

ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ШЛЯХОМ СИМУЛЯЦІЇ КІБЕРАТАКИ НА МЕРЕЖУ ІНФРАСТРУКТУРНОГО ОБ'ЄКТА

Г. В. Хоменко¹, В. В. Личик¹

¹ Навчально-науковий Фізико-технічний інститут

Анотація

У цій роботі запропоновано метод кількісного оцінювання кіберстійкості енергетичного об'єкта критичної інфраструктури. Розроблено та реалізовано імітаційну модель мережі енергетичного об'єкта в середовищі GNS3. Проведено серію симуляцій кібератак за допомогою платформи MITRE Caldera для трьох різних рівнів захищеності. На основі отриманих даних розроблено математичну модель на базі ланцюгів Маркова та алгоритм розрахунку інтегрального індикатора кіберстійкості.

Ключові слова: кіберстійкість, ланцюг Маркова, MITRE Caldera, критична інфраструктура, кібератака.

Вступ

У сучасних умовах стрімкої цифровізації об'єкти критичної інфраструктури, зокрема енергетичні системи, стали першочерговими цілями для складних кібератак, що підтримуються на державному рівні. Атаки FrostyGoop у 2024 році на Львівський теплопостачальний об'єкт та кампанії угруповання Sandworm проти підприємств АСКТП України у 2024–2025 рр. засвідчили, що традиційний підхід до кібербезпеки, орієнтований виключно на превентивний захист, є недостатнім [1, 2]. Зокрема, атака FrostyGoop спричинила відключення теплопостачання для близько 600 багатоквартирних будинків у розпал зимового сезону, що наочно демонструє реальні наслідки кібервпливу на фізичну інфраструктуру.

Існуючі методи оцінки значною мірою базуються на суб'єктивних експертних оцінках та не надають об'єктивних кількісних показників, порівнянних між різними об'єктами. Це зумовлює потребу у розробленні механізму оцінювання кіберстійкості, що ґрунтується на об'єктивних технічних параметрах і результатах практичного тестування [3].

1. Побудова моделі мережі енергетичного об'єкта

Для проведення дослідження розроблено імітаційну модель мережі розподільчої підстанції в середовищі GNS3, розгорнутому на хмарній платформі GCP (рис. 1). Модель охоплює 12 віртуальних вузлів і побудована за принципом ешелонованого захисту з трьома ізольованими сегментами:

- DMZ;
- корпоративний сегмент;
- технологічний сегмент SCADA.

DMZ містить вузли, які доступні ззовні — Web-сервер та DNS-сервер, що є першою точкою конта-

кту для потенційного зловмисника. Корпоративний сегмент об'єднує внутрішні сервери — App-сервер, HDS та контролер домену. Технологічний сегмент SCADA є найбільш критичним — він містить промислові контролери та інтерфейси керування, безпосередньо пов'язані з фізичним обладнанням підстанції.

Роль критичної цілі в моделі відведено комунікаційному шлюзу FEP — єдиному вузлу, що забезпечує зв'язок між IT-інфраструктурою та промисловими контролерами RTU. Для обґрунтування параметрів атак використано базу CVE та метрики CVSS. Зокрема, вразливість CVE-2023-35078 (CVSS 10,0) моделює компрометацію зовнішнього периметра, а CVE-2021-3493 (CVSS 7,8) — горизонтальне переміщення всередині мережі.

Вибір GNS3 як середовища моделювання обумовлений можливістю точного відтворення мережевої топології з реальними мережевими стеками, на відміну від суто симуляційних підходів. Це забезпечує відповідність поведінки віртуальних вузлів реальним умовам функціонування промислових мереж.

2. Симуляція кібератаки на мережу підстанції

Для тестування захищеності моделі використано платформу MITRE Caldera — інструмент для автоматизованої симуляції дій зловмисника, що базується на базі знань MITRE ATT&CK [4]. Метою кожного сценарію було досягнення критичного технологічного шлюзу FEP, оскільки його компрометація унеможливує передачу команд керування до польових пристроїв, що рівнозначно втраті контролю над усією підстанцією. Проведено три послідовних сценарії з різними рівнями впроваджених контрзаходів.

