УДК 004.738.53

Савчук Д.О.
Карпінець В.В.

ПІДВИЩЕННЯ ЗАХИСТУ ОНЛАЙН-СЕРВІСІВ ДЛЯ АНОНІМНОГО ОБМІНУ ІНФОРМАЦІЄЮ

Вінницький Національний Технічний Університет

Анотація

У цій статті розглядаються та обираються методи та технології, які дозволять підвищити рівень захисту та зберегти свою ідентичність, гарантуючи конфіденційність під час обміну інформацією в Інтернеті.

***Ключові слова**: анонімність, інсайдерська інформація, безпечний онлайн-сервіс, інструменти для анонімного перебування в мережі, Мережа Tor, анонімізація, секретні запитання, наскрізне шифрування, видалення метаданих, капча.*

Abstract

This article discusses and selects methods and technologies that will allow you to increase your level of protection and preserve your identity while guaranteeing confidentiality when exchanging information online.

***Keywords**: anonymity, insider information, secure online service, tools for anonymous surfing, Tor Network, anonymization, secret questions, end-to-end encryption, metadata removal, captcha.*

Вступ

Стрімкий розвиток технологій здійснив революцію в журналістиці, трансформувавши способи збору, передачі та споживання інформації. З появою цифрових платформ журналісти отримали доступ до широкого спектру ресурсів, що дозволяє їм збирати та поширювати інформацію з безпрецедентною ефективністю. Цей цифровий ландшафт відкрив нові можливості для проведення журналістських розслідувань і значно розширив охоплення та вплив журналістики. Однак на тлі цієї цифрової революції журналісти часто покладаються на інсайдерську інформацію, щоб розкрити приховану правду, викрити корупцію та пролити світло на критичні питання. Інсайдерська інформація може надати неоціненну інформацію та слугувати каталізатором для новаторських журналістських розслідувань. Однак вона також несе в собі певні ризики, оскільки джерела, які надають конфіденційну інформацію, можуть зіткнутися з серйозними наслідками, якщо їхні імена будуть розкриті.

Щоб вирішити цю проблему, необхідно запроваджувати та вдосконалювати методи та технології для захисту онлайн-сервісу для обміну інформацією. Така платформа забезпечила б журналістам безпечне та конфіденційне середовище для отримання цінної інформації, захищаючи анонімність їхніх джерел. Забезпечуючи безпечні та анонімні канали зв'язку, журналісти можуть розвивати довіру до своїх джерел і заохочувати викривачів до викриття, не боячись відплати або компрометації.

Для розробки такого сервісу потрібно вибрати технології що будуть забезпечувати максимальну анонімність та захист інсайдерів при її використанні. Тому буде досліджено технології які найкраще підійдуть для розробити безпечного онлайн-сервісу.

Дослідження

Одним із ключових аспектів забезпечення анонімності є використання спеціальних засобів та технологій, які дозволяють користувачам захистити свою ідентичність та забезпечити конфіденційність під час передачі інформації в Інтернеті. Буде проведено докладний аналіз різних інструментів для анонімного перебування в мережі та оцінено їх ефективність, переваги та обмеження.

Мета полягає в виборі оптимального набору засобів, які будуть використані для розробки захищеного онлайн-сервісу. Важливо розуміти, що журналістам, які працюють з такою цінною інформацією, потрібні надійні інструменти, що дозволять їм захистити свої джерела та зберегти анонімність.

Інструментів для збереження анонімності в інтернеті є багато, тому було відібрано та проаналізовано найкращі з них. Для аналізу обрано наступні засоби для анонімного перебування в мережі: VPN, мережа Tor, мережа I2P.

Для полегшення порівняння було створено таблицю 1, яка містить стислий огляд VPN, Tor-мережі та I2P-мережі. Ця таблиця допоможе у виборі оптимального набору інструментів для розробки безпечного онлайн-сервісу, забезпечення захисту джерел та збереження анонімності журналістів. Розглядаючи різні критерії та характеристики цих інструментів, можна краще зрозуміти, наскільки вони відповідають поставленій меті.

