УДК 004.056

КОНЦЕПЦІЯ ПОКРАЩЕННЯ ЗАХИСТУ АНОНІМНОСТІ КОРИСТУВАЧІВ МЕРЕЖІ TOR ЧЕРЕЗ ЗАСТОСУВАНЯН ДОДАТКОВОГО ШАРУ ЗАХИСТУ ТА ТЕХНОЛОГІЇ БЛОКЧЕЙН

**Василь ПОБЕРЕЖНИК[1], Іван ОПІРСЬКИЙ[1],
Валерія БАЛАЦЬКА[2]**

1. Національний університет «Львівська політехніка»
2. Львівський державний університет безпеки життєдіяльності

Анотація. *Розглянуто концепцію методу покращення захисту анонімності користувачів мережі Tor, через застосування додаткових шарів захисту та транзитної точки, яка повинна розривати можливі зловмисні маршрути. Запропоновано застосування технології блокчейн для забезпечення збереження прозорої та стійкої до підробок інформації про вузли захисту, які застосовуються у системі*

Ключові слова: *блокчейн, Tor, анонімність, приватність, багатошарова маршрутизація.*

Abstract*. The concept of a method for improving the protection of the anonymity of the Tor network users is considered, using additional layers of protection and a transit point that should break possible malicious routes. The use of blockchain is proposed to preserve the transparent and tamper-resistant information about the protection nodes used in the system*

Keywords: *blockchain, Tor, anonymity, privacy, onion routing*.

Приватність та анонімність користувачів є важливим атрибутом користувачів різних сервісів у мережі. За допомогою різних сервісів забезпечення анонімності та приватності, користувачів намагаються захистити свою приватність в мережі, обійти різного роду обмеження чи захистити власні персональні дані, від надмірного збору чи несанкціонованого використання зі сторони провайдерів різних сервісів.

Одним із способі захисту власної приватності є використання мережі Tor. Ця технологія дозволяє забезпечувати захист анонімності користувачів, через встановлення багатошарової маршрутизації між вузлами мережі. Найменшою кількістю вузлів, для встановлення захищеного з'єднання із застосуванням мережі Tor є три вузли: вхідний, проміжний і вихідний.

Однак, застосування такого підходу не є гарантією збереження анонімності, оскільки існує ряд атак на користувачів мережі, який дозволяє деанонімізувати користувача мережі. Наприклад, дозволяє встановлювати особу користувача шляхом застосування різних деанонімізуючих засобів, наприклад аналіз вхідного і вихідного трафіку, використання зловмисних вузлів тощо [1]. Також нещодавно було продемонстровано техніку, яка дозволяла не тільки визначити користувача, який користується мережею, але й із допомогою зловмисних вузлів розривати захищене з'єднання і спрямовувати трафік на маршрут, який є контрольованим зловмисником [2].

Одним із принципів Tor є збереження інформації про вихідні вузли у відкритому доступі, що дозволяє зловмиснику без будь-яких перешкод, що спрощує атаки на ці вузли, їхнє цензурування тощо. Хоча сам підхід до відкритості є одним із ключових аспектів мережі Tor, який з одного боку покликаний підвищити довіру до мережі, а з іншого – є важливим функціональним аспектом, оскільки ця відкритість вузлів є необхідною для забезпечення встановлення маршруту між вузлами, користувачем та точкою призначення [3]. Проте така відкритість може стати своєрідним “modus operandi”, що може призвести до компрометації з’єднання та подальшої атаки на користувача, цензурування, деанонімізації тощо.

Зважаючи на це, можна вважати, що критичними точками у такій системі є вузол входу та виходу, оскільки перший знає інформацію про користувача, а останній – про точку призначення. Опираючись на це, можна розробити концепцію захисту від зловмисних вузлів, яка б могла протидіяти згаданій вразливості. Основна ідея пропонованого методу полягає в тому, що для захисту з’єднання і самого користувача необхідно встановити додатковий шар захисту та точку розриву маршруту, що схематично зображено на рисунку 1.

