НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»
УДК _____

ДО ЗАХИСТУ ДОПУЩЕНО
Завідувач кафедри
_____ Дмитро ЛАНДЕ
«___»_____2026 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
зі спеціальності 125 «Кібербезпека»

на тему: Кількісне оцінювання кіберстійкості мережі інфраструктурного об’єкта на основі імітаційного моделювання загроз

Виконав: здобувач вищої освіти **IV** курсу, групи ФБ-23

Хоменко Гліб Вячеславович _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник: асистент кафедри ІБ Личик В. В. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент: доцент кафедри ММАД, к.т.н. Лавренюк Алла Миколаївна _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач ступеня бакалавра _____
(підпис)

Київ – 2026 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
«___»_____2026 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Хоменку Глібу Вячеславовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: «Кількісне оцінювання кіберстійкості мережі інфраструктурного об'єкта на основі імітаційного моделювання загроз»

науковий керівник роботи Личик Владислав Васильович, асистент кафедри ІБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «____»_____2026 р. №

2. Термін подання здобувачем дипломної роботи: 10.06.2026 р.

3. Вихідні дані: методології оцінювання рівня кіберстійкості об'єктів критичної інфраструктури.

4. Зміст роботи: дослідження методів кібератак на об'єкти критичної інфраструктури та існуючих підходів до оцінювання їх захищеності, моделювання мережевої топології розподільчої підстанції, симуляція сценаріїв кіберзагроз, а також створення програмного інструменту для обчислення показника кіберстійкості системи.

5. Орієнтований перелік ілюстративного матеріалу: презентація до захисту дипломної роботи.

6. Дата видачі завдання: 1 вересня 2025 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Визначення напрямку ДР	08.10.2025 – 25.11.2025	Виконано
2	Визначення теми ДР	26.11.2025 – 02.12.2025	Виконано
3	Збір та аналіз літературних джерел	03.12.2025 – 03.01.2026	Виконано
4	Дослідження кібератак на об’єкти критичної інфраструктури	04.01.2026 – 20.01.2026	Виконано
5	Огляд сучасних методів оцінки кіберстійкості	21.01.2026 – 31.01.2026	Виконано
6	Написання першого розділу	01.02.2026 – 10.02.2026	Виконано
7	Дослідження архітектури мережі енергетичного об’єкта	11.02.2026 – 25.02.2026	Виконано
8	Аналіз існуючих інструментів для моделювання мережі об’єкта критичної інфраструктури	26.02.2026 – 05.03.2026	Виконано
9	Побудова та розгортання імітаційної моделі мережі енергетичного об’єкта	06.03.2026 – 21.03.2026	Виконано
10	Написання другого розділу	21.03.2026 – 31.03.2026	Виконано
11	Аналіз існуючих інструментів для імітації кібератаки	01.04.2026 – 07.04.2026	Виконано
12	Проведення симуляцій кібератак та збір експериментальних даних	08.04.2026 – 22.04.2026	Виконано
13	Написання третього розділу	22.04.2026 – 30.04.2026	Виконано
14	Формулювання математичного апарата для оцінки кіберстійкості	01.05.2026 – 14.05.2026	Виконано
15	Розробка програмного застосунку	15.05.2026 – 20.05.2026	Виконано
16	Написання четвертого розділу	21.05.2026 – 28.05.2026	Виконано
17	Оформлення ДР	29.05.2026 – 10.06.2026	Виконано
18	Передзахист	11.06.2026	Виконано
19	Захист	19.06.2026	Виконано

Здобувач вищої освіти _____ Гліб ХОМЕНКО

Керівник роботи _____ Владислав ЛИЧИК

РЕФЕРАТ

Дипломна робота складається з 4 розділів, містить 61 сторінку, 18 рисунків, 5 таблиць та 16 джерел за переліком посилань.

Мета роботи – дослідження методів обрахунку кіберстійкості критичної інфраструктури та розробка програмного рішення для оцінювання кіберстійкості об’єкта.

Об’єкт дослідження – процес забезпечення кіберстійкості та функціонування ІТ-мережі об’єкта критичної інфраструктури.

Предмет дослідження: методи та механізми кількісного оцінювання кіберстійкості інформаційних мереж об’єктів критичної інфраструктури.

Методи дослідження: імітаційне моделювання мережевої інфраструктури, автоматизована симуляція кібератак на основі бази знань MITRE ATT&CK, теорія марковських процесів з неперервним часом, розв’язання систем диференціальних рівнянь, кількісний аналіз вразливостей на основі метрик CVSS.

Результати досліджень було апробовано на XXIV Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» КПІ ім. Ігоря Сікорського, 13-16 травня 2026 р.

Ключові слова: кіберстійкість, критична інфраструктура, кібератака, ІТ-мережа, CVE-вразивості, ланцюг Маркова, MITRE Caldera.

ABSTRACT

This work consists of 4 chapters, contains 61 pages, 18 figures, 5 tables and 16 sources in the list of references.

The purpose of the work – studying methods for calculating the cyber resilience of critical infrastructure and developing a software solution for assessing the cyber resilience of an object.

The object of the research – the process of ensuring cyber resilience and functioning of the IT network of a critical infrastructure object.

The subject of the research: methods and mechanisms for quantitative assessment of the cyber resilience of information networks of critical infrastructure objects.

Research methods: simulation modeling of network infrastructure, automated cyber attack simulation based on the MITRE ATT&CK knowledge base, continuous-time Markov process theory, solving systems of differential equations, quantitative vulnerability analysis based on CVSS metrics.

The results of the study were tested at the XXIV All-Ukrainian Scientific and Practical Conference of Students, Postgraduate Students and Young Scientists "Theoretical and applied problems of physics, mathematics and informatics" of Igor Sikorsky Kyiv Polytechnic Institute, May 13-16, 2026.

Keywords: cyber resilience, critical infrastructure, cyber attack, IT network, CVE vulnerabilities, Markov chain, MITRE Caldera.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

C2 – Command and Control

CVE – Common Vulnerabilities and Exposures

CVSS – Common Vulnerability Scoring System

DMZ – Demilitarized Zone

DoS – Denial of Service

FEP – Front-End Processor

GCP – Google Cloud Platform

GNS3 – Graphical Network Simulator-3

HDS – Historical Data Server

HMI – Human machine interface

ICS – Industrial Control System

RTU – Remote Terminal Unit

ВСТУП

Актуальність роботи:

У сучасних умовах стрімкої цифровізації та зростання кількості кібератак особливої актуальності набуває проблема забезпечення високої кіберстійкості об’єктів критичної інфраструктури, зокрема енергетичних систем. Відомі підходи до оцінювання захищеності таких систем часто не враховують комплексний вплив атак у реальних умовах функціонування мереж. Це зумовлює необхідність застосування методів моделювання та симуляції кібератак для більш точної оцінки рівня кіберстійкості, що є важливим для підвищення національної безпеки України.

Мета дослідження: дослідження методів обрахунку кіберстійкості критичної інфраструктури та розробка програмного рішення для оцінювання кіберстійкості об’єкта.

Завдання дослідження:

1. Провести аналіз сучасних методів оцінювання кіберстійкості.
2. Дослідити типові кібератаки на об’єкти критичної інфраструктури.
3. Розробити модель мережі енергетичного об’єкта та реалізувати її.
4. Провести симуляцію кібератак на ІТ-мережу.
5. Розробити програмне рішення для кількісного обрахунку кіберстійкості та провести оцінювання на основі отриманих даних.

Об’єкт дослідження: процес забезпечення кіберстійкості та функціонування ІТ-мережі об’єкта критичної інфраструктури.

Предмет дослідження: методи та механізми кількісного оцінювання кіберстійкості інформаційних мереж об’єктів критичної інфраструктури.

Методи дослідження: імітаційне моделювання мережевої інфраструктури, автоматизована симуляція кібератак на основі бази знань MITRE ATT&CK, теорія марковських процесів з неперервним часом, розв’язання систем диференціальних рівнянь, кількісний аналіз вразливостей на основі метрик CVSS.

Наукова новизна дослідження: запропоновано метод кількісного оцінювання кіберстійкості об’єктів критичної інфраструктури, що базується на поєднанні результатів практичної симуляції кібератак з математичною моделлю марковських процесів.

Практичне значення одержаних результатів: розроблений програмний застосунок та методика можуть застосовуватися фахівцями з кібербезпеки для порівняльного оцінювання архітектурних рішень захисту мереж енергетичних об’єктів, обґрунтування пріоритетності інвестицій у засоби захисту, а також при розробці планів реагування на кіберінциденти в умовах гібридної війни.

Апробація результатів роботи: XXIV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» КПІ ім. Ігоря Сікорського, 13-16 травня 2026 р.

1 ОГЛЯД СУЧАСНИХ МЕТОДІВ ОЦІНКИ КІБЕРСТІЙКОСТІ ТА АНАЛІЗ АТАК НА КРИТИЧНУ ІНФРАСТРУКТУРУ

У сучасному науковому дискурсі поряд із кібербезпекою дедалі частіше розглядається концепція кіберстійкості. Якщо кібербезпека зосереджена на превентивному захисті систем від атак, то кіберстійкість є ширшим поняттям, що охоплює здатність системи передбачати, протистояти, відновлюватися та адаптуватися до кібератак [1, 2].

Кіберстійкість визначається як властивість системи зберігати здатність виконувати критичні функції навіть в умовах кібератак, збоїв або непередбачених відмов компонентів. Ключова ідея полягає в тому, що компрометація системи розглядається не як виключна подія, а як прогнозований сценарій, до якого система повинна бути підготовлена. На відміну від традиційної кібербезпеки, кіберстійкість не ставить за мету абсолютне запобігання атакам. Вона орієнтована на збереження функціональності під час атаки та швидке відновлення після неї.

Концептуально кіберстійкість описується через чотири взаємопов’язані цілі, що утворюють замкнений цикл: передбачення загроз до їх реалізації, протистояння атаці в момент її розгортання, відновлення після інциденту та адаптація системи на основі отриманого досвіду. Результати останньої фази безпосередньо підвищують якість передбачення у наступному циклі, що робить кіберстійкість процесом постійного вдосконалення.

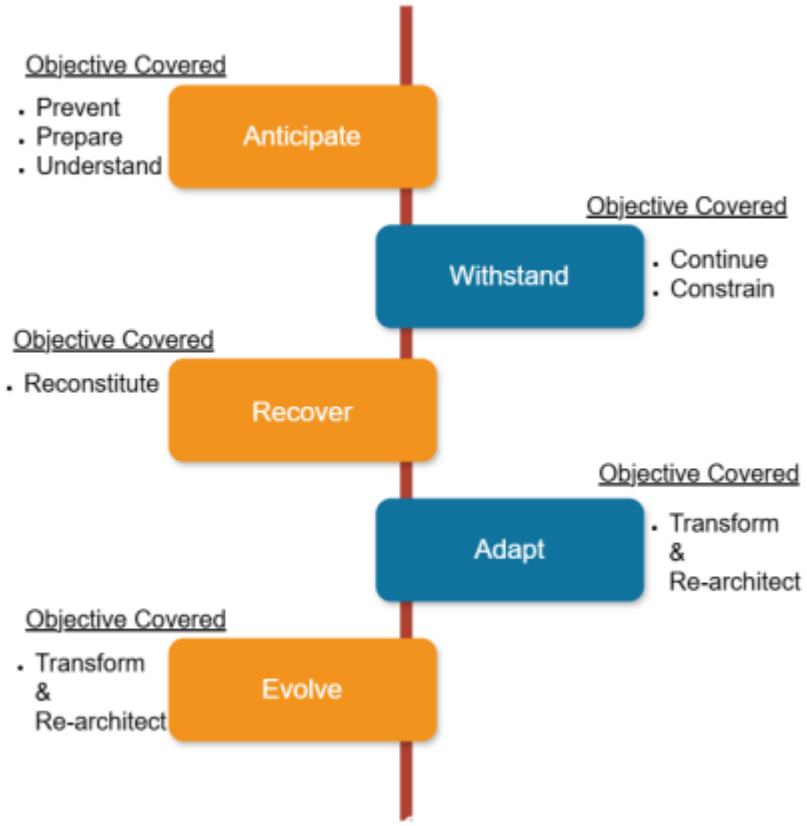

Рисунок 1.1 – Життєвий цикл кіберстійкості [1]

1.1 Сучасні методології та моделі оцінювання кіберстійкості

1.1.1 Модель CERT-RMM та метод оцінки Cyber Resilience Review

Фундаментальною розробкою у сфері управління кіберстійкістю є CERT Resilience Management Model (CERT-RMM) – модель зрілості, створена Інститутом програмної інженерії (SEI) при Університеті Карнегі-Меллон. CERT-RMM надає організаціям структурований підхід до управління операційною стійкістю, об’єднуючи три ключові функції: кібербезпеку, безперервність бізнесу та управління IT-операціями. Модель описує що потрібно робити для досягнення стійкості, а не як це технічно реалізувати, і складається з 26 процесних областей, які групуються у чотири категорії: Enterprise Management, Engineering, Operations

Management, and Process Management. CERT-RMM дозволяє оцінити поточний рівень зрілості процесів за шкалою від 0 до 4 (Incomplete, Performed, Managed, Defined), що дає організації розуміння, наскільки її процеси є передбачуваними та ефективними, особливо в умовах стресу [3].

На основі моделі CERT-RMM розроблено практичний метод оцінки Cyber Resilience Review (CRR), який є стандартизованим інтерв'ю-базованим інструментом самооцінки. Метод створений Агентством з кібербезпеки та безпеки інфраструктури США (CISA) і дозволяє організаціям швидко оцінити стан своєї операційної стійкості щодо критичних послуг через 10 доменів (Asset Management, Controls Management, Configuration and Change Management, Vulnerability Management, Incident Management, Service Continuity Management, Risk Management, External Dependencies Management, Training and Awareness, Situational Awareness). Оцінка проводиться у форматі структурованих інтерв'ю з ключовими учасниками з різних підрозділів, де учасники досягають консенсусу щодо відповідей на 299 питань. Результати представляються у вигляді звіту про зрілість процесів за шкалою Maturity Indicator Levels (MIL 0-3), з рекомендаціями щодо усунення прогалин. Метод добре інтегрується з NIST Cybersecurity Framework [4].

Практична цінність методу CRR полягає в тому, що він є повністю безкоштовним, простим у впровадженні та не вимагає складного технічного інструментарію, завдяки чому може використовуватися організаціями будь-якого розміру. CRR ефективно оцінює зрілість організаційних процесів, дозволяє швидко виявляти прогалини в забезпеченні кіберстійкості критичних послуг і сприяє конструктивному діалогу між різними підрозділами через структуровані інтерв'ю. Крім того, метод добре інтегрується з NIST Cybersecurity Framework і надає практичний звіт із чіткими рекомендаціями щодо подальшого вдосконалення.

Поряд із вищезазначеними позитивними аспектами, даній методиці притаманна низка обмежень. Зокрема, така оцінка значною мірою є суб'єктивною, оскільки сильно залежить від якості відповідей учасників інтерв'ю та досягнутого консенсусу. CRR не містить точних кількісних метрик, фокусуючись переважно на зрілості процесів, а не на технічній глибині аналізу. Через це результати важко порівнювати між різними організаціями, а сам метод краще підходить для початкової діагностики, ніж для детального технічного оцінювання кіберстійкості складних систем.

