Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет “Львівська політехніка”

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІБІТ 2024

Збірник наукових праць
V Міжнародної науково-практичної конференції

27 листопада 2024 року

Львів – 2024

ББК 32.81+78.362
І 74

Інформаційна безпека та інформаційні технології: збірник наукових праць V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, Растр-7, 2024, 636 с.

ISBN 978-617-8537-86-9

ISBN 978-617-8537-86-9

ЧЛЕНИ ПРОГРАМНОГО КОМІТЕТУ:

Ростислав Львович ТКАЧУК – доктор технічних наук, професор, начальник кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності.

Олександр Володимирович ПРИДАТКО – кандидат технічних наук, доцент, проректор з навчальної та методичної роботи Львівського державного університету безпеки життєдіяльності.

Богдан Васильович ДУРНЯК – доктор технічних наук, професор, в.о. ректора Української академії друкарства.

Любомир Степанович СІКОРА – доктор технічних наук, професор, професор кафедри автоматизованих систем управління Національного університету "Львівська політехніка".

Валерій Богданович ДУДИКЕВИЧ – доктор технічних наук, професор, професор кафедри захисту інформації Національного університету "Львівська політехніка".

Іван Романович ОПІРСЬКИЙ – доктор технічних наук, професор, завідувач кафедри захисту інформації Національний університет "Львівська політехніка".

Ігор Михайлович ЖУРАВЕЛЬ – доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного університету "Львівська політехніка".

Максим Володимирович КОРОБЧИНСЬКИЙ – доктор технічних наук, професор п'ятої кафедри Воєнно-дипломатичної академія ім. Євгенія Березняка Міністерства оборони України.

Роман Святославович ЯКОВЧУК – доктор технічних наук, доцент, начальник факультету цивільного захисту, Львівський державний університет безпеки життєдіяльності.

Володимир Афанасійович РОМАКА – доктор технічних наук, професор, профе-

Викрадення або втрата пристрою	Автоматичне відключення доступу до ресурсів у разі заволодіння фізичним пристроєм, віддалене очищення критичних даних. Встановлення програм для дистанційного очищення, таких як Prey або Find My Device, допомагає швидко нейтралізувати загрозу несанкціонованого доступу з боку третіх осіб

Висновки. Децентралізоване середовище міжнародної рекламної агенції вимагає комплексного підходу до кібербезпеки та захисту інтелектуальних прав. Використання Zero Trust Architecture, багатофакторної автентифікації, UEBA- та SIEM-систем знижує ризики компрометації даних і забезпечує безпечний доступ до корпоративних ресурсів. Особисті пристрої потребують MDM, шифрування та засобів для віддаленого очищення даних.

Захист інтелектуальної власності на контент і витвори є ключовим для конкурентоспроможності агенції. DRM рішення запобігають несанкціонованому копіюванню, а моніторинг змін у хмарних середовищах і аудит дій користувачів забезпечують контроль. Відділ організації, відподідальний за кібербезпеку має забезпечити реагування на порушення, впроваджуючи технології захисту авторських прав і моніторинг контенту. Такий підхід гарантує як збереження даних, так і захист інтелектуальної власності, що є основою успіху агенції.

Інформаційні джерела

1. Verizon. Data Breach Investigations Report 2023. Verizon Communications, 2023. URL: https://www.verizon.com/business/resources/reports/dbir/

УДК 004.056.5

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАХИЩЕНИХ КАНАЛІВ, ПОБУДОВАНИХ НА ПРОТОКОЛАХ WIREGUARD ТА OPENVPN

Богдан ФІЛІПЧУК
Ростислав ТКАЧУК
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The article provides a comparative analysis of secure channels built on the WireGuard and OpenVPN protocols, with an emphasis on their performance, flexibility, compatibility, and security. WireGuard is characterized by high speed, ease of configuration, and modern cryptographic algorithms, which makes it optimal for mobile devices and simple networks. OpenVPN provides wide versatility, support for legacy systems and complex network architectures, but is inferior to WireGuard in speed and resource consumption. The conclusion emphasizes that the choice between the protocols depends on the context of use: WireGuard is suitable for fast and simple solutions, and*

OpenVPN is suitable for complex corporate environments with high requirements for configuration and compatibility.

Keywords: *WireGuard, OpenVPN, VPN protocol, performance, security, cryptography, compatibility, corporate networks.*

Анотація. *У статті здійснено порівняльний аналіз захищених каналів, побудованих на протоколах WireGuard та OpenVPN, з акцентом на їхню продуктивність, гнучкість, сумісність і безпеку. WireGuard вирізняється високою швидкістю, простотою налаштувань та сучасними криптографічними алгоритмами, що робить його оптимальним для мобільних пристроїв та простих мереж. OpenVPN забезпечує широку універсальність, підтримку застарілих систем і складних мережевих архітектур, але поступається WireGuard у швидкодії та ресурсозатратності. Висновок підкреслює, що вибір між протоколами залежить від контексту використання: WireGuard підходить для швидких і простих рішень, а OpenVPN – для складних корпоративних середовищ із високими вимогами до налаштувань і сумісності.*

Ключові слова: *WireGuard, OpenVPN, VPN-протокол, продуктивність, безпека, криптографія, сумісність, корпоративні мережі.*

У сучасному світі зростає потреба в захищених каналах зв’язку через збільшення кіберзагроз, витоків даних та конфіденційної інформації. Організації та особи прагнуть забезпечити безпечний зв’язок у їхніх онлайн-діях, що підвищує актуальність вивчення сучасних протоколів, таких як WireGuard та OpenVPN.

