У разі виникнення проблем з підключенням або при завантаженні потрібних сайтів після застосування фільтрів, користувачеві необхідно скористатися функцією очищення файлу *hosts* для повернення до стандартних налаштувань.

ВИСНОВКИ

У межах дипломного дослідження було проаналізовано актуальність проблеми блокування реклами в операційній системі Windows, вивчено існуючі інструменти та методи фільтрації — як браузерного рівня, так і системного. Особливу увагу приділено ефективності та універсальності використання системного файлу *hosts*, який забезпечує просту, стабільну та незалежну від сторонніх сервісів модель блокування.

Було зроблено висновок, що редагування *hosts*-файлу — один із найбільш надійних і доступних способів блокування реклами в межах усієї операційної системи. На його основі доцільно реалізувати спеціалізовану утиліту, яка дозволить автоматизувати процес оновлення списків доменів і спростить керування фільтрацією навіть для недосвідчених користувачів. Це дозволить підвищити комфорт, безпеку та продуктивність роботи на персональному комп’ютері.

Створення утиліти для фільтрації реклами при веб-серфінгу та роботі з додатками спонукало до глибокого аналізу не лише технічних аспектів реалізації, а й користувацького досвіду для реалізації інтуїтивно зрозумілого інтерфейсу. Розробка програми вимагала реалізації підходу до обробки прав доступу, оскільки робота з файлом *hosts* вимагає адміністраторських привілеїв. Це призвело до створення механізму, який перевіряє наявність необхідних прав та надає зрозумілі повідомлення у разі виявлення обмеженого доступу.

Було визначено важливим завданням і забезпечення стабільності роботи як утиліти, так і операційної системи внаслідок її використання. Система автоматичного створення резервних копій перед внесенням змін дозволяє уникнути порушення стабільності функціонування системи у разі непередбачених помилок. Це важливо з огляду на те, що файл *hosts* є критичним елементом системи, і його пошкодження може призвести до порушення мережевої роботи комп'ютера.

При розробці утиліти також враховувались різноманітні сценарії її використання. Програма добре підходить як для досвідчених користувачів, які бажають реалізовувати контроль над мережевими підключеннями, так і для тих, хто просто хоче заблокувати рекламу та інший небажаний вміст. Гнучкі налаштування та можливість ручного редагування дозволяють адаптувати утиліту під конкретні потреби кожного, хто буде користатися нею.

ПЕРЕЛІК ПОСИЛАНЬ

1. AdBlock [Електронний ресурс] – Режим доступу до ресурсу: https://chromewebstore.google.com/detail/adblock-%E2%80%93-%D0%B1%D0%BB%D0%BE%D0%BA%D0%B8%D1%80%D0%BE%D0%B2%D0%BA%D0%B0-%D1%80%D0%B5%D0%BA%D0%BB/gighmmpiobklfepjocnamgkkbiglidom

2. uBlock Origin - Free, open-source ad content blocker [Електронний ресурс] – Режим доступу до ресурсу: https://ublockorigin.com/

3. Ghostery [Електронний ресурс] – Режим доступу до ресурсу: https://www.ghostery.com/

4. NextDNS. The new firewall for the modern Internet [Електронний ресурс] – Режим доступу до ресурсу: https://nextdns.io/

5. Pi-hole [Електронний ресурс] – Режим доступу до ресурсу: https://pi-hole.net/

6. Easylist [Електронний ресурс] – Режим доступу до ресурсу: https://easylist.to/

7. Oisd blocklist [Електронний ресурс] – Режим доступу до ресурсу: https://oisd.nl/

8. Raspberry Pi [Електронний ресурс] – Режим доступу до ресурсу: https://www.raspberrypi.com/

9. DNS over HTTPS [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/DNS_over_HTTPS

10. Hosts File Format for TCP/IP [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/docs/en/aix/7.1.0?topic=formats-hosts-file-format-tcpip

11. StevenBlack / hosts [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/StevenBlack/hosts/blob/master/alternates/fakenews-gambling-social/readme.md

12. Best AdAway Host Sources 2024 [Електронний ресурс] – Режим доступу до ресурсу: https://magiskmodule.gitlab.io/blog/best-adaway-host-sources-2024

