УДК 004.72/0.738:004.77 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.66

І. С. ЧЕПУРНА
асистентка кафедри електронних обчислювальних машин
Харківський національний університет радіоелектроніки
ORCID: 0009-0008-2442-6221

# МЕТОД ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО СЕГМЕНТА ПРИВАТНИХ SDN-МЕРЕЖ НА ОСНОВІ ПРОТОКОЛУ BITTORRENT

*В статті запропоновано метод організації захищеного сегмента приватної SDN-мережі з використанням протоколу BitTorrent для передачі даних. Цей метод поєднує гнучкість централізованого управління, що реалізується SDN-контролером, з високою ефективністю розподіленої передачі даних між вузлами ізольованого захищеного сегмента мережі.*

*Для досягнення поставленої мети було проведено експериментальне моделювання та дослідження трьох варіантів організації захищеного доступу до сегмента корпоративної комп'ютерної мережі на базі локальної мережі кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки. В першій моделі реалізовано доступ із використанням протоколу OpenVPN, що забезпечує базову конфіденційність та цілісність даних, але обмежує масштабованість системи та відмовостійкість. Друга модель передбачала застосування протоколу BitTorrent для організації захищеної та розподіленої передачі даних між вузлами, проте вона не забезпечує централізованого контролю. Третя модель, на якій ґрунтується запропонований метод, передбачає побудову логічно ізольованого SDN-сегмента, що враховує обмеження попередніх моделей. Передача даних в межах цього сегменту здійснюється за допомогою протоколу BitTorrent, що дозволяє розвантажити центральні канали та забезпечити відмовостійкість окремих вузлів. Водночас, централізований SDN-контролер забезпечує моніторинг, маршрутизацію та контроль доступу, забезпечуючи високий рівень безпеки. Таке поєднання мінімізує затримки, оптимізує використання мережних ресурсів та підвищує загальну пропускну здатність системи.*

*Оцінка запропонованого підходу показала, що використання логічно ізольованих сегментів у SDN-мережах сприяє зменшенню внутрішніх затримок та покращує контроль над маршрутизацією трафіку. Отримані результати підтверджують практичну доцільність застосування запропонованого методу для побудови захищених і високопродуктивних сегментів корпоративних мереж з метою забезпечення надійної передачі даних.*

***Ключові слова:*** *SDN, Bittorrent, децентралізація, безпека, затримка.*

I. S. CHEPURNA
Assistant at the Department of Electronic Computers
Kharkiv National University of Radio Electronics
ORCID: 0009-0008-2442-6221

## MULTI-LEVEL VPN-TUNNELING METHOD FOR ENSURING REMOTE ACCESS TO EXTRANET NETWORK NODES

*The article proposes a method for organizing a secure segment of a private SDN network using the BitTorrent protocol for data transmission. This method combines the flexibility of centralized management, implemented through an SDN controller, with the high efficiency of distributed data transfer between Nodes of an isolated secure network segment.*

*To achieve the stated goal, experimental modeling and the study of three variants of secure access organization to a segment of a corporate computer network were conducted based on the local network of the Department of Electronic Computers at Kharkiv National University of Radio Electronics. In the first model, access was implemented using the OpenVPN protocol, which provides basic data confidentiality and integrity but limits system scalability and fault tolerance. The second model involved the use of the BitTorrent protocol to organize secure and distributed data transfer between Nodes; however, it does Not provide centralized control. The third model, which underlies the proposed method, involves the construction of a logically isolated SDN segment that addresses the limitations of the previous models. Data transmission within this segment is carried out using the BitTorrent protocol, which helps offload central channels and ensure fault tolerance of individual Nodes. Simultaneously, the centralized SDN controller provides monitoring, routing, and access control, ensuring a high level of security. This combination minimizes latency, optimizes the use of network resources, and increases the overall throughput of the system.*

*The evaluation of the proposed approach demonstrated that the use of logically isolated segments in SDN networks contributes to the reduction of internal delays and enhances control over traffic routing. The obtained results confirm the practical feasibility of applying the proposed method to construct secure and high-performance segments of corporate networks to ensure reliable data transmission.*

***Key words:*** *SDN, Bittorrent, decentralization, security, latency.*

© Чепурна І. С., 2025
Стаття поширюється на умовах ліцензії CC BY 4.0

**Постановка проблеми**

В сучасних корпоративних комп'ютерних мережах зростає потреба в оптимізації методів передачі великих обсягів даних.

На тлі стрімкого розвитку розподілених систем дедалі більшого поширення набуває концепція програмно-конфігурованих мереж (SDN), яка ґрунтується на централізованому управлінні маршрутами та політиками доступу для передачі даних [1]. Це забезпечує динамічну адаптацію мережної інфраструктури до змін трафіку в режимі реального часу, підвищуючи ефективність функціонування мережі. Згідно з даними Global Market Insights, обсяг світового ринку SDN у 2023 році склав 28,2 млрд доларів США, з прогнозованим середньорічним темпом зростання понад 17 % у період 2024–2032 років [2]. Це свідчить про зростаючий попит на інноваційні рішення, орієнтовані на гнучкість, централізований контроль та підвищений рівень безпеки у віртуалізованих середовищах.

Розподілені системи обміну інформацією, зокрема пірингові мережі, сприяють підвищенню масштабованості, відмовостійкості та ефективному використанню обчислювальних і мережних ресурсів [3, 4]. Протокол BitTorrent, як один з найпоширеніших у піринговых мережах, призначений для передачі великих обсягів даних шляхом їх фрагментації та розподіленої передачі між учасниками мережі [5–7]. Проте в корпоративних мережах його застосування ускладнюється через високе навантаження на сервери, нестабільність маршрутів, відсутність централізованого контролю за трафіком, що збільшує затримки та ускладнює моніторинг. Крім того, використання BitTorrent підвищує ризики несанкціонованого доступу до критичних вузлів та витоку конфіденційної інформації, що обмежує його застосування в корпоративних інфраструктурах [8].

Постійне зростання обсягів даних вимагають від сучасних корпоративних мереж поєднання гнучкості та масштабованості розподілених систем з централізованим управлінням, властивим архітектурі SDN. Традиційні VPN-рішення забезпечують захист каналів, але не гарантують оптимальної пропускної здатності в разі інтенсивного обміну великими обсягами даних між віддаленими сегментами. Водночас, протокол BitTorrent ефективно розподіляє навантаження між вузлами, проте його застосування в корпоративному середовищі обмежене через відсутність централізованого контролю доступу, складність моніторингу та ризик витоку конфіденційної інформації [9].

Отже, актуальним завданням є розробка та впровадження методу, який інтегрує механізми SDN для централізованого управління маршрутизацією та політиками безпеки з перевагами протоколів одноранговых мереж для розподіленої передачі даних. Це дозволить мінімізувати затримки, підвищити ефективність використання ресурсів та забезпечити захист критичних вузлів.

