УДК 004.77.056

# МЕТОД ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ДОСТУПУ ДО РЕСУРСІВ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Романов Д.О.
e-mail: daniil.romanov1@nure.ua
Науковий керівник – ас. Чепурна І.С.
Харківський національний університет радіоелектроніки, каф. ЕОМ
м. Харків, Україна

Останні десятиліття характеризуються стрімким розвитком інформаційних технологій, що зумовлює еволюцію IT-екосистем в бізнес-середовищі та державному секторі. Період глобального локдауну, спричиненого COVID-19, воєнні конфлікти та активне впровадження технологій віртуалізації і хмарних рішень зумовили перехід до гнучких моделей організації бізнес-процесів [1]. Такі моделі передбачають широке залучення віддалених працівників і потребують забезпечення оперативного та безпечного доступу до корпоративних ресурсів.

В таких умовах традиційні підходи до інформаційної безпеки, що обмежуються захистом периметра локальної мережі, виявляються недостатніми для забезпечення належного рівня захисту корпоративних ресурсів. Водночас зростання кількості користувачів мережі Інтернет супроводжується підвищенням ризиків несанкціонованого доступу, перехоплення та витоку інформації, особливо під час передачі даних через відкриті канали зв'язку [2].

Таким чином, актуалізується потреба в розробці та впровадженні ефективних методів забезпечення конфіденційності, цілісності та автентичності даних при їх передачі незахищеними мережами зв'язку.

Існуючі методи організації захищеного доступу включають використання проксі-серверів, міжмережних екранів та технологій віртуальних приватних мереж (VPN). Застосування проксі-серверів дозволяє приховати реальну IP-адресу користувача, а міжмережні екрани реалізують контроль мережного трафіку на основі визначених правил безпеки. Проте застосування проксі-серверів та міжмережних екранів не забезпечують повною мірою захист даних під час їх передачі відкритими каналами зв'язку з високим рівнем конфіденційності та цілісності даних.

Водночас комплексний підхід, що ґрунтується на використанні технологій тунелювання в поєднанні з криптографічними методами захисту інформації, що реалізовані у VPN, забезпечує організацію захищеного каналу передачі даних. Це дозволяє забезпечити конфіденційність, цілісність та автентичність даних при передачі незахищеними мережами [3].

Метою роботи є розробка методу організації захищеного доступу до ресурсів корпоративної комп'ютерної мережі, що забезпечує високий рівень

захисту даних від ризиків несанкціонованого доступу, перехоплення та витоків інформації.

Досягнення поставленої мети передбачає огляд останніх досліджень і публікацій щодо існуючих методів організації захищеного доступу та аналіз принципів функціонування віртуальних приватних мереж та протоколів, що використовуються для побудови захищених тунелів.

Запропонований метод організації захищеного доступу до корпоративних ресурсів комп'ютерної мережі базується на реалізації віртуального захищеного каналу між сервером корпоративної мережі та віддаленими користувачами (рис. 1).

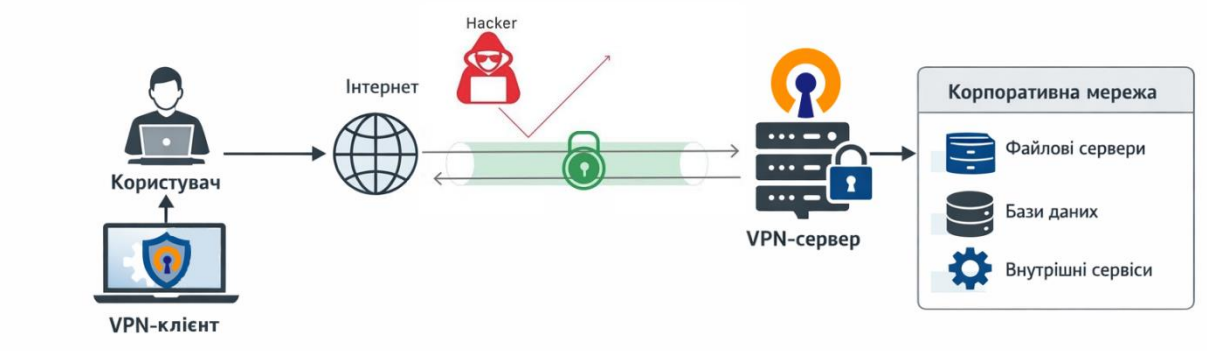


Рисунок 1 – Схема організації захищеного доступу до ресурсів корпоративної комп'ютерної мережі

