

**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
«__» _____ 20__ р.

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

на тему: Модель оцінювання часу компрометації об'єкта критичної енергетичної
інфраструктури при багатостадійних кібератаках

Виконав (-ла): здобувач (-ка) вищої освіти **IV** курсу, групи ФБ-24
(шифр групи)

_____ **Шевченко Вікторія Миколаївна** _____
(прізвище, ім'я, по батькові) (підпис)

Керівник _____ **Гальчинський Леонід Юрійович, доцент кафедри ІБ** **к.т.н. доцент** _____
(посада, науковий ступінь, вчене звання, ім'я, прізвище) (підпис)

Рецензент _____
(посада, науковий ступінь, вчене звання, науковий ступінь, ім'я, прізвище) (підпис)

Засвідчую, що у цій дипломній роботі немає
запозичень з праць інших авторів без відповідних
посилань.

Здобувач вищої освіти _____
(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
(підпис)

«16» червня 2026 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти
Шевченко Вікторії Миколаївні
(прізвище, ім'я, по батькові)

1. Тема роботи: Модель оцінювання часу компрометації об'єкта критичної енергетичної інфраструктури при багатоетапних кібератаках ,

керівник роботи: Гальчинський Леонід Юрійович, к.т.н, доцент ,

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «29» травня 2026р. № 2001-с

2. Термін подання роботи здобувачем вищої освіти «08» червня 2026 р.

3. Вихідні дані до роботи: опис типової архітектури мережі диспетчерського SCADA-центру керування об'єкта електроенергетики; база CVE-вразливостей NVD та каталоги CISA KEV/CSAF (2020–2025 pp.); специфікація CVSS v3.1; модель Time-to-Compromise McQueen та її ICS-адаптація TTCICS.

4. Зміст (дипломної роботи) пояснювальної записки (перелік завдань, які потрібно розробити): провести аналіз стану кібербезпеки об'єктів критичної енергетичної інфраструктури та структури багатоетапних кібератак на енергооб'єкти; дослідити базову модель Time-to-Compromise McQueen та її ICS-адаптацію TTCICS; розробити формальну модель TTCAG як дворівневу структуру з коефіцієнтами AV_w та γ ;

сформувати датасет CVE-вразливостей тестової архітектури мережі енергооб'єкта та побудувати граф атак засобами інструменту MulVAL; виконати обчислення TTCAG для шляхів атаки до цільової підстанції та сформулювати висновки щодо придатності розробленої моделі.

5. Перелік графічного (ілюстративного) матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо): презентація.

6. Дата видачі завдання: 30 жовтня 2025 року.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Формулювання теми та завдання дипломної роботи	30.09.2025 – 30.10.2025	Виконано
2	Вивчення наукової літератури	31.10.2025 – 02.03.2026	Виконано
3	Аналіз стану кібербезпеки об'єктів критичної енергетичної інфраструктури та структури багатоетапних кібератак	03.03.2026 – 02.04.2026	Виконано
4	Дослідження базової моделі Time-to-Compromise	03.04.2026 – 20.04.2026	Виконано
5	Розробка формальної моделі TTCAG, обґрунтування числових значень параметрів	21.04.2026 – 03.05.2026	Виконано
6	Формування датасету CVE-вразливостей та побудова графа атак засобами інструменту MulVAL	04.05.2026 – 15.05.2026	Виконано
7	Обчислювальний експеримент: розрахунок TTCAG	16.05.2026 – 24.05.2026	Виконано
8	Оформлення дипломної роботи згідно методичних вказівок	25.05.2026 – 07.06.2026	Виконано
9	Передзахист дипломної роботи	08.06.2026	
10	Захист дипломної роботи	16.06.2026	

Здобувач вищої освіти

_____ (підпис)

Вікторія ШЕВЧЕНКО
(Власне ім'я, ПРІЗВИЩЕ)

Керівник роботи

_____ (підпис)

Леонід ГАЛЬЧИНСЬКИЙ
(Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг роботи 84 сторінки, 6 ілюстрацій, 14 таблиць, 3 додатки, 34 джерела літератури.

Об'єкт дослідження: процес поширення багатоетапної кібератаки в мережі диспетчерського SCADA-центру керування об'єкта електроенергетики від точки входу зловмисника у зовнішній мережі до компрометації цільового вузла підстанції.

Предмет дослідження: методи кількісного оцінювання часу компрометації критичних вузлів мережі ICS з урахуванням накопичення привілеїв при латеральному русі зловмисника.

Мета дослідження: підвищення захищеності об'єктів критичної енергетичної інфраструктури від багатоетапних кібератак шляхом розширення моделі оцінювання Time-to-Compromise з урахуванням топології мережі та ефекту накопичення привілеїв на графі атак.

Методи дослідження: логічний аналіз вразливостей засобами інструменту MulVAL для побудови графу атак; нормалізація стандартизованих коефіцієнтів CVSS v3.1 для обґрунтування числових значень параметрів моделі TTCAG; чисельне моделювання та аналіз чутливості для практичної реалізації моделі.

Отримані результати: розроблено формальну модель TTCAG як дворівневу структуру, що усуває ключові обмеження існуючих моделей TTC McQueen та TTCICS для багатоетапних атак. Сформовано датасет із 1 975 записів CVE 2020-2025 рр. для 10 вузлів типової архітектури SCADA-центру. Побудовано граф атак засобами MulVAL (128 вершин, 166 ребер) і обчислено TTCAG для п'яти основних шляхів атаки. Встановлено, що врахування накопичення привілеїв зменшує оцінку часу компрометації на 17-30% залежно від довжини шляху атаки.

Результати роботи були представлені на XXIV Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (13-16 травня 2026 р.,

м. Київ) у секції «Математичні методи кібернетичної безпеки», де опубліковано наукову статтю за матеріалами дослідження.

Ключові слова: КРИТИЧНА ЕНЕРГЕТИЧНА ІНФРАСТРУКТУРА, ЧАС КОМПРОМЕТАЦІЇ, БАГАТОЕТАПНА КІБЕРАТАКА, ГРАФ АТАК, МОДЕЛЬ TTCAG, CVSS V3.1.

ABSTRACT

The volume of the work is 84 pages, 6 illustrations, 14 tables, 3 appendices, 34 references.

Object of research: the process of a multi-stage cyberattack propagating through the network of a SCADA dispatch control center of a power energy facility, from the attacker's entry point in the external network to the compromise of the target substation node.

Subject of research: improving the security of critical energy infrastructure against multi-stage cyberattacks by extending the Time-to-Compromise model with network topology and privilege accumulation effects on attack graph.

Research objective: construction of a formal TTCAG model for quantitative estimation of the time to compromise a critical energy infrastructure facility under multi-stage cyberattacks, incorporating the attacker's skill level and privilege accumulation during lateral movement, with justification of the model's numerical parameter values through the official CVSS v3.1 specification.

Research methods: logical vulnerability analysis using the MulVAL tool for attack graph construction; normalization of standardized CVSS v3.1 coefficients to justify the numerical parameter values of the TTCAG model; numerical simulation and sensitivity analysis for practical implementation of the model.

Results obtained: a formal TTCAG model was developed as a two-level structure that eliminates the key limitations of the existing TTC McQueen and TTCICS models for multi-stage attacks. A dataset of 1,975 CVE records from 2020-2025 was compiled for 10 nodes of a typical SCADA control center architecture. An attack graph was constructed using MulVAL (128 vertices, 166 edges), and the TTCAG was computed for five primary attack paths. It was established that accounting for privilege accumulation reduces the time-to-compromise estimate by 17-30%, depending on the length of the attack path.

The results of the work were presented at the XXIV All-Ukrainian Scientific and Practical Conference of Students, Postgraduates, and Young Scientists "Theoretical and

Applied Problems of Physics, Mathematics and Informatics" (May 13-16, 2026, Kyiv) in the section "Mathematical Methods of Cybersecurity," where a scientific article based on the research materials was published.

Keywords: CRITICAL ENERGY INFRASTRUCTURE, TIME TO COMPROMISE, MULTI-STAGE CYBERATTACK, ATTACK GRAPH, TTCAG MODEL, CVSS V3.1.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	10
ВСТУП.....	14
1 КРИТИЧНА ЕНЕРГЕТИЧНА ІНФРАСТРУКТУРА ЯК ОБ’ЄКТ КІБЕРЗАГРОЗ. МЕТОДИ ОЦІНЮВАННЯ ЧАСУ ЇЇ КОМПРОМЕТАЦІЇ	17
1.1 Критична енергетична інфраструктура як предметна область дослідження та об’єкт кіберзагроз.....	17
1.2 Багатоетапні кібератаки на енергетичну інфраструктуру	19
1.3 Час як ключовий ресурс кіберзахисту енергооб’єкта	23
1.4 Методи кількісного оцінювання часу компрометації ICS-мереж.....	25
Висновки до розділу 1	28
2 ФОРМАЛЬНА МОДЕЛЬ TTCAG	30
2.1 Базова модель часу компрометації TTC McQueen	30
2.2 Адаптація моделі для ICS-середовища – TTCICS	36
2.3 Обмеження моделі TTCICS для багатоетапних атак.....	37
2.4 Формальний апарат моделі TTCAG	39
2.5 Обґрунтування числових значень параметрів моделі TTCAG.....	42
2.6 Стохастичні властивості загального розподілу TTCAG	46
Висновки до розділу 2	50
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ TTCAG ДЛЯ МЕРЕЖІ ОБ’ЄКТА КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ	51
3.1 Опис тестової мережі автоматизованої підстанції	51
3.2 Формування датасету CVE для вузлів мережі	53
3.3 Побудова графу атак засобами MulVAL	56
3.4 Аналіз отриманого графу атак	57
3.5 Розрахунок показника TTC* для вузлів мережі.....	59
3.6 Розрахунок TTCAG для шляхів атаки.....	61
3.7 Порівняння базової TTCAG ⁰ та повної TTCAG версій моделі	62
3.8 Аналіз чутливості моделі до рівня кваліфікації зловмисника.....	64
3.9 Практична цінність отриманих результатів	65
Висновки до розділу 3	66
ВИСНОВКИ.....	67

	9
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ.....	70
ДОДАТОК А.....	75
ДОДАТОК Б.....	77
ДОДАТОК В.....	83

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

APT – Advanced Persistent Threat, цілеспрямована довготривала кіберзагроза підвищеної складності

AV – Attack Vector, вектор атаки (поле метрики CVSS v3.1)

AVw – Attack Vector weight, ваговий коефіцієнт вектора атаки у моделі TTCAG

BAG – Bayesian Attack Graph, байєсівський граф атак

CIA – Confidentiality, Integrity, Availability, конфіденційність, цілісність, доступність

CISA – Cybersecurity and Infrastructure Security Agency, агентство з кібербезпеки та захисту інфраструктури (США)

CVE – Common Vulnerabilities and Exposures, загальний перелік вразливостей та загроз

CVSS – Common Vulnerability Scoring System, загальна система оцінювання вразливостей

DAG – Directed Acyclic Graph, орієнтований ациклічний граф

DCS – Distributed Control System, розподілена система керування

DMZ – Demilitarized Zone, демілітаризована зона мережі

FEP – Front End Processor, фронтальний процесор зв'язку з польовим рівнем

FIRST – Forum of Incident Response and Security Teams, міжнародний форум груп реагування на інциденти та безпеки

GOOSE – Generic Object Oriented Substation Event, протокол передачі подій підстанції стандарту IEC 61850

HACL – Host Access Control List, список контролю доступу хоста

HMI – Human-Machine Interface, людино-машинний інтерфейс

ICS – Industrial Control Systems, промислові системи керування

IDS – Intrusion Detection System, система виявлення вторгнень

IEC – International Electrotechnical Commission, міжнародна електротехнічна комісія

IED – Intelligent Electronic Device, інтелектуальний електронний пристрій

IRP – Incident Response Plan, план реагування на інцидент

IT – Information Technology, інформаційні технології

MCMC – Markov Chain Monte Carlo, метод Монте-Карло на основі ланцюгів Маркова

MMS – Manufacturing Message Specification, специфікація виробничих повідомлень (протокол IEC 61850)

MTBV – Mean Time Between Vulnerabilities, середній час між появою нових вразливостей

MTTC – Mean Time to Compromise, середній час компрометації мережі

MulVAL – Multi-host Multi-stage Vulnerability Analysis, інструмент логічного аналізу вразливостей для побудови графу атак

NIST – National Institute of Standards and Technology, національний інститут стандартів і технологій (США)

NVD – National Vulnerability Database, національна база даних вразливостей (США)

OPC – OLE for Process Control, стандарт обміну даними у промислових системах керування

OT – Operational Technology, операційні технології (промисловий рівень керування)

PDF – Probability Density Function, функція щільності розподілу ймовірностей

PERA – Purdue Enterprise Reference Architecture, еталонна архітектура промислових мереж Пурдью

PERT – Program Evaluation and Review Technique, метод оцінки та аналізу програм

PLC – Programmable Logic Controller, програмований логічний контролер

PR – Privileges Required, необхідний рівень привілеїв для експлуатації вразливості (поле CVSS v3.1)

RTU – Remote Terminal Unit, дистанційний термінальний пристрій

SAS – Substation Automation System, система автоматизації підстанції

SCADA – Supervisory Control and Data Acquisition, диспетчерське керування та збір даних

SMP – Semi-Markov Process, напівмарківський процес

SV – Sampled Values, вибіркові значення (протокол передачі вимірювань IEC 61850)

TTC – Time-to-Compromise, час компрометації вузла

TTCAG – Attack-Graph aware Time-to-Compromise, час компрометації з урахуванням графу атак (модель, розроблена у даній роботі)

TTCICS – Time-to-Compromise ICS, час компрометації для промислових систем керування (модель Rencelj Ling та Ekstedt)

UI – User Interaction, взаємодія з користувачем (поле метрики CVSS v3.1)

RITICS – Repository of Industrial Control Systems Threats Information and Classification Scheme, спеціалізований датасет вразливостей промислових систем керування

KEV – Known Exploited Vulnerabilities, каталог відомих активно експлуатованих вразливостей (CISA)

CSAF – Common Security Advisory Framework, стандарт структурованих бюлетенів безпеки (OASIS)

AM – кількість вразливостей компонента, для яких зловмисник даного рівня кваліфікації може знайти або розробити робочий експлоїт

b^* – скоригований параметр MTBV, що запобігає артефакту нульового значення через підстановку категорійного середнього

CVSSnorm – нормована базова оцінка CVSS (ділиться на 10; пріоритет версії v3.1 над v2)

ET – expected tries, очікувана кількість спроб зловмисника до знаходження придатної вразливості (Процес 2)

f – частка вразливостей компонента, доступних для експлуатації зловмисником даного рівня кваліфікації ($f = AM/V$)

k – загальна кількість CVE у базі (у моделі McQueen $k = 9\,447$; у TTCICS $k = 2\,740$)

m – кількість експлоїтів, доступних зловмиснику даного рівня кваліфікації (використовується у формулі P_1)

NM – кількість вразливостей компонента, недоступних для експлуатації зловмисником даного рівня ($NM = V - AM$)

P_1 – ймовірність того, що зловмисник перебуває у Процесі 1 (наявний готовий публічний експлойт)

P_2 – ймовірність того, що зловмисник перебуває у Процесі 2 (самостійна розробка експлойта; $P_2 = 1 - P_1$)

t_1, t_2, t_3 – очікуваний час компрометації за Процесами 1, 2 та 3 відповідно у моделі McQueen

TTC* – вдосконалений час компрометації окремого вузла у моделі TTCAG з урахуванням коефіцієнтів AV_w та $CVSS_{norm}$

u – ймовірність невдачі Процесу 2 (зловмисник не знаходить придатної вразливості серед відомих)

V – загальна кількість відомих вразливостей компонента (вузла мережі)

γ – коефіцієнт глибини шляху атаки у моделі TTCAG; моделює прискорення атаки внаслідок накопичення привілеїв зловмисника при латеральному русі

VPN – Virtual Private Network, віртуальна приватна мережа

ВСТУП

Електричні підстанції є ключовими вузлами електроенергетичної системи, що здійснюють перетворення, комутацію та розподіл електричної енергії. Перехід від традиційних електромеханічних підстанцій до автоматизованих, у яких функції захисту, керування та обміну телеметричною інформацією реалізуються програмованими електронними пристроями у єдиній інформаційній мережі, суттєво підвищив ефективність експлуатації енергооб'єктів. Водночас цифровізація перетворила підстанцію на кіберфізичний об'єкт, для якого з'явився принципово новий клас загроз – багатоетапні кібератаки.

Атаки BlackEnergy (2015), Industroyer (2016) та Industroyer2 (2022) на українську енергосистему підтвердили реальність цього вектора загроз і виявили потребу в кількісних інструментах оцінювання часу компрометації як основи для проактивного захисту.

Актуальність роботи. Багатоетапні кібератаки на мережі автоматизованих підстанцій характеризуються тривалою підготовчою фазою, що вимірюється місяцями. Це створює часовий проміжок для виявлення та реагування, кількісна оцінка якого є інструментом для обґрунтованого вибору засобів захисту. Кількісною основою такої оцінки є модель Time-to-Compromise (TTC), запропонована McQueen у 2005 році, та її ICS-адаптація TTCICS (Rencelj Ling, Ekstedt, 2023). Проте обидві моделі оцінюють час компрометації лише окремого вузла і для шляху атаки пропонують просте підсумовування, що ігнорує накопичення привілеїв при латеральному русі. Подолання цього обмеження визначає актуальність дослідження.

Мета роботи. Підвищення захищеності об'єктів критичної енергетичної інфраструктури від багатоетапних кібератак шляхом розширення моделі оцінювання Time-to-Compromise з урахуванням топології мережі та ефекту накопичення привілеїв на графі атак.

Завдання роботи:

1. Проаналізувати сучасний стан кібербезпеки об'єктів критичної енергетичної інфраструктури, охарактеризувати структуру багатоетапних кібератак на енергооб'єкти та виявити обмеження наявних моделей оцінювання часу компрометації;
2. Дослідити базову модель Time-to-Compromise McQueen та її ICS-адаптацію TTCICS;
3. Розробити формальну модель TTCAG як дворівневу структуру, що усуває обмеження;
4. Проаналізувати стохастичні властивості загального розподілу TTCAG як суперпозиції розподілів окремих процесів;
5. Сформувати датасет CVE-вразливостей для типової архітектури мережі енергооб'єкта, побудувати граф атак засобами інструменту MulVAL та обчислити значення TTCAG для шляхів атаки до підстанції;
6. Виконати аналіз чутливості моделі TTCAG до рівня кваліфікації зловмисника та сформулювати висновки щодо придатності розробленої моделі для практичного застосування у задачах захисту об'єктів критичної енергетичної інфраструктури.

Об'єкт дослідження. Процес поширення багатоетапної кібератаки в мережі диспетчерського SCADA-центру керування об'єкта електроенергетики від точки входу зловмисника у зовнішній мережі до компрометації цільового вузла підстанції.

Предмет дослідження. Методи кількісного оцінювання часу компрометації критичних вузлів мережі ICS з урахуванням накопичення привілеїв при латеральному русі зловмисника.

Методи дослідження. У роботі застосовано логічний аналіз вразливостей засобами інструменту MulVAL для побудови графу атак; нормалізацію стандартизованих коефіцієнтів CVSS v3.1 для обґрунтування числових значень параметрів моделі TTCAG; чисельне моделювання та аналіз чутливості для практичної реалізації моделі. Початкові дані отримано з баз NVD, CISA KEV/CSAF за період 2020-2025 р.