**Аналіз останніх досліджень і публікацій**

Останні дослідження в галузі віртуальних комп'ютерних мереж акцентують увагу на інтеграції технологій пірингового обміну даними з централізованими моделями управління трафіком, що реалізуються в SDN [10–15]. Попри переваги, які надає кожен з підходів, залишаються невирішеними питання забезпечення балансу між масштабованістю, властивою P2P-мережам, та можливостями централізованого контролю, характерними для SDN-архітектур. Для аналізу існуючих підходів та оцінки ефективності таких рішень було здійснено огляд наукових публікацій і досліджень, що розкривають актуальні проблеми оптимізації продуктивності, мінімізації затримок та підвищення гнучкості мережної інфраструктури в умовах високих навантажень.

В роботі [10] досліджено поєднання реактивних алгоритмів маршрутизації з P2P-протоколами, зокрема BitTorrent. Однак автори відзначають, що хоча такий підхід сприяє розвантаженню центральних вузлів і покращує масштабованість, динамічне формування правил маршрутизації для кожного нового з'єднання може збільшувати затримки та ускладнювати управління пропускною здатністю, що негативно впливає на якість обслуговування.

Переваги програмно-конфігурованих мереж, зокрема чітке розділення площин керування та передачі даних, описані в роботі [11]. Це забезпечує можливість програмованого управління маршрутами та політиками доступу в режимі реального часу. Однак автори підкреслюють, що централізована архітектура SDN створює вразливість в разі компрометації центрального контролера, що може призвести до повної втрати управління мережею. Тому для інтеграції з P2P-системами пропонується багаторівнева система захисту, що враховує класифікацію можливих атак і передбачає розподіл функцій контролю між кількома вузлами.

Для вирішення проблеми перевантаження в SDN-мережах, в роботі [12] автори пропонують багатоклієнтську платформу, що забезпечує надання ізольованих інтерфейсів кожному клієнту, а також реалізує функції розподілу ресурсів та ізоляції трафіку. Для уникнення перевантаження та досягнення енергозбереження, впроваджено схему маршрутизації, яка фокусує трафік на мінімальній кількості каналів, переводячи інші комутатори в «сплячий» режим. Цей підхід значно покращує використання пропускної здатності, зменшує середню затримку та підвищує загальну продуктивність SDN-мережі.

В роботі [13] автори зазначають, що масштабованість в існуючих SDN-архітектурах часто досягається за рахунок використання багатьох контролерів, що призводить до перевантаження та ускладнює балансування навантаження. Для вирішення цих проблем пропонується підхід, що забезпечує послідовний зв'язок між центральним контролером, підлеглими контролерами, які керують окремими сегментами, та пристроями. Це дозволяє значно підвищити масштабованість мережі без надмірної складності.

В роботі [14] наведено підхід до побудови приватних SDN-сегментів з вбудованими механізмами розподіленої передачі даних, що дозволяє мінімізувати внутрішні затримки та забезпечувати контрольований доступ до ресурсів. Автори відзначають, що ізоляція сегментів мережі знижує ризики витоку конфіденційної інформації, а використання BitTorrent у межах приватної інфраструктури з централізованим моніторингом сприяє підвищенню ефективності та відмовостійкості системи.

Дослідження [15] підкреслює економічну доцільність інтеграції SDN з P2P-протоколами в корпоративних середовищах. Завдяки інтелектуальному вибору маршрутів та оптимізації розподілу трафіку досягається значне зниження навантаження на сервери та скорочення часу доставки великих обсягів даних, що особливо актуально для медіаконтенту та резервного копіювання в розподілених інфраструктурах.

Таким чином, аналіз останніх досліджень і публікацій [10-15] показує, що інтеграція можливостей P2P-протоколів, зокрема BitTorrent, з централізованим управлінням SDN є перспективним напрямом для оптимізації корпоративних комп'ютерних мереж. Поєднання масштабованості та автономності пірингових систем з гнучкістю, безпекою та контролем SDN відкриває можливості створення мережної інфраструктури з високою продуктивністю, стійкістю до збоїв та адаптивним управлінням ресурсами.

**Формулювання мети дослідження**

Метою дослідження є розробка методу інтеграції протоколу BitTorrent в приватні сегменти програмно-конфігурованих мереж для забезпечення ефективної та безпечної передачі великих обсягів даних в корпоративних мережах. Запропонований метод дає змогу мінімізувати затримки передачі, оптимізувати використання мережних ресурсів та знизити ризики несанкціонованого доступу до конфіденційних даних, особливо в умовах обмеженості обчислювальних ресурсів.

**Викладення основного матеріалу дослідження**

Для підвищення безпеки передачі даних в корпоративних комп'ютерних мережах традиційно застосовуються технології віртуальних приватних мереж (VPN), які забезпечують конфіденційність, цілісність та автентичність інформаційних потоків. Модель передачі даних через VPN на основі OpenVPN передбачає використання єдиного захищеного тунелю, що з'єднує клієнтський вузол з серверним сегментом корпоративної мережі за маршрутом «клієнт – VPN-сервер – цільовий вузол» (рис. 1) [16].

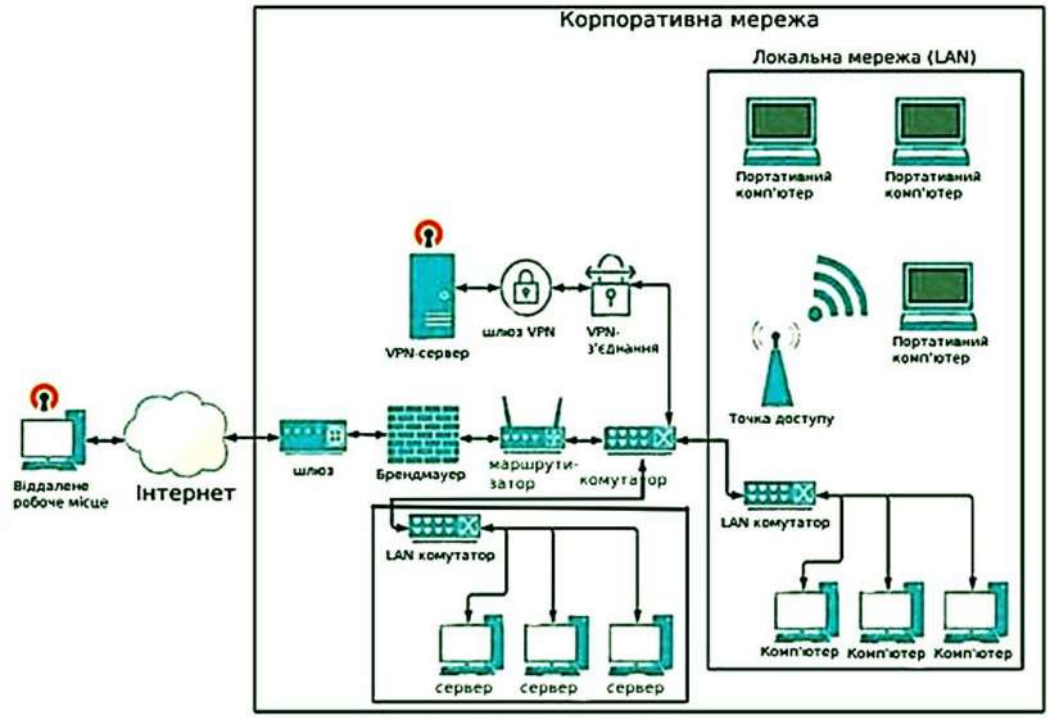


**Рис. 1. Модель сегменту корпоративної мережі з OpenVPN-доступом**

Надалі архітектура поступово ускладнюється від базової VPN-конфігурації до комбінованої схеми SDN + VPN + BitTorrent, що передбачає моделювання ізольованого сегмента приватної SDN-мережі. Це дозволяє поєднати захищений канал зв'язку на основі VPN з високою ефективністю передачі даних в складних мережних інфраструктурах в умовах підвищених вимог до безпеки передачі даних та обмежених апаратних ресурсах.

