МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ТИМЧАК Андрій Миколайович

АЛГОРИТМИ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ У КІБЕРФІЗИЧНИХ СИСТЕМАХ / ALGORITHMS FOR PROTECTING CONFIDENTIAL DATA IN CYBER-PHYSICAL SYSTEMS

спеціальність: 125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
А. М. Тимчак

Науковий керівник
к.т.н., доцент Н.Г.Яцків

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2024 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ - 2024

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 - Кібербезпека та захист інформації
освітньо-професійна програма –Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ТИМЧАК АНДРІЙ МИКОЛАЙОВИЧ
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Алгоритми захисту конфіденційних даних у кіберфізичних системах / Algorithms for Protecting Confidential Data in Cyber-Physical Systems
керівник роботи к.т.н., доцент Н.Г.Яцків
затверджені наказом по університету від 12 грудня 2023 року № 753
2. Строк подання студентом закінченої випускної кваліфікаційної роботи 12 грудня 2024 року.
3. Вихідні дані до кваліфікаційної роботи: завдання на випускну кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити:
– дослідити сферу застосування кіберфізичних пристроїв та їх типи;
– провести аналіз потенційних загроз для кіберфізичних систем;
– описати структуру та методи виявлення атак на кіберфізичні системи;
– провести дослідження ефективності застосування honeypot для захисту кіберфізичних систем;
– запропонувати алгоритм захисту даних на основі аналізу трафіку;
– розробити сніфер пакетів, для відстеження та перевірки даних в мережі;
– розробити засіб для аналізу перехоплених даних та роботи з білим списком доступу.
5. Перелік графічного матеріалу у роботі:

- Кіберфізичні системи
- Октет безпеки інформації
- Анатомія кібератаки
- Модель моніторингу даних
- Характеристика поведінки трафіку КФС
- Діаграма застосування пакетного сніфера
- Графік втрати пакетів
- Інтерфейс аналізатора IP адрес.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 12 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Типи та властивості кіберфізичних систем	12.2023 р. – 03.2024 р.	
2	Аналіз потенційних загроз для кіберфізичних систем	03.2024 р. – 06.2024 р.	
3	Розробка сніфера для аналізу та блокування небажаного трафіку	06.2024 р. – 11.2024 р.	

Студент _____ Андрій ТИМЧАК
(підпис)

Керівник роботи _____ к.т.н., доцент Наталя ЯЦКІВ
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Алгоритми захисту конфіденційних даних у кіберфізичних системах» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека та захист інформації» освітньо-професійної програми «Кібербезпека» написана обсягом 65 сторінок і містить 29 рисунків, 3 таблиці та 58 джерел за переліком посилань.

Метою кваліфікаційної роботи є дослідження алгоритмів та методів захисту конфіденційних даних у кіберфізичних системах на основі аналізу трафіку.

Методи досліджень. Для розв'язання поставлених задач у даній кваліфікаційній роботі використано: методи аналізу та контролю трафіку, обмеження доступу, процеси автентифікації.

Результати дослідження: проведено аналіз сфери застосування кіберфізичних систем та запропоновано алгоритм захисту від кібератак на основі білого списку доступу.

Результати роботи можуть успішно застосовуватися при контролі доступу до кіберфізичних систем та для захисту конфіденційних даних.

Ключові слова: кібербезпека, кіберфізичні системи, Інтернет речей, захист даних, пошук вразливостей, мережева розвідка, аналіз трафіку, honeypot, сніфери пакетів, контроль доступу.

ABSTRACT

The graduate work on the topic «Algorithms for Protecting Confidential Data in Cyber-Physical Systems» for Master’s degree on speciality 125 "Cybersecurity and Information Protection" is written on 65 pages and contains 29 illustrations, 3 tables and 58 references.

The aim of the qualification work is to study algorithms and methods for protecting confidential data in cyber-physical systems based on traffic analysis.

Research Methods. To solve the assigned tasks, the following methods were used in this qualification work: traffic analysis and monitoring methods, access restriction techniques, and authentication processes.

Results of the study. The study includes an analysis of the application domain of cyber-physical systems and proposes an algorithm for protection against cyberattacks based on a whitelist access approach.

The results of the work can be successfully applied to access control for cyber-physical systems and for the protection of confidential data.

KEYWORDS: CYBERSECURITY, CYBER-PHYSICAL SYSTEMS, INTERNET OF THINGS, DATA PROTECTION, VULNERABILITY ASSESSMENT, NETWORK RECONNAISSANCE, TRAFFIC ANALYSIS, HONEYPOT, PACKET SNIFFERS, ACCESS CONTROL.

.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

КФС - кіберфізична система.

BMS - автоматизована система управління в будівлі.

NIST - Національний інститут стандартів і технологій.

CIA (КЦД) - конфіденційність, цілісність, доступність.

АСУ - автоматизовані системи управління.

СУП - системи управління процесами.

SCADA - системи диспетчерського контролю та збору даних.

IIoT - промисловий Інтернет речей.

IoT - Інтернет речей.

DPI - глибока перевірка пакетів.

NIDS - датчики системи виявлення вторгнень у мережу.

AS - автономні системи.

ISP - постачальник інтернет послуг.

ВСТУП

Кіберфізичні системи (КФС) широко використовуються в технологічній та промисловій сферах для оптимізації процесів та забезпечення функціональності, яка раніше була недоступна. Однак за останнє десятиліття вони були ключовими цілями в деяких із найбільш розголошених порушень безпеки.

Використання концепцій лише кібернетичної або фізичної безпеки не можуть захистити КФС самі по собі, оскільки складні взаємозалежності та перехресні ефекти можуть створити несподівані вразливості – фізичні атаки можуть пошкодити або скомпрометувати інформаційну систему на пристрої, а кібератаки можуть спричинити фізичні збої.

Через багато критичних програм, де використовується КФС, будь-який вид атаки на них може призвести до пошкодження або втрати інформації, тому безпека та конфіденційність мають бути ключовими при проектуванні, розробці та експлуатації КФС.

Мета і завдання дослідження. Метою роботи є дослідження технологій та алгоритмів захисту конфіденційних даних у кіберфізичних системах на основі аналізу трафіку.

Досягнення визначеної мети передбачає вирішення таких завдань:

– дослідити сферу застосування кіберфізичних пристроїв та їх типи;

– провести аналіз потенційних загроз для кіберфізичних систем;

– описати структуру та методи виявлення атак на кіберфізичні системи;

– провести дослідження ефективності застосування honeypot для захисту кіберфізичних систем;

– запропонувати алгоритм захисту даних на основі аналізу трафіку;

– розробити сніфер пакетів, для відстеження та перевірки даних в мережі;

– розробити засіб для аналізу перехоплених даних та роботи з білим списком доступу.

Об’єкт дослідження – процеси здійснення кібератак та захисту від них.

Предмет дослідження – алгоритми та методи захисту даних при передачі в кіберфізичних системах.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи аналізу та контролю трафіку, обмеження доступу, процеси автентифікації.

Наукова новизна одержаних результатів. Проведено аналіз сфери застосування кіберфізичних систем та запропоновано алгоритм захисту від кібератак на основі білого списку доступу.

Практичне значення отриманих результатів. Розроблено програмну реалізацію сніфера пакетів та захисту трафіку на основі білого списку доступу.

Публікації та апробація до магістерської роботи.

1. Микита Онищенко, Андрій Тимчак, Геннадій Понедєльніков. (2024). Забезпечення захисту кіберфізичних систем за допомогою моніторингу. *Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2024)*, Тернопіль, с. 46-48.

2. Микита Онищенко, Андрій Тимчак, Геннадій Понедєльніков. (2024). Захист даних у кіберфізичних системах. *Збірник матеріалів науково-практичного симпозіуму «Захист Інформації».* Тернопіль, с. 73-75.

РОЗДІЛ 1. ТИПИ ТА ВЛАСТИВОСТІ КІБЕРФІЗИЧНИХ СИСТЕМ

1.1. Основні поняття та терміни в області захисту конфіденційних даних в кіберфізичних системах

КФС використовуються в різних сферах, для забезпечення оптимізації процесів, а поєднання мережевих цифрових систем та аналогових фізичних процесів створює унікальні характеристики, які змінюють спосіб застосування теорії безпеки (рис. 1.1). Проте, перш ніж досліджувати захист конфіденційних даних у КФС, необхідно зрозуміти визначення термінів, що описують функціонал та властивості таких систем [1].

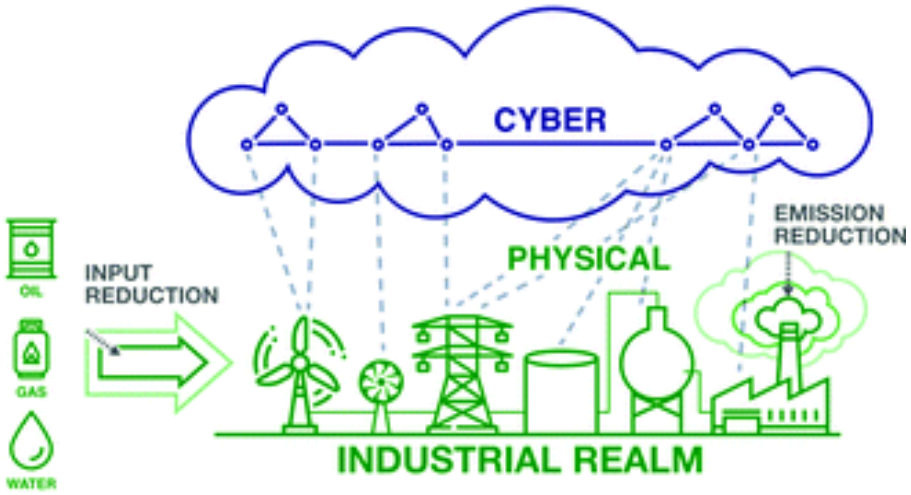


Рисунок 1.1 – Кіберфізичні системи

Заходи безпеки — це набір заходів, які гарантують, що система зможе досягти своєї мети за призначенням, одночасно пом’якшуючи непередбачені негативні наслідки. Коли до системи додаються функції, застосовується безпека, щоб гарантувати, що доповнення не порушують заплановану функціональність і не створюють нових векторів атак.

Національний інститут стандартів і технологій (NIST) визначає конфіденційність як «гарантію того, що конфіденційність і доступ до певної інформації про організацію захищені» [2]. Суб'єктом в цьому випадку може

бути як корпорація чи установа, так і окрема особа, а під «певною інформацією» варто розуміти будь-яку конфіденційну інформацію, наприклад особиста інформація.

Безпека та конфіденційність мають спільні поняття належного використання та захисту інформації. Конфіденційність часто розглядають як свободу від спостереження, занепокоєння чи небажаної уваги громадськості та здатність індивіда чи групи обмежувати своє самовираження. Конфіденційність часто розглядається як аспект безпеки, можливість конфіденційності, оскільки безпечна система повинна захищати конфіденційність своїх користувачів. Конфіденційність зазвичай означає, що інформація не передається стороннім особам, але конфіденційність має більш динамічний вимір, дозволяючи власникам самостійно контролювати розповсюдження своєї інформації.

Концепції безпеки та конфіденційності можна застосовувати як до кібер, так і до фізичної сторони КФС. Для цих понять існує багато термінів, що збігаються, зокрема кібербезпека, інформаційна безпека, забезпечення інформації та інші. Для оцінки захисту конфіденційних даних варто розглядати нефізичний, інформаційний бік КФС. Таким чином, термін інформаційна безпека, як визначено NIST, буде достатнім – умова, яка є результатом встановлення та підтримки захисних заходів, які дозволяють підприємству виконувати свою місію або критичні функції, незважаючи на ризики, пов’язані з загрозами для використання ним інформаційних систем. Захисні заходи можуть включати поєднання стримування, уникнення, запобігання, виявлення, відновлення та виправлення, які повинні становити частину підходу підприємства до управління ризиками [3].

Інформаційна безпека загалом характеризується трьома основними принципами, які визначають як:

• Конфіденційність – доступ до пов’язаних з комп’ютером активів мають лише авторизовані сторони.

• Цілісність – активи можуть бути змінені лише уповноваженими сторонами або лише дозволеними способами.

• Доступність – активи доступні для уповноважених сторін у відповідний час.

Разом вони відомі як тріада CIA або тріада КЦД в Україні, та забезпечують надійний доступ до правильної інформації для потрібних людей/програм/машин (рис. 1.2).

Рисунок 1.2 – Тріада CIA (КЦД)

Тріада КЦД є основою інформаційної безпеки, проте вважається неповною. Неодноразово обговорюються спроби удосконалити тріаду шляхом заміни її на октет безпеки інформації [4]. Запропонований октет безпеки інформації, окрім тріади включає в себе підзвітність, автентифікацією та надійність, можливість перевірки, неспростовність та конфіденційність (рис. 1.3).

Повний перелік цілей безпеки остаточно не узгоджено, але до тріади зазвичай додають два додаткові елементи, які найбільше стосуються фізичної сторони КФС.

Ці два останні принципи часто об’єднують у принцип цілісності, але вони достатньо важливі, щоб заслуговувати на окрему увагу:

● Автентифікація – перевіряє особу, часто як передумову доступу.

● Невідмовність – захищає від помилкового заперечення особою виконання певної дії та фіксує, чи виконав користувач певні дії (наприклад, надсилання чи отримання повідомлення) [5].

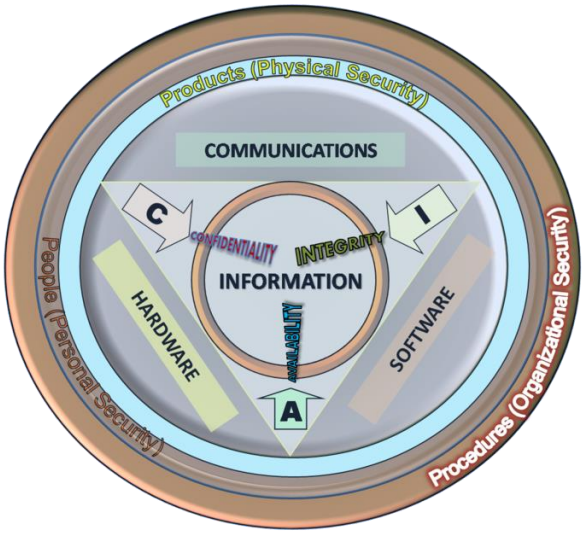


Рисунок 1.3 – Октет безпеки інформації

Існує ряд засобів реалізації кожного з цих принципів кібербезпеки. Наприклад, шифрування забезпечує конфіденційність, захищаючи дані та функції системи від несанкціонованого використання. Цифрові підписи та безпечні геші забезпечують цілісність, гарантуючи, що дані чи оновлення програмного забезпечення не змінюються. Резервування ресурсів забезпечує доступність системи для призначених користувачів для належного використання в будь-який час, навіть під час стресу. Особи, сертифікати та паролі є прикладами механізмів автентифікації, які гарантують, що лише авторизовані користувачі можуть отримати доступ до ресурсів, захищених заходами конфіденційності. Автентифікація забезпечує цілісність шляхом перевірки повноважень суб’єктів, які змінюють актив. Автоматично зібрані записи та журнали цих змін можуть показувати, який користувач відкривав або змінював певні частини системи. Коли ці журнали захищені певним механізмом цілісності, результатом є система з неспростуванням. Невідмовність робить порушення цілісності очевидними та надає криміналістично корисну інформацію, коли захист не працює [2].

Конфіденційність в інформаційному розумінні цього слова зазвичай відноситься до принципу конфіденційності, але це також стосується контрольованого розкриття інформації. Люди хочуть мати можливість

розкривати інформацію одним, а не іншим, і вони хочуть мати можливість контролювати те, що робиться з розкритою інформацією.

Таким чином, конфіденційність є аспектом цілісності особистої інформації, тому що, хоча дані про особу можуть передаватися, інформація, яка в них міститься, завжди є власністю ідентифікованої ним особи.

Іншою стороною КФС, яку згадували раніше є фізичний захист. Він має на меті захищати простір відповідно до принципів, узятих із [6] і [7]:

• Стримування – реальна загроза контрзаходів, яка запобігає діям проти системи, роблячи передбачувану вартість атаки значно вищою ніж передбачувана користь від неї.

• Виявлення – позитивна оцінка того, що певний об’єкт спричинив тривогу та/або повідомлення про потенційну зловмисну дію за допомогою сигналізації.

• Затримка – перешкоди, що уповільнюють або перешкоджають зловмиснику отримати доступ та виконати зловмисну дію по відношенню до захищеного активу.

• Відповідь – дії, вжиті з належною силою, призначені для зупинки просування супротивника.

• Нейтралізація – унеможливлення втручання зловмисника у певну операцію.

Стримування може бути настільки ж нешкідливим, як знак, що вказує на наявність компонентів фізичної безпеки, або охоронець, розміщений на видному місці, щоб попередити потенційного супротивника про наслідки нападу. Крім цього, виявлення зазвичай здійснюється за допомогою технологій спостереження, спостерігачів або оперативних процесів. Сигнали тривоги можуть поєднуватися з виявленням, щоб попередити тих, хто захищає актив, або щоб налякати зловмисника. Бар’єри, такі як стіни, розгорнуті перешкоди, контейнери для зберігання, замки та пристрої, стійкі до несанкціонованого доступу, потребують часу, щоб ворог проникнув, забезпечуючи затримку і певний стримуючий ефект, якщо заходи помітні. Реакція на випадки

вторгнення має бути негайною та ефективною, та може включати в себе виклик представників влади з достатньою силою, щоб зупинити атаку. Без своєчасної реакції неможливо повністю нейтралізувати жодну загрозу. Реагувальники нейтралізують усіх зловмисників, заарештовуючи їх або якимось іншим чином унеможливлюючи повторну атаку на систему таким чином. Якщо ці фізичні елементи безпеки не використовувати належним чином, навіть найнепроникніші захисні засоби зрештою будуть зруйновані.

Конфіденційність у сфері фізичної безпеки часто тягне за собою компроміси з безпекою. Контроль доступу, спостереження, виявлення та оцінка, а також реагування – це принципи фізичного захисту, які вимагають точної ідентифікації, відстеження та моніторингу осіб під час перебування в охоронюваній зоні. Дозвіл цим системам фізичного захисту відстежувати кожен рух людини має бути пов’язаний із припущенням, що ця інформація буде використана лише за призначенням і захищена від будь-якого зловмисного використання чи несанкціонованого доступу. Однак угода про надання цієї інформації іншим довіреним особам для подальшого підвищення безпеки зазвичай чітко висловлюється.

1.2. Типи та поширення кіберфізичних систем

1.2.1. Властивості об’єктів IoT та класифікація кіберфізичних систем

Кіберфізичні системи це загальний термін, який включає системи багатьох видів, включаючи робототехніку, автоматику машин, автоматизовані системи управління (АСУ), системи управління процесами (СУП), системи диспетчерського контролю та збору даних (SCADA), промисловий Інтернет речей (IIoT) та Інтернет речей (IoT). Ці системи мають різні програми, архітектури та поведінку, але всі вони містять спільні ключові атрибути.

У звіті Національного консультативного комітету з питань науки і технологій президента США про IoT [8] зазначено три загальні властивості об’єктів IoT:

1. Звичайні об’єкти індивідуально адресуються в мережі.

2. Фізичні об’єкти взаємопов’язані.

3. Пристрої є інтелектуальними, і багато з них можуть виконувати функції адаптивно, окремо або як частина більшої групи.

Ці загальні властивості IoT широко застосовуються до КФС загалом. КФС може являти собою один об'єкт чи систему об'єктів з невизначеними межами та охоплювати широкий діапазон прикладних областей, надаючи можливість контролювати, маніпулювати та автоматизувати пристрої від особистих зручностей до критичної інфраструктури. Хоча ці системи дають нам змогу бути ефективнішими в масштабах, які виходять за межі наших індивідуальних можливостей, вони також становлять додатковий ризик.

Чим більше інтегрованих КФС стає в наше життя, тим більше шансів, що їх збій або маніпуляції можуть мати кардинальні наслідки. КФС є дуже загальним терміном у цій галузі.

Вбудована система — це старіший термін для обчислювальних можливостей, поєднаних із звичайними низькоінтелектуальними системами; однак вбудованим системам не потрібно спілкуватися одна з одною або з Інтернетом.

Промисловий Інтернет речей, у свою чергу, зазвичай відносять до АСУ та зв’язків типу «бізнес-бізнес», і не враховувють споживчі пристрої. І навпаки, IoT став найпопулярнішим терміном для КФС, але він здебільшого викликає зображення комерційних споживчих пристроїв. КФС використовується для позначення сукупності всіх цих систем.