Наукова новизна одержаних результатів. Запропоновано модель TTCAG для задачі оцінювання часу компрометації об'єктів критичної енергетичної інфраструктури, що враховує накопичення привілеїв зловмисника при латеральному русі через коефіцієнт глибини шляху γ . На відміну від наявних моделей TTC та TTCICS, які обмежуються рівнем окремого вузла, модель TTCAG дає реалістичнішу оцінку часу для багатоетапних атак за рахунок прискорення на проміжних вузлах внаслідок накопиченого контексту.

Практичне значення одержаних результатів. Модель TTCAG дозволяє кількісно оцінювати очікуваний час досягнення зловмисником цільової підстанції для різних рівнів його кваліфікації та різних архітектур мережі енергооб'єкта, що робить її придатною для пріоритизації захисних заходів з кібербезпеки. Результати обчислювального експерименту на прикладі типової архітектури демонструють конкретні значення часу компрометації для чотирьох рівнів кваліфікації зловмисника та чутливість моделі до варіації параметрів.

Вихідні дані до роботи. Опис типової архітектури мережі диспетчерського SCADA-центру керування; перелік ідентифікаторів CVE для типових активів мережі; офіційна специфікація CVSS v3.1 з числовими коефіцієнтами для метрик Attack Vector та Privileges Required.

Апробація результатів роботи. Результати дослідження представлено на XXIV Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (13-16.05.2026 р., м. Київ) у секції «Математичні методи кібернетичної безпеки».

Публікації. За матеріалами дослідження опубліковано наукову статтю Шевченко В. М. та Гальчинського Л. Ю. «Вдосконалена модель TTCAG для оцінювання часу компрометації вузлів ICS-мережі на основі графа атак та метрик CVSS v3» у збірнику XXIV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (2026).

1 КРИТИЧНА ЕНЕРГЕТИЧНА ІНФРАСТРУКТУРА ЯК ОБ'ЄКТ КІБЕРЗАГРОЗ. МЕТОДИ ОЦІНЮВАННЯ ЧАСУ ЇЇ КОМПРОМЕТАЦІЇ

1.1 Критична енергетична інфраструктура як предметна область дослідження та об'єкт кіберзагроз

Критична інфраструктура є сукупністю об'єктів і систем, безперервне функціонування яких становить необхідну умову забезпечення національної безпеки, економічної стабільності та повсякденного життя суспільства. Енергетичний сектор традиційно посідає у складі критичної інфраструктури особливе місце, оскільки припинення електропостачання на масштабному рівні викликає відмовний ефект, що зупиняє транспорт, фінансові послуги, водопостачання, медичні заклади та системи зв'язку. Саме тому енергетична інфраструктура у міжнародних та національних нормативних документах визначається як критична інфраструктура з найвищим пріоритетом захисту [1, 4].

Технологічною основою сучасної енергетичної інфраструктури є автоматизовані системи керування виробництвом, передаванням і розподілом електричної енергії, що належать до загального класу промислових систем керування (Industrial Control Systems, ICS) [1]. До ICS входять диспетчерські системи моніторингу й керування SCADA, розподілені системи DCS, програмовані логічні контролери PLC та спеціалізовані системи автоматизації енергооб'єктів. Для електричних підстанцій вузькоспеціалізованим підкласом ICS виступають системи автоматизації підстанцій (Substation Automation Systems, SAS), що працюють згідно з міжнародним стандартом IEC 61850 [6, 7]. SAS об'єднують інтелектуальні електронні пристрої (IED), пристрої безпосереднього керування комутаційним обладнанням (RTU), людино-машинні інтерфейси (HMI) та сервери диспетчерського контролю у єдину інформаційну мережу. Завдяки такій інтеграції підстанція функціонує як кіберфізична система, у якій

інформаційні та комунікаційні технології тісно взаємодіють із фізичним обладнанням і процесами його керування [3, 8].

Принципова особливість кіберзагроз для енергетичної інфраструктури полягає в тому, що наслідки кібератак виходять за межі суто інформаційних. У типових корпоративних мережах успішна атака зазвичай завершується фінансовими втратами або витоком даних. Компрометація ОТ-сегмента (Operational Technology) енергетичного об'єкта здатна спричинити фізичну шкоду обладнанню, аварійні режими в електроенергетичній системі та загрозу життю людей. У межах класичної моделі Purdue Enterprise Reference Architecture [17] цей поділ описано через ієрархію функціональних рівнів промислової мережі, що на практиці зводиться до двох її основних сегментів – інформаційного (ІТ) та операційно-технологічного (ОТ).

На рівні наслідків кіберінцидентів спостерігається істотна асиметрія між ІТ- та ОТ-сегментами. ІТ-інцидент здебільшого має оборотний характер, оскільки дані можуть бути відновлені з резервних копій, фінансові втрати компенсовані страховими механізмами, а доступ до сервісів поновлений за лічені години. Інакше виглядає ОТ-інцидент. Зокрема, відключені споживачі несуть прямі втрати від простою, а у разі аварійних режимів в електроенергетичній системі під загрозою опиняються життя і здоров'я людей. Суттєво і те, що відновлення після ОТ-інциденту потребує фізичного втручання у польовий рівень мережі і може тривати від кількох діб до тижнів. Саме така асиметрія наслідків і пояснює, чому захист ОТ-сегмента потребує спеціалізованого підходу, а не простого перенесення практик ІТ-кібербезпеки на промислові мережі [1, 9].

Кібербезпека критичної енергетичної інфраструктури утворює самостійну предметну область, що поєднує елементи інформаційної безпеки, теорії надійності та електроенергетики. Її центральне завдання охоплює не лише запобігання інцидентам, а й мінімізацію їхніх фізичних наслідків. Тобто потрібно не допустити переходу зловмисника з ІТ-сегмента в ОТ-сегмент мережі енергооб'єкта.

1.2 Багатоетапні кібератаки на енергетичну інфраструктуру

Кібератаки на об'єкти критичної енергетичної інфраструктури мають специфічний профіль. Якщо для корпоративного сегмента характерні швидкоплинні атаки з використанням програм-вимагачів, фінансового шахрайства або викрадення персональних даних, то загрози для енергетики мають інший характер та реалізуються переважно як тривалі цілеспрямовані кампанії класу АРТ (Advanced Persistent Threat). Зловмисник у такій кампанії тривалий час перебуває у мережі непомітно, поступово закріплюється на нових вузлах, накопичує привілеї та готує цільовий вплив, який реалізується в один обраний момент [11, 12].

Атаки на енергетичну інфраструктуру переважно асоціюються з державними або пов'язаними з державою кібергрупами, які мають доступ до спеціалізованого інструментарію, вразливостей нульового дня та значних ресурсів для розвідки. Їхні цілі мають стратегічний характер і передбачають послаблення енергосистеми супротивника, демонстрацію можливостей або підготовку інфраструктури для подальших операцій [9, 12]. Такі мотиви відрізняють цих зловмисників від типових кіберзлочинців і пояснюють готовність витратити місяці на підготовку однієї атаки.

1.2.1 Структура багатоетапної атаки за моделлю ICS Cyber Kill Chain

Для опису структури багатоетапних атак на ICS використовується модель ICS Cyber Kill Chain, описана М. Assante та R. Lee у роботі SANS 2015 року як адаптація класичної моделі Cyber Kill Chain корпорації Lockheed Martin [11] до промислового середовища. У звіті E-ISAC і SANS ICS, присвяченому розслідуванню атаки BlackEnergy на українську енергосистему у 2015 році, цю модель застосовано для систематизації та аналізу послідовності дій зловмисників [12].

Згідно з цією моделлю, атака на ICS складається з двох послідовних стадій. Перша стадія «Stage 1: Cyber Intrusion Preparation and Execution» охоплює підготовку та виконання кібервторгнення в інформаційну інфраструктуру об'єкта. Друга «Stage 2: ICS Attack Development and Execution» охоплює розробку та виконання атаки безпосередньо на ICS-обладнання [12].

Stage 1 складається з таких кроків: Reconnaissance (розвідка), Weaponization/Targeting (підготовка інструментарію та вибір цілей), Delivery (доставка), Exploit (експлуатація), Install/Modify (закріплення у системі), C2 (керування через канал command-and-control) та Act (дії всередині мережі). Завершення Stage 1 означає успішне проникнення зловмисника у мережу й закріплення у ній, проте ще не є власне атакою на ICS [12]. У межах кроку Act зловмисник проводить латеральний рух, збирає облікові дані та виконує розвідку ОТ-середовища. Саме на цьому етапі формується підґрунтя для подальшої цілеспрямованої атаки на ICS.

Stage 2 включає кроки Develop (розроблення інструментарію саме під виявлене ICS-середовище), Test (тестування у внутрішніх умовах зловмисника), Deliver (доставку інструментів у мережу цілі), Install/Modify (їх встановлення на конкретних активах ICS) та Execute ICS Attack (виконання атаки) [12]. Лише після завершення Stage 2 атака стає тим, що SANS визначає як «успішну кібератаку на ICS», тобто такою, що впливає на роботу промислової системи [12].

У межах даної роботи Stage 1 розглядається у декомпозиції на два логічні підетапи – первинне проникнення в IT-периметр і латеральний рух з накопиченням привілеїв. Такий поділ зумовлений моделюванням часу компрометації. Між цими підетапами найбільш виражено проявляється ефект накопичення зловмисником привілеїв і контексту, що враховується в моделі TTСAG через коефіцієнт глибини шляху γ (розділ 2). Разом із Stage 2 ці підетапи утворюють трирівневу структуру, яка використовується далі. Детально про кожен етап:

1. Первинне проникнення в IT-периметр. Зловмисник отримує перший доступ до інформаційної мережі енергооб'єкта. У задокументованих кампаніях SANS [12] основним вектором первинного проникнення була фішингова

розсилка. Інші можливі вектори охоплюють експлуатацію вразливості зовнішнього сервісу або компрометацію облікового запису. Цілями такого етапу зазвичай стають вебсервери, файлові сервери, поштові системи й адміністративні робочі станції, тобто компоненти ІТ-сегмента. Безпосередньої загрози для технологічних процесів електропостачання тут ще немає, але створюються передумови для подальшого просування [12].

2. Латеральний рух у внутрішній мережі. На цьому етапі зловмисник збирає облікові дані, виконує підвищення привілеїв і просувається мережею, у тому числі до сегментів, де розташовані SCADA-робочі станції та сервери [12]. У звіті SANS зафіксовано, що в українському інциденті 2015 року зловмисники використовували викрадені облікові дані для з'єднання з ICS-мережею через існуючі VPN-канали (Stage 1, крок Act). Цей етап у моделі SANS належить ще до Stage 1, але виокремлений тут окремо, оскільки саме на ньому зловмисник накопичує контекст, який прискорює подальшу атаку на ICS-обладнання.

3. Атака на ICS-обладнання. Зловмисник переходить до Stage 2 моделі SANS. Він розробляє інструменти, специфічні для виявленого ICS-середовища, тестує їх, доставляє у мережу цілі та виконує безпосередній вплив на промислове обладнання [12]. Саме цей етап несе фізичну загрозу. У документованому інциденті BlackEnergy 2015 зловмисники використали HMI у SCADA-середовищі для віддаленого відкриття вимикачів, додатково завантажили шкідливу прошивку у конвертори serial-to-Ethernet на підстанціях і застосували модифікований KillDisk для приховування слідів [12].

Описана структура є стійкою і повторюється у документованих атаках на енергооб'єкти. Її стійкість пояснюється тим, що вона відповідає об'єктивній структурі мережі: ІТ-сегмент завжди є межевою зоною із зовнішнім світом, ОТ-сегмент – зоною безпосереднього керування фізичним обладнанням, а між ними розташована проміжна зона з трансферними системами. Інше будувати неможливо без втрати функціональності об'єкта. Саме ця передбачувана трирівнева структура дозволяє формалізувати шлях атаки у вигляді графу і застосувати до нього кількісну модель часу компрометації.

1.2.2 Відомі інциденти на українській енергосистемі

Українська енергосистема залишається найдетальніше задокументованим у відкритих джерелах об'єктом реальних кібератак на ICS. Далі проаналізовано три ключові інциденти у хронологічному порядку.

Атака BlackEnergy 2015 – перша у світі підтверджена кібератака, що призвела до відключення електропостачання реальних споживачів. 23 грудня 2015 року три українські обленерго зазнали скоординованої кібератаки [12]. За даними звіту E-ISAC і SANS ICS, зловмисники почали свою діяльність ще навесні 2015 року, тобто за понад шість місяців до виконання атаки [12]. Первинне проникнення здійснено через цільову розсилку шкідливих Microsoft Office-документів з BlackEnergy 3, які доставлялися електронною поштою співробітникам ІТ-мереж компаній [12]. Після закріплення у мережі зловмисники викрали облікові дані, виявили VPN-з'єднання до ICS-мережі та використали їх для отримання доступу до SCADA-робочих станцій. У результаті атаки зловмисники через НМІ вручну відкривали вимикачі на 30 підстанціях рівня напруги 35 кВ та 110 кВ. Одночасно завантажувалася шкідлива прошивка у конвертори serial-to-Ethernet на підстанціях. Це робило неможливим повернення системи до стандартного режиму після відновлення робочих станцій (за висловом авторів звіту – «blowing the bridges»). Додатково проти кол-центру одного з обленерго проведено телефонну DoS-атаку, що ускладнювало приймання повідомлень від абонентів. Інцидент знеструмив приблизно 225 000 споживачів на кілька годин, а обленерго ще тривалий час оперували у режимі ручного керування [12]. Між першим проникненням навесні 2015 року і моментом виконання атаки у грудні минуло понад шість місяців, упродовж яких системи захисту не виявили присутність зловмисника [12].

У грудні 2016 року під час атаки на українську енергосистему було використано шкідливе програмне забезпечення Industroyer (CrashOverride). Industroyer став першим публічно задокументованим шкідливим програмним забезпеченням, здатним безпосередньо керувати комутаційним обладнанням

електричних підстанцій через стандартні промислові протоколи [14]. На відміну від BlackEnergy, що використовував людський оператор для взаємодії з HMI, Industroyer самостійно взаємодівав з обладнанням підстанції через промислові протоколи IEC 60870-5-101, IEC 60870-5-104, IEC 61850 та OPC DA [14]. У термінах моделі ICS Cyber Kill Chain це означало якісне ускладнення Stage 2, оскільки виявлення такої активності вимагає не моніторингу аномальної поведінки користувачів, а саме аналізу трафіку промислових протоколів.

Далі у 2022 році було вдосконалено версію до Industroyer2, яка орієнтована виключно на протокол IEC 60870-5-104. Параметри атаки, зокрема IP-адреси цільових пристроїв і послідовність команд, були заздалегідь вшиті у бінарний файл [15]. Це свідчить про попередню детальну розвідку конкретної мережі – результат тривалої роботи на Stage 1 моделі SANS. Атака мала на меті відключення електропостачання у воєнних умовах, проте була виявлена та нейтралізована CERT-UA спільно з ESET до її повної реалізації [15]. Цей випадок підтверджує практичну можливість зупинення атаки до завдання фізичної шкоди за умови раннього виявлення.

1.3 Час як ключовий ресурс кіберзахисту енергооб'єкта

Аналіз інцидентів, які наведені у попередньому підрозділі, виявляє асиметрію між зловмисником і захистом у питанні часу. Для зловмисника час підготовки атаки – це інвестиція в результат. Чим довша розвідка, тим вища ймовірність успіху на третьому етапі. Для захисту, навпаки, час між моментом первинного проникнення і моментом реалізації атаки виступає ресурсом, упродовж якого можна виявити присутність зловмисника, локалізувати її і нейтралізувати до того, як буде завдана фізична шкода обладнанню.

Документована тривалість підготовчої фази багатоетапних атак (так званий dwell time) на об'єктах критичної енергетичної інфраструктури вимірюється не годинами чи днями, а місяцями. Більше того, у звіті Mandiant M-Trends 2026 [13] окремо наголошується на тенденції до багаторічних вторгнень (multi-year

intrusions), що демонструють екстремальну стійкість (extreme persistence) зломисників у цільових мережах, зокрема на об'єктах критичної інфраструктури, ядром якої є енергетичний сектор. Такий тривалий час прихованого перебування перед переходом до активних дій в ОТ-сегменті підтверджує, що dwell time варто розглядати як ключову та кількісно керовану характеристику системи захисту енергооб'єкта.

З наведеного впливає логіка захисту мережі енергооб'єкта, що формує методологічну основу даного дослідження.

Перше твердження стосується ієрархії потенційних втрат. Потенційні втрати від кібератаки зростають з кожним наступним етапом її розгортання. Інцидент, зупинений на першому етапі, обмежується ІТ-наслідками: компрометацією робочих станцій, можливим витоком даних, але без фізичного впливу на енергооб'єкт. Інцидент, дозволений до другого етапу, додає ризики компрометації даних про конфігурацію ОТ-обладнання та можливості подальшого розвитку атаки. А вже інцидент, який досяг третього етапу, призводить до прямих фізичних наслідків, наприклад відключень споживачів, пошкоджень обладнання, аварійних режимів. Кожний крок зломисника в напрямі ОТ-сегмента означає експоненційне зростання потенційних втрат.

Друге твердження стосується принципу раннього зупинення зломисника. Ефективність захисту визначається тим, наскільки рано зломисник буде зупинений на шляху від точки проникнення до цільових підстанцій через диспетчерський SCADA-центр. Принцип зупинення зломисника на рівні периметру або у SCADA LAN до того, як він досягне польового ОТ-рівня, є фундаментальним для архітектури захисту критичної інфраструктури і прямо впливає з ієрархії потенційних наслідків. Цей принцип лежить в основі рекомендацій NIST SP 800-82 [1] щодо сегментації мережі, систем виявлення вторгнень (IDS) та принципу defense-in-depth для ICS-середовищ.

Третє твердження стосується потреби у кількісній оцінці. Для практичної реалізації принципу раннього зупинення потрібно мати кількісну оцінку часу, який вона матиме на реагування для конкретної конфігурації мережі і конкретного типу зломисника. Без такої оцінки неможливо ні раціонально

планувати процедури реагування на інциденти (Incident Response Plan, IRP), ні пріоритизувати заходи захисту, ні обґрунтувати бюджет на засоби моніторингу. Якісних експертних оцінок недостатньо для прийняття обґрунтованих інженерних рішень.

З наведених тверджень випливає запит, що визначає мету даної роботи – розроблення моделі, яка для заданої архітектури мережі енергооб’єкта і заданих характеристик зломисника дозволяє кількісно оцінити очікуваний час від моменту первинного проникнення до моменту досягнення цільової підстанції ОТ-рівня через диспетчерський SCADA-центр. Така модель створює основу для прийняття інженерних рішень з мінімізації потенційних втрат від багатоетапних кібератак на об’єкти критичної енергетичної інфраструктури.

1.4 Методи кількісного оцінювання часу компрометації ICS-мереж

Інженерний запит, сформульований у попередньому підрозділі, ставить чіткі вимоги до математичного апарату моделі. Він має враховувати характеристики наявних вразливостей у вузлах мережі, рівень кваліфікації зломисника, структуру можливих шляхів атаки та параметри захищеності окремих сегментів. За останні два десятиріччя у науковій літературі сформувалося кілька підходів до розв’язання цієї задачі. Умовно їх можна розділити на три групи: структурні (графи атак), імовірнісні (байєсівські мережі) та часові (моделі Time-to-Compromise). У межах цього огляду основна увага зосереджена на часових моделях, оскільки саме вони ключові для поставленої задачі.