Базова модель передбачає шифрування трафіку стандартними криптографічними алгоритмами, які реалізуються обраним протоколом, автентифікація користувачів забезпечує контроль доступу та реалізацію політик

безпеки відповідно до їх прав і привілеїв, що гарантує конфіденційність та цілісність даних. Основними перевагами цього підходу є простота конфігурації та адміністрування, а також висока сумісність з широким спектром клієнтських пристроїв та операційних систем.

Модель, що поєднує VPN-доступ на основі OpenVPN з передачею даних через протокол BitTorrent, покликана усунути обмеження традиційних централізованих систем, ефективність яких суттєво знижується під час пікових навантажень, особливо в корпоративних мережах з підвищеними вимогами до надійності та відмовостійкості (рис. 2). Функціонування цієї моделі передбачає, що клієнтський вузол спочатку встановлює захищене з'єднання з VPN-сегментом, після чого обмін інформацією здійснюється в межах децентралізованої пірингової мережі BitTorrent. Це дає змогу вузлам взаємодіяти безпосередньо, розподіляючи трафік та обчислювальні ресурси, що забезпечує високу швидкість та стабільність передавання великих обсягів даних при збереженні захищених каналів доступу.

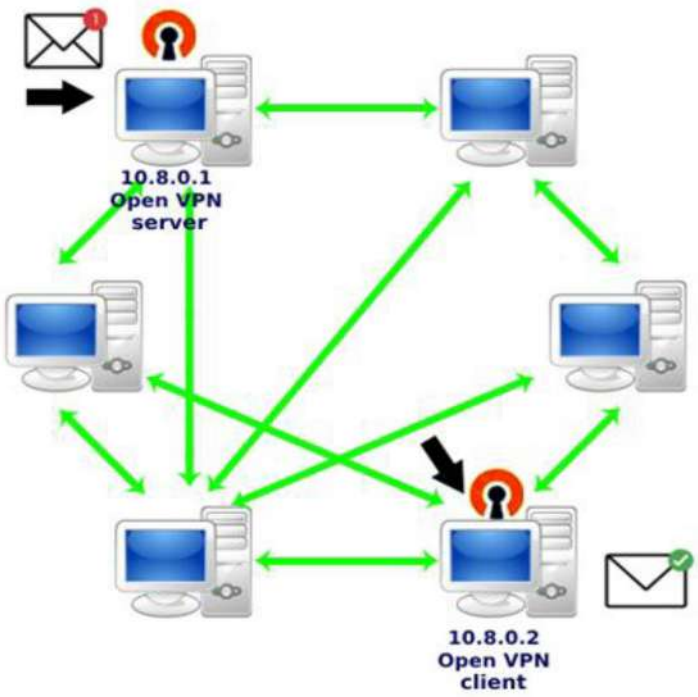


**Рис. 2. Схема сегменту мережі з VPN-доступом та передачею даних через протокол BitTorrent**

Ключовими перевагами такого підходу є зниження навантаження на центральний VPN-сервер та підвищення відмовостійкості системи завдяки використанню розподіленої архітектури, що дозволяє зберігати працездатність мережі в разі виходу з ладу окремих вузлів. Однак ця модель має ризики витоку метаданих та потенційного несанкціонованого доступу до окремих ресурсів.

Модель ізольованого сегмента приватної SDN-мережі на основі комбінації OpenVPN, BitTorrent та централізованого управління через SDN-контролер представляє кінцеву стадію розвитку попередніх моделей, інтегруючи їх переваги та мінімізуючи ключові обмеження. В порівнянні з класичними централізованими VPN-мережами ця архітектура дозволяє знизити навантаження на центральний вузол та забезпечити масштабований внутрішній обмін даними завдяки застосуванню протоколів пірингових мереж. На відміну від моделі, де BitTorrent функціонує всередині єдиного VPN-сегмента без чіткої сегментації, запропонований метод забезпечує повну логічну ізоляцію сегментів завдяки використанню SDN, що унеможливлює несанкціонований витік даних між ними. SDN-контролер виконує роль центрального вузла сегмента, формуючи маршрути, застосовуючи політики безпеки та контролюючи доступ в режимі реального часу. В корпоративній мережі реалізується ієрархічна структура контролерів, де один з них забезпечує централізоване управління в межах ізольованого сегмента, тоді як інші забезпечують маршрутизацію суміжних сегментів мережі, що дозволяє гнучко балансувати навантаження та швидко адаптуватися до змін мережної топології. Інтеграція BitTorrent в межах ізольованого SDN-сегмента забезпечує стійкість до відмов окремих вузлів, підвищуючи загальну резильєнтність системи (рис. 3).

Реалізація такої архітектури можлива на основі технологій віртуалізації, зокрема за допомогою віртуальних машини або контейнерів на платформах Proxmox та Docker. Це забезпечує спрощене масштабування, оптимізацію витрат на інфраструктуру, а також можливість інтеграції з фізичним обладнанням та хмарними середовищами для підвищення рівня безпеки, гнучкості та відмовостійкості.

