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
(підпис)
«_____»_____2025 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека та захист інформації»

на тему: Оцінка кібернадійності SCADA-систем критичної інфраструктури з використанням SMP

Виконав (-ла): здобувач вищої освіти II курсу, групи ФБ-41мп

Тостоган Євгенія Геннадіївна
(прізвище, ім'я, по батькові) (підпис)

Керівник: к.т.н., доцент кафедри Інформаційної безпеки,
Гальчинський Леонід Юрійович
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент:
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2025 року

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

Рівень вищої освіти – другий (магістерський)
Спеціальність – 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«___»_____2025 р.

ЗАВДАННЯ
на магістерську дисертацію здобувачу вищої освіти

Тостоган Євгенії Геннадіївні
(прізвище, ім'я, по батькові)

1. Тема роботи : Оцінка кібернадійності SCADA-систем критичної інфраструктури з використанням SMP
керівник роботи: Гальчинський Леонід Юрійович, к.т.н., доцент, доцент кафедри Інформаційної безпеки
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від 04 листопада 2025 р. № 4797-с

2. Термін подання здобувачем вищої освіти роботи 9 грудня 2025 р.

3. Вихідні дані до роботи: формалізована модель кібератаки на SCADA-систему критичної інфраструктури на основі напівмарковських процесів і систематизована інформація про кібератаки

4. Зміст роботи: аналіз архітектури SCADA/ICS і сценаріїв кібератак, побудова напівмарковської моделі розвитку атаки для оцінки кібернадійсності та аналіз результатів.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація.

6. Дата видачі завдання 8 вересня 2025

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Отримання завдання на магістерську дисертацію	08.09.2025	виконано
2	Пошук та опрацювання літературних джерел	09.09.2025-30.09.2025	виконано
3	Огляд та аналіз предметної області. Ознайомлення з архітектурою SCADA та загрозами, поняттям кібернадійності	01.10.2025-12.10.2025	виконано
4	Ознайомлення з напівмарковськими процесами для використання у вирішенні поставленої задачі	13.10.2025-24.10.2025	виконано
5	Розробка SMP-моделі: сценарії атак, стани, переходи, матриці ймовірностей	25.10.2025-09.11.2025	виконано
6	Оцінювання часових параметрів та ймовірностей переходів	10.11.2025-23.11.2025	виконано
7	Розрахунок MTTC та аналіз результатів	24.11.2025-30.11.2025	виконано
8	Оформлення магістерської роботи відповідно до методичних вказівок	01.12.2025-15.12.2025	виконано
9	Передзахист магістерської дисертації	16.12.2025	виконано
10	Захист магістерської дисертації	23.12.2025	

Здобувач вищої освіти _____ Євгенія ТОСТОГАН
(підпис) **(Власне ім'я, ПРІЗВИЩЕ)**

Керівник роботи _____ Леонід ГАЛЬЧИНСЬКИЙ
(підпис) **(Власне ім'я, ПРІЗВИЩЕ)**

РЕФЕРАТ

Робота складається з 4 розділів, містить 24 ілюстрації, 13 таблиць, 2 додатки та 27 літературних джерел, загальний обсяг роботи – 89 сторінок.

Метою роботи - підвищення безпеки SCADA-систем критичної інфраструктури за рахунок впровадження підходу до кількісної оцінки кібернадійності, що базується на показнику середнього часу до компрометації та враховує рівень підготовки атакуючих.

Об’єктом дослідження є SCADA/ICS-системи критичної інфраструктури та процеси їх функціонування в умовах кібервпливів.

Предметом дослідження є моделі та методи оцінювання кібернадійності SCADA-систем на основі напівмарковських процесів.

Методами дослідження – аналіз літературних джерел пов’язаних з тематикою, розгляд та аналіз архітектури SCADA-систем та їх вразливостей, напівмарковське моделювання сценаріїв кібератак, статистичний аналіз (визначення ймовірностей).

Результати роботи можуть бути використані для кількісної оцінки кібернадійності SCADA- та інших OT-систем, підтримки прийняття рішень щодо модернізації засобів захисту об’єктів критичної інфраструктури.

Результати роботи були опубліковані на II International Scientific and Theoretical Conference «Modern science and innovation: trends, challenges, and breakthroughs», с. 210-220.

Ключові слова: SCADA-система, критична інфраструктура, кібернадійність, напівмарковський процес, середній час до компрометації.

ABSTRACT

The work consists of 4 chapters and includes 24 illustrations, 13 tables, 2 appendix, and 27 literary references, the total volume of the work is 89 pages.

The purpose of the work is to improve the security of SCADA systems in critical infrastructure by introducing an approach to quantitative assessment of cyber reliability based on the average time to compromise indicator and taking into account the level of preparedness of attackers.

The object of the study is SCADA/ICS systems of critical infrastructure and the processes of their functioning under cyber impact.

The subject of the study is models and methods for assessing the cyber-reliability of SCADA systems based on semi-Markov processes.

The research methods are the analysis of literature related to the topic, examination and analysis of SCADA system architectures and their vulnerabilities, semi-Markov modelling of cyber-attack scenarios, and statistical analysis (probability estimation).

The results of the work can be used for quantitative assessment of the cyber-reliability of SCADA and other OT systems, as well as to support decision-making on the modernization of protection measures for critical infrastructure facilities.

The results of the study were published at the II International Scientific and Theoretical Conference “Modern science and innovation: trends, challenges, and breakthroughs”, p 210-220.

Keywords: SCADA system, critical infrastructure, cyber-reliability, semi-Markov process, mean time to compromise.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 8
ВСТУП 9
1 ОГЛЯД СТАНУ КІБЕРБЕЗПЕКИ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 11
1.1 Важливість критичної інфраструктури 11
1.2 Архітектура ICS та SCADA як ключовий компонент управління 13
1.3 Безпека SCADA 17
1.4 Поняття кібернадійності та її роль у критичній інфраструктурі 22
1.5 Огляд сучасних підходів до оцінки кібернадійності 24
Висновки до розділу 1 26
2 МОДЕЛЮВАННЯ ВПЛИВУ АТАК НА SCADA-СИСТЕМУ 28
2.1 Напівмарковські процеси у моделюванні кібератак 29
2.2 Сценарії атак та формалізація моделі 33
2.3 Визначення ймовірностей переходу транзитних станів 38
2.4 Методика оцінюваня 40
2.5 Реалізація МСМС та аналіз результатів 43
Висновки до розділу 2 49
3 ОЦІНКА MTTC 51
3.1 Навички атакуючих 51
3.2 Програмна реалізація 52
3.3 Отримані результати MTTC 54
Висновки до розділу 3 58
4 РОЗРОБКА СТАРТАП-ПРОЄКТУ 60
4.1 Опис ідеї стартап-проєкту 60
4.2 Технологічний аудит ідеї проєкту 64
4.3 Аналіз можливості запуску стартап-проєкту на ринок 65
4.4 Розробка ринкової стратегії продукту 72
4.5 Розробка маркетингової програми 74
Висновки до розділу 4 75

ВИСНОВКИ 76
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 78
Додаток А Лістинг програми 1 82
Додаток Б Лістинг програми 2 86

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SCADA – Supervisory Control and Data Acquisition – диспетчерська система керування та збору даних.

ICS – Industrial Control System – промислова система керування.

OT – Operational Technology – оперативні технології, сукупність апаратних і програмних засобів керування технологічними процесами.

DMZ – Demilitarized Zone – демілітаризована (проміжна) зона між корпоративною та зовнішньою/технологічною мережами.

HMI – Human–Machine Interface – інтерфейс «людина–машина» для взаємодії оператора з системою керування.

RTU – Remote Terminal Unit – віддалений термінальний пристрій (модуль збору даних і керування у полі).

PLC – Programmable Logic Controller – програмований логічний контролер для автоматизації технологічних процесів.

MTTC – Mean Time To Compromise – середній час до компрометації.

SMP – Semi-Markov Process – напівмарковський процес.

MCMC – Markov Chain Monte Carlo – методи Монте-Карло на основі марковських ланцюгів

ВСТУП

Стрімка цифровізація об’єктів критичної інфраструктури та інтеграція OT-середовищ із корпоративними IT-мережами суттєво підвищили ефективність управління технологічними процесами, але водночас розширили поверхню кібератак на ICS/SCADA. Інциденти в таких системах можуть спричиняти не лише втрати даних чи зупинку сервісів, а й фізичні наслідки для виробництва та безпеки населення. Тому актуальним є перехід від переважно якісного аналізу загроз до кількісного оцінювання кібернадійності SCADA-систем, зокрема з урахуванням часової динаміки атак і реальних сценаріїв компрометації.

Мета роботи полягає у підвищення безпеки SCADA-систем критичної інфраструктури за рахунок впровадження підходу до кількісної оцінки кібернадійності, що базується на показнику середнього часу до компрометації та враховує рівень підготовки атакуючих.

Об’єкт дослідження: SCADA/ICS-системи критичної інфраструктури та процеси їх функціонування в умовах кібервпливів.

Предмет дослідження: моделі та методи оцінювання кібернадійності SCADA-систем на основі напівмарковських процесів.

Методами дослідження є аналіз літературних джерел пов’язаних з тематикою, розгляд та аналіз архітектури SCADA-систем та їх вразливостей, напівмарковське моделювання сценаріїв кібератак, статистичний аналіз (визначення ймовірностей).

Наукова новизна дослідження полягає у впровадженні підходу до кількісної оцінки їх кібернадійності з використанням SMP на основі показника середнього часу до компрометації з урахуванням рівня підготовки атакуючих.

Практичне значення одержаних результатів полягає у можливості використання запропонованої моделі для кількісної оцінки кібернадійності

реальних SCADA-систем критичної інфраструктури, підтримки рішень щодо пріоритизації захисних заходів, прогнозування часу до компрометації та порівняння альтернативних конфігурацій безпеки на основі вимірюваних показників ризику.

Публікація за результатами досліджень: за тематикою магістерської дисертації було написано статтю на тему “Моделювання кібернадійності SCADA-систем критичної інфраструктури з використанням напівмарковських процесів”, яку було представлено на II International Scientific and Theoretical Conference «Modern science and innovation: trends, challenges, and breakthroughs».

1 ОГЛЯД СТАНУ КІБЕРБЕЗПЕКИ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Важливість критичної інфраструктури

Критична інфраструктура (КІ) відіграє ключову роль у забезпеченні стабільності та безпеки сучасного суспільства. Вона охоплює системи та активи, безперебійне функціонування яких є життєво необхідним для економіки, охорони здоров'я, безпеки та соціального добробуту населення. З огляду на технологічний прогрес і зростаючу взаємозалежність систем, значення критичної інфраструктури постійно зростає, а її визначення та підходи до захисту еволюціонують.

Європейський Союз приділяє особливу увагу захисту критичних об'єктів, визначаючи їх як елементи, що забезпечують надання основних послуг. Згідно з Директивою ЄС 2022/2557, держави-члени повинні ідентифікувати власні критичні об'єкти, аналізувати ризики та впроваджувати заходи для підвищення стійкості до загроз. До таких секторів належать енергетика, транспорт, банківська сфера, охорона здоров'я, цифрові інфраструктури, водопостачання, державне управління та інші (рис. 1.1). [1]

Сучасні системи критичної інфраструктури, оснащені цифровими компонентами та автоматизованими системами управління, таких як система диспетчерського контролю та збору даних (SCADA), забезпечують високу ефективність, але одночасно піддаються підвищеному ризику кібератак. Зростання взаємозв'язку критичної інфраструктури із зовнішніми системами збільшує кількість потенційних точок доступу для зловмисників, що робить її захист та стабільність одним із ключових пріоритетів.

Таким чином, наслідки кібератак на критичну інфраструктуру можуть мати надзвичайно негативні наслідки, створюючи серйозні загрози для національної безпеки та економічної стабільності. Порушення функціонування систем КІ здатні ускладнити повсякденне життя та навіть

зупинити критично важливі послуги, що акцентує потребу у всебічному захисті від кібератак.

Рисунок 1.1 - Критичні сектори суб'єктів господарювання

Приклади атак на енергетичний сектор

Останні десятиліття характеризуються суттєвим зростанням кількості кібератак на енергетичні об’єкти через розвиток цифрових технологій. Як приклад, тільки атаки програм-вимагачів вже демонструють масштабність загроз, з якими стикається енергетичний сектор, хоча вони становлять лише частину ширшої картини кіберризиків. У звіті компанії Sophos, опублікованому в липні 2024 року, 67% із 275 опитаних керівників у сфері кібербезпеки та IT з енергетичного, нафтогазового та комунального секторів у 14 країнах повідомили про атаки програм-вимагачів протягом останнього року.[2] Хоча ці показники залишаються стабільними, звіт TrustWave за січень 2025 року зафіксував 80% зростання кількості таких атак у 2024 році порівняно з попереднім роком.[3]

Однак масштаби загроз виходять далеко за межі програм-вимагачів. Досить відомим є випадок, який стався у грудні 2015 року, SCADA-система державної енергетичної інфраструктури України стала об’єктом цілеспрямованої атаки, яка спричинила масштабне відключення електроенергії, що торкнулося понад 225 тисяч споживачів [4].

У 2019 році аналогічна атака у Венесуелі призвела до знеструмлення 11 штатів. Після двох днів аварійних робіт близько 30 % житлових районів залишалися без електропостачання [5].

У квітні 2021 року внаслідок кібератаки на найбільшого оператора газопроводів США, Colonial Pipeline, було призупинено його діяльність. Це змусило 17 штатів і округ Колумбія оголосити надзвичайний стан для забезпечення стабільного постачання пального. Зловмисники викрали 100 Гб конфіденційної інформації та висунули вимогу щодо сплати викупу [6].

Кібератаки на енергетичні об’єкти - це лише зовнішній прояв глибших проблем, пов’язаних із складністю та взаємозалежністю сучасних технологій. Енергетика становить лише одну частину великої та складної системи критичної інфраструктури, інші сектори так само взаємопов’язані та вразливі до загроз. Це означає, що проблема захисту КІ є набагато масштабнішою.

1.2 Архітектура ICS та SCADA як ключовий компонент управління

Сучасні системи критичної інфраструктури характеризуються високим рівнем автоматизації та інтеграцією інформаційно-комунікаційних технологій. Для забезпечення ефективного управління та захисту таких систем застосовується багаторівнева архітектура, що визначає взаємодію між рівнями виробництва, контролю та корпоративного управління. Для опису взаємозв’язку між операційними технологіями (OT) та інформаційними системами (IT) застосовується модель Пердью (Purdue Model), яка дозволяє

формалізувати рівні взаємодії між польовими пристроями, системами керування та корпоративними мережами.

На рисунку 1.2, зображено багаторівневу архітектуру промислової системи управління (ICS), побудовану відповідно до моделі Пердью (Purdue Model for ICS Security):

- Рівень 0 - Fieldbus Network (польова мережа)

  На цьому рівні розташовані фізичні польові пристрої (Field Devices) - сенсори, датчики, приводи, які безпосередньо взаємодіють із технологічним обладнанням. Вони збирають дані та передають їх контролерам.
- Рівень 1 - Controller Network (мережа контролерів)

  Містить віддалені термінали (RTU), програмовані логічні контролери (PLC), інтелектуальні електронні пристрої (IED), що приймають сигнали з польових пристроїв, виконують обробку даних та керують технологічними процесами. Цей рівень відповідає за автоматизацію на об’єкті.
- Рівень 2 - Supervisory Network (супервізорна мережа, центр керування)

  Тут розміщені станції операторів (HMI, Workstations) і SCADA MTU, які здійснюють моніторинг та керування процесами. Оператори можуть взаємодіяти з системою в реальному часі через інтерфейс HMI.
- Рівень 3 - DMZ / Operational Traffic (операційний рівень)

  Демілітаризована зона (DMZ) виконує функцію контролю обміну даними між виробничими системами (OT) і корпоративною мережею (IT), забезпечуючи безпечну взаємодію між цими двома середовищами. Її основне призначення - фільтрація та перевірка внутрішньої комунікації, щоб запобігти несанкціонованому доступу та поширенню загроз. Відповідно до моделі Пердью, увесь трафік між мережами OT та IT має проходити саме через DMZ, де здійснюється його моніторинг і контроль. Проте на практиці це правило часто порушується,

переважно через складність технічної реалізації, загалом, через недостатню увагу компаній до аспектів безпеки на етапі побудови галузі [8]. Цей рівень може містити application servers, historian (для зберігання історичних даних) і domain controller, що підтримують роботу SCADA та забезпечують безпечний обмін даними.

- Рівень 4 - Corporate Network (корпоративна мережа)

  Найвищий рівень, який з'єднаний із Інтернетом і включає веб-сервери, поштові сервери та бізнес-додатки. Він використовується для управління підприємством, аналізу виробничих показників та прийняття стратегічних рішень.