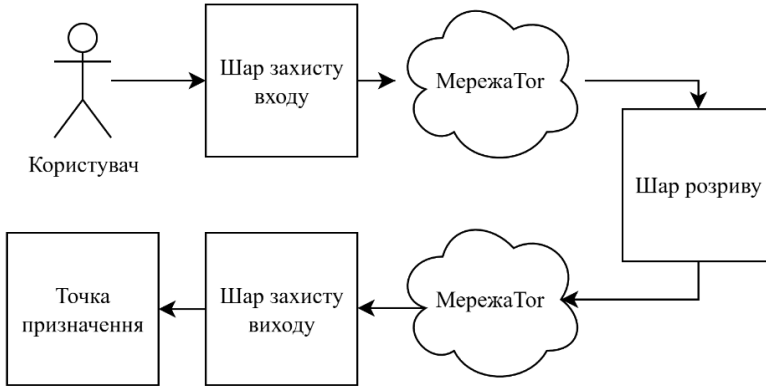

Рисунок 1 – Схематичне зображення методу із застосуванням розриву та додаткових шарів захисту

Безпека шарів захисту повинна забезпечуватися через застосування технології блокчейн як реєстру довірених вузлів: вузли вхідного і вихідного шару зберігають інформацію про себе у мережі блокчейн, що дозволить точно впевнитися в автентичності вузла, а вузол розриву слугує для захисту від зловмисної вихідної точки, оскільки він виконує роль транзитної точки, яка є одночасно кінцевою точкою для одного маршруту і початком нового, який буде вести до за шару виходу з мережі Tor. Отже суть підходу полягає в тому, щоб анонімізувати користувача ще до входу в мережу Tor, а також розірвати

можливе зловмисне з'єднання через створення двох маршрутів, де вхідна і вихідна точки є надійними. Застосування блокчейну в такому підході є важливим, оскільки сам він дозволить забезпечити надійне збереження даних про вузли, через свої властивості збереження інформації у незмінному вигляді та прозорість [4]. Також пропонується застосування гібридного підходу, де вузли обробляють інформацію підходом off-chain, оскільки обробка інформації великих обсягів або чутливої до затримок є недоцільною у самому блокчейні [5].

Аргументом для застосування такої концепції є те, що вона може використовувати уже готову інфраструктуру, як от публічний блокчейн, наприклад Ethereum, Solana тощо, та мережу Tor, яка є розвинутою дозволяє обробляти відносно великі об'єми трафіку даних.

Також ця концепція має і свої недоліки, які можуть стати на заваді реалізації системи, одним з них є необхідність підтримки роботи вузлів пропонованої системи, оскільки вона потребуватиме для своєї роботи постійного оновлення даних в мережі блокчейн та обслуговування самих вузлів.

Зважаючи на переваги та недоліки, можна зробити висновок, що застосування запропонованого підходу може дозволити покращити захищеність анонімності та приватності користувачів, а застосування гібридних технологій дозволяє застосовувати сильні сторони технологій, як от стійкість до змін та прозорість даних у блокчейні, та нівелювати їхні обмеження, як от низька толерантність до обробки великих масивів даних чи відносно низька швидкодія. Також концепція потребує подальшого дослідження, щоб дослідити доцільність застосування такого підходу та можливі шляхи застосування.

Література

1. Tor project | network attackers on the tor network. Tor Project | Join the Tor Community. URL: https://community.torproject.org/threat-model/threat-positioning/network/ (дата звернення: 21.11.2025).

2. An anonymity vulnerability in tor / Q. Tan та ін. IEEE/ACM transactions on networking. 2022. С. 1–14. URL: https://doi.org/10.1109/tnet.2022.3174003

3. You should hide the list of tor relays, so people can't block the exits. Support. URL: https://support.torproject.org/about-tor/alt-design/hide-list-of-exits/ (дата звернення: 21.11.2025).

4. Балацька В. С., Побережник В. О., Стефанків А. В., Шевчук Ю. А. Розробка методу забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів. Комп'ютерні системи та мережі. 2025. Т. 7, № 1. С. 1–16. DOI: https://doi.org/10.23939/csn2025.01.001

5. Дослідження швидкодії методу передачі повідомленнь із застосуванням off-chain обробки даних для забезпечення цілісності та незмінності даних. Сучасний захист інформації. 2025. Т. 63, № 3. С. 230–242. URL: https://doi.org/10.31673/2409-7292.2025.032280 (дата звернення: 21.11.2025).