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

протистояння (Withstand) через систематичне управління ризиками [1]. ISO/IEC 27031 визначає готовність ІКТ-інфраструктури до забезпечення безперервності бізнесу, допомагає визначити рівень готовності для досягнення цільових метрик безперервності [2]. NIST CSF описує життєвий цикл стійкості через п'ять основних функцій: ідентифікація, захист, виявлення, реагування та відновлення [3]. NIST SP 800-160: пропонує інженерний підхід, розглядаючи безпеку як невід'ємну властивість архітектури (Security by Design) та включає принципи надмірності та «м'якої деградації» [4].

Для переведення підходів, описаних у стандартах, у практичну площину застосовуються спеціалізовані методики оцінювання. Для детального аналізу було обрано п'ять методологій, що різняться за фокусом та інструментарієм - CRR [6], CAF [8], C-RA[9], CRI [7] та IT Governance [10] (табл. 1).

Таблиця 1

Порівняльний аналіз методик оцінки кіберстійкості інформаційних ресурсів

Методологія	*Фокус оцінки*	*Динаміка*	*Джерело даних*
CRR (CISA)	Зрілість процесів (якісна)	Статична	Опитування, документація
CAF (UK NCSC)	Досягнення цілей (якісна)	Статична	Аудит доказів
C-RAF (НКМА)	Гібридний (зрілість + тех.)	Динамічна	Тестування (iCAST), опитування
CRI (Академічні)	Кількісні метрики (MTTR)	Статична	Технічні показники
IT Governance	Управлінська зрілість	Статична	Консалтинговий аудит

Проведений аналіз провідних фреймворків показав, що якісні моделі (CRR, IT Governance) зосереджені на оцінці зрілості процесів, але базуються на суб'єктивних опитуваннях, що дає уявлення про «паперову стійкість». CRA базується на якості і достатності зібраних доказів для проведення оцінки. Кількісні моделі (CRI) закладають до об'єктивність оцінки через метрики часу (MTTR, RTO), проте часто не враховують організаційний контекст та бізнес-пріоритети. Динамічне тестування застосовується тільки у вузькоспеціалізованому фреймворку C-RAF, де використовується моделювання атак на основі Threat Intelligence (iCAST).

Ключовим недоліком фреймворків є відсутність механізмів перевірки адекватності та достовірності вихідних даних. Якісні моделі залежать від компетентності відповідей при самооцінці, кількісні моделі - від актуальності метрик, що використовуються для оцінки, що може призвести до формування хибного уявлення про захищеність ІР.

Отже, аналіз показав, що жодна з розглянутих методологій не вирішує проблему адекватності вхідних даних. Перспективою досліджень є розробка механізму, що поєднав би кількісні архітектурні метрики з оцінкою зрілості процесів та обов'язковим коефіцієнтом валідації вхідних даних.

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy

protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/27001
2. ISO/IEC 27031:2025. Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity. URL: https://www.iso.org/standard/27031
3. The NIST Cybersecurity Framework (CSF) 2.0. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
4. NIST Special Publication 800-160, Volume 2. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
5. MITRE ATT&CK Framework. URL: https://attack.mitre.org/\
6. Cyber Resilience Review. URL: https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr
7. Cyber Resilience Index. URL: https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf
8. Cyber Assessment Framework. URL: https://www.ncsc.gov.uk/collection/cyber-assessment-framework
9. Cyber Resilience Assessment Framework. URL: https://uploads-ssl.webflow.com/59d28ad983887e000196f803/5fecc1fe13498132b4fa835b_HKMA CFI - Cyber Resilience Assessment Framework - Dec 2016.pdf
10. IT Governance Cyber Resilience Framework. URL: https://www.itgovernance.co.uk/cyber-resilience-framework

Мережева безпека IoT-пристроїв у кіберфізичних системах розумного міста

УДК 004.056:004.738.5:681.5

Андрій Микитишин[1], Сергій Козак[2]
Роман Ніколайчук[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]mikitishin@gmail.com, [2]serhii_kozak1710@tntu.edu.ua,
[3]romanikolaychuk2017@gmail.com

Концепція розумного міста передбачає використання кіберфізичних систем, у яких IoT-пристрої поєднують фізичні об'єкти інфраструктури з цифровими сервісами, сенсорними мережами, edge-вузлами, хмарними платформами та системами підтримки рішень. Вони забезпечують телеметрію, дистанційне керування, автоматичне реагування й інтеграцію з сервісами освітлення, транспорту, екологічного моніторингу, енергоменеджменту, водопостачання та безпеки громадських просторів. Ключовою проблемою є мережева безпека IoT-пристроїв, оскільки через мережеву взаємодію передаються дані між сенсорами, шлюзами, платформами оброблення й операторськими інтерфейсами. Розподіленість вузлів, різнорідні протоколи, обмежені ресурси, фізична доступність частини обладнання, бездротові канали й залежність від хмарних сервісів підвищують ризик перехоплення або підміни телеметрії, відмови сервісу, втрати керованості виконавчими механізмами та помилкових