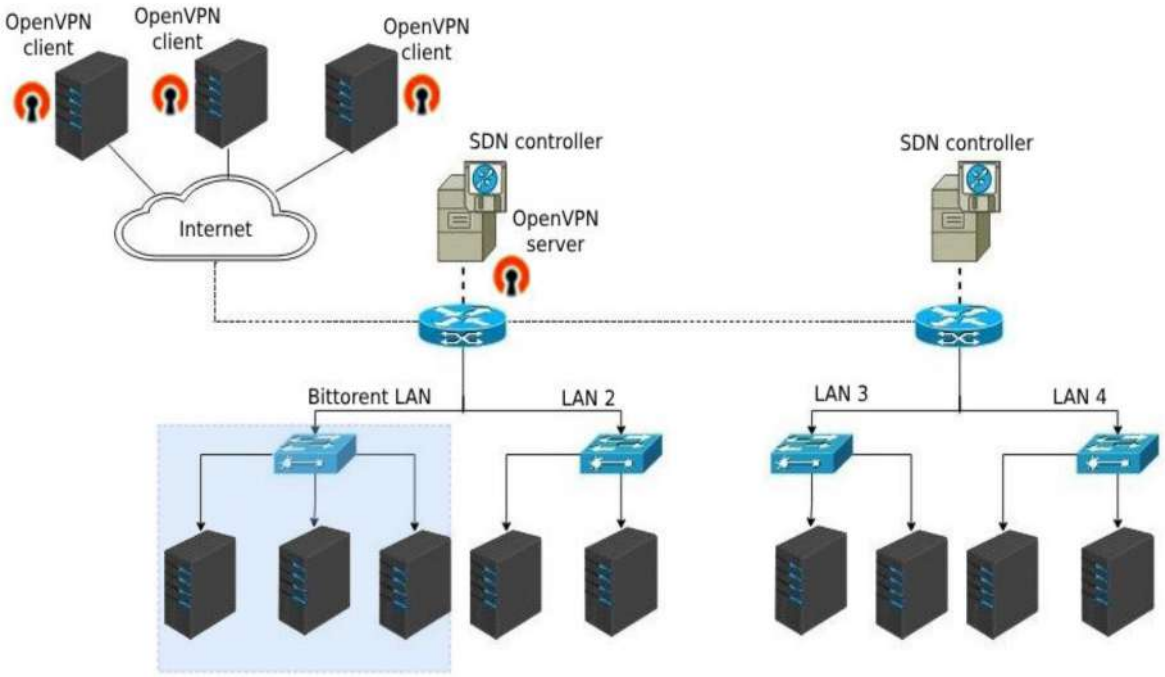


**Рис. 3. Схема ізольованого сегменту приватної корпоративної SDN-мережі**

**Алгоритм розгортання ізольованого сегмента приватної SDN-мережі**

Розгортання ізольованого сегмента приватної SDN-мережі передбачає виконання наступних етапів:

Побудова локальної SDN-мережі.

На цьому етапі формується мережна структура з логічним розділенням площин управління та передачі даних. Для цього використовуються комутатори, сумісні з протоколом OpenFlow, які забезпечують маршрутизацію трафіку відповідно до політик доступу, налаштованих на ієрархічній структурі SDN-контролерів приватної корпоративної мережі. Один з таких контролерів забезпечує централізоване управління ізольованим сегментом, тоді як інші забезпечують маршрутизацію суміжних сегментів приватної SDN-мережі. Також налаштовуються базові правила маршрутизації та моніторинг трафіку між ізольованим сегментом і зовнішніми ресурсами мережі.

Впровадження VPN-доступу через OpenVPN.

На другому етапі на SDN-контролері, який виконує роль шлюзового вузла між зовнішніми користувачами та внутрішньою мережею ізольованого сегмента, розгортається OpenVPN-сервер, що забезпечує надійне шифрування трафіку та автентифікацію клієнтів, а також виконується налаштування його параметрів відповідно до корпоративних політик безпеки. Це включає механізми контролю доступу, що визначають права користувачів та систем, а також моніторингу та логування VPN-сесій. Інтеграція VPN-сервера з SDN-контролером на одному пристрої спрощує управління ізольованим сегментом та забезпечує гнучке розмежування прав доступу на основі ролей, атрибутів користувачів і поточного стану мережі. Реалізація цього етапу гарантує доступ до сегмента лише авторизованим користувачам, захищаючи його від несанкціонованих підключень.

Налаштування обміну даними через BitTorrent.

На цьому етапі організовується обмін даними всередині ізольованого сегмента за допомогою протоколу BitTorrent. Ключовою особливістю є статичне призначення IP-адрес вузлам ізольованого сегменту, що усуває необхідність централізованих трекерів та дозволяє кожному піру бути ідентифікованим і доступним. BitTorrent-клієнти вузлів ізольованого сегмента налаштовуються на приватний режим роботи, що запобігає несанкціонованому витоку конфіденційної інформації поза межами сегмента. На SDN-контролері встановлюються правила фільтрації та сегментації трафіку, суворо регламентуючи канали обміну та забезпечуючи ізоляцію сегмента.

Реалізація політик маршрутизації SDN-контролером.

Фінальний етап цього алгоритму забезпечує реалізацію динамічного управління маршрутами, балансування навантаження та застосування політик якості обслуговування QoS. На SDN-контролер додаються правила застосування політик QoS, які виконуються автоматично з урахуванням поточного стану мережі. Використання QoS дозволяє пріоритезувати критично важливий трафік, зокрема транзакційні дані або керуючі повідомлення, та забезпечити гнучке реагування на зміни мережної топології і навантаження. Політики контролю доступу запобігають несанкціонованому перенаправленню трафіку та витоку даних між сегментами, підвищуючи рівень безпеки та надійності мережі.

**Оцінка ефективності розробленого методу**

На основі запропонованого алгоритму побудови ізольованого сегменту приватної SDN-мережі було сформульовано багатокритеріальну оптимізаційну задачу. Її основною метою є комплексне підвищення ефективності функціонування сегмента шляхом мінімізації ключових критеріїв, зокрема затримки при передачі даних захищеним каналом, використання ресурсів для забезпечення відмовостійкості роботи SDN-контролера та ймовірності отримання не цілісного обсягу даних.

Загальна ефективність ізольованого сегменту визначається величиною, оберненої зваженій суми цих критеріїв, що забезпечує комплексну оцінку продуктивності системи. При цьому враховується, що пропускна здатність в межах ізольованого сегмента повинна бути не меншої пропускної здатності захищеного каналу, а кількість одночасних з'єднань не повинна перевищувати максимальну кількість з'єднань, обмежених конфігурацією VPN-сервера. Водночас використання ресурсів SDN-контролера не перевищує його конфігураційної ємності, а в межах сегмента повинен бути щонайменше один активний вузол для забезпечення надійного обміну даними. Такий підхід забезпечує комплексну оцінку продуктивності системи. Загальна цільова функція ефективності функціонування ізольованого сегменту формулюється у вигляді наступної багатокритеріальної оптимізаційної задачі:

$$\min F = w_1 \cdot F_L + w_2 \cdot F_R + w_3 \cdot F_P, \ при \begin{cases} B \geq B_{VPN}, \\ R < R_{\max}, \\ N \geq N_{\min}, \\ m < m_{\max}, \end{cases} \tag{1}$$

де $w_i$ – вагові коефіцієнти, які визначають пріоритети компонентів оптимізаційної задачі та задовольняють вимогам $w_i \geq 0, \ \sum_{i=1}^{3} w_i = 1;$ $F_L$ – функція затримки передачі даних; $F_R$ – функція використання ресурсів SDN-контролера; $F_P$ – функція ймовірності отримання не цілісного обсягу даних; $B$, $B_{VPN}$ – пропускна здатність ізольованого сегменту та захищеного VPN-каналу відповідно, біт/с; $R$, $R_{\max}$ – використані (CPU, RAM, I/O тощо) та доступні ресурси SDN-контролера відповідно; $N$, – загальна кількість вузлів – пірів в ізольованому сегменті, од.; $N_{\min}$ – кількість активних вузлів – пірів в межах сегмента, од.; $m_{\max}$ – максимальна кількість одночасних з'єднань, обмежених конфігурацією VPN-сервера, од.; $m$ – кількість одночасних з'єднань під час роботи ізольованого сегменту, од.

