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

**ОНИЩЕНКО Микита Олексійович**

# Алгоритми автентифікації пристроїв промислового Інтернету речей / Algorithms for authentication of industrial Internet of Things devices

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -21
М. О. Онищенко

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
«____» _____ 2023 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

**ОНИЩЕНКО Микита Олексійович**
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Алгоритми автентифікації пристроїв промислового Інтернету речей / Algorithms for authentication of industrial Internet of Things devices

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

затверджені наказом по університету від 12 грудня 2023 року № 753

2. Строк подання студентом закінченої кваліфікаційної роботи 12 грудня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
- дослідити існуючі алгоритми автентифікації, їх переваги та недоліки;
- визначити особливості застосування алгоритмів в умовах IioT;
- адаптувати сучасні алгоритми автентифікації до специфіки IIoT-середовища;
- забезпечити підтримку багатофакторної автентифікації та захист від атак, зокрема MITM та Replay;
– створити програмні прототипи розроблених алгоритмів;
– протестувати їх у середовищі, яке імітує умови IIoT.

5. Перелік графічного матеріалу у роботі:
–загрози в промисловому IoT;

– схема обміну ключами на основі алгоритму Діффі – Хелмана;
– порівняння схем автентифікації пристроїв;
– алгоритм автентифікації для IioT;
– багатофакторна автентифікація пристроїв.

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 | Механізми автентифікації в промисловому інтернеті речей | 12.2023 р. – 03.2024 р. | |
| 2 | Загрози конфіденційності в промисловому інтернеті речей | 03.2024 р. – 06.2024 р. | |
| 3 | Розробка та дослідження алгоритмів автентифікації пристроїв інтернету речей | 06.2024 р. – 11.2024 р. | |

Студент _____ Онищенко М. О.
( підпис )

Керівник роботи _____ к.т.н., доцент Н.Г. Яцків
( підпис )

# АНОТАЦІЯ

Кваліфікаційна робота на тему «Алгоритми автентифікації пристроїв промислового Інтернету речей» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека та захист інформації» освітньо-професійної програми «Кібербезпека» написана обсягом 62 сторінки і містить 6 ілюстрацій, 1 таблиця, 2 додатки та 32 джерела за переліком посилань.

Метою кваліфікаційної роботи є підвищення ефективності алгоритмів автентифікації пристроїв промислового Інтернету речей.

Методи досліджень. Для розв'язання поставлених задач у даній кваліфікаційній роботі використано: теоретичний аналіз, експериментальні методи, порівняльний аналіз, алгоритмічний синтез.

Результати дослідження. Розроблено алгоритми автентифікації при яких пакети, що передаються між пристроями шифруються, що не дозволяє зловмисникам дізнатися їх вміст, навіть якщо вони перехоплять пакети.

Практичне значення. Запропонований алгоритм автентифікації ефективно протистоїть атакам повторного відтворення, атакам підслуховування, атакам «людина посередині» та імітованим атакам.

Результати роботи можуть бути використані при розробці систем промислового Інтернету речей.

Ключові слова: АВТЕНТИФІКАЦІЇ, ЗАГРОЗА, КОНФІДЕНЦІЙНІСТЬ, ІНТЕРНЕТ РЕЧЕЙ, ЦІЛІСНІСТЬ.

# ABSTRACT

Qualification thesis on the topic "Algorithms for authentication of industrial Internet of Things devices" for obtaining the educational degree "Master" in the specialty 125 "Cybersecurity and Information Protection" under the educational-professional program "Cybersecurity" comprises 62 pages and includes 6 illustrations, 1 table, 2 appendices, and 32 references in the bibliography.

Objective of the qualification work. The aim of this qualification work is to improve the efficiency of authentication algorithms for industrial Internet of Things (IIoT) devices.

Research Methods. To achieve the set objectives, the following methods were used in this work: theoretical analysis, experimental methods, comparative analysis, and algorithmic synthesis.

Research Results. Authentication algorithms were developed in which packets transmitted between devices are encrypted. This prevents attackers from accessing their contents, even if the packets are intercepted.

Practical Significance: The proposed authentication algorithm effectively resists replay attacks, eavesdropping attacks, man-in-the-middle attacks, and spoofing attacks.

The results of this work can be applied in the development of industrial Internet of Things systems.



**Keywords:** AUTHENTICATION, THREAT, CONFIDENTIALITY, INTERNET OF THINGS, INTEGRITY.

ЗМІСТ

# ВСТУП

**Актуальність роботи.** Розвиток технологій промислового Інтернету речей (IIoT) сприяє автоматизації виробничих процесів, підвищенню ефективності роботи обладнання та покращенню управління виробництвом. Однак разом із перевагами зростають і ризики, пов’язані з безпекою інформації. Автентифікація пристроїв є ключовим аспектом забезпечення цілісності, конфіденційності та достовірності даних в IIoT-системах. Недосконаліть традиційних методів автентифікації, їх вразливість до сучасних атак, зокрема, квантових, вимагають створення та аналізу нових алгоритмів, адаптованих до специфіки IIoT.

В деяких аспектах IIoT схожа на загальний IoT, і дослідницькі проблеми IoT, такі як розробка безпечних криптосистем для пристроїв з обмеженими ресурсами, впровадження механізмів для надійної та безпечної роботи в умовах збоїв та успішних атак, а також розробка механізмів безпечної аналітики даних, є важливими і для IIoT. Однак IIoT призначена для підтримки промислових систем, які покладаються на залежну від часу інформацію, наприклад, дані сенсорів в реальному часі та керуючі команди, тому будь-який механізм безпеки повинен забезпечувати безпеку, при цьому гарантуючи безперервність своєчасної передачі даних.