Таблиця 1 – Порівняння інструментів для анонімного перебування в мережі

Критерії	VPN(за [1])	Мережа Tor (за [2])	Мережа I2P(за [3])
Анонімність	Забезпечує часткову анонімність	Забезпечує надійну анонімність	Забезпечує надійну анонімність
Шифрування	Шифрує дані між пристроєм користувача та VPN-сервером	Шифрує дані між пристроєм користувача та вузлами входу	Шифрує дані між пристроями користувача в мережі
Маскування IP-адрес	Замінює IP-адресу користувача на IP-адресу VPN-сервера	Маршрутизує трафік через кілька ретрансляторів, маскуючи IP-адресу користувача	Маршрутизує трафік через кілька проміжних вузлів, маскуючи IP-адресу користувача
Продуктивність	Як правило, швидше завдяки виділеним серверам та оптимізованим мережам	Може працювати повільніше через кілька реле та шарів шифрування	Може бути повільнішим через маршрутизацію через кілька вузлів і шарів шифрування
Доступність	Може бути обмежено в певних регіонах або країнах	Може обходити певні обмеження та цензуру	Може обходити певні обмеження та цензуру
Структура мережі	Централізована мережа	Децентралізована мережа з декількома ретрансляційними вузлами	Децентралізована мережа з декількома проміжними вузлами
Зручність для користувача	Зручний для використання з простими параметрами налаштування та конфігурації	Зручний для користувача інтерфейс, але може мати складнощі	Можуть знадобитися технічні знання та навички конфігурації

Проаналізувавши та порівнявши VPN, Tor-мережі та I2P-мережі, стає очевидним, що кожен інструмент має свої сильні та слабкі сторони з точки зору анонімності, шифрування, маскування IP-адреси, продуктивності, доступності та зручності для користувача. Однак, якщо розглядати конкретні вимоги до розробки безпечного онлайн-сервісу, то мережа Tor виявляється найбільш підходящим вибором.

Мережа Tor забезпечує надійну анонімність, маршрутизуючи трафік через кілька ретрансляторів, ефективно маскуючи IP-адресу користувача і ускладнюючи відстеження його онлайн-активності. Вона пропонує надійне шифрування і має добре зарекомендовану репутацію щодо конфіденційності та безпеки. Крім того, мережа Tor дозволяє користувачам обходити певні обмеження і цензуру, забезпечуючи доступ до інформації навіть у регіонах з обмеженою свободою Інтернету.

Також важливим аспектом захисту є безпечне зберігання особистих даних інсайдерів. Найкращий варіант це повна анонімізація користувача без використання конкретних особистих даних при реєстрації та публікації інсайдерської інформації. Тому найліпшим варіантом буде генерація імен та логінів користувача при реєстрації, які ніяк не будуть пов’язані з особистістю інсайдера. Але постає інша проблема, без використання прив’язки акаунту користувача до пошти або номера телефону стає неможливим функція відновлення паролю при його втраті. Для вирішення цієї проблеми пропонується використання секретних запитань, що будуть застосовуватися для процесу відновлення пароля без пошти чи номеру телефону.

При спілкуванні є можливість перехоплення переписки між інсайдером та іншими користувачами. Для вирішення цієї проблеми можна використовувати шифрування. Шифрування має бути наскрізним,

щоб навіть при викрадені бази даних, зловмисники не могли розшифрувати вміст переписок між користувачами.

При викладені інсайдерської інформації, публікації у вигляді фото можуть містити велику кількість даних, що можуть викрити або якось зашкодити інсайдеру. Тому пропонується введення механізму видалення метаданих у зображеннях, що підвищить безпеку та анонімність користувачів.

Також не слід забувати про використання ботів, що можуть зашкодити сайту. Для боротьби з ними пропонується використання капчі для перевірки користувача при реєстрації, вході, публікації та інших діях на безпечному онлайн-сервісі.

Висновок

Впроваджуючи ці методи захисту та анонімізації користувача, а також використовуючи мережу Tor для розміщення, онлайн-сервіс може створити надійну систему захисту конфіденційності, яка відповідає потребам журналістів та інсайдерів. Ця система сприяє збереженню цілісності інформації, якою обмінюються, захисту джерел та їх конфіденційності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Альшалан А., Пішароді С., Хуан Д. Огляд мобільних технологій VPN. IEEE Опитування та навчальні посібники з комунікацій. 2016. Т. 18, № 2. С. 1177–1196. URL: https://ieeexplore.ieee.org/abstract/document/7314859 (дата звернення: 19.05.2023).

2. Лоран М., Леваллуа-Барт К. Управління конфіденційністю та захист персональних даних. Управління цифровою ідентифікацією. 2015. Т. 9. С. 137–205. URL: https://www.sciencedirect.com/science/article/abs/pii/B9781785480041500043 (дата звернення: 19.05.2023).

3. I2P – чудовий варіант анонімності в Інтернеті. Ubunlog. URL: https://ubunlog.com/uk/i2p-una-excelente-opcion-para-el-anonimato-en-la-red/ (дата звернення: 19.05.2023).

Савчук Дар'я Олександрівна - студентка групи КІТС-19б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail dasha.savchuk.2001@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** – кандидат технічних наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: karpinets@gmail.com.

Savchuk Daria Oleksandrivna - student of KITS-19b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail dasha.savchuk.2001@gmail.com

Supervisor: Vasyl Vasylovich Karpinets - candidate of technical sciences, associate professor of the department of management and security of information systems, Vinnytsia National Technical University, Vinnytsia, e-mail: karpinets@gmail.com.