УДК 004.7:004.056

Пухта В.М.

Кирилащук Т. Г.

ІНТЕГРАЦІЯ КОНЦЕПЦІЙ ZERO TRUST ТА BLOCKCHAIN У ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ ДЛЯ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ

Вінницький національний технічний університет

Анотація

У роботі розглянуто проблему підвищення безпеки програмно-конфігурованих мереж (SDN) шляхом інтеграції концепцій Zero Trust та Blockchain. Проаналізовано основні загрози SDN-архітектурі, зокрема атаки на централізований контролер, DDoS-атаки, маніпуляції маршрутизацією, компрометацію API та інсайдерські загрози. Запропоновано модель інтеграції багаторівневої аутентифікації, мікросегментації та розподіленого журналювання транзакцій на основі Blockchain. Результати моделювання підтвердили зростання рівня протидії загрозам до 96–98 % при незначному збільшенні затримок обробки запитів. Отримані результати демонструють доцільність комплексного застосування Zero Trust та Blockchain для забезпечення стійкості SDN-мереж критичної інфраструктури.

Ключові слова: *SDN, Zero Trust, Blockchain, контроль доступу, мікросегментація, кібербезпека.*

Abstract

This paper addresses the problem of enhancing the security of Software-Defined Networks (SDN) through the integration of the Zero Trust and Blockchain concepts. The main threats to SDN architecture are analyzed, including attacks on the centralized controller, DDoS attacks, routing manipulation, API compromise, and insider threats. A model is proposed that integrates multi-level authentication, microsegmentation, and distributed transaction logging based on Blockchain technology. Simulation results confirmed an increase in threat resistance to 96–98% with only a slight increase in request processing delays. The obtained results demonstrate the feasibility and effectiveness of the combined application of Zero Trust and Blockchain to ensure the resilience of SDN networks for critical infrastructure.

Keywords: *SDN, Zero Trust, Blockchain, access control, microsegmentation, cybersecurity.*

Вступ

Стрімкий розвиток цифрових технологій, активне впровадження хмарних обчислень, IoT-платформ, 5G-мереж та сервісно-орієнтованих архітектур суттєво трансформують підходи до побудови телекомунікаційної інфраструктури. Програмно-конфігуровані мережі (SDN) забезпечують гнучке та централізоване управління мережевими ресурсами шляхом відокремлення площини керування від площини передавання даних, що дозволяє оперативно змінювати політики маршрутизації, оптимізувати трафік та автоматизувати адміністрування. Проте централізований характер SDN-контролера формує єдину точку відмови, що робить такі мережі вразливими до DDoS-атак, маніпуляцій маршрутами, атак на API та внутрішніх загроз[1]. Компрометація контролера може призвести до порушення цілісності всієї мережевої інфраструктури, неконтрольованого перенаправлення потоків даних та втрати доступності сервісів.

Додатковим фактором ризику є зростання кількості взаємодіючих компонентів у розподілених середовищах, що підвищує складність контролю довіри між елементами мережі. Традиційні периметрові моделі безпеки, які передбачають довіру до внутрішніх суб'єктів, виявляються недостатньо ефективними в умовах динамічних та гібридних мережевих середовищ. Дослідження у сфері блокчейн-орієнтованих механізмів захисту SDN підтверджують, що децентралізація управління, використання смарт-контрактів та незмінність журналів транзакцій дозволяють суттєво зменшити ризики компрометації контролера і підвищити прозорість мережевих операцій[2]. Блокчейн-технологія забезпечує криптографічно захищене зберігання політик доступу та змін конфігурації, що унеможливлює їх приховану модифікацію.

Результати дослідження

У межах дослідження проведено системний аналіз актуальних загроз SDN-мережам, зокрема атак на контролер, підміну правил маршрутизації, несанкціонований доступ через API, а також внутрішні загрози, пов'язані з компрометацією облікових записів. На основі отриманих результатів розроблено концептуальну модель нейтралізації цих загроз шляхом інтеграції Zero Trust і Blockchain[5].

Запропонована модель передбачає:

– постійну багатофакторну аутентифікацію користувачів і пристроїв із перевіркою контексту доступу;

– мікросегментацію мережі для ізоляції критичних ресурсів та обмеження горизонтального переміщення атак;

– децентралізоване зберігання журналів доступу й змін політик у Blockchain-реєстрі;

– застосування гібридного алгоритму консенсусу для зменшення навантаження на систему та скорочення затримок;

– використання смарт-контрактів для автоматизованого контролю відповідності дій встановленим політикам безпеки.