У першому сценарії мережа функціонувала без сегментації — міжмережеві екрани виконували ви-

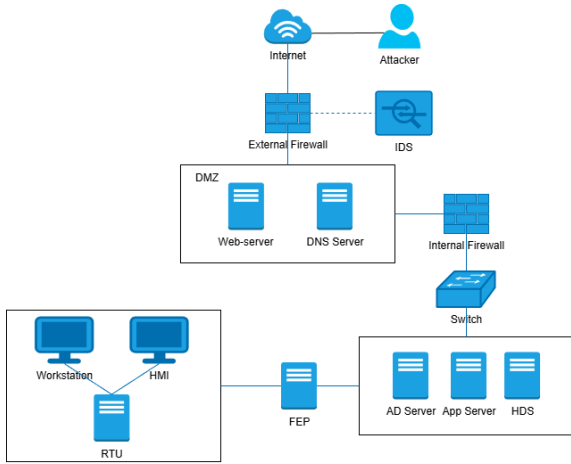


Рис. 1. Схема мережі енергетичного об'єкта

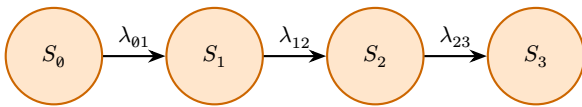


Рис. 2. Граф станів

ключно роль маршрутизаторів. За таких умов зловмисник безперешкодно просунувся від зовнішнього периметра до цільового вузла за мінімальний час, використавши лише один проміжний крок. Ймовірність компрометації $P_3(t)$ сягнула 1,00 вже впродовж перших хвилин спостереження, а індикатор кіберстійкості склав $K_{res} = ,02$, що фактично відповідає повній відсутності стійкості.

У другому сценарії було впроваджено мережеву сегментацію, що дозволило заблокувати прямий доступ між зовнішнім периметром та технологічним сегментом. Це змусило зловмисника шукати обхідний маршрут через проміжні вузли, що суттєво збільшило кількість кроків та загальний час атаки порівняно з першим сценарієм. Зокрема, значення $P_3(t) = ,5$ було досягнуто лише на 14-й хвилині, а K_{res} зріс до ,36.

У третьому сценарії, на додаток до сегментації, було проведено зміцнення конфігурацій кінцевих точок — усунено надлишкові довірчі зв'язки між вузлами. Попри це, зловмисник все одно досяг цільового вузла, однак лише на 22-й хвилині, а фінальна ймовірність компрометації знизилась до $P_3(50) = ,81$ при $K_{res} = ,51$. Отримані результати наочно демонструють залежність між рівнем захисту та стійкістю системи (рис. 3).

3. Кількісний розрахунок індикатора кіберстійкості

Для кількісного оцінювання кіберстійкості застосовано математичний апарат марковських процесів із неперервним часом. Мережу підстанції формалізовано як граф із чотирьох станів (рис. 2):

- S_0 — вихідний стан;
- S_1 — компрометація DMZ;
- S_2 — компрометація корпоративного сегмента;

• S_3 — компрометація технологічного сегмента. Інтенсивність переходів λ_{ij} розраховується за формулою (1):

$$\lambda = \frac{1}{T \cdot (1 - S_{norm})} \cdot (1 - E) \quad (1)$$

де T — час, необхідний зловмиснику для переходу між вузлами, S_{norm} — нормований бал CVSS, E — ефективність контрзаходів.

Ключовим вхідним параметром моделі є нормований бал вразливості S_{norm} , що обчислюється на основі метрики CVSS [5]. Система CVSS є міжнародним стандартом кількісної оцінки критичності вразливостей програмного забезпечення та формує числовий бал у діапазоні від 0 до 10 на основі трьох груп метрик.

Базові метрики відображають незмінні характеристики вразливості: вектор доступу, складність експлуатації та необхідний рівень привілеїв. Тимчасові метрики враховують поточний стан доступності експлуату та рівень готовності патча. Контекстні метрики адаптують оцінку до конкретного середовища розгортання системи.

У даній роботі використовуються базові метрики CVSS, оскільки вони є об'єктивними та відтворюваними незалежно від умов. Чим вищий бал CVSS, тим вища інтенсивність атаки λ , тобто, зловмисник швидше долає відповідний бар'єр.

