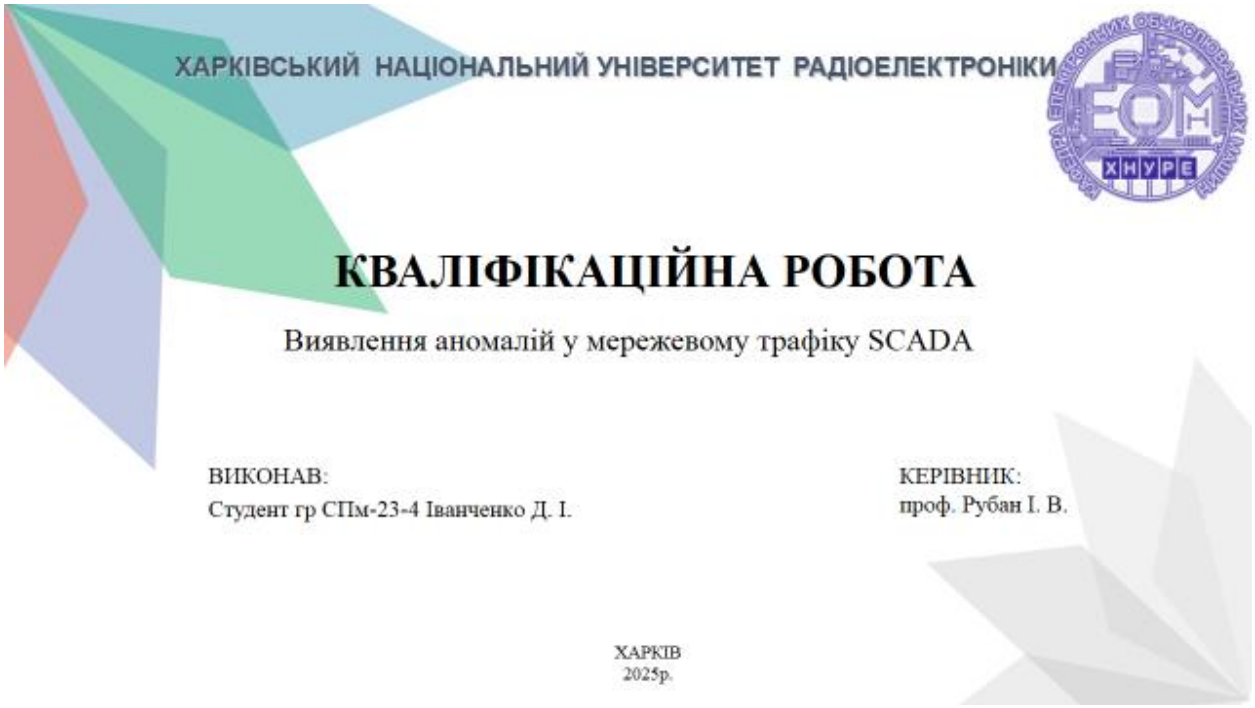
ДОДАТОК А

Графічний матеріал кваліфікаційної роботи



Актуальність дослідження

SCADA-системи (Supervisory Control and Data Acquisition) є критичними для управління інфраструктурою — енергетикою, водопостачанням, транспортом тощо

Їх **відкритість до мережевих підключень** робить ці системи вразливими до кібератак

Більшість атак на SCADA не викликає миттєвих збоїв, а проявляється у вигляді **аномальної активності в мережевому трафіку**

Своєчасне виявлення аномалій дозволяє попередити порушення роботи критичних об’єктів

икористання **методів машинного навчання** у поєднанні з попередньо зібраними шаблонами (white-listing) підвищує **надійність і точність** захисту