Домен КФС поділяється на дві великі категорії: інфраструктурні та персональні. Хоча функціональні концепції КФС є узгодженими між двома категоріями, ризики та проблеми безпеки часто відрізняються.

Інфраструктурні КФС включають АСУ, які керують фабриками, нафтопереробними заводами та іншими типами промислової інфраструктури. Персональні КФС включають пристрої кінцевих користувачів, такі як смартфони, годинники, побутові прилади та домашні системи [9].

1.2.2. Інфраструктурні кіберфізичні системи

У промисловості повно інфраструктурних КФС, які є критичними для сучасного життя. В АСУ наголошується на фізичній стороні та додається кіберсторона для зручного доступу та керування фізичним обладнанням тощо. Однак точки з'єднання між обладнанням і зовнішніми комп'ютерними мережами можуть бути не задокументованими або погано зрозумілими, оскільки зв'язок часто розвивався протягом тривалого часу. періоди часу [10].

Деякі серйозні проблеми полягають у тому, щоб уникнути пошкодження майна, економічних збитків і фізичної шкоди. Однак для промислових систем, які є частиною критично важливих інфраструктур, що надають такі життєво важливі послуги, як електроенергія та вода, доступність є найважливішою проблемою, оскільки сучасні суспільства глибоко від них залежать. Прикладом може бути КФС для електроенергії, які відповідають критеріям NSTAC IoT, і є в багатьох галузях промисловості, включаючи нафту та газ, водопостачання та водовідведення, хімічну та промислову промисловість.

Інфраструктурні КФС використовуються для моніторингу кожної частини електричної мережі від виробництва електроенергії до передачі до споживання кінцевими користувачами та обліку споживаної електроенергії. Ці КФС повинні контролювати турбіни, лінії електропередач, трансформатори, фідери та інше критично важливе обладнання, яке розподілено по великих географічних регіонах [11].

Іноді АСУ розміщуються на віддалених опорах і підстанціях без безпосереднього нагляду людини. Їх розподілений характер ускладнює моніторинг КФС створюючи вразливі місця безпеки як у кібернетичному, так і у фізичному доменах.

В останнє десятиліття використання розумної енергосистеми все більше підштовхнуло до автоматизації більшості мережевих пристроїв у сфері енергетики, керуючись бажанням працювати з електромережами набагато ефективніше, зменшити навантаження на поточні системи та знизити вартість розгортання майбутніх систем. Розумні лічильники, системи домашнього

енергоменеджменту та інші розумні прилади обіцяють допомогти населенню краще розпоряджатися обмеженими енергетичними ресурсами. Однак взаємодія людини-оператора ускладнює захист цих систем, оскільки люди регулярно перетинають межі системи та можуть наражати конфіденційні дані та служби на непередбачені види ризику, створюючи додаткові вразливості, які зазвичай не враховуються. Завдяки інтелектуальній мережі інфраструктурний КФС може непомітно проникати в особистий простір, як-от будинки, і створювати ненавмисні ризики, включаючи втрату послуг, крадіжку енергії та втрату конфіденційності, завдяки аналізу життєвого циклу [12].

1.2.3. Персональні кіберфізичні системи

Персональні технології КФС мали на меті створити економічну цінність шляхом автоматизації рутинних завдань. У персональній КФС підкреслюється кіберсторона та додається фізичний вимір, щоб підвищити корисність інформаційної системи. Повсюдне поширення цих пристроїв може приховати їхні обчислювальні аспекти та небезпечні ризики. Ці системи часто зберігають конфіденційну персональну інформацію і можуть записувати деталі нашого особистого життя. Раніше для спостереження та вивчення закономірностей нашого життя потрібна була близька фізична близькість. Тепер ці пристрої можуть надавати можливість робити це з будь-якої точки світу через підключення до Інтернету. З цієї причини конфіденційність є головною проблемою персональних КФС. Однак безпека може бути першочерговою проблемою персональних медичних пристроїв, а конфіденційність — другорядною. Оскільки особиста КФС може мати довірчі відносини з офісними або промисловими системами та АСУ, то безпека є важливим питанням третього рівня [13].

КФС включають в себе побутову техніку, утиліти, які можна носити, новинки, іграшки, мітки для відстеження, медичні пристрої та безліч пристроїв, які входять у наше життя на особистому рівні під час підключення до широкого Інтернету. Удома часто є високошвидкісний доступ до Інтернету, перевагами

якого все частіше користуються інтелектуальні пристрої, щоб зробити свої послуги доступними для перегляду або он-лайн. Холодильники можуть замовляти продукти та повідомляти, коли їжа псується, телевізори вивчають улюблені станції та програми, і навіть лампочки можуть виявляти рух і контролювати стан будинку. Оскільки люди вдома регулярно користуються цими предметами, їх необхідно захистити, щоб уникнути витоку інформації, яка б дозволила проаналізувати життєві процеси. Витік інформації може призвести до небажаної уваги власника будинку з боку рекламодавців або опортуністичних злодіїв. Крім того, ці пристрої часто створюють для «телефонування додому» своїй материнській компанії або її філіям, передаючи потенційно конфіденційну інформацію за межі дому невідомим особам. Таким чином, персональні CPS можуть непомітно проникати в інфраструктурні та комерційні простори, забезпечуючи непомітний вплив зовнішніх організацій [14].

1.3. Безпека та конфіденційність у кіберфізичних системах

Взаємозв'язок КФС призводить до взаємозалежностей і системних взаємодій, які неочевидні навіть для ретельного огляду. Сама природа КФС надає шляхи як для кібератак, так і для фізичних атак, що значно розширює можливості супротивника. Окремі набори вразливостей на кібер- і фізичній стороні не просто складаються, вони множаться [15].

Наявність фізичного доступу до кіберсистеми робить можливими певні атаки, яких інакше не було б. Додавання мережевого кібервиміру до фізичної системи збільшує складність системи, збільшує масштаб того, що може бути атаковано, і відстань, з якої може бути здійснена атака. Окремі шляхи атаки можуть бути повністю захищені лише в одному чи іншому домені, але по-справжньому захищені лише ті частини системи, де обидва домени захищені одночасно. У той же час засоби захисту як кібернетичної, так і фізичної компоненти можуть використовуватися для захисту іншого компонента

більшою мірою, ніж чиста кібернетична чи фізична система. Наприклад, комп'ютеризовані датчики ковзання захищають водіїв від фізичної небезпеки ожеледі доріг.

Таким чином, додавання двох доменів значно ускладнює оцінку безпеки об'єднаної системи. Точки атаки на безпеку та конфіденційність у КФС можуть бути на інтерфейсах між пристроями, на самих пристроях, в інфраструктурі, яка їх підтримує, з Інтернету та навіть від зловмисних користувачів. Зловмисники можуть скористатися неоднозначністю вразливих протоколів зв'язку, щоб здійснити атаку через інтерфейс. Вони можуть використовувати недоліки безпеки в слабких реалізаціях інтерфейсів прикладного програмування, щоб скомпрометувати компонент. Крім того, вони можуть скористатися перевагами довірчих відносин між одноранговими пристроями або між пристроями та інфраструктурою, клієнтами та користувачами, з якими вони спілкуються. Кожна з цих точок вразливості має бути покрита захистом або розглядатися як потенційно скомпрометовані компоненти системи з точки зору інших компонентів [16].

Безпека та конфіденційність у КФС є складнішими, ніж здається. Доки системи не будуть проаналізовані комплексно, наслідки для безпеки та конфіденційності неможливо повністю зрозуміти. Частина складності КФС полягає в тому, що вони непомітно підключені до великої мережі яка, у свою чергу, може бути підключена до Інтернету. Обсяг обмежень безпеки та конфіденційності для пристрою може раптово стати глобальним. На основі вище зазначеного можна стверджувати, що безпека є однією із найважливіших характеристик, які необхідно забезпечувати при розробці та впроваджені КФС.

Подібно до того, як правильне розуміння безпеки в КФС вимагає розуміння як фізичного, так і кібердоменів так і їх взаємодії, конфіденційність у КФС є складнішою, ніж здається. Наслідки конфіденційності неможливо повністю зрозуміти без повного знання всієї системи та її зв'язків. Частина проблеми з КФС полягає в тому, що підключення до великих мереж або Інтернету неочевидні.

Споживачі дуже стурбовані даними, які про них збираються, і тим, як вони будуть використані. В епоху Інтернету речей дані збираються й потенційно передаються непомітно. Раніше дані потрібно було вручну вводити в комп'ютер. Тепер такі пристрої, як мобільні телефони, розумні пристрої, підключені автомобілі, підключені будинки та багато інших пристроїв збирають невідомі обсяги та типи інформації про людей, які часто не усвідомлюють, що ці пристрої взаємодіють через Інтернет. Люди, які розуміють, що їхні пристрої підключені до Інтернету, часто не розуміють наслідків для конфіденційності. Через ці з'єднання може витікати інформація, яка може бути передана, зібрана або викрадена без відома користувача [17].

Одним із таких шляхів витоку інформації є розумні пристрої які взаємодіють з пунктами збору даних в магазинах, ресторанах, уздовж автомагістралей або будь-де, де їх власник переміщується протягом дня, і зазвичай ці пункти збору інформації є неочевидними. Пункти збору можуть змусити пристрої поблизу розкрити свою особу та підключитися до Інтернету, використовуючи пункт збору як посередника. Одним із прикладів цього є симулятор активного стільникового зв'язку або пристрої-перехоплювачі Глобальної системи мобільного зв'язку. Засоби контролю, які регулюють збір і обмін даними, часто незрозумілі, і наслідки обміну можуть бути зрозумілі лише після того, як станеться витік даних [18].

Іншим шляхом витоку персональних даних користувачів може бути «розумна» побутова техніка. Такі пристрої, підключені до мережі, стають звичним явищем у домівках та офісах. Підключення цих пристроїв покликане полегшити життя споживачів шляхом автоматичного пристосування до їхніх моделей життя та надання додаткових зручностей. Підключені термостати можуть регулювати нагрівання та охолодження відповідно до кількості людей удома та очікуваного розкладу. Підключені холодильники можуть автоматично складати запаси продуктів і навіть замовляти основні продукти, коли їх кількість невелика. Голосова активація та присутність в Інтернеті можуть дозволити споживачам користуватися деякими приладами без використання

рук, навіть якщо вони знаходяться поза домом. Але знову ж таки, очікування щодо обміну зібраними даними є непослідовними, незрозумілими та можуть бути приховані глибоко в ліцензійній угоді кінцевого користувача (EULA), яку споживач ніколи не читає та не звертає на неї уваги [19]. Навіть у випадку, коли користувачі погоджувалися ділитися даними з компаніями, у середньому 48% із понад 2000 опитаних Ґрупманом та Етлінгером людей відчували дискомфорт від того, що компанії фактично використовують їхні дані, а 58% не влаштовували продаж цих даних [17]. Лише 20% учасників опитування вважали, що переваги їхніх інтелектуальних пристроїв переважують їхні проблеми з конфіденційністю.

Хоча індустрія поспішає зробити безліч пристроїв розумнішими, вони виявили, що додавання датчика до чогось чарівним чином не надає йому цінності для користувача, особливо якщо порівнювати його з потенційними ризиками. Враховуючи такий рівень дискомфорту, незрозуміло, чому люди взагалі погоджуються на передачу персональних даних.

Однак серед переваг, які роблять людей бажаючими збирати їхні дані, вони виявили, що рекламні акції з економією грошей, надання допомоги у прийнятті рішень, допомога з усунення несправностей та інформація про місцезнаходження є найбільш переконливими причинами, чому люди готові відмовитися від певної міри своєї конфіденційності. Їхні рекомендації включали забезпечення того, щоб споживачі були поінформовані про те, як, коли та з якою метою їхня інформація ділиться, і забезпечення того, щоб споживачі мали адекватні стимули для поширення [17].

РОЗДІЛ 2. АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ДЛЯ КІБЕРФІЗИЧНИХ СИСТЕМ

2.1. Механізми пошуку вразливостей у кіберфізичних системах

Системи диспетчерського контролю та збору даних (SCADA) є досить популярними для використання в промислових, комунальних і виробничих процесах. Хоча така технологія продовжує розвиватися в контексті КФС, виникають нові парадигми, такі як IoT та IIoT, загроза таких систем залишається відносно неясною, особливо з точки зору кібербезпеки. Різноманітні перешкоди заважають аналізу кібербезпеки таких систем, включаючи відсутність емпіричних даних та численні проблеми з логістикою, конфіденційністю та репутацією [20].

З врахування вище зазначеного, можна виділити кілька факторів що впливають на безпеку КФС:

- в ідеальній ситуації для захисту мережі КФС ізолюють від зовнішньої незахищеної мережі (наприклад, Інтернет), однак оскільки існує необхідність доступу до таких систем віддалено за допомогою зовнішніх пристроїв цей метод захисту не застосовують;
- при роботі обслуговуючого персоналу, консультантів та постачальників, які підключають свої пристрої до мережі КФС для різних цілей, створюються потенційні ризики для безпеки КФС [21]:
- для зниження вартості у мережах КФС здійснюється заміна оригінальних частин низькоякісним обладнанням, що призводить до погіршення захисту систем КФС та створенню безлічі нульових уразливостей [22, 23];
- модернізація розумних міст, взаємопов’язаних пристроїв та Інтернету речей збільшує вектор загроз проти систем SCADA.

За даними Групи реагування на надзвичайні ситуації в системі промислового управління (ICS-CERT) [24], групи з оцінки виявили сотні

вразливостей в архітектурних проектах КФС. А зростання кількості атак на КФС порівняно з 2016 роком пояснюється широким впровадженням технології IoT та IIoT.

Для визначення можливих вразливостей КФС використовують наступні механізми їх пошуку:

• розгортання розподілених моніторів SCADA, зазвичай honeypots, у різних країнах;

• аналіз і дослідження підозрілих комунікацій SCADA;

• вимірювання та підтвердження впливу таких заходів на SCADA.

Завдяки впровадженню таких механізмів та поширенню звітів їх діяльності неодноразово здійснене попередження кібератак та значно покращені інструменти реагування. Також, науковцям вдалося виділити дві категорії для подальшого дослідження. Однією з цих категорій є мережева розвідка, іншою – аналіз трафіку кіберфізичних систем [23].

2.1.1. Мережева розвідка

Кіберсканування або мережева розвідка викликає зростаюче занепокоєння в кібербезпеці через те, що це первинний етап спроби вторгнення, який дозволяє зловмиснику віддалено знаходити, націлюватися та згодом використовувати вразливі системи. Це в основному основна техніка та головний фасилітатор згаданих вище кібератак [25]. На рисунку 2.1 зображено анатомію кібератаки, де видно, що кіберсканування відіграє ключову роль.

Рисунок 2.1 – Анатомія кібератаки

Як бачимо з рисунку 2.1 кібератака містить наступні етапи:

- кіберсканування;
- підбір даних для проникнення;
- сама спроба проникнення;
- підвищення привілеїв для виконання зловмисних дій;
- виконання зловмисних дій;
- розгортання зловмисного програмного забезпечення або створення бекдору;
- видалення будь-яких згадок про проведену атаку.

Все починається з мережевої розвідки, оскільки зловмисники свої дії починають з дослідження цільової організації. Вони сканують IP-адреси, діапазони мереж, доменні імена та адреси електронної пошти всередині організації, наприклад IT-спеціалістів, фінансових та технічних директорів.

Після збору пакету даних достатнього для здійснення атаки відбувається саме проникнення. У випадку успішного проникнення в систему здійснюються різноманітні дії для отримання необхідних привілеїв в середині системи.

Якщо всі попередні завдання були успішно виконані зловмисники починають свою повномасштабну атаку. Цей крок може включати видалення або викрадення даних із системи, збій у роботі служби чи розміщення програмного забезпечення - вимагача.

Програми-вимагачі – це зловмисне програмне забезпечення, яке розповсюджується за допомогою зловмисного програмного забезпечення , яке шифрує дані жертви, а потім хакери вимагають викуп за оприлюднення даних, надаючи компанії код розблокування. У сучасному технологічному світі програми-вимагачі є основною причиною того, що компанії залишаються під загрозою пошкодження систем зловмисним програмним забезпеченням на основі шифрування.

Крок виконання зловмисних дій може включати в себе не тільки атаку на цільову систему або компанію, а і проникнення в усі системи, підключені до

мережі, що дозволяє зловмисникам ховатися в кількох системах і відновлювати доступ до мережі навіть після їх виявлення.

Досвідчені зловмисники витрачають час, щоб видалити докази своєї присутності в мережі та системах жертви. Вони очищають журнали, щоб видалити всю історію своєї присутності. Замітання слідів таким чином дозволяє їм втекти, а також, повторно проникнути в систему в майбутньому. Ведення журналів може допомогти організаціям виявити події безпеки та відновити послідовність атаки.

Оскільки кіберсканування є важливою темою для вимірювань кібербезпеки та Інтернету, вона є в центрі уваги в багатьох наукових працях.

У [25] автори провели опитування, у якому вони класифікували теми сканування на основі їх природи, стратегії та підходу.

Леонард та ін. у [26] виконали стохастичне виведення ряду співвідношень, щоб запропонувати оптимальну скануючу діяльність розподілу невидимості на основі ймовірності виявлення. Автори врахували точку зору зловмисників (а не точку зору вимірювання), щоб значно мінімізувати ймовірність виявлення.

У [27] і [28] автори вивчали зондування великої мережі кампусу, використовуючи дані netflow. Вони намагалися знайти різні стратегії дослідження та вивчити їх шкідливість. Вони проаналізували поведінку сканування, представивши поняття сірого IP-простору та методи виявлення потенційних сканерів. Прядкін та ін. в [29] провели емпіричну оцінку кіберпростору, щоб зробити висновок про зайнятість IP-адрес.

Крім того, [30] була однією з перших робіт з огляду периферійних хостів у загальнодоступному Інтернеті.

В [31] автори проаналізували масштабне сканування та представили кількісну нижню межу кількості вразливих вбудованих пристроїв у глобальному масштабі. А, в [32] автори проаналізували дані з великої темної мережі, що складається з 5,5 мільйонів адрес, щоб вивчити сканувальну діяльність у всьому Інтернеті. Вони виявили події сканування як великі

сплески, породжені унікальними джерелами. Крім того, у [33] було запропоновано гібридний підхід, заснований на аналізі часових рядів і покроковому хешуванні, викликаному контекстом, у застосуванні до пасивного набору даних Darknet для висновку, характеристики та кластерного сканування, націленого на протоколи КФС.

За останні кілька років спалахи зловмисних програм швидко поширилися серед уразливих систем. Фактично, були спалахи хробаків, які змогли просканувати та заразити 90% усіх уразливих кібер-хостів менш ніж за 10 хвилин. Крім того, останнім часом спостерігається розквіт кіберфеномену, який отримав назву кампанії кіберсканування. Це надзвичайно розповсюджені методи сканування, які володіють комплексними можливостями скритності та високою координацією. Замість того, щоб зосереджуватися на конкретних хостах або мережах, ці кампанії спрямовані на дослідження та, як наслідок, використання послуг та інфраструктури Інтернету. Отже, здатність виявляти та приписувати різну сканувальну діяльність є дуже важливим завданням, оскільки це запобігає фактичній кібератаці.

2.1.2. Моніторинг та аналіз трафіку у кіберфізичних системах

Для розуміння та оптимізації функціонування КФС важливою складовою є аналіз та моніторинг трафіку. Він допомагає виявляти залежності, покращувати продуктивність і забезпечувати надійність системи в цілому. При цьому програмне забезпечення для захисту КФС та антивірусне програмне забезпечення також використовує технологію моніторингу для виявлення потенційно шкідливих дій. Для перехоплення та запису мережевого трафіку, що проходить через мережеві інтерфейси використовуються спеціальні програми, які називаються сніферами (packet sniffers). Перехоплені дані включають в себе інформацію про передачу пакетів, включаючи джерело, призначення, протоколи, порти та вміст пакетів. Зазвичай при використанні моніторингу система відстежує кожну дію та миттєво сповіщає користувачів,

що знижує можливість зловмисників проникнути в систему та перейти до наступних кроків кібератаки.

Моніторинг і аналіз мережевого трафіку КФС можна умовно розділити на дві основні категорії, а саме пасивний та інтерактивний моніторинг.

Пасивний моніторинг працює шляхом перенастроювання мережі за допомогою дзеркала або порту монітора для копіювання пакетів трафіку, що надсилається між пристроями в мережі. Потім ці скопійовані пакети даних надсилаються на локальний або хмарний сервер для аналізу за допомогою глибокої перевірки пакетів (DPI), яка ідентифікує відповідні пакети та їх постачальника, модель, операційну систему та інші дані.