13. StevenBlack hosts alternates (Updates from BigDargon, URLHaus, someonewhocares.org, and KADhosts) [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/StevenBlack/hosts/tree/master/alternates
14. StevenBlack hosts change history [Електронний ресурс] – Режим доступу до ресурсу:https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts_file_size_history.png
15. EnergizedProtection / EnergizedHosts [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/EnergizedProtection/EnergizedHosts
16. Energized Adware [Електронний ресурс] – Режим доступу до ресурсу: https://raw.githubusercontent.com/EnergizedProtection/EnergizedHosts/master/EnergizedAd/energized/hosts
17. Energized Malware [Електронний ресурс] – Режим доступу до ресурсу: https://raw.githubusercontent.com/EnergizedProtection/EnergizedHosts/master/EnergizedMalware/energized/hosts
18. Energized Unified [Електронний ресурс] – Режим доступу до ресурсу: https://raw.githubusercontent.com/EnergizedProtection/EnergizedHosts/master/EnergizedUnified/energized/hosts
19. Ad-blocking for your Android [Електронний ресурс] – Режим доступу до ресурсу: https://adaway.org/
20. Blokada Community [Електронний ресурс] – Режим доступу до ресурсу: https://community.blokada.org/t/is-there-a-maximum-number-of-lists-one-should-subscribe-to/14025
21. AdAway [Електронний ресурс] – Режим доступу до ресурсу: https://f-droid.org/uk/packages/org.adaway/
22. Dan Pollock’s hosts [Електронний ресурс] – Режим доступу до ресурсу: https://someonewhocares.org/hosts/
23. Host’s update [Електронний ресурс] – Режим доступу до ресурсу: https://someonewhocares.org/hosts/#:~:text=,Jun%202025%20at%2023%3A01%3A29%20GMT

24. jerryn70 / GoodbyeAds [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/jerryn70/GoodbyeAds
25. CleanBrowsing | DNS Filtering Platform | Affordable DNS Filtering [Електронний ресурс] – Режим доступу до ресурсу: https://cleanbrowsing.org/solutions/web-filtering

Додаток А

Фрагмент програмного коду

PingUtility.cs

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.IO;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace HostsAdBlock
{
    public partial class Form1 : Form
    {
        // Шлях до директорії з файлами для блокування
        private readonly string dbPath =
Path.Combine(AppDomain.CurrentDomain.BaseDirectory, "DB");

        // Шлях до файлу hosts
        private readonly string hostsPath =
Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder
.System), @"drivers\etc\hosts");

        // Словник для зберігання шляхів до файлів для кожного
чекбоксу
        private readonly Dictionary<CheckBox, string>
checkBoxFileMap;

        public Form1()
        {
```

```
            InitializeComponent();

            // Ініціалізація словника відповідності чекбоксів та
файлів
            checkBoxFileMap = new Dictionary<CheckBox, string>
            {
                { checkBox1, Path.Combine(dbPath,
"adware_malware.txt") },
                { checkBox2, Path.Combine(dbPath,
"fakenews.txt") },
                { checkBox3, Path.Combine(dbPath,
"gambling.txt") },
                { checkBox4, Path.Combine(dbPath, "social.txt")
}
            };

            // Перевірка та створення директорії DB, якщо вона
не існує
            if (!Directory.Exists(dbPath))
            {
                Directory.CreateDirectory(dbPath);
                CreateDefaultFilterFiles();
            }

            // Завантаження поточного вмісту hosts файлу
            LoadCurrentHosts();

            // Підписка на події
            button1.Click += ButtonSelectAll_Click;
            button2.Click += ButtonDeselectAll_Click;
            button3.Click += ButtonApply_Click;
            button4.Click += ButtonAddToHosts_Click;
            button5.Click += ButtonExport_Click;
            button6.Click += ButtonClear_Click;
            button7.Click += ButtonExit_Click;
```

```
            // Встановлення тексту форми
            this.Text = "HostsAdBlock";
        }