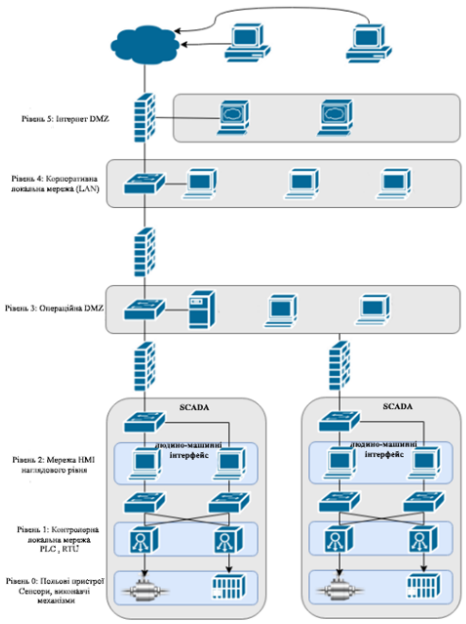
Мета та завдання

Мета дослідження
Розробка методу виявлення аномалій у мережевому трафіку SCADA-систем на основі аналізу протоколів (зокрема IEC 60870-5-104 та ARP) з використанням механізмів білого списку та часових характеристик.

Завдання

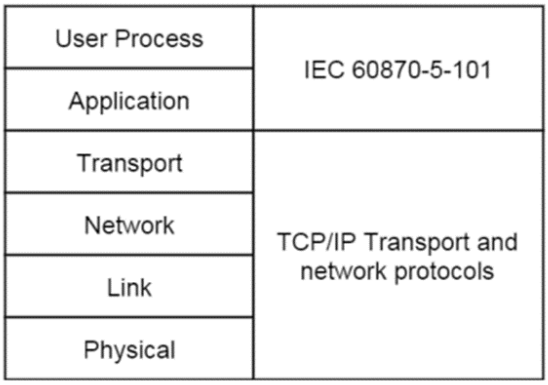
- Дослідити особливості мережевого трафіку SCADA-систем
- Визначити типові сценарії атак (spoofing, port scan, MITM тощо)
- Розробити структуру whitelist-моделі для ARP, портів і таймінгу
- Реалізувати механізм виявлення аномалій на основі часових відхилень
- Провести тестування моделі на реальних або емульованих даних
- Оцінити ефективність запропонованого підходу за метриками точності

3



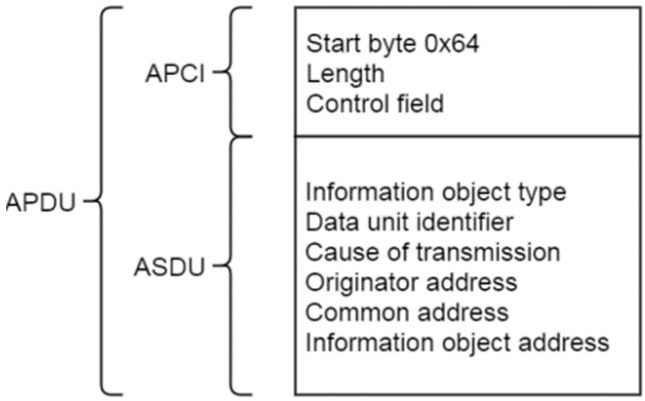
4

Огляд стеку протоколів



5

Формат блоку даних протоколу додатку (APDU)



6

Типи атак на SCADA

ARP Spoofing (Підміна ARP)

- Маніпулювання ARP-таблицями для створення MITM-умов
- Атакуючий перехоплює або змінює пакети між HMI та RTU

Port Scanning (Сканування портів)

- Визначення відкритих портів на пристроях SCADA
- Може бути виконано як ззовні, так і з компрометованого вузла

MITM (Man-in-the-Middle)

- Повне перехоплення трафіку між легітимними вузлами
- Може супроводжуватись модифікацією або затримкою команд

Packet Injection (Ін’єкція пакетів)

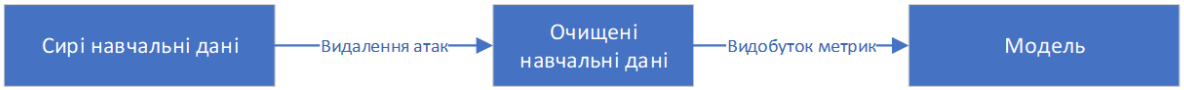
- Вставлення фальшивих команд або даних у мережу
- Особливо небезпечно при підміні команд управління