Динаміка ймовірностей описується системою диференціальних рівнянь Колмогорова [6]. У загальному вигляді для лінійної структури переходу $S_0 \rightarrow S_1 \rightarrow S_2 \rightarrow S_3$ система має вигляд (2):

$$\begin{cases} \frac{dP_0(t)}{dt} = -\lambda_{01}P_0(t) \\ \frac{dP_1(t)}{dt} = \lambda_{01}P_0(t) - \lambda_{12}P_1(t) \\ \frac{dP_2(t)}{dt} = \lambda_{12}P_1(t) - \lambda_{23}P_2(t) \\ \frac{dP_3(t)}{dt} = \lambda_{23}P_2(t) \end{cases} \quad (2)$$

де $P_i(t)$ — ймовірність того, що в момент часу t система перебуває у стані S_i . Сума всіх ймовірностей у будь-який момент часу повинна дорівнювати одиниці, що відображає умову повноти групи подій.

Фінальний інтегральний індикатор кіберстійкості обчислюється за формулою (3):

$$K_{res} = 1 - \frac{1}{T} \int_0^T P_3(t) dt \quad (3)$$

де $P_3(t)$ — ймовірність компрометації фінальної цілі у момент часу t , а T — загальний час спостереження. Значення $K_{res} \in [0; 1]$ дозволяє об'єктивно класифікувати рівень стійкості архітектури.

За результатами трьох сценаріїв симуляції отримано значення індикатора K_{res} , що зростає від першого сценарію до третього, підтверджуючи кількісну ефективність кожного рівня впроваджених контрзаходів. Це дозволяє не лише порівнювати архітектури між собою, а й обґрунтовувати пріоритетність інвестицій у конкретні захисні заходи.

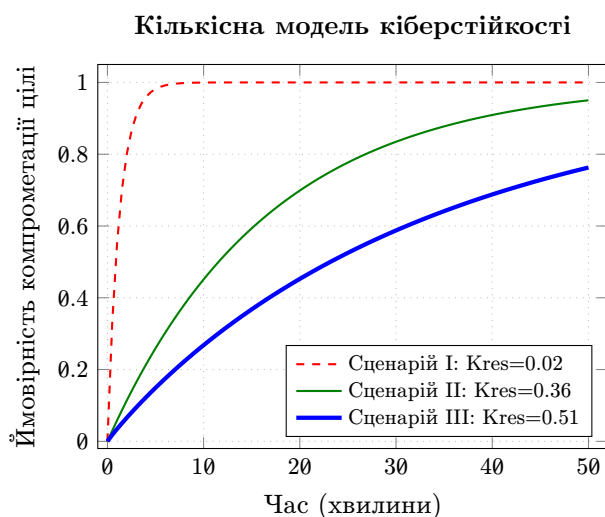


Рис. 3. Результати імітаційного моделювання динаміки кіберстійкості за різними сценаріями атак

Висновки

Проведене дослідження підтверджує актуальність впровадження механізмів кількісного оцінювання кіберстійкості для об'єктів критичної інфраструктури. Розроблена марковська модель дозволяє замінити суб'єктивні експертні оцінки об'єктивним числовим індикатором, що ґрунтується на реальних параметрах мережевої архітектури та результатах симуляції. Запропонований підхід може слугувати практичним інструментом при проектуванні захищеної ІТ-інфраструктури енергетичних об'єктів та розроб-

ці планів реагування на кіберінциденти в умовах гібридної війни.

Перелік використаних джерел

1. *Dragos Inc.* FrostyGoop ICS Malware Intelligence Brief. — 2024. — URL: https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_r2.pdf.
2. *CERT-UA.* Кібератаки, здійснені угрупованням UAC-0133 (Sandworm) на об'єкти критичної інфраструктури України. — 2024. — URL: <https://cert.gov.ua/article/6282517>.
3. Галущинський Л., Личик В. Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження) // Інформаційні технології та суспільство. — 2023. — 2 (8). — С. 27—33. — DOI: [10.32689/mup.it.2023.2.3](https://doi.org/10.32689/mup.it.2023.2.3).
4. *MITRE ATT&CK for ICS.* MITRE ATT&CK Matrices for ICS. — URL: <https://attack.mitre.org/matrices/ics/>.
5. Личик В. В., Галущинський Л. Ю. Використання моделі мереж Баеса для раннього оцінювання загроз кібератак об'єкта електроенергетики // Реєстрація, зберігання і оброб. даних. — 2025. — Т. 27, № 2. — С. 70—85. — DOI: [10.35681/1560-9189.2025.27.2.345591](https://doi.org/10.35681/1560-9189.2025.27.2.345591).
6. *Ross S. M.* Introduction to Probability Models. — 12th ed. — Academic Press, 2019. — URL: <https://dokumen.pub/introduction-to-probability-models-12nbsped-0128143460-9780128143469.html> ; 826 p.