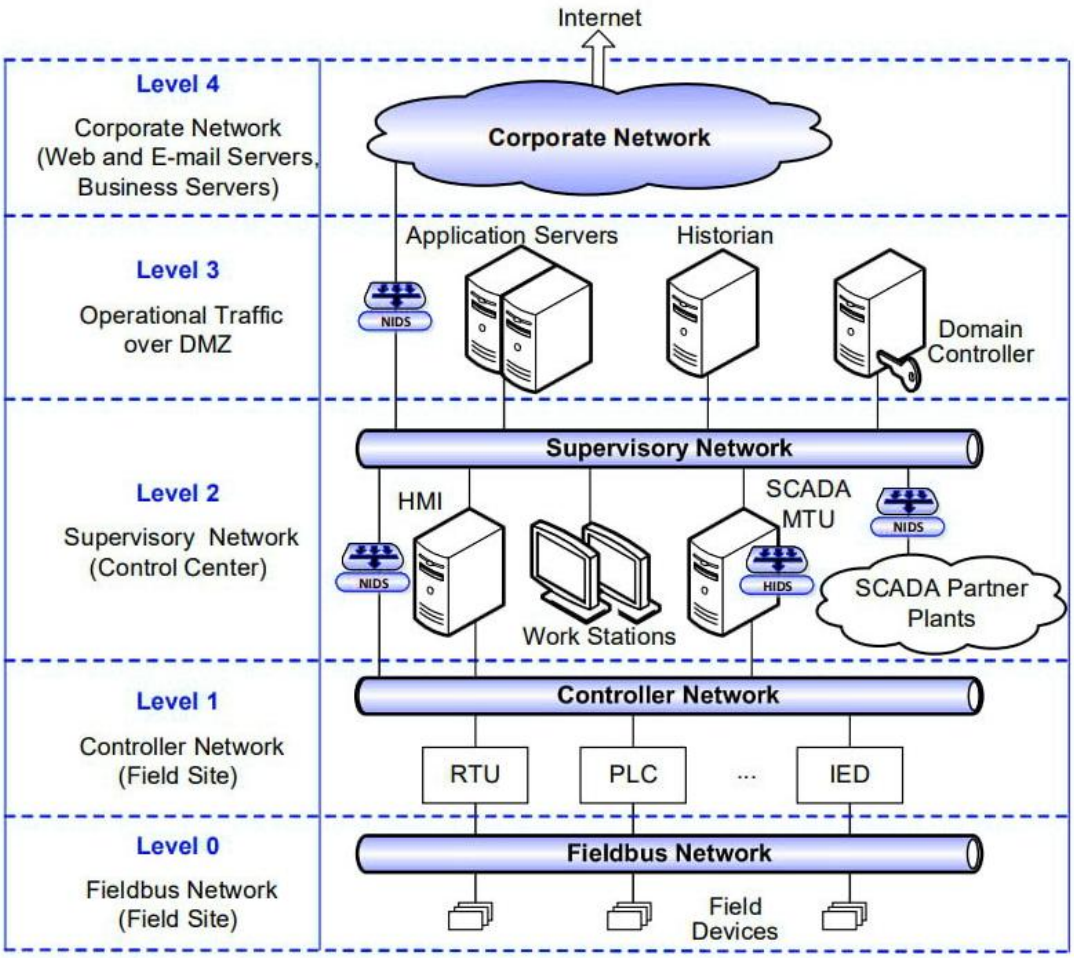

Рисунок 1.2 - Архітектура моделі ICS Purdue[7]

SCADA

Сервер SCADA вважається серцем центру управління. Основною метою системи диспетчерського контролю та збору даних (SCADA) є збір даних у реальному часі, моніторинг та контроль обладнання та процесів на відповідній інфраструктурі. Основні компоненти SCADA можна класифікувати відповідно до їхніх функцій[9]:

- Наглядовий контроль: Основна функція SCADA реалізується через HMI, який забезпечує моніторинг промислових процесів. Центральний наглядовий контролер, головний термінал (MTU), взаємодіє з польовими пристроями, RTU, через промислову мережу.
- Збір даних: Дані надходять із програмованих логічних контролерів та RTU. На основі заданої логіки PLC передає оброблені дані до центру управління для відображення на HMI оператору. Процес роботи PLC включає три етапи: зчитування вхідних сигналів, виконання програми управління та оновлення вихідних пристроїв. RTU та PLC виконують схожі функції як інтерфейси між SCADA і польовими пристроями, однак відрізняються масштабом і способом взаємодії: RTU оптимальні для великих географічних територій завдяки бездротовому зв’язку, тоді як PLC більш ефективні для локального управління.
- Зберігання даних: Для архівації інформації системи SCADA зазвичай використовують бази даних SQL з часовими мітками. Спеціалізоване програмне забезпечення Historian інтегрується в SCADA для збору та збереження даних у реальному часі з різних пристроїв.
- Обмін даними: Взаємодія між компонентами SCADA здійснюється через стандартизовані протоколи зв’язку, що забезпечують надійний і ефективний потік інформації в системі.

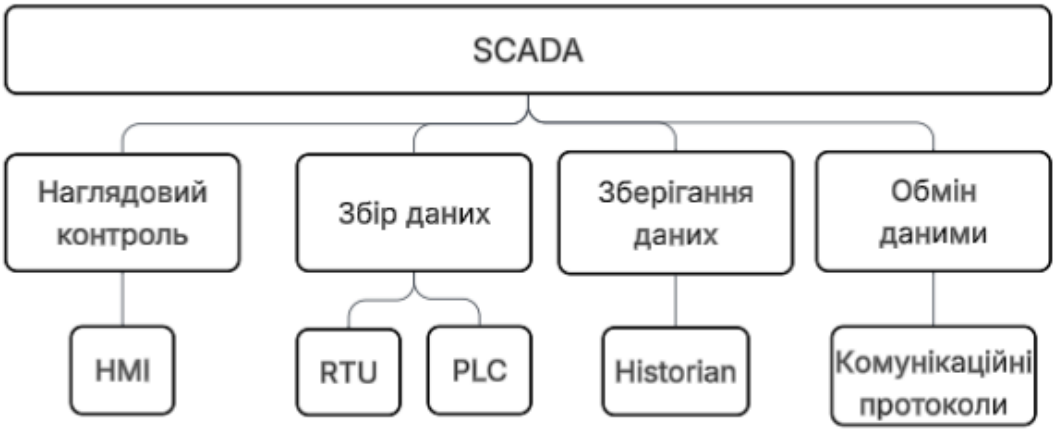

Рисунок 1.3 — Компоненти SCADA

Підсумовуючи, SCADA виконує роль ключового вузла обміну інформацією та управління технологічними процесами в системах КІ. Через свою критичну роль у функціонуванні систем критичної інфраструктури, її захист стає пріоритетним завданням, що вимагає комплексних заходів з кіберзахисту.

1.3 Безпека SCADA

Подібно до інших складних технічних систем, SCADA-системи є вразливими до різноманітних типів атак - як фізичних дій з боку людини, так і впливу шкідливого програмного забезпечення, здатного пошкодити систему або використати її ресурси у власних цілях. Будь-яке втручання в роботу SCADA може становити серйозну небезпеку. Оскільки енергетичні мережі є критичною складовою національної безпеки, як раніше зазначалося, будь-яка атака на них може призвести до масштабних наслідків. За даними досліджень, кількість атак на SCADA-системи з початку XXI століття зросла щонайменше у десять разів[10].

Ключова проблема полягає в тому, що більшість SCADA-систем були розроблені ще до появи сучасних комп’ютерних та комунікаційних технологій. Унаслідок цього їх розвиток відбувався повільніше, ніж еволюція

IT-інфраструктури та мереж зв’язку. Попри те, що ранні SCADA-системи вважалися безпечними завдяки обмеженню фізичного доступу, нинішні можливості віддаленого управління й мережевої взаємодії породжують нові виклики для кіберзахисту. Основним підходом до забезпечення безпеки досі залишається контроль та обмеження несанкціонованого доступу. Водночас складність мережевої інфраструктури часто призводить до недооцінки наявних вразливостей, що, своєю чергою, спричиняє численні інциденти безпеки в останні роки.

Загрози в мережах SCADA загалом можна класифікувати за трьома основними типами:

- втрата доступності;
- втрата цілісності;
- втрата конфіденційності[11].

Втрата доступності

Втрата доступності передбачає порушення стабільного та своєчасного доступу до систем чи даних, що є критично важливим для безперервного функціонування SCADA. Такі збої можуть призвести до затримок або неможливості виявлення та локалізації несправностей, а також ускладнити процес відновлення електропостачання в аварійних ситуаціях, наприклад, під час масштабних відключень електроенергії. Крім того, зниження доступності негативно впливає на ефективність усього ланцюга енергопостачання, викликаючи збої в роботі обладнання та зменшення продуктивності системи загалом.

Втрата цілісності

Порушення цілісності даних у системах SCADA означає несанкціоноване змінення, підробку або знищення інформації, що безпосередньо впливає на правильність функціонування технологічних процесів. Такі дії можуть призвести до серйозних наслідків — від

помилкового відображення стану обладнання та неправильних керуючих рішень до аварій чи фізичних пошкоджень елементів критичної інфраструктури.

Щоб запобігти таким загрозам, необхідно впроваджувати комплексні засоби перевірки достовірності даних. Для захисту від внутрішніх зловмисників доцільно застосовувати механізми цифрового підпису та автентифікації джерела даних, що гарантують справжність походження інформації та неможливість її зміни без виявлення. У випадку зовнішніх атак ефективним засобом є коди автентифікації повідомлень (MAC), які забезпечують контроль цілісності при передачі даних між компонентами системи. Крім того, важливим напрямом є впровадження журналювання змін і механізмів контролю версій даних, що дозволяють відстежувати будь-які спроби несанкціонованого втручання.

Втрата конфіденційності

Втрата конфіденційності означає несанкціоноване розкриття, перехоплення або аналіз інформації, що передається між компонентами SCADA. Зловмисники можуть отримати доступ до конфіденційних даних, наприклад, до показників енергоспоживання або параметрів керування технологічним обладнанням, що створює ризики як для окремих користувачів, так і для всієї енергетичної інфраструктури.

Типовим прикладом є перехоплення даних (sniffing) у комунікаційних каналах між віддаленими термінальними пристроями (RTU), інтелектуальними електронними пристроями (IED) та центральною системою управління. Для мінімізації таких ризиків необхідно впроваджувати шифрування трафіку за допомогою сучасних криптографічних протоколів (наприклад, TLS або IPSec), використовуючи захищене управління ключами. Також важливо застосовувати сегментацію мережі, ізоляцію критичних компонентів і багаторівневі механізми автентифікації користувачів.

Отже, традиційні принципи інформаційної безпеки - цілісність, доступність і конфіденційність - формують основу захисту SCADA-систем, однак у сучасних умовах цього вже недостатньо та ефективність захисту залежить від здатності системи витримувати як зовнішній тиск, так і внутрішні загрози. Зовнішні атаки можуть бути спрямовані на порушення комунікацій або компрометацію компонентів мережі, тоді як внутрішні часто пов’язані з людським фактором, помилками персоналу або зловмисними діями всередині організації.

Вразливості

Відповідно до досліджень роботи [9] вразливості SCADA можна поділити на два великих класи:

- проблеми впровадження – вразливості, спричинені помилками реалізації в дизайні та архітектурі;
- проблеми неправильної конфігурації безпеки – вразливості, що виникають через реалізацію слабких методів безпеки.

До вразливостей реалізації програмного забезпечення відносять неправильні обмеження пам’яті й помилки в обробці даних. Коли в SCADA-компоненті (HMI, сервер, PLC/RTU-модуль, інженерна станція) некоректно задані межі буферів або відсутня перевірка розміру й формату вхідних повідомлень, це створює умови для переповнення буфера. Такі помилки напряму ведуть до відмов у сервісі (DoS) або до корупції пам’яті, а в окремих випадках - до виконання довільного коду в процесі SCADA.

Наступним джерелом проблем є недостатня валідація і нейтралізація вхідних даних у прикладних та веб-компонентах SCADA. Багато сучасних SCADA-рішень мають веб-HMI, панелі керування, API або бази даних Historian. Якщо такі модулі приймають неочищені дані, виникають типові для веб-середовища, але критичні для OT уразливості: SQL-ін’єкції (через неправильну санітизацію параметрів запитів), XSS (коли у веб-сторінку

можна вставити шкідливий скрипт), CSRF (нав’язування виконання дій від імені легітимного користувача), а також path traversal (обхід файлових обмежень через підставні шляхи). Для SCADA наслідки тяжчі, ніж у звичайних IT-системах: злам веб-інтерфейсу часто стає точкою входу до технологічної мережі.

Ще одним джерелом вразливостей є недостатньо надійні механізми автентифікації та управління обліковими даними. У системах SCADA часто спостерігаються такі проблеми, як:

- обхід автентифікації - наявність альтернативних шляхів доступу без належної перевірки користувача.
- атаки типу capture-replay - перехоплення та повторне використання автентифікаційних повідомлень для отримання доступу.
- слабкий захист паролів - наприклад, зберігання хешів без використання «солі» (unsalted hashes), що значно спрощує їх підбір за допомогою райдужних таблиць.

Особливо небезпечними є випадки використання дефолтних або hard-coded паролів і ключів. Якщо пристрій або сервіс постачається з відомими за замовчуванням обліковими даними чи не передбачає можливості їх зміни, зловмисник фактично отримує готовий «бекдор» у систему.

Ще одна категорія вразливостей пов’язана з некоректним контролем доступу та відсутністю належної перевірки автентичності даних. Якщо PLC, RTU або інший компонент приймає команди без перевірки прав доступу чи не підтверджує достовірність отриманих повідомлень, з’являється можливість надсилання неавтентифікованих пакетів. Це створює ризик зміни технологічних параметрів або навіть модифікації логіки керування.

Ще одна категорія вразливостей стосується криптографічних та протокольних слабкостей. Багато промислових протоколів були розроблені для роботи в ізольованих мережах, тому не мають вбудованого шифрування

та сучасних механізмів автентифікації. Відсутність або слабкість криптографічних механізмів відкриває можливості для перехоплення трафіку, аналізу команд, а також їх підміни між MTU та польовими пристроями. Це, у свою чергу, призводить до витоку даних, порушення цілісності телеметрії та керуючих сигналів і створює основу для більш складних атак.

Таким чином, з огляду на зростання кількості кібератак та ускладнення їхніх механізмів, дедалі важливішою стає здатність системи зберігати працездатність навіть у кризових умовах. Ця здатність формує основу кібернадійності, яка визначає рівень довіри до інформаційних і технологічних систем критичної інфраструктури та характеризує їхню готовність функціонувати без збоїв у динамічному середовищі загроз.

1.4 Поняття кібернадійності та її роль у критичній інфраструктурі

У сучасному світі, де критична інфраструктура дедалі більше залежить від цифрових технологій, питання її захищеності набуває особливої актуальності. Традиційні підходи до кібербезпеки вже не завжди здатні забезпечити необхідний рівень стійкості до складних та цілеспрямованих атак. У цьому контексті все більшого значення набуває поняття кібернадійності - здатності системи не лише протистояти загрозам, а й зберігати функціональність, швидко відновлюватися після інцидентів та адаптуватися до нових умов.

Кібернадійність (cyber reliability) — це здатність системи зберігати коректне надання послуги з прийнятною частотою та тривалістю відмов попри наявність кіберризиків. У межах загальної теорії dependability кібернадійність безпосередньо пов’язана з класичними атрибутами надійності/безвідмовності, доступності та підтримуваності[13]. Формально

вона вимірюється через імовірності відмов і часові індикатори: MTTF/MTBF, Availability, у кібер-контексті — TTC/MTTC (час/середній час до компрометації), а також частки часу, коли функції лишаються неушкодженими. [12]

Коли інцидент усе ж настає, в дію вступає кіберстійкість, що описує глибину відхилення функції та швидкість повернення до номінального режиму. Поняття кібернадійності тісно пов’язане з концепцією кіберстійкості (cyber resilience) і розглядається як складова абсорбційної здатності системи, що дозволяє їй поглинати вплив кіберзагрози на певному етапі кібератаки. [14]. Відповідно до дослідження [15] поняття стійкості в межах окремих дисциплін має спільні концептуальні основи, хоча й розглядається з різних точок зору:

- Інфраструктурні системи: Стійкість визначається як здатність системи зменшувати масштаб і тривалість порушень, що виникають унаслідок зовнішніх впливів. Вона базується на здатності передбачати загрози, поглинати їхній вплив, адаптуватися до змін і швидко відновлюватися.
- Економічні системи: Стійкість проявляється у здатності реагувати на ризики таким чином, щоб мінімізувати економічні втрати на рівні окремих підприємств і ринків загалом. Це включає виживання та адаптацію бізнесу після ринкових або екологічних потрясінь.
- Соціальні системи: Стійкість громади полягає у здатності витримувати соціальні, політичні та економічні зміни, зберігаючи функціональність і здатність до розвитку в умовах стресу та нестабільності.
- Організаційні системи: Стійкість організації визначається її здатністю виявляти ризики та ефективно реагувати на порушення, що впливають на ключові компетенції, стратегії та внутрішню координацію.

Згідно зі стандартом IEEE 610.12.1990, надійність визначається як здатність системи функціонувати коректно за умов надзвичайних або несприятливих впливів.

Таким чином, поняття надійності можна адаптувати до систем критичної інфраструктури, де воно трактується як здатність витримувати та зменшувати інтенсивність і/або тривалість порушень.

У контексті критичної інфраструктури надійність означає здатність системи забезпечувати безперервність основних функцій навіть за умов зовнішніх або внутрішніх загроз. Коли мова йде про **кібернадійність**, це поняття розширюється і охоплює здатність інформаційно-комунікаційних систем протистояти кіберінцидентам, зберігати цілісність, доступність та конфіденційність даних.

Таким чином, кібернадійність є одним з ключових елементів забезпечення безпеки критичної інфраструктури в умовах зростаючих кіберзагроз. Її роль полягає у гарантуванні безперервності критичних процесів, збереженні цілісності даних та запобіганні порушенням, що можуть призвести до масштабних наслідків.

1.5 Огляд сучасних підходів до оцінки кібернадійності

Існує багато фреймворків, які допомагають організаціям підвищити ефективність кіберзахисту, наприклад NIST, ISO, PCI DSS. Вони дозволяють оцінити ризики, вразливості та сформувати стратегії захисту. Однак традиційні підходи до кібербезпеки вже не завжди здатні забезпечити необхідний рівень стійкості до складних та цілеспрямованих атак. Більшість моделей не враховують надійність системи[4].