Таким чином, розробка ефективних та безпечних алгоритмів автентифікації для пристроїв IIoT є актуальним завданням.

**Мета і завдання дослідження.** Метою роботи є підвищення ефективності алгоритмів автентифікації пристроїв промислового Інтернету речей.

Досягнення визначеної мети передбачає вирішення таких завдань:

- дослідити існуючі алгоритми автентифікації, їх переваги та недоліки;
- визначити особливості застосування алгоритмів в умовах IioT;

− адаптувати сучасні алгоритми автентифікації до специфіки IIoT-середовища;

− забезпечити підтримку багатофакторної автентифікації та захист від атак, зокрема MITM та Replay;

– створити програмні прототипи розроблених алгоритмів;

– протестувати їх у середовищі, яке імітує умови IIoT.

**Об'єкт дослідження** – процеси автентифікації пристроїв промислового Інтернету речей;

**Предмет дослідження –** алгоритми та механізми автентифікації пристроїв промислового Інтернету речей.

**Методи досліджень.** Для розв'язання поставлених задач у даній кваліфікаційній роботі використано: теоретичний аналіз, експериментальні методи, порівняльний аналіз, алгоритмічний синтез, статистичний аналіз.

**Наукова новизна одержаних результатів.** Наукова новизна полягає у розробці алгоритмів автентифікації при яких пакети, що передаються між пристроями шифруються, що не дозволяє зловмисникам дізнатися їх вміст, навіть якщо вони викрадуть пакети.

**Практичне значення.** Запропонований механізм ефективно протистоїть атакам повторного відтворення, атакам підслуховування, атакам «людина посередині» та імітованим атакам.

**Результати дослідження.** Запропонований механізм демонструє покращення ефективності завдяки криптографії еліптичних кривих.

**Публікації та апробація КР**.

1. Онищенко М., Тимчак А., Понедєльніков Г. Забезпечення захисту кіберфізичних систем за допомогою моніторингу. Матеріали проблемно-наукової міжгалузевої конференції «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2024), Тернопіль, 2024. – С. 46-48.

2. Онищенко М., Тимчак А., Понедєльніков Г. Захист даних у кіберфізичних системах. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. – С. 73-75.

# 1 МЕХАНІЗМИ АВТЕНТИФІКАЦІЇ В ПРОМИСЛОВОМУ ІНТЕРНЕТІ РЕЧЕЙ

## 1.1 Принципи функціонування промислового Інтернету речей

Промисловий Інтернет речей (IIoT) [1, 2] зародився у 1980-х роках, коли деякі компанії почали використовувати технології автоматичного виробництва для збільшення ефективності виробництва та зниження затрат. З розвитком мережевих технологій концепція IIoT поступово визрівала і привернула до себе все більше уваги на початку 2000-х років. Наразі розвиток IIoT поділяється на три етапи.

Перший етап припав на перші дні розвитку Інтернету речей (IoT), коли технологія IIoT в основному була зосереджена на моніторингу окремих пристроїв, включаючи технології автоматизації та датчики. З 2000 по 2010 рік технологія IIoT вступила у другий етап, який характеризувався стрімким розвитком. Популярність хмарних обчислень дозволила зберігати і застосовувати промислові дані для інших суміжних цілей. Крім того, швидкий розвиток штучного інтелекту і машинного навчання дозволив певним пристроям оптимізувати свою роботу. Крім того, розвиток технологій бездротового зв'язку полегшив передачу даних, зібраних термінальними пристроями IoT, через бездротові мережі. Однак у міру того, як IIoT стрімко розвивався, а зручність його використання швидко зростала, було виявлено кілька проблем з безпекою. На відміну від традиційних промислових середовищ, сучасні промислові середовища використовують бездротові мережі як середовище передачі даних між термінальними пристроями IoT і внутрішніми серверами. Однак таким мережевим середовищам не вистачає заходів інформаційної безпеки. Як тільки зловмисники отримують доступ до мережі в промисловому середовищі, вони можуть легко отримати відповідні пакети передачі в мережі і передати пакети на пристрої в мережі.

У сучасному промисловому середовищі більшість передачі даних здійснюється за допомогою протоколу Modbus. Modbus є популярним

протоколом зв'язку завдяки своїй простоті, легкості у використанні та масштабованості, і використовується в багатьох промислових середовищах [3].

Однак Modbus має суттєвий недолік: він передає дані у вигляді відкритого тексту, а це означає, що якщо зловмисники перехоплять пакет, вони зможуть легко розшифрувати його вміст. Це створює значні вразливості конфіденційності під час передачі даних. У термінальних пристроях Інтернету речей, оскільки в сучасному промисловому середовищі відсутня функція взаємної автентифікації між термінальними пристроями Інтернету речей і внутрішніми серверами, сервери, які збирають дані з внутрішньої частини, будуть приймати дані, надіслані з будь-якого пристрою. Це означає, що якщо зловмисники отримають доступ до мережі в такому промисловому середовищі, вони зможуть передавати фальшиві дані на сервер, що призведе до помилок в даних, неточної оцінки стану обслуговування пристрою і непотрібного збільшення витрат. Крім того, використання алгоритму шифрування RSA для реалізації механізму автентифікації в минулому було основним підходом. Найбільшою проблемою алгоритму RSA є тривалий час шифрування та розшифрування, що вимагає значних обчислювальних ресурсів. Однак більшість кінцевих пристроїв в промислових середовищах не мають достатніх обчислювальних ресурсів, що призводить до труднощів або надмірного часу обробки для багатьох з цих пристроїв.