Проте пасивний моніторинг має певні недоліки, оскільки він працює шляхом перевірки трафіку, то не підходить для виявлення пристроїв, які рідко спілкуються (і, отже, рідко генерують трафік). Надлишкові пристрої, які зазвичай зустрічаються в мережах та обмінюються даними лише в ситуаціях відмов є одними з прикладів таких пристроїв.

Але навіть серед пристроїв, які часто генерують трафік, деякі все ще є проблематичними для пасивного моніторингу через їхні специфічні протоколи. Наприклад, Modbus, протокол, який широко використовується на пристроях BMS, зазвичай розкриває дуже мало про пристрої у своїх комунікаціях. Отже, хоча пасивний моніторинг може визначити, що пристрій Modbus є, наприклад, ліфтом, він може не мати змоги точно визначити його постачальника, мікропрограму чи інші деталі, які є ключовими для захисту цього ліфта та критичної функції, яку він виконує.

Тому для захисту даних часто застосовують так звані медові пастки - honeypot. Основна їх мета здаватися чимось, до чого зловмисники хочуть підключитися, щоб фахівці могли ідентифікувати потенційно шкідливий трафік у мережі та зібрати інформацію про методи атак та відвернути їх від справжніх цілей.

Перевага honeypot полягає в тому, що це пристрій, який зазвичай не використовується для нормальної роботи всередині організації, ніхто не

повинен передавати файли або підключатися до нього, чи отримувати з ним будь-які інші форми інтерактивності. Коли honeypot бачить інтерактивність, він знає, що це може бути щось підозріле, тому реєструює цю активність і попереджає адміністратора, повідомляючи йому, що вона була перевірена, і потенційний зловмисник, можливо, переглядає її. Це стає системою раннього попередження. Зловмисник досліджує пристрій, який насправді взагалі не повинен досліджуватися. Honeypot не обслуговує файли і не запускає програми, і він не робить нічого іншого, окрім як сидить та чекає, коли з'явиться потенційний зловмисник. Коли зловмисник відвідує honeypot, інформація про нього збирається.

З одного боку, honeypots є прикладом систем моніторингу на основі пасток із низьким або високим рівнем взаємодії. Перший КФС honeypot, відомий як проект SCADA HoneyNet, був розроблений і розгорнутий у 2004 році компанією Cisco Systems [34]. Digital Bond, компанія, яка спеціалізується на кібербезпеці КФС, розгорнула два приманки SCADA у 2006 році [35].

Випуск Conpot у 2013 році значно полегшив розгортання та керування приманками КФС [36]. Щоб оцінити силу даної приманки в обмані зловмисників, Sysman та інші у [37] ввів поняття «Індикатори обману», де досліджувалися деякі з найпопулярніших приманок із низькою та середньою взаємодією.

Індикатором обману є дія, виконана honeypot, яка може сповістити зловмисників про те, що вони взаємодіють із honeypot. Наприклад, Artillery [38] honeypot за замовчуванням блокує будь-які шкідливі дії, які намагаються з’єднатися зі службами, які вони емулюють. Тому таку приманку легко ідентифікувати лише завдяки дії за замовчуванням. Тому розгорнутий Conpot був ретельно налаштований, щоб обдурити зловмисників непомітно.

З іншого боку, з точки зору пасивного аналізу, такі методи включають вивчення трафіку мережевих екранів для створення статистичних даних і тенденцій, пов’язаних з різними передбачуваними проступками КФС.

Перше обмежене дослідження мережевого екрану, яке стосувалося безпеки протоколів КФС, було проведено в 2008 році командою Cymru [39]. Їхній звіт містив приблизну статистику сканувань, націлених на широко використовувані протоколи КФС, такі як протокол розподіленої мережі (DNP3) [40], Modbus [41] і Rockwell-encap [42].

У [43] автори запропонували багатоетапну систему виявлення атак на основі аналізу сигнатур атаки за допомогою КФС honeypot.

2.2. Відстеження вхідного сканування на основі honeypot

У роботі запропоновано модель КФС honeypot на основі мобільного пристрою, який відстежує вхідні дії зондування. На відміну від роботи, представленої в [43], запропонована модель представляє перше широкомасштабне експериментування розгортання та роботи специфічних для КФС атак шляхом використання існуючої приманки КФС, яка виконує важливу аналітику атак, націлених на служби КФС у темній мережі. На відміну від поточної практики, у цій роботі запропоновано створити широкомасштабну інфраструктуру honeynet для збору та контролю даних КФС з безлічі систем і конфігурацій. Хоча використання honeypots у задачах кібербезпеки, безумовно, не є новим, випадки їх використання, як правило, були випадковими, незалежними та не орієнтованими на КФС. Таким чином, пропонується систематичний та спільний підхід до збору даних КФС-приманок в Інтернет-масштабі поетапним способом.

Запропонована у роботі методологія складається з трьох етапів:

1) моніторинг даних, який включає збір даних;
2) аналітика даних, яка надає статистику та інформацію про зібрані дані;
3) підтвердження результату, яке доводить та підтверджує отримані результати.

Відстежувана діяльність в Інтернеті об’єднується в централізовану базу даних для аналізу та формування розуміння, а результати перевіряються за допомогою надійних наборів даних третьої сторони.

На рисунку 2.2 представлено огляд запропонованої моделі. На етапі моніторингу даних кожному хосту призначається загальнодоступна IP-адреса в Інтернеті, щоб привернути будь-яку несанкціоновану діяльність. Згодом використовується три типи датчиків, які працюють одночасно на вхідному трафіку.

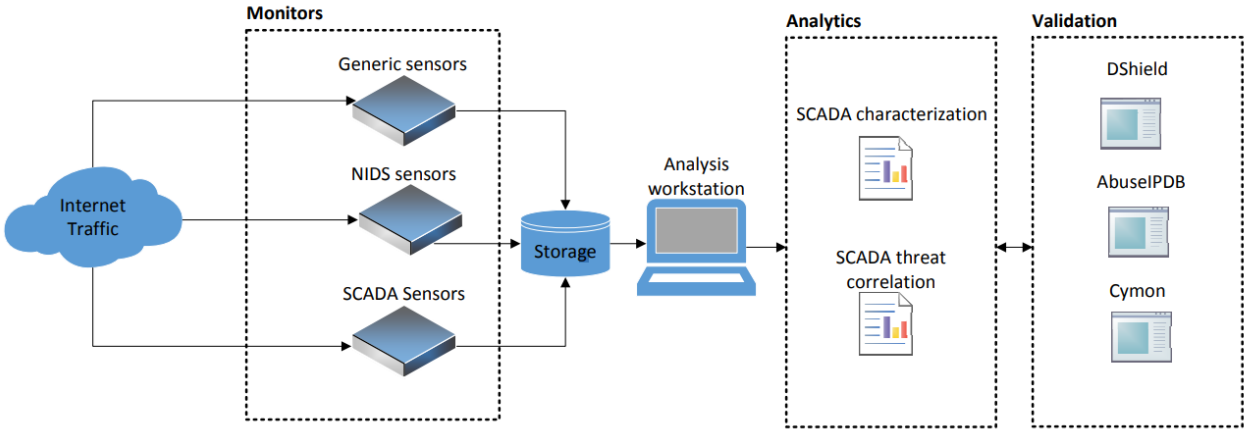


Рисунок 2.2 – Модель моніторингу даних

Зазначені датчики можуть бути кількох типів, перші з них, це **загальні датчики**, які налаштовані для збору даних із різних протоколів зв’язку, як SCADA, так і не-SCADA. Ці датчики спрямовані на збір усіх дій для дослідження мережі та допомогу в розрізненні випадкових і цілеспрямованих дій SCADA. Розгорнута інфраструктура імітує внутрішню динаміку систем КФС, де зовнішня точка огляду захищена базовою конфігурацією.

Датчики системи виявлення вторгнень у мережу (NIDS), які є мережевою системою виявлення вторгнень, використовуються для виявлення загроз, спрямованих як на загальні датчики, так і на датчики SCADA. Такі датчики дають більше інформації про намір зафіксованої мережевої активності. Запропоновано використовувати механізм Snort [44], відкритий NIDS, для виявлення та класифікації вторгнень.

Датчики SCADA, які є типовими приманками SCADA, налаштованими в інтерактивному режимі. Датчики SCADA налаштовані для моніторингу вхідного трафіку, орієнтованого на протоколи SCADA, а саме Modbus і протокол розподіленої мережі DNP3 відповідно до налаштувань за замовчуванням [21].

Було емульовано типову динаміку КФС (тобто керування та зв'язок), яку забезпечує Modbus на порту TCP 502 і Siemens на порту TCP 102. Також, варто зазначити, що honeypots було налаштовано з загальнодоступними IP-адресами, проте не було анонсовано публічно, щоб запобігти їх негайному використанню.

На етапі аналізу зібрані дані з датчиків надсилаються в нереляційну базу даних для подальшого аналізу. У цьому контексті використовується кілька інструментів з відкритим кодом (наприклад, whois [45]), щоб охарактеризувати діяльність SCADA та ідентифікувати країни, міста та назви автономних систем. Крім того, об'єднання на попередньому етапі дозволяє співвідносити дані загальних датчиків і датчиків NIDS з даними датчиків SCADA. Наприклад, визначити відсоток зв'язку SCADA порівняно з загальними зв'язками та типи загроз, пов'язаних із діяльністю SCADA.

Такі набори даних надають детальну інформацію про підозрілу діяльність в Інтернеті, наприклад типи загроз і репутацію IP-адрес.

2.3. Ефективність запропонованої системи відстеження вхідного сканування на основі honeypot

Ефективність запропонованої системи відстеження вхідного сканування на основі honeypot можна оцінити на основі даних зібраних із датчиків запропонованих для використання у моделі, які збирали інформацію про мережевий трафік та включає звичайні Інтернет-комунікації і діяльність SCADA а саме DShield [47], AbuseIPDB [48].] і Cymon [49]. Навіть якщо налаштовано загальнодоступний датчик SCADA дії зловмисників можуть бути націлені на служби SCADA на додаток до будь-яких інших послуг (портів),

доступних на цьому датчику. У режимі за замовчуванням датчик, емулює базовий хост SCADA.

На рисунку 2.3 згідно проведених розрахунків наведено огляд будь-яких дій в Інтернеті та мережевого трафіку, націлених на розгорнуті датчики.

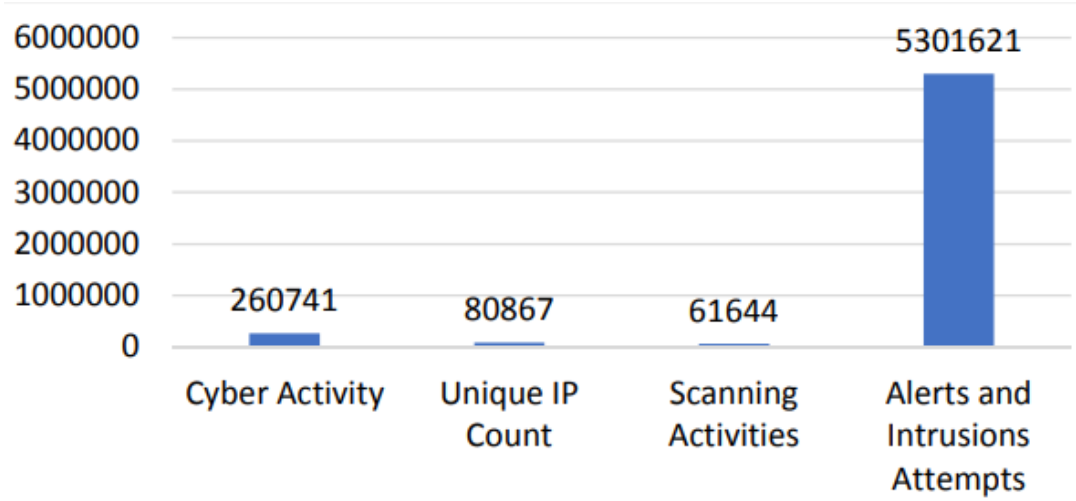


Рисунок 2.3 – Характеристика поведінки трафіку КФС

Отримані дані містили:

1) кількість ідентифікованих потоків, де потік визначається як набір пакетів, що надходять з однієї IP-адреси джерела на одну або кілька IP-адрес призначення;

2) загальну кількість унікальних IP-адрес;

3) загальну кількість дій сканування у всіх потоках;

4) сповіщення та вторгнення, пов’язані з цими потоками.

Кількість сповіщень і вторгнень, виявлених за допомогою мережевих систем моніторингу, є відносно високою через те, що одна IP-адреса джерела в межах потоку може створювати численні загрози на кількох датчиках.

Наступним кроком дослідження було проведення аналізу географічного розміщення пристроїв з яких було здійснено атаки.

На рисунку 2.4 наведено 10 найбільших країн-джерел, які ініціювали небажані кібер-активності, націлені на датчики.

Згідно рисунку 2.4 Сполучені Штати лідирують за обсягами діяльності, за ними йде Китай, потім Бразилія та Росія. Варто зазначити, що Сполучені Штати згенерували близько 44 500 потоків, що становить майже 38% світових лідерів. Варто відзначити дивовижну появу малих країн в Азії, таких як В'єтнам та Індонезія, які породили відносно велику кількість (майже 30%) діяльності.

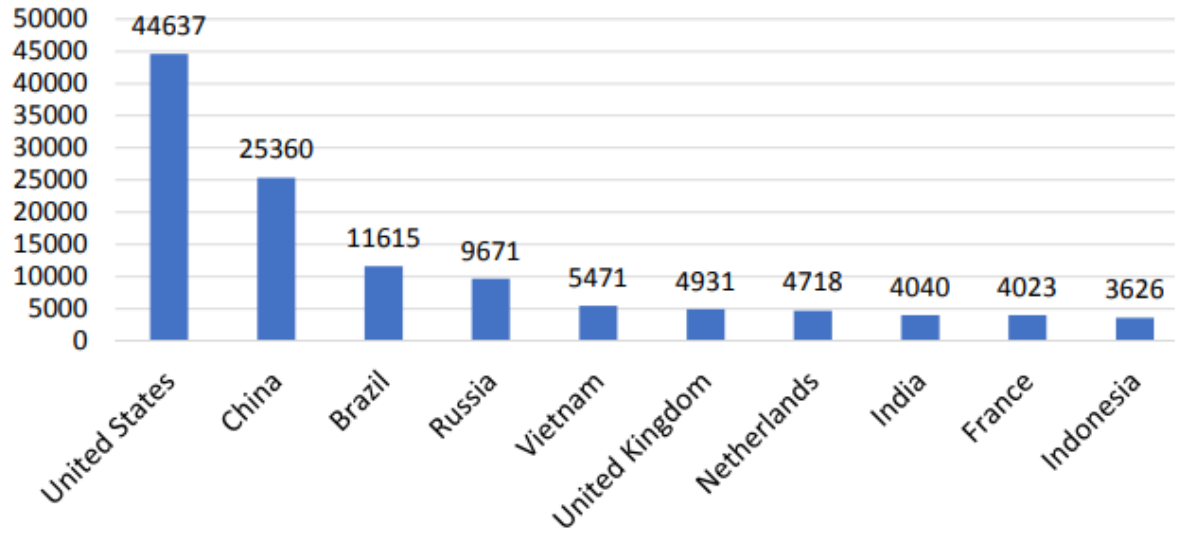


Рисунок 2.4 – 10 найбільших країн-джерел, які ініціювали небажані кібер-активності, націлені на датчики

Наступним кроком є класифікація мережевого трафіку на основі ініціюючих автономних систем (AS). Номер AS може унікально ідентифікувати постачальників послуг Інтернету (ISP).

На рисунку 2.5 перелічено 10 найпопулярніших номерів AS відповідно до трафіку, спрямованого на загальні датчики.

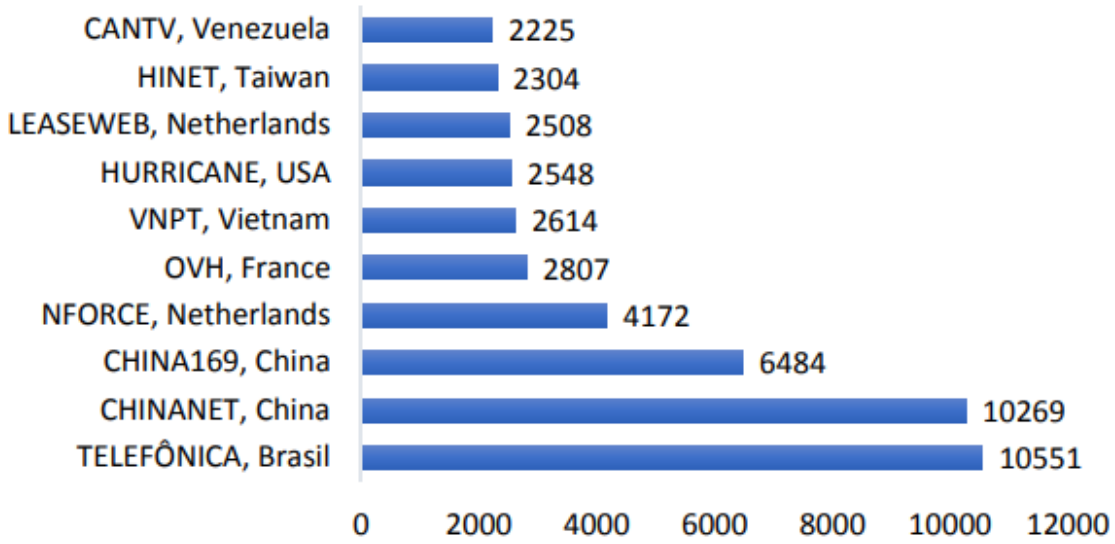


Рисунок 2.5 – Топ -10 джерел AS чисел

Варто зазначити, що, враховуючи, що Сполучені Штати вважаються країною з найбільшим обсягом інтернет-трафіку, однак, на основі класифікації AS, Бразилія визначена як найвища з 22,6% загального трафіку. Це означає, що більше мережевих потоків походить від одного номера AS у Бразилії порівняно зі Сполученими Штатами, де більше розподілених потоків походить від різних номерів AS. Варто відзначити, що китайські AS, які займають друге і третє місця, разом згенерували близько 35% трафіку провідних AS.

Із зазначеної статистики можна зробити висновок про поширені події кіберрозвідки, націлені на основні протоколи зв'язку та керування SCADA відповідно до розгортання датчиків. Використавши це розгортання, було ідентифіковано 54 511 кіберактивностей SCADA, в яких задіяно 1173 унікальні IP-адреси. Ця кількість дій становить майже 21% від загальної кількості 260 741 типових кіберподій, які були визначені раніше. Як показано на рисунку 2.6, майже половина (48,4%) найпопулярніших видів діяльності SCADA здійснюється в Сполучених Штатах.

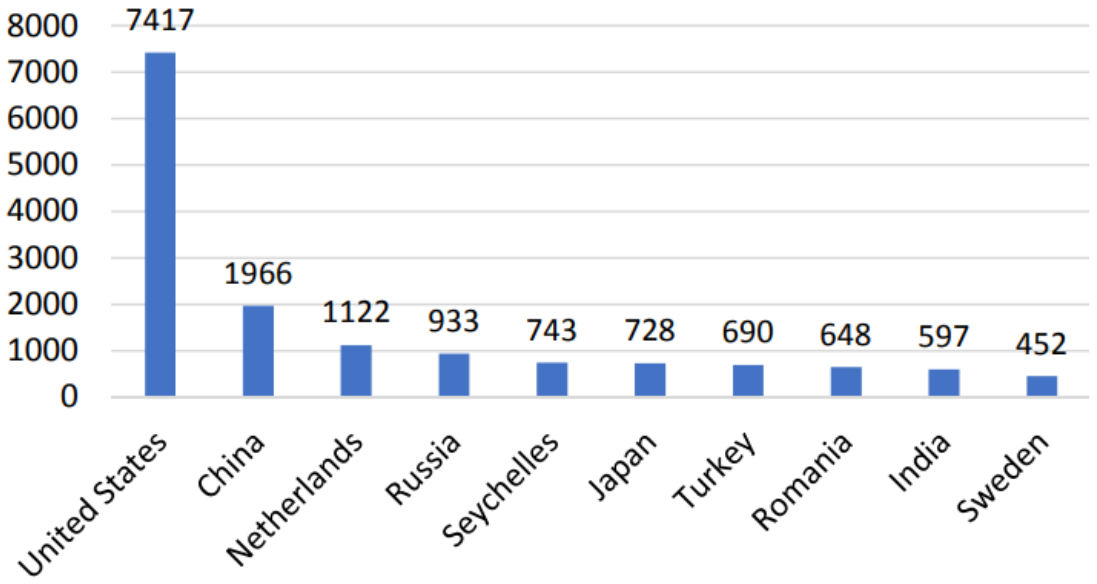


Рисунок 2.6 – Найбільші країни-джерела - діяльність SCADA

Крім того, згідно з представленням імен AS на рисунку 2.7, AS Сполучених Штатів домінують з CariNet у верхній частині списку.