Більшість існуючих методів оцінювання кібернадійності мають певні обмеження. Для їх подолання дослідники застосовують різноманітні техніки, серед яких - якісні та кількісні методи, моделювання, симуляції, воєнні ігри

(wargaming) та red teaming. Якісні оцінки забезпечують суб’єктивне уявлення про рівень надійності, тоді як ресурсоємні методи - моделювання, симуляція, воєнні сценарії та командне тестування - дозволяють комплексно оцінити реакцію системи на множинні або тривалі кіберзагрози.

У наукових працях також розглядаються траєкторії стійкості, що також впливає на надійність, поширення впливу, динамічні підходи, а також імовірнісні та статистичні моделі. Зокрема, моделювання та симуляція є ефективними інструментами для аналізу складних соціотехнічних систем, таких як електроенергетичні мережі, які є критично важливими для національної безпеки.

У роботі [18] виокремлено три основні групи технік оцінювання кіберстійкості:

- Методи оцінювання кіберстійкості, включаючи аналітичні, якісні та кількісні підходи;
- Методи командної роботи та тестування;
- Сучасні техніки, що включають моделювання, машинне навчання та симуляції, з використанням ймовірнісних, оптимізаційних та нечітких моделей логіки.

У межах цієї роботи ці групи доцільно розглядати як взаємодоповнювальні інструменти формування та верифікації показників кібернадійності SCADA-систем. На відміну від загального поняття кіберстійкості, яке фокусується на здатності системи протистояти та відновлюватися після атак, кібернадійність акцентує увагу на збереженні критичних властивостей SCADA у часі під дією кібервпливів. Передусім ідеться про підтримання доступності та цілісності процесів керування, а також про прогнозування деградації цих властивостей при реалізації типових сценаріїв атак.

Аналітичні, якісні та кількісні методи забезпечують перехід від опису загроз до вимірюваних показників кібернадійності. Якісні підходи формують

перелік релевантних вразливостей і сценаріїв атак для SCADA, а кількісні дозволяють обчислювати метрики на кшталт імовірності компрометації, інтенсивностей переходів між етапами атаки та очікуваного часу до компрометації (MTTC/ET). Саме ці часові й імовірнісні характеристики і відображають рівень кібернадійності системи.

Як засвідчує аналіз наукових джерел, оцінювання кібернадійності SCADA спирається на широкий спектр підходів. Кожен із цих інструментів розкриває різні аспекти надійної роботи системи під кібервпливами та має власні сильні сторони й обмеження, а їх поєднання дає змогу отримати більш повну й об’єктивну картину ризиків, часових характеристик компрометації та здатності SCADA зберігати критичні властивості в динамічному середовищі. Така різноманітність підходів свідчить про багатогранність поняття кібернадійності та необхідність його глибокого аналізу в контексті сучасних викликів.

Висновки до розділу 1

У першому розділі показано, що критична інфраструктура є основою життєзабезпечення держави й суспільства, тому її стійкість до кібервпливів безпосередньо визначає рівень національної безпеки та безперервність надання ключових послуг. З огляду на це, системи ICS/SCADA, які відповідають за моніторинг і керування технологічними процесами, розглянуто як центральний елемент функціонування об’єктів критичної інфраструктури, а їх багаторівнева архітектура - як фактор, що одночасно забезпечує керованість процесів і формує широку поверхню атаки.

Проаналізовано стан безпеки SCADA та встановлено, що сучасні загрози для OT-середовища зумовлені поєднанням історично застарілих протоколів і механізмів захисту, інтеграцією з IT-мережами, а також наявністю типових уразливостей реалізації й конфігурації. Наслідки кібератак у SCADA виходять за межі інформаційних втрат і можуть

призводити до порушення доступності, цілісності керування та фізичних інцидентів на об’єктах, що підкреслює пріоритетність комплексного підходу до захисту таких систем.

У розділі обґрунтовано поняття кібернадійності як здатності ICS/SCADA зберігати критичні властивості функціонування у часі за умов кібервпливів. Огляд сучасних підходів до оцінки кібернадійності засвідчив наявність широкого спектра методів - від якісних і аналітичних оцінок до кількісного моделювання, симуляцій та тестування - кожен з яких висвітлює різні аспекти проблеми. Це підтвердило необхідність використання формалізованих часових і ймовірнісних моделей, здатних описувати динаміку компрометації та надавати вимірювані метрики, що створює підґрунтя для подальших розділів і вибору підходу для кількісної оцінки кібернадійності SCADA-систем.

2 МОДЕЛЮВАННЯ ВПЛИВУ АТАК НА SCADA-СИСТЕМУ

Як можна зрозуміти з першого розділу, SCADA-системи відіграють критичну роль в управлінні критичною інфраструктурою, але водночас є вразливими до різноманітних кіберзагроз. Тому безпека SCADA-інфраструктури визначає стійкість та надійність усієї системи КІ. Для оцінювання рівня кібернадійності важливо не лише визначати вразливі елементи та потенційні загрози, а й кількісно описувати процес реалізації кібератак, враховуючи їхню тривалість і ймовірність успіху на кожному етапі. Саме такий підхід дозволяє зрозуміти, як конкретні дії зловмисника впливають на загальний стан безпеки системи, і які ланки є найуразливішими.

З огляду на значущість впливу різних типів атак на стійкість SCADA-систем та прагнення охопити найпоширеніші і потенційно найнебезпечніші сценарії, було вирішено зосередитися на двох класифікаційних групах загроз. Для практичного дослідження було обрано два основні класи сценаріїв атак: зовнішні та внутрішні. Зовнішні атаки передбачають проникнення через мережеві або інтернет-канали, сканування системи, експлуатацію вразливостей і подальшу ескалацію привілеїв. Внутрішні загрози, що реалізуються особами з легітимним доступом до системи, можуть мати більший руйнівний потенціал порівняно із зовнішніми кібератаками через можливість цілеспрямованого впливу на критичні компоненти інфраструктури.

Для оцінки стійкості SCADA-систем до кібератак застосовується метрика MTTC (Mean Time To Compromise). Вона дозволяє кількісно вимірювати час, необхідний для успішної реалізації атаки, і перетворює абстрактні сценарії загроз на зрозумілі та порівнянні показники. Одним з варіантів оцінки середнього часу до компрометації (MTTC) є застосування напівмарковського процесу (SMP) як базової моделі поведінки зловмисника та еволюції атаки в часі, запропонований в [19]. SMP дозволяє моделювати залежності між

кроками та враховувати, що час перебування в стані може мати загальну (неекспоненційну) розподілену природу, що робить модель більш реалістичною для прикладних сценаріїв SCADA. Такий підхід дозволяє враховувати часові характеристики атак, їхню послідовність та ймовірність успішного проникнення, що є ключовими для оцінки кібернадійності енергетичних систем.

2.1 Напівмарковські процеси у моделюванні кібератак

Марковський процес — це стохастична модель, у якій система переходить між дискретними станами з певними ймовірностями. Основна властивість такого процесу полягає в тому, що наступний стан залежить виключно від поточного, а не від послідовності попередніх, що дозволяє спростити аналіз динаміки системи [20]. У випадку дискретного набору станів марковський процес повністю визначається поточним станом системи.

Напівмарковський процес (SMP) — процес, який здійснює переходи від стану до стану, як і марковський процес, але в якому час, проведений у кожному стані перед переходом до наступного стану, є довільною випадковою величиною, що залежить від наступного стану, в який перейде процес. У класичному марковському процесі майбутня еволюція системи повністю визначається її поточним станом: розподіл наступного стану не залежить від тривалості перебування в поточному стані. У безперервному часі це еквівалентно припущенню про експоненційний, тобто безпам’ятний, розподіл часу перебування. У напівмарковському процесі зазначене обмеження знімається: для кожної пари станів може бути задано довільний розподіл часу перебування, що дає змогу явно враховувати часові характеристики станів. Завдяки цьому напівмарковський підхід є більш гнучким та придатним для моделювання систем, у яких «вік» стану істотно впливає на ймовірність переходу.

У контексті моделювання кібератак на SCADA-системи важливо не лише враховувати ймовірність переходу між станами атаки, але й час, який атакуючий витрачає на кожен етап проникнення. Саме цей часовий аспект є критичним для оцінки кібернадійності енергетичної системи, зокрема при розрахунку середнього часу до компрометації (MTTC).

Теоретичне підґрунтя

У загальному випадку система, що описується SMP, може перебувати в одному з дискретних станів $S = \{1,2, \dots, n\}$. Перехід між станами відбувається у випадкові моменти часу, а проміжок часу між переходами — час очікування або тривалість перебування в стані — визначається довільним розподілом і може залежати як від поточного, так і від наступного стану.

Дискретний простір станів SMP - це стохастичний процес $\{X(t): t \geq 0\}$ з траєкторією

$$X(t) = \xi_N(t) \tag{2.1}$$

що пов’язана з марковським процесом оновлення (MRP) $\{(\xi_n \vartheta_n): n \in \mathbb{N}_0\}$ з початковим розподілом $p = [p_i(0): i \in S]$ та ядром $H(t) = \left[H_{ij}(t): i, j \in S\right], t \geq 0$, де S - скінченний дискретний простір станів. [21]

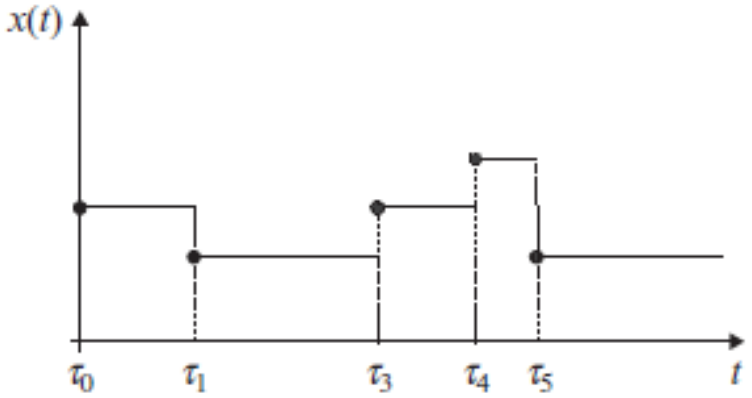

Рисунок 2.1 - Приклад траєкторії напівмарковського процесу (SMP)

Рисунок 2.1 показує графік, який є східчастою функцією, яка показує, як змінюється стан x(t) у часі. Зміни відбуваються у моменти $\tau_0, \tau_1, \tau_3, \tau_4, \tau_5$, між цими моментами стан залишається незмінним, що ілюструє перебування в одному стані протягом певного часу - ключова особливість SMP.

У межах поглинаючих дискретних марковських ланцюгів фундаментальна матриця визначається як:

$$N = (I - Q)^{-1} = I + Q + Q^2 + \cdots \quad (2.2)$$

де Q - матриця переходів між транзитними станами. Кожен елемент n_{ij} - це очікувана кількість відвідувань транзитного стану j, якщо процес стартує з транзитного стану i, до моменту поглинання. [22] Матриця N існує, якщо $\rho(Q) < 1$, що еквівалентно поглинанню з імовірністю 1.

З визначення SMP також випливає, що випадкова послідовність $\{X(\tau_n): n \in \mathbb{N}_0\}$ є однорідним марківським ланцюгом з простором станів S, де:

$$p_{ij} = \lim_{t \to \infty} H_{ij}(t). \quad (2.3)$$

Матриця переходів між транзитними n станами буде мати наступний вигляд:

$$Q = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{bmatrix}$$

Рисунок 2.2 – Матриця переходів SMP моделі

MTTC - це середній час, за який напівмарковський процес досягає абсорбуючого стану (тобто стану компроментації системи). “скільки разів заходимо в кожен стан” × “скільки триває цей стан” у сумі:

$$MTTC = \sum_{j \in S_T} n_j T_j \quad (2.4)$$

n_j— середня кількість разів, коли стан j був відвіданий до досягнення кінцевого стану відмови, а T_j — середній час перебування в стані j.

Для кожного стану в наборі перехідних станів S_T, середня кількість відвідувань n_j може бути виражена як:

$$n_j = p_j + \sum_i n_i p_{ij},\ i,j \in S_T \quad (2.5)$$

де p_j є ймовірністю того, що стан j є початковим станом дискретного марковського ланцюга (DTMC). Припускаємо, що атака починається з хорошого стану G. Таким чином, $p_G=1$, в іншому випадку p=0 для всіх $j \neq G$. p_j є елементом матриці переходу Q.

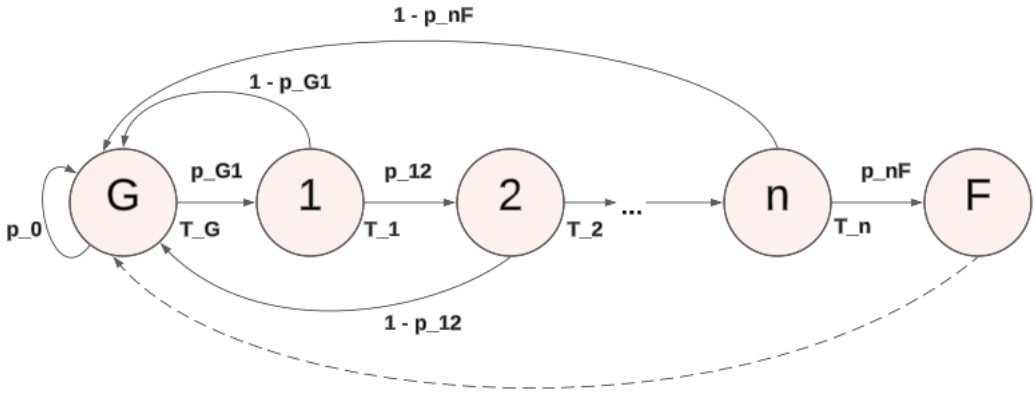

Рисунок 2.3 – Загальна SMP модель процесу вторгнення

На рисунку 2.3 представлено узагальнену модель напівмарківського процесу, яка описує етапи вторгнення в систему. Початковий стан G відповідає безпечному стану, коли система ще не зазнала впливу зловмисника. Станами 1 до n є проміжні етапи, що відображають поступові дії атакуючого, спрямовані на отримання дедалі більшого доступу до системи. Кінцевим етапом є стан компрометації F, який означає, що система повністю зламана. Стан G та проміжні стани 1–n є перехідними, тобто з них можливий подальший розвиток подій. Натомість стан F є поглинаючим, оскільки після його досягнення процес не повертається до попередніх станів. Ймовірність переходу між станами, наприклад зі стану i до стану j, позначається як p_j

2.2 Сценарії атак та формалізація моделі

У контексті забезпечення кібербезпеки SCADA-систем в енергетичному секторі, локальні мережі центру управління (LAN) та корпоративні LAN виступають основними об'єктами для потенційних атак. Зловмисники здійснюють спроби проникнення шляхом виявлення та експлуатації вразливостей у компонентах кіберінфраструктури. Для формалізації процесу вторгнення було побудовано стохастичні моделі на основі марківських процесів (SMP), які охоплюють сценарії атак через обидві LAN.

Розглянемо два типи атак: зовнішні, що здійснюються сторонніми суб’єктами, та внутрішні, ініційовані особами з доступом до системи. Результати моделювання дозволять порівняти ефективність та наслідки кожного типу загроз.

Зовнішні атаки на LAN центру управління

На рисунку 2.4 представлено структурну схему LAN центру управління. Зовнішня атака передбачає проходження кількох етапів: спочатку зловмисник обходить апаратний брандмауер, використовуючи спеціально розроблену стратегію вторгнення. Далі він отримує доступ до мережевого комутатора через сканування портів, після чого здійснює пошук вразливих хостів і серверів. Основними цілями є сервер історичних даних та application сервер, який забезпечує зберігання інформації та її передачу до клієнтських інтерфейсів, зокрема HMI.

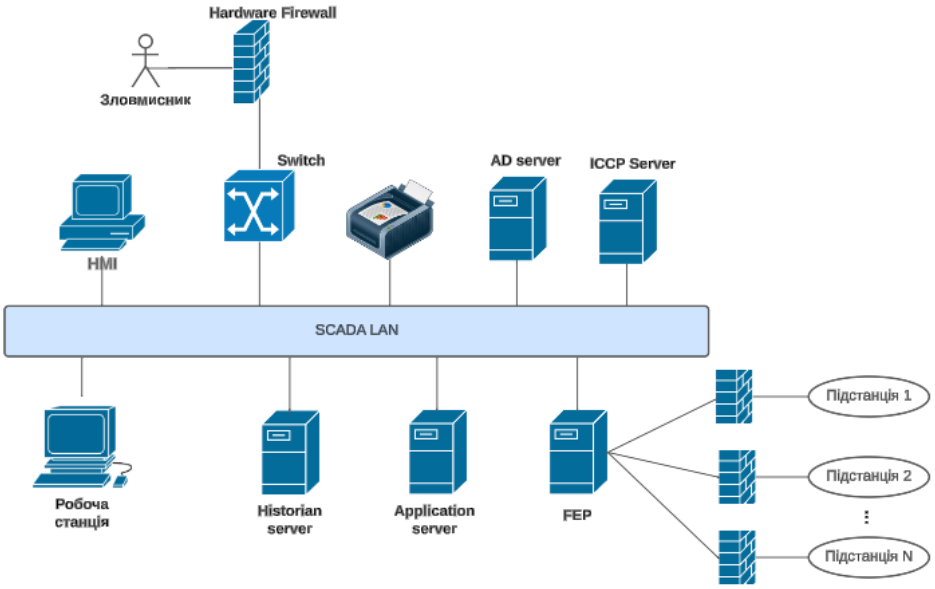

Рисунок 2.4 – Шлях атаки на локальну мережу центру управління

Внутрішні атаки

Внутрішні загрози пов’язані з діями осіб, які мають доступ до конфігурації SCADA-системи. Такі користувачі можуть навмисно змінювати налаштування або зловживати привілеями доступу. У цьому випадку компрометація сервера історичних даних може відбутися без необхідності подолання зовнішніх засобів захисту, що значно спрощує процес атаки.