Застосування блокчейн-механізмів у SDN забезпечує незмінність політик маршрутизації, захист від їх підміни та підвищує прозорість управління трафіком[2][3]. Завдяки розподіленому зберіганню даних усі зміни конфігурації фіксуються у вигляді криптографічно підтверджених транзакцій, що унеможливлює їх несанкціоноване редагування. Інтеграція Zero Trust дозволяє впровадити динамічний контроль доступу, заснований на аналізі поведінкових характеристик і ризикових параметрів кожного запиту[4].

Моделювання трьох сценаріїв атак — соціальної інженерії, компрометації мережевих компонентів та комбінованих атак із використанням вразливостей протоколів — продемонструвало суттєве підвищення рівня захищеності мережі. У порівнянні з традиційною моделлю безпеки здатність протидії загрозам зросла з 40 % до 96–98 %, стабільність з'єднання під час атак перевищила 92 %, а прозорість доступу досягла 100 % завдяки використанню розподіленого реєстру[5]. Середня затримка обробки запитів зросла лише на 5–10 мс, що є прийнятним компромісом з огляду на значне підвищення рівня безпеки та стійкості системи.

Отримані результати свідчать, що інтегрована модель не лише підвищує рівень захисту, а й забезпечує більш структурований аудит подій та покращує керованість політик доступу в умовах високого навантаження.

Висновки

Інтеграція концепцій Zero Trust і Blockchain у програмно-конфігурованих мережах забезпечує істотне підвищення рівня кібербезпеки за рахунок постійної верифікації доступу, децентралізації управління та незмінності журналів транзакцій. Запропонований підхід дозволяє мінімізувати ризики компрометації SDN-контролера, підвищити стійкість до DDoS-атак і внутрішніх загроз, забезпечити прозорий аудит змін конфігурації та контроль цілісності політик маршрутизації.

Комплексне поєднання Zero Trust і Blockchain створює багаторівневу систему захисту, здатну ефективно протидіяти сучасним кіберзагрозам у критичних та корпоративних мережах. Подальші дослідження доцільно спрямувати на оптимізацію алгоритмів консенсусу, зменшення ресурсомісткості блокчейн-рішень та впровадження інтелектуальних механізмів автоматизованого управління доступом із використанням методів машинного навчання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Guo, X., Wang, C., Cao, L., Jiang, Y., & Yan, Y. (2022). A novel security mechanism for software defined network based on blockchain. Computer Science and Information Systems, 19(2), 523-545. https://doi.org/10.2298/CSIS210222001G.
2. Li, W., Meng, W., Liu, Z., & Au, M.-H. (2020). Towards blockchain-based software-defined networking: Security challenges and solutions. IEICE Transactions on Information and Systems, E103.D(2), 196-203. https://doi.org/10.1145/3569966.3570015
3. Das, D., Banerjee, S., Dasgupta, K., Chatterjee, P., Ghosh, U., & Biswas, U. (2023). Blockchain enabled SDN framework for security management in 5G applications. In *ICDCN 23: Proceedings of the 24th International Conference on Distributed Computing and Networking* (pp. 414–419). doi: 10.1145/3571306.3571445.
4. Yan, X., & Wang, H. (2020). Survey on zero-trust network security. In *Artificial Intelligence and Security* (pp. 50–60). Springer. doi: 10.1007/978-981-15-8083-3_5.
5. Pidpalyi, O., & Romanov, O. (2025). Integration of Zero Trust and Blockchain in SDN networks: An overview of threats and methods of their elimination. *Information Technologies and Computer Engineering*, 22(1), 55–68. doi: 10.63341/vitce/1.2025.55.

Пухта Владислав Максимович – студент групи 2КІТС-24б, Вінницький національний технічний університет, м. Вінниця, vlad.puhta@gmail.com

Науковий керівник: Тетяна Генадіївна Кирилащук – асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: kgt0998@gmail.com.

Pukhta Vladyslav Maksymovych – student of group 2KITS-24b, Vinnytsia National Technical University, Vinnytsia, vlad.puhta@gmail.com

Supervisor: Tatiana G. Kyrylashchuk – Assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com.