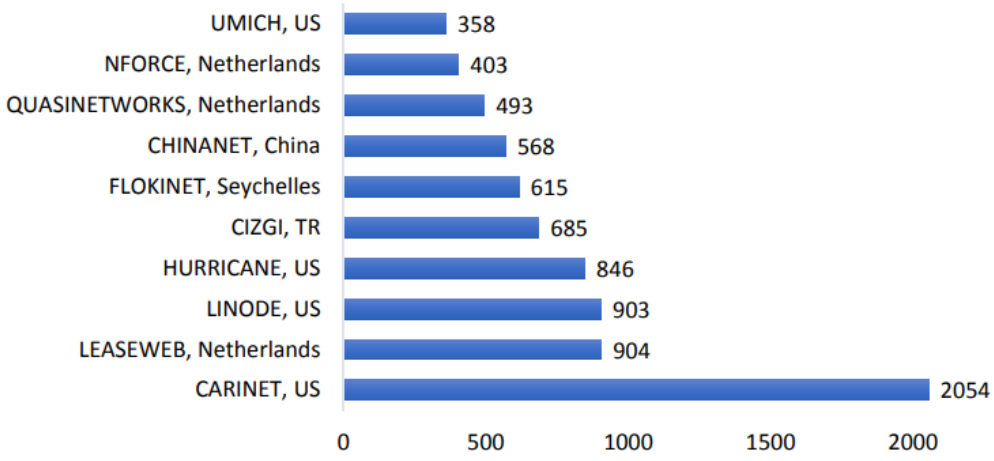


Рисунок 2.7 – Найпопулярніші імена AS джерел

У світлі даних відображених на рисунку 2.7 можна класифікувати події мережевого сканування на основі пов’язаних AS служб. Наприклад, що Сейшельські острови входять до п’ятірки кращих країн-джерел із 743 видами діяльності і серед багатьох інших островів, є хорошим місцем для зловмисників, які знаходять країни зі слабкою політикою кібербезпеки або де її

взагалі немає. Загалом, такі острови можна легко використати для ботнету, командно-контрольних серверів чи сховищ викраденої інформації.

Щоб оцінити загрозу таких дій SCADA, потрібно класифікувати трафік відповідно до таблиці 2.1.

Таблиця 2.1

Рейтинг серйозності мережевого сканування КФС

Тип активності	Рівень загрози
Сеанс	Середній
Запит/Відповідь	Високий
Трафік/З’єднання	Критичний

Запропонована класифікація, позначає рівень загрози мережі як середній, після створення сеансу, високий якщо генерується запит або відповідь, і критичний, якщо повідомлення передаються або обмінюються між розгорнутими моніторами та вихідними IP-адресами.

Оскільки датчики моніторингу встановлюються на невикористовуванні IP-адреси, будь-який трафік, націлений на них, вважається підозрілим і/або несанкціонованим або принаймні неправильно налаштованим. Згідно з вищезазначеним підходом, розслідування показало, що 13% кіберактивності SCADA мають середній рівень загрози, 64% – високий рівень та 23% – критичний рівень, що і показано на рисунку 2.8.

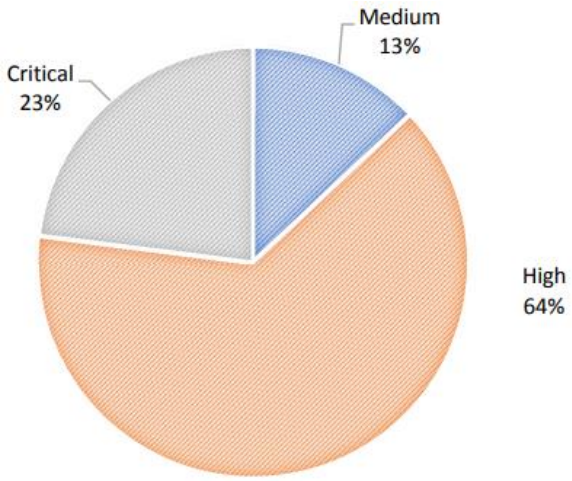


Рисунок 2.8 – Рівень загрози SCADA

Наступним кроком аналізу ефективності моделі буде визначення зв’язку за цільовими портами, які представляють конкретні керовані служби. На рисунку 2.9 показано розподіл запитів для тих, які мають критичний рівень загрози, тобто такі дії, які не просто перевіряли з’єднання або сеанс із розгорнутими моніторами, але також мали спільний доступ до даних після встановлення з’єднання.

Не дивно, що Modbus є найбільш (75%) послугою SCADA, яка зазнає критичних атак. Такий результат підтверджує результати досліджень науковців [33], які вже отримали подібні результати на основі аналізу датчиків пасивного моніторингу. Також важливо зазначити, що Modbus є найбільш широко використовуваною службою SCADA сьогодні. На додаток до S7comm і BACnet, які посіли друге і третє місце після Modbus відповідно, також було знайдено інтелектуальний інтерфейс управління платформою (IPMI), але з дуже мінімальною кількістю (загалом 4%).

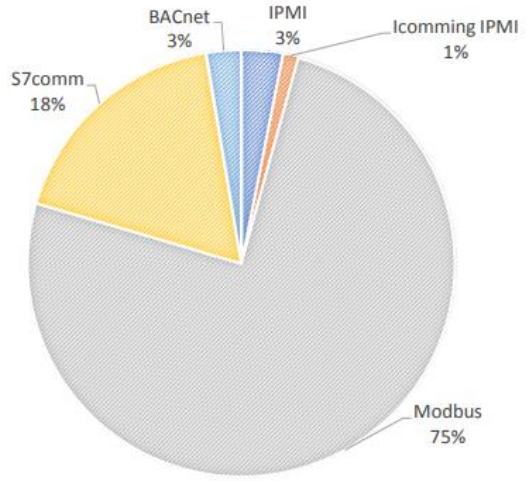


Рисунок 2.9 – Найбільш загрозливі служби SCADA

Застосування загальнодоступних онлайн баз даних, а саме DShield, AbuseIPDB і Cymon призводить до кращої перевірки отриманих результатів.

DShield — це система кореляції журналів брандмауера спільноти, яка зберігає записи про повідомлені підозрілі IP-адреси. Крім того, загальнодоступна база даних повертає шкалу ризику, цілеспрямовані атаки та загальну кількість підрахунків у звіті. DShield повідомляє про привидність повідомленої IP-адреси за шкалою від 0% (найнижча) до 100% (найвища). Як зазначалося раніше, ми перевірили вихідні IP-адреси мережевої комунікаційної діяльності SCADA. Аналіз показав, що 100% вихідних IP-адрес у всьому світі було знайдено в DShield із середньою шкалою ризику 53%. Серед високоризикованих зловмисних джерел зв'язку SCADA, де шкала ризику становила 90% або 100%, максимальна кількість атак становить 2946 і 53215 повідомлень. Загалом середня кількість атак на виявлені вихідні IP-адреси становить 1199, тоді як середня кількість зареєстрованих шкідливих IP-адрес становила 22 016. Резюме результатів DShield наведено в таблиці 2.2.

Щоб виміряти рівень достовірності виявлених дій SCADA, використовувався онлайн-репозиторій AbuseIPDB, який як повідомляють постачальники послуг і оператори магістральних мереж, індексує підозрілі IP-адреси масштабу Інтернету.

Таблиця 2.2

Резюме результатів

	Dshield			AbuseIPDB
	Масштаб ризику	Кількість атак	Кількість звітів	Рівень довіри
Мінімум	0 %	133	3000	15 %
Максимум	100 %	2946	65158	100 %
Середнє	53 %	1199	22016	67 %

Дослідження показало, що середній рівень впевненості зловживань у небажаній взаємодії становить 67,4%, при цьому максимальний рівень достовірності зловживань становить 100%, а мінімальний – 15%.

При спробі зіставити результати, отримані від AbuseIPDB, до DShield, було зауважено, що, незважаючи на високий масштаб джерела трафіку SCADA, рівень впевненості зловживань коливався від 15% до 57%. Це означає, що для цих IP-адрес у DShield зареєстровано випадки зловживання, про які не було повідомлено в AbuseIPDB. Щоб визначити тип активності мережевого трафіку, використовувався онлайн-репозиторій Cymon [29].

Cymon — це найбільший трекер з відкритим кодом шкідливого програмного забезпечення, ботнетів тощо. Згідно з висновками, 66,6% зловмисних дій були атаками на електронну пошту, а 50% - web-атаки, протокол доступу до Інтернет-повідомлень, атаки Secure Shell і атаки протоколу передачі файлів. На додаток до атак було виявлено 16,6% дій сканування, таких як атаки на службу доменних імен, спроби розкриття пароля, сканування telnet і сканування протоколу віддаленого робочого столу.

Враховуючи все вище сказане, можна зазначити, що більшість атак на кіберфізичні системи здійснюється з IP адрес, що не належать до самої структури мережі, тому розробка аналізатора мережевого трафіку із застосуванням білого списку доступу та суворий контроль до нього дасть змогу уникнути значної частини кібератак та забезпечити ефективну роботу кіберфізичних систем.

РОЗДІЛ 3. РОЗРОБКА СНІФЕРА ДЛЯ АНАЛІЗУ ТА БЛОКУВАННЯ НЕБАЖАНОГО ТРАФІКУ

3.1 Основні завдання та принципи функціонування сніферів пакетів

Розробка програмного забезпечення, яке б мало можливість відстежувати та перевіряти/аналізувати численні дані, що передаються через комп'ютерну мережу, є одним із способів вирішення проблеми систем моніторингу. Програмне забезпечення зробить доступною можливість захоплення даних у формі формалізованого блоку даних, відомого як пакет. Зібрані дані у двійковому форматі відображаються у такому вигляді, який дає змогу мережевим адміністраторам або фахівцям із безпеки контролювати інформацію.

Сніффер пакетів, також відомий як аналізатор пакетів/аналізатор протоколів/аналізатор мережі, є одним із таких рішень, яке має здатність фіксувати дані, що передаються через мережу, перетворювати їх у читабельний формат і зчитувати вміст даних. Відомо, що він має багато різноманітних застосувань, оскільки сніффер пакетів може законно використовуватися мережевим або системним адміністратором для моніторингу та усунення несправностей мережевого трафіку [49].

Це також важливий інструмент для виявлення зловмисників у мережі. Він відіграє важливу роль у захисті мережевих систем, вирішенні проблем, що виникають у мережі, і виявленні несумісних з'єднань. Сніффер пакетів є одним з інструментів, який використовується для моніторингу, перехоплення та декодування пакетів даних під час їх передачі через мережі.

Сніффер пакетів у сучасному світі має кілька важливих застосувань, які більшість експертів з безпеки використовують, щоб зробити мережу безпечною для передачі даних, не турбуючись про атаку. Він використовується для моніторингу та фільтрації мережевого трафіку та є ефективним інструментом для тестування протоколів, діагностики мережевих проблем, виявлення

проблем конфігурації. Команди інформаційних технологій покладаються на сніфери пакетів, щоб виявити будь-яке зловживання мережею, а також вирішити проблеми з вузькими місцями. У системі моніторингу вторгнень сніфери пакетів відіграють життєво важливу роль, оскільки моніторинг даних здійснюється перед виявленням і запобіганням підозрілій або зловмисній діяльності.

На основі досліджень проведених у другому розділі можна сказати, що більшість загроз для КФС становлять кібератаки з невідомих IP-адрес. Тому розробка сніфера, що аналізуватиме трафік та блокуватиме доступ з адрес які не знаходяться в білому списку дасть можливість значно підвищити захист та стійкість таких систем.

Кожна машина в мережі має власну апаратну адресу, яка відрізняється від іншої. Коли дані надсилаються через мережу, вони надсилаються у формі пакетів. Ці пакети являють собою фрагменти даних, які спрямовуються до певної призначеної системи, але вони проходитимуть через деякі вузли в мережі. Зазвичай конкретна система в мережі призначена для отримання та читання лише тих даних, які призначені для неї, тому з цієї причини мережева інтерфейсна плата (NIC) працює в нерозбірливому режимі та нерозбірливому режимі. Коли мережевий адаптер отримує пакет, він спочатку порівнює адресу призначення пакета зі своєю власною. Якщо MAC-адреса збігається, пакет приймається, інакше фільтрується. Цей режим роботи, коли мережева карта відкидає всі пакети, які не містять її власної MAC-адреси, називається режимом non promiscuous, що в основному означає, що кожна мережна карта читає лише кадри, призначені для неї. Таким чином, аналізатор пакетів перехоплює пакети, встановлюючи плату NIC своєї системи в безладний режим, і коли пакет надходить до NIC, він копіюється в пам’ять драйвера пристрою, а потім передається в ядро.

Сніффер пакетів – це програма, що працює в мережевому пристрої, яка пасивно отримує всі кадри канального рівня, що проходять через мережевий адаптер пристрою [50]. Використовуючи інформацію, отриману сніфером

пакетів, адміністратор може ідентифікувати помилкові пакети та використовувати зібрані дані для виявлення вузьких місць і підтримки ефективної передачі даних у мережі. Дані, адресовані іншим машинам, можна отримувати за допомогою аналізатора пакетів, на відміну від стандартних мережевих хостів, які отримують трафік, надісланий саме їм. Раніше було відомо, що аналізатори пакетів були дуже дорогими спеціальними апаратними пристроями, але нові досягнення в технології дозволили розробити програмні мережеві аналізатори, що робить їх більш зручними та доступними.

Сніфери пакетів можуть бути автономним апаратним пристроєм зі спеціальним програмним забезпеченням або просто програмним забезпеченням, яке можна встановити на комп'ютерній системі [51]. Вони доступні як безкоштовно, так і комерційно, з великою різницею залежно від таких функцій, як кількість підтримуваних протоколів, які можна декодувати, інтерфейс користувача та статистичні можливості. Зазвичай, сніффер пакетів це поєднання апаратного та програмного забезпечення.

Аналіз мережі може бути проведений як на користь, так і на шкоду мережі, тому сніфери пакетів, які є інструментами, і, як і всі інші інструменти, можуть використовуватися для виконання цих зловмисних дій. При використанні зловмисниками сніфери можуть представляти значну загрозу безпеці мережі [52]. І навпаки, сніфери пакетів можна використовувати в тестуванні на проникнення, яке було визначено як законна та дозволена спроба знайти та успішно використовувати комп'ютерні системи з метою підвищення безпеки систем від зловмисних атак/загроз. Відомо, що тестування на проникнення визначає, як система реагує на атаку та чи може бути зламаний захист системи і яку інформацію можна отримати в результаті тестування. Пасивний характер аналізатора пакетів ускладнює їх виявлення в мережі.

Як програма, аналізатор пакетів працює в мережевому пристрої, який пасивно отримує всі кадри канального рівня, що проходять через мережевий адаптер пристрою. Сніффер пакетів, як зазначено, фіксує дані, адресовані іншим машинам, зберігаючи їх для подальшого аналізу. Протягом багатьох

років було враховано декілька підходів, щоб визначити найкращий спосіб відстеження мережі. Метод перехоплення пакетів є одним із таких способів і використовувався кількома способами. Існують різні типи інструментів мережевого аналізу залежно від мережі, програми чи протоколів, доступних на ринках. Розглянемо основні та найбільш корисні аналізатори пакетів.

Wireshark Джеральда Комбса — це аналізатор пакетів, який використовується для пошуку та аналізу мережевих проблем. Спочатку названий Ethereal, у травні 2006 року проект був перейменований на Wireshark через проблеми з торговою маркою. Він є кросплатформним, використовує pcap для захоплення пакетів і працює на різних Unix-подібних операційних системах, Solaris і Microsoft Windows. Це дозволяє користувачеві перевести мережеві інтерфейси, які підтримують безладний режим, у цей режим, щоб бачити весь трафік, видимий на цьому інтерфейсі, а не лише трафік, адресований одній із налаштованих адрес інтерфейсу, і широкомовний/багатоадресний трафік [53].

Wireshark — це програмне забезпечення, яке «розуміє» структуру різних мережевих протоколів. Таким чином, він здатний відображати інкапсуляцію та поля разом із їхніми значеннями різних пакетів, визначених різними мережевими протоколами. Він надає користувачам можливість перехоплювати пакети, що проходять по всій мережі на певному інтерфейсі в певний час. Однак wireshark має обмеження щодо не повідомляти про деякі зловмисні наміри, здійснені в мережі [54].

Tcpdump від McCanne, Leres and Jacobson — це звичайний аналізатор пакетів, який запускається в командному рядку. Це дозволяє користувачеві перехоплювати та відображати TCP/IP та інші пакети, що передаються чи приймаються через мережу, до якої підключено комп’ютер. Він працює на більшості Unix-подібних операційних систем: Linux, Solaris, BSD і Mac OS. У цих системах tcpdump використовує бібліотеку libpcap для захоплення пакетів. Порт tcpdump для Windows називається WinDump і використовує WinPcap — порт libpcap для Windows. Він аналізує поведінку мережі, продуктивність і

програми, які генерують або отримують мережевий трафік. Його також можна використовувати для аналізу самої мережевої інфраструктури, визначаючи, чи вся необхідна маршрутизація виконується належним чином, що дозволяє користувачеві додатково ізолювати джерело проблеми. Також можна використовувати tcpdump для певних цілей перехоплення та відображення повідомлень іншого користувача чи комп'ютера [55].

Capsa — це мережевий аналізатор для LAN і WLAN, який виконує захоплення пакетів у реальному часі, цілодобовий моніторинг мережі, розширений аналіз протоколів, поглиблене декодування пакетів і автоматичну експертну діагностику. Він забезпечує повну видимість високого рівня для всієї вашої мережі, допомагає мережевим адміністраторам або мережевим інженерам швидко визначати та вирішувати різноманітні проблеми додатків, а отже покращує роботу кінцевого користувача та гарантує продуктивне мережеве середовище. Він може ідентифікувати та аналізувати понад 300 мережевих протоколів, а також мережеві додатки на основі протоколів [54].

Таблиця 3.1

Порівняння характеристик TCPdump, Wireshark, Capsa та EtherApe

№ з\п	Властивості	Wireshark	TCPDump	Capsa	EtherApe
1.	Підтримка ОС	Windows, Unix	Unix	Windows	Unix
2.	Використання диска	81MB Windows та 449MB Unix	448 KB	32 MB	
3.	Форма поширення	Безкоштовно	Безкоштовно	Платно	Безкоштовно
4.	Відкритий код	+	+	-	+
5.	Відображення протоколу в структурі рівня OSI	+	-	+	+
6.	Використання Libpcap	+	+	+	+
7.	Користувацький інтерфейс	GUI/CLI	CLI	GUI	GUI

Поширеними типами використовуваних методів перехоплення є перехоплення на основі IP-адреси, перехоплення на основі MAC-адреси та перехоплення на основі ARP, яке не переводить мережевий адаптер у безладний режим. Це ефективний метод для перехоплення даних в комутаційному середовищі [54].

Кілька факторів або параметрів впливають на продуктивність перехоплення пакетів. Розмір пакета є одним із таких факторів, але немає правильної відповіді на питання, який розмір пакета забезпечує найкращу продуктивність [56]. Відомо, що короткі пакети збільшують навантаження на пристрої, тоді як довгі пакети збільшують навантаження на мережу, тобто чим менше довгих пакетів, тим менше навантаження на мережу. Довгі пакети означають високе співвідношення корисного навантаження та заголовків пакетів. Інструменти, які підтримують максимум пакетів середнього розміру, є кращим інструментом у цьому тесті. Крім того, пропускна здатність означає кількість даних, які система обробляє в бітах на секунду (біт/с). Таким чином, інструмент із вищою пропускною спроможністю забезпечить кращу продуктивність, але інструменти з великим діапазоном швидких змін пропускної здатності призводять до випадкових змін пропускної здатності, що погано впливає на продуктивність мережі. З іншого боку, інструменти з діапазоном у шаблоні хороші для мережі та демонструють узгоджену поведінку [57].

Іншими показниками продуктивності є швидкість відкидання пакетів і час відповіді. Причини надмірної втрати пакетів можуть бути пов’язані з відсутністю буфера, тому всі пакети, що надходять до мережевого адаптера, не можуть бути збережені. Однак час відповіді — це час, необхідний для отримання підтвердження між взаємодіючими вузлами. Менший час відповіді означає меншу кількість повторних передач, а менший час відповіді означає кращу продуктивність. Багато мережевих адміністраторів витрачають багато часу, намагаючись дізнатися, що погіршує продуктивність їхньої мережі. Типовим рішенням проблеми перевантажень може бути оновлення мережевої

інфраструктури, тобто заміна серверів на високоякісні сервери та збільшення пропускної здатності. Однак це рішення є дорогим, короткостроковим і не повністю масштабованим, оскільки після виконання оновлення; Проблема перевантаження на деякий час покращується, а пізніше поступово погіршуватиметься, коли користувачі змінять свою поведінку у відповідь на оновлення.