1.1.2 Фреймворк CREF та ситуаційна методика оцінювання SSM-CR

Cyber Resiliency Engineering Framework (CREF) – фреймворк, створений корпорацією MITRE у тісній співпраці з Національним інститутом стандартів і технологій США (NIST), є практичним інструментом для проєктування, аналізу та підвищення стійкості систем до кібератак. Він базується на ключових положеннях публікації NIST SP 800-160, Volume 2 (Rev. 1), присвяченої розробці кіберстійких систем [5]. CREF надає інженерам та архітекторам систем набір тактик, необхідних для того, щоб проєктувати стійкість як невід'ємну властивість системи. В основі фреймворку лежать чотири ключові стратегічні цілі:

1. Anticipate – підтримувати стан поінформованої готовності, щоб запобігти компрометації критичних бізнес-функцій;
2. Withstand – продовжувати виконання основних функцій навіть при частково успішній атаці;
3. Recover – відновити порушені функції після атаки;
4. Evolve – змінювати бізнес-функції або кіберспроможності для мінімізації наслідків від поточних або прогнозованих атак [6].

На основі цього фреймворку було розроблено метод кількісної оцінки Situated Scoring Methodology for Cyber Resiliency (SSM-CR). Якщо CREF визначає

що потрібно робити для досягнення стійкості, то SSM-CR пропонує механізм як це виміряти. Методика дозволяє адаптувати цілі та підцілі CREF під конкретну архітектуру системи, модель загроз, операційне середовище та пріоритети зацікавлених сторін. Оцінка проводиться шляхом пріоритизації цілей і підцілей, а потім експертної оцінки рівня виконання відповідних активностей і технік за шкалою від 0 до 5. Результати агрегуються від нижчого рівня (активностей) до вищого (підцілей і цілей), формуючи відносний бал кіберстійкості системи. Це дає змогу чітко виявляти прогалини в захисті та порівнювати різні варіанти архітектурних рішень [7].

Ключова перевага впровадження методики SSM-CR полягає в її високій гнучкості та адаптивності, оскільки вона завжди враховує конкретну систему, загрози та пріоритети. Він поєднує якісні експертні судження з можливістю кількісного розрахунку відносного балу стійкості, забезпечує чітку прослідковуваність від прогалин до можливих архітектурних покращень і добре підходить для інженерного аналізу складних систем та порівняння альтернативних варіантів підвищення кіберстійкості.

Поряд із цим, практичне застосування SSM-CR супроводжується певними обмеженнями. Зокрема, цей метод вимагає значної експертної підготовки, участі зацікавлених сторін і часу на адаптацію фреймворку під конкретний контекст, що робить його менш зручним для швидкої самооцінки. Оцінки залишаються частково суб’єктивними через експертні судження, а результати є відносними, тому їх складно безпосередньо порівнювати між різними організаціями без урахування контексту.

1.1.3 Матричний метод аналізу операційної стійкості Resilience Matrix

Матричний метод Resilience Matrix, запропонований Ігорем Лінковом, поєднує фази кіберстійкості (Plan & Prepare, Detect/Absorb, Recover, Adapt) з

чотирма доменами (Physical, Information, Cognitive, Social). У результаті утворюється матриця, заповнена метриками, які оцінюються через опитування експертів або самооцінку. Метод дозволяє цілісний аналіз стійкості системи на різних рівнях і добре інтегрується з іншими фреймворками, такими як NIST Cybersecurity Framework [8].

Головна перевага використання Resilience Matrix полягає в тому, що цей підхід забезпечує комплексне, міждисциплінарне бачення кіберстійкості, враховуючи не лише технічні, а й організаційні, когнітивні та соціальні аспекти. Метод зручний для стратегічного порівняння між різними секторами чи організаціями і допомагає візуально виявляти слабкі зони в матриці. Він також сприяє системному мисленню при плануванні заходів підвищення стійкості.

Проте методу притаманна суб’єктивність через експертний підхід, а відсутність чітких математичних формул і великі затрати часу на збір даних ускладнюють його повторюваність у динамічних умовах.

1.2 Аналіз атак на критичну інфраструктуру

1.2.1 Дослідження інциденту із застосуванням спеціалізованого ШПЗ FrostyGoop

У січні 2024 року було зафіксовано масштабну кібератаку на комунальне енергетичне підприємство у місті Львів. Внаслідок інциденту понад 600 багатоквартирних будинків на два дні залишилися без централізованого опалення в зимовий період. Атака була здійснена із застосуванням нового типу шкідливого програмного забезпечення, яке отримало назву FrostyGoop.

Особливістю FrostyGoop є те, що це перше ICS-специфічне ШПЗ, яке використовує протокол Modbus для безпосередньої взаємодії з контролерами в операційному середовищі. Зловмисники надсилали Modbus-команди на

контролери ENCO, що призвело до спотворення вимірювальних даних і неправильної роботи системи опалення. Важливою технічною деталлю є те, що зловмисники відкотили версію прошивки контролерів до версії, яка не мала необхідних механізмів моніторингу. Це дозволило їм уникнути виявлення під час атаки [9].

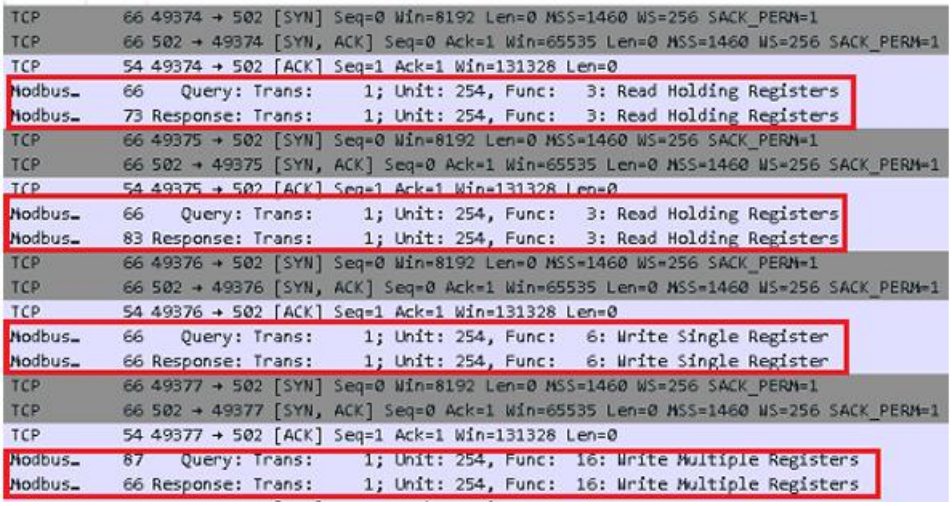

Рисунок 1.2 – Приклад мережевого трафіку FrostyGoop [9]

Розслідування, проведене CERT-UA спільно з компанією Dragos, виявило, що початковим вектором проникнення стала вразливість у зовнішньому маршрутизаторі Mikrotik. Критичним фактором, що сприяв успіху атаки, стала недостатня сегментація мережі. Маршрутизатор, сервери управління та контролери системи опалення перебували в одному сегменті, що дозволило шкідливому програмному забезпеченню поширюватися горизонтально.

1.2.2 Кампанія угруповання Sandworm (UAC-0133) проти підприємств життєзабезпечення

У березні 2024 року CERT-UA виявила та заблокувала масштабну зловмисну кампанію, спрямовану на порушення стабільного функціонування інформаційно-комунікаційних систем близько 20 підприємств енергетичної,

водопровідної та теплопостачальної галузей у 10 регіонах України. Атака була спланована з метою підсилення впливу ракетних ударів по критичній інфраструктурі України у весняний період 2024 року [10].

Кампанія була атрибутована угрупованню UAC-0133, яке з високим рівнем впевненості пов’язується з діяльністю російського державного угруповання Sandworm (APT44). Зловмисники застосували тактики атак на ланцюги постачання, отримавши первинний доступ через компрометацію щонайменше трьох постачальників послуг, які мали технічні можливості для віддаленого обслуговування систем критичної інфраструктури.

Технічний арсенал атакуючих включав як відоме, так і нове шкідливе програмне забезпечення. На Linux-системах використовувалися бекдори, а також нові інструменти, призначені для управління технологічними процесами через спеціалізоване ПЗ. На Windows-системах застосовувалися засоби для створення проксі та тунелювання мережевого трафіку. Особливістю одного з інструментів стало його розгортання у вигляді зашифрованого файлу, прив’язаного до конкретного сервера, що ускладнювало виявлення. Додатково застосовувалися засоби для приховування активності в системі.

Ключовими факторами, що сприяли успішності атак, стали недостатня сегментація мереж, що дозволяла доступ між системами постачальників та організаційними мережами, а також недбалість постачальників у забезпеченні належної безпеки програмного забезпечення

1.2.3 Кібератаки субкластера Sandworm (UAC-0212) на розробників та постачальників рішень АСКТП

Окремою масштабною кампанією, що тривала з липня 2024 року по лютий 2025 року, стала діяльність угруповання UAC-0212, яке є субкластером

Sandworm (APT44). Ця кампанія була спрямована на постачальників та інтеграторів автоматизованих систем комерційного та технологічного обліку – ключових елементів управління технологічними процесами в енергетиці [11].

За даними CERT-UA, від початку січня до 20 лютого 2025 року було задокументовано кібератаки щонайменше на 25 українських підприємств, які займаються розробкою систем управління технологічними процесами та виконанням електромонтажних робіт . Ці підприємства обслуговують сотні українських компаній у сферах енергозабезпечення, теплопостачання та водовідведення [11].

Тактика атакуючих базувалася на соціальній інженерії: зловмисники представлялися потенційними замовниками, вели тривалу переписку та надсилали PDF-файли зі шкідливим вмістом під приводом ознайомлення з технічною документацією. Після активації шкідливого файлу відбувалося закріплення в системі та горизонтальне переміщення мережею. CERT-UA зазначає, що просте виявлення та «перевірка антивірусом» ураженого комп’ютера не вирішує проблеми, оскільки зловмисники протягом кількох годин здійснюють горизонтальне переміщення на серверне та мережеве обладнання [11

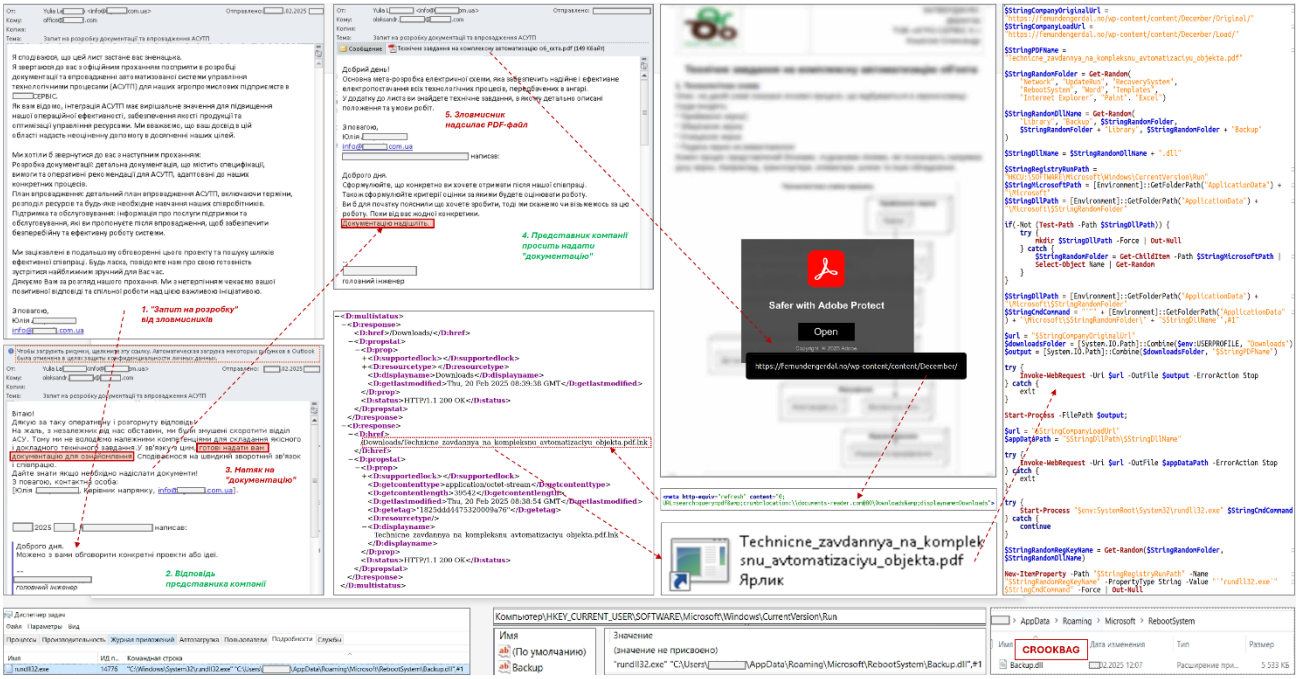

Рисунок 1.3 – Приклад ланцюга ураження [11]

Висновки до розділу 1

Проведений у першому розділі аналіз сучасних методів оцінки кіберстійкості та кібератак на критичну інфраструктуру дозволяє зробити висновок, що традиційний підхід, орієнтований виключно на кібербезпеку, є недостатнім для захисту об’єктів критичної інфраструктури. Сучасні кібератаки стають більш складними, цілеспрямованими та руйнівними, про що свідчать проаналізовані інциденти, які призводили до тривалих порушень у роботі енергетичних об’єктів. У цих умовах абсолютний захист є недосяжним, тому на перший план виходить здатність системи виконувати свої функції навіть в умовах успішної атаки.

Розглянуті методи оцінки кіберстійкості, незважаючи на їхні переваги, мають суттєві обмеження. Вони значною мірою базуються на суб’єктивних експертних судженнях, зосереджені переважно на оцінці організаційних процесів

і не дозволяють отримати об’єктивні кількісні показники, які можна було б порівнювати між різними об’єктами. Крім того, ці методи недостатньо враховують специфіку сучасних загроз, зокрема атаки на ланцюги постачання та наслідки недостатньої сегментації мереж. Таким чином, існує потреба в розробленні нового механізму оцінювання кіберстійкості, який би ґрунтувався на об’єктивних технічних параметрах мережевої архітектури та дозволяв кількісно оцінювати рівень стійкості об’єкта до сучасних кіберзагроз [12].

Для узагальнення розглянутих методів наведено порівняльну таблицю 1.1.

Таблиця 1.1 – Порівняльна характеристика

Метод	**Тип методу**	**Базова модель**	**Шкала оцінювання**	**Структура**
CRR	Якісний	CERT-RMM	0-3	10 доменів
SMM-CR	Напівкількісний	CREF	0-5	4 стратегічні цілі
Resilience Matrix	Якісний	Linkov model	Немає стандарту	4 фази х 4 домени

2 ПОБУДОВА МОДЕЛІ МЕРЕЖІ ЕНЕРГЕТИЧНОГО ОБ'ЄКТА

2.1 Архітектура мережі енергетичного об'єкта

Для проведення симуляції кібератак та оцінки кіберстійкості інфраструктурного енергетичного об'єкта в рамках дипломної роботи було розроблено спрощену модель мережі розподільчої підстанції. Модель відображає типову архітектуру сучасних розподільчих підстанцій, що використовуються в енергетичних системах України, з урахуванням основних компонентів системи SCADA.

External Firewall – це пристрій периметрового захисту, який розташований на межі між зовнішньою мережею та внутрішньою мережею організації. Він виконує фільтрацію всього вхідного та вихідного трафіку, застосовує правила доступу, NAT та забезпечує перший рівень сегментації мережі.