Метою даної роботи є порівняння протоколів WireGuard і OpenVPN за ключовими характеристиками: безпекою, продуктивністю та зручністю використання. Завдання полягає у вивченні особливостей кожного з протоколів, доходячись до рекомендацій щодо їх використання в різних сценаріях.

WireGuard – це сучасний, високошвидкісний і безпечний VPN-протокол із мінімальною кодовою базою, розроблений для спрощення налаштування та підвищення продуктивності мережі. Його відрізняє мінімалізм і орієнтованість на безпеку, що робить його особливо затребуваним у конфіденційних та продуктивних VPN-системах. Важливою особливістю WireGuard є мінімальна база кодів: він складається лише з кількох тисяч рядків коду, що проводить аудит і перевірку на вразливість у порівнянні з іншими VPN-протоколами, такими як OpenVPN чи IPsec. Це полегшує виявлення та усунення ваших проблем безпеку [1].

WireGuard використовує сучасні криптографічні алгоритми, зокрема ChaCha20 для шифрування, Poly1305 для аутентифікації, Curve25519 для обміну ключами та BLAKE2s для хешування, що забезпечує надійний захист даних і високу продуктивність. Налаштування WireGuard максимально просто й може обмежувати інсталяційні ключі та IP-адресу, що робить його зручним як для адміністраторів, так і для кінцевих корінь.

Протокол забезпечує високу швидкість передачі даних і низьких затримок, працює на рівнях ядра Linux, завдяки чому перевершує продуктивність

багатьох інших VPN-протоколів, особливо на мобільних та вбудованих пристроях. Також WireGuard підтримує роумінг і автоматично відновлює з'єднання при зміні IP-адреси, що особливо зручно для користувачів, які часто змінюють мережу. У протоколі використовується модель ключів без статичної IP-адресації, де обмін ключами побудований на методі криптографічної перевірки ідентифікаторів, що знижує ймовірність витоку даних і ускладнює аналіз трафіку. Завдяки своїй простоті, безпеці та високій продуктивності WireGuard широко використовується в корпоративних і хмарних VPN-мерах [2].

OpenVPN є одним із найпопулярніших та багатофункціональних VPN-протоколів, що забезпечує високу гнучкість у налаштуванні та сумісність із різними мережевими конфігураціями. Використовуючи криптографічні алгоритми, такі як AES для шифрування та SHA для хешування, OpenVPN забезпечує високий рівень захисту даних при їх передачі через незахищені мережі. Завдяки інтеграції з OpenSSL протокол підтримує функції аутентифікації, включно із сертифікатами та двофакторною аутентифікацією, що підвищує надійність підключення [3].

Особливістю OpenVPN є його здатність працювати як на UDP, так і на TCP-портах, що дозволяє ефективно обходити мережеві обмеження та підтримувати стабільність з'єднання в умовах фільтрації трафіку. Додатково, можливість роботи через порт HTTPS забезпечує приховування VPN-трафіку серед звичайного веб-трафіку, що є важливим для обхід блокувань у країнах із суворою цензурою. OpenVPN підтримує як точка-точка, так і клієнт-сервер архітектури, що робить його придатним як для персонального, так і для корпоративного використання [4–6].

Протокол вирізняється підтримкою широкого спектра платформ, включно з Windows, macOS, Linux, Android та iOS, що забезпечує універсальність його використання. Для адміністраторів OpenVPN пропонує розширені можливості управління, такі як налаштування рівнів доступу, обмеження швидкості та дозволів, що робить його ефективним рішенням для корпоративних мереж зі складними політиками безпеки. Поєднання високої гнучкості, надійного шифрування та сумісності робить OpenVPN провідним VPN-протоколом, придатним для застосування у різноманітних мережевих середовищах [7–9].

WireGuard і OpenVPN є провідними VPN-протоколами, але мають різні переваги. WireGuard вирізняється швидкістю, мінімалістичним дизайном і сучасними криптографічними алгоритмами, що робить його ідеальним для мобільних пристроїв та простих конфігурацій. Завдяки мінімальній кодовій базі він забезпечує високий рівень безпеки та простоту використання, але обмежений у гнучкості для складних сценаріїв. OpenVPN, натомість, пропонує широку сумісність, багаті налаштування та підтримку навіть застарілих систем, що робить його незамінним у корпоративних середовищах і мережах із суворими обмеженнями. Проте OpenVPN поступається WireGuard у

швидкості, простоті й продуктивності, але залишається надійним вибором для складних та універсальних VPN-рішень (табл. 1) [10–11].