Вибір протоколу OpenVPN для організації захищеного доступу до корпоративних ресурсів обґрунтовується його характеристиками та високим рівнем безпеки. OpenVPN підтримує сучасні криптографічні алгоритми, зокрема AES-256, що забезпечує надійне шифрування даних під час їх передачі через відкриті мережі зв'язку. Протокол є сумісним із різними операційними системами та хмарними платформами, що забезпечує його застосування в інформаційних системах з гетерогенною інфраструктурою [4].

OpenVPN реалізує передачу еластичних та нееластичних даних з підтримкою TCP та UDP-з'єднань, що дозволяє забезпечити задовільну продуктивність каналу зв'язку. Крім того, протокол передбачає інтеграцію з існуючими системами контролю доступу та корпоративними політиками безпеки, що сприяє мінімізації ризиків несанкціонованого доступу до ресурсів корпоративної комп'ютерної мережі.

Запропонований метод базується на використанні протоколу OpenVPN та криптографічного алгоритму AES-256 для побудови захищеного віртуального тунелю між віддаленим користувачем та ресурсами корпоративнї комп'ютерної мережі. Практична реалізація здійснюється на базі ОС Ubuntu 20LTS. Процес налаштування включає генерацію сертифікатів, ключів сервера та клієнта, параметрів криптографічного алгоритму Діффі-Хеллмана. Конфігурування сервера OpenVPN передбачає

пере направлення трафіку та налаштування правил файрволу для підвищення рівня безпеки з’єднань.

В результаті проведеного дослідження запропонований метод організації захищеного доступу на основі протоколу OpenVPN дозволяє реалізувати надійний захищений канал зв’язку між віддаленими користувачами та ресурсами корпоративної комп’ютерної мережі відповідно до підвищених вимог до конфіденційності та цілісності інформації. Такий підхід сприяє мінімізації ризиків несанкціонованого доступу, модифікації та ризиків витоку інформації під час доступу до ресурсів корпоративної комп’ютерної мережі. Подальші наукові дослідження доцільно спрямувати на розробку та вдосконалення механізмів VPN-з’єднань в агрегованих системах доставки контенту, що дозволить підвищити ефективність, відмовостійкість та масштабованість захищених корпоративних комп’ютерних мереж.

Список використаних джерел

1. He W., Zhang Z., Li W. Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. International Journal of Information Management. 2021. Vol. 57. P. 102287. URL: https://doi.org/10.1016/j.ijinfomgt.2020.102287

2. Network Security Concepts, Dangers, and Defense Best Practical. *Computer Engineering and Intelligent Systems*. 2023. URL: https://doi.org/10.7176/ceis/14-2-03 (дата звернення: 02.03.2026).

3. Чепурна І. С. Алгоритм організації віддаленого доступу до захищеного сегменту корпоративних комп’ютерних мереж. Радіоелектроніка та молодь у XXI столітті: матеріали 28-го Міжнар. молодіж. форуму, 16–18 квітня 2024 р. Харків : ХНУРЕ, 2024. Т. 5. С. 76–78. DOI: https://doi.org/10.30837/IYF.PCEIP.2024.076.

4. Верховський І., Ткачов В. Методи побудови віртуальних тунелів extranet-систем. Scientific review. 2023. Т. 4, No 89. С. 22. URL: https://doi.org/10.26886/2311-4517.4(89)2023.2