

**Автор:**

Карпенко Андреа Тарасович,  
студент 2 курсу магістратури,  
спеціальності «Комп'ютерні науки»

**Науковий керівник:**

кандидат педагогічних наук, доцент,  
доцент кафедри комп'ютерної та  
програмної інженерії  
Галицький Олександр Вадимович

## РОЗРОБКА ПРОКСІ РОЗШИРЕННЯ

**Анотація.** У роботі розглядається створення браузерного проксі розширення для Google Chrome, яке дає можливість користувачеві здійснювати управління мережевими з'єднаннями на рівні веббраузера без зміни його налаштувань. Розширення підтримує підключення до HTTP та SOCKS5 проксі, роботу з переліком серверів, вимірювання затримки, облік трафіку та автоматичну заміну недоступних проксі. Передбачено режими маршрутизації за доменами, базовий захист конфігурації за допомогою PIN коду та можливість синхронізації основних налаштувань між пристроями.

**Ключові слова:** проксі розширення, браузер, HTTP, SOCKS5, маршрутизація трафіку, пінг, облік трафіку, інформаційна безпека.

**Вступ.** Зростання обсягів вебтрафіку, поширення географічних та мережевих обмежень, а також потреба в контролі за переданими даними призводять до активного використання проксі серверів. У більшості випадків налаштування проксі виконується або на рівні операційної системи, або через окремі клієнтські програми, що ускладнює щоденну роботу користувача. Браузерні розширення дають змогу винести управління проксі безпосередньо в інтерфейс веббраузера та поєднати налаштування, моніторинг і діагностику в одному інструменті.

При цьому прості розширення обмежуються лише перемикачем "вкл/викл" та одним проксі сервером, а складні рішення часто орієнтовані на конкретні платні сервіси. Тому виникає практичне завдання створення незалежного проксі розширення, яке підтримує кілька типів проксі, роботу з переліком серверів, гнучку маршрутизацію трафіку, моніторинг якості з'єднання та базовий захист налаштувань.

**Постановка задачі.** У межах роботи передбачено виконання таких основних кроків:

- ✓ проаналізувати протоколи та технології, що використовуються для організації проксі з'єднань у веббраузерах, а також типові загрози безпеки під час їх використання;
- ✓ дослідити можливості браузерних API для управління проксі налаштуваннями та зберігання конфігурації;
- ✓ виконати огляд наявних проксі розширень, оцінити їхню функціональність, зручність та обмеження;
- ✓ сформулювати вимоги до функціональності розширення, яке підтримує роботу з кількома проксі, режимами all/whitelist/blacklist, моніторингом пінгу та трафіку;
- ✓ спроектувати архітектуру розширення з виокремленням фонового модуля, спливаючого вікна, сторінки налаштувань та моделі даних;
- ✓ реалізувати та протестувати прототип розширення, перевірити коректність роботи основних режимів і механізмів автоматичної заміни проксі.

**Мета роботи.** Метою роботи є розроблення браузерного проксі розширення для веббраузера Google Chrome, яке забезпечує:

- ✓ зручне керування списком HTTP та SOCKS5 проксі серверів з можливістю швидкого додавання записів у форматі ip:port або ip:port:логін:пароль;

- ✓ перемикання між режимами маршрутизації трафіку: увесь трафік через проксі, використання проксі лише для "білого" списку доменів, обходження проксі для доменів з "чорного" списку;
- ✓ вимірювання затримки, масову перевірку працездатності проксі та відображення статусу сервера;
- ✓ облік обсягів трафіку по кожному проксі та загалом, з формуванням статистики за останні 24 години;
- ✓ автоматичну заміну недоступних проксі та інформування користувача про такі події;
- ✓ базовий захист конфігурації через PIN код та опціональну синхронізацію основних налаштувань між пристроями.

**Основна частина.** У першій частині роботи розглянуто теоретичні основи організації проксі з'єднань. Подано класифікацію проксі серверів за типом протоколу, рівнем анонімності, призначенням та способом розміщення в мережі. Окремо проаналізовано загрози безпеки, пов'язані з використанням проксі, зокрема можливість перехоплення трафіку, атаки типу "людина посередині", витоки облікових даних та особливості роботи з ненадійними публічними серверами.