Метод графів атак дозволяє автоматично побудувати орієнтований граф можливих шляхів атаки за вхідним описом топології мережі та переліком CVE-вразливостей. Найвідомішою реалізацією методу є інструмент MulVAL [19]. На даний момент він є фактичним стандартом для логічного аналізу вразливостей мереж [20]. Перевагою підходу є повна автоматизація; проте обмеженням є відсутність часової оцінки. Граф атак показує, який шлях існує, але не відповідає на питання, протягом якого часу він буде пройдений. Для поставленої задачі граф

атак виступає необхідним структурним компонентом, проте недостатнім для отримання повної відповіді.

Байєсівські граfi атак доповнюють метод графів імовірнісним компонентом. Кожному вузлу графу ставиться у відповідність таблиця умовних ймовірностей, апіорні значення яких визначаються на основі метрик CVSS [21]. У роботі [10] такий підхід застосовано до інформаційно-телекомунікаційної мережі енергооб'єкта. У ній отримано ймовірності реалізації атаки на RTU від 1 % до 78 % залежно від конфігурації захисту. Метод відповідає на питання про ймовірність компрометації, але часової оцінки не дає.

Модель Time-to-Compromise (TTC), запропонована McQueen et al. у 2005 році [16], стала першою систематичною спробою введення часу у моделювання кіберзагроз. Дії зловмисника представлено як суперпозицію трьох взаємовиключних процесів: використання вже наявного публічного експлойта (Процес 1), самостійна розробка експлойта (Процес 2) та очікування появи нової вразливості (Процес 3). Класична модель McQueen стала основою для значної кількості подальших досліджень. Однак при безпосередньому застосуванні до промислових систем вона виявляє суттєве обмеження, модель була розрахована на загальну базу CVE з переважанням ІТ-вразливостей.

Розширення β -TTC, запропоноване у роботі [22], усуває деякі математичні неточності оригінальної формули та диференціює вразливості за компонентами СІА-тріади. Проте це розширення працює лише на рівні окремого вузла і не враховує багатостадійної природи реальних атак.

Модель TTCICS була запропонована Rencelj Ling та Ekstedt у 2023 році [23]. Автори використали спеціалізований датасет ІCS-вразливостей RITICS та оновили параметри моделі McQueen під специфіку промислових систем. Завдяки цій адаптації модель уперше дала кінцеві значення часу компрометації для типових ІCS-активів для чотирьох рівнів кваліфікації зловмисника. Водночас ця модель зберігає ключове обмеження оригінальної моделі. Вона обчислює час лише для окремого вузла, а для повного шляху атаки пропонує просте підсумовування часів окремих вузлів, що ігнорує специфіку багатостадійних атак.

Поєднання TTC з марківськими ланцюгами, реалізоване у роботах [24] та [25], дозволяє агрегувати характеристики по мережі і оцінити середній час компрометації мережі (Mean Time-to-Compromise, MTTC). Розширення цього підходу через напівмарківський процес [26] усуває обмеження експоненційного припущення про розподіл часу та емпірично встановлює, що розподіл MTTC у задачах кібербезпеки SCADA найкраще описується гамма-розподілом. Спільним обмеженням цих агрегаційних методів є те, що вони працюють зі значеннями TTC окремих вузлів, і не модифікують їх з урахуванням позиції вузла на шляху атаки.

Узагальнений порівняльний аналіз розглянутих методів наведено у таблиці 1.1.

Таблиця 1.1 – Порівняльний аналіз методів оцінювання захищеності ICS-мереж

Метод	Кількісний результат	Основне обмеження	Джерело
Граф атак (MulVAL)	Структура шляхів атаки	Немає часової та ймовірнісної оцінки	[19]
Байєсівський граф атак	Ймовірність компрометації	Немає часової оцінки	[10, 21]
TTC (McQueen)	Час компрометації окремого вузла	Не адаптовано для ICS; одновузловий	[16]
β -TTC	Уточнений час окремого вузла	Не враховує накопичення привілеїв	[22]
TTCICS	Час компрометації ICS-вузла	Просте підсумовування для шляху; ігнорує латеральний рух	[23]
MTTC + марківський ланцюг	Середній час для мережі	Експоненційне припущення про розподіл	[24, 25]
SMP + MCMC	Розподіл MTTC	Не модифікує TTC окремих вузлів за позицією у графі	[26]

Порівняльна таблиця виявляє ключову прогалину у наявних підходах. Жоден з них не виконує коригування часу компрометації окремого вузла залежно від його позиції на шляху атаки. Класична модель ТТС та її адаптації оперують вузлами як ізольованими об'єктами. Агрегаційні марківські та напівмарківські моделі підсумовують або інтегрують отримані ТТС, проте не коригують їх з урахуванням попередньої компрометації мережі. Водночас реальні багатоетапні атаки демонструють зовсім іншу картину. Після компрометації першого вузла зломисник отримує облікові дані, сесійні токени, знання топології і внутрішніх сервісів, у результаті чого подальша атака суттєво прискорюється. Атака на другий вузол після успішної компрометації першого займає значно менше часу, ніж та сама атака без попереднього доступу. Просте підсумовування ТТС окремих вузлів цей ефект ігнорує і дає систематично завищений час компрометації. Для практичних рекомендацій з реагування на інциденти це означає необґрунтовано оптимістичні оцінки захисного часу.

Висновки до розділу 1

За результатами аналізу, проведеного у першому розділі, сформульовано наступні узагальнення.

Охарактеризовано мережу автоматизованої підстанції як кіберфізичну систему з ієрархією наслідків інцидентів, у якій компрометація ОТ-сегмента призводить до прямих фізичних наслідків, тоді як ІТ-сегмент є основним каналом первинного проникнення. Така структура визначає ОТ-сегмент як цільову зону, а ІТ-сегмент – як простір, у якому ефективні захисні заходи мають максимальний потенціал зупинення зломисника.

На основі аналізу документованих інцидентів BlackEnergy, Industroyer та Industroyer2 встановлено трирівневу структуру багатоетапної атаки на енергооб'єкт: проникнення в ІТ-периметр, латеральний рух з накопиченням привілеїв, взаємодія з пристроями керування фізичним обладнанням. Тривалість підготовчої фази, що вимірюється місяцями, утворює часове вікно реагування,

кількісна оцінка якого є передумовою раціональної пріоритизації захисних заходів.

Проведено порівняльний аналіз наявних моделей кількісного оцінювання часу компрометації, а саме моделей McQueen TTC, TTCICS, β -TTC. Виявлено чотири методологічні обмеження TTCICS: змішування метрик CVSS v2 і v3, ігнорування поля Attack Vector вектора CVSS v3, артефакт MTBV=0 та ігнорування накопичення привілеїв при латеральному русі. Останнє з них є критичним для багатоетапних атак і не усувається наявними розширеннями моделі. Це зумовлює доцільність розроблення моделі, яка враховує накопичений злоумисником контекст на шляху до цільового вузла – модель TTCAG.

2 ФОРМАЛЬНА МОДЕЛЬ TTCAG

У попередньому розділі обґрунтовано потребу у кількісній оцінці часу, який зловмисник витрачає на проходження шляху від точки входу в ІТ-сегмент цільового ОТ-вузла (підстанції) через диспетчерський SCADA-центр керування. У даному розділі побудовано формальну модель такої оцінки – TTCAG (Attack-Graph aware Time-to-Compromise). Модель спирається на класичну концепцію Time-to-Compromise McQueen [16] і успадковує її стохастичну природу, що час компрометації трактується як випадкова величина. Зміст розділу охоплює опис базової моделі та трьох розподілів часу, на яких вона ґрунтується; аналіз обмежень моделі при її застосуванні до багатоетапних атак; формальний апарат запропонованої моделі TTCAG; обґрунтування числових значень її параметрів через офіційну специфікацію CVSS v3.1 [27]; аналіз повної функції щільності розподілу TTCAG.

2.1 Базова модель часу компрометації TTC McQueen

2.1.1 Концепція трьох процесів зловмисника

Модель Time-to-Compromise, запропонована McQueen, Boyer, Flynn і Beitel у роботі Idaho National Laboratory [16], – перша спроба формального кількісного опису часу компрометації окремого вузла як випадкової величини. Автори ввели припущення, що дії зловмисника, спрямовані на експлуатацію вразливостей вузла, можна представити як суперпозицію трьох взаємовиключних сценаріїв.

Процес 1. Зловмисник має готовий публічний експлойт для однієї з відомих вразливостей цільового вузла. Це найшвидший сценарій атаки, оскільки компрометація зводиться до конфігурування і запуску готового інструмента.

Процес 2. Зловмисник знає про існування вразливості, проте готового експлойта для неї немає. Доводиться розробляти його самостійно. Такий сценарій

моделюється послідовністю незалежних спроб з певною ймовірністю успіху для кожної.

Процес 3. Жодна з відомих вразливостей не придатна для експлуатації цим зловмисником, тому він очікує появи нової вразливості. Після її появи зловмисник переходить до Процесу 2 і починає її експлуатацію.

Три процеси утворюють повну класифікацію можливих сценаріїв дій зловмисника. Реальна атака реалізується за одним із них залежно від рівня кваліфікації зловмисника та стану бази відомих вразливостей цільового вузла.

Особливість моделі McQueen полягає у тому, що час кожного з трьох процесів моделюється як випадкова величина зі своїм законом розподілу ймовірностей. Це робить модель статистично обґрунтованою і дозволяє характеризувати не лише середнє значення часу компрометації, але й, у принципі, його повну ймовірнісну характеристику. Далі детально розглянуто, який саме розподіл обрано для кожного процесу і чому.

2.1.2 Розподіл часу для Процесу 1: β -розподіл

Для опису часу Процесу 1 у роботі [16] обрано β -розподіл. Це двопараметричний неперервний розподіл з обмеженим діапазоном носія. Вибір саме β -розподілу зумовлений двома обставинами. По-перше, β -розподіл широко застосовується у моделях надійності та проєктному управлінні (зокрема, у методі PERT) для опису часу простих однокрокових дій з невизначеною тривалістю. По-друге, його щільність має характерну форму асиметричного піку – близька до нуля на початку діапазону, швидко зростає до максимуму у перших днях, а потім поступово спадає до нуля при наближенні до верхньої межі. Така форма відповідає природі Процесу 1, оскільки у переважній більшості випадків зловмисник з готовим експлойтом здійснює компрометацію за лічені години-дні, а довгі затримки малоімовірні.

Параметри розподілу обрано як $\alpha=1,3$ і $\beta=5,2$ на діапазоні $[0; 5]$ днів таким чином, щоб математичне сподівання дорівнювало одному дню. Калібрування у

один день обґрунтовано у [16] двома незалежними емпіричними джерелами. Jonsson показав, що команда з двох непрофесійних учасників витрачала в середньому близько чотирьох годин на компрометацію навчальної системи. Cohen припустив, що для підготовки серйозної атаки досвідченому зловмиснику потрібно декілька днів. Один робочий день є значенням, що узгоджується з обома оцінками, і характеризує типовий випадок експлуатації відомого експлойта [16].

Ймовірність того, що зловмисник перебуває у Процесі 1, обчислюється за формулою [16]:

$$P_1 = 1 - e^{(-V \cdot m/k)} \quad (2.1)$$

де V – кількість відомих вразливостей компонента; m – кількість експлойтів, доступних зловмиснику даного рівня кваліфікації (50/150/250/450); k – загальна кількість CVE у базі ICAT ($k = 9447$).

На рисунку 2.1 зображено функцію щільності β -розподілу з параметрами $\alpha=1,3$; $\beta=5,2$ на діапазоні $[0; 5]$ днів.

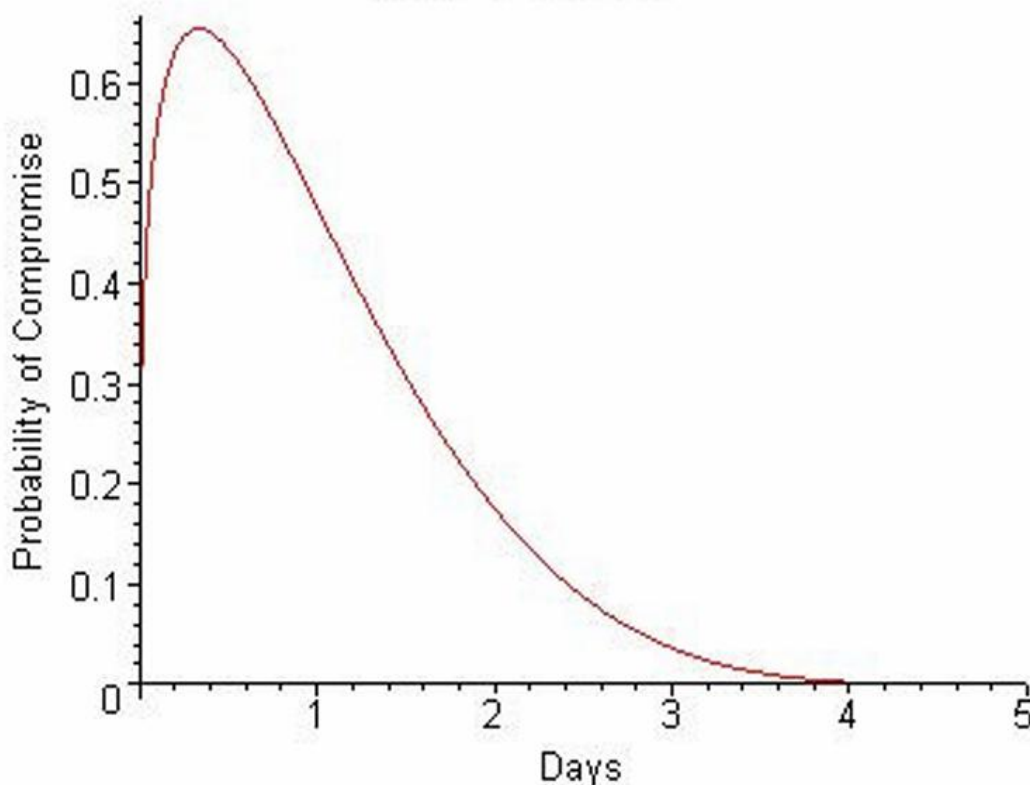


Рисунок 2.1 – Функція щільності β -розподілу часу Процесу 1 (за McQueen [16])

2.1.3 Розподіл часу для Процесу 2 – гамма-розподіл

Для опису Процесу 2 у роботі [16] обрано гамма-розподіл. Вибір обґрунтовано тим, що функція щільності гамма-розподілу дорівнює нулю в точці $t=0$, зростає до максимуму, а потім асимптотично спадає до нуля, але ніколи його не досягає. Така форма підходить до опису Процесу 2, тому що миттєва компрометація неможлива, а успіх не гарантований у межах будь-якого скінченного часу. Базове середнє значення PDF для Процесу 2 вибране як середній час від оголошення вразливості до появи відповідного коду експлойту, який, за даними Symantec Internet Security Threat Report (2004), становить 5,8 дні.

Ця базова PDF відповідає ідеальному випадку, коли зловмисник знаходить придатну вразливість з першої спроби. У загальному випадку зловмисник послідовно перебирає відомі вразливості. На кожній ітерації він обирає одну невипробовану вразливість і намагається знайти або написати для неї експлойт. Кожна така спроба тривалістю 5,8 дня є незалежною, а її результат залежить від того, чи належить обрана вразливість до категорії експлуатованих для даного рівня кваліфікації зловмисника. Очікуваний час Процесу 2 обчислюється як:

$$t_2 = 5,8 \cdot ET \quad (2.2)$$

де ET – очікувана кількість спроб, що визначається за формулою:

$$ET = \frac{AM}{V} \cdot \left(1 + \sum_{tries=2}^{V-AM+1} \left[tries \cdot \prod_{i=2}^{tries} \frac{NM-i+2}{V-i+1} \right] \right) \quad (2.3)$$

де AM – середня кількість вразливостей, для яких зловмисник даного рівня кваліфікації може знайти або розробити робочий експлойт; $NM = V - AM$ – кількість вразливостей, недоступних для даного рівня; V – загальна кількість відомих вразливостей компонента.

Вразливість відноситься до рівня Novice, якщо для неї не потрібен код або він тривіальний у використанні. Згідно з дослідженням у роботі [16] цьому критерію відповідали 3 з 20 вразливостей (15%). До рівня Beginner додавали вразливості з доступним і легкозрозумілим кодом – ще 3 пари, тобто разом 6 (30%). До рівня Intermediate відносили випадки зі складним для розуміння кодом

або лише прикладами реалізації – ще 5 пар, разом 11 (55%). Решта 9 вразливостей, для яких код був відсутній або потребував суттєвого доопрацювання, доступні лише Expert (100%).

Для рівня Expert очікувана кількість спроб дорівнює 1. Зі зниженням рівня кваліфікації ЕТ зростає, оскільки менш досвідчений зломисник у середньому потребує більше спроб до першого успіху.

Ймовірність того, що зломисник перебуває у Процесі 2, є доповненням до ймовірності Процесу 1:

$$P_2 = 1 - P_1 = e^{-v \cdot m/k} \quad (2.4)$$

оскільки Процес 1 і Процес 2 є взаємовиключними при $V > 0$.

На рисунку 2.2 зображено базову функцію щільності імовірності для Процесу 2 – гамма-розподіл з параметрами форми 2 і 2,9 та математичним сподіванням 5,8 дня. Ця базова PDF відповідає випадку, коли зломисник знаходить придатну вразливість з першої спроби. При збільшенні очікуваної кількості спроб ЕТ форма розподілу модифікується відповідно, проте гамма-характер зберігається.

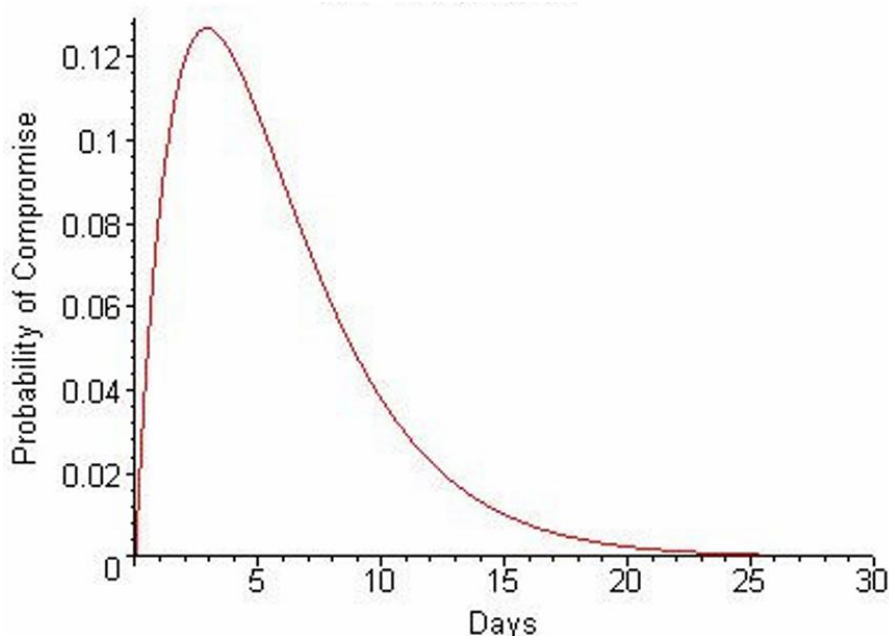


Рисунок 2.2 –Базова функція щільності імовірності для Процесу 2. (за McQueen [16])

2.1.4 Розподіл часу для Процесу 3: експоненційний розподіл

Для опису Процесу 3 у роботі [16] обрано експоненційний розподіл. Якщо появи нових вразливостей є рідкісними незалежними подіями, що відбуваються з постійною середньою інтенсивністю, то їх послідовність утворює пуассонівський потік, а інтервали між сусідніми подіями підпорядковуються експоненційному закону розподілу. Це класичний результат теорії ймовірностей. Він застосовується у багатьох предметних областях для моделювання часу до появи незалежних рідкісних подій, зокрема, у задачах надійності технічних систем та теорії масового обслуговування.