Web-server – це сервер, який надає веб-послуги та може бути доступним з мережі Інтернет. У моделі він розташований у DMZ, що дозволяє зовнішнім користувачам отримувати доступ до веб-ресурсів організації без прямого доступу до внутрішньої мережі.

DNS Server – це сервер доменних імен, який перетворює доменні імена в IP-адреси. Він розташований у DMZ, що дозволяє зовнішнім клієнтам розв'язувати доменні імена організації без доступу до внутрішньої мережі.

Internal Firewall – це другий міжмережевий екран, який розділяє DMZ та внутрішню мережу. Він забезпечує додатковий рівень захисту, контролюючи трафік між DMZ та внутрішніми ресурсами.

Switch – це мережевий комутатор, який забезпечує комунікацію між пристроями в межах мережі. Для додаткової сегментації може підтримувати VLAN.

Workstation – це робоча станція корпоративної мережі, яка використовується офісними працівниками для виконання повсякденних завдань. Вона є типовою ціллю для фішингових атак та може бути початковим вектором проникнення.

AD Server – це сервер, що забезпечує централізоване керування обліковими записами користувачів, їхніми правами доступу та політиками безпеки в корпоративній мережі.

Application Server – це сервер, на якому виконуються бізнес-додатки, що не впливають безпосередньо на технологічний процес, але необхідні для роботи підприємства.

HMI – це робоче місце оператора-диспетчера, яке забезпечує візуалізацію технологічного процесу у вигляді мнемосхем, графіків та індикаторів. Через HMI оператор віддає команди на керування обладнанням.

HDS – це сервер архівації та довгострокового зберігання історії технологічних параметрів. Він накопичує дані від SCADA-системи, контролерів та інших пристроїв управління, та зберігає їх у структурованому вигляді для подальшого аналізу, формування звітів, побудови трендів та розслідування аварійних ситуацій.

FEP – це спеціалізований шлюз, який виконує конвертацію промислових протоколів, буферизацію даних та розвантаження верхніх рівнів системи управління від низькорівневого опитування польових пристроїв. Він перетворює промислові протоколи верхнього рівня на польові протоколи для зв’язку з

контролерами та терміналами. Крім того, FEP накопичує дані при тимчасовій втраті зв’язку з верхніми рівнями та передає їх після відновлення з’єднання.

Remote Terminal Unit - це термінали, які безпосередньо підключаються до первинного обладнання підстанції. Вони збирають телеметрію, виконують локальну автоматику та передають дані. RTU отримують команди від оператора, змінюють стан виконавчих механізмів та повертають актуальні показники датчиків.

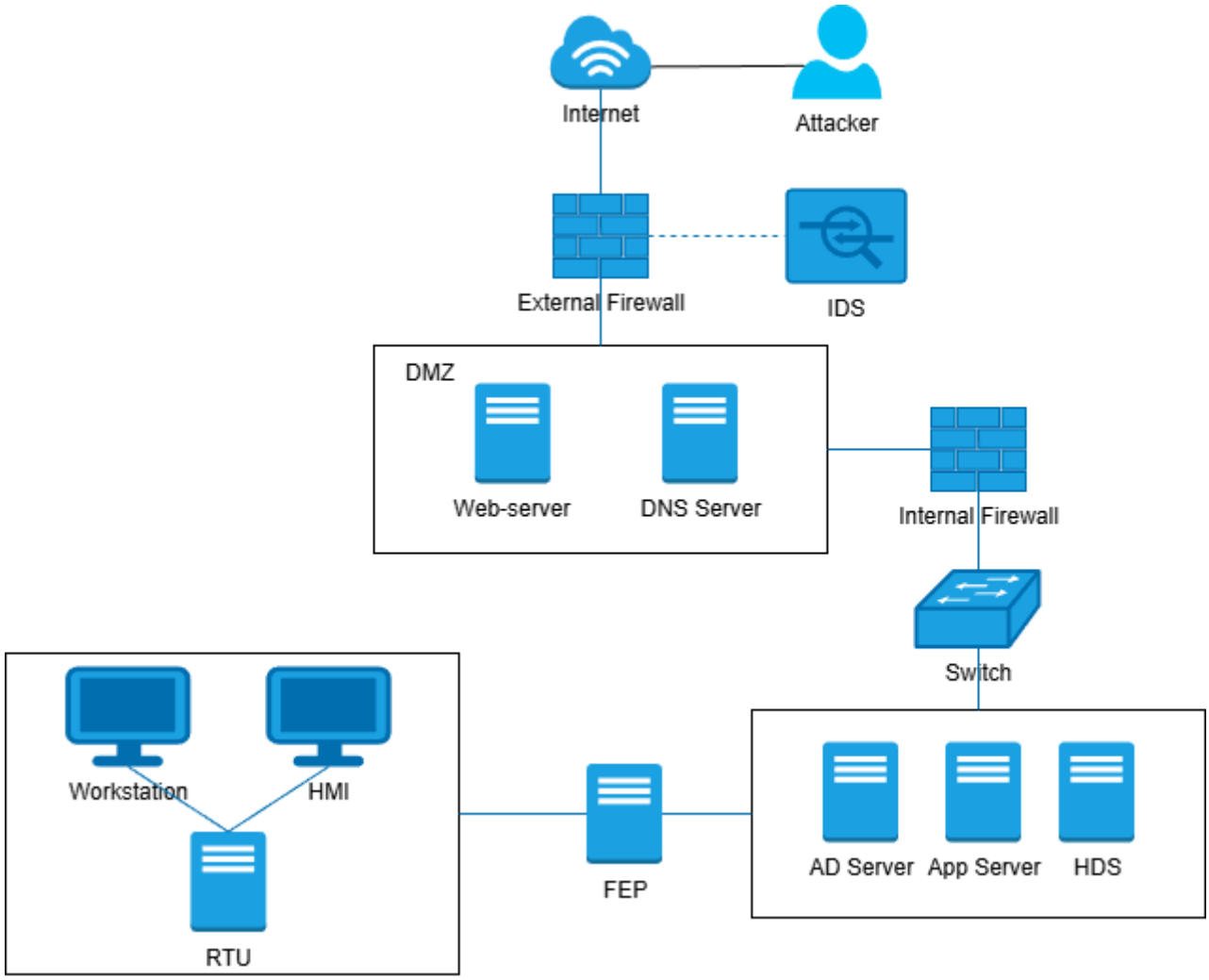

Рисунок 2.1 – Схема IT-мережі енергетичного об’єкта

2.2 Використання GNS3 для побудови моделі

Для створення імітаційної моделі мережі енергетичного об’єкта та проведення симуляції кібератак було обрано програмне середовище мережевої емуляції GNS3 [13]. Даний вибір обумовлений технологічною гнучкістю платформи, яка дозволяє комбінувати емуляцію реальних операційних систем мережевого обладнання з повноцінною віртуалізацією кінцевих вузлів на базі гіпервізорів QEMU та Docker. Це дозволяє максимально наблизити архітектуру імітаційної моделі до реальних умов експлуатації об’єктів критичної інфраструктури, враховуючи специфіку мережевих стеків та особливості взаємодії промислових протоколів.

Особлива увага при проектуванні середовища була приділена питанню обчислювальних ресурсів, оскільки одночасний запуск великої кількості віртуальних машин створює значне навантаження на апаратну частину. У зв’язку з цим, розгортання імітаційного стенда було виконано з використанням хмарної інфраструктури, що забезпечило необхідний рівень продуктивності, масштабованості та відмовостійкості. Основний обчислювальний вузол GNS3 Server було розгорнуто на базі платформи GCP з використанням спеціалізованого інстансу типу n2-standard-8 (8 vCPU, 32 ГБ RAM).

Використання хмарних потужностей дозволило винести процеси віртуалізації за межі локальної робочої станції, забезпечуючи стабільну роботу моделі навіть при симуляції інтенсивного мережевого трафіку або проведенні ресурсоємних процедур сканування вразливостей. Безпека керування хмарним сервером була забезпечена шляхом створення захищеного тунелю між локальним клієнтом GNS3 та інстансом у GCP, що дозволило здійснювати конфігурацію вузлів та моніторинг стану мережі в режимі реального часу без ризику несанкціонованого доступу до середовища моделювання.

Важливим аспектом налаштування імітаційної моделі стала детальна конфігурація кожного мережевого інтерфейсу та системних параметрів вузлів для відповідності архітектурі розподільчої підстанції. Це включало в себе налаштування статичної маршрутизації, правил міжмережевого екранування та розподіл IP-адресації згідно з розробленим планом сегментації. Повний перелік системних характеристик можна побачити в Таблиці 2.1

Таблиця 2.1 – Перелік компонентів імітаційної моделі

Компонент	**Операційна система**	**IP-адреса**
Attacker	Kali Linux 2026.1	192.168.122.163
External Firewall	pfSense 2.8.1	WAN: 192.168.122.147 LAN: 10.0.1.1
Internal Firewall	pfSense 2.8.1	WAN: 10.0.1.2 LAN: 10.0.2.1
Web-Server	Debian 12	10.0.1.10
DNS Server	Debian 12	10.0.1.11
App Server	Debian 12	10.0.2.10
HDS	Debian 12	10.0.2.11
AD Server	Windows Server 2022	10.0.2.13
FEP	Debian 12	Internal: 10.0.2.100 SCADA: 10.0.3.1
Workstation	Windows 11	10.0.3.10
HMI	Windows 11	10.0.3.11
RTU	Debian 12	10.0.3.12

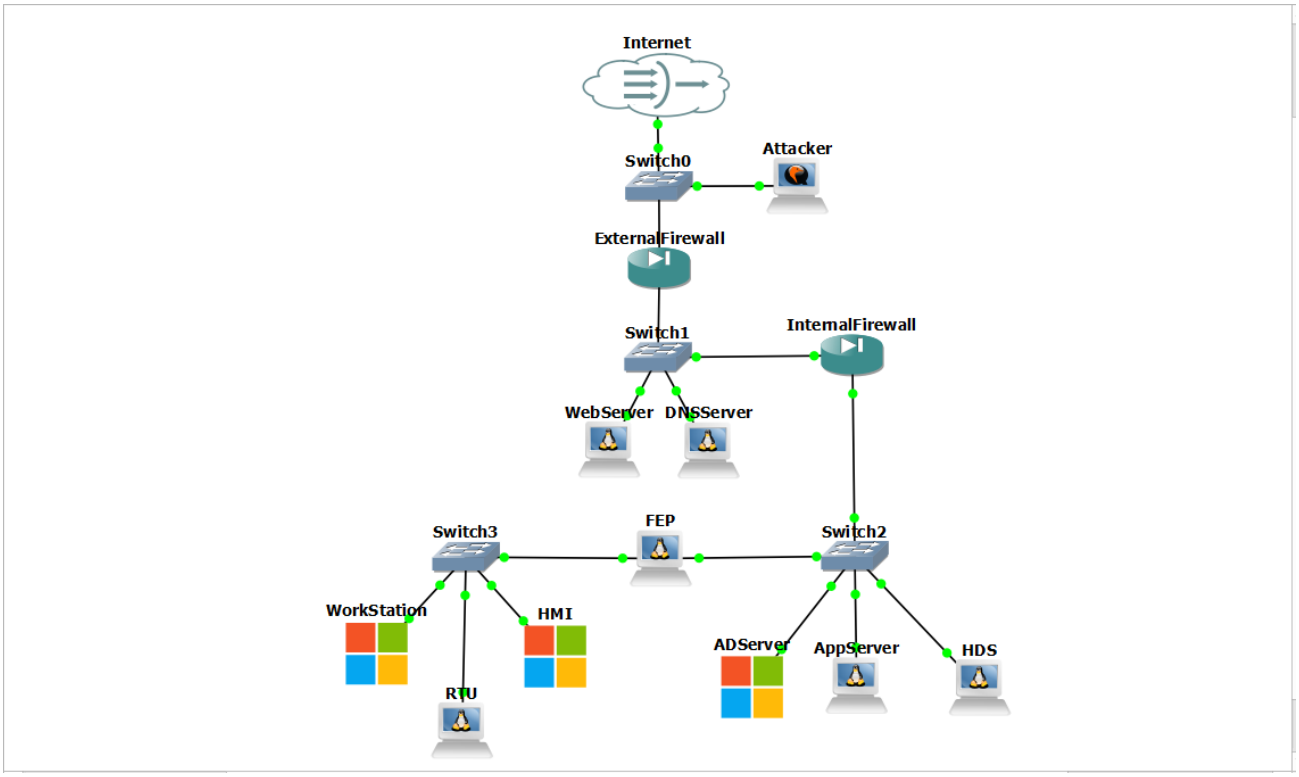

Рисунок 2.2 – Топологія імітаційної моделі в середовищі GNS3

Як можна побачити на рисунку 2.2, архітектура імітаційної моделі побудована за принципом ешелонованого захисту та розділена на три чітко ізольовані сегменти, що дозволяє симулювати реальні умови функціонування об’єкта критичної інфраструктури. Зовнішній периметр моделі представлений мережею загального доступу, де розміщено вузол атакуючої сторони на базі Kali Linux. Цей сегмент відокремлений від внутрішніх ресурсів зовнішнім міжмережевим екраном External Firewall, який виконує роль першого бар’єра та контролює трафік між зовнішнім середовищем і демілітаризованою зоною, де функціонують публічні сервіси, такі як Web-Server та DNS.

Наступний рівень інфраструктури складає корпоративний сегмент, що об’єднує підмережі для управління базами даних та системними додатками. Тут розташовані критично важливі для бізнес-логіки вузли, зокрема App Server, HDS та AD Server. Зв’язок у цій зоні жорстко регламентується правилами

внутрішнього міжмережевого екрана Internal Firewall, що перешкоджає вільному розповсюдженню потенційних загроз у напрямку технологічної мережі. Особливе місце в цій структурі посідає комунікаційний сервер FEP, який має два мережеві інтерфейси та виступає в ролі шлюзу між IT-інфраструктурою та операційним середовищем.

Найбільш захищеним сегментом моделі є технологічна мережа SCADA, яка повністю ізольована від прямих зовнішніх підключень. У цій зоні зосереджено кінцеві елементи автоматизації та управління, такі як інженерна станція Workstation, людино-машинний інтерфейс HMI та віддалений термінал керування RTU. Така багаторівнева побудова мережі дозволяє детально проаналізувати механізми реалізації складних багатовекторних атак, оцінити ефективність налаштованих правил фільтрації на кожному етапі просування зловмисника та дослідити загальну стійкість технологічного процесу до кібератак.

2.3 Аналіз потенційних векторів атак на основі бази вразливостей CVE та метрик CVSS

Оцінювання кіберстійкості енергетичного об’єкта потребує детального розгляду конкретних технічних недоліків програмного забезпечення, які зловмисник може використати для просування вглиб технологічної мережі. Для систематизації цих загроз у роботі використано базу CVE – міжнародний стандарт ідентифікації вразливостей. Кожен запис у цьому реєстрі містить унікальний ідентифікатор, що дозволяє точно зіставити компоненти розробленої моделі із реальними загрозами, зафіксованими в індустрії.

Для кількісного вимірювання критичності виявлених недоліків застосовується система CVSS. Вона дозволяє трансформувати якісні характеристики вразливості у числове значення від 0 до 10 [14, 15]. Розрахунок

бала базується на аналізі вектора доступу, складності експлуатації та необхідного рівня привілеїв, що дозволяє об’єктивно оцінити потенційний вплив на конфіденційність, цілісність та доступність даних у кожному сегменті мережі.