        // Створення порожніх файлів фільтрів за замовчуванням
        private void CreateDefaultFilterFiles()
        {
            // Створення порожніх файлів, якщо вони не існують
            foreach (var file in checkBoxFileMap.Values)
            {
                if (!File.Exists(file))
                {
                    File.WriteAllText(file, "# Файл для
блокування " + Path.GetFileNameWithoutExtension(file));
                }
            }
        }

        // Завантаження поточного вмісту hosts файлу
        private void LoadCurrentHosts()
        {
            try
            {
                richTextBox1.Text = File.ReadAllText(hostsPath,
Encoding.UTF8);
            }
            catch (Exception ex)
            {
                MessageBox.Show($"Помилка завантаження файлу
hosts: {ex.Message}", "Помилка",
                    MessageBoxButtons.OK, MessageBoxIcon.Error);
            }
        }
```

```
        // Обробник події для кнопки "Виділити все"
        private void ButtonSelectAll_Click(object sender,
EventArgs e)
        {
            foreach (var checkBox in checkBoxFileMap.Keys)
            {
                checkBox.Checked = true;
            }
        }

        // Обробник події для кнопки "Скинути"
        private void ButtonDeselectAll_Click(object sender,
EventArgs e)
        {
            foreach (var checkBox in checkBoxFileMap.Keys)
            {
                checkBox.Checked = false;
            }
        }

        // Обробник події для кнопки "Застосувати"
        private void ButtonApply_Click(object sender, EventArgs
e)
        {
            try
            {
                var sb = new StringBuilder();

                // Зчитуємо поточний вміст hosts файлу
                if (File.Exists(hostsPath))
                {
                    sb.AppendLine(File.ReadAllText(hostsPath));
                }

                // Додаємо заголовок
```

```
                sb.AppendLine("\n# Додано HostsAdBlock");
                sb.AppendLine("# " +
DateTime.Now.ToString("yyyy-MM-dd HH:mm:ss"));

                // Додаємо вибрані фільтри
                foreach (var kvp in checkBoxFileMap)
                {
                    if (kvp.Key.Checked &&
File.Exists(kvp.Value))
                    {
                        sb.AppendLine($"\n#
{Path.GetFileNameWithoutExtension(kvp.Value)}");

sb.AppendLine(File.ReadAllText(kvp.Value));
                    }
                }

                // Зберігаємо оновлений вміст у richTextBox
                richTextBox1.Text = sb.ToString();

                // Записуємо у файл hosts
                File.WriteAllText(hostsPath, richTextBox1.Text,
Encoding.UTF8);

                MessageBox.Show("Файл hosts успішно оновлено!",
"Успіх",
                    MessageBoxButtons.OK,
MessageBoxIcon.Information);
            }
            catch (UnauthorizedAccessException)
            {
                MessageBox.Show("Недостатньо прав для запису у
файл hosts. Запустіть програму від імені адміністратора.",
                    "Помилка доступу", MessageBoxButtons.OK,
MessageBoxIcon.Error);
```

```
            }
            catch (Exception ex)
            {
                MessageBox.Show($"Помилка при оновленні файлу
hosts: {ex.Message}",
                    "Помилка", MessageBoxButtons.OK,
MessageBoxIcon.Error);
            }
        }

        // Обробник події для кнопки "Додати"
        private void ButtonAddToHosts_Click(object sender,
EventArgs e)
{
    try
    {
        string currentContent = "";
        if (File.Exists(hostsPath))
        {
            currentContent = File.ReadAllText(hostsPath,
Encoding.UTF8);
        }

        string newContent = currentContent + "\n" +
richTextBox1.Text;

        if (TryWriteToFile(hostsPath, newContent))
        {
            richTextBox1.Text = newContent;
            MessageBox.Show("Записи успішно додано до файлу
hosts!", "Успіх",
                MessageBoxButtons.OK,
MessageBoxIcon.Information);
        }
    }
```

```
    catch (Exception ex)
    {
        MessageBox.Show($"Помилка при додаванні записів:
{ex.Message}",
            "Помилка", MessageBoxButtons.OK,
MessageBoxIcon.Error);
    }
}

