першому кільці лишків, а внутрішні — у другому, що повністю унеможливлює частотний криптоаналіз. Для руйнування візуальних патернів застосовується позиційно залежна квадратична маска, яка додає унікальне псевдовипадкове зміщення на основі глобальних координат блоку [1].

Для внутрішніх елементів реалізовано механізм алгебраїчного зчеплення через знаходження їхньої суми та різниці в модульному просторі, що створює потужний лавинний ефект. Використання цих операцій формує нерозривну залежність між сусідніми пікселями, тому будь-яка спроба локальної модифікації руйнує весь зашифрований блок, надійно захищаючи цілісність документа. Повна математична оборотність системи при використанні мультиплікативного оберненого елемента забезпечує бездоганне побітове відновлення оригінального зображення без жодних структурних втрат чи артефактів.

Проведені дослідження підтверджують, що поєднання векторного розбиття, двокільцевої обробки та позиційно-залежної маски забезпечує абсолютно рівномірний розподіл інтенсивностей на гістограмі шифротексту. Це повністю перетворює початкові візуальні дані на гетерогенний псевдовипадковий шум та експоненціально ускладнює проведення диференціальних і статистичних атак, роблячи запропонований підхід ефективним методом для конфіденційного електронного документообігу.

1. Zhang B., Liu L. Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics*. 2023. Vol. 11, no. 11. P. 2585. DOI: https://doi.org/10.3390/math11112585

Порівняльний аналіз SDN-систем за критеріями кібербезпеки

УДК 004.056:004.7

Юрій Кльоц[1], Олексій Федоров[2]

Хмельницький національний університет, [1]klots@khmnu.edu.ua, [2] fedorovoo@khmnu.edu.ua

Програмно-конфігурована мережа є архітектурою, у якій функції керування трафіком логічно відокремлюються від функцій його передавання. На відміну від традиційної мережевої інфраструктури, де рішення щодо маршрутизації або комутації приймаються розподілено на кожному пристрої, у SDN значна частина логіки керування концентрується в контролері. Це забезпечує централізоване застосування політик, гнучке програмне керування трафіком, швидке впровадження змін конфігурації та можливість побудови систем автоматизованого виявлення аномалій [1].

З погляду кібербезпеки SDN-архітектура має подвійний характер. З одного боку, централізоване керування спрощує реалізацію політик сегментації, ізоляції вузлів, динамічного блокування потоків, перенаправлення трафіку на засоби аналізу та збирання телеметрії з мережевих пристроїв. З іншого боку, контролер, southbound-канали та програмно-керовані комутатори стають критичними об’єктами захисту. Компрометація контролера або порушення цілісності правил потоків може призвести до порушення роботи всієї мережевої

інфраструктури. Тому під час порівняння SDN-систем доцільно оцінювати не лише їхню продуктивність, масштабованість і підтримку протоколів, а й здатність забезпечувати виявлення шкідливих дій на рівні кінцевих пристроїв, контролера та програмно-керованого обладнання [2].

Для порівняльного аналізу SDN-систем доцільно використовувати такі критерії: архітектурна роль системи, підтримувані протоколи керування, масштабованість, наявність відкритих API, можливість інтеграції з системами моніторингу й аналізу трафіку, підтримка журналювання подій, можливість отримання статистики потоків, підтримка механізмів контролю доступу, захищеність керуючих інтерфейсів, придатність до виявлення атак на кінцеві пристрої, а також придатність до виявлення атак на сам SDN-контролер і мережеве обладнання.

Порівняння SDN-систем доцільно виконувати не за кількістю підтримуваних протоколів, а за придатністю до виявлення шкідливих дій у трьох зонах: на кінцевих пристроях, на рівні контролера та на рівні програмно-керованого обладнання. Перша зона охоплює сканування, spoofing, DDoS-активність і порушення політик доступу. Друга зона стосується захисту API, застосунків контролера, автентифікації та перевантаження Packet-In подіями. Третя зона пов’язана з контролем flow-таблиць, southbound-з’єднань, стану портів і коректності топологічної інформації.