На першому етапі атаки основним вектором є компрометація зовнішнього периметра через вразливості веб-сервісів. У даній роботі для моделювання цього етапу використано вразливість CVE-2023-35078 (CVSS 9,8) – критична помилка обходу автентифікації в Ivanti Endpoint Manager Mobile, яка дозволяє неавторизованому зловмиснику звертатись до захищених API-шляхів без жодних облікових даних. Практична небезпека цієї вразливості підтверджена реальними інцидентами: за даними CISA, вона активно експлуатувалась у цільових атаках на урядові мережі. Наявність подібної вразливості на зовнішньому шлюзі означає, що початковий етап проникнення може відбутися практично миттєво, без необхідності складної підготовки.

Після успішного закріплення на Web-сервері зловмисник переходить до горизонтального переміщення у корпоративний сегмент. Для цього етапу використано вразливість CVE-2021-3493 (CVSS 7,8) – підвищення привілеїв через некоректну перевірку файлових можливостей у реалізації OverlayFS ядра Linux на системах Ubuntu. Вразливість дозволяє локальному зловмиснику з мінімальними привілеями отримати права суперкористувача, що є необхідною умовою для встановлення агента Caldera та подальшого просування мережею. Ефективність сегментації безпосередньо впливає на цей етап: навіть за наявності вразливості, відсутність прямих мережевих маршрутів між сегментами змушує зловмисника витрачати значно більше часу на пошук обхідних шляхів.

Завершальна стадія атаки, а саме досягнення технологічного шлюзу FEP, у третьому сценарії реалізується через зловживання механізмом переадресації портів SSH. Для цього використано вразливість CVE-2023-38408 (CVSS 9,8) – критична помилка у компоненті ssh-agent OpenSSH, яка дозволяє зловмиснику,

що вже контролює проміжний вузол, виконувати довільний код через маніпуляцію з агентом переадресації та завантаженням бібліотек PKCS#11. Це дає можливість встановити тунель між HDS та FEP, маскуючи зловмисний трафік під легітимний технологічний обмін даними. Впровадження суворої політики мінімальних привілеїв та заборона безпарольної автентифікації ускладнюють, але не унеможливлюють цей вектор, оскільки вразливість закладена в самому механізмі переадресації агента.

Таким чином, використання метрик CVSS дозволяє трансформувати технічні параметри виявлених вразливостей у конкретні числові дані, що характеризують складність та швидкість реалізації атак. Чим вищий базовий бал CVSS та чим нижча складність експлуатації, тим вищою є ймовірність успішного подолання відповідного захисного бар’єру в заданий проміжок часу. Ця кількісна основа є необхідною для подальшого аналізу динаміки розвитку інцидентів та параметризації математичної моделі у четвертому розділі.

Висновки до розділу 2

У межах другого розділу було розроблено та обґрунтовано архітектуру імітаційної моделі мережі розподільчої підстанції. Модель базується на принципах ешелонованого захисту та включає три ізольовані сегменти: демілітаризовану зону, корпоративну мережу та технологічний сегмент SCADA. Такий підхід дозволяє відтворити специфіку реальних об’єктів критичної інфраструктури та забезпечує необхідні умови для моделювання складних векторів атак.

Технічна частина моделі реалізована в GNS3 з використанням хмарних потужностей GCP, що дало змогу стабільно запустити 12 віртуальних машин. Завдяки професійним інструментам фільтрації трафіку та емуляції промислових

шлюзів, модель максимально точно відтворює обмін даними між корпоративними та технологічним рівнями підстанції.

Створена модель є повноцінним середовищем для перевірки кіберстійкості в реальних умовах. Чіткий поділ на зони та наявність окремого вузла атаки дозволяють наочно оцінити роботу міжмережевих екранів і виявити слабкі місця в захисті енергетичного об’єкта при спробах зовнішнього та внутрішнього зламу.

3 СИМУЛЯЦІЯ КІБЕРАТАКИ НА МЕРЕЖУ ОБ'ЄКТА

3.1 MITRE Caldera

Для проведення об'єктивного тестування кіберстійкості розробленої моделі мережі було впроваджено платформу MITRE Caldera, яка є сучасним інструментом для автоматизації симуляції дій зловмисника. Вибір даного фреймворку обумовлений його глибокою інтеграцією з базою знань MITRE ATT&CK, що дозволяє моделювати складні багатоетапні атаки у контрольованому середовищі. На відміну від традиційних сканерів вразливостей, Caldera імітує реальну поведінку порушника, поєднуючи окремі технічні дії у логічні ланцюжки, що дозволяє оцінити не лише наявність вразливостей, а й здатність засобів захисту протидіяти динамічному просуванню зловмисника всередину периметра.

Архітектура симуляційного стенда базується на взаємодії C2 сервера, розгорнутого на вузлі Attacker, та агентів Sandcat. Серверна частина відповідає за координацію операцій, збереження бази «фактів», отриманих під час розвідки, та прийняття рішень щодо наступних кроків атаки на основі доступних інструментів. Агенти, у свою чергу, виступають виконавцями команд у різних сегментах мережі, що дозволяє симулювати як зовнішні загрози, так і дії внутрішнього зловмисника або наслідки компрометації робочих станцій персоналу.

Процес симуляції реалізується через запуск спеціалізованих профілів, які складаються з послідовних технік і тактик. Кожна операція в Caldera є ітеративним процесом: система аналізує вихідні дані попередньої команди для автоматичного планування наступної дії. Наприклад, виявлення нових IP-адрес під час ARP-сканування автоматично розблоковує можливості для портового

сканування або спроб горизонтального переміщення. Такий підхід дозволяє виявити слабкі місця в конфігурації міжмережевих екранів pfSense, які можуть бути непомітними при статичному аналізі правил фільтрації.

Використання Caldera в межах даного дослідження дозволяє реалізувати порівняльний аналіз трьох різних сценаріїв захищеності об’єкта. Шляхом повторного запуску ідентичних сценаріїв атак на мережу з різними рівнями конфігурації безпеки – від відсутності обмежень до комплексного захисту – стає можливим кількісно оцінити ефективність впроваджених заходів. Це забезпечує можливість наочної демонстрації того, на якому саме етапі впроваджені засоби захисту стають критичною перешкодою для зловмисника, що є ключовим показником стійкості критичної інфраструктури.

3.2 Імітація кібератак

Для отримання кількісних та якісних показників кіберстійкості розробленої моделі, експериментальна частина розділена на три етапи, кожен з яких відповідає певному рівню зрілості системи захисту. Основною метрикою ефективності в кожному сценарії обрано здатність зловмисника досягти комунікаційного сервера FEP та час, витрачений на подолання встановлених бар’єрів. Вибір FEP як головної цілі обумовлений його роллю критичного технологічного шлюзу: захоплення цього вузла дозволяє порушити передачу даних між корпоративним та технологічним сегментами або здійснювати маніпуляцію командами управління.

З метою мінімізації похибки, для всіх випробувань зафіксовано єдину точку входу – зовнішній вузол Attacker – та незмінний набір інструментарію в межах обраного профілю Caldera. Це дозволяє ізолювати вплив мережевих конфігурацій на хід атаки. Кожен сценарій передбачає перевірку ефективності конкретних механізмів: від базової маршрутизації до аналізу трафіку системами

виявлення вторгнень. Нижче наведено детальну характеристику кожного рівня захищеності та результати їхнього тестування.

Перший етап дослідження присвячений оцінюванню базового рівня кіберстійкості мережі за умови відсутності сегментації. У межах цього сценарію міжмережеві екрани налаштовані таким чином, що пропускають будь-який трафік, виконуючи виключно роль маршрутизаторів між сегментами. Політики безпеки не передбачають жодної фільтрації пакетів між підмережами: дозволено весь трафік незалежно від протоколу, порту чи напрямку.

Така конфігурація створює умови, за яких зловмисник, подолавши зовнішній периметр, може безперешкодно переміщуватися між усіма сегментами мережі – від DMZ до корпоративної та технологічної зон. Відсутність логічної ізоляції дозволяє верифікувати гіпотезу про те, що недостатня сегментація є критичним фактором зниження кіберстійкості енергетичного об’єкта, оскільки внутрішній периметр залишається повністю відкритим для горизонтального переміщення атакуючого.

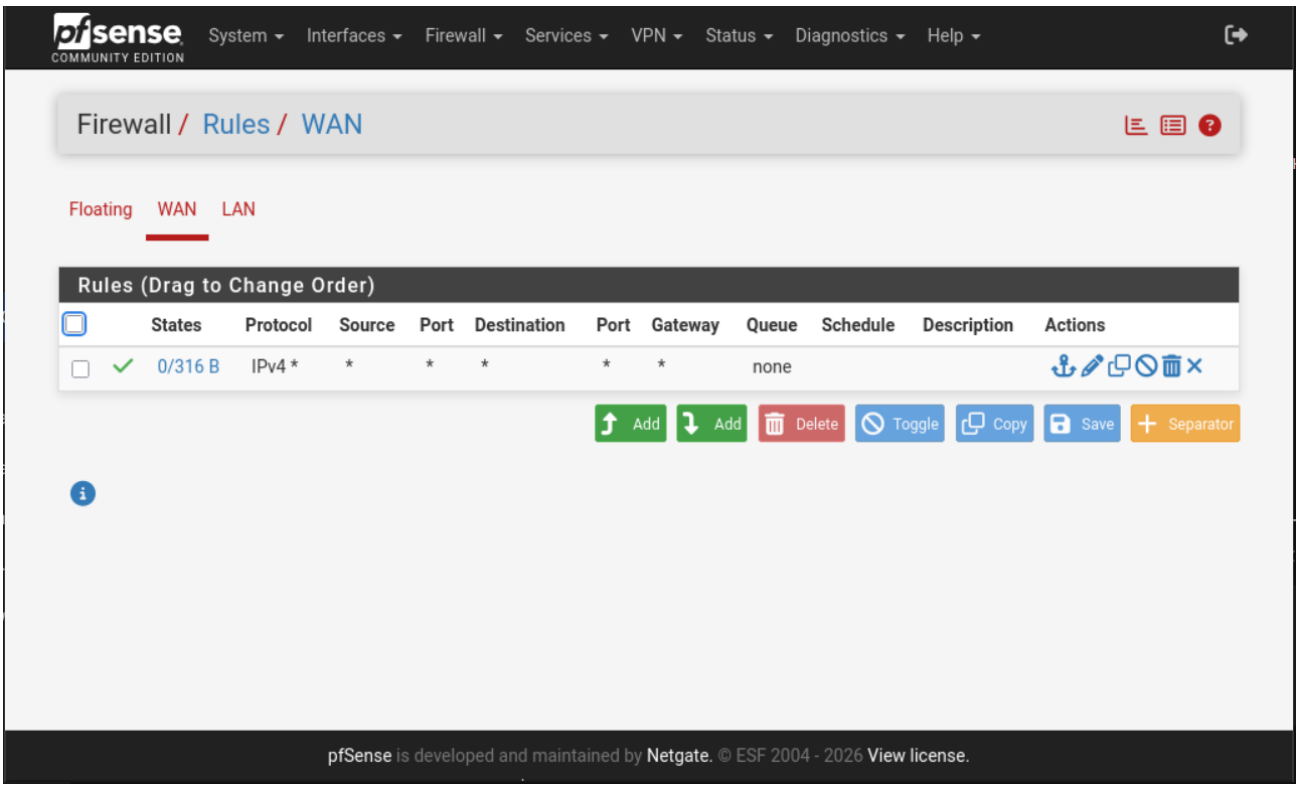

Рисунок 3.1 – Конфігурація міжмережевого екрану з дозволом будь-якого трафіку

Реалізація загрози розпочинається із зовнішнього периметра, де вузол Attacker імітує дії зловмисника в Інтернеті. Першим кроком є етап розвідки, під час якого проводиться сканування публічного адресного простору DMZ. За допомогою інструментарію Caldera зловмисник ідентифікує активний вузол Web-server та визначає відкриті сервіси, доступні для зовнішньої експлуатації.

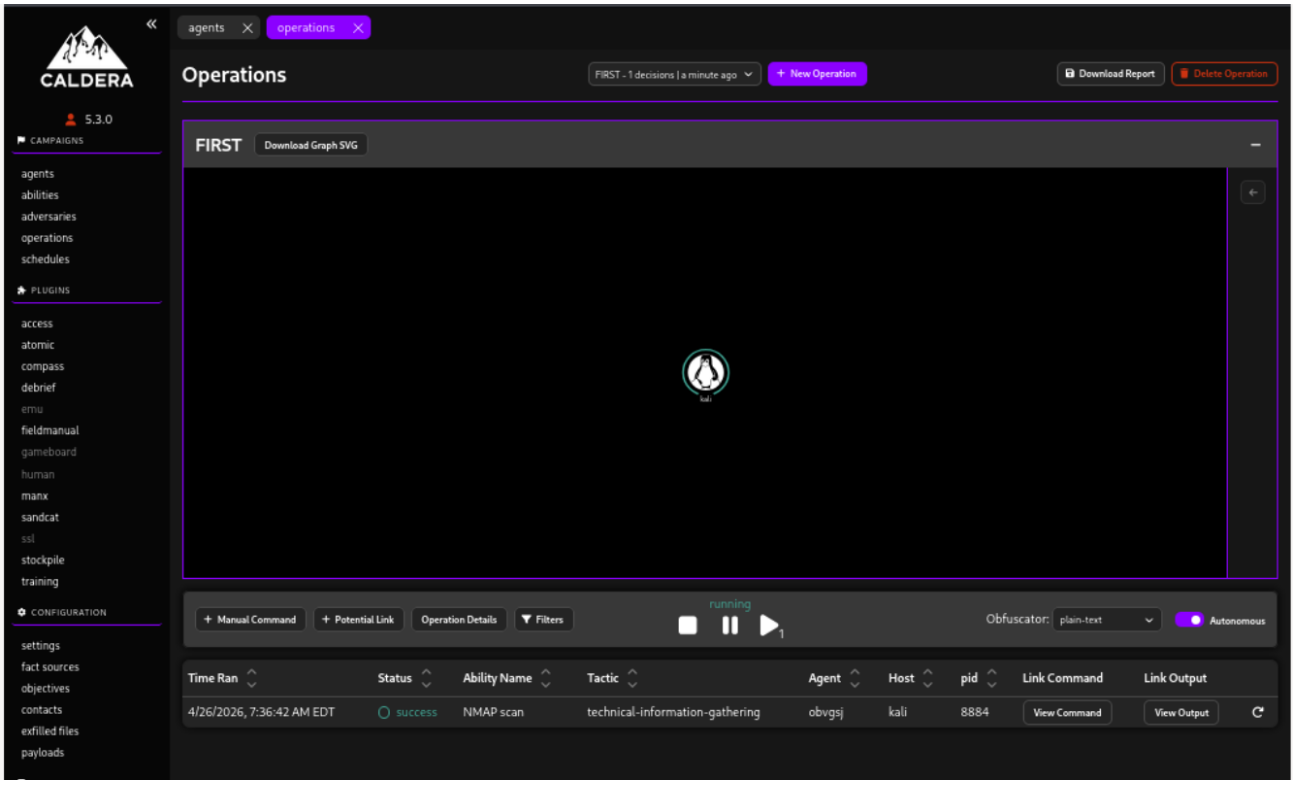

Рисунок 3.2 – Ідентифікація активних сервісів у сегменті DMZ з боку зовнішнього зловмисника

Виявивши вразливість у конфігурації сервісу віддаленого доступу або скориставшись скомпрометованими обліковими даними, атакуючий реалізує етап первинного проникнення. Платформа Caldera ініціює завантаження та запуск агента Sandcat на Web-server. Оскільки вхідний трафік на зовнішньому шлюзі не обмежений суворими політиками фільтрації, агент успішно встановлює зворотний зв’язок із сервером управління, що означає створення першого плацдарму всередині інфраструктури.