7

Огляд системи виявлення аномалій

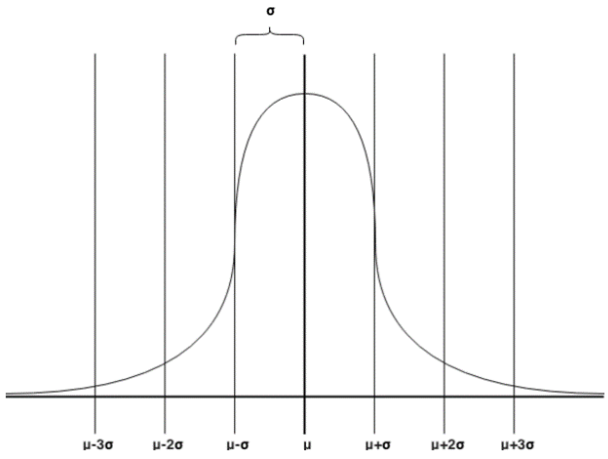
8

Огляд процесу створення моделі системи



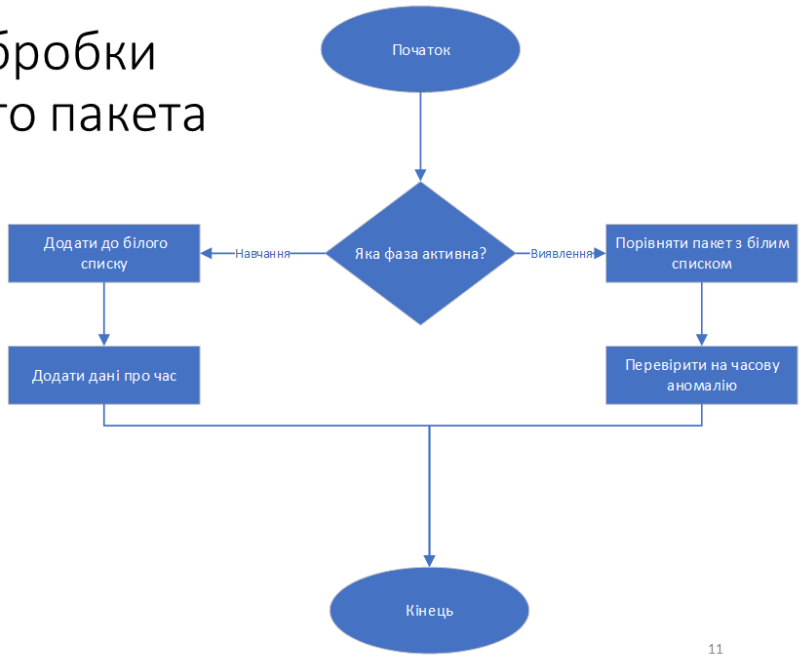
9

Показано нормальний розподіл із середнім значенням та стандартним відхиленням



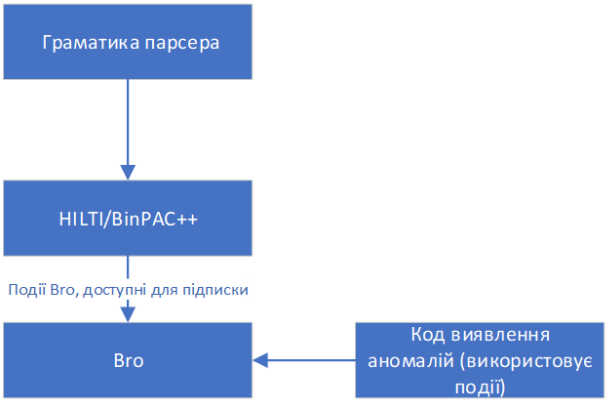
10

Блок-схема обробки новоприбулого пакета



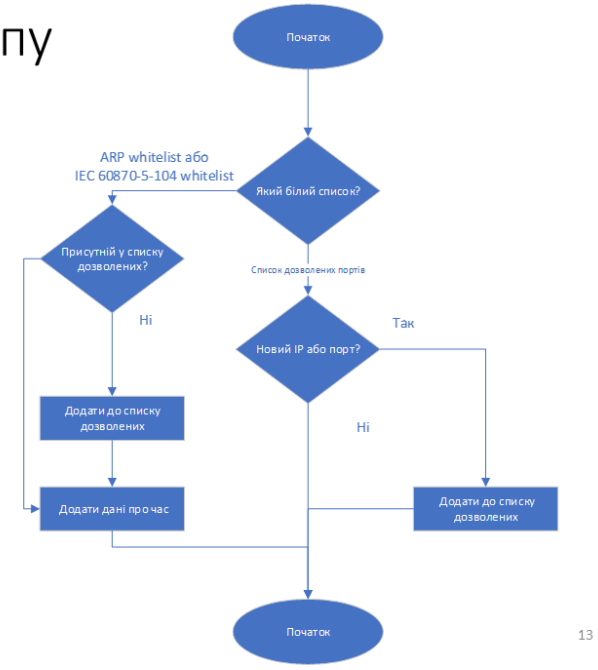
11

Огляд компонентів системи



12

Блок-схема для етапу навчання



13

Першим кроком є обчислення інтервалу часу між оброблюваним пакетом та попереднім пакетом того самого типу. Це показано у формулі (3.1). Варто зазначити, що для обчислення різниці часу потрібні принаймні два пакети, тому ця формула застосовується лише за умови n ≥ 2.

$$\Delta t_n = t_n - t_{n-1}, \quad для\ n \geq 2 \tag{3.1}$$