Функція щільності експоненційного розподілу часу Процесу 3 має вигляд:

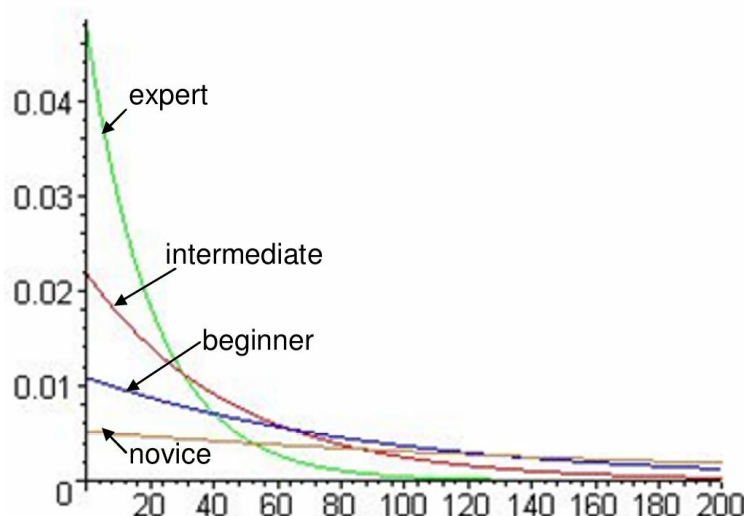
$$f_{T_3}(t) = \frac{1}{MTBV} \cdot e^{-t/MTBV}, t \geq 0 \quad (2.5)$$

де $MTBV$ – середній час між появою нових вразливостей.

Оскільки зловмисник може використовувати лише частку V/AM вразливостей, математичне сподівання часу Процесу 3 коригується масштабним коефіцієнтом:

$$t_3 = E[T_3] = \left(\frac{V}{AM} - 0,5 \right) \cdot MTBV + \tau \quad (2.6)$$

де τ – середній час від оголошення вразливості до появи експлойта.



**Рисунок 2.3 – Функція щільності експоненційного розподілу часу Процесу 3
(за McQueen [16])**

2.1.5 Очікуваний час компрометації за моделлю McQueen

Об'єднання трьох процесів за формулою повної ймовірності дає очікуваний час компрометації вузла як зважену суму математичних сподівань трьох процесів зі своїми ймовірностями реалізації:

$$T = t_1 \cdot P_1 + t_2 \cdot (1 - P_1) \cdot (1 - u) + t_3 \cdot u \cdot (1 - P_1) \quad (2.7)$$

де T – очікуване значення часу компрометації; t_1 – очікуване значення Процесу 1 (1 день); t_2 – очікуване значення Процесу 2 згідно з формулою (2.2); t_3 – очікуване значення Процесу 3 згідно з формулою (2.3); $u = (1 - (AM/V))^V$ – ймовірність того, що Процес 2 є невдалим ($u = 1$ при $V = 0$); V – кількість відомих вразливостей; P_1 – згідно з формулою (2.1); $AM/V = f$ – згідно з Таблицею 2.1.

Для подальших розрахунків у роботі [16] використано лише математичні сподівання трьох процесів, а не їхні повні функції щільності. Це методологічне рішення робить аналіз обчислювально простим, але приховує цінну інформацію про дисперсію часу компрометації та його довірчі інтервали. У підрозділі 2.6 даного розділу повний розподіл TTCAG розглянуто як суперпозицію розподілів окремих процесів, що дозволяє повернути цю інформацію у явний вигляд.

2.2 Адаптація моделі для ICS-середовища – TTCICS

Класичну модель McQueen [16] розраховано на загальну базу CVE, до якої входили переважно вразливості ІТ-систем. У роботі Rencelj Ling та Ekstedt [23] показано, що статистичні характеристики ICS-вразливостей суттєво відрізняються від загальних. Вони мають нижчу частоту появи через відносно невелику кількість виробників промислового обладнання, інший розподіл за критичністю та інший середній час до публікації функціональних експлойтів. Тому пряме застосування параметрів моделі McQueen до ICS-середовища дає некоректні

результати, і потрібна окрема адаптація моделі під специфіку промислових систем.

У роботі [23] запропоновано модель TTCICS. Її ключові відмінності від оригінальної моделі McQueen полягають у такому. Замість загальної бази CVE ($k = 9447$ у [16]) використано спеціалізований ICS-датасет RITICS з $k = 2740$ вразливостей, релевантних для промислових систем керування. Значення часу t_2 для різних рівнів кваліфікації перераховано на основі статистики появи функціональних експлойтів саме для ICS-вразливостей. Значення $f=AM/V$ перевизначено на основі експертного аналізу ICS-CVE з датасету RITICS.

Числові значення параметрів моделі TTCICS для чотирьох рівнів кваліфікації зловмисника наведено у таблиці 2.1.

Таблиця 2.1 – Параметри рівнів навички зловмисника у моделі TTCICS [23]

Рівень навички	Частка f	t_2 (дні)	Діапазон CVSS exploitability
Novice	0,05	37	0,1 – 1,2
Beginner	0,24	27	0,1 – 2,1
Intermediate	0,50	16	0,1 – 3,0
Expert	1,00	6	0,1 – 3,9

Параметр MTBV у моделі TTCICS, на відміну від моделі McQueen, розраховується індивідуально для кожного активу та типу вразливості з реальних дат публікації CVE у відсортованому списку. У даній роботі для уточнення MTBV використано дані NVD, CISA KEV та CISA CSAF за період 2020–2025 р., що відображає сучасний стан ICS-вразливостей значно точніше за оригінальний датасет RITICS, обмежений 2020 роком.

2.3 Обмеження моделі TTCICS для багатоетапних атак

Під час аналізу моделі TTCICS до реальних мереж об'єктів критичної енергетичної інфраструктури було виявлено чотири методологічних обмеження.

У роботі [28], що стала апробацією результатів дипломної роботи, ці обмеження були послідовно проаналізовані як основа для побудови моделі TTCAG.

1. Змішування метрик CVSS v2 і v3 у одній формулі. Параметр CVSS у моделі McQueen використовується для оцінки складності експлуатації вразливості. Проте за двадцять років після виходу оригінальної моделі стандарт CVSS зазнав значної еволюції. Версія v3.0 була прийнята у 2015 році, а v3.1 – у 2019 році [27]. У CVSS v3 введено принципово нові поля – Privileges Required (PR), User Interaction (UI), розширений Attack Vector з чотирма значеннями замість трьох. У сучасних базах NVD та RITICS значна частина CVE має оцінки тільки за v2, частина – за v3, тож їхнє пряме арифметичне поєднання у одній формулі є некоректним з точки зору стандартизації [27].

2. Ігнорування фактичних умов експлуатації вразливості. У моделі TTCICS вразливості з однаковим числовим значенням базової оцінки CVSS отримують однаковий очікуваний час компрометації. При цьому неважливо, чи можуть вони бути використані дистанційно з мережі, з сусіднього сегмента, з локальної консолі або через фізичний доступ. Поле Attack Vector, що є найважливішим індикатором зручності експлуатації для багатоетапної атаки, у формулі TTCICS повністю ігнорується [28].

3. Некоректна обробка випадку $MTBV = 0$. Параметр MTBV у TTCICS розраховується з дат публікації відомих CVE для конкретного активу. Якщо для певного активу всі відомі CVE опубліковано в один день, то MTBV формально дорівнює нулю. У такому випадку формула t_3 спрощується до $t_3 = 5,8$ дня, що робить третій процес McQueen малозначущим і не відповідає реальній динаміці поширення вразливостей [28].

4. Ігнорування накопичення привілеїв при латеральному русі. Це найважливіше з точки зору моделювання багатоетапних атак обмеження. Класична TTCICS дає оцінку для одного вузла. Для повного шляху атаки автори моделі пропонують просте підсумовування ТТС всіх вузлів цього шляху. Проте такий підхід некоректний з огляду на динаміку реальних атак. Після компрометації першого вузла зловмисник отримує облікові дані, сесійні токени, знання про топологію мережі та внутрішні сервіси. Атака на другий вузол займає

значно менше часу, ніж атака на той самий вузол без попередньої компрометації мережі. Просте підсумовування TTC ігнорує цей ефект, що призводить до систематичного завищення часу компрометації [28].

Усунення цих чотирьох обмежень становить мету моделі TTCAG.

2.4 Формальний апарат моделі TTCAG

Модель TTCAG (Attack-Graph aware Time-to-Compromise) реалізується як дворівнева структура. На рівні окремого вузла усуваються методологічні обмеження 1-3 через введення додаткових множників у формулу очікуваного часу, а саме вагового коефіцієнта AV_w для поля Attack Vector та скоригованого параметра MTBV b^* . На рівні шляху атаки усувається обмеження 4 шляхом введення коефіцієнта глибини шляху γ . Цей коефіцієнт залежить від поля Privileges Required CVSS v3 і моделює прискорення атаки внаслідок накопичення зломисником привілеїв з попередніх компрометованих вузлів.

2.4.1 Виправлений час процесу P_1 для окремого вузла

Для усунення обмежень 1 і 2 у моделі TTCAG введено виправлений час процесу P_1 [28]:

$$t_1^*(h_i) = \frac{t_{1,base}}{CVSS_{norm}(h_i) \cdot AV_w(h_i)} \quad (2.8)$$

де $t_{1,base}=2$ дні – базовий час процесу P_1 ; $CVSS_{norm}(h_i) \in [0; 1]$ – базова оцінка CVSS, нормована діленням на 10, з пріоритетом версії v3.1 над v2; $AV_w(h_i)$ – ваговий коефіцієнт вектора атаки за CVSS v3.1, числові значення якого обґрунтовуються у підрозділі 2.5.

За даними Dragos OT Red Team Services [34], типова тривалість ICS-пентесту становить 5-10 днів на 4-6 критичних вузлів цільової мережі, що дає 1-2,5 діб на вузол як емпіричний еталон активного часу компрометації. У моделі TTCAG прийнято $t_{1,base}=2$ діб як середнє значення цього діапазону, що відповідає

також Mandiant M-Trends 2026 [13] (5-7 діб для IT) з врахуванням ICS-модифікатора через Stage 2 ICS Cyber Kill Chain (Assante & Lee, SANS 2015).

Логіка формули (2.8) у тому, що чим вища нормована оцінка CVSS і чим вищий ваговий коефіцієнт AV_w , тим легше зловмиснику експлуатувати вразливість і тим менший очікуваний час процесу P_1 . Для вразливостей з нижчою CVSS-оцінкою або менш зручним вектором атаки час P_1 пропорційно зростає.

Для усунення обмеження 3 у моделі TTCAG введено скоригований параметр MTBV [28]:

$$b^*(h_i) = \max(b(h_i), \bar{b}_{cat}) \quad (2.9)$$

де $b(h_i)$ – індивідуальне значення MTBV, розраховане з дат публікації CVE конкретного активу; $\bar{b}_{cat}$ – середнє значення MTBV для вразливостей тієї самої категорії за всією базою NVD. При $b(h_i) = 0$ у формулу підставляється категорійне середнє, що запобігає некоректному спрощенню формули і зберігає внесок Процесу 3 у повному обсязі.

Об'єднання виправленого часу t^*_1 і скоригованого параметра b^* дає вдосконалену формулу TTC для окремого вузла:

$$TTC^*(h_i) = t^*_1(h_i) \cdot P_1 + t_2 \cdot P_2 \cdot (1 - u) + t_3(b^*) \cdot P_3 \quad (2.10)$$

де $P_2 = 1 - P_1$; $P_3 = u \cdot (1 - P_1)$ – імовірність того, що Процес 2 виявився невдалим і зловмисник перебуває у Процесі 3, $t_3(b^*) = (V/AM - 0,5) \cdot b^*(h_i) + 5,8$ – час третього процесу McQueen, де V – кількість CVE компонента, AM – кількість вразливостей, доступних зловмиснику даного рівня, використано b^* замість оригінального b у формулі для t_3 ; інші параметри визначено як у формулах (2.1) і (2.4).

2.4.2 Коефіцієнт глибини шляху γ

Для усунення обмеження 4 у моделі TTCAG створено коефіцієнт глибини шляху γ . Він знижує очікуваний час атаки кожного наступного вузла на шляху внаслідок накопиченого зловмисником контексту з попередніх вузлів [28].

Значення γ залежить від поля Privileges Required (PR) вектора CVSS v3. Такий підхід методологічно коректно відображає те, що прискорення залежить від типу привілеїв, потрібних для експлуатації.

Для лінійного шляху атаки $ap = \langle h_1, h_2, \dots, h_n \rangle$ загальна формула TTCAG має вигляд:

$$TTC_{AG}(ap) = TTC^*(h_1) + \sum_{i=2}^n TTC^*(h_i) \cdot \prod_{j=1}^{i-1} \gamma(h_j) \quad (2.11)$$

Перший вузол h_1 атакується без накопиченого контексту, тому його час компрометації входить у суму у повному обсязі. Для кожного наступного вузла h_i час коригується накопиченим добутком коефіцієнтів γ усіх попередніх вузлів $h_1 \dots h_{i-1}$. Добуток відображає реальне накопичення привілеїв при латеральному русі зловмисника через попередні вузли шляху. При PR=None на всіх вузлах $\gamma=1,0$, і формула (2.11) зводиться до простого підсумовування. Це означає, що TTCICS є частковим випадком TTCAG.

2.4.3 Обчислення TTCAG для графу атак з декількома шляхами

У реальних мережах об'єктів критичної енергетичної інфраструктури до цільового вузла ОТ-рівня (підстанції чи RTU) зазвичай ведуть декілька шляхів атаки, які можуть мати спільні проміжні вузли. Формула (2.11) є коректною для лінійного шляху, проте не описує випадку, коли граф атак є орієнтованим ациклічним графом з розгалуженнями.

Для вирішення цієї задачі у роботі [29] запропоновано використовувати структуру даних compromise graph. Це орієнтований граф, у якому вузли представляють стани атаки, а ребра представляють переходи між станами з очікуваним часом компрометації як вагою. Ребра класифікуються за типом компрометації: Reconnaissance, Breach, Penetrate, Escalate і Damage. Dominant attack path визначається як шлях з мінімальним накопиченим часом, оскільки мінімальний час компрометації відповідає максимальному ризику [29].

У моделі TTCAG використано аналогічний підхід з урахуванням коефіцієнта глибини γ . На відміну від [29], де пошук домінантного шляху

виконується вручну для конкретного графа, у моделі TTCAG введено рекурсивну формулу для довільного вузла h_j :

$$TTC_{AG}(h_j) = \min_{l \in Pa(h_j)} \left[TTC_{AG}(h_l) + TTC^*(h_j) \cdot \gamma(h_j)^{d_l(h_j)-1} \right] \quad (2.12)$$

де $Pa(h_j)$ – множина безпосередніх попередників вузла h_j у графі атак; $d_j(h_j)$ – глибина вузла h_j на шляху що проходить через попередника h_l ; для початкового вузла $TTC_{AG}(h_1) = TTC^*(h_1)$.

Зміст формули (2.12) полягає в тому, що зломисник обирає найшвидший шлях до кожного проміжного вузла. Такий підхід враховує наступні важливі аспекти. Спільні проміжні вузли компрометуються лише один раз, а не повторно для кожного шляху, також паралельні шляхи розглядаються як альтернативи, з яких обирається оптимальна. Формула (2.12) обчислюється стандартним обходом DAG.

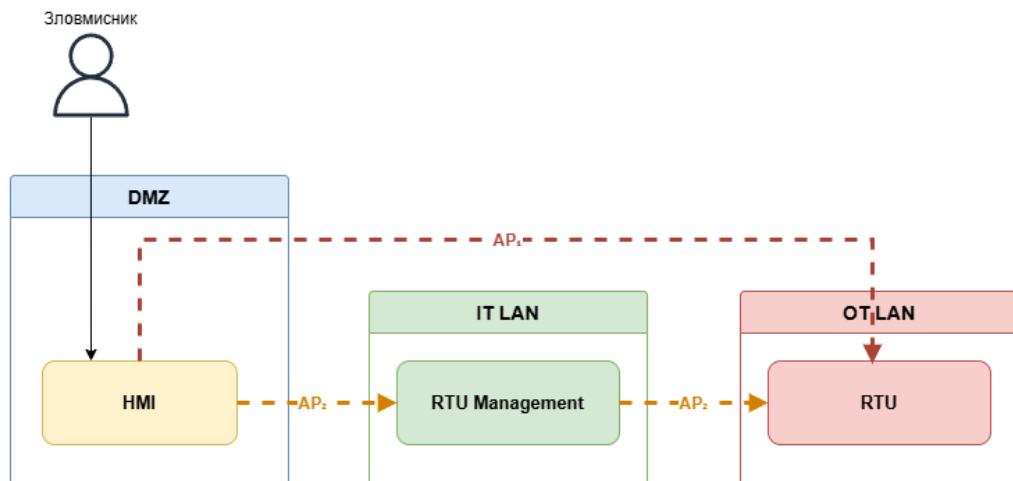


Рисунок 2.4 – Приклад графу атак з декількома шляхами до цільового вузла RTU

2.5 Обґрунтування числових значень параметрів моделі TTCAG

Числові параметри AV_w і γ моделі обґрунтовано експертними оцінками. Їх отримано через методичний аналіз офіційних коефіцієнтів специфікації CVSS v3.1, наведених у документі Forum of Incident Response and Security Teams [27]. Таке обґрунтування забезпечує узгодженість параметрів моделі з міжнародним стандартом CVSS і можливість їх верифікації незалежним аналітиком.

2.5.1 Офіційні коефіцієнти CVSS v3.1

Стандарт CVSS v3.1 специфікації [27] визначає такі числові коефіцієнти для метрик Attack Vector (AV) і Privileges Required (PR), що входять до формули ExploitabilitySubScore:

Таблиця 2.2 – Офіційні коефіцієнти CVSS v3.1 для метрик AV і PR [27]

Метрика	Значення	Scope = Unchanged	Scope = Changed
Attack Vector (AV)	Network (N)	0,85	0,85
	Adjacent (A)	0,62	0,62
	Local (L)	0,55	0,55
	Physical (P)	0,20	0,20
Privileges Required (PR)	None (N)	0,85	0,85
	Low (L)	0,62	0,68
	High (H)	0,27	0,50

У документі CVSS v3.1 [27] вказано, що коефіцієнти підібрано експертною групою CVSS Special Interest Group у співпраці з компанією Deloitte & Touche LLP. Підбір зроблено таким чином, щоб результати застосування формули CVSS v3.1 узгоджувалися з якісними оцінками критичності вразливостей у реальних випадках. Таким чином, коефіцієнти специфікації CVSS v3.1 є не довільними константами, а емпірично обґрунтованими значеннями, що відображають колективну експертну думку спільноти кібербезпеки щодо відносної небезпечності різних характеристик вразливості.