Альтернативним рішенням цієї проблеми є розгортання масштабованої системи моніторингу та аналізу мережевого трафіку, щоб чітко розуміти динаміку трафіку та зміни в Інтернеті разом із загальною стабільністю мережі.

На додаток до знання працездатності мережі, моніторинг мережевої активності також має переваги виявлення атак відмови в обслуговуванні (DoS) і крадіжки пропускної здатності. Щоб провести аналіз широкого діапазону поведінки мережі, необхідно збирати мережевий трафік на безперервній основі, а не як одноразову подію, яка фіксує лише тимчасову поведінку, що дає змогу зрозуміти проблеми мережі. Збір довгострокових даних про мережевий трафік надасть цінну інформацію для покращення та розуміння фактичної динаміки мережі [58].

3.2 Алгоритм аналізу трафіку та оцінка його ефективності

На основі проведених досліджень можна запропонувати алгоритм захисту даних, який міститиме кілька основних кроків, розділених на два основних фрагменти, а саме аналіз трафіку за допомогою сніфера пакетів та формування білого списку, що відповідатиме за доступ до системи. Алгоритм роботи запропонованого сніферу пакетів представлено у вигляді діаграм потоків даних, а його робота не впливає на мережевий трафік та не вноситиме жодних змін у будь-які пакети, а лише копіюватиме та аналізуватиме їх. Для візуалізації процесу обробки даних та представлення самих потоків необхідно побудувати діаграми потоків даних, що дозволить ілюструвати рух між пристроями при обміні даних.

На діаграмі потоку даних 0 рівня (рис. 3.1) вхідні дані це пакети, що переміщуються через мережевий інтерфейс, у якому налаштовано безладний режим, а виходом є інформація, що міститься в пакетах у формі, зрозумілій для людини.

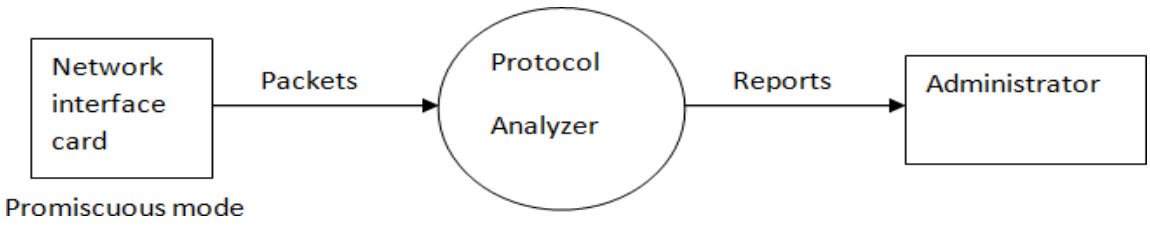


Рисунок 3.1 – DFD 0 рівня

На рисунку 3.2 представлено діаграму потоку даних 1 рівня для аналізатора потоків.

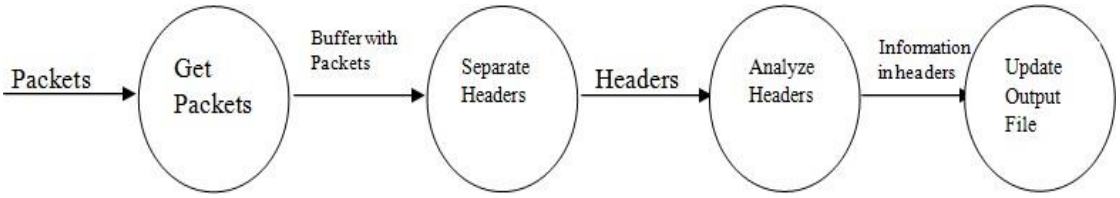


Рисунок 3.2 – DFD 1 рівня

На рисунку 3.3 представлено схему потоку даних 2 рівня для аналізатора потоків.

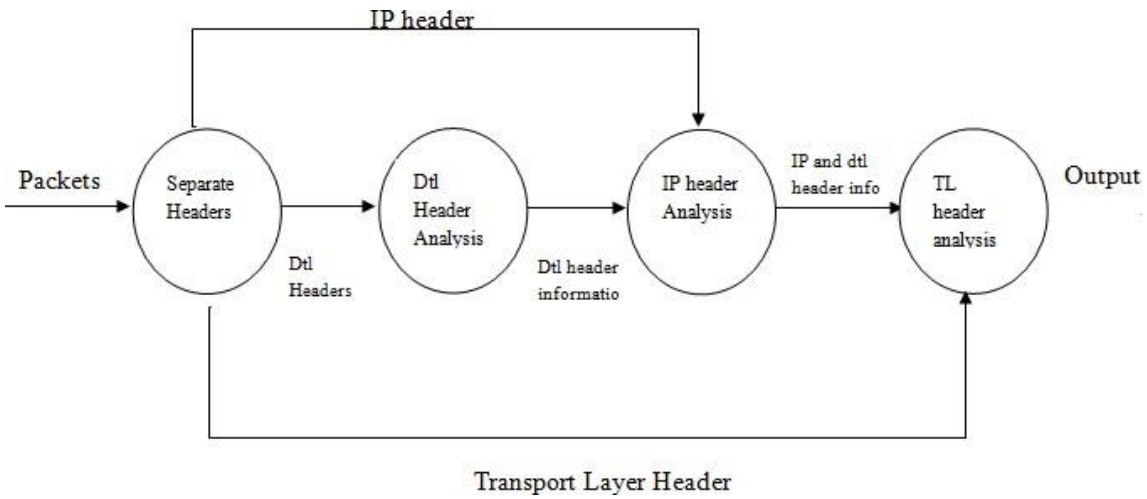


Рисунок 3.3 – DFD 2 рівня

Діаграми потоків даних 1 та 2 рівня (рис 3.2 та 3.3) охоплюють весь процес. Вхідні дані отримуються як пакети з мережевого інтерфейсу за допомогою процесу «Get packets». Для здійснення цього процесу визначається пакетний сокет, а необроблені пакети отримуються з мережевого інтерфейсу та зберігаються в буфері. Буфер, який зараз містить пакети, передається до процесу «separate header», який відділяє різні заголовки пакета в заголовок Інтернет-протоколу (IP) і заголовок протоколу керування передачею (TCP) і передає їх процесу «analyze headers», де вони аналізуються, а інформація передається до процесу «update output file». Тут вихідний файл буде оновлено останньою інформацією, отриманою з пізніших процесів.

Діаграми варіантів використання моделюють функціональність системи та варіанти використання. Вони описують послідовність дій, які надають користувачу вимірну цінність, і малюється як горизонтальний еліпс. Користувач — це особа, організація або зовнішня система, яка відіграє певну роль в одній або кількох взаємодіях із системою.

Діаграма варіантів використання запропонованого програмного забезпечення наведена на рисунку 3.4. Для наведеної вище діаграми варіантів використання в сценарії система спочатку ініціюється, щоб розпочати моніторинг. Потім користувач починає захоплювати пакети. Система отримує заголовок пакета та пакетні дані, зберігає та відкриває пакетні дані. При потребі користувач зупиняє перехоплення.

Алгоритм контролю доступу на основі білого списку міститиме наступні кроки:

1. Адміністратор системи формує початковий список користувачів, яким потрібно надати доступ до системи;
2. При спробі доступу до системи ззовні IP адреса користувача буде передаватися на перевірку;
3. У випадку коли IP адреса користувача присутня в списку йому надається доступ до мережі, в іншому випадку запит відхиляється.

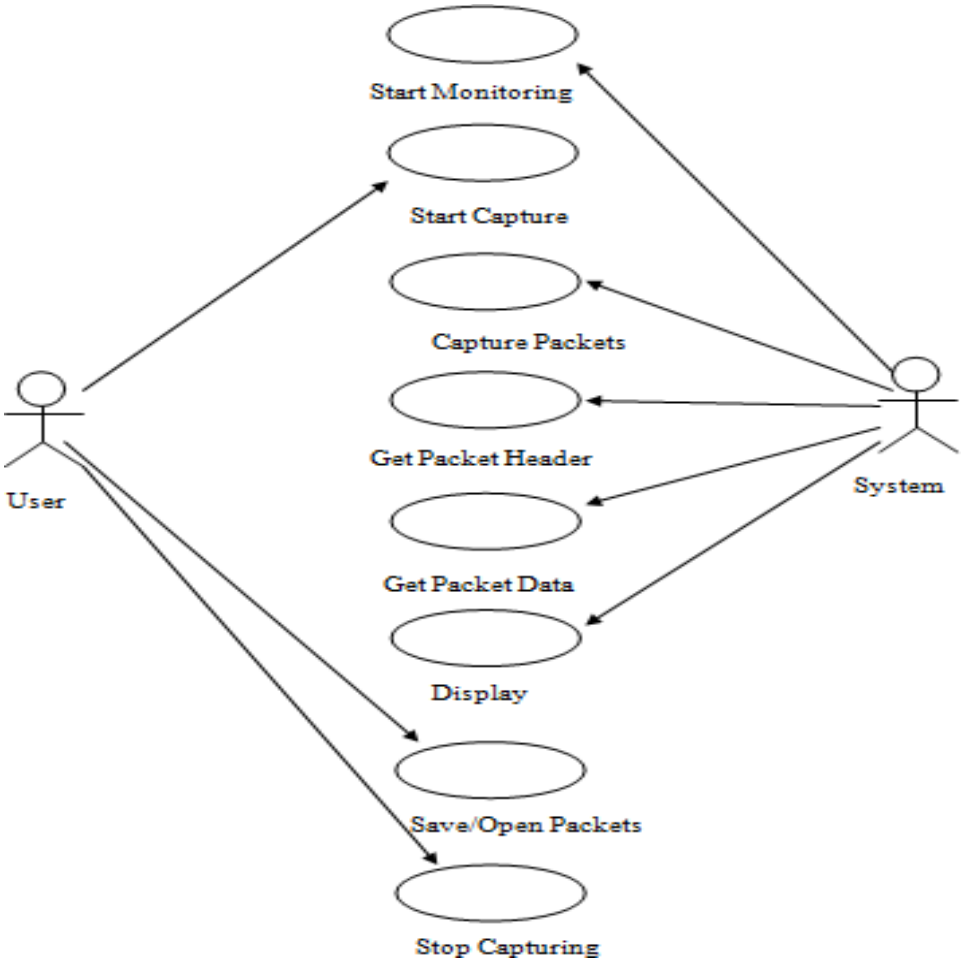


Рисунок 3.4 – Діаграма застосування пакетного сніфера

Одним із параметрів для оцінки продуктивності є обчислення втрати пакетів, яка виникає, коли один або більше пакетів даних, що переміщуються через комп'ютерну мережу, не досягають місця призначення. Втрата пакетів у розмірі 0,1% у протоколах TCP/IP зазвичай допускається, оскільки 1 втрачений пакет на кожні 1000 пакетів є прийнятним. Однак очікується, що все, що вище, матиме негативний вплив і потребує вирішення. За визначенням з [49] коефіцієнт втрати пакетів L розраховується як:

$$L = \frac{n_l}{n_l + n_s}, \tag{3.1}$$

де n_l – кількість втрачених пакетів, а n_s – кількість успішно доставлених.

Пропускна здатність визначається як кількість даних, які система обробляє, або кількість бітів на секунду (біт/с).

Традиційно визначається як відношення кількості переданих даних до часу, необхідного для їх передачі. З огляду на те, що дані успішно отримані, загальна формула пропускної здатності *T* подається як:

$$T = \frac{D}{t}, \tag{3.2}$$

де *D* – отримані дані, а *t* – час передачі.

Теоретична пропускна здатність розраховується на одного користувача, щоб не було колізій в мережі. Якщо взяти розмір даних D = 1498 байтів (1478 корисного навантаження UDP і заголовка UDP плюс 20 байт заголовка IP), то загальну формулу (3,2) пропускної здатності можна використовувати для розрахунку теоретичної пропускної здатності:

$$T = \frac{D}{t} = \frac{1498 \text{ x } 8 \text{ біт}}{t}. \tag{3.3}$$

Проте існує зв’язок між двома властивостями - коефіцієнтом втрат пакетів та пропускною здатністю. Це співвідношення можна розрахувати наступним чином – представимо формулу 3.1 у наступному вигляді:

$$L = \frac{n-n_s}{n}, \tag{3.4}$$

де *n* – загальна кількість пакетів.

Розділивши обидна значення на *n* отримаємо:

$$L = 1 - \frac{n_s}{n}. \tag{3.5}$$

Відповідно, пропускну здатність (формула 3.2) на основі кількості отриманих пакетів можна представити в наступному вигляді:

$$B = \frac{n_s}{t}. \quad (3.6)$$

А з урахування формули (3.5) n_s можна представити як:

$$n_s = n * (1 - L) \quad (3.7)$$

Підставивши значення формули (3.7) у (3.8) отримаємо:

$$B = \frac{n*(1-L)}{t} = \frac{n}{t}(1 - L). \quad (3.6)$$

де, $\frac{n}{t}$ – швидкість передачі даних, а $(1 - L)$ – співвідношення не втрачених пакетів.

Виходячи з вище зазначеного можна сказати, що пропускна здатність залежить від двох незалежних значень, а саме швидкості передачі даних та співвідношення не втрачених пакетів.

3.3 Практична реалізація сніфера пакетів

Як зазначалося раніше, для реалізації компонентів представлених у діаграмах потоків даних необхідно виконати їх практичну реалізацію. Мовою програмування для реалізації цієї ідеї була обрана інтерпретована об'єктно-орієнтована мова програмування високого рівня Python. Дана мова програмування використовується в багатьох областях досліджень, оскільки містить тисячі сторонніх модулів, що робить її ідеальною для написання різних скриптів та швидкої розробки програм.

Для реалізації проекту необхідно інсталювати відповідні модулі. Для цього ми спочатку переходимо у відповідну директорію та перевіряємо вже про інстальовані модулі (рис. 3.5).

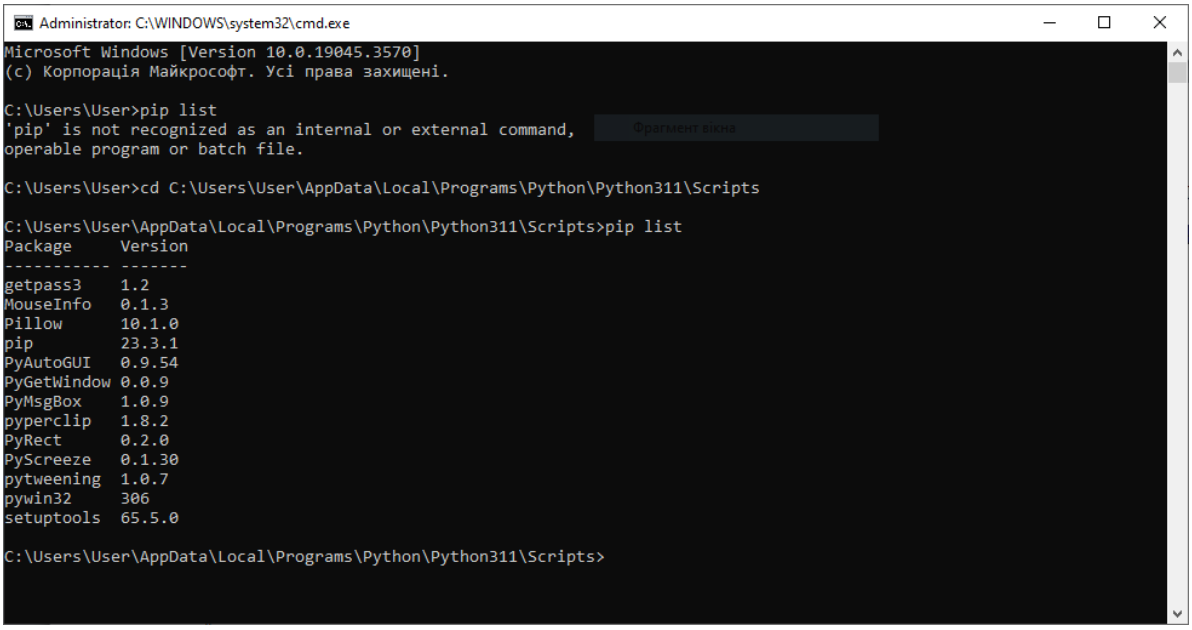


Рисунок 3.4 – Поточні модулі Python

Наступним кроком є інсталяція модулів, що необхідні в розробці проекту, а саме:

- NumPy – який додає підтримку великих багатовимірних масивів і матриць та дає змогу виконувати численні обчислення за допомогою Python (рис 3.5).

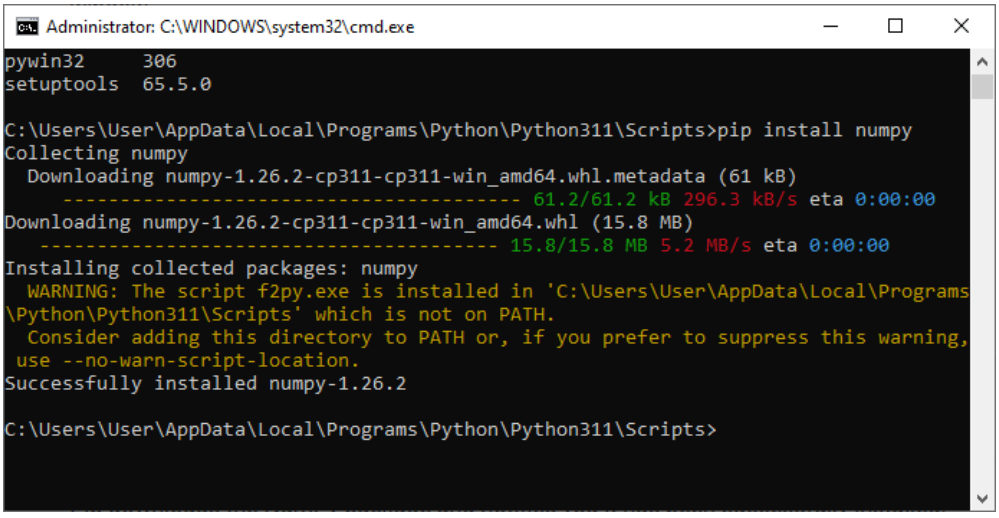


Рисунок 3.5 – Інсталяція NumPy

- Impacket — це набір класів Python для роботи з мережевими протоколами. Impacket зосереджений на забезпеченні низькорівневого програмного доступу до пакетів, а для деяких протоколів (наприклад, SMB1-3 і

MSRPC) на саму реалізацію протоколу. Пакети можна створювати з нуля, а також аналізувати з необроблених даних, а об'єктно-орієнтований API спрощує роботу з глибокими ієрархіями протоколів (рис 3.6).

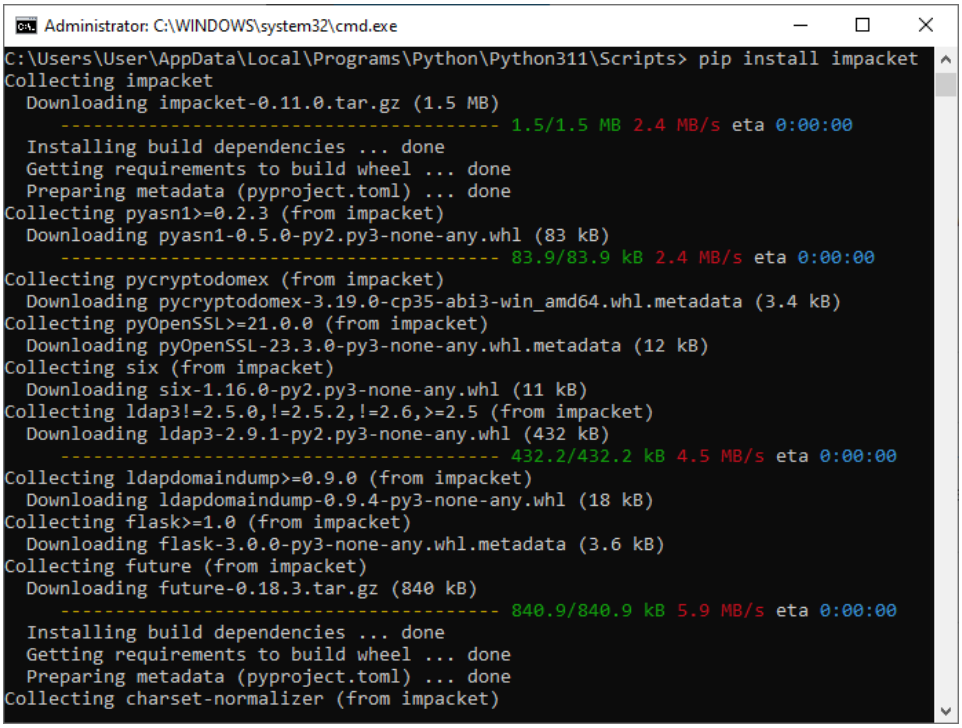


Рисунок 3.6 – Інсталяція Impacket

- PyParsing – модуль для створення та виконання простих граматик порівняно з традиційним підходом lex/yacc або використанням регулярних виразів. Модуль PyParsing надає бібліотеку класів, які клієнтський код використовує для побудови граматики безпосередньо в коді Python (рис 3.7).