Загальна ефективність функціонування ізольованого сегмента розраховується як:

$$E = \frac{1}{F} = w_1 \cdot F_L + w_2 \cdot F_R + w_3 \cdot F_P. \tag{2}$$

Компоненти оптимізаційної задачі (2) представлені нижче:

1. Мінімізація функції затримки передачі даних забезпечується зниженням часу процесів шифрування та дешифрування при передачі даних через захищений канал та зниженням часу пошуку пірів в межах ізольованого сегмента. Складність криптографічних алгоритмів збільшує час шифрування/дешифрування, а час пошуку активних пірів для завантаження цілісного обсягу даних може збільшувати затримку передачі даних в разі непрацездатності піру з необхідним фрагментом даних, що спричиняє додатковий час для пошуку дубльованого фрагменту на активних пірах. Функція затримки передачі даних формулюється як:

$$F_L = f(L_t, V, N_{\min}, m), \ при \begin{cases} B \leq B_{SDN}, \\ V \leq V_{\max}, \\ N \geq N_{\min}, \\ m < m_{\max}, \end{cases} \tag{3}$$

де $L_t$ – загальна затримка передачі даних, с; $V$ – швидкість пошуку пірів в межах ізольованого сегменту, од./с;

Загальна затримка передачі даних в межах ізольованого сегмента залежить від пропускної здатності VPN-каналу, кількості одночасних з'єднань та швидкості пошуку пірів. Загальна затримка передачі даних розраховується як:

$$L_t = \alpha_1 \cdot m \cdot L_{VPN} + \alpha_2 \cdot L_{P2P}, \tag{4}$$

де $\alpha_1$, $\alpha_2$ – вагові коефіцієнти, що визначають пріоритети компонентів оцінки та задовольняють вимогам $\alpha_1 \geq 0$, $\alpha_2 \geq 0$, $\alpha_1 + \alpha_2 = 1$; $L_{VPN}$ – затримка передачі даних, що виникає в захищеному каналі, с; $L_{P2P}$ – затримка передачі даних, що виникає через пошук активних пірів, с.

Затримка передачі даних в захищеному каналі залежить від пропускної здатності каналу та часу шифрування/дешифрування даних в залежності від обраного криптографічного алгоритму та розраховується як:

$$L_{VPN} = \frac{m \cdot D}{B_{VPN}} = t_{tr} + t_{enc} + t_{dec},\ при\ B_{VPN} \le B_{SDN}, \tag{5}$$

де $D$ – обсяг даних, переданих через VPN-канал за визначений проміжок часу $t$, біт; $B_{VPN}$ – пропускна здатність VPN-каналу з шифруванням та дешифруванням даних, біт/с; $B_{SDN}$ – пропускна здатність VPN-каналу без шифрування, який визначено для обслуговування ізольованого сегменту на SDN-контролері, біт/с; $t_{tr}$ – час передачі даних через VPN-канал без шифрування, с; $t_{enc}$ – час шифрування даних на VPN- каналі, с; $t_{dec}$ – час дешифрування даних наVPN- каналі, с.

Швидкість пошуку активних пірів залежить від кількості пірів у сегменті та продуктивності SDN-контролера, зокрема кількості операцій I/O, та розраховується як:

$$V = \frac{Z_{SDN}}{t}, \tag{6}$$

де $Z_{SDN}$ – кількість операцій, необхідних для перевірки активності одного піру; $t$ – час виконання цих операцій, с.

Відповідно, затримка, яка виникає через пошук активних пірів, розраховується як:

$$L_{P2P} = \frac{Z_{SDN} \cdot N_{\min}}{V}, \tag{7}$$

де $Z_{SDN}$ – кількість операцій, необхідних для перевірки активності одного піра, од.;

2. Мінімізація функції використання ресурсів SDN-контролера забезпечується використанням доступних ресурсів, зокрема пам'яттю, кількістю процесорів та додатковими операціями для забезпечення управління трафіком та надійної роботи реалізованого на SDN-контролері VPN-сервера. Функція використання ресурсів SDN-контролера формулюється як:

$$F_R(R, R_{e/d}, R_q, m) = \beta_1 \cdot R + \beta_2 \cdot m \cdot R_{e/d} + \beta_3 \cdot R_q, \quad при (R + R_{e/d} + R_q) \le R_{\max}, \quad m < m_{\max}, \tag{8}$$

де $\beta_1$, $\beta_2$ – вагові коефіцієнти які визначають пріоритети компонентів оцінки та задовольняють вимогам $\beta_1 \ge 0$, $\beta_2 \ge 0$, $\beta_1 + \beta_2 = 1$; $R_{e/d}$ – використані ресурси (CPU, RAM, I/O тощо) контролера на процеси шифрування/дешифрування під час передачі даних захищеним VPN-каналом; $R_q$ – використані ресурси (CPU, RAM, I/O тощо) для управління трафіком;

3. Функція ймовірності отримання не цілісного обсягу даних зменшується зі зростанням кількості пірів у сегменті, але може зростати через велику кількість одночасних з'єднань під час роботи ізольованого сегмента. Функція ймовірності отримання не цілісного обсягу даних формулюється як:

$$F_P = \gamma_1 \cdot \frac{1}{N_{\min}} + \gamma_2 \cdot \frac{m}{N},\ при\ N \ge N_{\min}, m < m_{\max}, \tag{9}$$

де $\gamma_1$, $\gamma_2$ – вагові коефіцієнти які визначають пріоритети компонентів оцінки та задовольняють вимогам $\gamma_1 \ge 0$, $\gamma_2 \ge 0$, $\gamma_1 + \gamma_2 = 1$.

Запропонований підхід дозволяє комплексно оцінити ефективність роботи ізольованого сегмента приватної SDN-мережі, враховуючи ключові параметри його функціонування. Це дозволяє кількісно оцінити вплив пропускної здатності, затримки передачі даних, складності криптографічних алгоритмів, ресурсоємності контролера та відмовостійкості на загальну продуктивність сегмента.

**Постановка експерименту**

Постановка експерименту була виконана на базі лабораторії обчислювальних систем і мережних технологій кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки. Для кожної з трьох моделей розгорнуто відповідну конфігурацію програмного забезпечення та визначено параметри тестування.

1. Модель з VPN-доступом.

VPN-сервер OpenVPN розгорнуто на віртуальній машині (ВМ) з операційною системою Ubuntu 20.04. ВМ оснащено чотириядерним процесором з тактовою частотою 3,0 ГГц та 4 ГБ оперативної пам'яті. Пропускна здатність мережного інтерфейсу становить до 100 Мбіт/с, що дозволяє обслуговувати до 100 одночасних клієнтських підключень відповідно до конфігурації VPN-сервера без значного зниження продуктивності. Також конфігурація VPN-сервера передбачає використання алгоритму симетричного шифрування AES-256 в поєднанні з протоколом захищеного обміну ключами TLS 1.3, автентифікація користувачів реалізується на основі цифрових сертифікатів. У брандмауері відкрито порти 943/TCP для адміністративного вебінтерфейсу OpenVPN GUI та 1194/TCP для VPN-з'єднань. Для підвищення рівня захисту сервера також налаштовано перенаправлення трафіку на інші порти.