Для вирішення вказаних проблем використовується протокол TLSv1.3 [4], який покращує протокол Modbus з точки зору комунікації. Протокол TLSv1.3 використовується для захисту безпеки мережевої передачі даних. Він використовується для передачі зашифрованих даних для захисту безпеки та конфіденційності переданих даних. Завдяки протоколу TLSv1.3 можна гарантувати, що передані дані не будуть доступні через крадіжку. В даний час кілька веб-сайтів використовують протоколи TLS для підвищення безпеки своїх комунікацій. Для автентифікації термінальних IoT-пристроїв та внутрішніх серверів часто використовується криптографія еліптичної кривої у поєднанні з довіреними токенами (JSON web token або JWT) [5, 6] для реалізації системи

автентифікації між термінальними IoT-пристроями та внутрішніми серверами. Цей метод гарантує, що дані, отримані внутрішнім сервером, надходять з легітимного пристрою, тим самим вирішуючи проблему легальності джерела даних. Кілька систем автентифікації раніше використовували алгоритми шифрування RSA для реалізації процесів автентифікації ідентичності [7]. Криптографія еліптичних кривих була обрана в якості методу реалізації, оскільки вона може досягти того ж рівня безпеки, що і RSA, при меншій довжині ключа. Експериментально продемонстровано, що криптографія еліптичних кривих перевершує RSA з точки зору ефективності та продуктивності і вимагає менше обчислювальних ресурсів, що робить її більш придатною для термінальних пристроїв IoT з обмеженими ресурсами [8].

## 1.2 Безпека і вразливості промислового Інтернету речей

З розвитком IIoT поступово виникають різні проблеми, пов'язані з інформаційною безпекою. Проведемо аналіз проблем безпеки та їх вирішення в IIoT з різних точок зору. Мережева безпека має на меті захистити весь IIoT від вторгнення та атак шляхом впровадження заходів безпеки, таких як налаштування брандмауерів, впровадження протоколів безпеки та встановлення безпечних з'єднань. По-друге, безпека даних має на меті гарантувати, що дані, які передаються в IIoT, не будуть порушені або змінені, і що безпека даних може бути забезпечена за допомогою шифрування і дешифрування. Нарешті, безпека пристроїв IIoT має вирішальне значення для забезпечення безпеки всієї системи IIoT. Необхідно переконатися, що пристрої не піддаються легкому вторгненню або атаці, і що вони можуть захистити свої ресурси і системи, що може бути досягнуто за допомогою аутентифікації і шифрування [9].

Технологія Інтернету речей стала важливою сферою уваги для багатьох компаній сьогодні, однак вона також викликала низку проблем у сфері безпеки, таких як автентифікація особистості та захист конфіденційності даних. Щоб

вирішити ці проблеми, дослідники почали вивчати різні протоколи узгодження ключів і механізми автентифікації особистості, постійно впроваджуючи інновації та вдосконалюючи їх. Серед цих протоколів і механізмів найбільш широко використовується криптографія еліптичних кривих. Вона забезпечує вищий рівень безпеки, менший розмір ключів і швидшу обробку даних. Крім того, хеш-функції є важливими інструментами для реалізації безпечних систем автентифікації, які можуть перетворювати великі обсяги даних у коротші хеш-значення, зберігаючи при цьому унікальність і незворотність хеш-значення. В роботі [8] JWT використовувався для автентифікації особи в мережах з нульовою довірою (ZTN). Оскільки мережі з нульовою довірою передбачають, що жодному пристрою в інфраструктурі мережі не можна довіряти, вони не можуть гарантувати, що власник JWT є очікуваним реєстрантом до реєстрації. Тому існують потенційні проблеми безпеки при використанні JWT для реєстрації одноразових токенів (OTT). Рішення полягає в тому, щоб вбудувати JWT як зашифровані метадані в не взаємозамінний токен (NFT), щоб забезпечити право власності на OTT. JWT шифрується за допомогою відкритого ключа блокчейну очікуваного реєстранта, а блокчейн забезпечує право власності на JWT шляхом його прив'язки до публічної адреси в блокчейні передбачуваного власника. В іншій статті [9] запропоновано механізм автентифікації особи на основі криптографії еліптичних кривих для систем SCADA з використанням OPTIGA Trust X як пристрою, що забезпечує безпечне зберігання ключів ECC. В роботі [10] досліджено автентифікацію ідентичності пристрою за допомогою методів на основі пароля, одноразового пароля (OTP) та сертифіката, проаналізувавши безпеку цих трьох підходів до автентифікації в контексті Інтернету речей (IoT). В роботі [11] розкрито важливість екстреної логістики для забезпечення постачання під час надзвичайних ситуацій і запропонували полегшений протокол безсертифікатної автентифікації (CL-LAP) без білінійного сполучення, який ефективно скорочує час і вартість автентифікації. В роботі [12]. запропоновано протокол автентифікації на основі токенів (TBLUA), який має низькі вимоги до використовуваних

обчислювальних ресурсів та ресурсів зберігання і швидкий час перевірки. Цей механізм підвищує надійність автентифікації особистості на основі технології токенів і підходить для використання в середовищах IoT з обмеженими ресурсами. В [13] розроблено механізм автентифікації на основі JWT, який використовує мітку часу для запису клієнтських запитів і часу відповіді сервера, вирішуючи суперечки щодо дійсності токенів, коли ідентифікатор клієнта відкликається.