        // Обробник події для кнопки "Експорт"
        private void ButtonExport_Click(object sender, EventArgs
e)
        {
            using (SaveFileDialog saveFileDialog = new
SaveFileDialog())
            {
                saveFileDialog.Filter = "Текстові файли
(*.txt)|*.txt|Всі файли (*.*)|*.*";
                saveFileDialog.FilterIndex = 1;
                saveFileDialog.RestoreDirectory = true;

                if (saveFileDialog.ShowDialog() ==
DialogResult.OK)
                {
                    try
                    {

File.WriteAllText(saveFileDialog.FileName, richTextBox1.Text,
Encoding.UTF8);
                        MessageBox.Show("Файл успішно
збережено!", "Експорт завершено",
                            MessageBoxButtons.OK,
MessageBoxIcon.Information);
                    }
                    catch (Exception ex)
```

```
                    {
                        MessageBox.Show($"Помилка при збереженні
файлу: {ex.Message}",
                            "Помилка", MessageBoxButtons.OK,
MessageBoxIcon.Error);
                    }
                }
            }
        }

        // Обробник події для кнопки "Очистити"
        private void ButtonClear_Click(object sender, EventArgs
e)
{
    if (MessageBox.Show("Ви впевнені, що хочете очистити вміст
файлу hosts?", "Підтвердження",
        MessageBoxButtons.YesNo, MessageBoxIcon.Question) ==
DialogResult.Yes)
    {
        try
        {
            string defaultContent = "# Copyright (c) 1993-2009
Microsoft Corp.\r\n" +
                                    "#\r\n" +
                                    "# This is a sample HOSTS file
used by Microsoft TCP/IP for Windows.\r\n" +
                                    "#\r\n" +
                                    "# This file contains the
mappings of IP addresses to host names.\r\n" +
                                    "#\r\n" +
                                    "127.0.0.1
localhost\r\n" +
                                    "::1
localhost\r\n";
```

```
            if (TryWriteToFile(hostsPath, defaultContent))
            {
                richTextBox1.Text = defaultContent;
                MessageBox.Show("Файл hosts успішно очищено.",
                    "Успіх", MessageBoxButtons.OK,
MessageBoxIcon.Information);
            }
        }
        catch (Exception ex)
        {
            MessageBox.Show($"Помилка при очищенні файлу hosts:
{ex.Message}",
                "Помилка", MessageBoxButtons.OK,
MessageBoxIcon.Error);
        }
    }
}

        // Обробник події для кнопки "Вихід"
        private void ButtonExit_Click(object sender, EventArgs
e)
        {
            this.Close();
        }

        // Method for safe file writing with retries
        private bool TryWriteToFile(string path, string content,
int maxRetries = 3, int delayMs = 100)
        {
            int attempts = 0;
            while (attempts < maxRetries)
            {
                try
                {
```

```
                    using (var fileStream = new FileStream(path,
FileMode.Create, FileAccess.Write, FileShare.None))
                    using (var writer = new
StreamWriter(fileStream, Encoding.UTF8))
                    {
                        writer.Write(content);
                    }
                    return true;
                }
                catch (Exception) when (attempts < maxRetries -
1)
                {
                    System.Threading.Thread.Sleep(delayMs);
                    attempts++;
                }
            }
            return false;
        }

    }
}
```

Додаток Б

Фрагмени файлів з переліком хостів для блокування

adware_malware.txt

```
#=====================================
# Title: Hosts contributed by Steven Black
# http://stevenblack.com