На рисунку 2.5 наведено SMP-модель атаки на LAN центру управління. Початковий стан G відповідає безпечному режиму функціонування системи. Перехід до стану F означає успішне вторгнення. Зловмисник переходить до стану 1 після обходу брандмауера, а до стану 2 — після отримання привілеїв, компрометації сервера історичних даних. У випадку внутрішньої атаки, інсайдер може легко зламати сервер історичних даних, не активуючи сповіщення системи виявлення вторгнень (IDS). З огляду на це, до наведеної на рисунку SMP-моделі, було інтегровано додатковий шлях переходу зі стану G безпосередньо до стану 2, що дозволяє врахувати сценарій внутрішньої атаки.

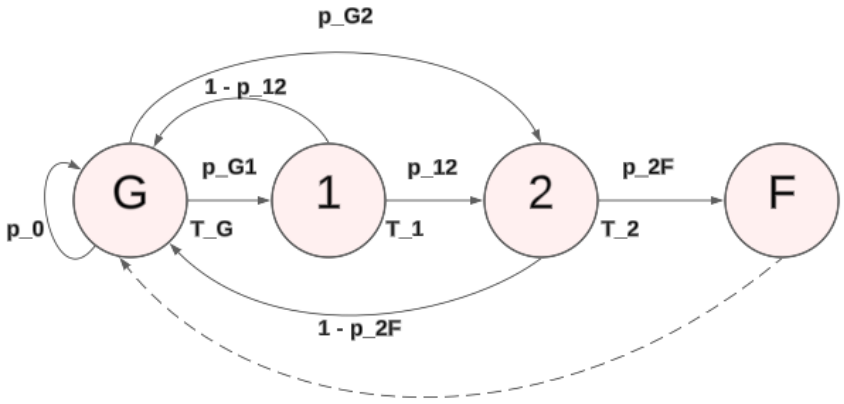

Рисунок 2.5 – SMP-модель атаки на LAN центру управління

Зважаючи на побудовану модель марківського процесу, було сформовано відповідну матрицю переходів транзитних станів, яка враховує як зовнішні, так і внутрішні сценарії атак на SCADA-систему.

$$Q = \begin{bmatrix} (1 - p_{G1} - p_{G2}) & p_{G1} & p_{G2} \\ 1 - p_{12} & 0 & p_{12} \\ 1 - p_{2F} & 0 & 0 \end{bmatrix}$$

Рисунок 2.6 – Матриця переходу транзитних станів моделі SMP

Зовнішні атаки на корпоративну LAN

Зовнішні та внутрішні атаки на корпоративні мережі, що межують із SCADA-середовищем, відрізняються стартовою точкою, але переслідують спільну мету - отримати контроль над даними та процесами, від яких залежать оперативні рішення й безпека технологічних об’єктів. На рисунку 2.7 зображено можливий шлях атаки на корпоративну локальну мережу.

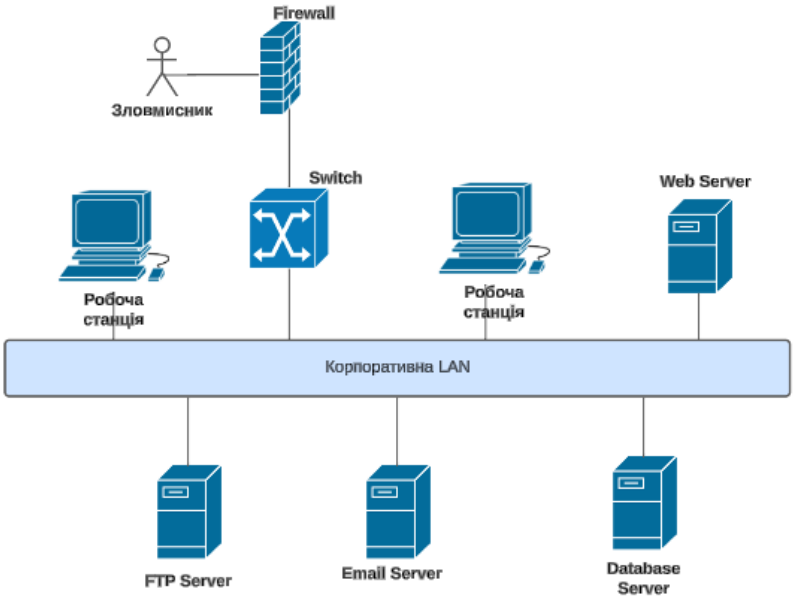

Рисунок 2.7 – Шлях атаки на корпоративну LAN

Через складну мережу зловмисники можуть спочатку отримати доступ до корпоративної локальної мережі через Інтернет. Зовнішній порушник починає з публічних або напівпублічних сервісів, дистанційного доступу, ланцюга постачання чи соціальної інженерії. Отримавши доступ до каналу зв'язку між центром керування та підстанціями, супротивник може встановити пасивні або активні засоби перехоплення трафіку як у дротовому, так і в бездротовому сегменті. Наслідки зовнішнього проникнення: контроль мережевого трафіку, перехоплення телеметрії/службових даних, підміна записів у БД через зламані додатки або ін'єкція фальшивих команд із компрометованих вузлів. У контексті SCADA це може призвести до спотворення звітності, історичних даних, або до непрямих операційних рішень на основі фальшивої інформації.

Внутрішні атаки на корпоративну LAN

На відміну від зовнішнього проникнення, внутрішній нападник часто вже має дозволи на критичні служби — від файлових сховищ і FTP/SFTP до historian/БД технологічних даних. Для SCADA-сценаріїв це означає можливість швидкої підміни технологічних даних і прямого впливу на

прикладні рішення, що спираються на ці дані (аналітика, звітність, автоматизовані процедури).

На рисунку 2.8 наведено SMP-модель атаки на корпоративну LAN. Стан G відображає «периметр/спостереження», за ним ідуть послідовні внутрішні стадії 1 → 2 → 3, а F — абсорбційний стан «компрометація/відмова». Між цими станами визначені ймовірності переходів pG1, p12, p23 і два «короткі шляхи» до відмови: p2F (характерний для внутрішнього нападника) і p3F (для зовнішнього нападника). Над кожним станом указані середні часи перебування τG, τ1, τ2, τ3 - це тривалість, упродовж якої атакувальник «застрягає» на відповідній стадії, перш ніж зробити наступний крок.

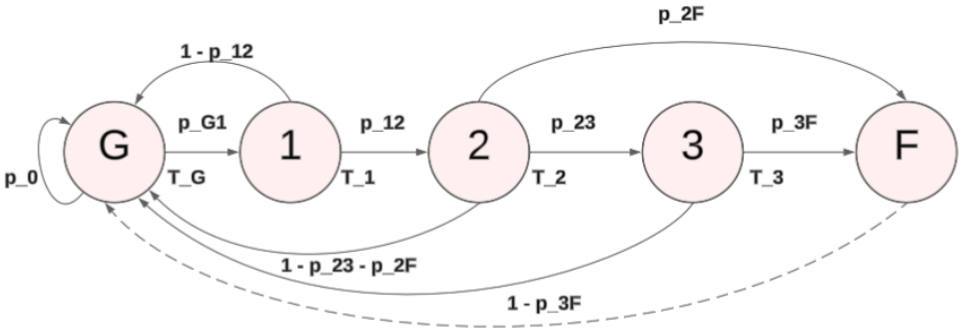

Рисунок 2.8 – SMP-модель атаки на корпоративну LAN

Наступним кроком так само як в попередньому випадку формуємо відповідну матрицю вбудованого марковського ланцюга для транзитних станів, яка враховує і зовнішні, і внутрішні сценарії атак.

$$Q = \begin{bmatrix} (1-p_{G1}) & p_{G1} & 0 & 0 \\ (1-p_{12}) & 0 & p_{12} & 0 \\ (1-p_{23}-p_{2F}) & 0 & 0 & p_{23} \\ (1-p_{3F}) & 0 & 0 & 0 \end{bmatrix}$$

Рисунок 2.9 – Матриця переходу транзитних станів моделі SMP

2.3 Визначення ймовірностей переходу транзитних станів

Розглянуті SMP-моделі описують послідовне проходження зловмисником етапів компрометації: від нормального режиму функціонування до успішного вторгнення. Для кількісного аналізу кібернадійності необхідно надати кожному переходу p_{ij} змістовну ймовірність, яка відображає реальну експлуатованість вразливостей на відповідному кроці атаки.

Кожен транзитний перехід у моделі можна інтерпретувати як узагальнений результат експлуатації певного набору вразливостей. Тобто кожен перехід у SMP-моделі пов’язати з конкретним набором вразливостей, описаних у базі CVE [23]. Для кожного з цих переходів можна сформувати множину CVE-ідентифікаторів, які репрезентують реальні відомі вразливості відповідних компонентів. Для кількісної оцінки експлуатованості обраних CVE використовується EPSS (Exploit Prediction Scoring System). EPSS - це ймовірнісний показник у діапазоні від 0 до 1, що відображає оцінку того, з якою ймовірністю конкретна вразливість CVE буде експлуатована в реальних умовах протягом найближчих 30 днів. На відміну від CVSS, який характеризує потенційну «тяжкість» вразливості, EPSS фокусується саме на фактичному ризику експлуатації «в полі». Значення EPSS розраховуються на основі статистичних і машинно-навчальних моделей, які враховують технічні атрибути вразливості, наявність публічних експлойтів, активність у відкритих джерелах, історичні дані про подібні CVE тощо, та регулярно оновлюються. Таким чином, для кожного CVE у множині можна отримати числову оцінку, яка безпосередньо інтерпретується як ймовірність успішної експлуатації цієї вразливості у заданому часовому вікні.

З огляду на те, що одна й та сама стадія атаки в моделі узагальнює декілька подібних вразливостей (наприклад, групу CVE для різних версій того самого firewall чи historian), у роботі використовується підхід

усереднення значень EPSS. Таким чином, p_{ij} інтерпретується як середня оцінка ймовірності успішної експлуатації типової вразливості, що відповідає даному кроку атаки.

Для першої SMP-моделі перехід $G \to 1$ можна пов'язати з вразливостями периметрових пристроїв (апаратні брандмауери, VPN-шлюзи), перехід $1 \to 2$ - з вразливостями сервера історичних даних та application-сервера, що забезпечують обробку і зберігання телеметрії, перехід $2 \to F$ - з вразливостями SCADA-рівня (HMI, сервер керування, інженерні станції). Додатковий перехід $G \to 2$, що моделює сценарій внутрішньої атаки, пов'язується з уразливостями, які можуть бути використані автентифікованим користувачем або оператором з розширеними правами.

Таким чином користуючись відкритими джерелами було обрано для кожного переходу було обрано від 10 до 15 CVE, що відповідають реальним вразливостям відповідних компонентів (периметрові засоби захисту, мережеве обладнання, сервери історичних даних, HMI/SCADA тощо). Для кожного з цих ідентифікаторів отримано значення EPSS, після чого для кожного переходу SMP-моделі обчислювалося середнє значення EPSS. В результаті було отримано: $p_{G1} \approx 62\%,\ p_{12} \approx 13\%,\ p_{2F} \approx 25\%$.

Для другої SMP-моделі кожен перехід також прив'язується до окремих класів вразливостей. Стан G відповідає периметру, тому перехід $G \to 1$ можна пов'язати з експлуатацією вразливостей публічних і напівпублічних сервісів корпоративної мережі (VPN, web-, email-шлюзи, служби дистанційного доступу), через які зловмисник отримує початковий доступ до корпоративної LAN. Перехід $1 \to 2$ відповідає уразливостям мережевої інфраструктури, що утворює канал зв'язку між центром керування та підстанціями (промислові маршрутизатори, комутатори, радіоканали), і дозволяє пасивне або активне перехоплення трафіку. Перехід $2 \to 3$ пов'язується з вразливостями серверів історичних даних, БД та прикладних SCADA/HMI-додатків, через які здійснюється підміна телеметрії,

модифікація записів у БД або ін’єкція фальшивих команд. Короткий перехід 2→F моделює сценарій внутрішнього нападника, який був згаданий раніше, тоді як перехід 3→F описує остаточну втрату керованості або достовірності даних SCADA-системи. В результаті було отримано: $p_{G1} \approx 73\%,\ p_{12} \approx 15\%,\ p_{23} \approx 25\%\ ,\ p_{3F} \approx 40\%$.

Водночас слід наголосити, що значення EPSS є динамічними й оновлюються щоденно, тому наведені у роботі показники використовуються передусім як ілюстративний приклад для побудови та параметризації моделі. На практиці організації можуть застосовувати спеціалізовані інструменти та платформи, які автоматично отримують актуальні дані з бази NVD та інших джерел, зіставляють їх із переліком встановленого ПЗ й виявлених вразливостей та підтягують поточні значення EPSS саме для їхньої інфраструктури. Це дає змогу інтегрувати аналогічний підхід у реальні процеси управління вразливостями та оцінки кіберризику.

2.4 Методика оцінювання

Розрахунок середнього часу до компрометації SCADA-системи можливий за умови, що відома або оцінена тривалість перебування зловмисника в кожному стані моделі атаки. Водночас ці часові інтервали є випадковими та несталими: на них впливають рівень підготовки атакувальника, наявність вразливостей, ефективність засобів виявлення, конфігурація мережі тощо. Тому використання фіксованих детермінованих значень може призводити до суттєвого викривлення оцінки ризику.

Щоб врахувати цю невизначеність і варіативність, для оцінювання параметрів розподілів часу перебування у станах було застосовано метод Монте-Карло на основі марковських ланцюгів (Markov Chain Monte Carlo, MCMC) [24].

Моделювання методом Монте-Карло - це імовірнісні процеси, які використовують повторну випадкову вибірку та закон великих чисел для чисельного наближення рішень складних задач [25]. Методи Монте-Карло можуть поєднуватися з ланцюгами Маркова для генерування випадкових вибірок із заданого цільового розподілу ймовірностей. Ідея підходів класу Markov Chain Monte Carlo (MCMC) полягає в тому, щоб побудувати ланцюг Маркова зі стаціонарним розподілом, який збігається або дуже добре наближає потрібний розподіл. Після цього ланцюг багаторазово «прокручують», і послідовність відвіданих ним станів (або її підмножина після відкидання початкової фази розігріву) розглядається як вибірка з цільового розподілу.

Оскільки аналітичний вигляд часто є складним, алгоритми MCMC будують ланцюг, спираючись на прості базові (пропозиційні) розподіли. На кожному кроці з цього базового розподілу генерується кандидат нового стану, який потім приймається або відхиляється за певним правилом (наприклад, методу Метрополіса–Гастінґса), що гарантує збіжність ланцюга до стаціонарного розподілу. У більш простому наближенні можна вважати, що пропозиційний розподіл задає механізм зміни поточного стану, а сама процедура прийняття/відхилення коригує ці пропозиції так, щоб отримана послідовність реалізацій відтворювала бажаний розподіл ймовірностей.

Алгоритм Метрополіса–Гастінгса - це класичний метод Марковського ланцюга Монте-Карло (MCMC), призначений для отримання послідовності випадкових вибірок із розподілу ймовірностей, з якого безпосередньо вибірку зробити складно або неможливо. Попри концептуальну простоту, на практиці алгоритм Метрополіса–Гастінгса у багатьох задачах виявляється повільним через виражену поведінку типу випадкового блукання та потребу у великій кількості кроків для достатнього «змішування» вибірки, особливо в багатовимірних просторах із сильно корельованими параметрами. Суттєвим кроком уперед для MCMC став гамільтонівський метод Монте-Карло (Hamiltonian Monte Carlo, HMC) - алгоритм, що будує ланцюг Маркова,

використовуючи градієнтну інформацію від цільової густини. Завдяки наближенню гамільтонівської динаміки він уникає випадкового блукання, рухаючись уздовж «траєкторій» високої правдоподібності й значно краще працюючи з корельованими параметрами. Це забезпечує набагато швидшу збіжність до цільового розподілу порівняно з простішими схемами.

Особливо важливим є удосконалення HMC [26], яке знімає потребу вручну задавати кількість кроків інтегрування. Цей алгоритм, відомий як No-U-Turn Sampler (NUTS), рекурсивно будує траєкторію з кандидатних точок, що охоплює суттєву частину цільового розподілу, і автоматично зупиняється, коли рух починає «розвертатися» назад, тобто потенційно дублювати вже пройдені області простору параметрів. Такий підхід поєднує високу ефективність HMC з більшою автоматизацією налаштування, що робить його особливо придатним для складних байєсівських моделей, зокрема й напівмарковських описів атак на SCADA-системи.

Реалізація алгоритму MCMC вимагає задання початкової моделі тривалості перебування зловмисника в кожному стані атаки. Як базове сімейство розподілів для цих часів було обрано розподіл Вейбулла, який є «природною» моделлю для часу до відмови чи зламу й широко використовується в задачах надійності технічних систем. Функція щільності має наступний аналітичний вигляд:

$$f_X(x) = \begin{cases} \frac{k}{\lambda}\left(\frac{x}{\lambda}\right)^{k-1} e^{-\left(\frac{x}{\lambda}\right)^k}, x \geq 0 \\ 0, x < 0 \end{cases} \quad (2.6)$$

У прийнятій моделі параметр k інтерпретується як параметр форми (shape), а λ - як параметр масштабу (scale). Вони визначають, наскільки «розтягнутим» є розподіл часу перебування у стані та як змінюється інтенсивність переходу до наступного кроку атаки. Зокрема, при $k = 1$ інтенсивність події залишається сталою в часі (експоненційний випадок), при $k < 1$ризик зменшується з часом (сценарій «ранніх відмов»), а при $k > 1$— зростає (накопичення умов для успішного зламу). Таким чином, вибір

вейбуллівського розподілу дає змогу явно моделювати часову залежність ризику та відходити від спрощувального припущення про постійну інтенсивність переходів.