Для порівняння SDN-систем використаємо такі критерії: OF — OpenFlow / відкритість, API — відкритість і програмованість API, T — можливість телеметрії та отримання статистики (3 – так, 2 – частково, 1 – ні), E — виявлення дій кінцевих вузлів, C — захист і контроль контролера, D — контроль програмно-керованого обладнання, SI — інтеграція із зовнішнім аналізом, Σ — узагальнена придатність. Результати порівняння представлено в таблиці 1.

Таблиця 1

Порівняння SDN-систем за безпековими критеріями

Система	Клас	OF	API	T	E	C	D	SI	Σ
OpenDaylight	SDN-контролер	+	3	3	3	3	3	3	3
ONOS	SDN-контролер	+	3	3	3	3	3	3	3
Ryu	фреймворк	+	3	2	3	2	2	2	2
Floodlight	SDN-контролер Ctrl	+	2	2	2	1	2	2	2
Open vSwitch	програмний комутатор vSw	+	2	3	2	1	2	3	2
VMware NSX	SDN/NFV-платформа	-	2	3	3	3	3	3	3
Omada	NMS	-	1	2	2	2	2	1	2

Результати порівняння свідчать, що системи програмно-конфігурованих мереж, незалежно від призначення, мають спільну особливість: централізація керування підвищує гнучкість адміністрування, але водночас формує нові критичні точки вразливості. SDN-контролер, northbound- і southbound-

інтерфейси, програмно-керовані комутатори та кінцеві пристрої утворюють багаторівневу поверхню атаки, тому безпека SDN-інфраструктури не може обмежуватися лише фільтрацією трафіку або налаштуванням політик доступу.

Наявність механізмів централізованого керування, телеметрії, журналювання, аналізу потоків і програмного застосування політик створює передумови для побудови ефективних засобів захисту. Водночас ці можливості не усувають вразливостей автоматично, тому розглянуті системи потребують додаткових механізмів виявлення атак, кореляції подій, контролю цілісності правил, аналізу поведінки кінцевих пристроїв і захисту каналів взаємодії між компонентами SDN-архітектури.

Отже, результати порівняння підтверджують актуальність розроблення методів захисту та виявлення атак у програмно-конфігурованих мережах. Особливо важливими є методи, що враховують стан контролера, зміни в таблицях потоків, поведінку програмно-керованого обладнання, активність кінцевих вузлів і параметри службової взаємодії між компонентами SDN.

1. Odarchenko, R.; Iavich, M.; Iashvili, G.; Fedushko, S.; Syerov, Y. Assessment of Security KPIs for 5G Network Slices for Special Groups of Subscribers. Big Data Cogn. Comput. 2023, 7, 169. https://doi.org/10.3390/bdcc7040169
2. Cherednichenko O., Sharonova N., Pliekhova G., Babkova N. Intelligent Methods of Secure Routing in Software-Defined Networks. CEUR Workshop Proceedings. 2024. Vol. 3664. P. 342–351. https://doi.org/10.31110/COLINS/2024-1/024

Аналіз методологічного забезпечення оцінювання кіберстійкості інформаційних ресурсів

УДК 004.056:006.01

Олександра Ковальчук[1], Євгенія Іванченко[2]

Державний університет інформаційно-комунікаційних технологій,
[1]oa.kovalchuk@duikt.edu.ua, [2]e.ivanchenko@duikt.edu.ua

У сучасних умовах зростання складності кібератак традиційні підходи до безпеки стають недостатніми. Актуальним є перехід від кібербезпеки до кіберстійкості (Cyber Resilience) – здатності інформаційних ресурсів (ІР) не лише протистояти загрозам, але й адаптуватися до них та швидко відновлюватися. Проте на практиці виникає проблема об'єктивної оцінки реального рівня такої стійкості.

Метою є аналіз методологій управління кіберстійкістю ІР для виявлення їхніх переваг та недоліків. Для досягнення поставленої мети необхідно здійснити порівняльний аналіз п’яти провідних фреймворків за критеріями фокусу оцінки, динаміки тестування та джерел даних.

Фундаментом для побудови систем кіберстійкості виступають міжнародні стандарти, зокрема ISO/IEC 27001 закладає основу через впровадження системи управління інформаційною безпекою (СУІБ) та забезпечує функцію