

## **ЗАХИСТ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ BLOCKCHAIN**

**Підпалій О.І.**

*Навчально-науковий інститут телекомунікаційних систем*

*КПІ ім. Ігоря Сікорського, Україна*

*Email: sashapispalyi@gmail.com*

### **SECURING SOFTWARE-CONFIGURABLE NETWORKS WITH BLOCKCHAIN TECHNOLOGY**

The study analyzes the integration of Software-Defined Networking (SDN) and Blockchain to improve network security. It has been established that the combination of SDN and Blockchain provides decentralized management, cryptographic protection, and immutability of network transactions. The key security mechanisms are identified: policy automation through smart contracts, decentralized event log management, and dynamic access control. The architectural solutions are effective for IoT, telecommunications and corporate networks. The scientific novelty is the substantiation of the concept of integrating SDN and Blockchain, which is superior to traditional approaches to cybersecurity.

Дослідження аналізує інтеграцію Software-Defined Networking (SDN) та Blockchain для підвищення мережевої безпеки. Встановлено, що поєднання SDN і Blockchain забезпечує децентралізацію управління, криптографічний захист та незмінність мережевих транзакцій. Визначено ключові механізми безпеки: автоматизація політик через смарт-контракти, децентралізоване управління журналами подій та динамічний контроль доступу. Архітектурні рішення ефективні для IoT, телекомунікаційних та корпоративних мереж. Наукова новизна – обґрунтування концепції інтеграції SDN і Blockchain, що перевершує традиційні підходи до кіберзахисту.

Сучасний розвиток інформаційно-комунікаційних технологій характеризується безперервним ускладненням мережевих архітектур та механізмів забезпечення кібербезпеки. Фундаментальні трансформації в галузі мережевих технологій, зокрема впровадження Software-Defined Networking (SDN) та блокчейн-технологій, зумовлені критичною необхідністю вирішення системних проблем інформаційної безпеки в умовах постійно еволюціонуючих кіберзагроз [1,2,3].

Дослідження інтеграції Software-Defined Networking (SDN) та блокчейн-технологій проводилося комплексно з використанням широкого спектру інформаційних джерел та методологічних підходів. Основним напрямком дослідження є безпека мережі [4,5,6].

Аналіз безпекових викликів SDN-архітектури виявляє три критичні вектори потенційних атак:

- уразливість контролера,
- DDoS-атаки на площину керування
- Атаки на площину даних

Дана робота розглядається на основі таких елементів мережі: користувачі, SDN комутатори, Контролер SDN, блокчейн додаток

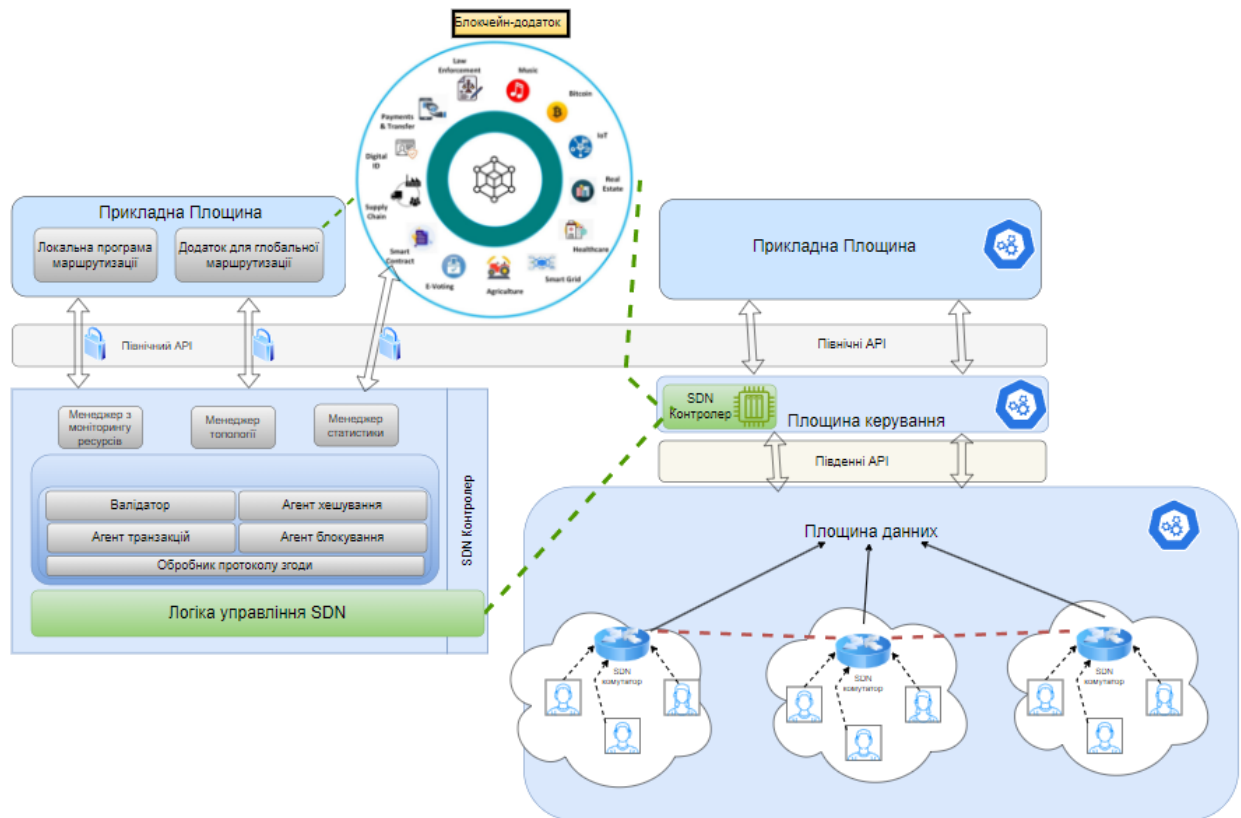


Рис.1. Схематична модель мережі з інтеграцією Blockchain у SDN.