Саме така гнучкість робить напівмарковський процес більш реалістичним для опису атак на SCADA-систему: момент переходу зі стану до стану вже не є незалежним від попередньої історії перебування в них, а залежить від того, скільки часу зловмисник перебував у поточній фазі атаки. Для того щоб підібрати параметри k та λ, які найкраще узгоджуються з даними (журнали подій, експертні оцінки, результати імітацій), організовується чисельний експеримент методом Монте-Карло.

У його межах МСМС використовується для отримання апостеріорних розподілів параметрів часу в кожному стані. Це дає змогу:

- отримати статистично обґрунтовані оцінки за умов невизначеності та неповноти початкових даних;
- врахувати варіативність часових характеристик атак (різні сценарії, рівні підготовки зловмисника, конфігурації мережі);
- згенерувати вибірки можливих значень тривалості перебування у станах і на їх основі обчислити розподіл та математичне сподівання MTTC, а також довірчі інтервали для нього.

У підсумку, комбінування вейбуллівської моделі часу до зламу з байєсівською оцінкою параметрів за допомогою МСМС дозволяє будувати напівмарковську модель атаки, що адекватніше відображає реальні часові профілі кіберзагроз для SCADA-систем.

2.5 Реалізація МСМС та аналіз результатів

Для обох сценаріїв як початкову модель випадкового часу перебування у станах беремо вейбуллівський розподіл із параметром форми в діапазоні $1 < k < 5$. Для параметрів цього розподілу задаємо такі апріорні розподіли:

рівномірний (Uniform) для k (shape) на відрізку $[1;5]$ та гамма-розподіл (Gamma) для λ (scale).

Для реалізації була обрана бібліотека Python pymc, яка містить функцію sample для сформованої моделі, яка і є реалізацією алгоритму NUTS. Зазначимо, що для розрахунку було використано 15000 ітерацій.

```
# --- MCMC-модель Weibull ---
with pm.Model() as model:
    k_G = pm.Uniform("k_G", lower=1, upper=5)
    k_1 = pm.Uniform("k_1", lower=1, upper=5)
    k_2 = pm.Uniform("k_2", lower=1, upper=5)

    lam_G = pm.Gamma("lam_G", alpha=2, beta=0.5)
    lam_1 = pm.Gamma("lam_1", alpha=2, beta=0.5)
    lam_2 = pm.Gamma("lam_2", alpha=2, beta=0.5)

    trace = pm.sample(samples, chains=1, tune=500, progressbar=False)
```

Рисунок 2.10 – Реалізація MCMC

Отримавши MCMC-вибірки параметрів для кожного стану, можна визначити математичне сподівання часу перебування в ньому за такою формулою:

$$\mathrm{E}[T_i] = \lambda_i \Gamma(1 + \frac{1}{k_i}) \tag{2.7}$$

```
# --- Очікуваний час у станах ---
E_G = trace.posterior['lam_G'].values.flatten() * gamma(1 + 1 / trace.posterior['k_G'].values.flatten())
E_1 = trace.posterior['lam_1'].values.flatten() * gamma(1 + 1 / trace.posterior['k_1'].values.flatten())
E_2 = trace.posterior['lam_2'].values.flatten() * gamma(1 + 1 / trace.posterior['k_2'].values.flatten())
```

Рисунок 2.11 – Реалізація

Далі, використовуючи вектор очікуваних тривалостей і фундаментальні матриці, можна визначити очікуваний час до поглинання:

$$\mathrm{E} = \sum N \cdot T \tag{2.8}$$

Використовуючи ймовірності, визначені в вище було отримано наступні результати для сценарію LAN центру керування:

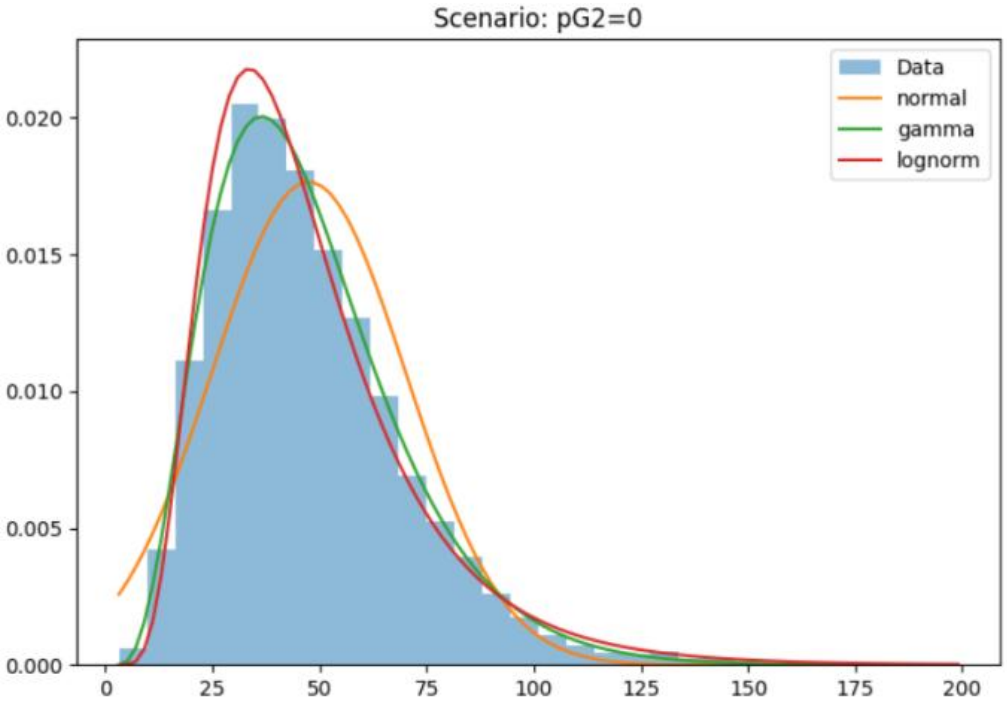

Рисунок 2.12 – Візуалізація результатів для сценарію зовнішнього атакуючого

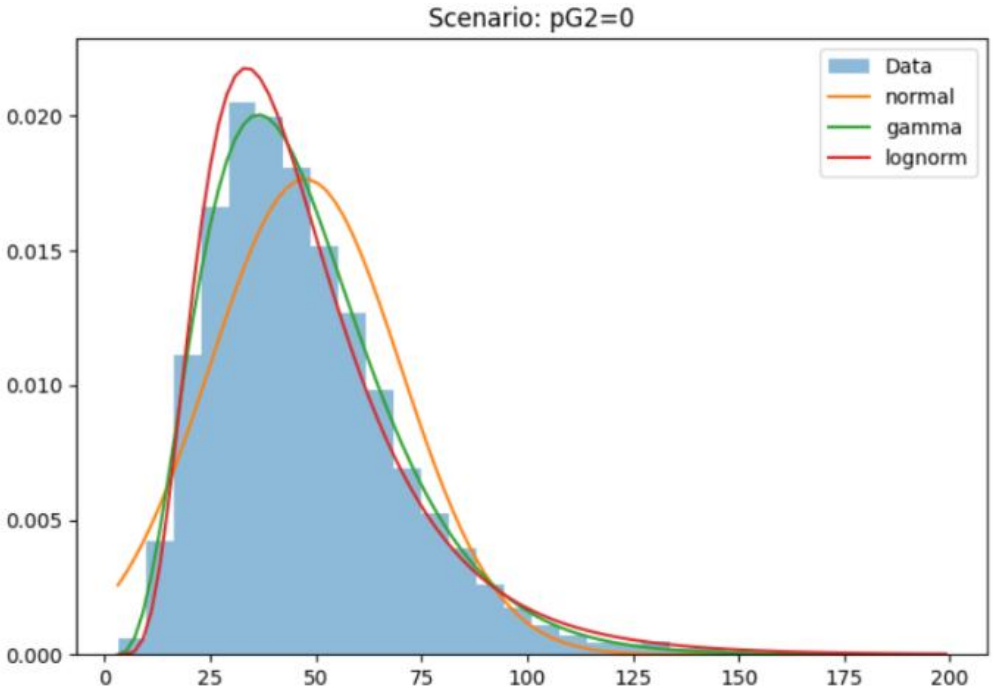

Рисунок 2.13 – Візуалізація результатів для сценарію внутрішнього атакуючого

Для сценарію атак на корпоративну LAN результати наступні:

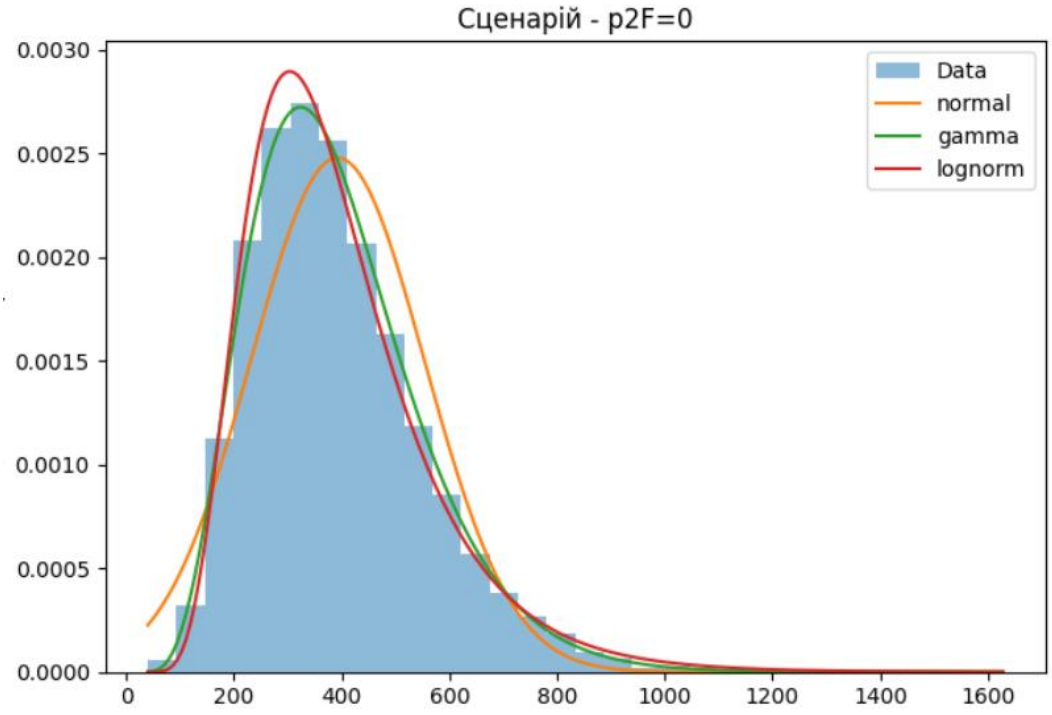

Рисунок 2.14 – Візуалізація результатів для сценарію зовнішнього атакуючого

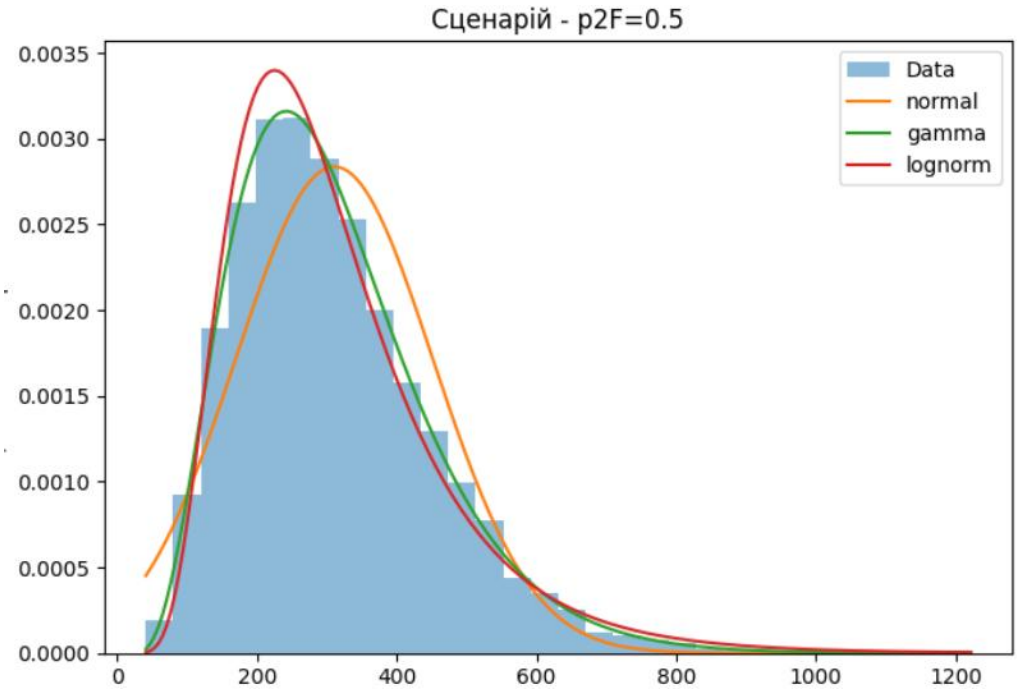

Рисунок 2.15 – Візуалізація результатів для сценарію внутрішнього атакуючого

Відповідно до аналізу проведеного у [24] для сценарію LAN центру керування, аналогічний підхід був застосований для сценарію з корпоративною LAN. Додатково можна висунути гіпотези щодо форми стаціонарного розподілу. Візуальний аналіз є корисним інструментом попередньої орієнтації , проте для надійного обґрунтування вибору моделі можна застосовувати формальні статистичні критерії.

Першим кроком є перевірка гіпотези про нормальність: якщо дані суттєво відхиляються від нормального розподілу, його можна відразу відкинути як кандидат на стаціонарний розподіл. Тест Андерсона–Дарлінга (AD) використовується для перевірки нульової гіпотези H_0 про те, що вибірка походить із заданого теоретичного розподілу.

Надалі постає завдання розрізнити, яка модель краще описує дані: логнормальна чи гамма-розподіл. Візуально ці розподіли часто виглядають подібно, оскільки обидва є правосторонньо асиметричними. Тому для формалізації вибору застосовано тест Колмогорова–Смірнова (KS), який порівнює емпіричну функцію розподілу з теоретичною, оцінюючи максимальне відхилення між ними. Значення $p > 0{,}05$ означає, що немає підстав відхиляти нульову гіпотезу, тобто дані узгоджуються з обраною моделлю.

Таблиця 2.1 – Результати аналізу

Показник	Корп. LAN (p2F=0)	Корп. LAN (p2F=0.5)	SCADA LAN (pG2=0)	SCADA LAN (pG2=0.5)
AD, A^2	163.5484	160.1622	188.1369	180.8006
KS gamma, p-value	0.9820	0.9596	0.8821	0.6248
KS lognorm, p-value	0.0000	0.0000	0.0000	0.0000

За тестом Андерсона–Дарлінга для перевірки нормальності стаціонарного розподілу одержано дуже великі значення статистики:

- корпоративна LAN: $A^2 = 163.55$ (p2F=0) та 160.16 (p2F=0.5);
- SCADA LAN: $A^2 = 188.14$ (pG2=0) та 180.80 (pG2=0.5).

Усі ці значення значно перевищують критичні пороги навіть для рівня значущості 1 %, тому нормальний розподіл однозначно відхиляється як модель стаціонарного розподілу часу до компрометації.

Натсупним кроком за тестом Колмогорова–Смірнова можна порівняти гамма- та логнормальний розподіли. Для гамма-розподілу отримано малі значення статистики й великі p-значення:

- корпоративна LAN: D = 0.0038, p = 0.9820 (p2F=0); D = 0.0041, p = 0.9596 (p2F=0.5);
- SCADA LAN: D = 0.0048, p = 0.8821 (pG2=0); D = 0.0061, p = 0.6248 (pG2=0.5).

У всіх випадках $p \gg 0.05$, отже, немає підстав відхиляти нульову гіпотезу, і дані добре узгоджуються з гамма-розподілом.

Для логнормального розподілу ситуація протилежна:

- корпоративна LAN: p = 0.0000 для обох сценаріїв;
- SCADA LAN: p = 0.0000 для обох сценаріїв.

Такі значення свідчать про суттєве відхилення емпіричних даних від логнормальної моделі.

Отримані результати корисні тим, що дають формально обґрунтований вибір стаціонарної моделі для часу до компрометації: нормальний і логнормальний розподіли статистично відкидаються, натомість гамма-розподіл узгоджується з даними для обох LAN і в обох сценаріях. Це означає, що подальші розрахунки MTTC, оцінка кібернадійності та порівняння сценаріїв атак спираються на коректну форму розподілу, а отже - на більш реалістичні й стабільні числові значення ризику. Крім того, така перевірка підтверджує адекватність побудованої SMP-моделі та дозволяє

використовувати гамма-розподіл у подальших аналітичних і імітаційних експериментах.

Висновки до розділу 2

У цьому розділі сформовано основу для кількісного аналізу кібернадійності SCADA-системи на базі напівмарковських процесів. SCADA-інфраструктуру було подано у вигляді послідовності дискретних станів, що відображають ключові кроки атаки в корпоративній та SCADA-LAN, включно з окремим шляхом для внутрішнього порушника. Такий підхід дозволив пов’язати топологію мережі та логіку розвитку інциденту з формальним стохастичним описом.