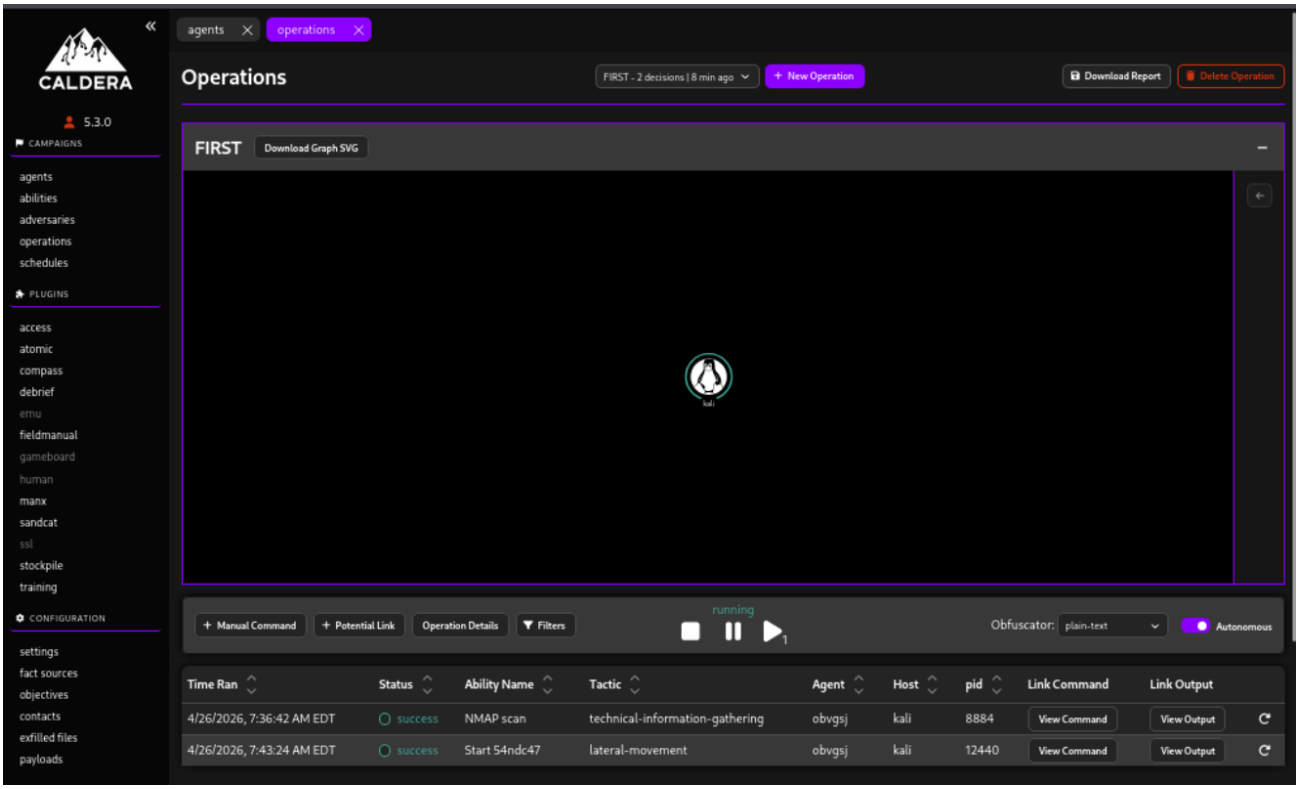

Рисунок 3.3 – Компрометація Web-Server

Отримавши контроль над Web-сервером, зловмисник використовує його як опорну точку для подальшого просування всередину мережі. Через відсутність сегментації між підмережами, атакуючий проводить сканування внутрішнього технологічного сегмента безпосередньо з захопленого вузла. В результаті виявляється цільовий об’єкт – комунікаційний сервер FEP, який у цій моделі виявляється повністю досяжним з DMZ.

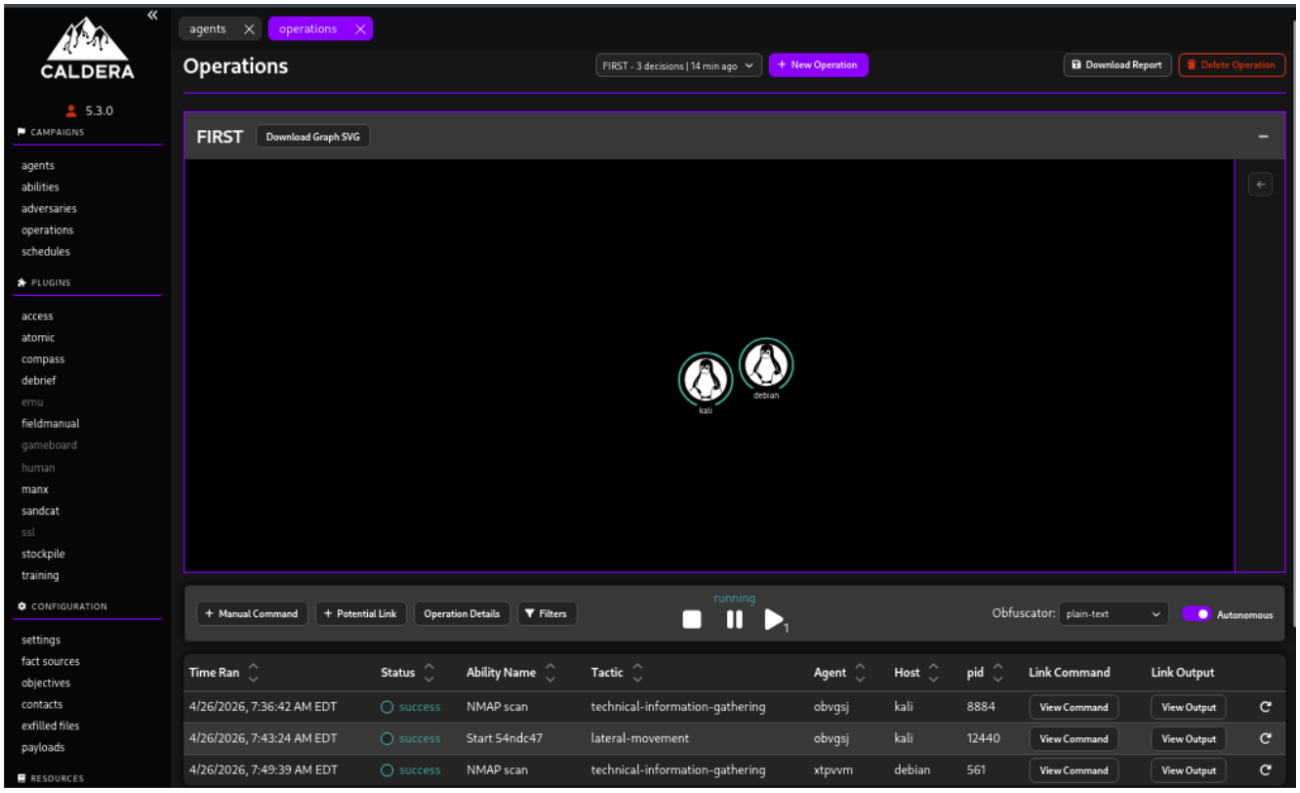

Рисунок 3.4 – Сканування внутрішньої мережі з скомпрометованого сервера

Завершальна стадія атаки полягає у прямому перенесенні активності на сервер FEP. Оскільки внутрішній екран пропускає будь-який трафік, зловмисник здійснює віддалений запуск агента на цільовому вузлі. Успішна реєстрація агента у системі Caldera підтверджує, що за відсутності сегментації зловмисник здатен досягти критичного технологічного рівня, зробивши лише один крок після прориву зовнішнього периметра.

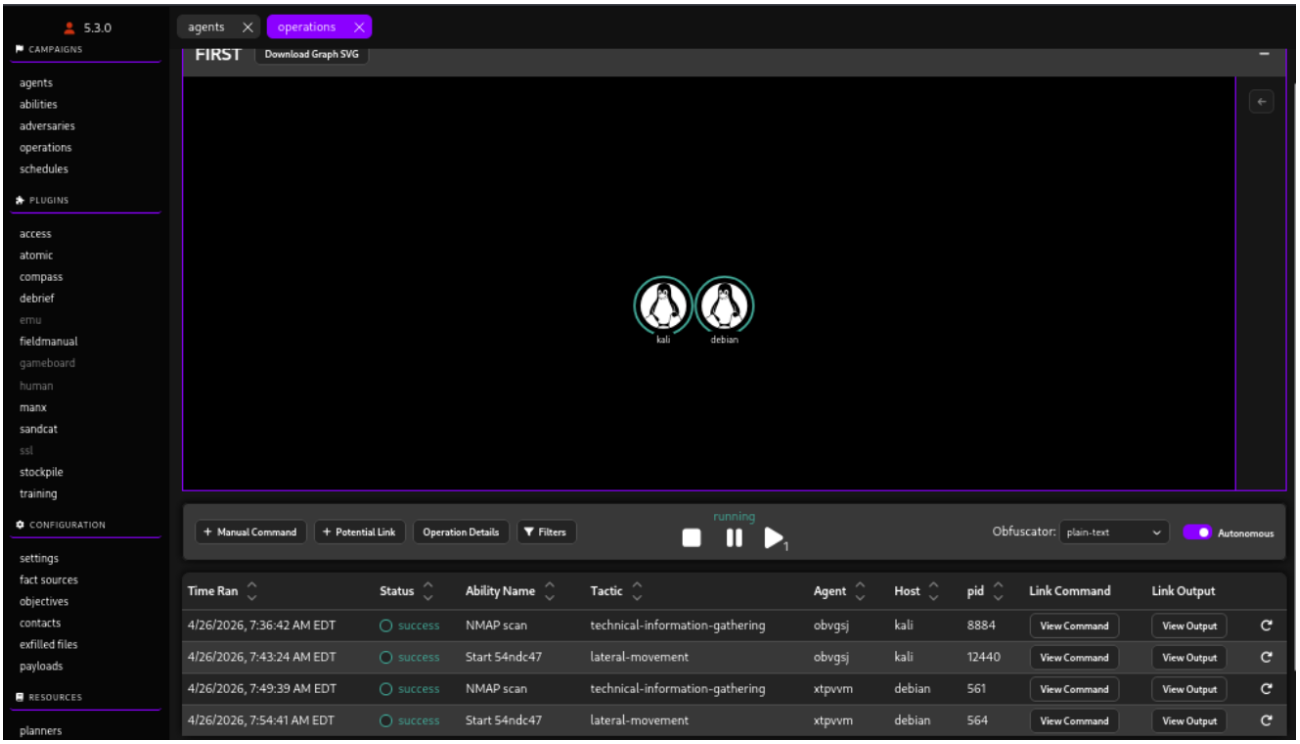

Рисунок 3.5 – Компрометація сервера FEP

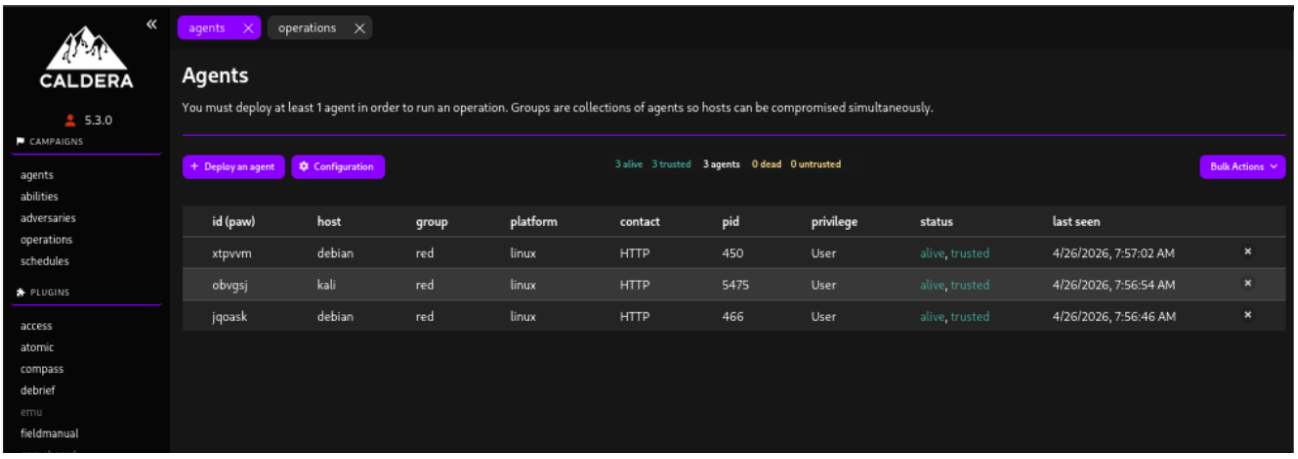

Рисунок 3.6 – Список агентів Caldera після завершення першої атаки

Другий етап дослідження спрямований на перевірку ефективності мережевої сегментації як бар’єра для прямого розповсюдження загроз. На відміну від попереднього сценарію, у конфігурацію міжмережевого екрана було внесено суворі обмеження: прямий зв’язок між сегментом DMZ та критичним

вузлом FEP було повністю заблоковано. Єдиним дозволеним маршрутом для Web-сервера залишився доступ до HDS.