У рамках дослідження було проведено тестування кількох типів атак, щоб оцінити ефективність Blockchain технологій у програмно-конфігурованих мережах (SDN) [7,8].

Результати тестування показали, що інтеграція Blockchain технології значно підвищила рівень безпеки програмно-конфігурованих мереж.

Таблиця 1. Результати тестування інтеграції Zero Trust і Blockchain

| Тип атаки                  | Вплив до впровадження               | Вплив після впровадження           | Заблоковано атак (%) | Час відповіді контролера (мс) |
|----------------------------|-------------------------------------|------------------------------------|----------------------|-------------------------------|
| DDoS-атаки                 | Повна втрата доступності контролера | Стабільна робота мережі            | 95%                  | 10                            |
| Атаки на площину керування | Зміна правил маршрутизації          | Неможливість зміни маршрутизації   | 98%                  | 12                            |
| Атаки на площину даних     | Перехоплення трафіку                | Автентифікація та шифрування даних | 97%                  | 8                             |

Під час тестування використовувалися такі основні метрики:

### 1. Час відповіді контролера ( $T_{resp}$ )

Визначався як середній час (у мілісекундах) між надсиланням запиту від мережевого пристрою та отриманням відповіді від SDN-контролера:

$$T_{resp} = \frac{\sum T_i}{N} \quad (1)$$

де:  $T_i$  – час відповіді для  $i$ -го запиту;  $N$  – загальна кількість запитів.

## 2. Кількість успішно заблокованих атак ( $P_{block}$ )

Оцінювалася як відсоток атак, які були виявлені та заблоковані системою безпеки, від загальної кількості атак:

$$P_{block} = \left( \frac{A_{blocked}}{A_{total}} \right) \times 100\% \quad (2)$$

де:  $A_{blocked}$  – кількість успішно заблокованих атак;  $A_{total}$  – загальна кількість атак.

**Висновки:** Результати тестування показують, що інтеграція Blockchain з SDN не лише підвищила рівень безпеки мережі, але й значно покращила її продуктивність і стійкість до атак. Скорочення часу відповіді контролера забезпечило швидке реагування на загрози, що є критично важливим для запобігання їх негативному впливу. Високий рівень блокування атак свідчить про надійність впроваджених механізмів захисту, а продуктивність блокчейну підтвердила його придатність для використання у масштабованих системах.

## Література

1. Romanov, O., Siemens, E., Nesterenko, M., Mankivskiy, V. Mathematical description of control problems in SDN networks/Proceedings of International Conference on Applied Innovation in IT, 2021, 9(1), стр. 33–39, <http://dx.doi.org/10.25673/36582>
2. Romanov, O., Nesterenko, M., Veres, L., Kamarali, R., Saychenko, I. Methods for calculating the performance indicators of ip multimedia subsystem (ims)/(2021) Lecture Notes in Networks and Systems, 152, pp. 229-256, DOI: 10.1007/978-3-030-58359-0\_13 [https://link.springer.com/chapter/10.1007/978-3-030-58359-0\\_13](https://link.springer.com/chapter/10.1007/978-3-030-58359-0_13)
3. Romanov O., Korniienko N., Obod I., Svyd I. Construction of the SDN Control Level Based on ONOS./ 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odesa, Ukraine, 2021, pp. 127-132, doi: 10.1109/UkrMiCo52950.2021.9716691.
4. Romanov, O., Nesterenko, M., Boggia, G., Striccoli, D. Construction and Methods for Solving Problems at the SDN Control Level // Lecture Notes in Electrical Engineering, 2023, 965 LNEE, p. 85–101 [https://link.springer.com/chapter/10.1007/978-3-031-24963-1\\_6](https://link.springer.com/chapter/10.1007/978-3-031-24963-1_6)
5. Al-Emari, S., Anbar, M., Sanjalawe, Y. K., Manickam, S., & Hasbullah, I. H. 2022. Intrusion detection systems using blockchain technology: a review, issues and challenges. Computer Systems Science and Engineering, 40(1), 87-112. <https://doi.org/10.32604/csse.2022.017941>
6. Algarni, S., Eassa, F., Almarhabi, K. A., Algarni, A., & Albeshri, A. 2022. Bcnbi: a blockchain-based security framework for northbound interface in software-defined networking. Electronics, 11(7), 996. <https://doi.org/10.3390/electronics11070996>
7. Alharbi, T. 2020. Deployment of blockchain technology in software defined networks: a survey. IEEE Access, 8, 9146-9156. <https://doi.org/10.1109/access.2020.2964751>
8. Ali, G. M. and Chen, H. 2023. Power of fuzzing and machine learning in smart contract security validation. Fuzzy Systems and Data Mining IX. <https://doi.org/10.3233/faia231090>