Запропоновано підхід до оцінки кібернадійності, у якому параметрами напівмарковської моделі виступають часові характеристики перебування зловмисника в кожному стані. Для їх опису використано вейбуллівську модель як початкову, а надалі – байєсівську оцінку параметрів за допомогою MCMC (зокрема, HMC/NUTS). Це дозволяє явно врахувати невизначеність і варіативність часових параметрів, замість спиратися на фіксовані детерміновані оцінки.

Для додатково аналізу було реалізовано процедуру статистичного відбору стаціонарного розподілу часу до компрометації з використанням тестів Андерсона–Дарлінга та Колмогорова–Смірнова. Показано, що нормальний та логнормальний розподіли не узгоджуються з емпіричними даними, тоді як гамма-розподіл є адекватною моделлю для обох мережевих сегментів і розглянутих сценаріїв.

Отже, у розділі побудовано узгоджену схему від опису архітектури SCADA-системи та сценаріїв атак - до формалізації їх у вигляді напівмарковських моделей, вибору статистичних розподілів і налаштування байєсівської процедури оцінювання параметрів. Розроблений підхід у подальшому застосовується в наступному розділі для проведення чисельних

експериментів, у межах яких інтегруються рівні підготовки атакуючих та виконується порівняльна оцінка кібернадійності за різними сценаріями.

3 ОЦІНКА MTTC

3.1 Навички атакуючих

У попередньому розділі було побудовано напівмарковську модель розвитку атаки на SCADA-систему та сформовано підхід до оцінки середнього часу до компрометації (MTTC) з урахуванням часових характеристик перебування в окремих станах. Однак реальний час проходження шляху атаки суттєво залежить не лише від топології мережі та наявних вразливостей, а й від рівня підготовки зловмисника. Той самий ланцюг кроків може бути реалізований за істотно різний час експертом, досвідченим порушником або початківцем.

У реальних умовах розвитку кіберінцидентів швидкість та ймовірність успішної компрометації системи істотно залежать від рівня підготовки зловмисника: один і той самий маршрут атаки може бути реалізований за хвилини досвідченим фахівцем або взагалі не завершитися успіхом у разі дій початківця. Тому для побудови адекватної моделі кібернадійності недостатньо враховувати лише технічні параметри інфраструктури; необхідно явно включати до моделі характеристики потенційного противника.

Для кількісного урахування впливу рівня підготовки зловмисника у моделі напівмарковського процесу було використано коефіцієнти, отримані на основі спеціалізованого дослідження вразливостей для ICS/SCADA-середовища, наведеного в [27].

У зазначеній роботі сформовано вибірку з 1916 вразливостей, для яких визначено ненульовий показник CVSS exploitability score у теоретичному діапазоні 0.1–3.9. Далі автори задали для кожного класу атакуючого інтервал значень exploitability score, який вважається досяжним для відповідного рівня навичок: 0.1–1.2 для Novice, 0.1–2.1 для Beginner, 0.1–3.0 для Intermediate та

0.1–3.9 для Expert. Підрахунок кількості вразливостей, що потрапляють до кожного з інтервалів (105, 455, 966 та 1916 записів відповідно), дав змогу визначити частки 0.05, 0.24, 0.50 та 1.0 від загального обсягу вибірки, які інтерпретуються як частка вразливостей, потенційно придатних до експлуатації атакуючим певного рівня компетентності.

Зазначені частки надалі інтерпретуються як коефіцієнти, що характеризують рівень навичок атакуючих:

- Novice – 0,05;
- Beginner – 0,24;
- Intermediate – 0,50;
- Expert – 1,0.

Їх застосування є обґрунтованим, оскільки вони базуються на емпіричному аналізі великої кількості вразливостей, специфічних для ICS, і безпосередньо пов’язані з метрикою експлуатованості CVSS. У подальшому ці коефіцієнти використовуються для масштабування базових ймовірностей переходів у напівмарковській моделі атак на SCADA-систему. Таким чином, у модель інтегрується людський фактор: із зниженням рівня підготовки атакуючого ефективна частка експлуатованих вразливостей зменшується, що приводить до зростання очікуваного часу до компрометації та забезпечує більш реалістичну оцінку кібернадійності.

3.2 Програмна реалізація

Для практичної оцінки середнього часу до компрометації (MTTC) та перевірки побудованих напівмарковських моделей було розроблено програмну реалізацію обраного підходу. Реалізацію виконано мовою Python з використанням бібліотек NumPy, SciPy, PyMC, pandas та Matplotlib, що

забезпечує як гнучке налаштування параметрів моделі, так і відтворюваність чисельних експериментів.

Загально, для обох сценаріїв атак було реалізовано такий алгоритм:

1. Побудова моделі поведінки системи як послідовності дискретних станів відповідно до обраних сценаріїв атаки. Визначення ймовірностей переходів між станами атаки.
2. Задання апріорних уявлень про часові характеристики перебування в кожному стані, які відображають початкову невизначеність параметрів.
3. Виконання MCMC-симуляцій для отримання вибірки часу перебування у транзитних станах.
4. На основі MCMC-вибірок обчислюються очікувані часи перебування в кожному стані напівмарковського процесу.
5. Для кожного рівня навичок атакуючого базові ймовірності переходів масштабуються відповідним коефіцієнтом, що моделює зниження ефективності атаки для менш досвідчених зловмисників.

```
# Масштабуємо ймовірності
pG1_scaled = pG1 * fraction
pG2_scaled = pG2_base * fraction
p12_scaled = p12 * fraction
p2F_scaled = p2F * fraction
```

Рисунок 3.1 – Програмна реалізація масштабування ймовірностей на прикладі першого сценарію

6. На основі фундаментальної матриці та очікуваних часів у станах обчислюються вибірки часу до поглинання (MTTC) для кожного сценарію та рівня навичок.

```
Q1 = np.array([
    [1 - pG1_scaled, pG1_scaled, 0],
    [0, 1 - p12_scaled, p12_scaled],
    [0, 0, 1 - p2F_scaled]
])
N1 = np.linalg.inv(I - Q1)
ET1 = np.sum(N1 @ T.T, axis=0)
```

Рисунок 3.2 – Приклад програмної реалізації фундаментальної матриці та очікуваних часів у станах

7. Результати агрегуються у вигляді середніх значень MTTC та візуалізуються для порівняння впливу навичок і сценаріїв. Результати подаються у табличній та графічній формах для демонстрації впливу навичок атакуючих та структури сценарію на кібернадійність SCADA-системи.

3.3 Отримані результати MTTC

Далі буде наведено результати чисельних експериментів з оцінки середнього часу до компрометації (MTTC) для розроблених напівмарковських моделей атак на SCADA-систему з урахуванням рівня підготовки атакуючих та різних сценаріїв розвитку подій. На їх основі проаналізовано, як змінюється кібернадійність системи залежно від структури шляху атаки та класу порушника.

Варто підкреслити, що використані параметри ймовірностей переходів та часових характеристик станів розглядаються як репрезентативний, але узагальнений приклад і не відображають параметри жодного конкретного об’єкта. Вони були обрані як узгоджений набір вхідних даних, достатній для демонстрації працездатності запропонованого підходу та ілюстрації того, яким чином напівмарковська модель у поєднанні з MCMC-оцінюванням може застосовуватися для кількісної оцінки MTTC у реальних задачах кібернадійності.

Для моделі сцентарію з LAN центру управління (рис. 3.3 та 3.4) одержано чітко виражену залежність MTTC від рівня підготовки атакуючого: із переходом від Expert до Novice середній час до компрометації зростає більш ніж на порядок (від ≈80 до ≈1600 умовних одиниць часу). Це означає, що за фіксованої топології шляху атаки людський фактор є домінувальним: малокваліфікований порушник значно довше «блукає» між станами моделі, перш ніж досягти поглинання.

Середній час до компрометації:

Навичка	pG2=0	pG2=0.5
Expert	79.19	67.26
Intermediate	158.39	134.52
Beginner	329.97	280.25
Novice	1583.87	1345.20

Рисунок 3.3 – Числові результати MTTC для LAN центру управління

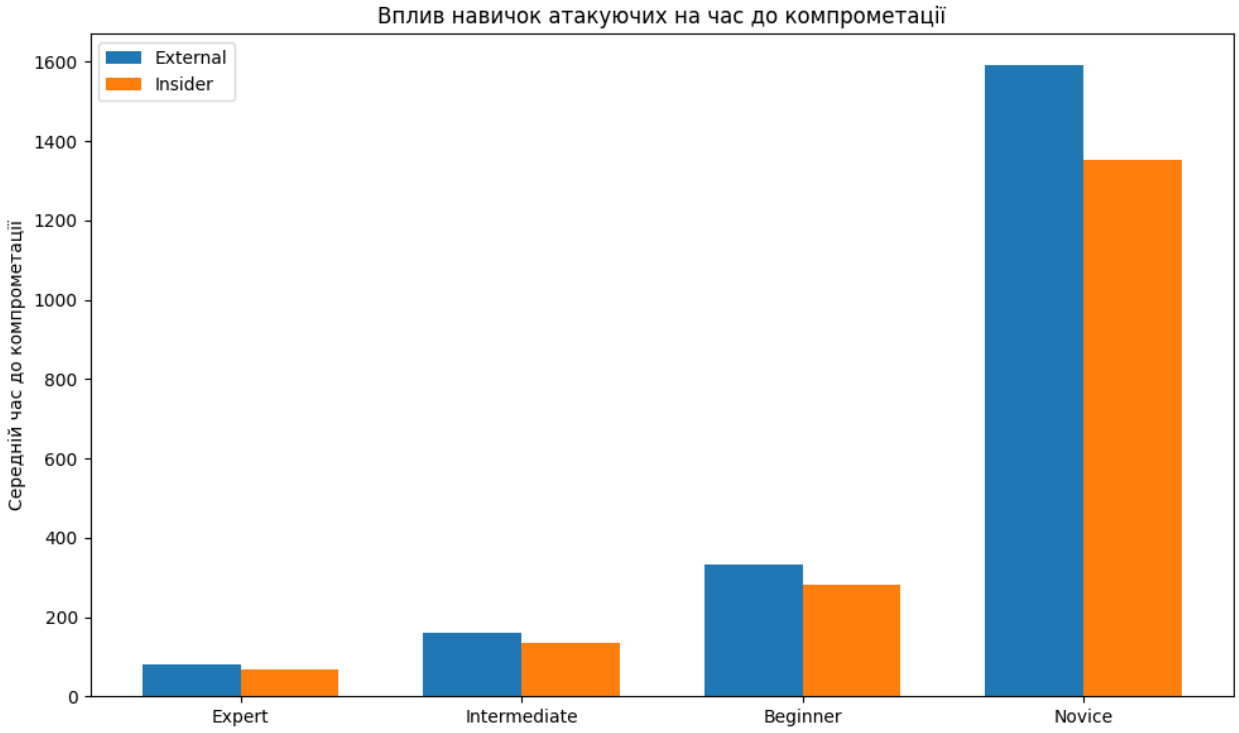

Рисунок 3.4 – Візуалізація результатів MTTC для LAN центру управління

Порівняння сценаріїв із відсутнім та наявним додатковим переходом показує, що введення цього каналу скорочує MTTC приблизно на 15 % для всіх класів атакуючих (як для Expert, так і для Novice). Тобто поява альтернативного, швидшого маршруту компрометації помірно, але стабільно знижує кібернадійність, причому ефект є порівнянним для всіх рівнів навичок.

У моделі сцентарію з корпоративною локальною мережею (рис. 3.5 та рис 3.6) розглянуто два якісно різні сценарії: зовнішній атакуючий (External), який починає з корпоративної мережі, та внутрішній порушник (Insider), що стартує ближче до SCADA-ресурсів. Для всіх рівнів навичок значення MTTC для зовнішнього зловмисника є більшими, ніж для внутрішнього, що відповідає очікуванням щодо додаткових бар'єрів доступу ззовні. Для Expert різниця становить близько 15% (≈100 проти ≈86), для Intermediate — вже понад 20%, тоді як для Beginner та Novice MTTC для зовнішньої атаки майже вдвічі перевищує показник для внутрішньої. Отже, додатковий проміжний стан/рівень мережі істотно «гасить» можливості малокваліфікованого нападника, але майже не впливає на експерта, який здатен ефективно долати більшість наявних бар'єрів.

Середній час до компрометації:

Навичка	External	Insider
Expert	100.35	85.87
Intermediate	223.78	171.36
Beginner	763.31	413.62
Novice	2832.59	1413.52

Рисунок 3.5 – Числові результати MTTC для корпоративної локальної мережі

Рисунок 3.6 – Числові результати MTTC для для корпоративної локальної мережі

Синтезуючи результати двох моделей, можна зробити висновок, що на середній час до компрометації одночасно впливають:

- архітектура шляху атаки (кількість та взаємозв'язки станів, наявність «швидких» переходів)
- профіль порушника (зовнішній/внутрішній, рівень навичок).

У сценарії, де шлях атаки є відносно простим і містить менше проміжних кроків, структурні зміни (наприклад, додавання альтернативного переходу) знижують MTTC приблизно на однакову відносну величину для всіх категорій атакуючих. Натомість у складнішому сценарії, що передбачає більшу кількість проміжних станів та додаткову сегментацію мережі (External проти Insider), вплив вихідного положення значно сильніше проявляється саме для слабких порушників. Це свідчить про те, що додаткові рівні сегментації та контролю доступу насамперед підвищують стійкість до «масових» атак з низькою кваліфікацією, тоді як проти цілеспрямованого висококваліфікованого противника ключову роль відіграють уже не стільки

структурні бар’єри, скільки інші засоби захисту (виявлення, моніторинг, реагування). Таким чином, модель дозволяє не лише кількісно оцінити MTTC, а й провести сценарний аналіз, який може бути використаний для обґрунтування пріоритетів посилення кіберзахисту SCADA-систем.

Висновки до розділу 3

У цьому розділі було здійснено кількісну оцінку середнього часу до компрометації (MTTC) на основі побудованих напівмарковських моделей атак на SCADA-систему з урахуванням людського фактора та різних сценаріїв розвитку інциденту. На відміну від попереднього розділу, де основна увага зосереджувалася на формуванні самої моделі та виборі адекватних розподілів часу перебування у станах, тут було зосереджено увагу на інтеграції рівнів підготовки атакуючих та інтерпретації отриманих числових результатів.

Було введено градацію навичок зловмисників (Novice, Beginner, Intermediate, Expert) на основі емпіричних коефіцієнтів, отриманих із спеціалізованого дослідження ICS-вразливостей та показника CVSS exploitability. Ці коефіцієнти були використані для масштабування базових ймовірностей переходів у напівмарковській моделі, що дозволило явно врахувати, яку частку доступних вразливостей кожен клас атакуючих здатен практично експлуатувати. Такий підхід дав змогу перейти від усередненої оцінки MTTC до сценарного аналізу, де один і той самий шлях атаки по-різному реалізується з точки зору часу залежно від профілю порушника.

На основі програмної реалізації моделі проведено чисельні експерименти для різних сценаріїв: із наявністю та відсутністю додаткового шляху в ланцюгу атаки, а також для випадків зовнішнього та внутрішнього порушника. Отримані результати демонструють монотонну залежність MTTC від рівня підготовки атакуючого: зі зниженням рівня навичок середній час до компрометації зростає на порядок і більше. Показано, що структурні

зміни в маршруті атаки впливають на всі класи зловмисників, але їхній відносний ефект найбільш відчутний для малокваліфікованих атакуючих, тоді як для експертів виграш або втрата у часі є суттєво меншими.

Порівняння сценаріїв із зовнішнім та внутрішнім атакуючим продемонструвало, що наявність додаткових бар’єрів доступу суттєвіше збільшує MTTC саме для низькорівневих порушників. Для висококваліфікованих зловмисників різниця між сценаріями є відносно помірною, що вказує на обмежену ефективність суто структурних заходів без належної підтримки засобами виявлення, моніторингу та реагування.

4 РОЗРОБКА СТАРТАП-ПРОЄКТУ

4.1 Опис ідеї стартап-проєкту

Розроблені в роботі напівмарковські моделі атак на SCADA-систему та підхід до оцінки середнього часу до компрометації (MTTC) можуть бути покладені в основу прикладного програмного продукту – сервісу кількісної оцінки кібернадійності об’єктів критичної інфраструктури. Ідеться про спеціалізовану платформу, яка поєднує математичні моделі, засоби статистичного аналізу та зручний інтерфейс для інженерів і фахівців з інформаційної безпеки.

Сутність запропонованої ідеї полягає у створенні спеціалізованого сервісу кількісної оцінки кібернадійності, який у напівавтоматичному режимі перетворює опис технологічної мережі на формальну модель ризику. Такий сервіс:

- приймає на вхід структурований опис архітектури технологічної мережі (рівні моделі Purdue, ключові вузли та критичні сервіси) разом із параметрами налаштувань безпеки;
- на основі цих даних формує відповідну напівмарковську модель потенційних сценаріїв атак;
- із використанням процедур MCMC-оцінювання параметрів і сценарного аналізу обчислює MTTC або інші узагальнені показники кібернадійності для різних рівнів підготовки зловмисників;
- подає результати у вигляді інтерактивних дашбордів, аналітичних звітів і рекомендацій щодо пріоритизації заходів захисту.