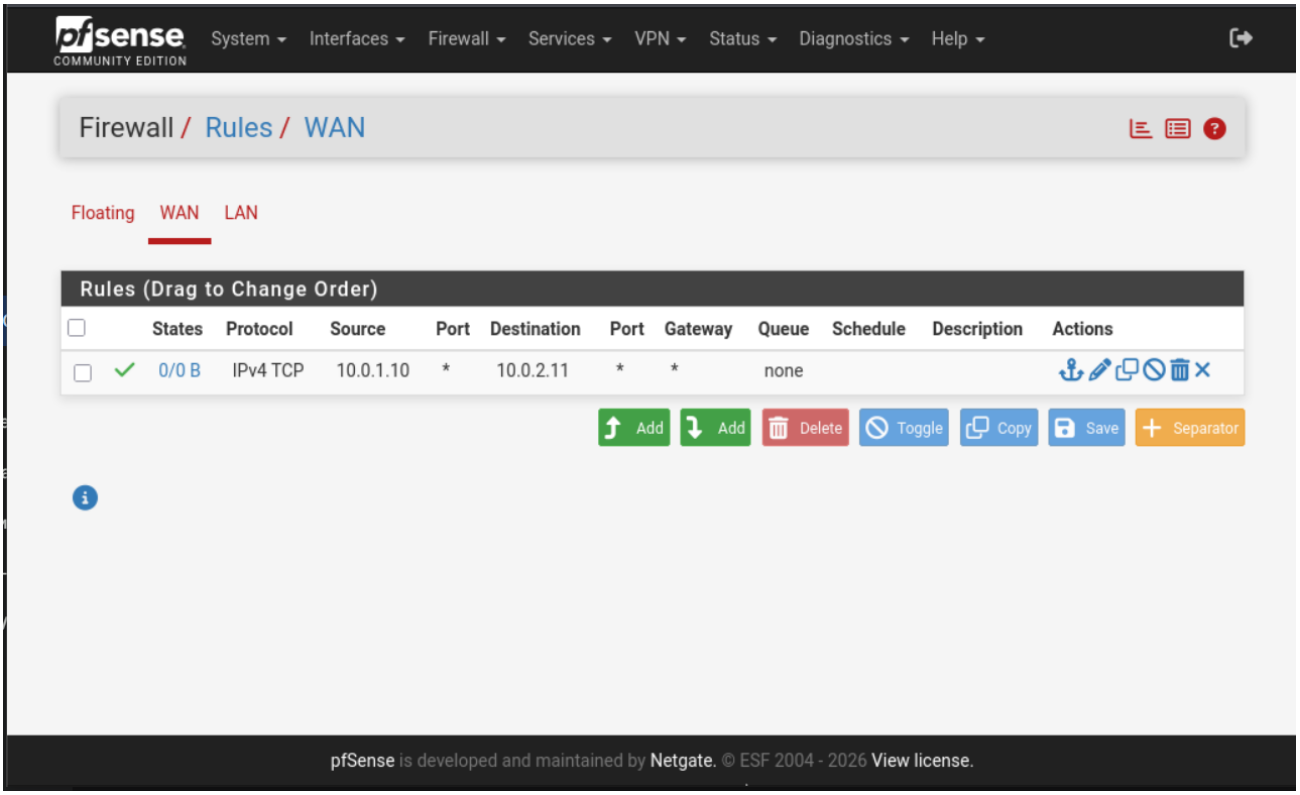

Рисунок 3.7 – Конфігурація міжмережевого екрану з обмеженим доступом

За таких умов пряма атака, реалізована на першому етапі, зазнає невдачі. Під час запуску операції в Caldera зловмисник виявляє, що цільовий вузол FEP більше не є досяжним безпосередньо з Web-сервера. Це змушує атакуючого використати проміжний вузел HDS як «трамплін» для подальшого просування всередину технологічної зони.

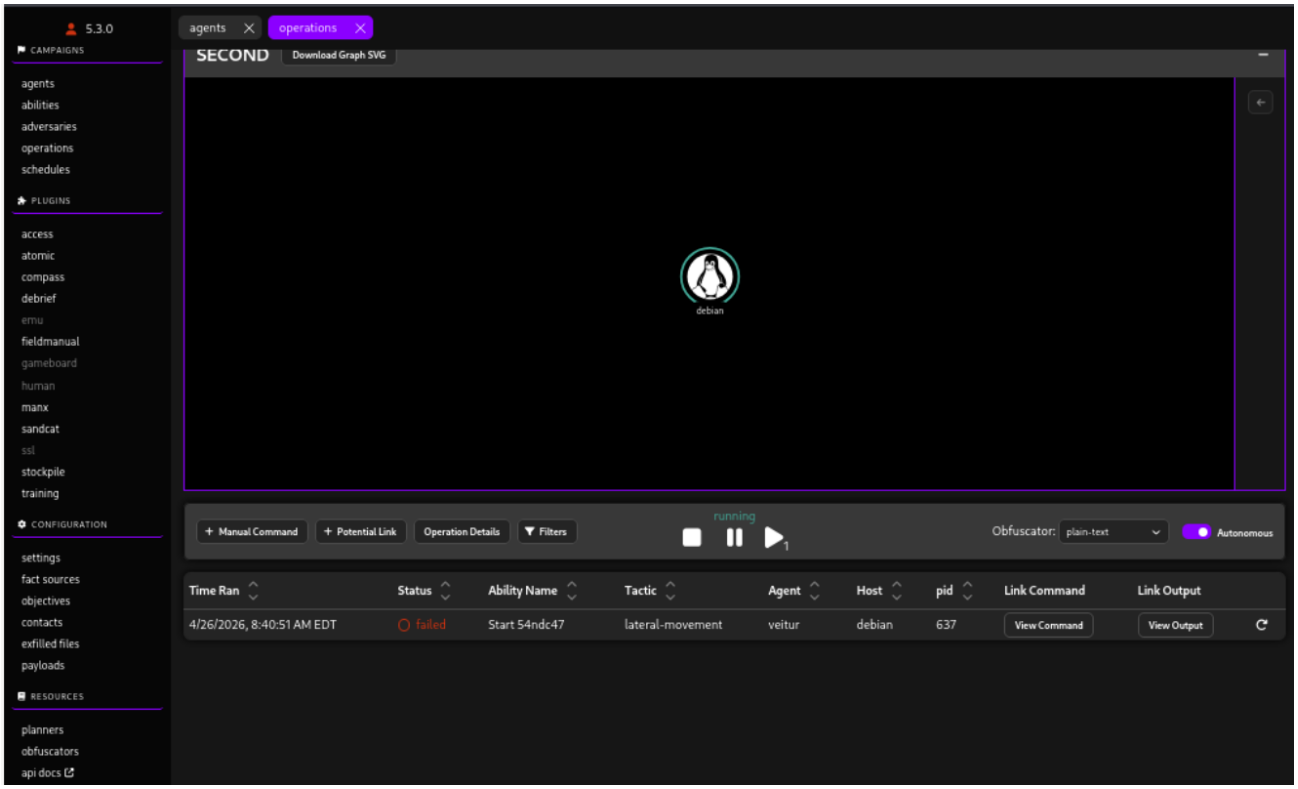

Рисунок 3.8 – Помилка передачі агента Sandcat на вузол FEP внаслідок блокування трафіку мережевим екраном

Успіх цього етапу базується на експлуатації довірчих відносин між серверами. Оскільки адміністративні процедури передбачають регулярний обмін даними між Web-сервером та HDS, атакуючий використовує заздалегідь налаштовані SSH-ключі для безпарольного доступу. Це дозволяє агенту Sandcat непомітно переміститися з одного сегмента в інший, маскуючись під легітимну активність системного адміністратора.

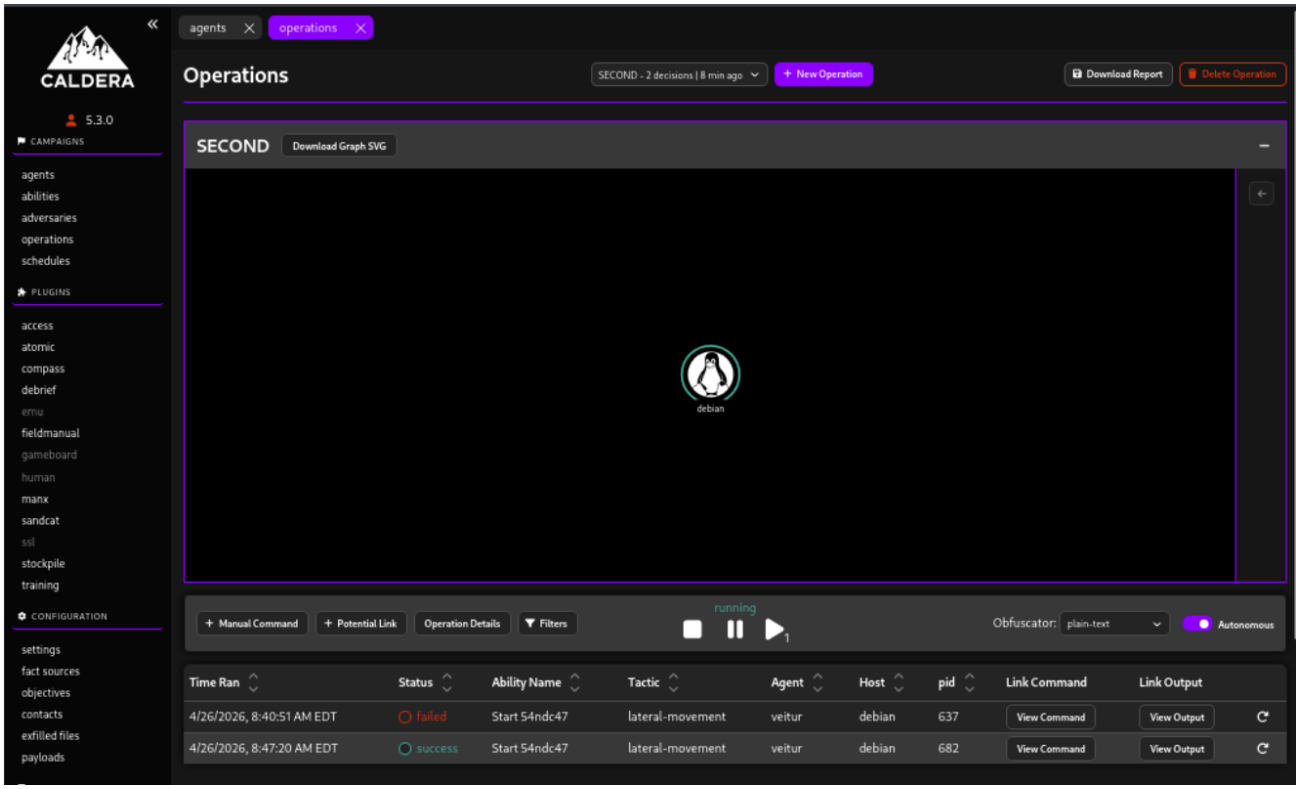

Рисунок 3.9 – Компрометація HDS

Внаслідок впровадження додаткових заходів безпеки спостерігається вимушена зміна траєкторії реалізації загрози: зловмисник змушений спочатку встановити контроль над HDS, який виконує роль довіреного вузла всередині інфраструктури. Лише після успішної компрометації цього проміжного хоста, атакуючий отримує можливість здійснити фінальний етап просування на сервер FEP, використовуючи легітимні маршрути доступу до технологічного рівня.

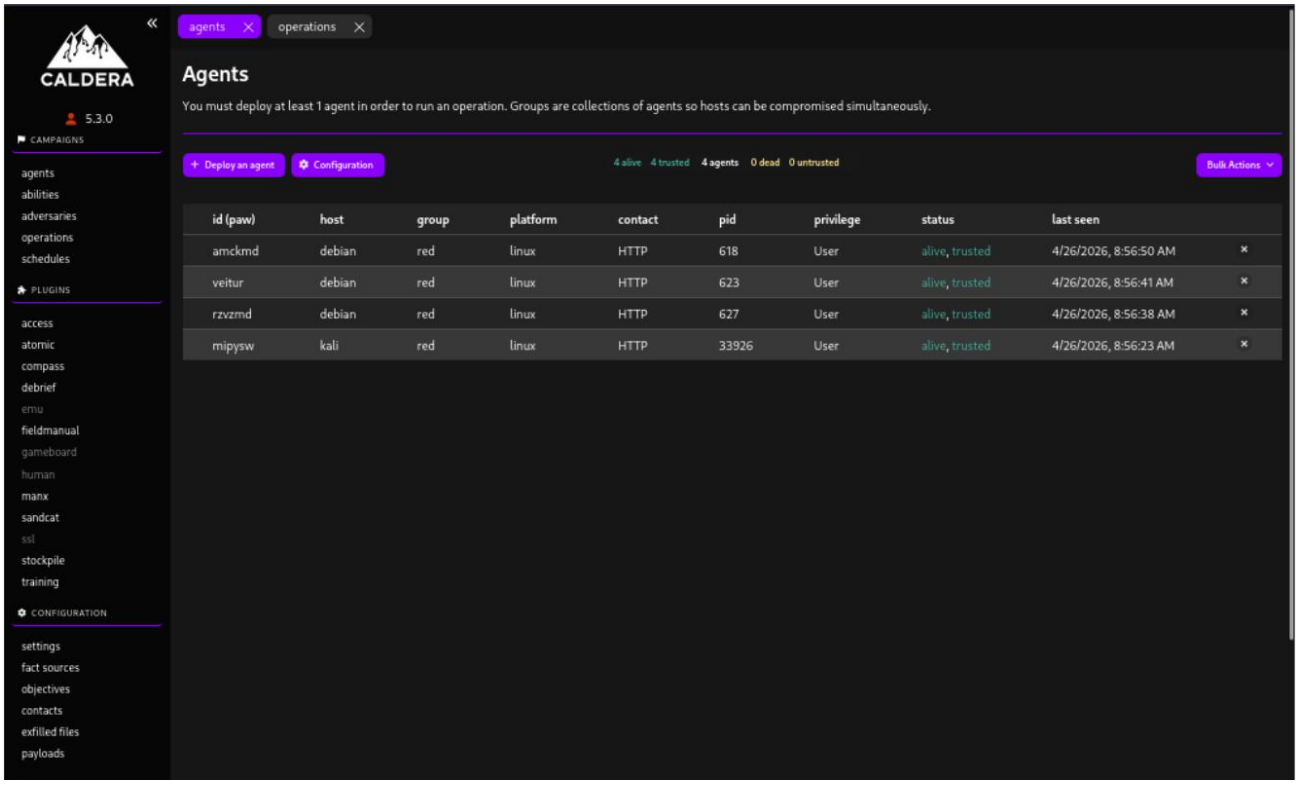

Рисунок 3.10 – Список агентів Caldera після завершення другої атаки

Такий багатоступеневий шлях суттєво підвищує складність проведення атаки, оскільки кожен додатковий вузол у ланцюжку вимагає від зловмисника витрат часу та ресурсів на ідентифікацію вразливостей, подолання локальних систем захисту та повторне закріплення. Це не лише сповільнює розвиток інциденту, а й створює додаткові умови для виявлення підозрілої активності на кожному етапі горизонтального переміщення між сегментами.

Третій етап дослідження присвячений перевірці гіпотези про те, що стійкість системи безпосередньо залежить від мінімізації довірчих зв’язків між її компонентами. У попередньому сценарії було продемонстровано, що наявність безпарольного доступу дозволила зловмиснику нівелювати переваги мережевої сегментації. Тому метою заключного етапу є впровадження політики мінімальних привілеїв на рівні хостів для забезпечення безперервного захисту критичного вузла FEP.

У межах цього сценарію було проведено системне зміцнення серверів, яке полягало у повному видаленні скомпрометованих SSH-ключів та деактивації механізмів безпарольної автентифікації. Такі заходи перетворюють HDS із потенційного «трампліна» на ізольовану точку, яка більше не має автоматичного доступу до технологічного шлюзу.

Під час повторного запуску атаки в Caldera спостерігається зупинка просування зловмисника. Після захоплення вузла HDS агент Sandcat намагається використати існуючий канал зв'язку для переходу на FEP, проте отримує відмову в автентифікації.