Значення Δt_n (різниця часу між поточним і попереднім пакетом) далі використовується для обчислення мінімального та максимального значення серед усіх отриманих пакетів, як показано у формулах (3.2) та (3.3).

$$\Delta tmin_n = \min(\Delta t_n, \Delta tmin_{n-1}) \tag{3.2}$$

$$\Delta tmax_n = \max(\Delta t_n, \Delta tmax_{n-1}) \tag{3.3}$$

Середнє значення обчислюється інкрементно, щоб уникнути збереження всіх значень і не витрачати пам'ять. Інкрементні формули наведені у рівняннях (3.4) та (3.5).

$$\mu_2 = t_2 - t_1 \tag{3.4}$$

$$\mu_n = \mu_{n-1} + \frac{\Delta t_n - \mu_{n-1}}{n-1}, \quad для\ n > 2 \tag{3.5}$$

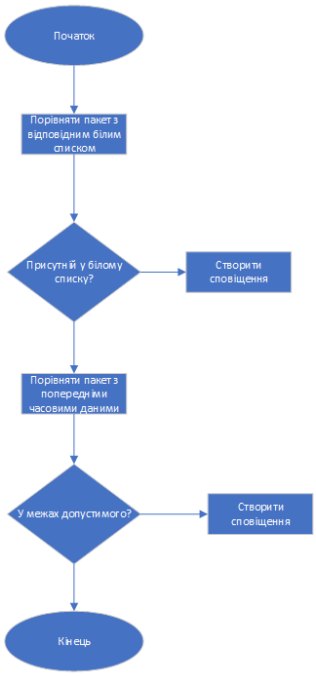
Змінна Sn обчислюється з використанням середнього значення, як показано у формулах (3.6) та (3.7).