До основних напрямів застосування такої платформи можна віднести:

- проведення аудиту кібернадійності SCADA- та ICS-систем на енергетичних, водоканальних, транспортних і промислових об’єктах;
- підтримку процесу прийняття рішень під час модернізації OT-інфраструктури (кількісна оцінка ефекту від сегментації, впровадження додаткових засобів захисту, зміни архітектури доступу тощо);
- підготовку формалізованих звітів для регуляторних органів та внутрішніх процедур комплаєнсу.

Для кінцевих користувачів - операторів технологічних систем, підрозділів інформаційної безпеки та консалтингових компаній - ключові переваги сервісу полягають у такому:

- можливість отримувати кількісні оцінки кібернадійності у звичних для інженерно-технічного персоналу метриках часу до ймовірної відмови або компрометації;
- здатність моделювати вплив різних сценаріїв атак та рівнів підготовки зловмисників без втручання в роботу реальної системи;
- можливість пріоритизувати інвестиції в засоби захисту, спираючись на зміну MTTC та інших формалізованих показників, а не лише на експертні судження й якісні оцінки ризику.

За аналогією з існуючими рішеннями, орієнтованими на оцінку надійності та стійкості об’єктів критичної інфраструктури, запропонований стартап-проєкт фокусується на вузькій, але надзвичайно актуальній ніші – кількісній оцінці кібернадійності саме OT/SCADA-середовищ. Його відмінністю є поєднання спеціалізованих математичних моделей зі зручним прикладним інструментом, орієнтованим на практичні потреби операторів критичної інфраструктури та фахівців з кібербезпеки.

Для комплексної оцінки доцільності впровадження запропонованої стартап-ідеї доцільно проаналізувати її техніко-економічні характеристики з погляду сильних, слабких та нейтральних сторін порівняно з потенційними конкуруючими продуктами. У таблиці узагальнено ключові параметри проєкту, а також визначено, чи виступають вони конкурентною перевагою, обмеженням або не мають істотного впливу на позиціонування продукту на ринку.

Таблиця 4.1 - Оцінка доцільності впровадження запропонованої ідеї

Характеристики ідеї проєкту	Потенційні конкуренти	Слабка сторона	Нейтральна сторона	Сильна сторона
Спеціалізація на SCADA/ICS та об’єктах критичної інфраструктури	Універсальні IT-рішення з кібербезпеки			+
Використання напівмарковських моделей для подальшої кількісної оцінки ризику	Класичні vulnerability scanners, індекси ризику без часової складової			+
Можливість сценарного аналізу	Рішення, що дають переважно статичний «рейтинг ризиків»			+

Кінець таблиці 4.1

Складність математичного апарату та потреба у поясненні результатів користувачам	Більш прості за логікою «чек-ліст»-рішення та дашборди без глибоких моделей	+		
Висока залежність точності результатів від якості та повноти вхідних даних	Рішення, що використовують більш спрощені або типові моделі без детального налаштування під конкретний об’єкт	+		
Орієнтовно нижча вартість впровадження порівняно з великими комплексними платформами	Великі комплексні платформи управління ризиками та ОТ-безпекою		+	

4.2 Технологічний аудит ідеї проєкту

Для реалізації запропонованої стартап-ідеї було проаналізовано наявність та доступність основних технологічних компонентів: математичного апарату, програмних засобів, механізмів інтеграції з OT/IT-інфраструктурою, а також обчислювальних ресурсів.

Математична основа проєкту є зрілою та добре описаною в літературі. Напівмарковські процеси, марковські ланцюги з поглинанням, методи Монте-Карло на основі марковських ланцюгів (MCMC), а також підходи до оцінки середнього часу до компрометації (MTTC) уже мають усталений теоретичний фундамент і успішно застосовуються в суміжних задачах надійності та кібербезпеки. У роботі продемонстровано, що відповідні моделі можуть бути реалізовані на практиці, дають стійкі числові результати та придатні для сценарного аналізу.

Програмна реалізація може базуватися на широко розповсюдженому та безплатному стеку відкритого програмного забезпечення. Для побудови та оцінювання моделей доцільно використовувати будь-яку мову програмування та бібліотеки, які забезпечують повний цикл від задання моделі і проведення MCMC-симуляцій до статистичного аналізу та візуалізації результатів. Потенційно можуть бути застосовані фреймворки для створення користувацького інтерфейсу й веб-доступу.

Також важливим є питання інтеграції з OT/IT-інфраструктурою потенційних користувачів. На початкових етапах можна передбачити імпорт описів архітектури, налаштувань безпеки та результатів аудитів, що не потребує глибокого втручання в існуючі системи. У подальшому, зі зростанням зрілості продукту, можливе підключення до SIEM-платформ, журналів подій, систем моніторингу та інвентаризації активів через стандартні API та протоколи. Таким чином, технічні можливості для інтеграції є, але потребують поступового розширення функціоналу та тестування на пілотних об’єктах.

Проте, MCMC-моделювання та сценарний аналіз можуть бути доволі ресурсоємними, особливо для великих моделей і значної кількості сценаріїв. Водночас сучасні хмарні платформи можуть дозволити гнучко масштабувати обчислювальні ресурси залежно від потреб.

Узагальнюючи результати технологічного аудиту, можна зробити висновок, що більшість ключових компонент є доступними й придатними для реалізації проєкту. Основні обмеження пов’язані не стільки з технологіями, скільки з необхідністю виділення часу та ресурсів на інженерну розробку, проєктування інтерфейсу (UX/UI) та валідацію продукту на реальних або пілотних об’єктах.

4.3 Аналіз можливості запуску стартап-проєкту на ринок

У цьому підрозділі наведено аналіз попиту, доступності та динаміки ринку для запуску сервісу кількісної оцінки кібернадійності SCADA- та інших OT-систем. Потенційний ринок формується під впливом посилення регуляторних вимог до кібербезпеки об’єктів критичної інфраструктури, зростання кількості кібератак на ICS/SCADA-середовище та потреби операторів у формалізованих, кількісних показниках стійкості.

Потенційними споживачами є оператори критичної інфраструктури (енергетика, водопостачання, транспорт, промисловість), консалтингові й інтеграційні компанії у сфері OT-безпеки, а також регулятори й органи нагляду, зацікавлені в обґрунтованій оцінці рівня кіберзахищеності.

Таблиця 4.2 – Характеристика потенційного ринку проєкту

	Показники стану ринку	Характеристика
1.	Кількість конкурентів у ніші спеціалізованих OT-рішень	Обмежена; переважають загальні IT-ризик-платформи

Кінець таблиці 4.2

2.	Загальний обсяг ринку	Суттєвий, формується за рахунок операторів КІ та їхніх підрядників
3.	Динаміка ринку	Зростаюча (посилення регуляцій, збільшення інцидентів)
4.	Наявність обмежень для виходу	Помірні; потрібна предметна експертиза в OT/ICS-безпеці
5.	Специфічні вимоги щодо сертифікації та стандартів	Необхідність урахування IEC 62443, NIS-вимог, галузевих регламентів

На підставі цих характеристик можна зробити висновок, що ринок рішень для оцінки кібернадійності OT/SCADA-систем має стійку тенденцію до зростання. Водночас для виходу на нього необхідно враховувати регуляторні вимоги та потребу в довірі з боку операторів критичної інфраструктури.

Потенційні клієнти сервісу поділяються на три основні групи. Насамперед це оператори енергетичних, водоканальних, транспортних та промислових об’єктів, які потребують кількісної оцінки кібернадійності своїх SCADA/OT-систем і інструменту для обґрунтування модернізації захисту. Вони очікують прозорих розрахунків, стандартизованих звітів для регулятора та інтеграції з наявними процесами управління ризиками.

Друга група - консалтингові та інтеграційні компанії у сфері OT-безпеки. Для них сервіс може виступати робочим інструментом в аудитах та проєктах із побудови систем захисту. Ключові вимоги цієї категорії - гнучкість налаштування моделей під різні об’єкти, можливість формувати звіти під власним брендом і «прозорість» методики розрахунків.

Третю групу становлять регуляторні та наглядові органи, які зацікавлені в уніфікованих і відтворюваних показниках рівня кіберзахищеності об’єктів критичної інфраструктури. Вони потребують

інструмент, що забезпечує методично коректні розрахунки, підтримує стандартизовані формати звітності та дозволяє порівнювати результати між різними підприємствами й галузями.

Було проаналізувано фактори ризику, які можуть виникнути та перешкодити запуску проекту та результати представлені в таблиці 4.3

Таблиця 4.3 – Фактори ризику

	Фактор	Зміст ризику	Можлива реакція
1.	Низька обізнаність про методи	Потенційні клієнти можуть недооцінювати користь від кількісної оцінки кібернадійності	Проведення навчальних вебінарів, публікація методичних матеріалів, демонстраційні пілотні проєкти
2.	Консервативність операторів КІ	Обережне ставлення до нових інструментів та змін у процесах кіберзахисту	Пілотні впровадження з обмеженим обсягом, поетапне розгортання, інтеграція в уже існуючі процедури
3.	Регуляторні обмеження	Необхідність узгодження використання сервісу з вимогами галузевих стандартів та сертифікацій	Співпраця з регуляторами, орієнтація на відповідність вимогам, залучення експертів з комплаєнсу

Кінець таблиці 4.3

4.	Наявність загальних IT-ризик-платформ	Клієнти можуть віддавати перевагу «універсальним» рішенням	Позиціонування як доповнення до існуючих платформ, акцент на спеціалізації в OT/SCADA та часових метриках

Наступним кроком було проведено аналіз конкуренції в галузі за Майклом Портером.

Таблиця 4.4 – Аналіз галузевої конкуренції за М.Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
Наявність конкурентів	Вендори OT-безпеки та IT-ризик-платформ	Нові стартапи в галузі кібернадійності КІ	Хмарні платформи, провайдери даних журналів	Оператори КІ, консалтингові компанії	Загальні інструменти оцінки ризиків
Загроза нових гравців	–	Висока для нішевих рішень	–	–	–
Залежність від постачальників	Невисока, використання open-source та стандартних протоколів	–	Постачальники хмарних сервісів і API	–	–

Кінець таблиці 4.4

Залежність від клієнтів	Суттєва, ринок вузький	–		Оператори КІ та регулятори	–
Загроза товарів-замінників	–	–		–	Низька, спеціалізовані інструменти практично відсутні

Узагальнюючи результати наведеного аналізу, можна стверджувати, що ринок для сервісу оцінки кібернадійності SCADA-систем є перспективним: попит підтримується регуляторними вимогами та зростанням кіберзагроз, а прямих конкурентів у вузькій ніші кількісної оцінки кібернадійності фактично немає. Тому за результатами були сформульований перелік факторів конкурентоспроможності (таблиця 4.5).

Таблиця 4.5 – Фактори конкуретноспроможності

	Фактор конкурентоспроможності	Обґрунтування
1.	Спеціалізація на SCADA/OT та об’єктах критичної інфраструктури	Орієнтація саме на технологічні мережі та промислові системи керування, тоді як більшість наявних рішень фокусуються на класичній IT-інфраструктурі, що забезпечує нішеву перевагу.

Кінець таблиці 4.5

2.	Кількісна оцінка кібернадійності	Сервіс надає формалізовані часові показники (середній час до компрометації), тоді як конкурентні продукти здебільшого оперують якісними рівнями ризику або агрегованими індексами.
3.	Сценарне моделювання	Можливість враховувати різні шляхи атаки, рівні підготовки зловмисника та невизначеність параметрів забезпечує більш реалістичне моделювання порівняно зі статичними рейтингами та чек-листами.

Таблиця 4.6 – Порівняльний аналіз

Фактор конкурентоспроможності	Бали 1–20	Рейтинг товарів-конкурентів						
		-3	-2	-1	0	1	2	3
Спеціалізація на SCADA/OT та об’єктах критичної інфраструктури	18							+
Кількісна оцінка кібернадійності	17						+	
Сценарне моделювання	15						+	

Таблиця 4.7 – SWOT-аналіз

Сильні сторони: 1. Спеціалізація на SCADA/OT та об’єктах критичної інфраструктури 2. Кількісна оцінка кібернадійності в метриці MTTC	**Слабкі сторони:** 1. Висока залежність від якості та повноти вхідних даних 2. Складність математичного апарату
Можливості: 1. Використання сервісу для обґрунтування інвестицій у модернізацію OT-мереж	**Загрози:** 1. Високі вимоги до безпеки самого сервісу та можливі додаткові сертифікаційні бар’єри

На основі проведеного SWOT-аналізу формуються можливі варіанти ринкової поведінки та визначаються напрями забезпечення максимально ефективного функціонування проєкту під час його виведення на ринок.

Таблиця 4.8 – Альтернативна ринкова поведінка

№ п/п	Альтернатива – орієнтований перелік заходів поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Залучення бізнес-ангела / seed-інвестора	Середня	12–24 місяці
2	Стратегічне партнерство з OT-інтегратором або вендором SCADA-рішень	Висока	12–18 місяців
3	Отримання міжнародних грантів у сфері кібербезпеки КІ	Низька	18–36 місяців

4.4 Розробка ринкової стратегії продукту

В основі ринкової стратегії запропонованого стартап-проєкту лежить концентрація на вузькому, але високовартісному сегменті - операторах об’єктів критичної інфраструктури та компаніях-інтеграторах, що супроводжують їхні ICS/SCADA-рішення. Такий підхід відповідає специфіці продукту: він орієнтований не на масовий IT-ринок, а на обмежене коло споживачів із високими вимогами до якості, обґрунтованості та надійності рішень у сфері кібербезпеки.

У Таблиці 4.9 узагальнено основні групи користувачів, які можуть стати цільовою аудиторією сервісу.

Таблиця 4.9 - Аналіз груп користувачів

№	Опис профілю	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах груп	Інтенсивність конкуренції в секторі	Простота входу
1	Оператори об’єктів критичної інфраструктури	Є потреба в формалізованих показниках кіберзахищеності, але висока консервативність	Високий	Середня	Потрібні пілотні проєкти та довгий цикл погоджень

Кінець таблиці 4.9

2	Консалтингові та інтеграційні компанії у сфері OT/ICS-безпеки	Продукт підсилює їхні послуги та створює додаткову цінність для клієнтів	Середній	Середня	Відносно проста за умови партнерської моделі та інтеграцій

Таблиця 4.10 – Визначення базової стратегії розвитку

Обрана альтернатива розвитку проєкту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції	Базова стратегія розвитку
Масштабування у партнерстві з OT-інтеграторами та консалтинговими компаніями	Інтеграції, рекламна кампанія	Спеціалізація на середовищі критичної інфраструктури	Стратегія зростання через розширення інтеграцій, формування довгострокових партнерств

Таблиця 4.11 - Визначення базової стратегії конкурентної поведінки

Чи є проєкт першопрохідцем ринку?	Чи будуть шукати нових споживачів чи збирати існуючих	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки
Так	Пошук нових споживачів	Запозичення базових очікуваних функцій	Стратегія диференціації

4.5 Розробка маркетингової програми

Маркетингова програма спрямована на формування розуміння продукту як інструмента, що перетворює складні моделі кіберризику на зрозумілі управлінські рішення.

Таблиця 4.11 – Визначення ключових переваг концепції потенційного товару

№	Потреби	Вигоди, що пропонує товар	Ключові переваги над конкурентами
1	Кількісна оцінка кібернадійності SCADA та підготовка звітів для регуляторів	Розрахунок кібернадійності у зрозумілих кількісних метриках	Використання кількісних показників замість узагальнених рейтингових індексів ризику
2	Прозорість методики оцінювання для аудиторів, консультантів і регуляторів	Документовані моделі, можливість відтворити розрахунки та перевірити припущення	Відкрита модель

Таблиця 4.12- Концепція маркетингових комунікацій

Специфіка поведінки цільових клієнтів	Канали комунікації клієнтів	Ключові пропозиції для позиціонування товару, і які саме	Завдання рекламного повідомлення
Потреба в формалізованих, доказових показниках безпеки	Галузеві конференції з кібербезпеки КІ, презентації, професійні видання	Інструмент кількісної оцінки кібернадійності SCADA	Пояснити, що сервіс зменшує невизначеність ризиків, допомагає планувати модернізацію

Кінець таблиці 4.12

Обережне ставлення до нових рішень	Партнерські програми, вебінари, професійні онлайн-спільноти, ділові соцмережі, спільні кейси з клієнтами	Прозорі, верифіковані моделі	Сформувати довіру до продукту, показати його надійність

Висновки до розділу 4

У четвертому розділі було обґрунтовано можливість перетворення результатів роботи на прикладний стартап-проєкт – сервіс кількісної оцінки кібернадійності SCADA -систем. Показано, що розроблений математичний апарат і програмні напрацювання можуть бути покладені в основу програмного продукту, здатного надавати оператором критичної інфраструктури та консультантам формалізовані показники MTTC і підтримувати прийняття управлінських рішень щодо кіберзахисту. Проведений технологічний аудит засвідчив наявність усіх необхідних передумов для реалізації проєкту. Ринковий аналіз і SWOT-оцінка показали, що в ніші спеціалізованих рішень для кількісної оцінки кібернадійності ICS-середовища конкуренція є помірною, а попит формується посиленням регуляторних вимог і зростанням кількості кіберінцидентів.

Також було сформовано базову ринкову стратегію та розроблено концепцію маркетингових комунікацій, включно з визначенням цільових груп, ключових повідомлень та каналів взаємодії, створює основу для практичної реалізації стартап-проєкту та подальшого комерційного розвитку отриманих наукових результатів.

Таким чином результати дослідження можуть бути трансформовані у конкурентоспроможний сервіс із чітко сформованими цільовими сегментами, стратегією виходу на ринок та моделлю взаємодії з клієнтами.