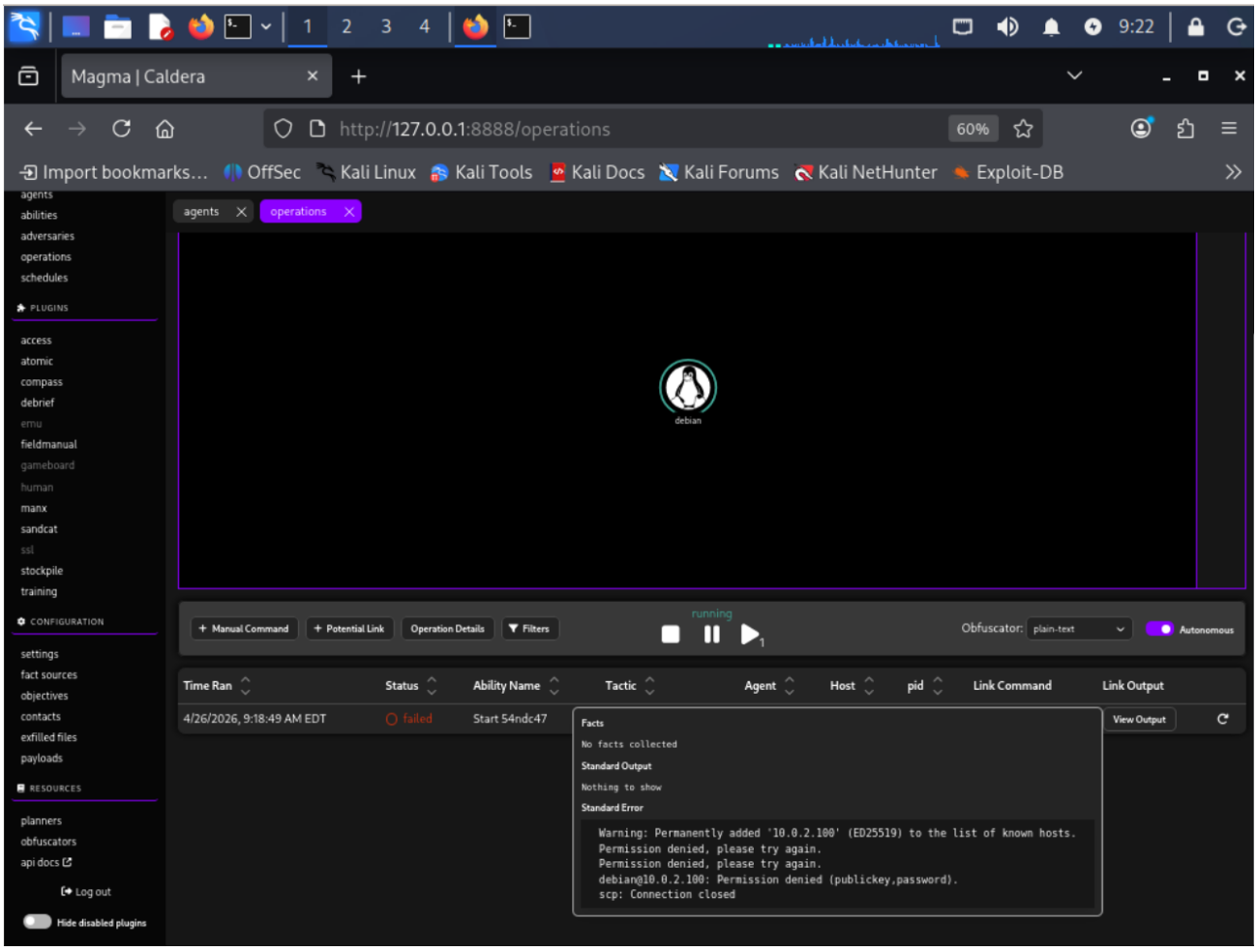

Рисунок 3.11 – Помилка автентифікації при спробі копіювання агента на FEP після скасування довірчих відносин

Замість зупинки зловмисник переходить до альтернативної техніки – переадресації портів через скомпрометований HDS. Оскільки між HDS та FEP існує легітимний мережевий маршрут для технологічного обміну даними, атакуючий встановлює тунель, що дозволяє проксіювати трафік через довірений вузол, маскуючи його під штатну активність. Цей підхід вимагає ручного підбору параметрів підключення та значно більших витрат часу порівняно з попередніми сценаріями.

У результаті зловмисник все ж досягає вузла FEP, однак загальний час атаки суттєво зростає. Це підтверджує, що впроваджені контрзаходи принципово ускладнюють атаку та збільшують її вартість для зловмисника, навіть якщо повністю не унеможливлюють її.

За результатами трьох етапів симуляції було зібрано статистичні дані, які демонструють зміну показників захищеності мережі енергетичного об’єкта залежно від впроваджених політик безпеки. Порівняльна характеристика наведена в таблиці 3.1:

Таблиця 3.1 – Порівняльна характеристика результатів симуляцій

Сценарій	I	II	III
Загальна кількість кроків	7	11	15
Успішно виконані дії	7	9	9
Невдалі спроби	0	2	6
Відсоток успішної експлуатації	100%	81%	60%
Час атаки	14 хв	23 хв	31 хв

Висновки до розділу 3

У третьому розділі за допомогою платформи MITRE Caldera проведено серію симуляцій кібератак для оцінювання кіберстійкості розробленої мережі. Експериментально підтверджено, що перехід від «плоскої» топології до сегментованої архітектури суттєво ускладнює просування зловмисника, змушуючи його використовувати багатоступеневі вектори атаки.

Встановлено, що найвищий рівень стійкості досягається завдяки поєднанню мережевого екранування та системного зміцнення кінцевих точок. Відмова від безпарольної автентифікації та мінімізація привілеїв унеможливили пряме горизонтальне переміщення на критичний шлюз FEP, змусивши зловмисника вдатися до більш складних технік – зокрема, тунелювання трафіку через довірений вузол. Попри те, що ціль була зрештою досягнута, загальний час атаки та кількість невдалих спроб суттєво зросли порівняно з попередніми сценаріями.

Результати тестування демонструють, що кожен доданий рівень захисту збільшує вартість атаки для зловмисника в термінах часу та ресурсів, що є ключовим показником для подальшого кількісного оцінювання.

4 КІЛЬКІСНИЙ ОБРАХУНОК ІНДИКАТОРА КІБЕРСТІЙКОСТІ

4.1 Ланцюг Маркова при оцінці кіберстійкості

Кількісне вимірювання індикатора кіберстійкості вимагає переходу від статичних оцінок захищеності до аналізу динаміки розвитку інциденту в реальному часі. У сучасних умовах, коли компрометація зовнішнього периметра вважається лише питанням часу, стійкість системи визначається її здатністю локалізувати загрозу та максимально уповільнювати просування зловмисника всередину інфраструктури. Такий підхід перетворює архітектуру мережі на послідовність логічних бар'єрів, подолання кожного з яких вимагає від атакуючого певних ресурсів та часу.

Математичним фундаментом для опису такої динамічної боротьби в даній роботі обрано апарат марковських процесів з безперервним часом. Головна перевага марковських моделей полягає в можливості формалізувати шлях зловмисника як послідовну зміну станів системи. Кожен стан у цій моделі є відображенням певного рівня контролю зловмисника над вузлами мережі. Це дозволяє трансформувати топологію підстанції у граф переходів, де ймовірність успіху атаки на кожній ділянці залежить від інтенсивності дій хакера та ефективності впроваджених механізмів захисту.

Для забезпечення об'єктивності моделювання інтенсивності переходів λ_{ij} розраховуються на основі аналізу конкретних вразливостей, притаманних програмному забезпеченню енергетичного об'єкта. Зокрема, використовуються метрики системи CVSS, де критичність вразливості безпосередньо впливає на швидкість її експлуатації. Наприклад, наявність вразливості із балом 9.8 на зовнішньому шлюзі зумовлює високу початкову інтенсивність атаки, тоді як вразливості середнього рівня із балом 5.1, значно уповільнюють просування зловмисника через складніші умови експлуатації.

Використання марковських ланцюгів дозволяє виміряти кіберстійкість через показник ймовірності перебування системи в безпечному стані протягом заданого інтервалу. На відміну від традиційних підходів, що фіксують лише поточний стан захищеності, марковська модель дозволяє розрахувати ймовірність компрометації цілі в будь-який момент часу. Це дає змогу кількісно оцінити внесок кожного захисного заходу – від сегментації мережі до зміцнення конфігурацій хостів – у загальний запас міцності об’єкта. Таким чином, марковська модель виступає об’єктивним інструментом, що переводить результати практичних симуляцій у площину математичного прогнозування стійкості інфраструктури.

4.2 Побудова графів станів та математичний опис моделі

Для перетворення результатів імітаційного моделювання у математичну форму необхідно визначити множину станів, у яких може перебувати система під час реалізації загрози. Кожен стан у марковському ланцюзі відповідає певному рівню компрометації об’єкта, що безпосередньо корелює зі структурою мережі підстанції. Для даного дослідження визначено чотири основні стани:

1. S_0 (Вихідний стан) – система перебуває в штатному режимі роботи, зовнішній периметр не порушено, зловмисник не має доступу до внутрішніх ресурсів;
2. S_1 (Компрометація DMZ) – зловмисник успішно встановив контроль над Web-сервером, отримавши плацдарм для подальшого просування;
3. S_2 (Компрометація корпоративного сегмента) – загроза поширилася на сервер HDS, що свідчить про подолання першого рівня сегментації;
4. S_3 (Компрометація технологічного сегмента) – зловмисник досяг комунікаційного шлюзу FEP, що означає повну втрату кіберстійкості щодо обраного вектора атаки.

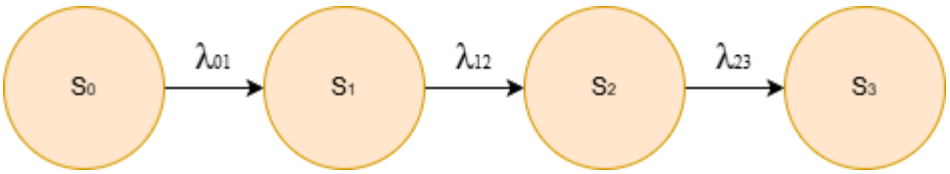

Рисунок 4.1 – Граф станів

Перехід системи між станами відбувається з інтенсивністю λ_{ij}. На відміну від класичних моделей, у даній роботі інтенсивність не є статичною величиною, а розраховується як похідна від теоретичної критичності вразливості та практичного часу її експлуатації. Математично це виражається формулою:

$$\lambda = \frac{1}{T \times (1 - S_{norm})} \times (1 - E) \tag{4.1}$$

де T – час, необхідний зловмиснику для успішного використання вразливості та переходу до наступного вузла, S_{norm} – нормований бал CVSS, а E – ефективність контрзаходів.

Математичний опис динаміки зміни ймовірностей здійснюється за допомогою системи диференціальних рівнянь Колмогорова [16]. У загальному вигляді для лінійної структури переходу $S_0 \to S_1 \to S_2 \to S_3$ система має вигляд:

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -\lambda_{01} P_0(t) \\ \dfrac{dP_1(t)}{dt} = \lambda_{01} P_0(t) - \lambda_{12} P_1(t) \\ \dfrac{dP_2(t)}{dt} = \lambda_{12} P_1(t) - \lambda_{23} P_2(t) \\ \dfrac{dP_3(t)}{dt} = \lambda_{23} P_2(t) \end{cases} \tag{4.2}$$

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

Розв’язання цієї системи дозволяє отримати часову залежність імовірності компрометації критичного вузла $P_i(t)$, яка і є головним кількісним показником кіберстійкості архітектури.

Для отримання фінального кількісного індикатора кіберстійкості K_{res} використовується інтегральний метод обчислення середньої ймовірності безпеки системи. Даний показник розраховується за формулою:

$$K_{res} = 1 - \frac{1}{T}\int_0^T P_3(t)dt \tag{4.3}$$

де $P_3(t)$ – ймовірність компрометації фінальної цілі, а T – загальний час спостереження. Значення K_{res} в межах від 0 до 1 дозволяє чітко класифікувати рівень стійкості архітектури: від критично вразливої до абсолютно стійкої в межах обраної моделі загроз.

4.3 Результати обрахунків

За результатами розрахунку, проведеного з використанням розробленої програми, отримано значення інтенсивностей переходів λ для кожного ребра графа станів у кожному сценарії. Вхідні параметри визначено на основі результатів симуляцій третього розділу та аналізу вразливостей CVE. Зведені значення λ наведено в таблиці 4.1.

Таблиця 4.1 – Розраховані значення інтенсивностей переходів

Перехід	Сценарій I	Сценарій II	Сценарій III
$S_0 \to S_1$	8,33	8	6,25
$S_1 \to S_2$	-	0,16	0,075
$S_2 \to S_3$	-	4,28	0,66
$S_1 \to S_3$	6,25	-	-

У першому сценарії граф має лише два переходи – $S_0 \to S_1 \to S_3$, оскільки за відсутності сегментації зловмисник переходить безпосередньо з DMZ до технологічного сегмента, оминаючи корпоративний. У другому та третьому сценаріях сегментація змушує зловмисника проходити через стан S_2, що додає додатковий рівень затримки та знижує загальну інтенсивність просування.

Після підстановки отриманих значень λ у систему рівнянь Колмогорова та чисельного інтегрування $P_3(t)$ на інтервалі $T = 50$ отримано значення індикатора K_{res} для кожного сценарію.

Таблиця 4.2 – Результати розрахунку індикатора кіберстійкості

Параметр	Сценарій I	Сценарій II	Сценарій III
Контрзаходи	Відсутні	Сегментація	Сегментація та зміцнення
Час до $P_3 = 0{,}5$	0,4 хв	4,62 хв	11 хв
$P_3(t)$	1	0,99	0,97
K_{res}	0,0055	0,12	0,29

Перший сценарій демонструє критично низький рівень захищеності. За відсутності будь-яких засобів протидії зловмисник майже миттєво долає периметр та компрометує цільовий вузол, через що система більшу частину часу спостереження перебуває у повністю дестабілізованому стані. Графік ймовірності зламу стрімко досягає свого максимуму вже на перших хвилинах симуляції, що підтверджує неспроможність архітектури без сегментації чинити опір цілеспрямованим атакам.

Впровадження мережевої сегментації у другому сценарії кардинально змінює динаміку розвитку кібератаки. Поділ інфраструктури на ізольовані зони та поява додаткових проміжних етапів змушують атакуючу сторону витрачати значно більше часу на горизонтальне переміщення всередині мережі. Це архітектурне рішення дозволяє суттєво відсунути момент критичного зламу та помітно підвищити інтегральний показник кіберстійкості системи, демонструючи високу ефективність навіть за мінімального рівня протидії на хостах.

Найвищу ефективність очікувано демонструє третій сценарій, який поєднує ізоляцію технологічних сегментів із комплексом заходів щодо зміцнення конфігурацій кінцевих точок. Завдяки суттєвому зниженню інтенсивностей переходів на кожному з етапів, крива ймовірності компрометації зростає максимально похило, а критична межа ймовірності досягається із великою затримкою. Навіть наприкінці інтервалу спостереження система зберігає здатність частково виконувати свої функції та уникає повного зламу, що доводить спроможність запропонованого комплексного підходу забезпечувати високу кіберстійкість критичної інфраструктури.