На рисунку 1.1 показано архітектуру системи без механізму автентифікації особистості. У промислових середовищах передачі даних без відповідних механізмів автентифікації особи пристрої зазвичай збирають дані через термінальні пристрої Інтернету речей і надсилають їх безпосередньо на внутрішній сервер для подальшої обробки або аналізу. Дані передаються за допомогою протоколу Modbus (рисунок 1.1).

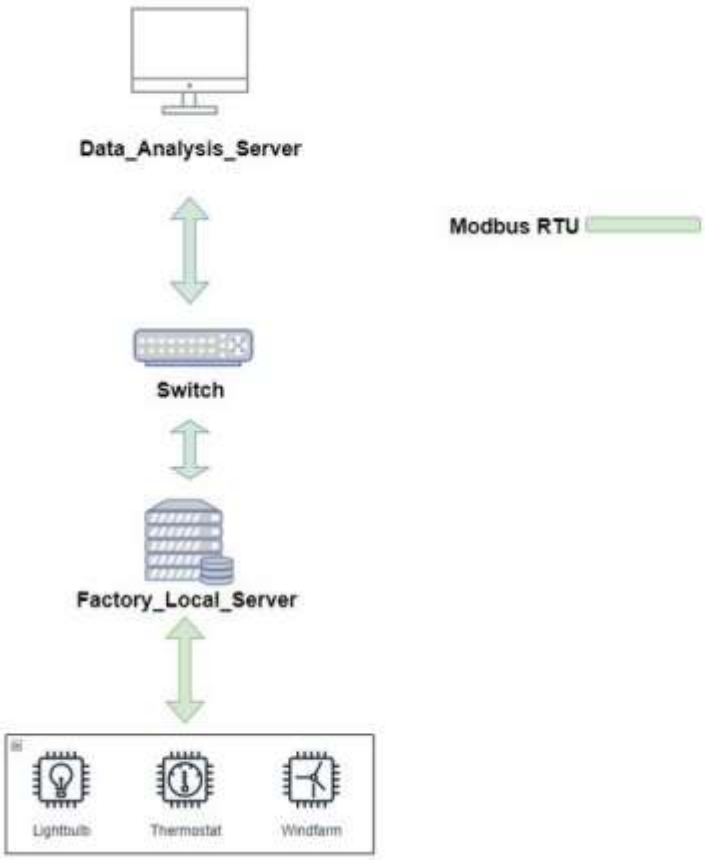


Рисунок 1.1 – Система без механізмів автентифікації в промисловому інтернеті речей

На рисунку 1.2 показано архітектуру системи автентифікації особистості. Система автентифікації особистості забезпечує безпечне середовище передачі даних і захисту конфіденційних даних, що передаються в промисловому середовищі. Нижче наведено опис кожного компонента (рисунок 1.2).

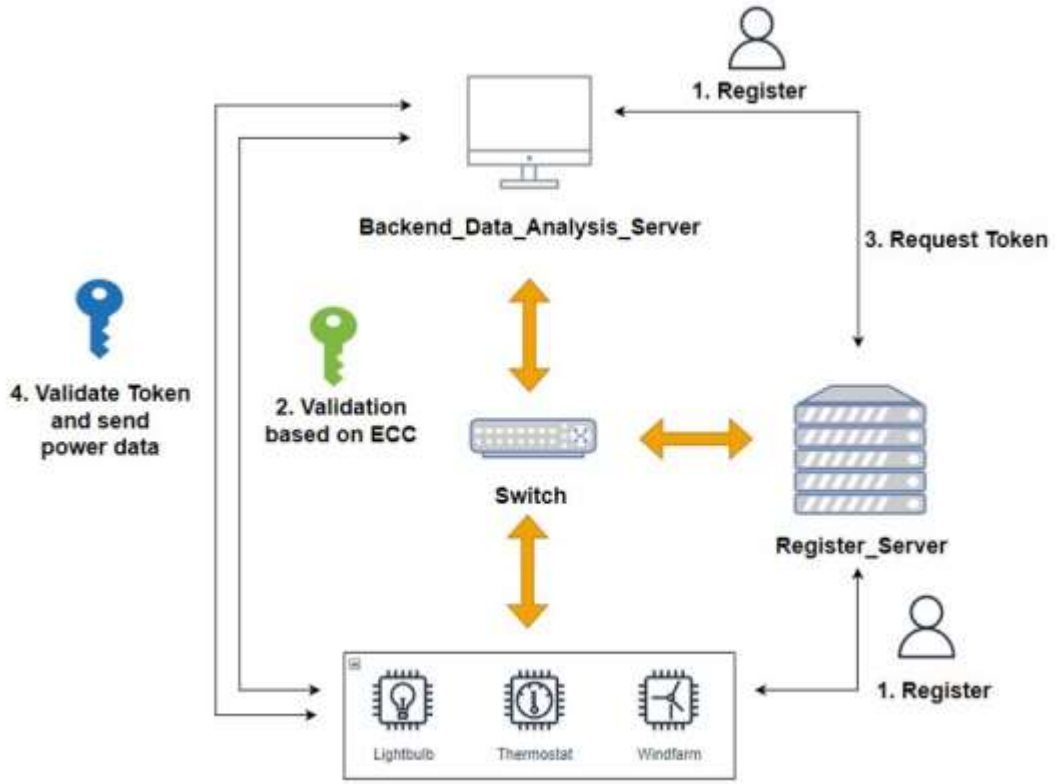


Рисунок 1.2 – Архітектура системи автентифікації особистості

В експериментальному сценарії, довірений реєстраційний сервер виконує дві функції:

- реєстрація ідентичності термінальних пристроїв на довіреному сервері реєстрації;

- генерувати JWT для пристроїв, які пройшли аутентифікацію на першому етапі.

