

ПРОБЛЕМИ ПЕРЕХОДУ РОЗШИРЕНЬ CHROMIUM-BASED БРАУЗЕРІВ НА MANIFEST V3

Тяжельников О. В.

email: oleksii.tiazhelnykov@nure.ua

Харківський національний університет радіоелектроніки, каф. КІТС
м. Харків, Україна

This paper examines the challenges associated with the transition of Chromium-based browsers to Manifest V3. While the new standard aims to enhance security and performance, it introduces significant limitations for developers, particularly in content filtering and request management. The paper discusses the impact of restrictions on ad blockers, background processes, and dynamic script execution, highlighting the difficulties faced by developers and users alike. Additionally, the study analyzes responses from various browser vendors and potential future developments in browser extension policies.

Перехід браузерів на основі Chromium до третьої версії маніфесту розширень (Manifest V3) викликав значний резонанс серед розробників та користувачів. Основна мета цієї зміни, за заявами Google, полягає в покращенні продуктивності, безпеки та керованості розширень [1]. Проте нововведення спричинили низку обмежень, які вплинули на функціональність багатьох популярних розширень, зокрема блокувальників реклами, VPN-сервісів та менеджерів паролів. Дана теза розглядає основні проблеми переходу на Manifest V3 та його вплив на екосистему веб-розширень.

Одна з найважливіших змін у Manifest V3 – заміна API `webRequest` на `declarativeNetRequest` (DNR). У попередній версії API дозволяв розширенням змінювати або блокувати мережеві запити в реальному часі. Натомість новий API вимагає попереднього декларування правил блокування, що значно обмежує гнучкість розширень. Наприклад, розширення `uBlock Origin` та `AdGuard` більше не можуть динамічно оновлювати та застосовувати складні фільтри, що знижує ефективність блокування реклами [2].

Manifest V3 скасовує використання постійно працюючих фонових скриптів (`background.js`) на користь `service workers`, які запускаються лише на короткий час і завершують роботу після виконання завдання [3]. Це створює проблеми для розширень, які потребують постійного доступу до певних даних або мають складну логіку взаємодії. Наприклад, менеджери паролів, які повинні зберігати стан між сесіями, зазнали значних труднощів через необхідність змінювати архітектуру своїх рішень.

Ще одним суттєвим обмеженням є заборона завантаження та виконання довільного JavaScript-коду з віддалених серверів. Хоча це нововведення спрямоване на покращення безпеки, воно також обмежує

можливості розширень, які динамічно змінювали свій функціонал або завантажували оновлення без потреби в повторній публікації.

Переваги нового маніфесту, зокрема покращена безпека, супроводжуються значними труднощами для розробників. Вони змушені адаптувати свої розширення до нових обмежень, що часто потребує значних змін у коді. Крім того, через обмеження у блокуванні запитів знижується ефективність захисту користувачів від реклами та відстеження. Деякі браузері, такі як Mozilla Firefox, продовжують підтримувати `webRequestBlocking`, що робить їх привабливішими для користувачів, яким важлива конфіденційність [4-5].

Перехід на Manifest V3 є суперечливим кроком у розвитку веб-розширень. З одного боку, він підвищує безпеку та продуктивність, з іншого – обмежує функціональність популярних розширень, особливо тих, що пов'язані з блокуванням реклами та захистом конфіденційності. Хоча Google частково враховує критику спільноти та збільшує допустиму кількість правил у DNR, ці зміни все ще не компенсують втрати можливостей порівняно з Manifest V2. У майбутньому можлива подальша еволюція стандарту, яка дозволить знайти компроміс між безпекою та функціональністю веб-розширень.

Список використаних джерел:

1. Chrome Users Beware: Manifest V3 is Deceitful and Threatening : Electronic Frontier Foundation. URL: <https://www.eff.org/deeplinks/2021/12/chrome-users-beware-manifest-v3-deceitful-and-threatening> (дата звернення: 27.02.2025).
2. Google Chrome's uBlock Origin phaseout has begun : The Verge. URL: <https://www.theverge.com/2024/10/15/24270981/google-chrome-ublock-origin-phaseout-manifest-v3-ad-blocker> (дата звернення: 02.03.2025).
3. Service worker overview : Chrome for developers. URL: <https://developer.chrome.com/docs/workbox/service-worker-overview> (дата звернення 24.02.2025).
4. `webRequest.BlockingResponse` : MDN Web Docs. URL: <https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/API/webRequest/BlockingResponse> (дата звернення 26.02.2025)
5. Rudenko O., Bezsonov O., Ilyunin O., Demirskiy O., Serdiuk N., Arsenyeva O., Semenenko O. Using a Neural Network Approach to Predict Deposits on the Surfaces of Heat Exchange Equipment. *Chemical Engineering Transactions*. 2023. № 103. Pp. 697-702.