Перспективним напрямком є інтелектуальний підхід, заснований на машинному навчанні та векторному описі хеш-даних. У межах такого підходу хеш-рядок розглядається як об’єкт із низкою параметрів: довжиною, алфавітною структурою, ентропією, наявністю сольового компоненту, сигнатурними характеристиками алгоритму та поведінковими патернами. На основі цих ознак формується багатовимірний простір, у якому класифікаційна модель визначає рівень криптографічного ризику без необхідності здійснення перебору або криптографічного зламу.

Підвищення ефективності аналізу хеш-даних можливе за умови поєднання інтелектуальних методів із комплексним урахуванням контексту їх використання. Це включає аналіз частоти появи певних типів хешів у корпоративних системах, оцінку відповідності політикам автентифікації, виявлення системних аномалій у структурі даних та зіставлення їх з чинними стандартами криптографічного захисту. Такий підхід дозволяє оцінювати не лише стійкість конкретного значення, а й прогнозувати потенційні маршрути атак, зумовлені слабкими ланками інфраструктури або помилками адміністрування.

Подальший розвиток інтелектуального аналізу хеш-функцій пов’язаний із впровадженням адаптивних моделей, здатних оновлювати правила класифікації відповідно до появи нових алгоритмів, технік обходу криптографічних бар’єрів та шаблонів атак. Важливим напрямом є також інтеграція таких систем із платформами моніторингу подій безпеки (SIEM), що забезпечує оперативне виявлення відхилень та підвищує рівень кіберстійкості. Застосування інтелектуальних технологій у поєднанні зі структурним криптоаналізом формує підґрунтя для створення проактивних інструментів захисту, які здатні запобігати інцидентам ще на етапі їх формування.

Література

1. Stallings W. 2023. Cryptography and Network Security: Principles and Practice. Pearson. P. 145–200.

2. Aghaei A., Homayoun H., Sasan A. 2020. Hash Function Security Evaluation via Machine Learning-Based Structural Analysis. ACM. P. 1–10.

3. Hindy H., Brosset D., Bayne E. et al. 2020. A Taxonomy and Survey of Intrusion Detection Systems Using Machine Learning. ACM Computing Surveys. P. 1–41.

4. Zhang Y., Wang L., Sun Q. 2021. A Survey on Deep Learning-Based Hashing Methods. IEEE Transactions on Knowledge and Data Engineering. P. 1–20.

УДК 004.056: 004.738.5

І. М. Чепіль, В.Д. Тимощук
(Тернопільський національний технічний університет імені Івана Пулюя)

МОДЕЛЬ НАДАННЯ МЕРЕЖЕВИХ СЕРВІСІВ У SDN З ПІДТРИМКОЮ BRING YOUR OWN CONTROL

I. Chepil, V. Tymoshchuk

A NETWORK SERVICE PROVISIONING MODEL IN SDN WITH BRING YOUR OWN CONTROL

Програмно-визначені мережі (SDN) дедалі частіше стикаються з обмеженнями традиційної моделі централізованого керування, яка ускладнює швидку адаптацію мережевих сервісів безпеки до динамічних загроз та індивідуальних потреб

користувачів [1]. У ситуаціях, коли політики безпеки повинні модифікуватися у реальному часі, а впровадження складних сервісів, таких як VPN чи IPS, залежить від рішень оператора, відсутність гнучкості та можливості клієнта впливати на процес керування призводить до затримок, зниження ефективності реагування та перевантаження площини керування.

У цьому контексті запропоновано застосування концепції Bring Your Own Control (BYOC), що забезпечує розподіл управлінських повноважень між оператором мережі та користувачем шляхом впровадження гостьового контролера (GC), який взаємодіє з контролером оператора (SO). Оператор зберігає контроль над інфраструктурою, глобальними політиками безпеки та ресурсами, тоді як клієнт через GC отримує можливість самостійно керувати сервісами безпеки у власному домені. Ключову роль відіграє північний інтерфейс (NBI), що реалізується як гібрид REST/XMPP [2]. REST використовується для синхронних операцій управління сервісом, тоді як XMPP забезпечує асинхронну доставку подій безпеки, публікацію та підписку на повідомлення IDS/IPS, а також ідентифікацію GC за допомогою ID.

Архітектура BYOC-сервісу кібербезпеки проілюстрована на прикладі захищеного VPN з інтегрованою IPS [3]. На кожному клієнтському майданчику розгортається IDS-end, інтегрований з OpenFlow-комутатором [4], який перенаправляє весь трафік через сенсор. Події безпеки формуються у вигляді OpenFlow PacketIn із маркуванням у полі IPProto для розрізнення log та alert-повідомлень. У Service Operator вони обробляються модулем Decision Engine, який, спираючись на базу рішень (Decision Base), визначає відповідний GC і передає події через Service Dispatcher за протоколом XMPP. У свою чергу Security Manager у складі GC аналізує події та генерує рішення щодо блокування, перенаправлення чи додаткового моніторингу трафіку, які надалі застосовуються до інфраструктури через SDN-контролер (OpenDaylight з OpenFlow-підтримкою [5]).

Розроблена модель демонструє можливість побудови двошарової системи керування, у якій поєднуються централізоване управління ресурсами з боку оператора та децентралізоване управління політиками безпеки з боку клієнта. Це скорочує час реакції на інциденти, підвищує адаптивність сервісів та спрощує інтеграцію сторонніх рішень кіберзахисту.

Література

1. Software Defined Networking (SDN). Microsoft Learn. URL: https://learn.microsoft.com/uk-ua/windows-server/networking/sdn/ (date of access: 30.11.2025).

2. Standards Process | XMPP - The universal messaging standard. URL: https://xmpp.org/about/standards-process/ (date of access: 30.11.2025).

3. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332. https://doi.org/10.62731/mcnd-29.11.2024.004

4. OpenFlow – protocol overview - EXATEL. URL: https://exatel.pl/en/knowledge/blog/articles/openflow-protocol-overview/ (date of access: 30.11.2025).

5. OpenDaylight. URL: https://www.opendaylight.org/ (date of access: 30.11.2025).