0.0.0.0 ad-assets.futurecdn.net
0.0.0.0 ck.getcookiestxt.com
0.0.0.0 eu1.clevertap-prod.com
0.0.0.0 wizhumpgyros.com
0.0.0.0 coccyxwickimp.com
0.0.0.0 webmail-who-int.000webhostapp.com
0.0.0.0 010sec.com
0.0.0.0 01mspmd5yalky8.com
0.0.0.0 0byv9mgbn0.com
0.0.0.0 ns6.0pendns.org
0.0.0.0 dns.0pengl.com
0.0.0.0 12724.xyz
0.0.0.0 21736.xyz
0.0.0.0 www.analytics.247sports.com
0.0.0.0 2no.co
0.0.0.0 www.2no.co
0.0.0.0 logitechlogitechglobal.112.2o7.net
0.0.0.0 www.logitechlogitechglobal.112.2o7.net
0.0.0.0 2s11.com
0.0.0.0 30-day-change.com
0.0.0.0 www.30-day-change.com
0.0.0.0 mclean.f.360.cn
0.0.0.0 mvconf.f.360.cn
0.0.0.0 care.help.360.cn
0.0.0.0 eul.s.360.cn
0.0.0.0 g.s.360.cn
0.0.0.0 p.s.360.cn
0.0.0.0 aicleaner.shouji.360.cn
0.0.0.0 ssl.360antivirus.org
0.0.0.0 ad.360in.com
0.0.0.0 mclean.lato.cloud.360safe.com
0.0.0.0 mvconf.lato.cloud.360safe.com
0.0.0.0 mclean.cloud.360safe.com
0.0.0.0 mvconf.cloud.360safe.com
0.0.0.0 mclean.uk.cloud.360safe.com
0.0.0.0 mvconf.uk.cloud.360safe.com
0.0.0.0 3lift.org
0.0.0.0 448ff4fcfcd199a.com
0.0.0.0 44chan.me
0.0.0.0 4ourkidsky.com
0.0.0.0 5kv261gjmq04c9.com
0.0.0.0 88chan.pw
0.0.0.0 new.915yzt.cn
```

fakenews.txt

```
0.0.0.0 100percentfedup.com
0.0.0.0 20minutenews.com
0.0.0.0 21stcenturywire.com
0.0.0.0 365usanews.com
0.0.0.0 4threvolutionarywar.wordpress.com
0.0.0.0 5galert.com
0.0.0.0 70news.wordpress.com
0.0.0.0 aanirfan.blogspot.com
0.0.0.0 abcnews.com.co
0.0.0.0 abilenetimes.com
0.0.0.0 abolishsocialism.com
0.0.0.0 abortions.news
0.0.0.0 abqtimes.com
0.0.0.0 absurd.news
0.0.0.0 actualidad.rt.com
0.0.0.0 adairmadisonnews.com
0.0.0.0 adamscountytimes.com
0.0.0.0 adareporter.com
0.0.0.0 addictinginfo.org
0.0.0.0 addiction.news
0.0.0.0 adobochronicles.com
0.0.0.0 africannewsupdates.com
0.0.0.0 ahtribune.com
0.0.0.0 aikentimes.com
0.0.0.0 akbusinessdaily.com
0.0.0.0 akronreporter.com
0.0.0.0 albanystandard.com
0.0.0.0 albusinessdaily.com
0.0.0.0 alertchild.com
0.0.0.0 aljazeera-channel.com
0.0.0.0 alleghenyhighlandstoday.com
0.0.0.0 allnewspipeline.com
0.0.0.0 almastandard.com
0.0.0.0 alohastatenews.com
0.0.0.0 altleft.news
0.0.0.0 altoonatimes.com
0.0.0.0 aluminum.news
0.0.0.0 alynews.com
0.0.0.0 amarillogazette.com
0.0.0.0 americancatholictribune.com
0.0.0.0 americanfreepress.net
0.0.0.0 americanlookout.com
0.0.0.0 americanmilitarynews.com
0.0.0.0 americannews.com
0.0.0.0 americanoverlook.com
0.0.0.0 americanpharmacynews.com
0.0.0.0 americanreviewer.com
0.0.0.0 americansecuritynews.com
0.0.0.0 americantoday.news
0.0.0.0 americantribune.org
```

gambling.txt