2.5.2 Обґрунтування коефіцієнта AV_w

Для отримання коефіцієнта AV_w офіційні коефіцієнти CVSS v3.1 для поля Attack Vector нормуються на максимальне значення, що відповідає вектору

Network (0,85). Отримані нормовані ваги безпосередньо приймаються як значення AV_w у моделі TTCAG і наведені у таблиці 2.3.

Таблиця 2.3 – Обґрунтування коефіцієнта AV_w через нормалізацію CVSS v3.1

AV	CVSS v3.1	$AV_w = \text{CVSS}/0,85$	Інтерпретація для TTCAG
Network (N)	0,85	1,00	Опорний рівень, атака дистанційно з мережі
Adjacent (A)	0,62	0,73	Потрібен доступ із сусіднього мережевого сегмента
Local (L)	0,55	0,65	Потрібен локальний доступ до системи
Physical (P)	0,20	0,24	Потрібен фізичний доступ до пристрою

Логіка цього обґрунтування у тому, що чим складніше реалізувати вектор атаки, тим довшим є очікуваний час компрометації за моделлю TTCAG, оскільки коефіцієнт AV_w входить у знаменник формули (2.8). Для Physical-вектора час Процесу 1 збільшується приблизно у 4 рази порівняно з Network-вектором, що відповідає реальній складності здійснення зловмисником фізичного впливу на промислове обладнання.

2.5.3 Обґрунтування коефіцієнта γ

Числове обґрунтування коефіцієнта γ для метрики Privileges Required має додаткову особливість. Специфікація CVSS v3.1 визначає коефіцієнти PR у двох варіантах, залежно від значення поля Score. Це поле у термінах CVSS відображає, чи виходить вплив експлуатації за межі простору, у якому знаходиться вразливий компонент. Для побудови γ необхідно явно обрати, який саме випадок є реалістичнішим для багатоетапної атаки на кожному з рівнів привілеїв.

- $\gamma(\text{None}) = 0,85/0,85 = 1,00$. Якщо для експлуатації вразливості не потрібні жодні привілеї, латеральний рух не дає зловмиснику жодної переваги, тож атака на наступний вузол не прискорюється.

- $\gamma(\text{Low}) = 0,62/0,85 = 0,73$. Якщо для експлуатації потрібні базові користувацькі привілеї, при латеральному русі зловмисник, як правило, уже має ці привілеї з попереднього вузла і залишається в межах того самого security score. Тому використовується значення CVSS для PR = Low при Score = Unchanged, що становить 0,62. Час експлуатації знижується приблизно на 27 %.

- $\gamma(\text{High}) = 0,50/0,85 = 0,59$. Якщо вузол вимагає адміністративних привілеїв, успішна експлуатація призводить до переходу на принципово новий рівень доступу – ситуація score change у термінах CVSS. Тому використовується значення CVSS для PR = High при Score = Changed, що становить 0,50. Час експлуатації знижується приблизно на 41 %.

Такий підхід забезпечує методологічну цілісність обґрунтування коефіцієнта γ . Значення для Low відповідає нормованому CVSS для PR = Low при Score = Unchanged, а значення для High – для PR = High при Score = Changed. Підсумкові значення наведено у таблиці 2.4.

Таблиця 2.4 – Обґрунтування коефіцієнта γ через нормалізацію CVSS v3.1

PR	Базис CVSS v3.1	γ (нормоване)	Інтерпретація для TTCAG
None (N)	0,85 (S=U)	1,00	Привілеї не потрібні, латеральний рух не дає прискорення
Low (L)	0,62 (S=U)	0,73	Привілеї користувацького рівня вже накопичені, час знижується на 27 %
High (H)	0,50 (S=C)	0,59	Адміністративні привілеї вимагають зміни score, час знижується на 41%

Базові значення $\gamma(\text{PR})$ застосовуються до окремої вразливості з конкретним PR. На вузлі мережі присутні десятки чи сотні CVE з різним розподілом за PR, тому для кожного вузла обчислюється зважений коефіцієнт глибини:

$$\gamma(h_i) = \sum_{\text{PR}} \frac{n_{\text{PR}}(h_i)}{n_{\text{tot}}(h_i)} \cdot \gamma(\text{PR}) \quad (2.13)$$

де $n_{\text{PR}}(h_i)$ – кількість CVE вузла h_i з рівнем привілеїв PR; $n_{\text{tot}}(h_i)$ – загальна кількість CVE вузла; $\gamma(\text{PR})$ – базові коефіцієнти згідно з таблицею 2.4. Значення $\gamma(h_i)$ обчислені для досліджуваної мережі наведено у таблиці 3.5.

2.6 Стохастичні властивості загального розподілу TTCAG

Як показано у підрозділі 2.1, час компрометації окремого вузла у моделі McQueen є випадковою величиною, що формується як суперпозиція трьох незалежних випадкових величин з власними розподілами. У моделі TTCAG ця стохастична природа зберігається, оскільки модифікації стосуються лише масштабування розподілів, а не їхньої форми. Це дає змогу явно побудувати повний розподіл TTCAG як суперпозицію трьох розподілів окремих процесів.

2.6.1 Загальний TTCAG як випадкова величина

Для окремого вузла h_i у моделі TTCAG час компрометації становить випадкову величину T_{AG} , що приймає значення з ймовірностями, рівними ймовірностям перебування зловмисника у відповідному процесі:

$$T_{\text{AG}} = \begin{cases} T_1^*, \text{ з ймовірністю } P_1 \\ T_2, \text{ з ймовірністю } (1 - P_1)(1 - u) \\ T_3^*, \text{ з ймовірністю } (1 - P_1) \cdot u \end{cases} \quad (2.14)$$

де T_1^* , T_2 , T_3^* – випадкові величини часу для Процесів 1, 2 і 3 у моделі TTCAG.

2.6.2 Масштабований β -розподіл для Процесу 1

У моделі TTCAG час Процесу 1 коригується множителем $k = t_{1,base} / (CVSS_{norm} \cdot AV_w)$ згідно з формулою (2.8). Для прийнятого у моделі значення це дорівнює $k = 2 / (CVSS_{norm} \cdot AV_w)$. Це означає, що модифікований час $T_1^* = k \cdot T_1$, де T_1 – оригінальна випадкова величина з β -розподілом. За правилом перетворення випадкової величини при лінійному масштабуванні, функція щільності модифікованого розподілу має вигляд:

$$f_{T_1^*}(t) = \frac{1}{k} \cdot f_{T_1}\left(\frac{t}{k}\right), \quad t \in [0; 5k] \quad (2.15)$$

Математичне сподівання модифікованого розподілу: $E[T_1^*] = k$ днів. Це і є виправлений час t^*_1 з формули (2.8). Масштабування не змінює форми β -розподілу. Він залишається асиметричним, змінюється лише розтягнення по осі часу.

2.6.3 Гамма-розподіл для Процесу 2

Процес 2 у моделі TTCAG зберігає гамма-характер розподілу без додаткового масштабування. Це обґрунтовано тим, що Процес 2 моделює час самостійної розробки експлойта, який залежить переважно від рівня кваліфікації зловмисника, а не від вектора атаки. Тому коефіцієнт AV_w до Процесу 2 не застосовується. Форма розподілу змінюється лише через параметр ET – очікувану кількість спроб, що визначається рівнем кваліфікації через частку $f = AM/V$.

2.6.4 Експоненційний розподіл для Процесу 3

Процес 3 у моделі TTCAG зберігає експоненційну форму розподілу, проте його параметр змінюється через використання скоригованого $MTBV$ b^* замість оригінального b . Функція щільності у моделі TTCAG:

$$f_{T_3^*}(t) = \frac{1}{b^*} \cdot e^{-t/b^*}, t \geq 0 \quad (2.16)$$

Експоненційна форма зберігається тому, що математична природа Процесу 3 не змінюється; змінюється лише оцінка частоти таких подій для конкретного активу.

2.6.5 Повний розподіл TTCAG

Згідно з формулою повної ймовірності, функція щільності загального розподілу TTCAG для окремого вузла є зваженою сумою функцій щільності трьох процесів:

$$f_{TAG}(t) = P_1 \cdot f_{T_1^*}(t) + (1 - P_1)(1 - u) \cdot f_{T_2}(t) + (1 - P_1) \cdot u \cdot f_{T_3^*}(t) \quad (2.17)$$

Ваги відповідають ймовірностям перебування у Процесах 1, 2 і 3. Математичне сподівання загального розподілу, обчислене за формулою (2.17), збігається з формулою (2.10), що становить принципову перевірку узгодженості теоретичного апарату моделі.

Аналіз формули (2.17) дозволяє виокремити якісні властивості розподілу TTCAG. Розподіл є мультимодальним, оскільки має пік від β -розподілу Процесу 1, плавний пік від гамма-розподілу Процесу 2 та плавно спадаючий експоненційний хвіст Процесу 3. Розподіл є асиметричним правосторонньо зміщеним, що типово для часових випадкових величин. Форма розподілу істотно залежить від рівня кваліфікації зловмисника: для Expert розподіл практично зводиться до β -розподілу Процесу 1; для Novice основний внесок дає експоненційний хвіст Процесу 3, що приводить до значних математичних сподівань – тисячі днів для добре захищених активів.

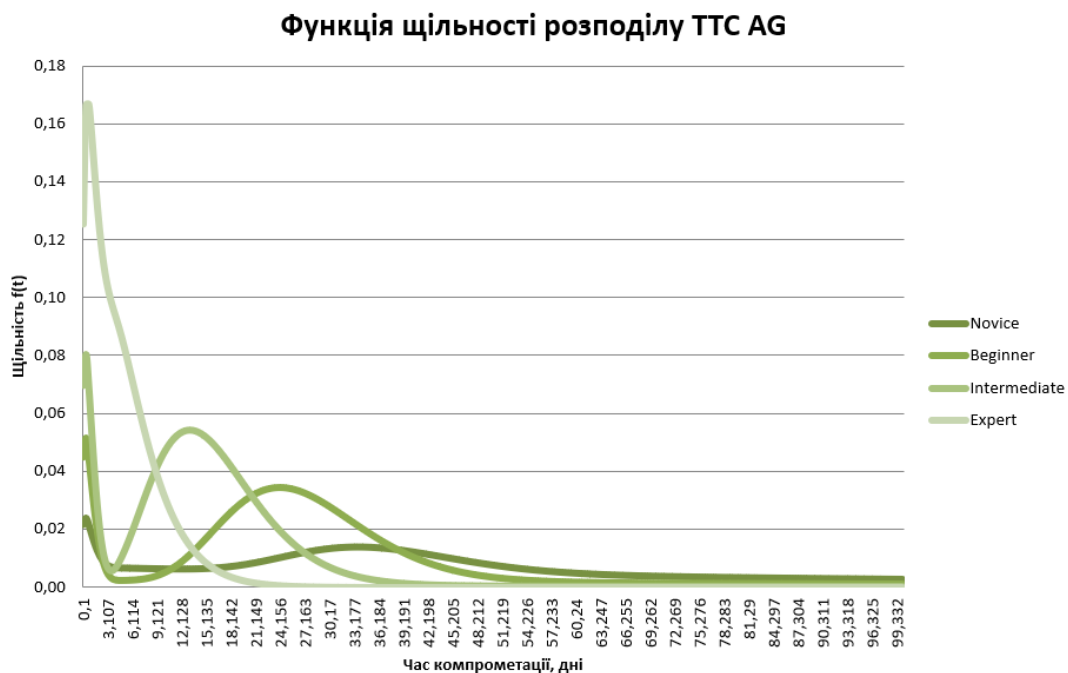


Рисунок 2.5 – Функція щільності загального розподілу TTCAG для типового вузла ICS-мережі для чотирьох рівнів кваліфікації зловмисника

2.6.6 Узгодженість з емпіричними результатами та обґрунтування точкової оцінки

Теоретичний розподіл TTCAG, побудований за формулою (2.17), узгоджується з емпіричним гамма-розподілом MTTC, отриманим у роботі [26] методом MCMC для SCADA-систем. Це узгодження не випадкове. Гамма-розподіл виникає природним чином при моделюванні сумішей експоненційних компонентів, а саме така структура виникає у Процесі 3 моделі McQueen. Цей емпіричний факт підтверджує відповідність моделі спостережуваним даним і обґрунтовує коректність використання математичного сподівання як точкової оцінки.

У всіх формулах моделі TTCAG (2.8), (2.10), (2.11) і (2.12) використовується лише математичне сподівання, а не повний PDF. Це методологічне рішення, успадковане від оригінальної моделі McQueen, обґрунтовується трьома аргументами:

- математичне сподівання обчислюється аналітично, що значно простіше за чисельне інтегрування повного розподілу;

- для практичних задач пріоритизації заходів захисту достатньо порівняння середніх значень;
- розподіл TTCAG є гамма-подібним з кінцевим математичним сподіванням і скінченною дисперсією, тому точкова оцінка становить достатню статистику для більшості задач.

Висновки до розділу 2

Побудовано формальну модель TTCAG як дворівневу структуру оцінювання часу компрометації мережі автоматизованої підстанції при багатоетапних кібератаках. На рівні окремого вузла введено виправлений час процесу P_1 через коефіцієнт AV_w і скоригований параметр $MTBV\ b^*$; на рівні шляху графу атак – коефіцієнт глибини шляху γ . Для випадку графу з декількома шляхами до цільового вузла обґрунтовано рекурсивну формулу обчислення TTCAG на основі концепції dominant attack path [29], що забезпечує коректне врахування спільних проміжних вузлів.

Числові значення коефіцієнтів AV_w та γ виведено через нормалізацію офіційних коефіцієнтів CVSS v3.1 [27], що забезпечує відтворюваність параметризації незалежним аналітиком та усуває залежність моделі від експертних оцінок, характерну для попередніх розширень TTC.

Проаналізовано стохастичні властивості загального розподілу TTCAG як суперпозиції масштабованого β -розподілу, гамма-розподілу та експоненційного розподілу. Встановлено, що розподіл є мультимодальним і правосторонньо асиметричним; його теоретична форма узгоджується з емпіричним гамма-розподілом MTTC, отриманим методом MCMC у роботі [26].

Побудована модель є завершеним формальним апаратом, що підлягає верифікації на типовій архітектурі мережі автоматизованої підстанції; ця задача є предметом третього розділу.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ TTCAG ДЛЯ МЕРЕЖІ ОБ'ЄКТА КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Метою третього розділу є практична верифікація моделі TTCAG на архітектурі мережі диспетчерського керування SCADA-системи енергетичного об'єкта. Виконано практичну реалізацію розробленої моделі оцінювання часу компрометації мережі SCADA-системи енергооб'єкта. Описано тестову мережу, побудовано датасет вразливостей на основі відкритих джерел NVD, CISA KEV та CISA CSAF, згенеровано вхідні дані для аналізатора MulVAL, отримано граф атак, виконано розрахунок показника TTCAG для всіх шляхів атаки.

3.1 Опис тестової мережі автоматизованої підстанції

Об'єктом моделювання є мережа диспетчерського центру керування енергооб'єкта, що відповідає 3-му рівню моделі Purdue (Operations Management). Архітектура мережі складається з єдиної логічної підмережі SCADA LAN, до якої через апаратний міжмережевий екран підключається зовнішнє середовище, а через спеціалізований шлюз – польовий рівень з електричними підстанціями (рисунок 3.1).

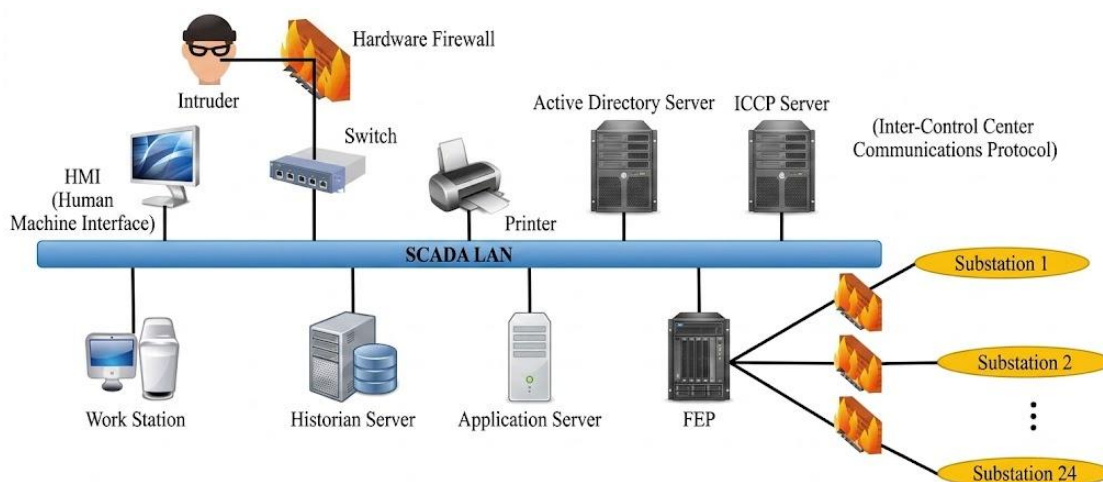


Рисунок 3.1 – Схема тестової мережі SCADA-системи диспетчерського центру

Топологію та склад мережі обрано на основі архітектури локальної мережі центру керування (control center LAN), детально описаної у роботі Tang, Liu та Wang [31]. У цьому дослідженні розглядається типова структура SCADA-мережі енергооб'єкта, що охоплює апаратний міжмережевий екран, комутатор, сервер історичних даних, сервер застосунків, людино-машинний інтерфейс HMI, а також шлюз FEP з підключеними підстанціями [31]. Аналогічна архітектура використовується у роботі Тостоган та Гальчинського [26], де ті самі компоненти локальної мережі центру керування та корпоративної мережі визначено як основні цілі зловмисників при кібератаках на SCADA-системи критичної інфраструктури.

Тестова мережа містить одинадцять вузлів, об'єднаних у три зони безпеки:

- **зона периметру (Perimeter)** – апаратний міжмережевий екран Hardware Firewall, який реалізує фільтрацію вхідного трафіку з мережі Інтернет та виступає єдиною точкою входу до інфраструктури енергооб'єкта;
- **зона SCADA LAN** – основна керуюча мережа, що містить людино-машинний інтерфейс HMI, робочу станцію оператора WorkStation, сервер історичних даних Historian Server, сервер застосунків Application Server, контролер домену Active Directory, сервер міждиспетчерського обміну ICCP Server, мережевий комутатор Switch та принтер Printer;
- **польова зона ОТ** – шлюз Front-End Processor (FEP) та електричні підстанції Substation 1–24, моделювання яких узагальнено в один логічний вузол substation. FEP забезпечує перетворення команд керування з протоколів верхнього рівня (OPC-UA, TASE.2) у промислові протоколи нижнього рівня (DNP3, IEC 60870-5-104, IEC 61850) для передачі на підстанції.