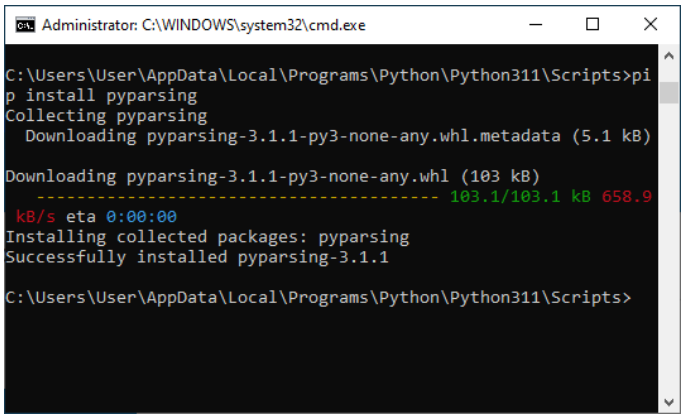


Рисунок 3.7 – Інсталяція PyParsing

- Matplotlib – комплексна бібліотека для створення статичних, анімованих та інтерактивних візуалізацій на Python (рис 3.8).

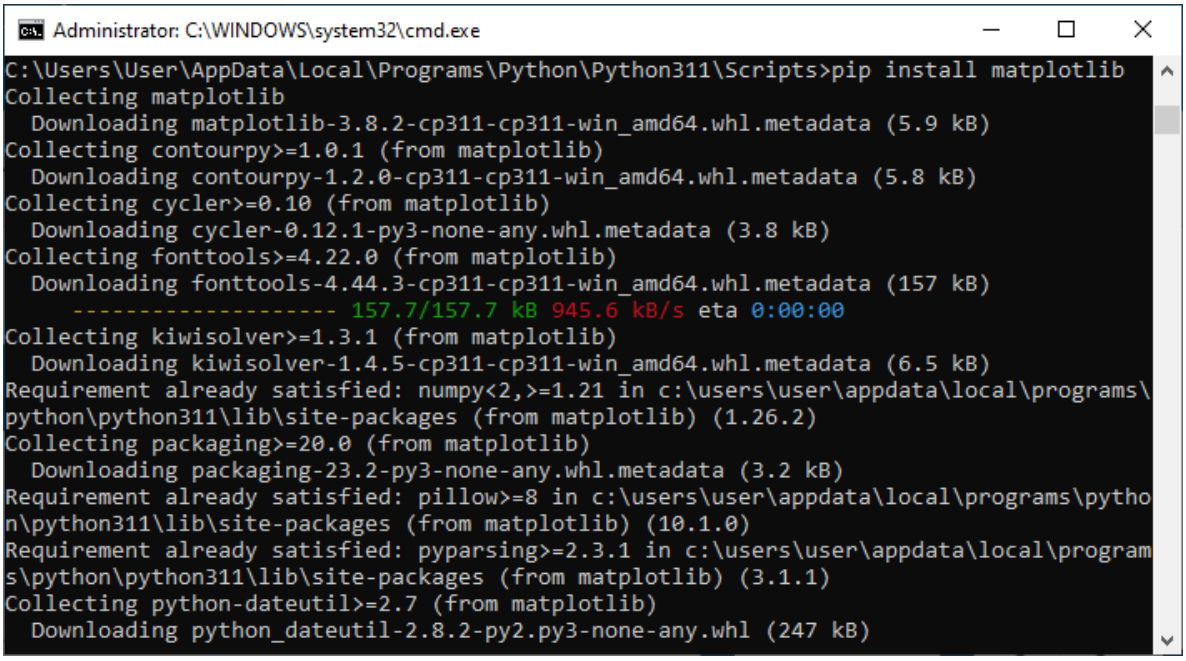


Рисунок 3.8 – Інсталяція Matplotlib

Інші модулі необхідні для розробки та запуску проекту, такі наприклад як PyWin32 та PyAutoGUI, вже інстальоване в Python заздалегідь.

Для захоплення пакетів використовується включена в Python бібліотека захоплення, а саме Pycap, а встановлене програмне забезпечення Winpcap дозволяє перехоплювати пакети бібліотекою захоплення. Інформацію про список та доступ до мережевих карт одержуємо завдяки модулю PyWin32. Код програмного рішення для представлено в додатку А.

Завданням сніффера пакетів є перехопити якомога більше пакетів у мережі. Це було реалізовано за допомогою аналізу продуктивності мережі шляхом вивчення коефіцієнта втрат пакетів із загальною кількістю пакетів (формула 3.3), які надходять у мережу.

Оцінка продуктивності мережі проводиться за допомогою графіка коефіцієнта втрат пакетів та графіка коефіцієнта втрат TCP, причому графік коефіцієнта втрат пакетів порівнює загальний коефіцієнт втрат пакетів із загальною кількістю пакетів (рис. 3.9), а графік коефіцієнта втрат TCP

порівнював коефіцієнт втрат пакетів TCP із загальною кількістю пакетів TCP (рис. 3.10).

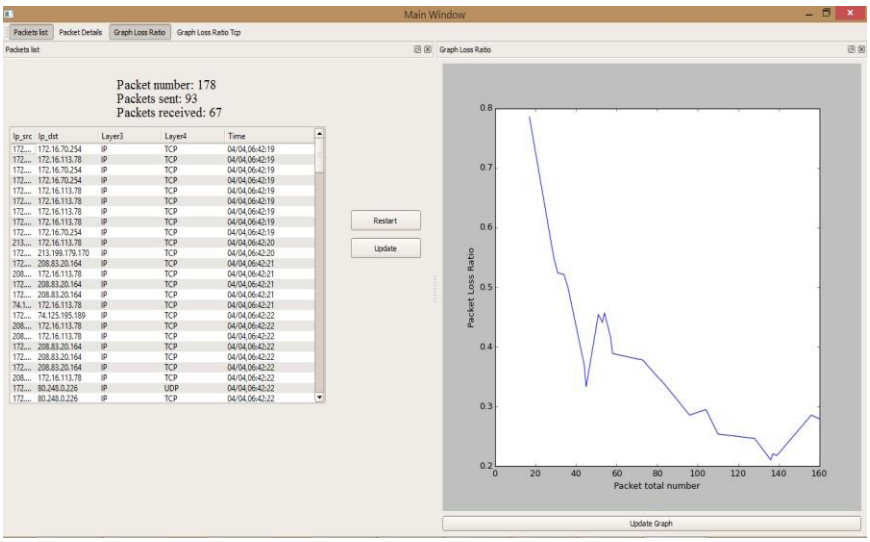


Рисунок 3.9 – Графік втрати пакетів

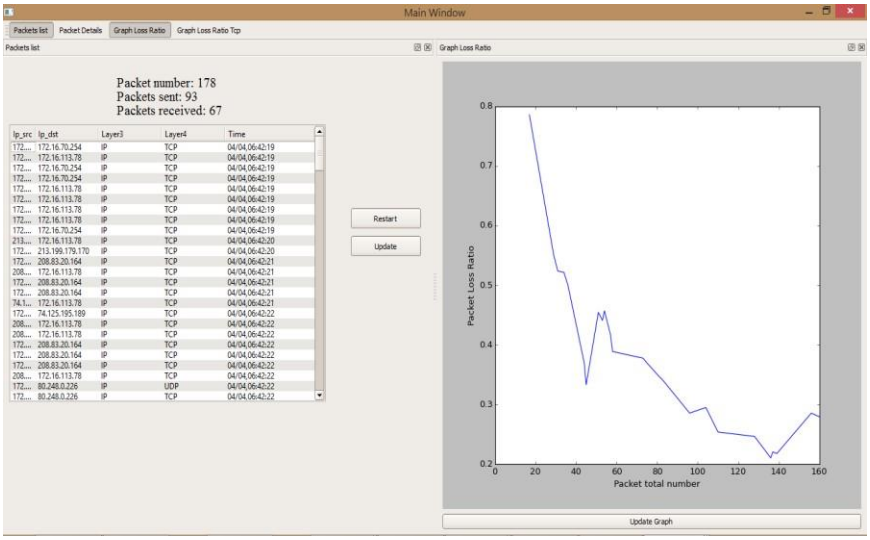


Рисунок 3.10 – Втрата TCP пакетів

Два графіки (рис 3.9 і 3.10) важливі для демонстрації того, як працює мережа та наскільки ефективно пакети доставляються й отримуються відповідними адресами.

Пакети перераховуються у вікні списку пакетів, де з першого погляду відображається кількість пакетів, захоплених у кожен момент часу, а також відображається IP-адреса джерела та призначення разом із протоколами рівня 3

і рівня 4 і часом, коли пакет досягає свого призначення.

Кожен пакет має MAC-адресу джерела та призначення, IP-адресу та номер порту, а заголовок пакета розбивається, щоб отримати деталі кожного пакета, щоб натиснувши кнопку, можна було виконати аналіз кожного пакета, як показано на рисунку 3.11.

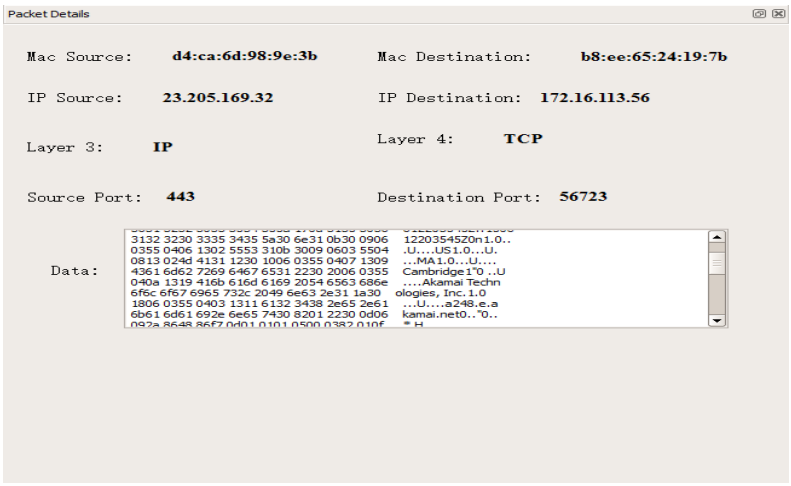


Рисунок 3.11 – Детальні відомості про пакет

Під час передачі даних один або кілька пакетів можуть не досягти місця призначення, і, як було сказано раніше, на графіках відображено коефіцієнт втрат пакетів від загальної кількості пакетів для моніторингу частоти помилок пакетів у мережі.

Окрім інформації про втрату пакетів даний сніффер дає змогу проаналізувати IP Source, тобто адресу відправника, завдяки чому можливим стає блокування небажаного трафіку, шляхом формування білого списку IP адрес та контролю доступу на його основі.

Сформувавши відповідний файл з білим списком IP адрес адміністратор має змогу в подальшому проводити його аналіз за допомогою спеціального модуля код якого представлено в додатку Б, а сам інтерфейс представлено на рисунку 3.12.

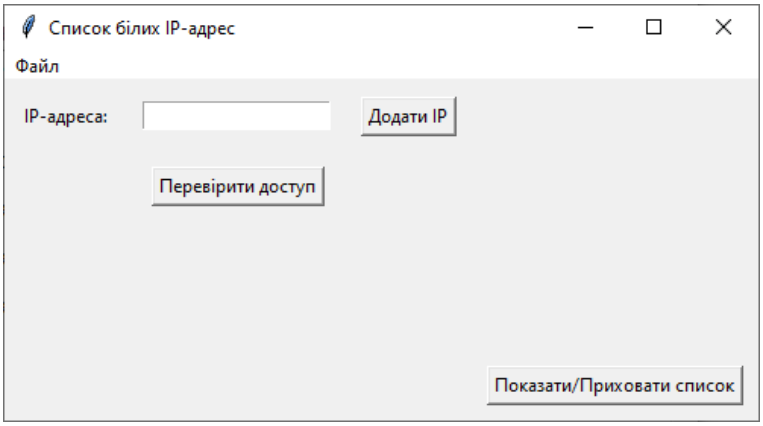


Рисунок 3.12 – Інтерфейс аналізатора IP адрес

Користувач має можливість за допомогою відповідної кнопки показати або приховати список IP адрес, які були досліджені. Як було досліджено в розділі 2, більшість атак на пристрої кіберфізичних систем здійснюються з невідомих IP адрес, тому перевірка користувачів за допомогою білого списку дає можливість значно покращити захист таких систем. Для адміністратора, який відповідає за роботу системи є можливість добавити необхідні IP адреси за допомогою відповідної кнопки (рис. 3.13).

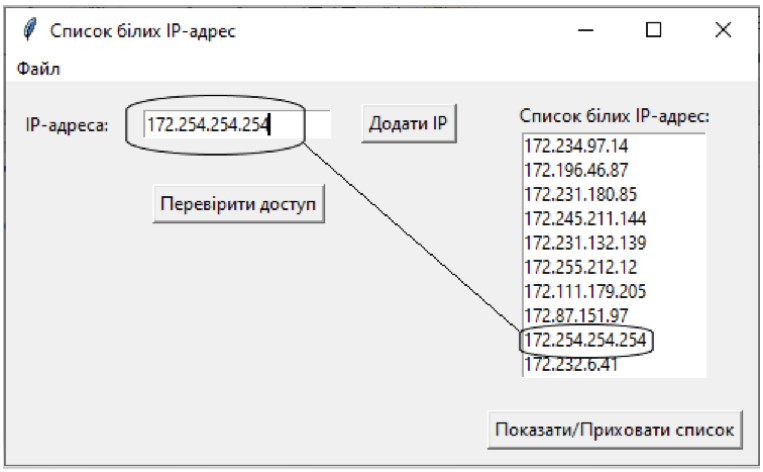


Рисунок 3.13 – Додавання IP адрес в білий список

Відповідно при перевірці цієї IP адреси ми отримає повідомлення, що вона має доступ до кіберфізичної мережі (рис. 3.14).

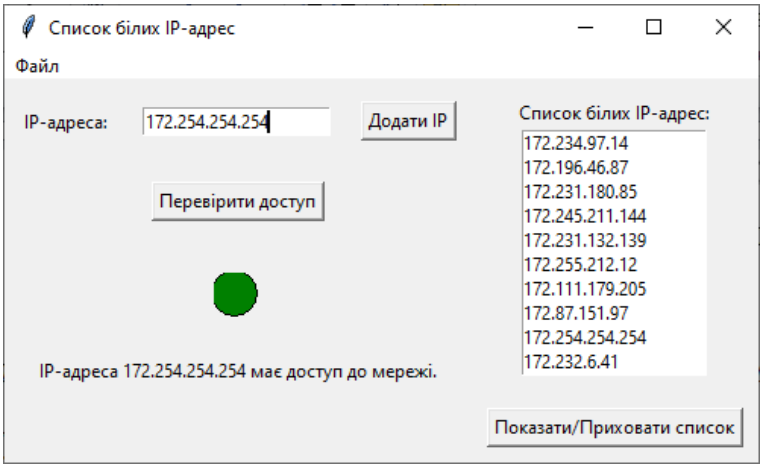


Рисунок 3.14 – Перевірка IP адреси що належить до білого списку

У випадку, коли користувач з певної IP адреси не має доступу до мережі адміністратор отримає про це відповідне повідомлення (рис. 3.15).

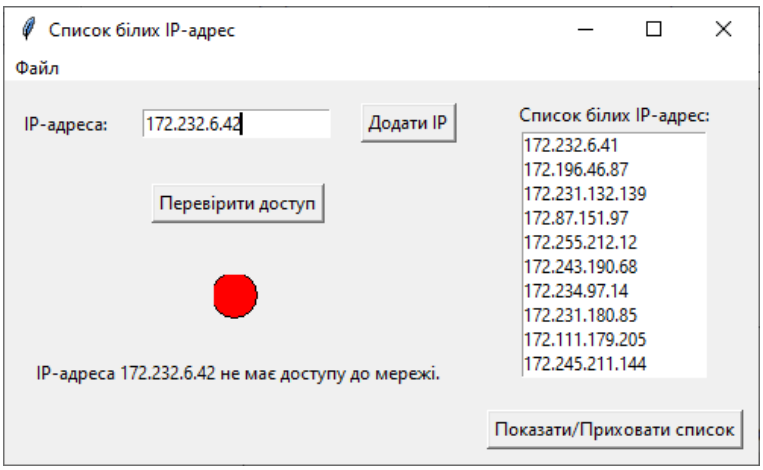


Рисунок 3.15 – Перевірка IP адреси що НЕ належить до білого списку

Для покращення взаємодії з іншими програмними компонентами та у випадку потреби передати список білих IP адрес в інший проект чи мережу адміністратору доступне зберігання списку поточних IP адрес у вигляді текстового файлу (рис. 3.16).

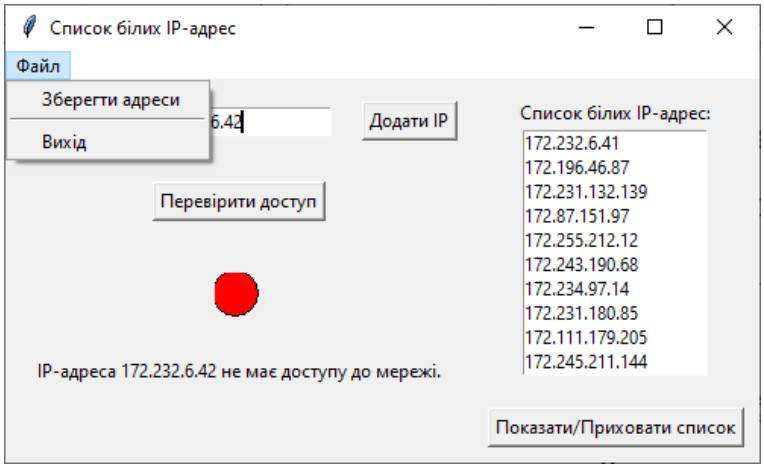


Рисунок 3.16 – Зберігання IP адрес

Використовуючи даний програмний модуль адміністратор системи здатний у будь-який момент переконатися чи знаходиться IP адреса в білому списку та у випадку необхідності добавити її.

ВИСНОВКИ

Моніторинг даних, що передаються та зберігається у різноманітних системах з кожним роком стає все складнішим завданням. Зростання їх розміру та складності приводить до збільшення кількості вразливостей в таких системах. Особливо вразливими є кіберфізичні системи, які потребують захисту як від фізичних, так і від кібератак.

У роботі проведено дослідження сфери застосування кіберфізичних систем та потенційних загроз для них. Визначено, що першим етапом кібератаки є мережева розвідка. У роботі запропоновано алгоритм захисту даних на основі використання білого списку IP адрес та сніфера пакетів для її визначення. Оскільки більшість атак здійснюється з вражених пристроїв по всьому світі, що підтверджено дослідженням із використанням даних, що знаходяться у вільному доступі на ресурсах DShield, AbuseIPDB і Cymon.

Представлено реалізацію сніфера пакетів, розробленого з використанням мови програмування Python, який перехоплює трафік та програмного модуля для адміністративного керування білим списком користувачів та перевірки їх повноважень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Duo, W., Zhou, M., & Abusorrah, A. (2022). A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica*, 9(5), 784-800.
2. NIST. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. NIST, Gaithersburg, MD. Available from: dx.doi.org/10.6028/NIST.SP.800-53r4.
3. Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems*, 77, 103201.
4. Daniel Fraunholz, Simon Duque Anton, and Hans Dieter Schotten. (2017). Introducing gamfis: A generic attacker model for information security. *International Conference on Software, Telecommunications and Computer Networks*, 25.
5. Bergeron, D. E., Cessna, J. T., Coursey, B. M., Fitzgerald, R., & Zimmerman, B. E. (2014). A review of NIST primary activity standards for 18F: 1982 to 2013. *Journal of Research of the National Institute of Standards and Technology*, 119, 371.
6. U.S. Department of Defense. (2016). Department of Defense Dictionary of Military and Associated Terms. Available from: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
7. U.S. Department of Energy. (2005). Safeguards and Security Program Glossary - DOE M 470.4-7. U.S. DOE, Washington, D.C.
8. President’s National Security Telecommunications Advisory Committee. (2014). NSTAC Report to the President on the Internet of Things.
9. Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). Cyber-physical systems and internet of things, 61.
10. Lv, Z., Chen, D., Lou, R., & Alazab, A. (2021). Artificial intelligence for securing industrial-based cyber–physical systems. *Future generation computer systems*, 117, 291-298.
11. Napoleone, A., Macchi, M., & Pozzetti, A. (2020). A review on the

characteristics of cyber-physical systems for the future smart factories. *Journal of manufacturing systems*, 54, 305-335.