У даній системі автентифікації термінальні IoT-пристрої повинні спочатку запросити реєстрацію на довіреному реєстраційному сервері. Довірений сервер реєстрації генерує T ID для термінального IoT-пристрою на основі запиту на реєстрацію і повертає цей T ID як термінальному IoT-

пристрою, так і внутрішньому серверу аналізу даних. Коли сервер ідентифікації термінального пристрою і внутрішній сервер аналізу даних проходять перший етап механізму перевірки ідентичності, довірений сервер реєстрації генерує легітимні токени, необхідні для подальшої передачі даних між ними, які використовуються на другому етапі механізму аутентифікації для визначення ідентичності легітимних пристроїв і коректності даних про потужність.

Внутрішній сервер аналізу даних використовується для моделювання даних про електроенергію. Сервер виконує дві функції. Датчики після того, як кінцевий IoT-пристрій зареєстрував свою ідентичність, він виконує перевірку своєї легітимності та генерує ключ сеансу. Він перевіряє легітимність токена, переданого термінальним IoT-пристроєм, щоб визначити, чи інформація про потужність у повідомленні походить від легітимного пристрою. Довірений сервер реєстрації повертає T ID термінального пристрою на сервер ідентифікації термінальних пристроїв. Внутрішній сервер аналізу даних виконує автентифікацію на першому етапі, використовуючи T ID та сервер ідентифікації термінального пристрою. Для легітимних пристроїв, які проходять механізм автентифікації на першому етапі, внутрішній сервер аналізу даних надає необхідну інформацію довіреному серверу реєстрації та застосовує набір токенів для легітимних пристроїв, які проходять механізм автентифікації на першому етапі, які використовуються для перевірки ідентичності та легітимності даних на другому етапі.

## 1.3 Стандарти та протоколи IIoT

Протоколи підключення периферії IIoT. Для забезпечення безпечного зв’язку в IIoT існує велика кількість протоколів підключення. На периферії мережі IIoT перевага віддається бездротовим технологіям, серед яких найпоширенішими є протоколи, що створюють бездротові PAN або LAN мережі.

Bluetooth [IEEE 802.15.1] (WPAN). Bluetooth розроблений як протокол зв’язку з низьким енергоспоживанням для коротких відстаней (від 1 до 100 метрів), що працює у частотному діапазоні 2,4 ГГц. Залежно від класу пристроїв, можуть досягатися різні радіуси зв’язку. У своєму базовому стані Bluetooth підтримує чотири режими безпеки: режим 1 є незахищеним, режим 2 забезпечує базову безпеку на рівні сервісу, режим 3 гарантує безпеку на рівні з’єднання, а режим 4 забезпечує безпеку сервісного рівня із шифрованим обміном ключами.

Режими 1 і 3 не надають специфікацій безпекових сервісів для реалізації, що робить протокол та пристрої вразливими до численних загроз, таких як шкідливе програмне забезпечення, атаки типу «відмова в обслуговуванні», перехоплення та спостереження. Режим 2 визначає базові сервіси, як-от автентифікацію, конфіденційність та авторизацію. Режим 4 забезпечує найвищий рівень безпеки завдяки використанню алгоритму SHA256 для хешування, AES-CCM для шифрування та захищеного парування для генерації ключів. Починаючи з версії Bluetooth 2.1, режим 4 став обов’язковим для всіх Bluetooth-з’єднань.

Варіант Bluetooth під назвою Bluetooth Low Energy (BLE) був розроблений для зменшення вартості та енергоспоживання трансиверів, забезпечуючи водночас діапазон зв’язку, еквівалентний класичному Bluetooth. Низьке енергоспоживання та низька швидкість передачі забезпечують діапазони зв’язку від 10 до 1000 метрів залежно від конфігурації мережі та операційного середовища. Максимальна потужність передачі становить 20 дБм (100 мВт).

Одним із обмежень BLE є те, що пристрій може підключатися лише до одного центрального пристрою одночасно через топологію ad hoc. Це не ідеально для IIoT, де вузол повинен підтримувати зв’язок із кількома вузлами "туману" чи шлюзів і передавати повідомлення через комунікаційну інфраструктуру.

BLE доповнює безпекові сервіси класичного Bluetooth, щоб забезпечити

конфіденційність, автентичність та цілісність даних кінцевих точок. На рівні каналу використовується AES128 для шифрування переданих даних. У разі відсутності підтримки AES цілісність і автентичність даних забезпечуються за допомогою CMAC на основі AES128. Для гарантування конфіденційності BLE-пристрої можуть часто змінювати свої адреси, забезпечуючи псевдоанонімність за межами довірених пар пристроїв. Під час процесу парування можлива опція створення довірених відносин між пристроями, у межах яких обмінюються інформація про ідентичність та криптографічні ключі, що дозволяє у подальшому здійснювати автономний зв'язок.

Zigbee 802.15.4 (WPAN). Протокол підключення Zigbee, розроблений Zigbee Alliance, є найпоширенішим розширенням стандарту IEEE 802.15.4 в галузі IoT, WSN та IIoT. Zigbee пропонує два стандарти мереж – Zigbee Pro і Zigbee RF4CE – з різними можливостями залежно від потреб мережевого застосунку. Додаткові функції, як-от автентифікація вузлів та криптографічні сервіси для безпеки зв'язку, реалізовані на основі базового стандарту 802.15.4 з мережевого рівня до рівня підприємства. Деякі версії Zigbee підтримують енергозбереження для продовження терміну служби вузлів.