Процедура підключення користувача передбачає встановлення клієнтського програмного забезпечення OpenVPN Client, імпорт конфігураційного файлу та відповідного сертифіката автентифікації. Адміністратор

мережі за допомогою вебінтерфейсу здійснює створення користувацьких облікових записів, призначення параметрів доступу та контроль за активними сесіями.

2. Модель з VPN-доступом та передачею даних через BitTorrent.

VPN-сервер було розгорнуто на віртуальній машині з ОС Ubuntu 20.04, оснащеній чотириядерним процесором. Обсяг оперативної пам'яті збільшено до 20 ГБ для зберігання тимчасових файлів та логів роботи BitTorrent-клієнтів. Пропускна здатність мережного інтерфейсу становить до 100 Мбіт/с. Для коректного функціонування протоколу були відкрито порти 6346/TCP/UDP та 6886/TCP/UDP, що забезпечують роботу клієнтів Gnutella та BitTorrent відповідно. Передача даних у мережі здійснювалася через налаштований VPN-сервер, який надавав клієнтам сертифікати створення захищеного каналу. Обмін даними організовувався через оверлейну мережу Gnutella, для взаємодії клієнтів в межах мережі було застосовано програмне забезпечення FrostWire, що підтримує передачу даних протоколами Gnutella та BitTorrent.

3. Модель з SDN-контролером, VPN-доступом та ізольованим сегментом з передачею через BitTorrent.

Запропонований метод було реалізовано моделюванням ізольованого сегмента приватної корпоративної мережі на основі SDN-контролера Ryu з реалізацією VPN-доступу на основі OpenVPN та внутрішньою передачею даних через протокол BitTorrent. Розгортання SDN-контролера та VPN-сервера здійснювалося на одній віртуальній машині з операційною системою Ubuntu 20.04, обладнаній центральним процесором з чотирма обчислювальними ядрами та тактовою частотою 3,0 ГГц. Обсяг оперативної пам'яті було збільшено до 20 ГБ, що забезпечило стабільну роботу обох сервісів без зниження продуктивності.

Шифрування даних реалізовано виключно на рівні VPN-сервера із застосуванням алгоритму AES-256 в поєднанні з протоколом TLS 1.3 та клієнтською аутентифікацією за допомогою цифрових сертифікатів. Передача внутрішнього трафіку в межах ізольованого сегмента здійснюється без додаткового шифрування, що знижує затримки та підвищує ефективну пропускну здатність системи.

На рівні SDN-контролера було реалізовано політики доступу до ізольованого сегмента, зокрема перенаправлення трафіку та відкриття порту 5555/TCP для VPN-каналу, через який здійснюється єдиний доступ до ізольованого SDN-сегмента. В межах ізольованого сегменту додатково здійснюється відкриття порту 6886/TCP для обміну даними через протокол BitTorrent, що гарантує контрольований обмін даними та підвищує безпеку внутрішнього трафіку. Передача даних за протоколом BitTorrent реалізована через TCP, тоді як UDP використовується переважно для службових операцій, зокрема пошуку активних вузлів у сегменті, що забезпечує контрольовану взаємодію між пірами. В межах ізольованого сегмента всім вузлам призначаються статичні IP-адреси, що спрощує процедуру виявлення пірів і скорочує затримки під час підключення нових вузлів.

Для оцінки безпеки передачі даних за межі ізольованого SDN-сегмента проведено аналіз трафіку за допомогою Wireshark. Моніторинг зосереджувався на потоці даних, що проходять через VPN-тунель, який забезпечує захищене з'єднання між ізольованим сегментом та SDN-контролером. Після фільтрації пакетів, що передавалися виключно через VPN-тунель, підтверджено, що їх вміст зашифрований (рис. 4). Передача даних відбувається всередині ізольованого сегменту за допомогою протоколу BitTorrent, тоді як вихід за його межі відбувається через захищене VPN-з'єднання, контрольоване SDN-контролером. Це забезпечує додатковий рівень безпеки та управління трафіком.

Запропонований метод забезпечує оптимізовану передачу даних в ізольованому сегменті приватної SDN-мережі, зберігаючи при цьому переваги децентралізованого поширення інформації та одночасно підвищуючи рівень безпеки, запобігаючи несанкціонованому доступу та витоку даних.

На графіку (рис. 5) представлено середню затримку передачі TCP-пакетів, що виникає в досліджуваних моделях на основі експериментальних даних. Результати демонструють, що впровадження SDN-контролера з реалізованим на ньому VPN-сервером дозволяє зменшити затримку передачі даних порівняно з моделлю захищеної передачі через мережу BitTorrent, при цьому зберігаючи ключові переваги P2P-передачі даних, зокрема масштабованість та децентралізацію, в межах ізольованого сегменту.

Крім того підтверджено, що застосування P2P-технологій в приватних SDN-мережах у поєднанні з локалізацією трафіку в межах ізольованого сегмента дозволяє мінімізувати затримки та покращити продуктивність системи, забезпечуючи необхідний рівень безпеки передачі даних.

**Висновки**

В роботі вперше запропоновано метод організації ізольованого сегмента приватної SDN-мережі із захищеним доступом через VPN та вбудованою P2P-дистрибуцією на основі протоколу BitTorrent, який інтегрує централізоване керування політиками та маршрутизацією на рівні SDN-контролера з децентралізованим розподілом трафіку всередині сегмента, що дозволяє одночасно підвищити рівень захищеності та керованості, мінімізувати внутрішні затримки завдяки балансуванню навантаження між вузлами, забезпечити пріоритезацію сервісів та масштабованість архітектури для критично важливих корпоративних і приватних блокчейн-систем.

Аналіз ефективності запропонованого методу підтвердив, що використання ізольованих сегментів у SDN мережах дозволяє мінімізувати внутрішні затримки та підвищити контроль над маршрутизацією трафіку.

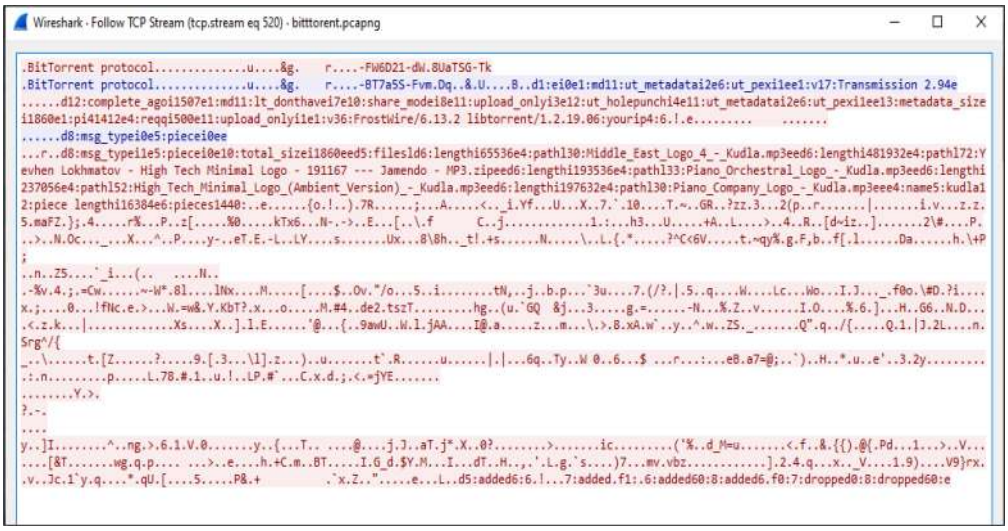


**Рис. 4. Візуалізація шифрованого потоку даних при передачі даних з використанням протоколу BitTorrent з ізольованого сегменту приватної SDN-мережі в Wireshark**