ВИСНОВКИ

У роботі виконано комплексне дослідження, спрямоване на розроблення підходу до кількісної оцінки кібернадійності SCADA-систем критичної інфраструктури на основі напівмарковських процесів. У першому розділі проаналізовано архітектуру SCADA/ICS-систем у контексті моделі Purdue, розглянуто типові вразливості технологічних мереж та актуальні підходи до оцінки кіберстійкості. Показано, що традиційні методи, орієнтовані переважно на якісні оцінки ризику або статичні індекси, є недостатніми для відображення часової динаміки кібератак та не забезпечують узгодження з класичними показниками надійності й доступності в OT-середовищі. Це обґрунтовує доцільність застосування стохастичних моделей, здатних враховувати як структуру маршруту атаки, так і часові характеристики її проходження.

У другому розділі побудовано напівмарковські моделі розвитку атак на SCADA-систему для різних сценаріїв компрометації, зокрема з урахуванням зовнішнього порушника та інсайдера, а також варіантів топології шляху атаки. Розроблено формалізований опис станів, переходів і поглинаючих подій, визначено структуру матриць перехідних ймовірностей для ланцюгів із поглинанням та виведено співвідношення для обчислення середнього часу до компрометації у вигляді MTTC. Окрему увагу приділено узгодженню напівмарковської моделі з часовими розподілами перебування у станах, що дало змогу перейти від абстрактного опису кроків атаки до кількісної оцінки кібернадійності системи.

У третьому розділі реалізовано підхід до оцінювання з введенням до моделі рівня підготовки атакуючих. На основі емпірично обґрунтованих коефіцієнтів, отриманих із вибірки ICS-вразливостей, сформовано чотири класи атакуючих, які використовуються для масштабування ймовірностей переходів у напівмарковській моделі. Проведено чисельні експерименти для різних сценаріїв. Отримано підтвердження, що рівень підготовки

зловмисника та конфігурація мережевої архітектури суттєво впливають на середній час до компрометації.

У четвертому розділі обґрунтовано можливість трансформації отриманих наукових результатів у прикладний стартап-проєкт. Проведено технологічний аудит, здійснено аналіз потенційного ринку, визначено цільові сегменти та сформовано базову ринкову та конкурентну стратегії, включно зі SWOT-аналізом і визначенням ключових переваг продукту. Показано, що завдяки нішевій спеціалізації, розроблений підхід має реальні передумови для комерціалізації.

Таким чином, було розроблено підхід до оцінки кібернадійності SCADA-систем, який поєднує структурний опис шляху атаки, часові характеристики її розвитку та рівень підготовки атакуючих у єдиній моделі. Отримані результати дозволяють переходити від суто якісних суджень про ризик до кількісних оцінок у вигляді середнього часу до компрометації, придатних для практичного використання при плануванні заходів кіберзахисту.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Andrea De Marco, Davide Berardi, Marta Galuppi, Mara Lombardi, Quantitative resilience assessment on critical infrastructures – A systematic literature review of the last decade (2014-2024), Journal of Safety Science and Resilience, Volume 6, Issue 3, 2025. [Електронний ресурс] — Режим доступу: https://doi.org/10.1016/j.jnlssr.2025.02.002.
2. The State of Ransomware in Critical Infrastructure 2024, A Sophos Whitepaper. July 2024. [Електронний ресурс] — Режим доступу: sophos-state-of-ransomware-critical-infrastructure-2024.pdf
3. 2025 Trustwave Risk Radar Report Energy and Utilities Sector. [Електронний ресурс] — Режим доступу: 2025_Trustwave_Energy_Utilities_Risk_Radar_Report.pdf
4. D. E. Whitehead, K. Owens, D. Gammel and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, USA, 2017, pp. 1-8. [Електронний ресурс] — Режим доступу: https://doi.org/10.1109/CPRE.2017.8090056
5. Devanny, J., Goldoni, L. R. F., & Medeiros, B. P. (2021). The 2019 Venezuelan Blackout and the consequences of cyber uncertainty. Revista Brasileira De Estudos De Defesa, 7(2). [Електронний ресурс] — Режим доступу: https://doi.org/10.26792/rbed.v7n2.2020.75204
6. Thomas Tongxin Li, Peijin Li, Mohannad Alhazmi, Cyber-resilient optimization for power systems: A two-stage strategy integrating social engagement for enhanced energy security engagement, Electric Power Systems Research, Volume 248, 2025). [Електронний ресурс] — Режим доступу: https://doi.org/10.1016/j.epsr.2025.111870
7. S. V. B. Rakas, M. D. Stojanović and J. D. Marković-Petrović, "A Review of Research Work on Network-Based SCADA Intrusion Detection Systems," in IEEE Access, vol. 8, pp. 93083-93108, 2020 [Електронний

ресурс] — Режим доступу: https://doi.org/10.1109/ACCESS.2020.2994961

8. Conti, Mauro & Donadel, Denis & Turrin, Federico. (2021). A Survey on Industrial Control System Testbeds and Datasets for Security Research. IEEE Communications Surveys & Tutorials. PP. 1-1. [Електронний ресурс] — Режим доступу: https://doi.org/10.1109/COMST.2021.3094360

9. Alanazi, Manar & Mahmood, Abdun & Chowdhury, Mohammad. (2022). SCADA Vulnerabilities and Attacks: A Review of the State-of-the-Art and Open Issues. Computers & Security. 125. 103028. [Електронний ресурс] — Режим доступу: https://doi.org/10.1016/j.cose.2022.103028

10. Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., Liang, W. and Philip Chen, C.L. (2014), SCADA communication and security issues. Security Comm. Networks, 7: 175-194. [Електронний ресурс] — Режим доступу: https://doi.org/10.1002/sec.698

11. Abdalhossein Rezai, Parviz Keshavarzi, Zahra Moravej, Key management issue in SCADA networks: A review, Engineering Science and Technology, an International Journal, Volume 20, Issue 1, 2017, Pages 354-363. [Електронний ресурс] — Режим доступу: https://doi.org/10.1016/j.jestch.2016.08.011.

12. Maglaras, Leandros. 2022. "From Mean Time to Failure to Mean Time to Attack/Compromise: Incorporating Reliability into Cybersecurity" Computers 11. [Електронний ресурс] — Режим доступу: https://doi.org/10.3390/computers11110159

13. Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. 2004. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Trans. Dependable Secur. Comput. [Електронний ресурс] — Режим доступу: https://doi.org/10.1109/TDSC.200

14. Гальчинський Л., Личик В. (2023). Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження).

Інформаційні технології та суспільство, 2 (8), 27–33. [Електронний ресурс] — Режим доступу: https://doi.org/10.32689/maup.it.2023.2.

15. Reza Arghandeh, Alexandra von Meier, Laura Mehrmanesh, Lamine Mili, On the definition of cyber-physical resilience in power systems, Renewable and Sustainable Energy Reviews, Volume 58, 2016. [Електронний ресурс] — Режим доступу: https://doi.org/10.1016/j.rser.2015.12.193

16. Emanuele Bellini, Giuseppe D'Aniello, Francesco Flammini, Rosario Gaeta, Situation Awareness for Cyber Resilience: A review, International Journal of Critical Infrastructure Protection, Volume 49, 2025. [Електронний ресурс] — Режим доступу: https://doi.org/10.1016/j.ijcip.2025.100755

17. A. Umunnakwe, H. Huang, K. Oikonomou, K.R. Davis, Quantitative analysis of power systems resilience: Standardization, categorizations, and challenges, Renewable and Sustainable Energy Reviews, Volume 149, 2021. [Електронний ресурс] — Режим доступу: https://doi.org/10.1016/j.rser.2021.111252

18. Saleh Mohammed Alhidaifi, Muhammad Rizwan Asghar, Imran Shafique Ansari, Cyber resilience quantification: A probabilistic estimation model for IT infrastructure, Reliability Engineering & System Safety, Volume 265, Part B, 2025. [Електронний ресурс] — Режим доступу: https://doi.org/10.1016/j.ress.2025.111473

19. 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, [Електронний ресурс] — Режим доступу: https://doi.org/10.1109/td39804.2020.9299922.

20. Ertel, Benjamin & Meer, Jann & Seifert, Udo. (2022). Operationally accessible uncertainty relations for thermodynamically consistent semi-Markov processes. Physical Review E. 105. [Електронний ресурс] — Режим доступу: https://doi.org/10.1103/PhysRevE.105.044113

21. Grabski, Franciszek. (2014). Semi-Markov Processes: Applications in System Reliability and Maintenance. Semi-Markov Processes: Applications

in System Reliability and Maintenance. 1-255. [Електронний ресурс] — Режим доступу: https://doi.org/10.1016/C2013-0-14260-2

22. Grinstead, C. M.; Snell, J. L. Introduction to Probability. AMS, 1997, 416-433. [Електронний ресурс] — Режим доступу: https://math.dartmouth.edu/~prob/prob/prob.pdf

23. CVE: Common Vulnerabilities and Exposures [Електронний ресурс] — Режим доступу: https://www.cve.org/

24. Гальчинський Л., Тостоган Є. (2025). Моделювання кібернадійності scada-систем критичної інфраструктури з використанням напівмарковських процесів, II International Scientific and Theoretical Conference «Modern science and innovation: trends, challenges, and breakthroughs», 210-220. URL https://doi.org/10.36074/scientia-21.11.2025

25. Karras, Christos & Karras, Aristeidis & Avlonitis, Markos & Sioutas, Spyros. (2022). An Overview of MCMC Methods: From Theory to Applications. 10.1007/978-3-031-08341-9_26.

26. Matthew D. Homan and Andrew Gelman. 2014. The No-U-turn sampler: adaptively setting path lengths in Hamiltonian Monte Carlo. J. Mach. Learn. Res. 15, 1 (January 2014), 1593–1623. https://doi.org/10.48550/arXiv.1111.4246

27. Rencelj Ling, E., Ekstedt, M. Estimating Time-To-Compromise for Industrial Control System Attack Techniques Through Vulnerability Data. *SN COMPUT. SCI.* **4**, 318 (2023). https://doi.org/10.1007/s42979-023-01750-z

Додаток А Лістинг програми 1

```
import pymc as pm
import numpy as np
import matplotlib.pyplot as plt
from scipy.special import gamma
from scipy.stats import gamma as gamma_dist, norm, lognorm

samples = 15000
pG1, p12, p2F = 0.62, 0.13, 0.25
pG2_base = 0.5
I = np.eye(3)

skill_fractions = {
    "Expert": 1.0,
    "Intermediate": 0.50,
    "Beginner": 0.24,
    "Novice": 0.05
}

with pm.Model() as model:
    k_G = pm.Uniform("k_G", lower=1, upper=5)
    k_1 = pm.Uniform("k_1", lower=1, upper=5)
    k_2 = pm.Uniform("k_2", lower=1, upper=5)

    lam_G = pm.Gamma("lam_G", alpha=2, beta=0.5)
```

```
    lam_1 = pm.Gamma("lam_1", alpha=2, beta=0.5)
    lam_2 = pm.Gamma("lam_2", alpha=2, beta=0.5)
    trace = pm.sample(samples, chains=1, tune=500, progressbar=False)


E_G = trace.posterior['lam_G'].values.flatten() * gamma(1 + 1 /
trace.posterior['k_G'].values.flatten())
E_1 = trace.posterior['lam_1'].values.flatten() * gamma(1 + 1 /
trace.posterior['k_1'].values.flatten())
E_2 = trace.posterior['lam_2'].values.flatten() * gamma(1 + 1 /
trace.posterior['k_2'].values.flatten())
T = np.vstack([E_G, E_1, E_2]).T


results = {}
fits_expert = {}


for skill, fraction in skill_fractions.items():
    # Масштабуємо ймовірності
    pG1_scaled = pG1 * fraction
    pG2_scaled = pG2_base * fraction
    p12_scaled = p12 * fraction
    p2F_scaled = p2F * fraction


    # --- Сценарій 1: pG2=0 ---
    Q1 = np.array([
        [1 - pG1_scaled, pG1_scaled, 0],
        [0, 1 - p12_scaled, p12_scaled],
```

```
        [0, 0, 1 - p2F_scaled]
    ])
    N1 = np.linalg.inv(I - Q1)
    ET1 = np.sum(N1 @ T.T, axis=0)

    # --- Сценарій 2: pG2=0.5 ---
    Q2 = np.array([
        [1 - pG1_scaled - pG2_scaled, pG1_scaled, pG2_scaled],
        [0, 1 - p12_scaled, p12_scaled],
        [0, 0, 1 - p2F_scaled]
    ])
    N2 = np.linalg.inv(I - Q2)
    ET2 = np.sum(N2 @ T.T, axis=0)

    results[skill] = {
        "pG2=0": np.mean(ET1),
        "pG2=0.5": np.mean(ET2)
    }

print("Середній час до компрометації:")
print("{:<12} {:>12} {:>12}".format("Навичка", "pG2=0", "pG2=0.5"))
for skill in skill_fractions:
    print("{:<12} {:>12.2f} {:>12.2f}".format(
        skill,
        results[skill]["pG2=0"],
```

```
        results[skill]["pG2=0.5"]
    ))


# --- Графік порівняння середніх часів ---
labels = list(skill_fractions.keys())
x = np.arange(len(labels))
width = 0.35


fig, ax = plt.subplots(figsize=(10, 6))
bar1 = ax.bar([i - width/2 for i in x], [results[lvl]["pG2=0"] for lvl in labels], width, label="External")
bar2 = ax.bar([i + width/2 for i in x], [results[lvl]["pG2=0.5"] for lvl in labels], width, label="Insider")
ax.set_ylabel('Середній час до компрометації')
ax.set_title('Вплив навичок атакуючих на час до компрометації')
ax.set_xticks(x)
ax.set_xticklabels(labels)
ax.legend(loc='upper left')
plt.tight_layout()
plt.show()
```

Додаток Б Лістинг програми 2

```
import pymc as pm
import numpy as np
from scipy.special import gamma

samples = 15000
pG1, p12, p23, p3F = 0.73, 0.15, 0.25, 40
p2F_base = 0.5          # для сценарію з p2F = 0.5
I = np.eye(4)

skill_fractions = {
    "Expert": 1.0,
    "Intermediate": 0.50,
    "Beginner": 0.24,
    "Novice": 0.05
}
with pm.Model() as model:
    k_G = pm.Uniform("k_G", lower=1, upper=5)
    k_1 = pm.Uniform("k_1", lower=1, upper=5)
    k_2 = pm.Uniform("k_2", lower=1, upper=5)
    k_3 = pm.Uniform("k_3", lower=1, upper=5)

    lam_G = pm.Gamma("lam_G", alpha=2, beta=0.5)
    lam_1 = pm.Gamma("lam_1", alpha=2, beta=0.5)
    lam_2 = pm.Gamma("lam_2", alpha=2, beta=0.5)
```

```
    lam_3 = pm.Gamma("lam_3", alpha=2, beta=0.5)
    trace = pm.sample(samples, chains=1, tune=500, progressbar=False)


E_G = trace.posterior["lam_G"].values.flatten() * gamma(1 + 1 / trace.posterior["k_G"].values.flatten())
E_1 = trace.posterior["lam_1"].values.flatten() * gamma(1 + 1 / trace.posterior["k_1"].values.flatten())
E_2 = trace.posterior["lam_2"].values.flatten() * gamma(1 + 1 / trace.posterior["k_2"].values.flatten())
E_3 = trace.posterior["lam_3"].values.flatten() * gamma(1 + 1 / trace.posterior["k_3"].values.flatten())
T = np.vstack([E_G, E_1, E_2, E_3]).T   # (samples × 4)


results = {}


for skill, fraction in skill_fractions.items():
    pG1_s  = pG1 * fraction
    p12_s  = p12 * fraction
    p23_s  = p23 * fraction
    p3F_s  = p3F * fraction
    p2F_s  = p2F_base * fraction

    # --- Сценарій 1: p2F = 0 ---
    Q1 = np.array([
        [1 - pG1_s,         pG1_s, 0,        0],
        [1 - p12_s,         0,     p12_s,    0],
        [1 - p23_s - 0.0,   0,     0,        p23_s],
```

```
        [1 - p3F_s,         0,     0,        0]
    ])
    N1 = np.linalg.inv(I - Q1)
    ET1 = np.sum(N1 @ T.T, axis=0)

    # --- Сценарій 2: p2F = 0.5 ---
    Q2 = np.array([
        [1 - pG1_s,             pG1_s, 0,        0],
        [1 - p12_s,             0,     p12_s,    0],
        [1 - p23_s - p2F_s,     0,     0,        p23_s],
        [1 - p3F_s,             0,     0,        0]
    ])
    N2 = np.linalg.inv(I - Q2)
    ET2 = np.sum(N2 @ T.T, axis=0)
    results[skill] = {
        "p2F=0":   np.mean(ET1),
        "p2F=0.5": np.mean(ET2)
    }

print("Середній час до компрометації:")
print("{:<12} {:>12} {:>12}".format("Навичка", "p2F=0", "p2F=0.5"))
for skill in skill_fractions:
    print("{:<12} {:>12.2f} {:>12.2f}".format(
        skill,
        results[skill]["p2F=0"],
```

```
        results[skill]["p2F=0.5"]
    ))

labels = list(skill_fractions.keys())
x = np.arange(len(labels))
width = 0.35

fig, ax = plt.subplots(figsize=(10, 6))
bar1 = ax.bar([i - width/2 for i in x], [results[lvl]["p2F =0"] for lvl in labels], width, label="External")
bar2 = ax.bar([i + width/2 for i in x], [results[lvl]["p2F =0.5"] for lvl in labels], width, label="Insider")
ax.set_ylabel('Середній час до компрометації')
ax.set_title('Вплив навичок атакуючих на час до компрометації')
ax.set_xticks(x)
ax.set_xticklabels(labels)
ax.legend(loc='upper left')
plt.tight_layout()
plt.show()
```