Zigbee RF4CE орієнтований на створення простих, недорогих бездротових мереж для побутових електронних пристроїв. Протокол RF4CE забезпечує захист від пасивного перехоплення та спотворення повідомлень завдяки використанню криптографічного захисту передачі. Безпекові сервіси, як-от конфіденційність даних, автентичність і захист від повторного використання повідомлень, є частиною визначення протоколу. Під час операцій парування створюються 128-бітні криптографічні ключі, які зберігаються у захищених таблицях парування.

Zigbee PRO призначений для забезпечення мережевої взаємодії пристроїв IoT і реалізується на мережевому та прикладному рівнях стеку протоколів OSI. Він підтримує низьке енергоспоживання для застосунків, що вимагають малопотужного підключення, а також гарантує підтримку великих мереж через використання радіо 802.15.4. Безпека у мережах PRO залежить від захисту

симетричних ключів, застосування захисних механізмів і криптографічних операцій, а також розробки відповідних політик безпеки. Основними засобами є генерація захищених ключів і шифрування передачі за допомогою AES128.

IEEE 802.15.4 (WPAN). Стандарт IEEE 802.15.4 передбачає різні варіанти протоколів для задоволення потреб різних застосунків, але всі вони використовують базові технології 802.15.4a/b. Мета стандарту полягає у забезпеченні базового зв'язку, який може бути розширений іншими протоколами у верхніх рівнях їхніх стеків.

На рівні MAC стандарт 802.15.4 забезпечує численні техніки безпеки, як-от цілісність та конфіденційність даних, використовуючи AES128 та MAC-коди (32, 64 або 128 біт). Основні елементи безпеки включають:

- конфіденційність: опційно підтримується шифрування даних за допомогою 128-бітових ключів AES у режимі Counter (CTR);
- контроль доступу, цілісність та автентичність: використовуються режими безпеки з AES і Cipher Block Chaining (CBC) для створення коду цілісності (MIC) або автентифікації (MAC).
- захист від повторних атак: кожне повідомлення отримує унікальний лічильник, щоб запобігти прийняттю пакетів із застарілими номерами.

Проте стандарт має виклики, пов'язані з правильним вибором підходу до керування ключами. Одним із недоліків є те, що використання одного спільного сесійного ключа не гарантує захисту від повторних атак, а пара ключів не отримала достатньої підтримки. Крім того, стандарт не забезпечує конфіденційності/цілісності для пакетів підтвердження.

NB-IoT (WWAN).NB-IoT (Narrowband IoT), визначений 3GPP, орієнтований на сервіси з низьким енергоспоживанням та малими обсягами даних, що потребують широкого покриття та адаптивного впровадження. NB-IoT базується на LTE, що забезпечує сумісність із наявними системами LTE, які використовують переваги мереж 4G, такі як зв'язок на великих відстанях. NB-IoT пропонує наскрізну безпеку для автентифікованого та захищеного зв'язку.

NB-IoT підтримує три режими роботи:

– автономний режим: використовує частоти GSM (900 або 1800 МГц);

– режим у смузі: використовує сегмент частот LTE, виділений оператором;

– режим у захисній смузі: розміщує NB-IoT між смугами LTE або WCDMA, що потребує синхронізації частот.

З іншого боку, однак, повністю відкритий доступ до не ліцензованих частотних діапазонів створює проблеми безпеки. Деякі зловмисні вузли можуть здійснювати перенаправлення трафіку в не ліцензованих діапазонах, що призводить до втрати конфіденційності для відповідних IoT мереж [14].

WirelessHART (WLAN). На відміну від інших протоколів, які забезпечують персональні мережі, WirelessHART надає локальну мережу, спеціально розроблену для промислових процесів управління [15]. Пропонуючи розширення протоколу HART та сумісність з існуючими проводовими пристроями HART, WirelessHART дозволяє використовувати топологію mesh у промислових контекстах і дозволяє пристроям на краю мережі виконувати маршрутизацію даних між сусідніми пристроями та шлюзами або пристроями fog. Будуючи на основі IEEE 802.15.4, цей протокол забезпечує платформу для інтеграції проводових пристроїв у промисловому процесі з бездротовими комунікаціями в межах IIoT.

Для забезпечення безпеки в мережі HART необхідно гарантувати конфіденційність і цілісність інформації, автентифікацію пристроїв та доступність інформації. WirelessHART надає цілісність інформації за рахунок механізмів, успадкованих від протоколу 802.15.4 [15]. Крім того, в протоколі WirelessHART інтегровані коди автентифікації повідомлень (MIC) та AES128 шифрування для забезпечення автентифікації та перевірки інформації на рівні мережі за допомогою мережевих та сеансових ключів [2]. Доступність з'єднання може бути загрожена перешкодами з боку інших бездротових комунікаційних протоколів, хоча вже було показано, що WirelessHART застосовує кілька механізмів для забезпечення сумісності в частотному діапазоні з іншими мережевими комунікаціями.

Два додаткових протоколи зв'язку можуть використовуватися на рівні периферії IIoT, працюючи на рівнях каналу та мережі.