Наступним кроком є аналіз сучасних проксі розширень. Оцінено їхні переваги та обмеження, типові підходи до побудови інтерфейсу, способи реалізації підтримки кількох проксі та режимів маршрутизації. На основі цього аналізу сформовано перелік функціональних та нефункціональних вимог до розроблюваного розширення, до якого включено підтримку режимів all/whitelist/blacklist, моніторинг пінгу, облік трафіку, механізм автозаміни та елементи захисту конфігурації.

Архітектурна модель розширення передбачає поділ на фоновий модуль, спливаюче вікно та сторінку налаштувань. Фоновий модуль відповідає за застосування проксі налаштувань до веббраузера, облік трафіку, виконання перевірок працездатності проксі, автоматичну заміну "мертвих" серверів, взаємодію зі сховищем даних та відправлення системних сповіщень. Спливаюче вікно забезпечує швидкий доступ до основних функцій: увімкнення або вимкнення проксі, вибір активного сервера, перегляд статусу та запуск разової перевірки пінгу. Сторінка налаштувань містить вкладки для роботи зі списком проксі, "білим" та "чорним" списками доменів, параметрами автоматичної заміни, лімітами трафіку, статистикою та PIN захистом.

Модель даних включає структури для зберігання списку проксі серверів, глобальних налаштувань, списків доменів, історії пінгу та трафіку. Для забезпечення переносимості конфігурації використовується розподіл між локальним сховищем та синхронізованим: базові налаштування (список проксі, режими, списки доменів) можуть синхронізуватися через обліковий запис веббраузера, а детальна статистика зберігається лише локально.

Реалізований прототип підтримує масову перевірку списку проксі з відображенням останнього пінгу та стану сервера, автоматичну заміну недоступного проксі найближчим придатним варіантом, побудову графіків трафіку та пінгу за останні 24 години на основі canvas, встановлення лімітів трафіку з генерацією сповіщень у разі перевищення, а також PIN захист доступу до налаштувань. Проведено тестування роботи розширення з декількома проксі серверами, у тому числі зі свідомо "мертвими" адресами, перевірено коректність роботи режимів all/whitelist/blacklist та механізму автозаміни при падінні активного проксі.

**Висновок.** У результаті виконання роботи сформовано структурований підхід до розроблення браузерного проксі розширення, побудовано архітектуру, модель даних та реалізовано прототип, що забезпечує підтримку кількох типів проксі, гнучку маршрутизацію трафіку, моніторинг пінгу та трафіку, автоматичну заміну недоступних серверів, PIN захист налаштувань та опціональну синхронізацію конфігурації. Отримане рішення може використовуватися як інструмент для дослідження впливу проксі на якість з'єднання, для роботи в умовах мережевих обмежень та в навчальних цілях під час вивчення мережевих технологій і клієнтських розширень.

## Список використаних джерел

1. Chrome.proxy | API | Chrome for Developers. *Chrome for Developers*. URL: <https://developer.chrome.com/docs/extensions/reference/api/proxy> (дата звернення: 15.11.2025).
2. Chrome.storage | API | Chrome for Developers. *Chrome for Developers*. URL: <https://developer.chrome.com/docs/extensions/reference/api/storage> (дата звернення: 15.11.2025).
3. Chrome.storage.sync vs chrome.storage.local. *Stack Overflow*. URL: <https://stackoverflow.com/questions/22636771/chrome-storage-sync-vs-chrome-storage-local> (дата звернення: 15.11.2025).
4. Frisbie M. Building Browser Extensions: Create Modern Extensions for Chrome, Safari, Firefox, and Edge. Apress L. P., 2022. 570 с.
5. Grigorik I. High Performance Browser Networking: What Every Web Developer Should Know about Networking and Web Performance. O'Reilly Media, Incorporated, 2013. 400 с.
6. Галицький О.В. Управління електронними освітніми ресурсами з використанням веб-орієнтованих комп'ютерних систем [Текст] : автореф. дис. ... канд. пед. наук : 13.00.02 / Галицький Олександр Вадимович; Нац. пед. ун-т ім. М. П. Драгоманова. Київ, 24 с.
7. Технології Data Mining : Програма навчальної дисципліни підготовки магістра галузь знань 12“Інформаційні технології” спеціальність 122“Комп’ютерні науки” / укл. : М.П. Малежик, П.М. Малежик, О.В. Галицький ; НПУ імені М. П. Драгоманова, Кафедра комп’ютерної інженерії та освітніх вимірювань. Київ : Вид-во НПУ імені М.П. Драгоманова, 2020 р. 20 с.