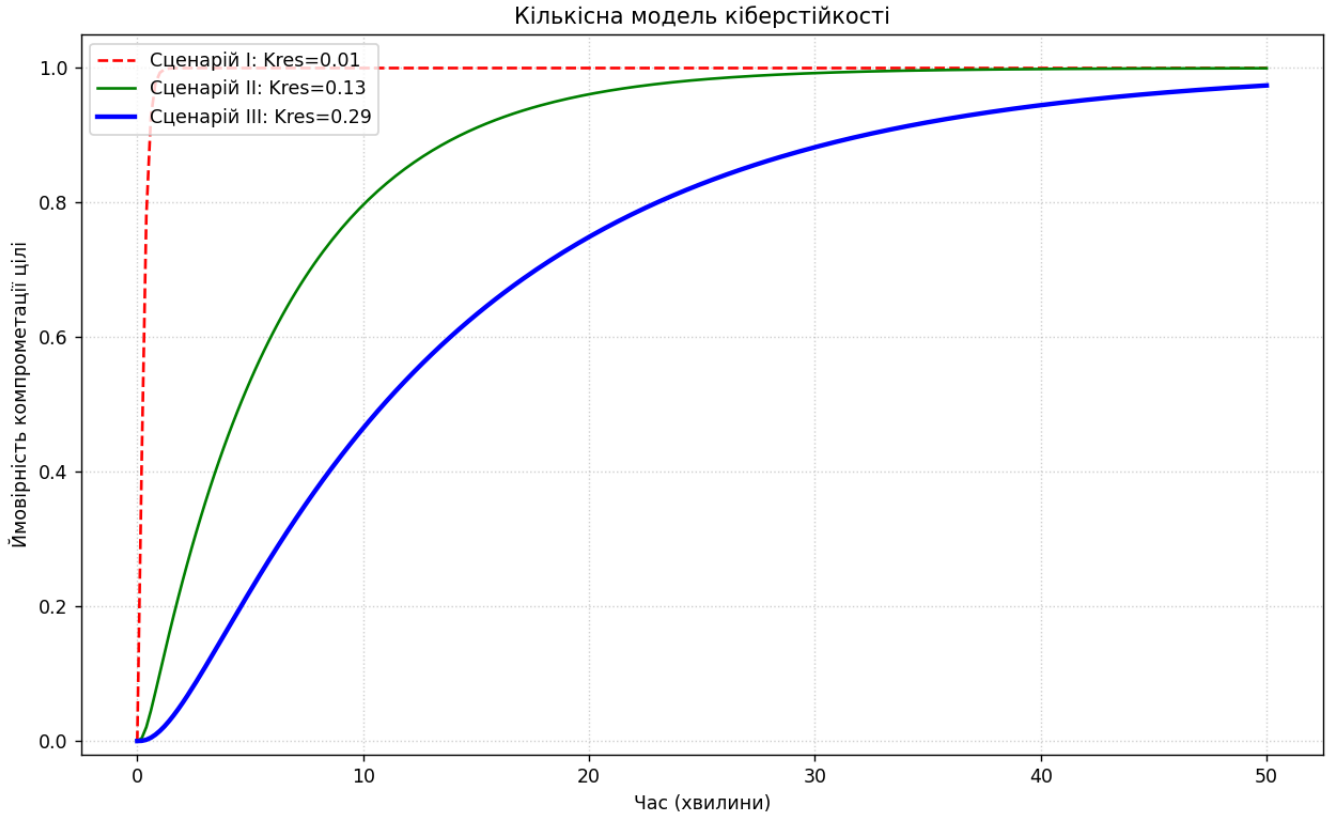

Рисунок 4.2 – Динаміка ймовірності компрометації FEP для трьох сценаріїв

Висновки до розділу 4

У четвертому розділі розроблено математичну модель кіберстійкості на основі неперервних ланцюгів Маркова та реалізовано алгоритм розрахунку інтегрального індикатора K_{res}. Інтенсивності переходів між станами параметризовано на основі реальних метрик CVSS та результатів симуляцій третього розділу, що забезпечує відтворюваність обчислень.

Побудовано граф станів із чотирма вузлами, що відповідають рівням компрометації мережі підстанції. Для кожного ребра графа розраховано інтенсивність переходу λ з урахуванням трьох факторів: критичності вразливості за шкалою CVSS, часу її практичної експлуатації та ефективності впроваджених контрзаходів. Динаміка ймовірностей станів описується системою

диференціальних рівнянь Колмогорова, розв’язання якої дозволяє отримати часову залежність ймовірності компрометації $P_3(t)$.

Фінальний індикатор обчислюється як різниця між одиницею та середньою за часом ймовірністю перебування системи у стані повної компрометації, що дозволяє звести динамічну часову функцію до єдиного порівнянного числового показника.

За результатами розрахунку отримано значення індикатора кіберстійкості для трьох сценаріїв. Ці значення підтверджують, що кожен доданий рівень захисту вносить вимірюваний внесок у стійкість об’єкта, а сама модель демонструє чутливість до архітектурних рішень. Запропонований підхід дозволяє перейти від якісних експертних оцінок до кількісного порівняння захищеності різних архітектур, що є принциповою перевагою перед існуючими фреймворками оцінки кіберстійкості.

ВИСНОВКИ

У дипломній роботі розглянуто проблематику оцінювання кіберстійкості для об’єктів критичної інфраструктури та запропоновано рішення на базі математичного апарату марковських процесів із безперервним часом.

За результатами аналізу існуючих методів і фреймворків оцінювання кіберстійкості, зокрема CERT-RMM і CRR, CREF і SSM-CR, а також Resilience Matrix, встановлено, що жоден із розглянутих підходів не забезпечує повноцінного кількісного вимірювання стійкості в динаміці. Усі три методи мають якісний або напівкількісний характер, що обмежує їхню практичну цінність для прийняття інженерних рішень щодо захисту конкретних об’єктів.

У ході дослідження типових кібератак на об’єкти критичної інфраструктури проаналізовано три реальні задокументовані інциденти: атаку з використанням ШПЗ FrostyGoop на комунальне підприємство Львова у січні 2024 року, що залишила понад 600 будинків без опалення, кампанію угруповання UAC-0133 проти близько 20 підприємств у 10 регіонах України, а також кампанію UAC-0212 з атаками щонайменше на 25 підприємств у період з липня 2024 по лютий 2025 року. У всіх трьох випадках спільним критичним фактором виявилася недостатня сегментація мережі, яка надала можливість зловмиснику виконати горизонтальне переміщення.

Для практичної перевірки теоретичних положень побудовано та розгорнуто в хмарному середовищі GCP імітаційну модель мережі розподільчої підстанції на базі платформи GNS3, що охоплює три ізольовані сегменти. Проведено аналіз потенційних векторів атак на основі CVE-вразливостей із оцінкою за шкалою CVSS.

За допомогою автоматизованої платформи MITRE Caldera проведено три сценарії симуляцій кібератак із різними рівнями захищеності. Результати порівняльного тестування наочно демонструють ефективність засобів захисту. У сценарії без сегментації зловмисник виконав 7 із 7 дій зі 100% успішністю за 14 хвилин; при впровадженні сегментації – 9 із 11 дій (81% успішності) за 23 хвилини; при додатковому зміцненні кінцевих точок – 9 із 15 дій (60% успішності) за 31 хвилину. Таким чином, комплексний захист більш ніж вдвічі збільшив тривалість атаки та знизив її ефективність.

На основі отриманих експериментальних даних розроблено програмне рішення для кількісного розрахунку індикатора кіберстійкості K_{res} з використанням ланцюгів Маркова з неперервним часом та рівнянь Колмогорова. Розраховані значення індикатора підтвердили висновки симуляцій: $K_{res} = 0{,}0055$ для плоскої топології без засобів захисту, $K_{res} = 0{,}12$ при впровадженні сегментації та $K_{res} = 0{,}29$ при комбінуванні сегментації зі зміцненням хостів. У підсумку, результати моделювання підтверджують високу ефективність запропонованих рішень та доводять, що послідовне впровадження архітектурних заходів захисту забезпечує принципове та суттєве підвищення загальної кіберстійкості об’єкта.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Verma P. та ін. Toward a Unified Understanding of Cyber Resilience: Concepts, Strategies, and Future Directions. IEEE Access. 2025. Vol. 13. P. 49945–49965. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10929043

2. Гальчинський, Л., & Личик, В. (2023). Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). Інформаційні технології та суспільство, (2 (8), С. 27-33. URL: https://doi.org/10.32689/maup.it.2023.2.3

3. Caralli R. A. та ін. CERT Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience. Carnegie Mellon University / Software Engineering Institute, 2014. URL: https://www.sei.cmu.edu/documents/2275/2014_004_001_93058.pdf

4. Cyber Resilience Review (CRR): Self-Assessment User Guide. Version 4.0. Cybersecurity and Infrastructure Security Agency (CISA), 2020. URL: https://www.cisa.gov/sites/default/files/publications/2_CRR%204.0_Self-Assessment_User_Guide_April_2020.pdf

5. Ross R. та ін. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, Volume 2, Revision 1. National Institute of Standards and Technology, 2021. DOI: https://doi.org/10.6028/NIST.SP.800-160v2r1

6. Bodeau D., Graubart R. Cyber Resiliency Engineering Framework. The MITRE Corporation, 2011. URL: https://www.mitre.org/sites/default/files/media/publication/11_4436_2.pdf

7. Bodeau D., Graubart R. Cyber Resiliency Metrics and Scoring in Practice: Use Case Methodologies and Examples. The MITRE Corporation, 2018. URL: https://www.mitre.org/sites/default/files/2021-11/prs-18-3375-cyber-resiliency-metrics-and-scoring-in-practice-use-case-methodologies-and-examples.pdf

8. Shirazi S. N. та ін. Resilience metrics for cyber systems. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. 2014. URL: https://www.researchgate.net/publication/263176904_Resilience_metrics_for_cyber_systems

9. FrostyGoop ICS Malware: Intelligence Brief. Dragos Inc., 2024. URL: https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_r2.pdf

10. Плани UAC-0133 (Sandworm) щодо кібердиверсії на майже 20 об'єктах критичної інфраструктури України. CERT-UA. 2024. URL: https://cert.gov.ua/article/6278706

11. Цільова активність UAC-0212 у відношенні розробників та постачальників рішень АСУТП з метою здійснення кібератак на об'єкти критичної інфраструктури України (CERT-UA#13702). CERT-UA. 2024. URL: https://cert.gov.ua/article/6282517

12. Личик, В. В. (2025). Адаптивний підхід до реагування на порушення кіберстійкості об'єктів критичної інфраструктури. КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО, (59), 16-28. https://doi.org/10.36910/6775-2524-0560-2025-59-02

13. Nedyalkov I. Application of GNS3 to Study the Security of Data Exchange between Power Electronic Devices and Control Center. Computers. 2023. Vol. 12, No. 5. P. 101. DOI: https://doi.org/10.3390/computers12050101

14. Common Vulnerability Scoring System v3.1: Specification Document. Forum of Incident Response and Security Teams (FIRST), 2019. URL: https://www.first.org/cvss/v3-1/specification-document

15. Личик, В. В., Гальчинський Л.Ю. (2025). Використання моделі мереж Баєса для раннього оцінювання загроз кібератак об'єкта електроенергетики. Інститут проблем реєстрації інформації НАН України.

Реєстрація, зберігання і оброб. даних. 2025, Т. 27, № 2. С. 70-85. DOI: 10.35681/1560-9189.2025.27.2.345591. URL: https://doi.org/10.35681/1560-9189.2025.27.2.345591.

16. Ross S. M. Introduction to Probability Models. 12th ed. Academic Press, 2019. 826 p. URL: https://dokumen.pub/introduction-to-probabilitymodels-12nbsped-0128143460-9780128143469.html

ДОДАТОК А

Лістинг коду програмного рішення

```
import numpy as np
from scipy.integrate import odeint, simpson
import matplotlib.pyplot as plt

def kolmogorov(P, t, lambdas):
    n = len(lambdas) + 1
    dPdt = np.zeros(n)
    dPdt[0] = -lambdas[0] * P[0]
    for i in range(1, n - 1):
        dPdt[i] = lambdas[i-1] * P[i-1] - lambdas[i] * P[i]
    dPdt[-1] = lambdas[-1] * P[-2]
    return dPdt

def cvss_to_lambda(cvss_score, time, efficiency=0.0):
    if cvss_score <= 0 or time <= 0:
        return 0
    normalized_score = cvss_score / 10.0
    base_lambda = 1.0 / (time * (1 - normalized_score))
    return base_lambda * (1.0 - efficiency)

stage1 = {
    '0->1': [9.8, 6, 0.0],
    '1->3': [9.8, 8, 0.0]
}

stage2 = {
    '0->1': [9.8, 5, 0.2],
    '1->2': [7.8, 11, 0.6],
    '2->3': [9.8, 7, 0.4]
}

stage3 = {
    '0->1': [9.8, 4, 0.5],
    '1->2': [7.8, 12, 0.8],
    '2->3': [9.8, 15, 0.8]
```

```
}

def get_lambdas_updated(cvss_data):
    return [cvss_to_lambda(val[0], val[1], val[2]) for val in
cvss_data.values()]

def calculate_kres(p_target_values, time_array):
    avg_compromise_prob = simpson(y=p_target_values, x=time_array) /
max(time_array)
    return 1 - avg_compromise_prob

t = np.linspace(0, 50, 250)

l_s1 = get_lambdas_updated(stage1)
l_s2 = get_lambdas_updated(stage2)
l_s3 = get_lambdas_updated(stage3)

res1 = odeint(kolmogorov, [1, 0, 0], t, args=(l_s1,))
res2 = odeint(kolmogorov, [1, 0, 0, 0], t, args=(l_s2,))
res3 = odeint(kolmogorov, [1, 0, 0, 0], t, args=(l_s3,))

kres1 = calculate_kres(res1[:, -1], t)
kres2 = calculate_kres(res2[:, -1], t)
kres3 = calculate_kres(res3[:, -1], t)

t_p05_s1 = t[np.where(res1[:, -1] >= 0.5)[0][0]] if any(res1[:, -1] >= 0.5)
else "не досягнуто"
t_p05_s2 = t[np.where(res2[:, -1] >= 0.5)[0][0]] if any(res2[:, -1] >= 0.5)
else "не досягнуто"
t_p05_s3 = t[np.where(res3[:, -1] >= 0.5)[0][0]] if any(res3[:, -1] >= 0.5)
else "не досягнуто"

print("--- СЦЕНАРІЙ I ---")
print(f"Інтенсивності: {l_s1}")
print(f"Час до P_3=0.5: {t_p05_s1:.2f} хв." if isinstance(t_p05_s1, float)
else f"Час до P_3=0.5: {t_p05_s1}")
print(f"Фінальна ймовірність P_3(t): {res1[-1, -1]:.4f}")
print(f"Коефіцієнт Kres: {kres1:.4f}\n")
```

```
        print("--- СЦЕНАРІЙ II ---")
        print(f"Інтенсивності: {l_s2}")
        print(f"Час до P_3=0.5: {t_p05_s2:.2f} хв." if isinstance(t_p05_s2, float)
        else f"Час до P_3=0.5: {t_p05_s2}")
        print(f"Фінальна ймовірність P_3(t): {res2[-1, -1]:.4f}")
        print(f"Коефіцієнт Kres: {kres2:.4f}\n")

        print("--- СЦЕНАРІЙ III ---")
        print(f"Інтенсивності: {l_s3}")
        print(f"Час до P_3=0.5: {t_p05_s3:.2f} хв." if isinstance(t_p05_s3, float)
        else f"Час до P_3=0.5: {t_p05_s3}")
        print(f"Фінальна ймовірність P_3(t): {res3[-1, -1]:.4f}")
        print(f"Коефіцієнт Kres: {kres3:.4f}\n")

        plt.figure(figsize=(12, 7))
        plt.plot(t, res1[:, -1], 'r--', label=f'Сценарій I: Kres={kres1:.2f}')
        plt.plot(t, res2[:, -1], 'g-',  label=f'Сценарій II: Kres={kres2:.2f}')
        plt.plot(t,  res3[:,  -1],  'b-',    linewidth=2.5,  label=f'Сценарій  III:
        Kres={kres3:.2f}')

        plt.title('Кількісна модель кіберстійкості')
        plt.xlabel('Час (хвилини)')
        plt.ylabel('Ймовірність компрометації цілі')
        plt.legend(loc='upper left')
        plt.grid(True, linestyle=':', alpha=0.6)
        plt.ylim(-0.02, 1.05)
plt.show()
```