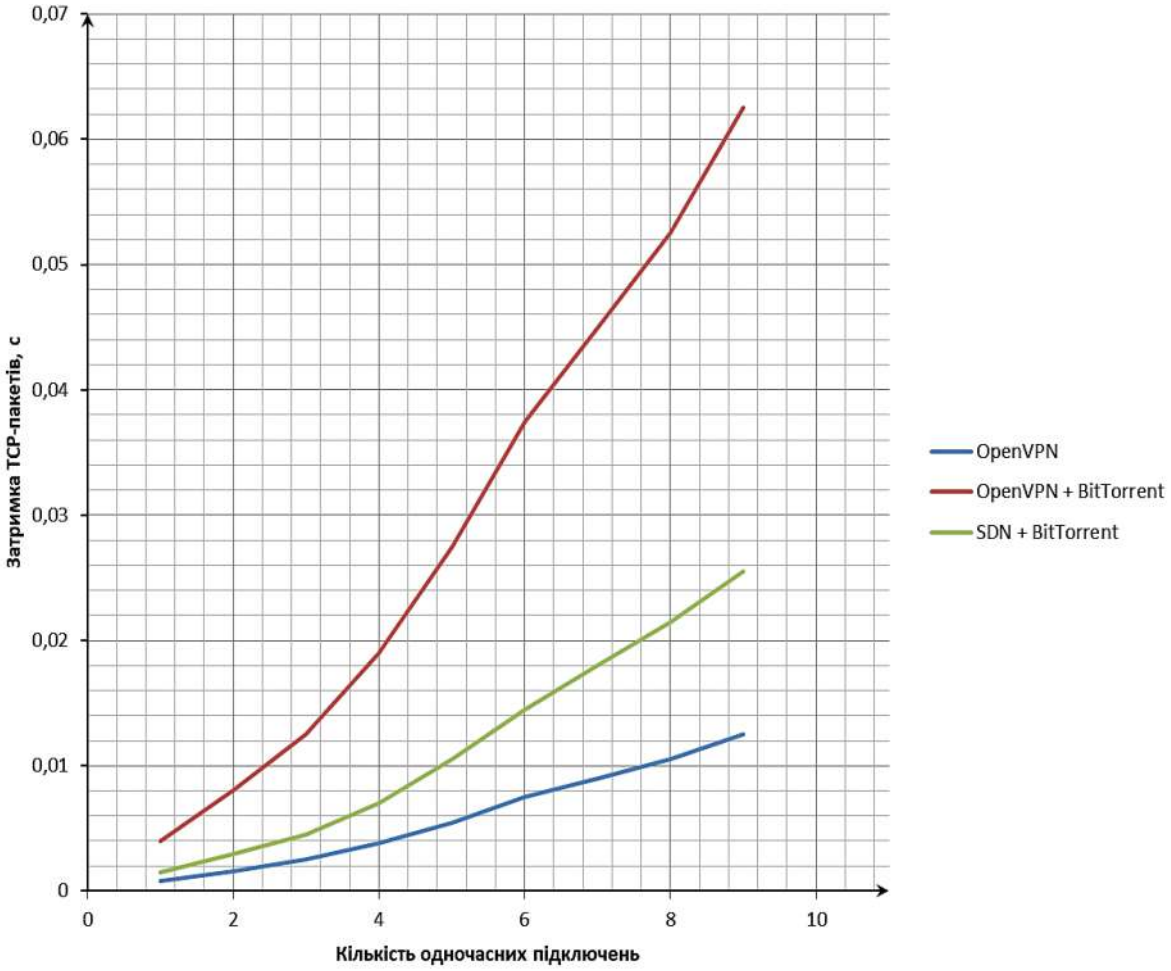


**Рис. 5. Діаграма середньої затримки TCP-пакетів в досліджуваних моделях**

При практичному застосуванні методу необхідно враховувати характер даних для передачі, вимоги до обчислювальних ресурсів SDN-контролера ізольованого сегмента, рівень захищеності та доступність ресурсів для реалізації сегмента. Отже, запропонований метод може бути корисним для малого та середнього бізнесу, який прагне створювати масштабовані та високопродуктивні корпоративні мережі, що відповідають сучасним вимогам до

мінімізації затримок, підвищення надійності та зниження внутрішнього навантаження, що є критичним для побудови складних інформаційних інфраструктур.

Крім того, така архітектура має значний потенціал для розгортання приватних блокчейн-мереж. Захищений доступ до вузлів блокчейна через VPN-тунель гарантує підключення лише авторизованих користувачів та систем. Водночас, SDN-контролер дозволяє управляти міжвузловими взаємодіями, налаштовувати пріоритети та обмеження для різних типів трафіку, зокрема транзакційних повідомлень або реплікації блоків.

Майбутні дослідження можуть бути спрямовані на оптимізацію цього методу в різних умовах та практичне застосування архітектури для побудови приватних блокчейн-мереж.

**Список використаної літератури**

1. Latif Z., Umer Q., Lee C., Sharif K, Li F., Biswas S. A Machine Learning-Based Anomaly Prediction Service for Software-Defined Networks. *Sensors*. 2022; vol. 22, No. 21. P. 8434.

2. Wadhwani P, Software Defined Networking Market – By Component (Solution [Physical Network Infrastructure, SDN Controller, SDN Application], Service [Professional, Managed]), By End Use (Enterprise, Cloud Service Provider, Telecom Service Provider) & Forecast, 2024–2032. URL https://www.gminsights.com/industry-analysis/software-defined-networking-sdn-market (дата звернення: 10.06. 2025).

3. Suliyanti W. N., Sari R. F. Blockchain-Based Double-Layer Byzantine Fault Tolerance for Scalability Enhancement for Building Information Modeling Information Exchange. *Big Data Cogn. Comput*. 2023. Vol. 7. P. 90.

4. Tanuja J., Goyal N., Ram M. An approach to analyze reliability indices in peer-to-peer communication systems. *Cybernetics and Systems*. 2022. Vol. 53. No. 8. P. 716–733.

5. Khalid M. I., Ehsan I., Al-Ani A., Iqbal J., Hussain S., Ullah S. S., Nayab A comprehensive survey on blockchain-based decentralized storage networks. *IEEE Access*. 2023.Vol. 11. P. 10995–11015.

6. М. Кренцін, Л. Куперштейн. Метод обміну ідентифікаційними даними між вузлами пірингової мережі на основі технології NFC. *Кібербезпека: освіта, наука, техніка*. 2024. вип. 1, № 25, С. 79–88.

