УДК 004.056.5:004.77

ДОСЛІДЖЕННЯ ПРИНЦИПІВ РОБОТИ АНОНІМНИХ БРАУЗЕРІВ

Лембей К.Д.
e-mail: kyrylo.lembei@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім В.В. Поповського
м. Харків, Україна

This article provides the comprehensive analysis of the core mechanisms underlying anonymous browsers, with a focus on the modern Tor browser. It explores the principles of onion routing, detailing the multi-layered encryption process that ensures anonymity and prevents third-party tracking. The study examines how encryption keys are exchanged between nodes and how the network dynamically adjusts to maintain security and performance. Additionally, the work delves into potential vulnerabilities within the Tor network, including risks associated with exit nodes, traffic correlation attacks, and fingerprinting techniques that could compromise user anonymity.

Концепт анонімних браузерів розроблявся з 1990 року, оскільки аспект анонімності в мережі на той час був вкрай слабкий, а кількість випадків використання інтернету для спостереження за людьми зростала. У наш час технологія анонімних браузерів набуває широкого поширення через зростаючу загрозу кібератак, посилення інтернет-цензури в деяких країнах, масові витоки персональних даних та можливе відстеження користувачів.

Основним механізмом, на якому базується робота сучасних анонімних браузерів, є “Цибулева маршрутизація” (англ. Onion Routing). Він включає в себе багатошарове шифрування на етапі інкапсуляції. Кожен шар шифрування відповідає окремому маршрутизатору, через який буде перенаправлений трафік, зазвичай це 3 пристрої, які називаються вхідним вузлом, проміжним вузлом та вихідним вузлом (англ. Entry node, Middle node, Exit node). Процес маршрутизації та дешифрування трафіку зображено на рисунках 1 та 2.

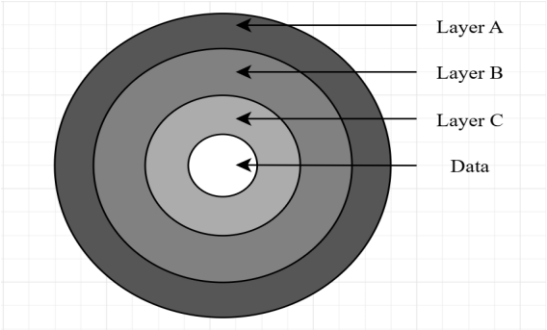

Рисунок 1 – Послідовність шарів шифрування

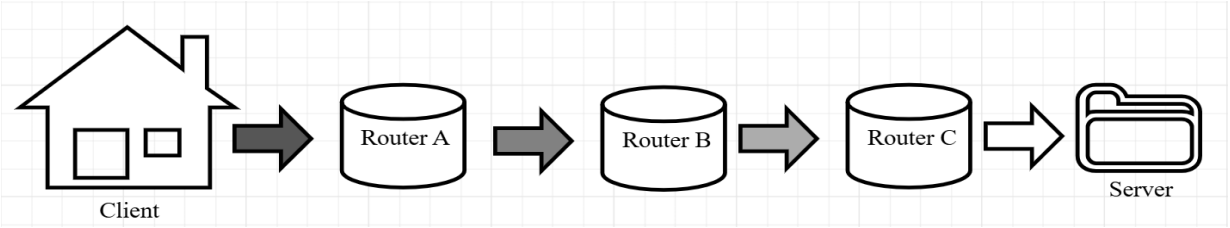

Рисунок 2 – Послідовність розшифрування трафіку

Кожен маршрутизатор знімає свій шар шифрування та передає інформацію наступному, що повторюється доки сервер не отримує повністю розшифрований запит від вихідного вузла. Для захисту даних використовується алгоритм AES-CTR, а обмін ключами здійснюється за допомогою гібридного шифрування та алгоритму Діффі-Геллмана (ECDH-256).

Перевагою і основною ідеєю «Onion routing» є принцип, за яким кожен вузол отримує лише інформацію про попередній та наступний пункт маршруту, що не дозволяє в певний момент часу перехопити повну інформацію про відправника і призначення.

Однак система «Onion routing» має деякі вразливості, перша з яких це безпека даних на вихідному вузлі. Останній маршрутизатор передає інформацію у відкритому вигляді до отримувача, це потенційно створює ризик перехоплення інформації сторонніми особами, чий пристрій виконує функцію вихідного вузла. Щодо браузеру Tor, то функції вузлів у ньому виконують не лише орендовані сервери та хмарні сервіси, а й волонтери та, інколи, звичайні користувачі. Отже організації, які зацікавлені у перехопленні трафіку користувачів, можуть зареєструвати свій пристрій у списку вузлів. Слід зазначити, що інформація з вихідного маршрутизатора не містить адресу пристрою користувача, однак відкриває сам запит та корисне навантаження, у якому можуть міститися дані для авторизації, номери телефонів, рахунків тощо. Також для встановлення зв’язку між відправником та вихідними запитами, при наявності контролю над вхідним і вихідним вузлами, можливе порівняння часових міток та розмір пакетів у логах, що дозволяє встановити адресу пристрою користувача. Насамкінець, використання анонімних браузерів не захищає від загроз з боку одержувача трафіку, оскільки кінцевий сервер може відстежувати активність користувача та аналізувати його дії.

В доповіді проведено аналіз особливостей функціонування анонімних браузерів та приведені методи цифрової криміналістичної експертизи браузера Tor.

Список використаних джерел:

1. Patel N. Tor Networking Vulnerabilities and Breaches. 2016. 15 с. URL: https://www.cs.tufts.edu/comp/116/archive/fall2016/npatel.pdf (Дата звернення: 02.03.2025).

2. Onion Routing: вебсайт URL: https://www.vpnunlimited.com/ua/help/cybersecurity/onion-

routing?srsltid=AfmBOoqC31X30fSjvYc4nBKwR6DdSkdmkm93YEpsWm6JM9IPfgcHZ6Vs (Дата звернення: 01.03.2025).