$$S_2 = 0 \tag{3.6}$$

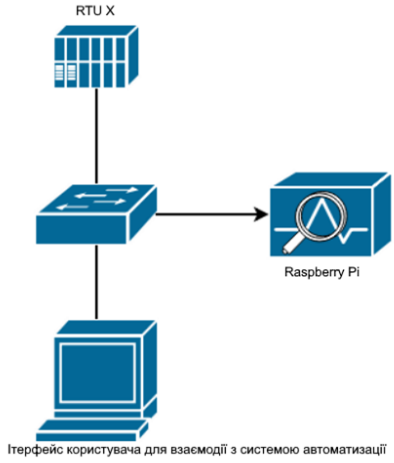
$$S_n = S_{n-1} + (\Delta t_n - \mu_{n-1})(\Delta t_n - \mu_n), \quad для\ n > 2 \tag{3.7}$$

14

Блок-схема етапу виявлення

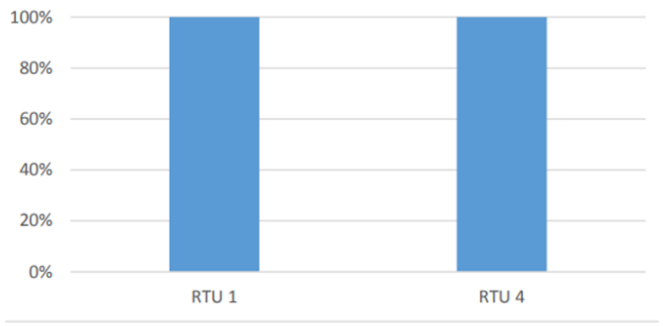


15



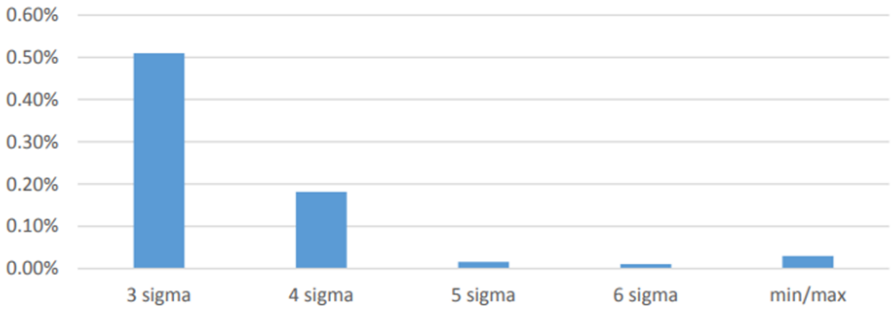
16

Відсоток позитивних результатів сканування портів



17

Середній FPR для RTU 1 та RTU 4 атаки MITM



18

Висновки

У межах цієї кваліфікаційної роботи було реалізовано систему виявлення аномалій у трафіку протоколу IEC 60870-5-104, який широко використовується в SCADA-системах. З урахуванням специфіки таких систем, де передавання даних відбувається у передбачуваному та детермінованому режимі, основною ідеєю проєкту стало використання часових характеристик мережевого трафіку для виявлення потенційних атак.

Для реалізації підходу було обрано платформу Bro (тепер Zeek), яка дозволила побудувати повноцінну аномалійну систему виявлення завдяки підтримці сценаріїв на власній мові програмування та можливості інтеграції з власноруч створеними парсерами протоколів. Було створено спеціальний парсер для IEC 60870-5-104 за допомогою генератора Spicy, що забезпечив гнучкий аналіз трафіку на прикладному рівні.

Система працює у двох режимах: навчальному та режимі виявлення. Під час навчання формується модель нормальної поведінки системи — будуються «білі списки» допустимих взаємодій хостів, портів та інтервалів між пакетами. У режимі виявлення усі вхідні пакети перевіряються на відповідність цим спискам, а також аналізуються за допомогою правила трьох сигм для оцінки відхилення часового інтервалу.

Апробація результатів: Мартовицький В. О., Шеховцов О. В., Алєйник Д. С., Пахомова Є. В. та Іванченко Д. І. «ПІДХІД ДО ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ РАДІОКЕРОВАНИХ МОДЕЛЕЙ ЗА ЇХ РАДІОСИГНАЛОМ» Вісник Херсонського національного технічного університету» для розміщення у № 2 (2025) 19