Таблиця 1.

Порівняння OpenVPN та WireGuard

Характеристика	*WireGuard*	*OpenVPN*
Кодова база	Мінімальна (~4 тис. рядків), легка для аудиту	Велика, складна для перевірки (~сотні тисяч рядків)
Швидкість	Висока, мінімальні затримки завдяки роботі в ядрі Linux	Помірна, вища затримка через роботу в користувацькому просторі
Гнучкість	Мінімалістична, прості налаштування, обмежений функціонал	Висока, підтримка складних конфігурацій і багатих налаштувань
Сумісність	Залежність від сучасних ОС, менше підтримки старих платформ	Універсальна, підтримка навіть застарілих пристроїв
Безпека	Використовує лише сучасні алгоритми, без “старих” опцій	Гнучкість налаштувань може призвести до помилок безпеки
Мобільність	Швидке перепідключення, ідеально для роумінгу	Затримки при перепідключенні через зміну мереж

На основі порівняння WireGuard та OpenVPN можна зробити висновок, що кожен із протоколів має свої переваги і обмеження, що визначають їхню доцільність для конкретних завдань (рис. 1).

Рисунок 1 – Протоколи VPN: WireGuard та OpenVPN

WireGuard демонструє високу продуктивність завдяки мінімалістичній архітектурі, роботі на рівні ядра операційної системи та використанню сучасних криптографічних алгоритмів, що робить його ідеальним вибором для мобільних пристроїв, динамічних середовищ і мережевих сценаріїв із високими вимогами до швидкості та ефективності. Водночас OpenVPN забезпе-

чує широку сумісність і гнучкість, підтримуючи великий спектр платформ, алгоритмів шифрування та розширених налаштувань, що є критично важливим для складних корпоративних середовищ, мереж із застарілими системами та умов, де необхідна максимальна адаптивність. Проте простота та продуктивність WireGuard роблять його менш придатним для складних сценаріїв із численними користувачами чи специфічними вимогами до мережевої архітектури, тоді як OpenVPN може бути менш ефективним у швидкості та ресурсозатратнішим через свою складність.

Висновки. Таким чином, вибір протоколу залежить від контексту використання: WireGuard оптимальний для сучасних і простих конфігурацій, тоді як OpenVPN залишається незамінним у задачах, що вимагають гнучкості, універсальності та підтримки складних інфраструктур. Вибір між WireGuard та OpenVPN слід робити залежно від завдань: обирайте WireGuard для швидких і простих конфігурацій, а OpenVPN – для складних середовищ із високими вимогами до гнучкості та сумісності.

Інформаційні джерела

1. OpenVPN vs WireGuard: який VPN краще? URL: https://hyperhost.ua/info/uk/openvpn-vs-wireguard-yakii-vpn-krashhe (дата звернення: 15.11.2024).

2. Stallings W. (2000). Network Security Essentials: Applications and Standards (pp. 45–60). Prentice Hall.

3. Snader J. C. (2006). VPNs Illustrated: Tunnels, VPNs, and IPsec (pp. 78–102). Addison-Wesley.

4. Donenfeld J. A. (2020). WireGuard: Next-Generation VPN (pp. 15–30). WireGuard.

5. Keijser J. J., & Ali S. (2014). The OpenVPN Cookbook (pp. 34–56). O'Reilly Media.

6. Sanders C., & Smith J. (2013). Applied Network Security Monitoring: Collection, Detection, and Analysis (pp. 120–135). Syngress.

7. Information-resource and cognitive concept of threat's influence identification on technogenic system based on the cause and category diagrams integration. L. Sikora, N Lysa, I. Dronyuk, O. Fedevych, R. Tkachuk, R. Talanchuk. CEUR Workshop Proceedings, pp. 398–416.

8. Military Applications of Data Analytics. New York : Auerbach Publications, 2018. 218 c.

9. Information and laser technologies for data flow selection and their cognitive interpretation in automated control systems. B. V. Durnyak, B. V. Durniak, L. S. Sikora, N. K. Lysa, R. L. Tkachuk, B. I. Yavorsky. Lviv: Ukrainian Academy of Printing.

10. Когнітивні моделі формування стратегій оперативного управління інтегрованими ієрархічними структурами в умовах ризиків і конфліктів: Монографія. Б. В. Дурняк, Л. С. Сікора, М. С. Антоник, Р. Л. Ткачук. Львів: Українська академія друкарства, 2013. – 449 с.

11. Порівняння протоколів VPN. URL: https://www.vpnunlimited.com/ua/help/vpn-protocols/comparison?srsltid=AfmBOooMlsJoDp4YGFAbJc4Q0JkV676mdjOzB3DziB23SqrLfBimjJw7 (дата звернення: 15.11.2024).

НАПРЯМ 5.
ГЕНДЕР У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