LoRaWAN (WWAN). LoRaWAN є протоколом вищого рівня для LoRa, що визначає конфігурацію та процес передачі даних до Мережевого сервера (NS) через Інтернет-протокол [6]. LoRaWAN забезпечує конфіденційність інформації, застосовуючи AES128 для процесів шифрування/розшифрування, MAC операції для забезпечення цілісності даних і Over-The-Air-Activation (OTAA) для загальної автентифікації пристроїв [16].

Різні проблеми безпеки були виявлені в LoRaWAN v1.0 [8], деякі з яких були усунуті в v1.1 [16]. Обидва варіанти, LoRaWAN v1.0 і LoRaWAN v1.1, виявилися вразливими до складних атак глушіння, таких як вибіркові атаки глушіння [9], через бездротові комунікації. Деякі залишкові вразливості безпеки в LoRaWAN v1.1 були виявлені авторами в як:

Криптографічні примітиви. Раніше дослідники виявили суттєві недоліки в AES за використання електронного кодового блокування (ECB) для шифрування повідомлення Join-accept в LoRaWAN v1.1 [17].

Попереднє завантаження ключів. Властивість контролю за ключами забезпечує, щоб жоден партнер у мережі не міг встановити спільний ключ на попередньо визначену величину з наміром обмежити контроль над іншою стороною.

Довіра інфраструктури. В [18] продемонстровано деякі слабкі місця LoRaWAN v1.0, такі як атака з інвертування біту, де зловмисник може змінити вміст повідомлення між мережевим сервером і сервером застосунку, що все ще актуально для v1.1.

Роумінг. Роумінг є однією з головних проблем LoRaWAN v1.1 через вразливість до атак типу MITM під час передачі даних [3].

ISA100.11a (Data Link). У вересні 2009 року Міжнародне товариство автоматизації (ISA) представило промислову бездротову систему ISA100.11a. ISA100.11a намагається забезпечити безпечну і надійну бездротову комунікацію для супервізорних контрольних застосунків і працює як міст між

канальними і мережевими протоколами. Подібно до WirelessHART, ISA100.11a використовує симетричне шифрування AES з 128-бітним ключем в режимі лічильника через Cipher Block Chaining-Message Authentication Code (CBC-MAC). ISA100.11a може забезпечити прямі підключення в режимі peer-to-peer, на відміну від WirelessHART. Менеджер безпеки в ISA100.11a має більш точні ролі, ніж його аналог в WirelessHART; він включає автентифікацію пристроїв на етапі приєднання, а також процес управління ключами, що включає повторне завантаження ключів, архівацію і відновлення ключів. На відміну від WirelessHART, для етапу приєднання в ISA100.11a застосовуються асиметричні ключі. Подібне шифрування на кінцевих етапах, як у WirelessHART, реалізується на рівні транспортного шару. У 2014 році були впроваджені нові процедури для поліпшення безпеки ISA100.11a в контексті знищення даних, фальсифікації, підробки та атак повтору [19].

6LoWPAN (Мережевий рівень). Деякі IIoT мережі з'єднуються з Інтернетом за допомогою IPv6 через 6LoWPAN [20], що визначає IP-комунікацію для мереж з обмеженими ресурсами. IPSEC [21] використовується для надання послуг безпеки на мережевому рівні в традиційному Інтернеті. Однак важка та складна природа IPSEC робить його непридатним для використання в середовищах IIoT. У [9] було запропоновано механізм інтеграції IPSEC в промислові IoT мережі, розширюючи оригінальну реалізацію таким чином, щоб це було можливим для малих пристроїв. В [9] продемонстровано, що IPSEC, налаштований для IoT, має кращу масштабованість порівняно з рішеннями на рівні каналу зв'язку, оскільки зростає розмір даних і кількість стрибків. IPSEC у IIoT також дозволяє забезпечити End-to-End (E2E) шифрування [4], чого неможливо досягти за допомогою традиційних механізмів безпеки каналу 802.15.4.

Усі проаналізовані протоколи здатні передавати дані в межах 2.4 ГГц діапазону, що робить захист від колізій і перешкод важливим аспектом для проектування IIoT мережі, щоб забезпечити доступність передач пристроїв. Однак це також означає, що комунікація між різними пристроями та їх

взаємодія краще досягаються без необхідності введення частотної модуляції для перетворення передач на спільний діапазон. Пряма залежність між споживаною потужністю трансиверів та досяжною дальністю протоколу означає, що буде потрібно детальний аналіз проектування мережі для розгортання IIoT. Оскільки топологія, яку підтримує протокол, також впливає на розширену дальність передачі, при виборі протоколу з'єднання слід враховувати кількість пристроїв, відстань між ними, здатність розширювати цю відстань та допустиме споживання потужності мережі для досягнення прийнятного компромісу між вартістю і ефективною роботою мережі.

## 1.4 Аналіз вразливостей промислового Інтернет речей

Рішення IIoT надають організаціям численні переваги, зокрема, підвищують операційну ефективність, зниження витрат і підвищення продуктивності. Завдяки автоматизації завдань, оптимізації процесів та ефективного управління ресурсами організації можуть мінімізувати простої оптимізувати та підвищити робочі процеси та досягти вищого рівня загальної ефективності. Використання дані, зібрані з підключених пристроїв і датчиків, організації можуть приймати обґрунтовані рішення, завдяки яким, оптимізувати розподіл ресурсів, виявляти та усувати вузькі місця. Результатами є підвищення продуктивності, зниження витрат і конкурентна перевага на ринку [22].