12. Malik, J. A., & Saleem, M. (2022). Blockchain and Cyber-Physical System for Security Engineering in the Smart Industry. *Security Engineering for Embedded and Cyber-Physical Systems*, 51-70.
13. Khujamatov, H., Reypnazarov, E., Khasanov, D., & Akhmedov, N. (2021). IoT, IIoT, and cyber-physical systems integration. *In Emergence of Cyber Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation*, 31-50.
14. Tyagi, A. K., & Sreenath, N. (2021). Cyber Physical Systems: Analyses, challenges and possible solutions. *Internet of Things and Cyber-Physical Systems*, 1, 22-33.
15. Zhang, D., Wang, Q. G., Feng, G., Shi, Y., & Vasilakos, A. V. (2021). A survey on attack detection, estimation and control of industrial cyber–physical systems. *ISA transactions*, 116, 1-16.
16. Luo, Y., Xiao, Y., Cheng, L., Peng, G., & Yao, D. (2021). Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. *ACM Computing Surveys (CSUR)*, 54(5), 1-36.
17. Groopman, J., Etlinger, S. (2015). Consumer Perceptions of Privacy in the Internet of Things: What Brands Can Learn from a Concerned Citizenry. *Altimeter Group*, June 2015.
18. Cao, K., Hu, S., Shi, Y., Colombo, A. W., Karnouskos, S., & Li, X. (2021). A survey on edge and edge-cloud computing assisted cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 17(11), 7806-7819.
19. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*, 9, 121975-121995.
20. Bodkhe, U., Mehta, D., Tanwar, S., Bhattacharya, P., Singh, P. K., & Hong, W. C. (2020). A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access*, 8, 54371-54401.
21. C. Scott and R. Carbone. (2014). Designing and implementing a honeypot for a

scada network. *The SANS Institute Reading Room*, 22, 2016.

22. M. Burmester, E. Magkos, and V. Chrissikopoulos.(2012). Modeling security in cyber-physical systems. *International journal of critical infrastructure protection*. 118-126.
23. E. Bou-Harb, M. Debbabi, and C. Assi (2013). A statistical approach for fingerprinting probing activities. *Availability, Reliability and Security (ARES)*. 2013 Eighth International Conference on. IEEE, 21–30.
24. Department of Homeland Security (DHS). (2018). ICS-CERT Monitor Newsletter. [Online]: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT Monitor Nov-Dec2017 S508C.pdf, retrieved: August, 2018.
25. E. Bou-Harb, M. Debbabi, and C. Assi. (2014). Cyber scanning: a comprehensive survey. *IEEE Communications Surveys & Tutorials*, 16, 1496-1519.
26. X. W. D. Leonard, Z. Yao and D. Loguinov. (2012). Stochastic analysis of horizontal ip scanning. *in INFOCOM, 2012 Proceedings IEEE*. 2077–2085.
27. Y. Jin, Z.-L. Zhang, K. Xu, F. Cao, and S. Sahu. (2007). Identifying and tracking suspicious activities through ip gray space analysis. *in Proceedings of the 3rd annual ACM workshop on Mining network data. ACM*, 7–12.
28. Y. Jin, G. Simon, K. Xu, Z. Zhang, and V. Kumar. (2007). Grays anatomy: Dissecting scanning activities using ip gray space analysis. *SysML07*.
29. Y. Pryadkin, R. Lindell, J. Bannister, and R. Govindan. (2004). An empirical evaluation of ip address space occupancy. *USC/ISI, Tech. Rep. ISITR-2004*, 598.
30. J. Heidemann, Y. Pradkin, R. Govindan, C. Papadopoulos, G. Bartlett, and J. Bannister. (2008). Census and survey of the visible internet. i*n Proceedings of the 8th ACM SIGCOMM conference on Internet measurement. ACM*, 169–182.
31. A. Cui and S. Stolfo. (2010). A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan. *in Proceedings of the 26th Annual Computer Security Applications Conference. ACM*, 97–106.
32. Z. Durumeric, M. Bailey, and J. A. Halderman. (2014). An internet-wide view of internet-wide scanning. *in USENIX Security Symposium*, 65–78.
33. C. Fachkha, E. Bou-Harb, A. Keliris, N. Memon, and M. Ahamad. (2017). Internet-scale probing of CPS: Inference, characterization and orchestration analysis. *in Network and Distributed System Security Symposium (NDSS)*.

34. V. Pothamsetty and M. Franz. (2008). Scada honeynet project: Building honeypots for industrial networks.
35. Digital Bond. SCADA Honeynet. (2018). [Online]: http://www.digitalbond.com/tools/scada-honeynet/, retrieved: August, 2018.
36. HoneyNet Project. (2018). "CONPOT ICS/SCADA Honeypot," [Online]: http://conpot.org/, retrieved: August, 2018.
37. D. Sysman, G. Evron, and I. Sher. (2015). Breaking honeypots for fun and profit," *in BLACKHAT*.
38. Project Artillery. (2018). SCADA Honeynet. [Online]: https://blog.binarydefense.com/project-artillery-now-a-binary-defense-project, retrieved: August, 2018.
39. Team CYMRU, "Who is looking for your SCADA infrastructure?" [Online]: https://www.team-cymru.com/ReadingRoom/Whitepapers/2009/scada.pdf, 2008, retrieved: August, 2018
40. DNP, "Overview of the DNP3 Protocol," [Online]: https://www.dnp.org/Pages/AboutDefault.aspx, 2011, retrieved: August, 2018.
41. Modicon, "Modbus," [Online]: http://www.modbus.org/, 2018, August, 2018.
42. Rockwell, "Rockwell Automation," [Online]: https://www. rockwellautomation.com /site-selection.html, 2018, retrieved: August, 2018
43. E. Vasilomanolakis, S. Srinivasa, C. G. Cordero, and M. Mhlhuser. (2016). Multi-stage attack detection and signature generation with ics honeypots. *in NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, 1227-1232.
44. M. Roesch. (1999). Snort: Lightweight intrusion detection for networks." *In Lisa*, 99, 1, 229–238.
45. "Whois," [Online]: https://www.whois.net/, 2018, retrieved: August, 2018.
46. Internet Storm Center, "DShield," [Online]:https://www.dshield.org/,August, 2018.
47. Digital Ocean, "AbuseIP DB," [Online]: https://www.abuseipdb.com/,August, 2018.
48. Open Threat Intelligence, "Cymon," [Online]: https://cymon.io/, retrieved: August, 2018.
49. PlallaviAsrodia, Vishal Sharma. (2013). Network Monitoring and Analysis by Packet Sniffing Method. *International Journal of Engineering Trends and*

Technology (IJETT), 5, May.

50. S. Ansari, Rajeev S.G. and Chandrasekhar H.S. (2003). Packet Sniffing: A Brief introduction. IEEE *Potentials*, Dec 2002-Jan 2003, 21, 5.
51. Awodele Oludele, Otusile Oluwabukola. (2013). The Design and Implementation of a packet sniffer (PSniffer) Model for Network Security", International Journal of Electronics Communication and Computer Engineering-volume 3, issue 6, ISSN (online): 2249-071X, ISSN (Print): 2278-4209.
52. Mohammed Abdul Qadeer, Mohammad Zahid, Arshad Iqbal, MisbahurRahman Siddiqui. (2010). Network Traffic Analysis and Intrusion Detection using Packet Sniffer", *2010 Second International Conference on Communication Software and Networks*.
53. A. Dabir, A. Matrawy. (2007). Bottleneck Analysis of Traffic Monitoring Using Wireshark. 4*th International Conference on Innovations in Information Technology*, IEEE Innovations '07, 18-20 Nov. 158- 162.
54. Otusile Oluwabukola, Awodele Oludele, A.C Ogbonna, Ajeagbu Chigozirim, Anyeahie Amarachi. (2013). A Packet Sniffer (PSniffer) Application for Network Security in Java. *Issues in Informing Science and Information Technology,* 10.
55. SB .A. Mohammed, Dr.S.M Sani, Dr. D.D. Dajab. (2013). Network Traffic Analysis: A Case Study of ABU Network. *Computer Engineering and Intelligent Systems*, 4.
56. A. Dabir, A. Matrawy. (2007). Bottleneck Analysis of Traffic Monitoring Using Wireshark. *4th International Conference on Innovations in Information Technology*, IEEE Innovations '07, 18-20 Nov. 158- 162.
57. Otusile Oluwabukola, Awodele Oludele, A.C Ogbonna, Ajeagbu Chigozirim, Anyeahie Amarachi. (2013). A Packet Sniffer (PSniffer) Application for Network Security in Java. *Issues in Informing Science and Information Technology,* 10.
58. Md. Kamrul Hasan, A.H.M. Amimul Ahsan, and M.Mostafizur Rahman. (2012). IEEE 802.11b Packet Analysis to Improve Network Performance. *JU Journal of Information Technology (JIT)*, 1, June.

ДОДАТОК А

Програмний код реалізації сніфера пакетів

```
import tkinter as tk
from matplotlib.figure import Figure
from matplotlib.backends.backend_tkagg import FigureCanvasTkAgg
import numpy as np
def generate_smooth_data():
    x_values = np.arange(1, 361)
    y_values = 0.8 - np.cumsum(np.random.uniform(-0.02, 0.02, size=360))
    y_values[50:100] += 0.1
    y_values[150:200] += 0.1
    y_values[250:300] += 0.1
    y_values += np.maximum(0, (1 - x_values / 360) * 0.8)
    y_values = y_values - y_values[0] + 0.8
    return x_values, y_values
def plot_graph():
    x_values, y_values = generate_smooth_data()
    # Створюємо фігуру Matplotlib
    fig = Figure(figsize=(5, 4), dpi=100)
    # Додаємо графік до фігури
    ax = fig.add_subplot(111)
    ax.plot(x_values, y_values, label='Графік з плавними даними')
    # Задаємо заголовок та підписи до вісей
    ax.set_title('Графік Packet Loss Ratio')
    ax.set_xlabel('Packet total number')
    ax.set_ylabel('Packet Loss Ratio')
    # Додаємо легенду
    ax.legend()
    # Очищаємо попередні значення при оновленні графіка
    for widget in graph_frame.winfo_children():
```

```
        widget.destroy()
    # Створюємо віджет Tkinter для відображення графіка
    canvas = FigureCanvasTkAgg(fig, master=graph_frame)
    canvas_widget = canvas.get_tk_widget()
    # Пакуємо віджет у вікно Tkinter
    canvas_widget.pack(side=tk.TOP, fill=tk.BOTH, expand=1)
# Створюємо головне вікно Tkinter
window = tk.Tk()
window.title("Графік та дані")
# Створюємо фрейм для графіка (права частина)
graph_frame = tk.Frame(window)
graph_frame.pack(side=tk.RIGHT, padx=10, pady=10)
# Створюємо фрейм для даних (ліва частина)
data_frame = tk.Frame(window)
data_frame.pack(side=tk.LEFT, padx=10, pady=10)
# Додаємо кнопки над лівою частиною
button_packets_list = tk.Button(data_frame, text="Packets List")
button_packets_list.pack(side=tk.TOP, pady=5)
button_packet_details = tk.Button(data_frame, text="Packet Details")
button_packet_details.pack(side=tk.TOP, pady=5)
button_graph_loss_ratio = tk.Button(data_frame, text="Graph Loss Ratio")
button_graph_loss_ratio.pack(side=tk.TOP, pady=5)
button_loss_ratio_top = tk.Button(data_frame, text="Loss Ratio Top")
button_loss_ratio_top.pack(side=tk.TOP, pady=5)
# Додаємо кнопку для виклику функції plot_graph
plot_button = tk.Button(data_frame, text="Побудувати графік",
command=plot_graph)
plot_button.pack(side=tk.TOP, pady=10)
# Запускаємо головний цикл Tkinter
window.mainloop()
```

ДОДАТОК Б

Програмний код організації білого списку IP адрес

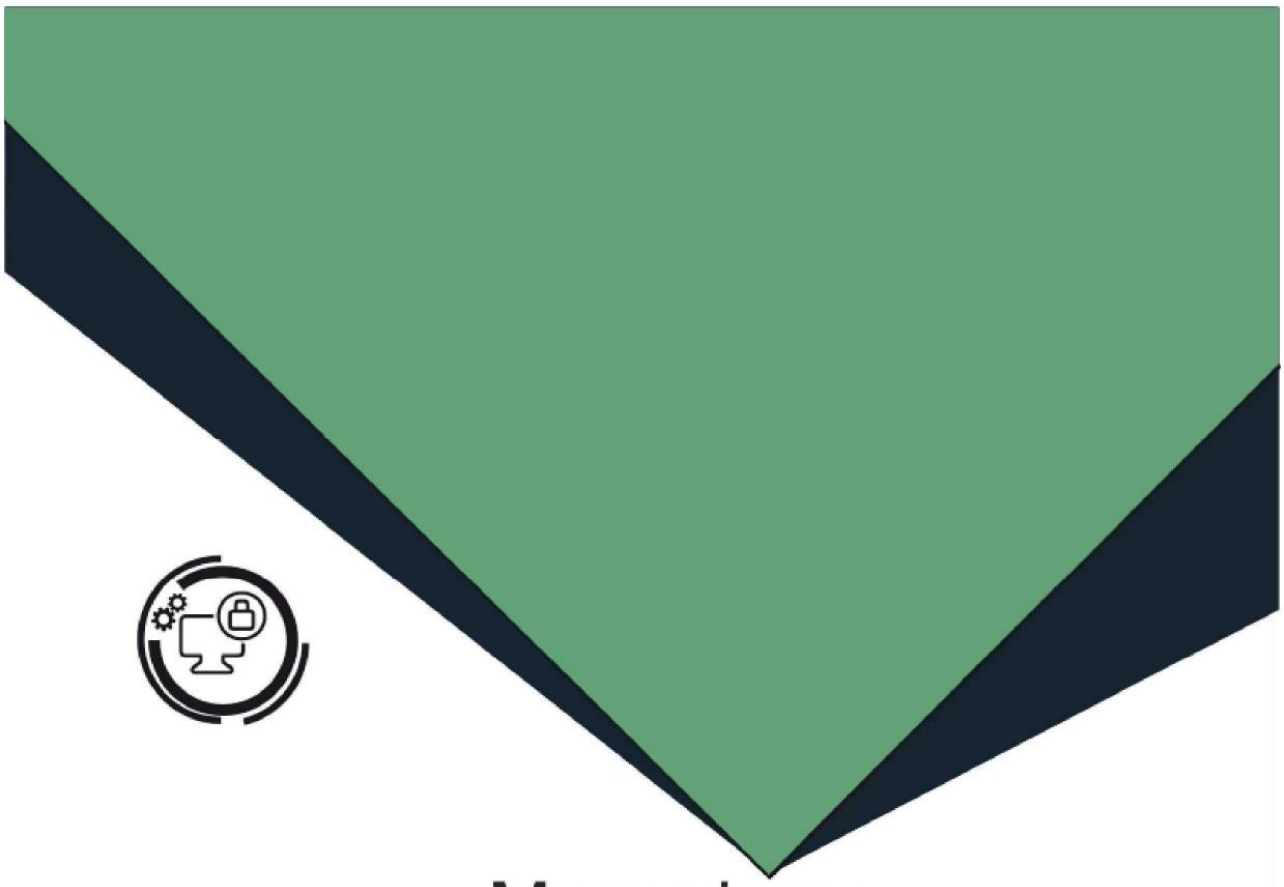
```
import tkinter as tk
from tkinter import filedialog
from PIL import Image, ImageTk
import random import os
class WhiteListApp:
    def __init__(self, master):
        self.master = master
        self.master.title("Список білих IP-адрес")
        self.white_list = set()
        self.file_path = "ip_addresses.txt"
        if os.path.exists(self.file_path):
            self.load_ip_addresses()
        else:
            for _ in range(10):
                random_ip = f"172.{random.randint(0, 255)}.{random.randint(0,
255)}.{random.randint(0, 255)}"
                self.white_list.add(random_ip)
        self.create_widgets()
    def create_widgets(self):
        self.menu_bar = tk.Menu(self.master)
        self.master.config(menu=self.menu_bar)
        self.file_menu = tk.Menu(self.menu_bar, tearoff=0)
        self.menu_bar.add_cascade(label="Файл", menu=self.file_menu)
        self.file_menu.add_command(label="Зберегти адреси",
command=self.save_addresses)
        self.file_menu.add_separator()
        self.file_menu.add_command(label="Вихід", command=self.exit_program)
        self.ip_entry_label = tk.Label(self.master, text="IP-адреса:")
        self.ip_entry_label.grid(row=0, column=0, sticky=tk.W, padx=10, pady=10)
        self.ip_entry = tk.Entry(self.master)
        self.ip_entry.grid(row=0, column=1, padx=10, pady=10)
```

```
        self.add_button = tk.Button(self.master, text="Додати IP",
command=self.add_ip)
        self.add_button.grid(row=0, column=2, padx=10, pady=10)
        self.check_button = tk.Button(self.master, text="Перевірити доступ",
command=self.check_access)
        self.check_button.grid(row=1, column=0, columnspan=3, pady=10)
        self.status_oval = tk.Canvas(self.master, width=30, height=30)
        self.status_oval.grid(row=2, column=1, pady=15)
        # Віджет для виведення результатів
        self.result_label = tk.Label(self.master, text="")
        self.result_label.grid(row=3, column=0, columnspan=3)
        self.list_frame = tk.Frame(self.master)
        self.list_frame.grid(row=0, column=3, rowspan=4, padx=10, pady=10)
        self.list_label = tk.Label(self.list_frame, text="Список білих IP-адрес:")
        self.list_label.pack()
        self.ip_listbox = tk.Listbox(self.list_frame, selectmode=tk.SINGLE)
        self.update_ip_listbox()
        self.ip_listbox.pack()
        self.toggle_list_button = tk.Button(self.master, text="Показати/Приховати
список", command=self.toggle_list)
        self.toggle_list_button.grid(row=4, column=3, padx=10, pady=10)
    def add_ip(self):
        ip_address = self.ip_entry.get()
        if ip_address:
            self.white_list.add(ip_address)
            self.ip_entry.delete(0, tk.END)  # Очищаємо поле введення
            self.update_ip_listbox()
            print(f"Додано IP-адресу: {ip_address}")
    def check_access(self):
        ip_to_check = self.ip_entry.get()
        if ip_to_check:
            if ip_to_check in self.white_list:
                result_text = f"IP-адреса {ip_to_check} має доступ до мережі."
                self.set_oval_color("green")  # Зелений колір для доступу
            else:
                result_text = f"IP-адреса {ip_to_check} не має доступу до мережі."
```

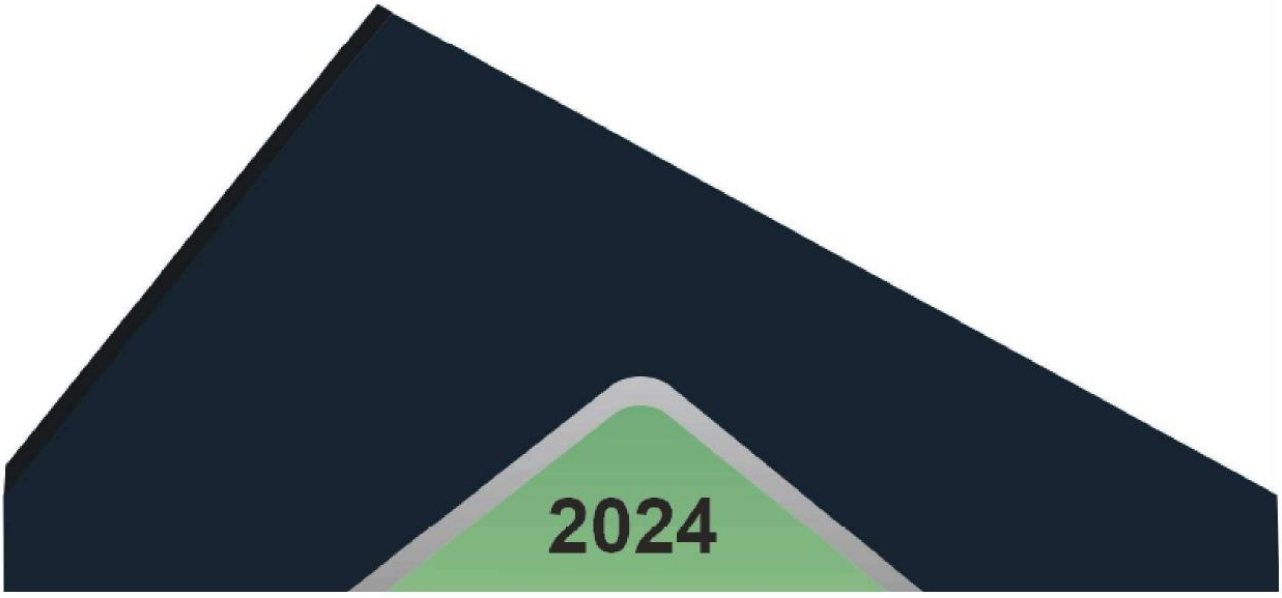
```
                self.set_oval_color("red")  # Червоний колір для недоступу
            self.result_label.config(text=result_text)
    def set_oval_color(self, color):
        self.status_oval.delete("all")
        self.status_oval.create_oval(0, 0, 30, 30, fill=color)
    def update_ip_listbox(self):
        self.ip_listbox.delete(0, tk.END)
        for ip_address in self.white_list:
            self.ip_listbox.insert(tk.END, ip_address)
    def toggle_list(self):
        current_state = self.list_frame.winfo_ismapped()
        new_state = not current_state
        self.list_frame.grid_forget() if current_state else self.list_frame.grid(row=0,
column=3, rowspan=4, padx=10, pady=10)
       #self.toggle_list_button.config(text="Показати " if new_state else "Приховати")
    def save_addresses(self):
        file_path = filedialog.asksaveasfilename(defaultextension=".txt",
filetypes=[("Text files", "*.txt")])
        if file_path:
            self.file_path = file_path
            self.save_ip_addresses()
    def load_ip_addresses(self):
        with open(self.file_path, "r") as file:
            for line in file:
                ip_address = line.strip()
                if ip_address:
                    self.white_list.add(ip_address)
    def save_ip_addresses(self):
        with open(self.file_path, "w") as file:
            for ip_address in self.white_list:
                file.write(f"{ip_address}\n")
    def exit_program(self):
        self.save_ip_addresses()
        self.master.destroy()
root = tk.Tk()
app = WhiteListApp(root)
```

ДОДАТОК В

КОПІЇ ПУБЛІКАЦІЙ



Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»



ГРОМАДСЬКА ОРГАНІЗАЦІЯ
«КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»

30 листопада 2024
Тернопіль

У збірнику опубліковано матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. - 130с.

