УДК 004.056.5

**І. С. Зоря**
**А.А. Гулевата**

# АРХІТЕКТУРА ТА ОРГАНІЗАЦІЯ БЕЗПЕКИ ПРОГРАМНОГО VPN-РІШЕННЯ З ПІДВИЩЕНИМ РІВНЕМ ШИФРУВАННЯ ДЛЯ КОРПОРАТИВНИХ КОРИСТУВАЧІВ

Вінницький національний технічний університет

***Анотація.*** *У роботі розглянуто архітектурні підходи до побудови безпечного програмного VPN-рішення з підвищеним рівнем шифрування для корпоративних користувачів. Проаналізовано сучасні механізми криптографічного захисту, зокрема застосування алгоритму AES-256, протоколів TLS 1.3 та механізму Perfect Forward Secrecy. Окрему увагу приділено організації автентифікації, управлінню ключами, журналюванню подій та реалізації принципів Zero Trust. Обґрунтовано необхідність комплексного підходу до побудови архітектури безпеки для мінімізації ризиків витоку інформації та несанкціонованого доступу в корпоративних інформаційних системах.*

***Ключові слова:*** *VPN, кібербезпека, архітектура безпеки, AES-256, Zero Trust, корпоративна мережа, криптографічний захист.*

***Abstract.*** *The paper examines architectural approaches to designing a secure software-based VPN solution with enhanced encryption for corporate users. Modern cryptographic protection mechanisms are analyzed, including AES-256 encryption, TLS 1.3 protocols, and Perfect Forward Secrecy. Special attention is given to authentication mechanisms, key management, security event logging, and the implementation of Zero Trust principles. The necessity of a comprehensive security architecture approach to minimize risks of data leakage and unauthorized access in corporate information systems is substantiated.*

***Keywords:*** *VPN, cybersecurity, security architecture, AES-256, Zero Trust, corporate network, cryptographic protection.*

## Вступ

У сучасних умовах цифрової трансформації підприємств та поширення віддалених форматів роботи забезпечення безпечного доступу до корпоративних ресурсів стає одним із ключових завдань кібербезпеки. Передача службової інформації через відкриті мережі створює підвищені ризики перехоплення даних та несанкціонованого доступу [1].

Одним із ефективних інструментів захисту мережевої взаємодії є технологія Virtual Private Network (VPN), що дозволяє створювати зашифрований тунель між користувачем та корпоративною інфраструктурою [1;2]. Проте сучасні умови функціонування інформаційних систем потребують удосконалення архітектурних підходів із урахуванням новітніх криптографічних стандартів та принципів Zero Trust [7].

Метою роботи є дослідження архітектури та організаційних аспектів забезпечення безпеки програмного VPN-рішення з підвищеним рівнем шифрування для корпоративних користувачів.

## Основна частина

Архітектура безпечного VPN-рішення повинна базуватися на принципах багаторівневого захисту (defense in depth), що передбачає поєднання криптографічних, програмних та організаційних механізмів безпеки [1].

Основою захисту каналу передачі даних є використання стійких алгоритмів симетричного шифрування, зокрема Advanced Encryption Standard із довжиною ключа 256 біт (AES-256), який рекомендований міжнародними стандартами криптографії [6]. Даний алгоритм забезпечує високий рівень стійкості до сучасних методів криптоаналізу.

Для встановлення захищеного з’єднання доцільно застосовувати протокол TLS версії 1.3, що визначений у RFC 8446 та забезпечує покращену продуктивність і зменшену поверхню атаки [3]. Серед

сучасних реалізацій VPN-протоколів доцільно відзначити WireGuard, який характеризується мінімалістичною архітектурою та підвищеним рівнем безпеки [4].

Важливим компонентом архітектури є реалізація механізму Perfect Forward Secrecy, що гарантує неможливість розшифрування попередніх сесій навіть у разі компрометації довгострокових ключів [1]. Це суттєво зменшує ризики масового розкриття конфіденційної інформації.

Організація безпеки VPN-рішення передбачає впровадження багатофакторної автентифікації, централізоване управління сертифікатами, застосування моделей розмежування доступу (RBAC), а також постійний моніторинг подій безпеки відповідно до рекомендацій міжнародних стандартів управління інформаційною безпекою [8; 9].

Особливу роль відіграє реалізація концепції Zero Trust Architecture, згідно з якою жоден користувач або пристрій не вважається довіреним за замовчуванням [7]. Кожна спроба доступу повинна проходити процедуру перевірки автентичності, авторизації та відповідності політикам безпеки.

Додатковими механізмами підвищення рівня захисту є функція «kill switch», запобігання витоку DNS-запитів, автоматичне перепідключення (failover) та журналювання подій для подальшого аудиту й аналізу інцидентів.

## Висновок

Таким чином, побудова архітектури безпечного програмного VPN-рішення для корпоративних користувачів потребує комплексного підходу, що поєднує сучасні криптографічні алгоритми, ефективні механізми автентифікації та організаційні заходи контролю доступу [6; 7].

Інтеграція протоколу TLS 1.3 [3], алгоритму AES-256 [6] та принципів Zero Trust [7] дозволяє мінімізувати ризики несанкціонованого доступу, витоку конфіденційної інформації та забезпечити належний рівень захисту корпоративних інформаційних систем.

Запропоновані архітектурні підходи можуть бути використані під час проєктування сучасних програмних рішень у сфері кібербезпеки інформаційних технологій.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Stallings W. Cryptography and network security: principles and practice. 7th ed. Pearson, 2017. 768 p.
2. Kaufman C., Perlman R., Speciner M. Network security: private communication in a public world. 2nd ed. Prentice Hall, 2002. 720 p.
3. Rescorla E. The transport layer security (TLS) protocol version 1.3. RFC 8446. IETF, 2018. 160 p.
4. Donenfeld J. WireGuard: next generation kernel network tunnel [Електронний ресурс]. 2020. Режим доступу: https://www.wireguard.com (дата звернення: 16.02.2026).
5. National Institute of Standards and Technology (NIST). Digital signature standard (DSS). FIPS PUB 186-4. Gaithersburg, 2013.
6. National Institute of Standards and Technology (NIST). Advanced encryption standard (AES). FIPS PUB 197. Gaithersburg, 2001.
7. Rose S., Borchert O., Mitchell S., Connelly S. Zero trust architecture. NIST Special Publication 800-207. Gaithersburg, 2020.
8. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva, 2022.
9. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva, 2022.
10. OWASP Foundation. OWASP Top 10: The ten most critical web application security risks [Електронний ресурс]. 2021. Режим доступу: https://owasp.org (дата звернення: 16.02.2026).



***Гулевата Анжеліка Андріївна*** **–** студентка групи КІТС-25м, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: gulevataanzhelika@gmail.com

Науковий керівник: ***Зоря Ірина Сергіївна*** – ас. каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: ira.zoria@vntu.edu.ua

***Hulevata Anzhelika A.***– student of group CITS-25m, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: gulevataanzhelika@gmail.com

Supervisor: ***Zoria Iryna S.*** – assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: ira.zoria@vntu.edu.ua