7. Abdullahi Yari I, Dehling T, Kluge F, Geck J, Sunyaev A, Eskofier B. Security Engineering of Patient-Centered Health Care Information Systems in Peer-to-Peer Environments: Systematic Review. *J Med Internet Res*. 2021. Vol. 23. No. 11. P. e24460.

8. BitTorrent : The World's Most Popular Torrent Client. URL:https://www.bittorrent.com/btt/btt-docs/BitTorrent_(BTT)_White_Paper_v0.8.7_Feb_2019.pdf (дата звернення: 21.07.2025).

9. Куперштейн Л. М. Аналіз тенденцій розвитку пірингових мереж. *Вісник Хмельницького національного університету. Технічні науки*. 2021. № 4. С. 25–29.

10. Aldabbas H. Efficient bandwidth allocation in SDN-based peer-to-peer data streaming using machine learning algorithm. *The Journal of Supercomputing*. 2023. Vol. 79. No. 6. P. 6802–6824.

11. Hill W., Acquaah Y. T., Mason, J., Limbrick D., Teixeira-Poit S., Coates C., Roy K. DDoS in SDN: A review of open datasets, attack vectors and mitigation strategies. *Discover Applied Sciences*. 2024. Vol. 6. No. 9. P. 472.

12. Pang S., Zeng D., Chen X. Research on SDN-based data center network traffic management and optimization. *2022 IEEE 2nd International Conference on Power, Electronics and Computer Applications (ICPECA)*, Shenyang, China, 21–23 January 2022. 2022. URL: https://doi.org/10.1109/icpeca53709.2022.9718973 (date of access: 15.08.2025).

13. Suhail A., Mir Ajaz H. Scalability, consistency, reliability and security in SDN controllers: a survey of diverse SDN controllers. *Journal of Network and Systems Management*. 2021. Vol. 29. No 1. P. 9.

14. Hwang I.-S., Rianto A., Kharga R., Ab-Rahman M. S. Global P2P BitTorrent Real-Time Traffic Over SDN-Based Local-Aware NG-PON2. *IEEE Access*. 2022. Vol. 10, P. 76884–76894.

15. Vemasani P., Modi S. Building Resilient Distributed Systems: Fault-Tolerant Design Patterns for Stateful Workflows. *International Journal of Computer Engineering and TechNology*. 2024. Vol. 15. P. 169–181.

16. Ткачов В. М., Чепурна І. С., Фесенко Т. Г. Метод мультирівневого VPN-тунелювання для забезпечення віддаленого доступу до вузлів екстранет-мережі. *Вісник Херсонського національного технічного університету*. 2024. № 3(90). С. 299–308.

**References**

1. Latif, Z., Umer, Q., Lee, C., Sharif, K., Li, F., & Biswas, S. (2022). A Machine Learning-Based Anomaly Prediction Service for Software-Defined Networks. Sensors, 22(21), 8434. https://doi.org/10.3390/s22218434

2. Preeti Wadhwani. 2024, February. Software Defined Networking Market – By Component (Solution [Physical Network Infrastructure, SDN Controller, SDN Application], Service [Professional, Managed]), By End Use (Enterprise, Cloud Service Provider, Telecom Service Provider) & Forecast, 2024 – 2032 (Report ID: GMI2395). Global Market Insights Inc. Retrieved June 10, 2025, from https://www.gminsights.com/industry-analysis/software-defined-networking-sdn-market

3. Suliyanti, W. N., & Sari, R. F. (2023). Blockchain-Based Double-Layer Byzantine Fault Tolerance for Scalability Enhancement for Building Information Modeling Information Exchange. Big Data and Cognitive Computing, 7(2), 90. https://doi.org/10.3390/bdcc7020090

4. Joshi, T., Goyal, N., & Ram, M. (2022). An approach to analyze reliability indices in peer-to-peer communication systems. *Cybernetics and Systems*, *53*(8), 716–733.

5. Khalid, M.I., Ehsan, I., Al-Ani, A.K., Iqbal, J., Hussain, S., Ullah, S.S., & Nayab. (2023). A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks. IEEE Access, 11, 10995–11015.

6. Krentsin, Mykhailo & Kupershtein, Leonid. (2024). NFC technology as a means of protected exchange of identification data between peer-to-peer network nodes Cybersecurity Education Science Technique. 1. 79–88. 10.28925/2663-4023.2024.25.7988. (in Ukrainian)

7. Abdullahi Yari, I., Dehling, T., Kluge, F., Geck, J., Sunyaev, A., & Eskofier, B. (2021). Security Engineering of Patient-Centered Health Care Information Systems in Peer-to-Peer Environments: Systematic Review. Journal of medical Internet research, 23(11), e24460. https://doi.org/10.2196/24460

8. BitTorrent. (2019, February). *BitTorrent (BTT) white paper v0.8.7*. Retrieved from https://www.bittorrent.com/btt/btt-docs/BitTorrent_(BTT)_White_Paper_v0.8.7_Feb_2019.pdf

9. Krentsin, Mykhailo & Kupershtein, Leonid. (2022). Analysis of peer-to-peer network protocols (in Ukrainian).

10. Aldabbas, H. (2023). Efficient bandwidth allocation in SDN-based peer-to-peer data streaming using machine learning algorithm. *The Journal of Supercomputing*, *79*(6), 6802–6824.

11. Hill, W., Acquaah, Y. T., Mason, J., Limbrick, D., Teixeira-Poit, S., Coates, C., & Roy, K. (2024). DDoS in SDN: a review of open datasets, attack vectors and mitigation strategies. *Discover Applied Sciences*, *6*(9), 472.

12. Pang, S., Zeng, D., & Chen, X. (2022, January). Research on SDN-based data center network traffic management and optimization. In *2022 IEEE 2nd International Conference on Power, Electronics and Computer Applications (ICPECA)* (pp. 600-604). IEEE.

13. Ahmad, Suhail & Mir, Ajaz. (2021). Scalability, Consistency, Reliability and Security in SDN Controllers: A Survey of Diverse SDN Controllers. Journal of Network and Systems Management. 29. 10.1007/s10922-020-09575-4.

14. Hwang, I. S., Rianto, A., Kharga, R., & Ab-Rahman, M. S. (2022). Global P2P BitTorrent real-time traffic over SDN-based local-aware NG-PON2. *IEEE Access*, *10*, 76884–76894.

15. Vemasani, P., & Modi, S. (2024). Building Resilient Distributed Systems: Fault-Tolerant Design Patterns for Stateful Workflows. *International Journal of Computer Engineering and Technology*, *15*, 169–181.

16. Tkachov V. M., Chepurna I. S., Fesenko T. H (2024). Metod mul'tyrivnevoho VPN-tunelyuvannya dlya zabezpechennya viddalenoho dostupu do vuzliv ekstranet-merezhi. *Visnyk Khersons'koho natsional'noho tekhnichnoho universytetu (electronic journal)*. vol. 3(90), pp. 299–308. Retrieved from: https://doi.org/10.35546/kntu2078-4481.2024.3.37 (accessed 10 August 2025).

*Дата першого надходження рукопису до видання: 24.09.2025*
*Дата прийнятого до друку рукопису після рецензування: 21.10.2025*
*Дата публікації: 28.11.2025*