Така архітектура є типовою для центрів керування розподільчими мережами, де SCADA-сервер забезпечує дистанційний моніторинг та керування численними віддаленими підстанціями [31]. Як зазначено у [26], саме локальна мережа центру керування та корпоративна локальна мережа є основними цілями зловмисників, які намагаються проникнути в SCADA-системи шляхом виявлення вразливостей серед компонентів кібермереж.

На відміну від мереж автоматизації окремої підстанції (SAS), де об'єктом захисту виступають RTU та інтелектуальні електронні пристрої IED у межах

однієї фізичної підстанції, у даній моделі розглядається вищий рівень – центр диспетчерського керування, компрометація якого через канал від FEP до Substation потенційно дозволяє зловмиснику отримати контроль одночасно над кількома десятками підстанцій. Саме за таким сценарієм відбулися атаки BlackEnergy (2015) та Industroyer/Industroyer2 (2016, 2022) на українську енергосистему.

Ціллю атаки у моделі прийнято подію `execCode(substation, root)` – виконання довільного коду з адміністративними правами на підстанції. У реальній експлуатації ця подія означає отримання контролю над RTU/IED підстанції та можливість видавати команди розмикання/замикання комутаційного обладнання, що відповідає сценарію Industroyer2.

3.2 Формування датасету CVE для вузлів мережі

Для розрахунку часу компрометації вузлів за моделлю TTCAG необхідно мати для кожного вузла мережі перелік відомих CVE-вразливостей з метриками CVSS v3.1, що дозволяють обчислити параметри AV_w , $CVSS_{norm}$ та γ (PR). У даному підрозділі описано методику добору вразливостей з відкритих джерел та наведено підсумкову статистику отриманого датасету.

3.2.1 Джерела даних

Як джерела використано три відкриті бази даних:

1. Національна база вразливостей NVD (National Vulnerability Database) Національного інституту стандартів і технологій США – основне джерело CVE з метриками CVSS v3.1;
2. Каталог відомих експлуатованих вразливостей CISA KEV (Known Exploited Vulnerabilities) – перелік вразливостей, що активно експлуатуються у реальних кібератаках;

3. Репозиторій CISA CSAF (Common Security Advisory Framework) у форматі OASIS CSAF 2.0 – структуровані бюлетені безпеки для промислових систем керування ICS-CERT.

Часовий діапазон добору вразливостей встановлено від 2020 до 2025 року. Більш ранні вразливості, як правило, вже закриті в актуальних версіях програмного забезпечення або не релевантні для сучасного обладнання.

3.2.2 Критерії добору вразливостей

Збір даних реалізовано програмно мовою Python з використанням NVD API v2.0 та офіційного GitHub-репозиторію `cisagov/CSAF`. Для кожного вузла тестової мережі визначено перелік продуктів-відповідників (наприклад, для HMI – Siemens WinCC, Rockwell FactoryTalk View, AVEVA InTouch; для FEP – Siemens SICAM, IEC 60870-5-104, DNP3; для Substation – Schneider Modicon, Siemens SIPROTEC, ABB Relion), та виконано пошук CVE за відповідними ключовими словами.

Після первинного збору застосовано фільтрацію за вектором атаки. Залишено CVE з характеристикою Attack Vector = NETWORK, ADJACENT або LOCAL. Перші два класи відповідають первинному мережевому вектору проникнення зловмисника, а локальні вразливості необхідні для коректного моделювання етапу підвищення привілеїв після початкової компрометації вузла. Це активує у MulVAL правило RULE 4 (local privilege escalation). Виключено лише вразливості з фізичним вектором (PHYSICAL), що потребують безпосереднього фізичного доступу до обладнання і не належать до мережеских атак.

3.2.3 Структура датасету

Підсумковий датасет містить для кожної вразливості такі поля: ідентифікатор CVE, назву вразливого продукту, відповідний вузол мережі, базову оцінку CVSS v3.1, метрику Attack Vector (AV), метрику Privileges Required (PR),

категорію вразливості та дату публікації. Повний перелік зібраних вразливостей, що формує датасет дослідження, наведено у додатку А.

Розподіл фінального датасету за вузлами наведено у таблиці 3.1.

Таблиця 3.1 – Розподіл CVE 2020–2025 рр. по вузлах тестової мережі

Вузол	Зона	К-сть CVE	Сер. CVSS	Дом. AV	Дом. PR
Hardware Firewall	Perimeter	167	7,073	NETWORK	NONE
HMI	SCADA LAN	185	7,550	NETWORK	NONE
WorkStation	SCADA LAN	190	7,490	LOCAL	NONE
Historian Server	SCADA LAN	63	7,657	NETWORK	NONE
Application Server	SCADA LAN	84	7,305	NETWORK	NONE
Active Directory	SCADA LAN	43	7,450	NETWORK	LOW
ICCP Server	SCADA LAN	49	7,347	NETWORK	NONE
Switch	SCADA LAN	965	6,913	NETWORK	NONE
FEP	OT	59	7,442	NETWORK	NONE
Substation	OT	170	7,644	NETWORK	NONE

Загалом сформовано датасет із 1975 унікальних записів CVE для 10 продуктивних вузлів мережі (1915 унікальних CVE-ідентифікаторів, 60 з яких присутні одночасно у кількох вузлах, наприклад, CVE-2021-44228 Log4Shell, яка є одночасно в Application Server, Hardware Firewall та Switch). Більшість вузлів має домінуючий вектор атаки NETWORK, що підтверджує наявність первинного мережевого вектора компрометації, яке є необхідною умовою застосування правила remoteExploit аналізатора MulVAL.

Виняток становить вузол WorkStation, для якого домінуючим вектором є LOCAL (AV_w=0,65). Це відповідає характеру вразливостей сучасних офісних пакетів та операційних систем – більшість критичних CVE для Microsoft Office (CVE-2024-21413, CVE-2023-23397) та компонентів Windows вимагають взаємодії з користувачем або локального доступу. Цей факт значно впливає на час компрометації WorkStation у моделі TTCAG, як буде показано у підрозділі 3.5.

Вузол Active Directory має домінуючий рівень привілеїв $PR = LOW$ ($\gamma = 0,73$), що теж зменшує час компрометації цього вузла на наступних етапах атаки, якщо попередньо було отримано облікові дані. Цей ефект є ключовим для демонстрації переваги моделі TTCAG над класичним TTCICS.

3.3 Побудова графу атак засобами MulVAL

MulVAL реалізує граф атак як логічне виведення на основі мови програмування Datalog. Опис мережі та її вразливостей подається у вигляді набору фактів та правил, після чого MulVAL автоматично виводить усі логічно можливі стани компрометації, що можуть бути досягнуті зловмисником з початкової точки. Результатом роботи інструменту є орієнтований ациклічний граф.

Опис тестової мережі для MulVAL виконано у файлі `input.P`, що містить шість логічних блоків. Повний лістинг вхідного файлу наведено у додатку Б.

У першому блоці задано положення зловмисника предикатом `attackerLocated(internet)` та ціль атаки `attackGoal(execCode(substation, root))`. Другий блок описує мережеву топологію набором фактів `haci(Src, Dst, Protocol, Port)`, що задають дозволені напрями трафіку відповідно до правил міжмережевих екранів. Третій блок містить факти `networkServiceInfo(Host, Service, Protocol, Port, User)` – описи мережесервісів на хостах. Четвертий блок описує облікові записи через предикат `hasAccount`. У ньому окремо задано факти `hasAccount(operator, hmi, user)` та `hasAccount(operator, workstation, user)`, що моделюють типову ситуацію спільного облікового запису оператора на кількох вузлах SCADA LAN. Ці факти активують у MulVAL правило RULE 11 (`password sniffing`) – компрометація НМІ надає зловмиснику облікові дані оператора, які автоматично поширюють доступ на WorkStation без застосування додаткового експлойту. Такий сценарій відповідає техніці T0859 (Valid Accounts) за класифікатором MITRE ATT&CK for ICS.

П'ятий, ключовий блок містить факти про вразливості у класичному форматі MulVAL [19], що складається з двох предикатів:

vulExists(Host, VulID, Software).

vulProperty(VulID, Range, Consequence).

Перший фіксує факт існування вразливості на хості, другий описує її властивості. Range набуває значень remoteExploit або localExploit, а Consequence – privEscalation, dos або confloss. Аналізатор MulVAL автоматично об'єднує ці предикати під час виведення графу атак за допомогою внутрішнього правила.

Прямий перенос усіх записів CVE у файл input.P неможливий через експоненціальну складність зворотного логічного виведення MulVAL. Для подолання цього обмеження застосовано дедуплікацію датасету за ключем (Host, Range, Consequence). З кожної групи вразливостей з однаковими властивостями виведення обрано одну з максимальним значенням CVSS. Така процедура є коректною з точки зору алгоритму MulVAL, оскільки граф атак будується на основі типу вразливості, а не її конкретного ідентифікатора, оскільки наявність будь-якої однієї CVE заданого типу породжує той самий ланцюг логічного виведення, що й сотні таких CVE.

Результатом є файл AttackGraph.txt з повним описом графу атак (фрагмент текстового виводу цього файлу для домінантного шляху атаки наведено у додатку В), а також його візуалізації у форматах PDF, EPS та DOT (GraphViz).

3.4 Аналіз отриманого графу атак

Згенерований аналізатором MulVAL граф атак для тестової мережі містить 128 вершин та 166 ребер. Серед вершин виокремлено три основні категорії:

- вершини типу LEAF (умови) – факти з вхідного файлу input.P, що відображають вразливості, мережеві з'єднання та конфігурацію хостів;
- вершини типу AND (правила) – застосовані правила взаємодії MulVAL, переважно RULE 2 (віддалена експлуатація серверного сервісу) та RULE 5 (багатоетапний мережевий доступ);

- вершини типу OR (стани) – досягнуті стани атаки `execCode(host, perm)` та проміжні предикати `netAccess(host, proto, port)`.

Стан виконання довільного коду `execCode` успішно досягнуто для всіх десяти продуктивних вузлів мережі. Окрім стану `execCode(host, root)`, у графі також присутні стани `execCode(hmi, user)` та `execCode(workstation, user)`, які виникли внаслідок спрацювання правил RULE 0 та RULE 11. Після компрометації одного з вузлів зловмисник отримує облікові дані оператора, що автоматично надає йому доступ до інших машин зі спільним обліковим записом без застосування додаткових експлойтів.

Після аналізу графу виокремлено п'ять основних шляхів атаки, що мають практичне значення для оцінювання захищеності мережі (таблиця 3.2). Усі шляхи починаються з зовнішнього вузла Internet, проходять через апаратний міжмережевий екран та завершуються компрометацією цільової підстанції через FEP.

Таблиця 3.2 – Основні шляхи атаки в графі MulVAL

№	Шлях атаки	Кількість
AP1	Internet → Hardware FW → Switch → Active Directory → App Server → FEP → Substation	6
AP2	Internet → Hardware FW → HMI → FEP → Substation	4
AP3	Internet → Hardware FW → Switch → WorkStation → FEP → Substation	5
AP4	Internet → Hardware FW → Switch → ICCP Server → FEP → Substation	5
AP5	Internet → Hardware FW → Switch → Historian Server → FEP → Substation	5

Шлях AP2 є найкоротшим – лише чотири переходи від периметру до цілі. Він використовує пряму компрометацію НМІ через апаратний фаєрвол (актуально для випадків винесення НМІ у напівдемілітаризовану зону для віддаленого доступу операторів) та подальший прямий канал від НМІ до FEP. Шлях AP1 є

найдовшим та проходить через контролер домену Active Directory, що типово для атак з використанням техніки латерального руху через credential dumping.

Ключові CVE, що використовуються в отриманих шляхах атаки, наведено у таблиці 3.3. Усі вони мають критичний рівень та входять до каталогу CISA KEV як такі, що активно експлуатуються.

Таблиця 3.3 – Ключові CVE, використані у шляхах атаки

Вузол	CVE-ID	CVSS	Опис
Hardware Firewall	CVE-2024-3400	10,0	Palo Alto PAN-OS, впровадження команд OS
Switch	CVE-2021-34770	10,0	Cisco IOS XE, переповнення буфера CAPWAP
HMI	CVE-2021-38397	10,0	AVEVA Edge HMI, віддалене виконання коду
WorkStation	CVE-2019-0708	9,8	BlueKeep, Windows RDP RCE
Active Directory	CVE-2022-45141	9,8	Samba/Heimdal Kerberos, RC4 ETYPE
App Server	CVE-2021-44228	10,0	Apache Log4j2 (Log4Shell), RCE
Historian Server	CVE-2021-3129	9,8	Laravel Ignition, RCE
ICCP Server	CVE-2022-3682	9,9	Hitachi Energy MicroSCADA, RCE через завантаження файлів
FEP	CVE-2021-45033	9,9	Siemens SICAM A8000, використання жорстко закодованих облікових даних
Substation	CVE-2024-11317	10,0	ABB ASPECT, перехоплення сесії

3.5 Розрахунок показника ТТС* для вузлів мережі

Розрахунок часу компрометації окремого вузла за моделлю TTCAG виконується за формулами (2.8) та (2.10) розділу 2.

Як базовий випадок прийнято рівень кваліфікації Expert ($t_2=6$ діб), що відповідає сценарію АРТ-атаки – найбільш релевантному типу загрози для об'єктів критичної енергетичної інфраструктури. Аналіз чутливості до інших рівнів кваліфікації виконано у підрозділі 3.8.

У таблиці 3.4 наведено результати розрахунку TTC* для кожного вузла мережі на основі агрегованих CVSS-метрик з датасету підрозділу 3.2.

Таблиця 3.4 – Розрахунок TTC* для вузлів тестової мережі

Вузол	CVSSnorm	Дом. AV	AVw	PR (дом.)	t_1^* , дн	TTC*, дн
Hardware Firewall	0,7073	NETWORK	1,00	NONE	2,83	2,83
HMI	0,7550	NETWORK	1,00	NONE	2,65	2,65
WorkStation	0,7490	LOCAL	0,65	NONE	4,11	4,11
Historian Server	0,7657	NETWORK	1,00	NONE	2,61	2,78
Application Server	0,7305	NETWORK	1,00	NONE	2,74	2,8
Active Directory	0,7450	NETWORK	1,00	LOW	2,68	3,11
ICCP Server	0,7347	NETWORK	1,00	NONE	2,72	3,04
Switch	0,6913	NETWORK	1,00	NONE	2,89	2,89
FEP	0,7442	NETWORK	1,00	NONE	2,69	2,89
Substation	0,7644	NETWORK	1,00	NONE	2,62	2,62

Як видно з таблиці, час компрометації більшості вузлів знаходиться у вузькому діапазоні 2,65-3,11 діб. Це пояснюється близькими значеннями mean_CVSS (6,9-7,7) для всіх вузлів. Датасет містить переважно критичні вразливості з каталогу CISA KEV. Виняток становить WorkStation з $TTC^*=4,11$ дн. Це є прямим наслідком домінуючого вектора атаки LOCAL, тому що для компрометації робочої станції зловмиснику потрібно або фішинг (для виконання шкідливого вкладення), або попередній доступ до сегменту мережі, що значно ускладнює атаку порівняно з прямою мережевою експлуатацією.

3.6 Розрахунок TTCAG для шляхів атаки

Загальний показник TTCAG для шляху атаки розраховується як зважена сума внесків кожного вузла з накопиченням коефіцієнта γ за рівнем привілеїв попередніх вузлів за формулою (2.11).

Схема відображає реальну логіку латерального руху зловмисника. Після компрометації першого вузла з PR=LOW атакуючий отримує облікові дані, що зменшують ефективні витрати часу на наступні етапи. Якщо ж жоден з вузлів попередніх етапів не давав PR=LOW або HIGH, накопичений γ залишається рівним 1,0 і модель зводиться до простого підсумовування TTC* по вузлах шляху.

Деталізований розрахунок для найдовшого шляху AP1 (шість вузлів через Active Directory) наведено у таблиці 3.5.

Таблиця 3.5 – Детальний розрахунок TTCAG для шляху AP1

i	Вузол	TTC*, дн	γ	$\prod \gamma_j$	Внесок, дн
0	Hardware Firewall	2,83	0,836	1,000	2,83
1	Switch	2,89	0,852	0,836	2,42
2	Active Directory	3,11	0,819	0,712	2,22
3	Application Server	2,8	0,964	0,583	1,63
4	FEP	2,89	0,913	0,562	1,62
5	Substation	2,62	0,945	0,513	1,34
	TTCAG(AP1) =				12,06

Зведені результати розрахунку TTCAG для всіх п'яти шляхів атаки наведено у таблиці 3.6.

Таблиця 3.6 – Значення TTCAG для всіх шляхів атаки

Шлях	Послідовність вузлів	К-сть вузлів	TTCAG, дн.
AP1	HW FW → Switch → AD → App Server → FEP → Substation	6	12,06
AP2	HW FW → HMI → FEP → Substation	4	9,06
AP3	HW FW → Switch → WorkStation → FEP → Substation	5	11,78

Кінець таблиці 3.6

Шлях	Послідовність вузлів	К-сть вузлів	TTCAG, дн.
AP4	HW FW → Switch → ICCP Server → FEP → Substation	5	10,70
AP5	HW FW → Switch → Historian Server → FEP → Substation	5	10,45

Шлях AP2 з найменшою кількістю проміжних вузлів демонструє і найменше значення TTCAG=9,06 дн. Це означає, що при наявності прямого каналу від HW Firewall до НМІ зловмиснику потрібно у середньому близько місяця для компрометації підстанції. Найдовший шлях AP1 з шістьма вузлами та проміжним проходженням через Active Directory дає TTCAG=12,06 дн.

Шляхи AP3 (через WorkStation), AP4 (через ICCP) та AP5 (через Historian) мають близькі значення TTCAG у діапазоні 10,45-11,78 дн. і відрізняються лише за рахунок різних показників CVSS обраних вузлів.

3.7 Порівняння базової TTCAG⁰ та повної TTCAG версій моделі

Для оцінки внеску запропонованого коефіцієнта γ у модель TTCAG, виконано порівняння двох її версій: базової TTCAG⁰ без накопиченого контексту, що відповідає простому підсумовуванню TTC* по вузлах шляху, як у моделі TTCICS та повної TTCAG з зваженим γ . Результати порівняння у таблиці 3.7.

Таблиця 3.7 – Порівняння базової TTCAG⁰ та повної TTCAG версій моделі

Шлях	TTCAG ⁰	TTCAG	Δ дн	Δ %
AP1	17,14	12,06	-5,08	-29,6 %
AP2	10,98	9,06	-1,92	-17,4 %
AP3	15,33	11,78	-3,55	-23,2 %
AP4	14,27	10,70	-3,57	-25,0 %
AP5	14,01	10,45	-3,56	-25,4 %

Найбільша різниця між моделями спостерігається на шляху AP1, де відмінність становить 5,08 дн. (зменшення на 29,6%). Ця різниця виникає за рахунок накопичення контексту по шести вузлах шляху, причому ключову роль відіграє контролер домену Active Directory ($\gamma = 0,73$) – після його компрометації зловмисник отримує облікові дані домену, що прискорюють атаку на наступні вузли. Для коротших шляхів ефект менший: AP2 (4 вузли) дає різницю 17,4%, а AP3-AP5 (5 вузлів) – від 23,2 % до 25,4 %. Збільшення довжини шляху прямо корелює зі зростанням впливу тактичного контексту, що свідчить про коректність застосування моделі TTCAG для кількісного оцінювання багатоетапних кібератак.