Технічний редактор: Давлетова А.Я.

Адреса редакції:
Громадська організація «Кібербезпека і автоматизація»
м. Тернопіль
Контактний телефон: (066)043-42-10
e-mail: conferencekb@gmail.com

УДК 004.056

Микита ОНИЩЕНКО, Андрій ТИМЧАК, Геннадій ПОНЕДЄЛЬНІКОВ

Західноукраїнський національний університет

ЗАХИСТ ДАНИХ У КІБЕРФІЗИЧНИХ СИСТЕМАХ

Вступ. Кіберфізичні системи знаходять широке застосування в технологічних і промислових галузях, сприяючи оптимізації процесів і наданню функціональних можливостей, які раніше були недоступними. Проте за останні десять років вони стали об'єктами деяких із найбільш масштабних порушень безпеки. Традиційні підходи до забезпечення лише кібернетичної або фізичної безпеки виявляються недостатніми для захисту КФС, адже складні взаємозв'язки та перехресні впливи в таких системах створюють нові вразливості. Оскільки КФС часто використовуються в критичних додатках, будь-яка атака на них може спричинити втрату або пошкодження даних. Це підкреслює важливість забезпечення безпеки та конфіденційності на всіх етапах - від проектування і розробки до експлуатації таких систем.

Мета: дослідження існуючих методів та способів захисту даних у кіберфізичних системах.

1. Сфери захисту даних в кіберфізичних системах

Кіберфізичні системи (КФС) застосовуються у різноманітних галузях для оптимізації процесів. Поєднання цифрових мережевих компонентів із аналоговими фізичними процесами створює унікальні властивості, які змінюють підходи до реалізації безпеки [1]. Під заходами безпеки розуміють комплекс дій, що забезпечують досягнення системою своїх цілей, мінімізуючи ризики непередбачених негативних наслідків. При впровадженні нових функцій безпека покликана гарантувати збереження запланованої функціональності та уникнення створення нових векторів атак. Національний інститут стандартів і технологій (NIST) визначає конфіденційність як «забезпечення захисту та обмеженого доступу до певної інформації організації» [2]. Під такою інформацією розуміють конфіденційні дані, наприклад, особисту інформацію, а суб'єктами можуть бути як компанії чи установи, так і окремі особи.

Безпека й конфіденційність тісно пов'язані, оскільки обидві концепції зосереджені на належному використанні інформації та її захисті. Конфіденційність зазвичай асоціюється зі свободою від стороннього спостереження, небажаної уваги або втручання, а також із можливістю обмежувати доступ до особистих даних. У цьому контексті конфіденційність розглядається як частина безпеки, адже безпечна система повинна забезпечувати захист конфіденційності. Однак вона має і динамічний аспект, дозволяючи власникам інформації самостійно контролювати її розповсюдження.

Концепції безпеки та конфіденційності можуть застосовуватись як до кіберкомпонентів, так і до фізичної складової КФС. Ці поняття часто пов'язані з термінами, що входять в одну галузь, наприклад такими як кібербезпека, інформаційна безпека та захист інформації. При аналізі захисту конфіденційних даних увага зосереджується на інформаційній стороні КФС. У цьому контексті достатньо використовувати визначення

інформаційної безпеки, запропоноване NIST - «це стан, що досягається шляхом впровадження та підтримки захисних заходів, які дозволяють організації виконувати свою місію або критично важливі функції, незважаючи на загрози, пов'язані з використанням інформаційних систем». У такому випадку захисні заходи охоплюють комплекс дій, включаючи стримування, уникнення, запобігання, виявлення, відновлення та усунення загроз, які мають бути складовою частиною стратегії управління ризиками організації [3].

Інформаційну безпеку характеризують три ключові принципи:

1. Конфіденційність - доступ до ресурсів мають виключно авторизовані користувачі.
2. Цілісність - зміни в ресурсах можуть вносити лише уповноважені особи або дозволеними методами.
3. Доступність - ресурси повинні бути доступними для авторизованих користувачів у потрібний час.

Ці принципи формують так звану тріаду КЦД (або CIA в міжнародній термінології), що забезпечує правильний доступ до необхідної інформації для відповідних користувачів, програм чи пристроїв (рисунок 1).

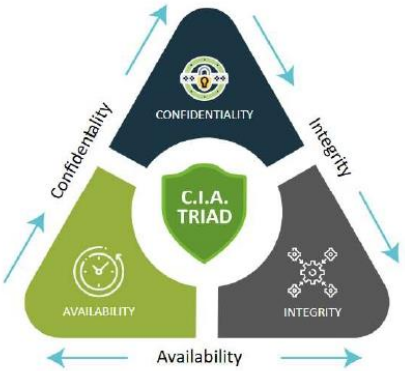


Рисунок 1 - Тріада КЦД

Хоча тріада КЦД є базисом інформаційної безпеки, її часто вважають неповною. Тривають обговорення щодо її вдосконалення, наприклад, шляхом розширення до так званого октету інформаційної безпеки [4].

Представлений на рисунку 2 октет інформаційної безпеки розширює базову тріаду КЦД, доповнюючи її такими елементами, як автентифікація, невідмовність, можливість перевірки, неспростовність і конфіденційність. Остаточний перелік цілей безпеки ще не сформований, проте до базової тріади зазвичай додають два важливих принципи, які найбільше стосуються фізичної сторони КФС.

Їх зазвичай відносять до цілісності, а повний перелік має наступні пункти:

- Автентифікація - підтверджує ідентичність суб'єкта, часто слугує попередньою умовою для отримання доступу.
- Невідмовність - запобігає неправомірному запереченню суб'єктом виконання певних дій, фіксуючи факти виконання, наприклад, надсилання або отримання повідомлення.

Існує ряд засобів реалізації кожного з цих принципів кібербезпеки. Наприклад, шифрування забезпечує конфіденційність, захищаючи дані та функції системи від несанкціонованого використання. Цифрові підписи та безпечні геші забезпечують цілісність, гарантуючи, що дані чи оновлення програмного забезпечення не змінюються.

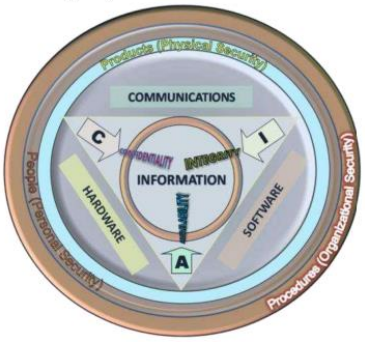


Рисунок 2 - Октет захисту інформації

Резервування ресурсів забезпечує доступність системи для призначених користувачів для належного використання в будь-який час, навіть під час стресу. Особи, сертифікати та паролі є прикладами механізмів автентифікації, які гарантують, що лише авторизовані користувачі можуть отримати доступ до ресурсів, захищених заходами конфіденційності. Автентифікація забезпечує цілісність шляхом перевірки повноважень суб'єктів, які змінюють актив. Автоматично зібрані записи та журнали цих змін можуть показувати, який користувач відкривав або змінював певні частини системи. Коли ці журнали захищені певним механізмом цілісності, результатом є система з неспростуванням. Невідмовність робить порушення цілісності очевидними та надає криміналістично корисну інформацію, коли захист не працює.

Висновок. Таким чином, конфіденційність можна розглядати як частину забезпечення цілісності персональної інформації, оскільки, хоча дані про особу можуть бути передані, сама інформація, яку вони містять, залишається власністю тієї особи, яку вони ідентифікують а поєднання всіх вище зазначених принципів дає змогу захистити дані на належному рівні та згідно загальноприйнятих вимог.

Перелік використаних джерел.

1. Мельник, В., Кривак, Д., Возний, К., Гуральник, О., Дрозд, А. (2024). Кіберфізичні системи для автоматизації приміщень підприємств. Herald of Khmelnytskyi National University. Technical sciences, 335(3 (1)), 429-435.
2. Duo, W., Zhou, M., Abusorrah, A. (2022). A survey of cyber attacks on cyber physical systems: Recent advances and challenges. IEEE/CAA Journal of Automatica Sinica, 9(5), 784-800.
3. NIST, 2013. Security and Privacy Controls for Federal Information Systems and Organizations. NIST, Gaithersburg, MD. Available from: dx.doi.org/10.6028/NIST.SP.800-53r4.
4. Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems, 77, 103201.



ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В'ЯЧЕСЛАВА ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2024)

науково-практична конференція
молодих вчених, аспірантів та студентів

26–28 серпня 2024
Тернопіль

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

2024

науково-практична конференція молодих вчених, аспірантів та студентів

Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2024), Тернопіль, 2024. - 160 с.

Адреса редакції:
Західноукраїнський національний університет, кафедра кібербезпеки,
вул. Олени Теліги 8, м. Тернопіль 46003
Контакти:
*e-mail:*conferencekb@gmail.com

ЗМІСТ

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

УДК 004.056

Микита ОНИЩЕНКО, Андрій ТИМЧАК, Геннадій ПОНЕДЄЛЬНІКОВ

Західноукраїнський національний університет

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІБЕРФІЗИЧНИХ СИСТЕМ ЗА ДОПОМОГОЮ МОНІТОРИНГУ

Вступ. Аналіз і моніторинг трафіку є важливим елементом для розуміння та оптимізації роботи кіберфізичних систем. Вони сприяють виявленню залежностей, підвищенню ефективності та забезпеченню загальної надійності системи.

Програмні засоби захисту КФС та антивірусні рішення також активно застосовують технології моніторингу для виявлення потенційно шкідливих дій. Для перехоплення й запису мережевого трафіку, що проходить через мережеві інтерфейси, використовуються спеціалізовані програми, відомі як сніфери (packet sniffers) [1].

Перехоплені дані містять інформацію про передачу пакетів, включаючи їхнє джерело, місце призначення, протоколи, порти та вміст. Завдяки моніторингу система постійно відстежує всі дії та негайно сповіщає користувачів про можливі загрози, що значно знижує ймовірність проникнення зловмисників у систему та реалізації подальших етапів кібератаки.

Мета: дослідження існуючих методів та способів захисту інформації в кіберфізичних системах шляхом моніторингу.

1. Аналіз і моніторинг трафіку в кіберфізичних системах

Моніторинг і аналіз мережевого трафіку в кіберфізичних системах можна умовно поділити на дві основні категорії: пасивний та інтерактивний.

Пасивний моніторинг передбачає налаштування мережі за допомогою дзеркалювання або використання моніторингового порту для створення копій мережевих пакетів, що передаються між пристроями. Зібрані дані направляються на локальний або хмарний сервер, де за допомогою глибокої перевірки пакетів (DPI) аналізується їхній вміст, визначаються джерело, протоколи, порти, модель пристрою, операційна система тощо.

Однак цей метод має обмеження. Наприклад, він неефективний для пристроїв, які генерують трафік лише у разі відмови або працюють зі специфічними протоколами. Зокрема, протокол Modbus, часто застосовуваний у системах BMS, надає мінімум інформації про пристрої, що ускладнює їхню ідентифікацію, наприклад визначення виробника або версії мікропрограми.

Для підвищення рівня безпеки часто використовують медові пастки (honeypots), які імітують вразливі системи (рисунок 1). Їх мета - привернути увагу зловмисників, допомогти ідентифікувати підозрілий трафік та відвернути атаки від реальних систем.

Розробка програмного забезпечення для ефективного моніторингу та аналізу мережевого трафіку є одним із шляхів вирішення цих проблем. Такі програми здатні захоплювати, структурувати та аналізувати дані, що проходять через мережу.

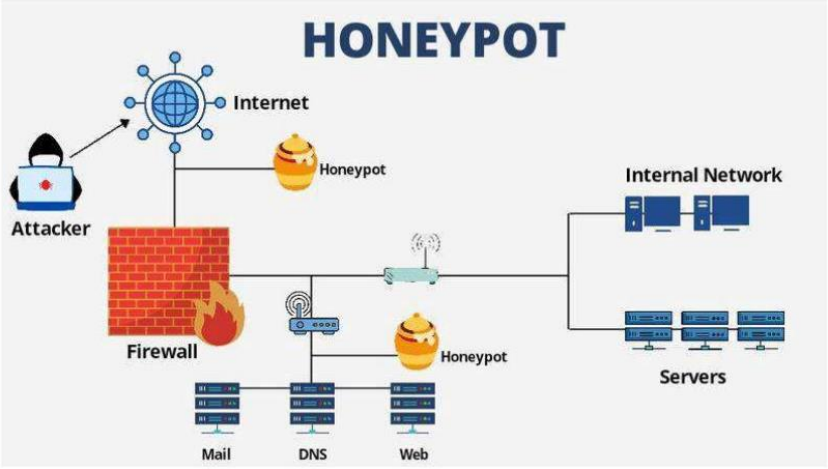


Рисунок 1 - Honeypots

Одним із ключових інструментів у цьому процесі є сніффери пакетів (packet sniffers), або аналізатори мережі [2].

Вони здійснюють атаки з перехопленням пакетів. Атака з перехопленням пакетів (або просто атака з перехопленням) - це мережева загроза, коли зловмисник захоплює мережеві пакети з наміром перехопити або викрасти трафік даних, який, можливо, залишився незашифрованим. Пакети даних збираються, коли вони проходять через комп'ютерну мережу.

Перехоплені пристрої або медіа, які використовуються для здійснення цієї атаки та збору пакетів мережевих даних, називаються перехоплювачами пакетів [3].

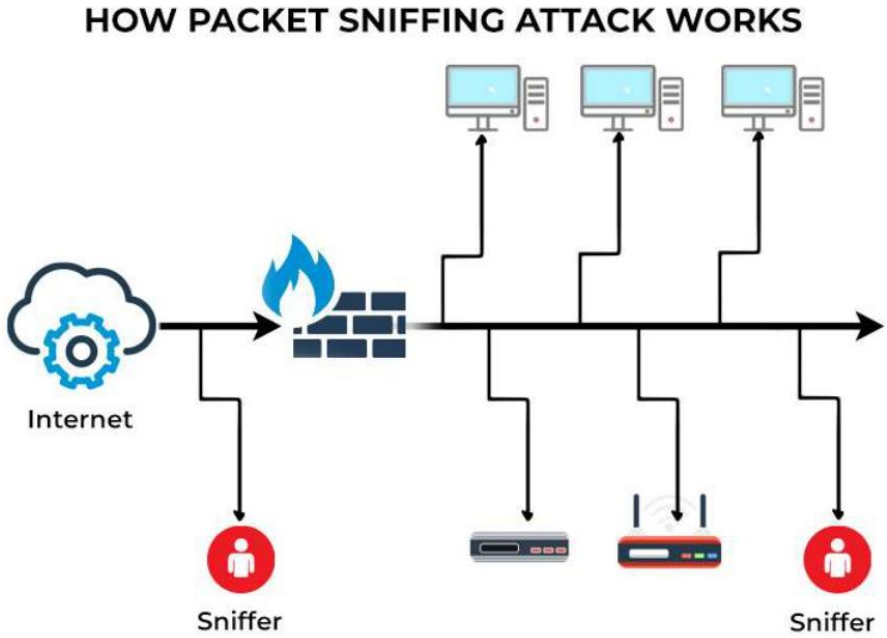


Рисунок 2 - Принцип роботи сніфера пакетів

Сніффери широко використовуються для:

- моніторингу та фільтрації мережевого трафіку,
- діагностики мережевих проблем,
- виявлення некоректних налаштувань,
- аналізу та усунення несправностей у роботі протоколів.

Окрім того, ці інструменти відіграють важливу роль у виявленні підозрілої діяльності в мережі та реагуванні на кіберзагрози [4]. У системах моніторингу вторгнень сніффери допомагають ідентифікувати шкідливу активність ще на етапі її прояву, що підвищує ефективність захисту мережевих інфраструктур.

Одним із таких інструментів є Wireshark [5]. Цей інструмент для аналізу мережевого трафіку, який дозволяє перехоплювати, відслідковувати та аналізувати пакети даних, що передаються через мережу. Він є одним з найбільш відомих сніферів пакетів, що використовується фахівцями з безпеки, адміністраторами мереж і розробниками програмного забезпечення для моніторингу та виявлення проблем у мережах.

Висновок. У світі, де ми все більше покладаємося на мережеві технології для виконання особистої та професійної діяльності, перехоплення даних становить серйозну небезпеку. Завдяки інформації, отриманій від сніфера пакетів, адміністратор може виявляти помилкові пакети та використовувати ці дані для ідентифікації вузьких місць, що допомагає оптимізувати передачу даних у мережі.

На відміну від стандартних мережевих хостів, які отримують лише трафік, адресований їм безпосередньо, аналізатор пакетів дозволяє отримувати дані, спрямовані на інші пристрої. Раніше аналізатори пакетів були дорогими апаратними пристроями, але завдяки новим технологіям розроблено програмні мережеві аналізатори, що робить їх доступнішими та зручнішими у використанні.

Перелік використаних джерел.

1. PlallaviAsrodia, Vishal Sharma. (2013). Network Monitoring and Analysis by Packet Sniffing Method. International Journal of Engineering Trends and Technology (IJETT). - vol 5. -May 2013.

2. S. Ansari, Rajeev S.G. and Chandrasekhar H.S. (2003). Packet Sniffing: A Brief introduction", IEEE Potentials, Dec 2002- Jan 2003, Volume: 21, Issue 5.

3. Awodele Oludele, Otusile Oluwabukola. (2012). The Design and Implementation of a packet sniffer (PSniffer) Model for Network Security. International Journal of Electronics Communication and Computer Engineering. Vol 3, ISSUE 6. ISSN (online): 2249-071X, ISSN (Print): 2278-4209.

4. Mohammed Abdul Qadeer, Mohammad Zahid, Arshad Iqbal, MisbahurRahman Siddiqui. (2010). Network Traffic Analysis and Intrusion Detection using Packet Sniffer. 2010 Second International Conference on Communication Software and Networks, Singapore, 2010, pp. 313-317, doi: 10.1109/ICCSN.2010.104.

5. A. Dabir, A. Matrawy. (2007). Bottleneck Analysis of Traffic Monitoring Using Wireshark. 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov, Page(s): 158- 162.