```
0.0.0.0 0000130.com
0.0.0.0 0066130.com
0.0.0.0 007win.com
0.0.0.0 007win.org
0.0.0.0 007win.shop
0.0.0.0 007winand.taive.app
0.0.0.0 009.casino
0.0.0.0 009.com
0.0.0.0 009songbai.com
0.0.0.0 016665.com
0.0.0.0 048.com
0.0.0.0 0909777.com
0.0.0.0 101ae888.com
0.0.0.0 111c54.com
0.0.0.0 1166130.com
0.0.0.0 118kbet.com
0.0.0.0 11bet.bz
0.0.0.0 11bet.club
0.0.0.0 11bet.com
0.0.0.0 11bet.fun
0.0.0.0 11bet.gg
0.0.0.0 11bet.in
0.0.0.0 11bet.life
0.0.0.0 11bet.mobi
0.0.0.0 11bet.mx
0.0.0.0 11bet.net
0.0.0.0 11bet.online
0.0.0.0 11bet.org
0.0.0.0 11bet.pro
0.0.0.0 11bet.us
0.0.0.0 11bet.vin
0.0.0.0 11bet.win
0.0.0.0 11betvnd.com
0.0.0.0 11zalo.com
0.0.0.0 123b.bet
0.0.0.0 123b.com
0.0.0.0 123b.net
0.0.0.0 123b.org
0.0.0.0 123b.town
0.0.0.0 123b.vn
0.0.0.0 123b03.com
0.0.0.0 123b04.com
0.0.0.0 123b05.com
0.0.0.0 123b06.com
0.0.0.0 123b09.com
0.0.0.0 123b333.com
0.0.0.0 123b88.com
0.0.0.0 123bdly.com
0.0.0.0 123bdy.com
0.0.0.0 123bhh.com
```

social.txt

```
0.0.0.0 0-act.channel.facebook.com
0.0.0.0 0-edge-chat.facebook.com
0.0.0.0 0.beta.facebook.com
0.0.0.0 1-act.channel.facebook.com
0.0.0.0 1-edge-chat.facebook.com
0.0.0.0 2-act.channel.facebook.com
0.0.0.0 2-edge-chat.facebook.com
0.0.0.0 3-act.channel.facebook.com
0.0.0.0 3-edge-chat.facebook.com
0.0.0.0 4-act.channel.facebook.com
0.0.0.0 4-edge-chat.facebook.com
0.0.0.0 5-act.channel.facebook.com
0.0.0.0 5-edge-chat.facebook.com
0.0.0.0 6-act.channel.facebook.com
0.0.0.0 6-edge-chat.facebook.com
0.0.0.0 a.ns.facebook.com
0.0.0.0 a1qa.m.facebook.com
0.0.0.0 a3.sphotos.ak.fbcdn.net
0.0.0.0 abc.facebook.com
0.0.0.0 about.facebook.com
0.0.0.0 act.channel.facebook.com
0.0.0.0 act.facebook.com
0.0.0.0 actcorp.m.facebook.com
0.0.0.0 ads.facebook.com
0.0.0.0 adsmanager.facebook.com
0.0.0.0 ae0.bb01.ams2.tfbnw.net
0.0.0.0 ae0.bb01.atl1.tfbnw.net
0.0.0.0 ae0.bb01.bos2.tfbnw.net
0.0.0.0 ae0.bb01.hkg1.tfbnw.net
0.0.0.0 ae0.bb01.hnd1.tfbnw.net
0.0.0.0 ae0.bb01.lhr2.tfbnw.net
0.0.0.0 ae0.bb01.lla1.tfbnw.net
0.0.0.0 ae0.bb01.mia1.tfbnw.net
0.0.0.0 ae0.bb01.nrt1.tfbnw.net
0.0.0.0 ae0.bb01.sin1.tfbnw.net
0.0.0.0 ae0.bb02.ams2.tfbnw.net
0.0.0.0 ae0.bb02.atl1.tfbnw.net
0.0.0.0 ae0.bb02.bos2.tfbnw.net
0.0.0.0 ae0.bb02.hkg1.tfbnw.net
0.0.0.0 ae0.bb02.lhr2.tfbnw.net
0.0.0.0 ae0.bb02.lla1.tfbnw.net
0.0.0.0 ae0.bb02.mia1.tfbnw.net
0.0.0.0 ae0.bb02.sin1.tfbnw.net
0.0.0.0 ae0.bb03.atn1.tfbnw.net
0.0.0.0 ae0.bb03.frc3.tfbnw.net
0.0.0.0 ae0.bb03.lla1.tfbnw.net
0.0.0.0 ae0.bb03.prn2.tfbnw.net
0.0.0.0 ae0.bb03.sjc1.tfbnw.net
0.0.0.0 ae0.bb04.atn1.tfbnw.net
0.0.0.0 ae0.bb04.frc3.tfbnw.net
```