Виявлений ефект є якісно тим самим, що і у дослідженні [28], де відмінність моделей складала до 50 % при наявності декількох вузлів з PR=LOW. У нашій тестовій мережі ефект складає від 17,4% до 29,6 % залежно від шляху. Це підтверджує, що значення TTCAG залежить не лише від загальної кількості вразливостей, а й від їхнього розподілу за рівнем необхідних привілеїв, параметра, який ігнорується у класичних моделях оцінки часу компрометації. На відміну від моделі з домінуючим PR, де ефект проявляється лише на шляхах через спеціалізовані вузли автентифікації, зважена модель γ виявляє внесок усіх вузлів пропорційно до реального розподілу їхніх вразливостей за рівнем PR. Аналіз датасету показав, що більшість вузлів містять значну частку CVE з PR=LOW або HIGH (Hardware Firewall – 31%, Historian Server – 48%, Switch – 49%, ICCP Server – 43%), що робить врахування зваженого γ методологічно обґрунтованим.

Таким чином, чим більше у мережі вузлів, експлойти яких потребують підвищених привілеїв, тим важливішим стає застосування моделі TTCAG з тактичним контекстом замість простого підсумовування часу компрометації окремих вузлів. Для досліджуваної тестової мережі SCADA-центру керування критичним напрямом захисту є шляхи з найбільшою кумулятивною часткою CVE з $PR \geq LOW$: AP1 через Active Directory ($\Delta = -29,6 \%$), AP4 через ICCP Server ($\Delta = -25,0 \%$) та AP5 через Historian Server ($\Delta = -25,4 \%$).

3.8 Аналіз чутливості моделі до рівня кваліфікації зловмисника

У базовій моделі McQueen [16] та її ICS-адаптації [23] передбачено розмежування часу пошуку експлойта (процес P_2) залежно від рівня кваліфікації зловмисника. Числові значення параметра t_2 для чотирьох рівнів кваліфікації наведено у таблиці 2.1 розділу 2. Для оцінки чутливості розробленої моделі TTCAG до рівня кваліфікації зловмисника виконано розрахунок TTCAG для всіх п'яти шляхів атаки досліджуваної мережі для кожного з рівнів. Результати наведено у таблиці 3.8.

Таблиця 3.8 – Значення TTCAG (діб) для різних рівнів кваліфікації зловмисника

Шлях	Послідовність	Expert ($t_2=6$)	Intermediate ($t_2=16$)	Beginner ($t_2=27$)	Novice ($t_2=37$)
AP1	HW FW → Switch → AD → App → FEP → Substation	12,06	17,29	31,99	153,19
AP2	HW FW → HMI → FEP → Substation	9,06	11,38	20,09	82,16
AP3	HW FW → Switch → WS → FEP → Substation	11,78	13,86	21,69	77,92
AP4	HW FW → Switch → ICCP → FEP → Substation	10,70	14,92	26,87	121,03
AP5	HW FW → Switch → Historian → FEP → Substation	10,45	13,96	25,03	93,75

Аналіз отриманих значень показує характерну для моделі TTCAG нелінійну залежність часу компрометації від рівня кваліфікації зловмисника. Для всіх досліджуваних шляхів атаки час компрометації зростає приблизно від 7 до 13 разів при переході від рівня Expert до рівня Novice, причому різниця у часі складає 66 до 141 діб залежно від довжини шляху. Найкоротший шлях AP2 через HMI дає мінімальне значення $TTCAG(Expert)=9,06$ діб та максимальне

TTCAG(Novice)=82,16 діб. Найдовший шлях AP1 через Active Directory характеризується значеннями від 12,06 діб для Expert до 153,19 діб для Novice.

3.9 Практична цінність отриманих результатів

Отримані значення TTCAG для досліджуваної SCADA-мережі диспетчерського центру керування формують кількісну основу для практичного застосування моделі при організації кіберзахисту об'єктів критичної енергетичної інфраструктури.

1. Отримані значення визначають верхню межу часового вікна реагування для служби моніторингу інцидентів (SOC). Протягом цього періоду команда захисту має виявити аномальну активність, провести криміналістичний аналіз та ізолювати скомпрометовані вузли до досягнення зловмисником польового OT-рівня. Найменше отримане значення TTCAG(AP2)=9,06 доби для рівня Expert є найкритичнішим орієнтиром для SOC. Цей час найбільш кваліфікований зловмисник здатен досягти цільового активу за відсутності протидії.

2. Діапазон значень TTCAG для різних шляхів атаки дозволяє пріоритизувати захисні заходи за критерієм найшвидшої компрометації. Шлях AP2 потребує першочергової уваги через прямий канал до HMI, що виникає при його винесенні у напівдемілітаризовану зону для віддаленого доступу операторів. Мережева сегментація з розміщенням HMI виключно у внутрішній SCADA LAN потенційно збільшить значення TTCAG найкритичнішого шляху за рахунок усунення прямого маршруту доступу до HMI.

3. Підвищення частки CVE з $PR \geq LOW$ через своєчасне патчування вузлів з $PR=NONE$ збільшує значення накопиченого добутку γ і, відповідно, розрахункове значення TTCAG. Посилення політики паролів та регулярна ротація облікових даних адміністраторів додатково ускладнюють реалізацію техніки латерального руху після початкової компрометації.

4. Регулярний перерахунок TTCAG при появі нових CVE у базах NVD та CISA KEV дозволяє динамічно відстежувати погіршення захищеності мережі після публікації нових вразливостей. Зниження середнього CVSS або зміна домінуючого AV безпосередньо впливають на розрахункові значення TTC* і TTCAG.

Розроблена модель може бути використана як складова систем підтримки прийняття рішень з оцінювання кіберризиків SCADA-систем об'єктів критичної енергетичної інфраструктури.

Висновки до розділу 3

У розділі виконано практичну реалізацію моделі оцінювання часу компрометації мережі SCADA-системи енергооб'єкта. Побудовано тестову мережу диспетчерського центру, сформовано датасет із 1975 записів CVE та реалізовано автоматизований процес підготовки вхідних даних для аналізатора MulVAL. За результатами аналізу отримано граф атак із 128 вершинами та 166 ребрами, виявлено п'ять основних шляхів досягнення цільового вузла. Розрахунок TTCAG для всіх шляхів атаки показав, що значення знаходяться у діапазоні 9,06-12,06 діб для рівня Expert та 77,92-153,19 діб для рівня Novice. Ці значення формують конкретне часове вікно реагування для SOC та дозволяють безпосередньо пріоритизувати захисні заходи за критерієм найшвидшої компрометації.

ВИСНОВКИ

У роботі вирішено завдання розроблення моделі оцінювання часу компрометації об'єктів критичної енергетичної інфраструктури при багатоетапних кібератаках з урахуванням накопичення привілеїв зловмисника при латеральному русі. Отримано такі основні результати.

1. За результатами аналізу сучасного стану кібербезпеки об'єктів критичної енергетичної інфраструктури встановлено, що багатоетапні кібератаки на диспетчерські SCADA-центри керування характеризуються тривалою підготовчою фазою у місяці, а реальні інциденти BlackEnergy (2015) та Industroyer/Industroyer2 (2016, 2022) на українській енергосистемі підтверджують саме цей вектор загроз. Виявлено ключове обмеження існуючих моделей оцінювання часу компрометації TTC McQueen та її ICS-адаптація TTCICS. Вони оперують лише на рівні окремого вузла та ігнорують ефект накопичення привілеїв при переході зловмисника між вузлами. Це приводить до систематичного завищення оцінки часу атаки порівняно з реальною динамікою.

2. В результаті дослідження функцій щільності розподілу часу для трьох процесів зловмисника у моделях McQueen та TTCICS встановлено, що базовий параметр $t_2=5,8$ діб (процес 2 – пошук нового експлойта) залишається придатним для ICS-середовища, тоді як параметр MTBV (середній інтервал між публікаціями CVE) у TTCICS становить 2 200 діб і завищений у 2-3 рази порівняно з реальною статистикою NVD для ICS-обладнання, що обґрунтовує необхідність корекції цього параметра у новій моделі.

3. Розроблено модель TTCAG як дворівневу структуру з усуненням двох ключових обмежень TTCICS. На рівні окремого вузла введено коефіцієнт впливу вектора атаки AV_w та скоригований параметр MTBV, на рівні шляху атаки введено зважений коефіцієнт глибини шляху γ як середнє значення коефіцієнтів привілеїв за розподілом CVE на вузлі. Розроблена модель дозволяє оцінити ефект накопичення привілеїв при латеральному русі зловмисника.

4. Проведено стохастичний аналіз загального розподілу TTCAG як суперпозиції трьох процесів з різними розподілами. Доведено, що сумарний розподіл TTCAG для шляху з n вузлами зберігає односторонньо-обмежений характер, характеризується «важкими хвостами» на правій частині, що відповідає випадкам очікування нових CVE. Це дозволяє практично оцінювати не лише очікуване значення TTCAG, а й верхню межу часу компрометації з заданою довірчою ймовірністю.

5. Сформовано датасет з 1975 записів CVE 2020-2025 рр. для 10 вузлів типової архітектури SCADA-центру. На основі датасету та граф атак, побудованого за допомогою MulVAL (128 вершин, 166 ребер), обчислено TTCAG для п'яти основних шляхів атаки до цільової підстанції. Отримано значення TTCAG від 9,06 діб (найкоротший шлях через HMI) до 12,06 діб (найдовший шлях через Active Directory), що дає практичний кількісний орієнтир для планування заходів виявлення та реагування на інциденти у SCADA-мережах енергооб'єктів.

6. За результатами обчислювального експерименту з порівняльним аналізом базової (без накопиченого тактичного контексту) та повної (з зваженим коефіцієнтом γ) версій моделі TTCAG встановлено, що врахування ефекту накопичення привілеїв зменшує оцінку часу компрометації на 17-30% залежно від довжини шляху атаки, причому найбільший ефект ($-29,6\%$) спостерігається на найдовшому шляху через Active Directory. Виявлено пряму кореляцію між довжиною шляху атаки та зростанням впливу тактичного контексту, що підтверджує адекватність моделі TTCAG для саме багатоетапних атак, де класичні моделі систематично переоцінюють захисний резерв часу.

Апробація результатів. Основні положення доповідалися на XXIV Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (13-16 травня 2026 р., м. Київ) у секції «Математичні методи кібернетичної безпеки», за матеріалами якої опубліковано наукову статтю Шевченко В. М. та Гальчинського Л. Ю. «Вдосконалена модель TTCAG для оцінювання часу компрометації вузлів ICS-мережі на основі графа атак та метрик CVSS v3».

Перспективи подальших досліджень. Розроблену модель доцільно розширити у трьох напрямках:

1. Інтеграція з мережевими IDS-сенсорами для динамічного перерахунку TTCAG при виявленні нових індикаторів компрометації.
2. Розширення формального апарату для урахування неоднорідних шляхів атаки з циклами та паралельними переходами.
3. Калібрування параметрів моделі на основі реальних логів інцидентів кібербезпеки енергооб'єктів, що дозволить уточнити емпіричні розподіли t_1 , t_2 , t_3 для специфіки ICS-середовища.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82, Revision 2. – Gaithersburg: National Institute of Standards and Technology, 2015. – 247 c. URL: <https://doi.org/10.6028/NIST.SP.800-82r3>
2. Galloway B., Hancke G. P. Introduction to Industrial Control Networks // IEEE Communications Surveys & Tutorials. – 2013. – Vol. 15, No. 2. – C. 860–880. URL: https://www.researchgate.net/publication/260671145_Introduction_to_Industrial_Control_Networks
3. McDonald J. D. Electric Power Substations Engineering. 3rd ed. – Boca Raton: CRC Press, 2012. – 536 c. ISBN: 978-1-4398-5638-3. URL: https://www.pce-fet.com/common/library/books/78/2784_ElectricPowerSubstationsEngineering.pdf
4. Liu C.-C., Stefanov A., Hong J., Panciatici P. Intruders in the Grid // IEEE Power and Energy Magazine. – 2012. – Vol. 10, No. 1. – C. 58–66. DOI: 10.1109/MPE.2011.943114. URL: <https://magazine.ieee-pes.org/wp-content/uploads/sites/50/2011/12/10mpe01-liu.pdf>
5. Knapp E. D., Langill J. T. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 2nd ed. – Waltham: Syngress, 2014. – 31,990 c. ISBN: 978-0-12-420114-9. URL: https://pbio.akademia.mil.pl/wp-content/scans/2024/CYBERBEZPIECZENSTWO/OCR/26653_III_OCR.pdf
6. IEC 61850. Communication networks and systems for power utility automation. Edition 2.0. – Geneva: International Electrotechnical Commission, 2013.
7. Mackiewicz R. E. Overview of IEC 61850 and Benefits // IEEE Power Engineering Society General Meeting. – Montreal, 2006. – C. 1–8. DOI: 10.1109/PES.2006.1709531,99.
8. Sun C.-C., Hahn A., Liu C.-C. Cyber Security of a Power Grid: State-of-the-Art // International Journal of Electrical Power & Energy Systems. – 2018. – Vol. 99. – C. 45–56. DOI: 10.1016/j.ijepes.2017.12.020.

9. Hemsley K. E., Fisher R. E. History of Industrial Control System Cyber Incidents : Technical Report INL/CON-18-44411. – Idaho Falls: Idaho National Laboratory, 2018. – 37 с. URL: <https://www.osti.gov/servlets/purl/1505628>
10. Гальчинський Л. Ю., Личик В. В. Використання моделі мереж Баєса для раннього оцінювання загроз кібератак об'єкта електроенергетики // Реєстрація, зберігання і обробка даних. – 2025. – Т. 27, № 2. – С. 70–85. URL: <https://doi.org/10.35681/1560-9189.2025.27.2.345591>
11. Hutchins E. M., Cloppert M. J., Amin R. M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains // Proceedings of the 6th International Conference on Information Warfare and Security. – Washington, DC, 2011. – С. 113–125. URL: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>
12. E-ISAC, SANS ICS. Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case. – Washington, DC: Electricity Information Sharing and Analysis Center, 2016. – 23 с. URL: <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf>
13. Mandiant. M-Trends 2026 Special Report. – Reston: Mandiant (Google Cloud), 2024. URL: <https://cloud.google.com/security/resources/m-trends>
14. Cherepanov A. WIN32/INDUSTROYER: A New Threat for Industrial Control Systems : White Paper. – Bratislava: ESET, 2017. – 17 с. URL: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf
15. ESET Research. Industroyer2: Industroyer reloaded // ESET WeLiveSecurity. – 2022, April 12. URL: <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded>
16. McQueen M. A., Boyer W. F., Flynn M. A., Beitel G. A. Time-to-Compromise Model for Cyber Risk Reduction Estimation // Quality of Protection: Security Measurements and Metrics. – Springer, 2006. – С. 49–64. URL: https://doi.org/10.1007/978-0-387-36584-8_5

17. Williams T. J. The Purdue Enterprise Reference Architecture // Computers in Industry. – 1994. – Vol. 24, No. 2–3. – C. 141–158. DOI: 10.1016/0166-3615(94)90017-5.
18. Phillips C., Swiler L. P. A Graph-Based System for Network-Vulnerability Analysis // Proceedings of the 1998 Workshop on New Security Paradigms (NSPW). – New York: ACM, 1998. – C. 71–79. DOI: 10.1145/310889.310919.
19. Ou X., Govindavajhala S., Appel A. W. MulVAL: A Logic-Based Network Security Analyzer // Proceedings of the 14th USENIX Security Symposium. – Baltimore, 2005. – C. 113–128. URL: https://www.usenix.org/legacy/event/sec05/tech/full_papers/ou/ou.pdf
20. Tayouri D., Baum N., Shabtai A., Puzis R. A Survey of MulVAL Extensions and Their Attack Scenarios Coverage // arXiv preprint arXiv:2208.05750. – 2022. – 28 c. URL: <https://arxiv.org/pdf/2208.05750>
21. Poolsappasit N., Dewri R., Ray I. Dynamic Security Risk Management Using Bayesian Attack Graphs // IEEE Transactions on Dependable and Secure Computing. – 2012. – Vol. 9, No. 1. – C. 61–74. URL: <https://doi.org/10.1109/TDSC.2011.34>
22. Zieger A., Freiling F. C., Kossakowski K.-P. The β -Time-to-Compromise Metric for Practical Cyber Security Risk Estimation // 11th International Conference on IT Security Incident Management & IT Forensics (IMF). – Hamburg, 2018. – C. 115–133. DOI: 10.1109/IMF.2018.00007.
23. Rencelj Ling E., Ekstedt M. Estimating Time-To-Compromise for Industrial Control System Attack Techniques Through Vulnerability Data // SN Computer Science. – 2023. – Vol. 4. – Art. 318. URL: https://www.researchgate.net/publication/369900555_Estimating_Time-To-Compromise_for_Industrial_Control_System_Attack_Techniques_Through_Vulnerability_Data
24. Leversage D. J., Byres E. J. Comparing Electronic Battlefields: Using Mean Time-to-Compromise as a Comparative Security Metric // Computer Network Security : MMM-ACNS 2007. – Springer, 2007. – C. 252–265. URL: https://doi.org/10.1007/978-3-540-73986-9_18

25. Yang J., Yang Y., Zheng L., Cheng R., Lin S. Network Security Situation Assessment Based on Attack Graph Techniques // Journal of Physics: Conference Series. – 2022. – Vol. 2310. – Art. 012071. DOI: 10.1088/1742-6596/2310/1/012071.
26. Тостоган Є. Г., Гальчинський Л. Ю. Моделювання кібернадійності SCADA-систем критичної інфраструктури з використанням напівмарківських процесів // SCIENTIA: Modern Science and Innovation. – New York, 2025. – С. 209–218.
27. FIRST. Common Vulnerability Scoring System v3.1: Specification Document. – Forum of Incident Response and Security Teams, 2019. URL: <https://www.first.org/cvss/v3-1/specification-document>
28. Шевченко В. М., Гальчинський Л. Ю. Вдосконалена модель TTCAG для оцінювання часу компрометації вузлів ICS-мережі на основі графа атак та метрик CVSS v3 // Теоретичні і прикладні проблеми фізики, математики та інформатики : матеріали XXIV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, [Київ], 13–16 травня 2026 р. / КПІ ім. Ігоря Сікорського. – Київ, 2026. – С. 286–289.
29. McQueen M. A., Boyer W. F., Flynn M. A., Beitel G. A. Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System // Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). – 2006. – С. 226. URL: <https://doi.org/10.1109/HICSS.2006.405>
30. Lopuhaä-Zwakenberg M., Stoelinga M. Attack Time Analysis in Dynamic Attack Trees via Integer Linear Programming // Software Engineering and Formal Methods : Lecture Notes in Computer Science. – Springer, 2023. – Vol. 14424. – С. 165–183. URL: <https://doi.org/10.48550/arXiv.2111.05114>
31. S. Tang, Z. Liu and L. Wang, "Power System Reliability Analysis Considering External and Insider Attacks on the SCADA System," 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Chicago, IL, USA, 2020, pp. 1-5, URL: <https://doi.org/10.1109/td39804.2020.9299922>.
32. NIST. National Vulnerability Database. – URL: <https://nvd.nist.gov>. National Institute of Standards and Technology.

33. Thomas R. J., Chothia T. RITICS ICS Vulnerability Dataset. – 2020. – URL: <https://github.com/UoB-RITICS/esorics2020-dataset>; GitHub repository.
34. Dragos Inc. OT Red Team & Penetration Testing Services. Hanover, MD: Dragos Inc – 2026. – URL: <https://www.dragos.com/services/red-team-services/> (дата звернення: 01.06.2026).

ДОДАТОК А

Для побудови графа атак використано датасет вразливостей. Він містить 1975 записів про вразливості для 10 вузлів тестової мережі. Повна версія датасету наведена за посиланням:

<https://docs.google.com/spreadsheets/d/1NA9Hkd4m252WyhxsuVAeXNb6dUt69eyK/edit?usp=sharing&ouid=114710168273986935997&rtpof=true&sd=true>

Таблиця А.1 – Структура полів сформованого датасету вразливостей

Поле	Опис
asset	Назва або ідентифікатор вузла мережі
zone	Мережевий сегмент
source	Джерело інформації про вразливість
keyword	Ключове слово для пошуку вразливостей
cve_id	Ідентифікатор вразливості CVE
published	Дата публікації CVE
modified	Дата останнього оновлення CVE
cvss_v3_score	Базова оцінка CVSS v3.1
cvss_v3_severity	Рівень критичності CVSS v3.1
cvss_v3_vector	Вектор CVSS v3.1
AV	Метрика Attack Vector
AC	Метрика Attack Complexity
PR	Метрика Privileges Required
UI	Метрика User Interaction
C_impact	Вплив на конфіденційність
I_impact	Вплив на цілісність
A_impact	Вплив на доступність
cvss_v2_score	Базова оцінка CVSS v2
cvss_v2_severity	Рівень критичності CVSS v2
cvss_v2_vector	Вектор CVSS v2
cwe	Ідентифікатор типу помилки CWE

Кінець таблиці A.1

Поле	Опис
description	Текстовий опис вразливості
cisa_kev	Ознака включення до каталогу CISA KEV
cisa_sector	Галузева категорія CISA
cisa_advisory_id	Ідентифікатор рекомендації CISA

ДОДАТОК Б

Вхідний файл input.P для генерації графа атак MulVAL:

```

/* =====
 * MulVAL input.P – SCADA LAN
 * ===== */

/* === 1. Зловмисник та ціль атаки === */
attackerLocated(internet).
attackGoal(execCode(substation, root)).
malicious(attacker).
hasAccount(attacker, internet, root).

/* === 2. HACL === */
hacl(internet, hardware_firewall, tcp, 80).
hacl(hardware_firewall, hmi, tcp, 80).
hacl(hardware_firewall, switch, tcp, 80).
hacl(switch, hmi, tcp, 80).
hacl(switch, workstation, tcp, 80).
hacl(switch, historian_server, tcp, 80).
hacl(switch, application_server, tcp, 80).
hacl(switch, active_directory, tcp, 80).
hacl(switch, iccp_server, tcp, 80).
hacl(switch, fep, tcp, 80).
hacl(switch, printer, tcp, 80).
hacl(hmi, workstation, tcp, 80).
hacl(hmi, application_server, tcp, 80).
hacl(hmi, historian_server, tcp, 80).
hacl(hmi, fep, tcp, 80).
hacl(workstation, active_directory, tcp, 80).
hacl(workstation, application_server, tcp, 80).
hacl(workstation, historian_server, tcp, 80).
hacl(workstation, fep, tcp, 80).
hacl(active_directory, hmi, tcp, 80).
hacl(active_directory, workstation, tcp, 80).
hacl(active_directory, application_server, tcp, 80).
hacl(active_directory, historian_server, tcp, 80).
hacl(active_directory, iccp_server, tcp, 80).
hacl(application_server, historian_server, tcp, 80).
hacl(application_server, fep, tcp, 80).
hacl(historian_server, fep, tcp, 80).
hacl(iccp_server, fep, tcp, 80).
hacl(fep, substation, tcp, 80).

/* === 3. networkServiceInfo === */
networkServiceInfo(hardware_firewall, httpd, tcp, 80, root).
networkServiceInfo(hmi, httpd, tcp, 80, root).
networkServiceInfo(workstation, httpd, tcp, 80, root).
networkServiceInfo(historian_server, httpd, tcp, 80, root).
networkServiceInfo(application_server, httpd, tcp, 80, root).

```

```

networkServiceInfo(active_directory, httpd, tcp, 80, root).
networkServiceInfo(iccp_server, httpd, tcp, 80, root).
networkServiceInfo(fep, httpd, tcp, 80, root).
networkServiceInfo(substation, httpd, tcp, 80, root).
networkServiceInfo(switch, httpd, tcp, 80, root).
networkServiceInfo(printer, httpd, tcp, 80, root).

```

```

/* === 4. hasAccount === */
hasAccount(admin, hardware_firewall, root).
hasAccount(admin, hmi, root).
hasAccount(operator, hmi, user).
hasAccount(admin, workstation, root).
hasAccount(operator, workstation, user).
hasAccount(admin, historian_server, root).
hasAccount(admin, application_server, root).
hasAccount(admin, active_directory, root).
hasAccount(admin, iccp_server, root).
hasAccount(admin, switch, root).
hasAccount(admin, fep, root).
hasAccount(admin, substation, root).
hasAccount(admin, printer, root).

```

```

/* === 4. Вразливості === */
/* --- SWITCH --- */
vulExists(switch, 'CVE-2021-34770_switch', httpd).
vulProperty('CVE-2021-34770_switch', remoteExploit, privEscalation).

```

```

/* --- HARDWARE_FIREWALL --- */
vulExists(hardware_firewall, 'CVE-2024-3400_hardware_firewall', httpd).
vulProperty('CVE-2024-3400_hardware_firewall', remoteExploit, privEscalation).

```

```

/* --- HMI --- */
vulExists(hmi, 'CVE-2021-38397_hmi', httpd).
vulProperty('CVE-2021-38397_hmi', remoteExploit, privEscalation).

```

```

/* --- SUBSTATION --- */
vulExists(substation, 'CVE-2024-11317_substation', httpd).
vulProperty('CVE-2024-11317_substation', remoteExploit, privEscalation).

```

```

/* --- APPLICATION_SERVER --- */
vulExists(application_server, 'CVE-2021-44228_application_server', httpd).
vulProperty('CVE-2021-44228_application_server', remoteExploit, privEscalation).

```

```

/* --- ICCP_SERVER --- */
vulExists(iccp_server, 'CVE-2022-3682_iccp_server', httpd).
vulProperty('CVE-2022-3682_iccp_server', remoteExploit, privEscalation).

```

```

/* --- FEP --- */
vulExists(fep, 'CVE-2021-45033_fep', httpd).
vulProperty('CVE-2021-45033_fep', remoteExploit, privEscalation).

```

```

/* --- ACTIVE_DIRECTORY --- */
vulExists(active_directory, 'CVE-2022-45141_active_directory', httpd).
vulProperty('CVE-2022-45141_active_directory', remoteExploit, privEscalation).

```

```

/* --- HISTORIAN_SERVER --- */
vulExists(historian_server, 'CVE-2021-3129_historian_server', httpd).
vulProperty('CVE-2021-3129_historian_server', remoteExploit, privEscalation).

/* --- WORKSTATION --- */
vulExists(workstation, 'CVE-2019-0708_workstation', httpd).
vulProperty('CVE-2019-0708_workstation', remoteExploit, privEscalation).

/* --- SWITCH --- */
vulExists(switch, 'CVE-2023-28578_switch', os).
vulProperty('CVE-2023-28578_switch', localExploit, privEscalation).

/* --- HMI --- */
vulExists(hmi, 'CVE-2020-12029_hmi', os).
vulProperty('CVE-2020-12029_hmi', localExploit, privEscalation).

/* --- ICCP_SERVER --- */
vulExists(iccp_server, 'CVE-2022-3388_iccp_server', os).
vulProperty('CVE-2022-3388_iccp_server', localExploit, privEscalation).

/* --- FEP --- */
vulExists(fep, 'CVE-2022-43722_fep', os).
vulProperty('CVE-2022-43722_fep', localExploit, privEscalation).

/* --- SWITCH --- */
vulExists(switch, 'CVE-2021-34769_switch', httpd).
vulProperty('CVE-2021-34769_switch', remoteExploit, dos).

/* --- APPLICATION_SERVER --- */
vulExists(application_server, 'CVE-2024-38286_application_server', httpd).
vulProperty('CVE-2024-38286_application_server', remoteExploit, dos).

/* --- HARDWARE_FIREWALL --- */
vulExists(hardware_firewall, 'CVE-2025-20253_hardware_firewall', httpd).
vulProperty('CVE-2025-20253_hardware_firewall', remoteExploit, dos).

/* --- SUBSTATION --- */
vulExists(substation, 'CVE-2025-55222_substation', httpd).
vulProperty('CVE-2025-55222_substation', remoteExploit, dos).

/* --- HMI --- */
vulExists(hmi, 'CVE-2025-2521_hmi', httpd).
vulProperty('CVE-2025-2521_hmi', remoteExploit, dos).

/* --- SUBSTATION --- */
vulExists(substation, 'CVE-2021-22778_substation', os).
vulProperty('CVE-2021-22778_substation', localExploit, privEscalation).

/* --- WORKSTATION --- */
vulExists(workstation, 'CVE-2025-47957_workstation', os).
vulProperty('CVE-2025-47957_workstation', localExploit, privEscalation).

/* --- APPLICATION_SERVER --- */

```

```

vulExists(application_server, 'CVE-2025-49124_application_server', os).
vulProperty('CVE-2025-49124_application_server', localExploit, privEscalation).

```

```

/* --- WORKSTATION --- */
vulExists(workstation, 'CVE-2022-23484_workstation', httpd).
vulProperty('CVE-2022-23484_workstation', remoteExploit, dos).

```

```

/* --- HISTORIAN_SERVER --- */
vulExists(historian_server, 'CVE-2020-10606_historian_server', os).
vulProperty('CVE-2020-10606_historian_server', localExploit, privEscalation).

```

```

/* --- HARDWARE_FIREWALL --- */
vulExists(hardware_firewall, 'CVE-2016-6367_hardware_firewall', os).
vulProperty('CVE-2016-6367_hardware_firewall', localExploit, privEscalation).

```

```

/* --- ICCP_SERVER --- */
vulExists(iccp_server, 'CVE-2020-6996_iccp_server', httpd).
vulProperty('CVE-2020-6996_iccp_server', remoteExploit, dos).

```

```

/* --- FEP --- */
vulExists(fep, 'CVE-2021-37185_fep', httpd).
vulProperty('CVE-2021-37185_fep', remoteExploit, dos).

```

```

/* --- HISTORIAN_SERVER --- */
vulExists(historian_server, 'CVE-2023-39477_historian_server', httpd).
vulProperty('CVE-2023-39477_historian_server', remoteExploit, dos).

```

```

/* --- ACTIVE_DIRECTORY --- */
vulExists(active_directory, 'CVE-2023-21816_active_directory', httpd).
vulProperty('CVE-2023-21816_active_directory', remoteExploit, dos).

```

```

/* --- HMI --- */
vulExists(hmi, 'CVE-2025-24482_hmi', os).
vulProperty('CVE-2025-24482_hmi', localExploit, dos).

```

```

/* --- ACTIVE_DIRECTORY --- */
vulExists(active_directory, 'CVE-2025-54882_active_directory', os).
vulProperty('CVE-2025-54882_active_directory', localExploit, privEscalation).

```

```

/* --- WORKSTATION --- */
vulExists(workstation, 'CVE-2025-53736_workstation', os).
vulProperty('CVE-2025-53736_workstation', localExploit, dos).

```

```

/* --- SWITCH --- */
vulExists(switch, 'CVE-2022-1015_switch', os).
vulProperty('CVE-2022-1015_switch', localExploit, dos).

```

```

/* --- FEP --- */
vulExists(fep, 'CVE-2023-38640_fep', os).
vulProperty('CVE-2023-38640_fep', localExploit, dos).

```

```

/* --- ICCP_SERVER --- */
vulExists(iccp_server, 'CVE-2025-39201_iccp_server', os).
vulProperty('CVE-2025-39201_iccp_server', localExploit, dos).

```

```

/* --- HMI --- */
vulExists(hmi, 'CVE-2024-4105_hmi', httpd).
vulProperty('CVE-2024-4105_hmi', remoteExploit, confloss).

/* --- SWITCH --- */
vulExists(switch, 'CVE-2022-40691_switch', httpd).
vulProperty('CVE-2022-40691_switch', remoteExploit, confloss).

/* --- HARDWARE_FIREWALL --- */
vulExists(hardware_firewall, 'CVE-2020-1997_hardware_firewall', httpd).
vulProperty('CVE-2020-1997_hardware_firewall', remoteExploit, confloss).

/* --- ICCP_SERVER --- */
vulExists(iccp_server, 'CVE-2020-10613_iccp_server', httpd).
vulProperty('CVE-2020-10613_iccp_server', remoteExploit, confloss).

/* --- FEP --- */
vulExists(fep, 'CVE-2022-29881_fep', httpd).
vulProperty('CVE-2022-29881_fep', remoteExploit, confloss).

/* --- SUBSTATION --- */
vulExists(substation, 'CVE-2023-0027_substation', httpd).
vulProperty('CVE-2023-0027_substation', remoteExploit, confloss).

/* --- APPLICATION_SERVER --- */
vulExists(application_server, 'CVE-2023-42795_application_server', httpd).
vulProperty('CVE-2023-42795_application_server', remoteExploit, confloss).

/* --- ACTIVE_DIRECTORY --- */
vulExists(active_directory, 'CVE-2020-15785_active_directory', httpd).
vulProperty('CVE-2020-15785_active_directory', remoteExploit, confloss).

/* --- WORKSTATION --- */
vulExists(workstation, 'CVE-2022-23280_workstation', httpd).
vulProperty('CVE-2022-23280_workstation', remoteExploit, confloss).

/* --- SUBSTATION --- */
vulExists(substation, 'CVE-2023-0898_substation', os).
vulProperty('CVE-2023-0898_substation', localExploit, dos).

/* --- HMI --- */
vulExists(hmi, 'CVE-2020-6980_hmi', os).
vulProperty('CVE-2020-6980_hmi', localExploit, confloss).

/* --- HARDWARE_FIREWALL --- */
vulExists(hardware_firewall, 'CVE-2020-2044_hardware_firewall', os).
vulProperty('CVE-2020-2044_hardware_firewall', localExploit, confloss).

/* --- ACTIVE_DIRECTORY --- */
vulExists(active_directory, 'CVE-2025-48064_active_directory', os).
vulProperty('CVE-2025-48064_active_directory', localExploit, confloss).

/* --- SUBSTATION --- */

```

```
vulExists(substation, 'CVE-2020-28214_substation', os).
vulProperty('CVE-2020-28214_substation', localExploit, confloss).

/* --- SWITCH --- */
vulExists(switch, 'CVE-2022-32296_switch', os).
vulProperty('CVE-2022-32296_switch', localExploit, confloss).

/* --- HISTORIAN_SERVER --- */
vulExists(historian_server, 'CVE-2021-43553_historian_server', httpd).
vulProperty('CVE-2021-43553_historian_server', remoteExploit, confloss).
```

ДОДАТОК В

Результати генерації графа атак аналізатором MulVAL (фрагмент). Текстовий вивід домінантного шляху атаки AP1 (витяг з AttackGraph.txt):

```
/* Ціль атаки: компрометація підстанції */
1,"execCode(substation,root)","OR",0
2,"RULE 2 (remote exploit of a server program)","AND",0
3,"netAccess(substation,tcp,80)","OR",0
4,"RULE 5 (multi-hop access)","AND",0
5,"hacl(fep,substation,tcp,80)","LEAF",1
4,5,-1

/* Крок 5: Компрометація шлюзу FEP */
6,"execCode(fep,root)","OR",0
7,"RULE 2 (remote exploit of a server program)","AND",0
8,"netAccess(fep,tcp,80)","OR",0
9,"RULE 5 (multi-hop access)","AND",0
10,"hacl(application_server,fep,tcp,80)","LEAF",1
9,10,-1
[...]

/* Крок 4: Компрометація Application Server */
11,"execCode(application_server,root)","OR",0
12,"RULE 2 (remote exploit of a server program)","AND",0
13,"netAccess(application_server,tcp,80)","OR",0
14,"RULE 5 (multi-hop access)","AND",0
15,"hacl(active_directory,application_server,tcp,80)","LEAF",1
14,15,-1
[...]

/* Крок 3: Компрометація Active Directory (накопичення привілеїв) */
16,"execCode(active_directory,root)","OR",0
17,"RULE 2 (remote exploit of a server program)","AND",0
18,"netAccess(active_directory,tcp,80)","OR",0
19,"RULE 5 (multi-hop access)","AND",0
20,"hacl(switch,active_directory,tcp,80)","LEAF",1
19,20,-1
[...]

/* Крок 2: Компрометація мережевого комутатора Switch */
21,"execCode(switch,root)","OR",0
22,"RULE 2 (remote exploit of a server program)","AND",0
23,"netAccess(switch,tcp,80)","OR",0
24,"RULE 5 (multi-hop access)","AND",0
25,"hacl(hardware_firewall,switch,tcp,80)","LEAF",1
24,25,-1
[...]

/* Крок 1: Проникнення через Hardware Firewall */
26,"execCode(hardware_firewall,root)","OR",0
```

```

27,"RULE 2 (remote exploit of a server program)","AND",0
28,"netAccess(hardware_firewall,tcp,80)","OR",0
29,"RULE 6 (direct network access)","AND",0
30,"haci(internet,hardware_firewall,tcp,80)","LEAF",1
29,30,-1

/* Початкова точка: Зловмисник в Інтернеті */
31,"attackerLocated(internet)","LEAF",1
29,31,-1
28,29,-1
27,28,-1

/* Застосування вразливостей (експлойти на шляху AP1) */
32,"networkServiceInfo(hardware_firewall,httpd,tcp,80,root)","LEAF",1
22,65,-1
33,"vulExists(hardware_firewall,'CVE-2024-
3400_hardware_firewall',httpd,remoteExploit,privEscalation)","LEAF",1
27,33,-1
26,27,-1
[...]
34,"networkServiceInfo(switch,httpd,tcp,80,root)","LEAF",1
22,34,-1
35,"vulExists(switch,'CVE-2021-34770_switch',httpd,remoteExploit,privEscalation)","LEAF",1
22,35,-1
21,22,-1
[...]
75,"networkServiceInfo(active_directory,httpd,tcp,80,root)","LEAF",1
17,75,-1
76,"vulExists(active_directory,'CVE-2022-
45141_active_directory',httpd,remoteExploit,privEscalation)","LEAF",1
17,76,-1
16,17,-1
[...]
85,"networkServiceInfo(application_server,httpd,tcp,80,root)","LEAF",1
12,85,-1
86,"vulExists(application_server,'CVE-2021-
44228_application_server',httpd,remoteExploit,privEscalation)","LEAF",1
12,86,-1
11,12,-1
[...]
125,"networkServiceInfo(fep,httpd,tcp,80,root)","LEAF",1
7,125,-1
126,"vulExists(fep,'CVE-2021-45033_fep',httpd,remoteExploit,privEscalation)","LEAF",1
7,126,-1
6,7,-1
[...]
127,"networkServiceInfo(substation,httpd,tcp,80,root)","LEAF",1
2,127,-1
128,"vulExists(substation,'CVE-2024-
11317_substation',httpd,remoteExploit,privEscalation)","LEAF",1
2,128,-1
1,2,-1

```