Однак пристрої IIoT так само вразливі, як і будь-які інші пристрої, підключені до Інтернету. Впровадження більш потужного і складного обладнання, такого як мікропроцесори, ускладнює вирішення проблем кібербезпеки та конфіденційності [8]. Приклади атак на промислові системи управління (ПСУ) включають розподілені системи управління, програмовані логічні контролери, диспетчерський контроль і збір даних, а також людино-машинні інтерфейси (Human-Machine Interface, HMI).

ІКС та HMI можуть бути вразливими до різних типів атак, які можуть мати серйозні наслідки для промислових операцій [23, 24].

1. Шкідливе програмне забезпечення та програми-вимагачі. Зловмисники можуть розгортати шкідливе програмне забезпечення або програми-вимагачі, спеціально призначене для систем ICS або HMI. Ці шкідливі програми можуть порушити функціонування критично важливих промислових процесів, порушити цілісність системи і навіть вимагати гроші в обмін на продовження нормальної роботи.

2. Розподілена відмова в обслуговуванні (DDoS). Така передбачає перевантаження системи потоком трафіку, що призводить до того, що система не реагує на запити або виходить з ладу. Коли зловмисник успішно запускає DDoS-атаку на систему ICS або HMI, він може порушити керуючі сигнали, затримати час відгуку або вивести систему з ладу, що призведе до перебоїв у виробництві або ризиків для безпеки.

3. Несанкціонований доступ і контроль. Якщо зловмисник отримує несанкціонований доступ до системи ICS або системи HMI, він може маніпулювати параметрами керування, змінювати уставки або видавати несанкціоновані команди. Несанкціоновані команди. Це може призвести до відхилень у технологічному процесі, пошкодження обладнання, загрози безпеці або навіть катастрофічних інцидентів.

4. Внутрішні загрози. Інсайдери зі зловмисними намірами, такі як незадоволені працівники або підрядники, можуть зловживати своїми привілеями. Підрядники, можуть зловживати своїм привілейованим доступом до систем ICS або HMI. Вони можуть навмисно втручатися в налаштування керування, саботувати обладнання або викрадати конфіденційні дані спричиняючи значні збої в роботі або порушуючи цілісність системи.

5. Соціальна інженерія. Зловмисники можуть застосовувати різноманітні методи соціальної інженерії, щоб залучити авторизованих користувачів до розголошення певної конфіденційної інформації або / та надання несанкціонованого доступу.

Наприклад, фішингові електронні листи чи телефонні дзвінки можуть обманом змусити працівників розкрити облікових даних для входу або виконання шкідливих команд, які можуть бути використані для компрометації ICS або HMI-системи.

6. Атаки на ланцюжок поставок: Системи ICS або HMI можуть бути атаковані через вразливості в ланцюжку поставок. Зловмисники можуть порушити цілісність обладнання, програмного забезпечення, або мікропрограми під час виробництва, розповсюдження або встановлення. Це може призвести до впровадження шкідливих компонентів або вразливостей, які можна використати системи. Важливо зазначити, що наведені приклади не є вичерпними, а конкретні вектори та методи атак можуть відрізнятися залежно від конкретної системи ICS або HMI, що використовується використання. Організаціям необхідно оцінювати та зменшувати ризики на основі своїх унікальних операційних вимог та потенційних загроз, з якими вони стикаються. Групування вразливостей за категоріями допомагає розробляти та впроваджувати на практиці заходів з мінімізації ризиків, оскільки всі СУІБ пов'язані з інформаційними технологіями (IT) та операційними технологіями (OT). Технологіями (OT) ці категорії поділяються на політичні та практичні проблеми і вразливості, виявлені на різних платформах (таких як апаратне забезпечення, операційні системи та додатки ICS). Вразливості можна згрупувати як проблеми політики, практичні проблеми, апаратні вразливості, вразливості операційних систем, вразливості додатків ІКС тощо, тощо. Ці категорії можуть допомогти у визначенні заходів щодо пом'якшення наслідків і пріоритетів у сфері безпеки [25]. Кожне середовище ІКС може мати недоліки, залежно від того, як воно налаштоване і для чого вони призначені для виконання. Ще одним фактором є розмір середовища ICS; чим більше середовище, тим вища ймовірність того, що може статися помилка. Середовище ICS, яке модернізувало свої застарілі системи і додало нові технології, такі як промисловий Інтернет речей (IIoT), також може мати більше вразливостей, якими можуть скористатися зловмисники.

# 2 ЗАГРОЗИ КОНФІДЕНЦІЙНОСТІ В ПРОМИСЛОВОМУ ІНТЕРНЕТІ РЕЧЕЙ

## 2.1 Дослідження загроз в промисловому IoT

Основні занепокоєння щодо захисту конфіденційності даних у промислових сферах переплітаються з більш загальними занепокоєннями щодо ризиків, пов'язаних з кожним сучасним мережевим пристроєм [8]. Загалом, найбільш базовими і поширеними загрозами конфіденційності, пов'язаними з IIoT, є наступні: ідентифікація та авторизація, локалізація та відстеження, профілювання, життєвий цикл обладнання, атака на інвентаризацію та зв'язок. Розглянемо вказані загрози детальніше.

1. Ідентифікація та авторизація. Це безпосередньо пов’язано з концепцією конфіденційності особистості. Це стосується спроб знайти кореляції між даними, які можна використати, виявляти, ідентифікувати та зловмисно копіювати застосування профілів (наборів пов’язаних дані) для персоналізації та запам'ятовування секретної, промислової інформації. Методи, такі як модуль ідентифікації абонента (SIM) і модуль ідентифікації машини (MIM), запропоновані в [26], є суттєвими рішеннями, які заслуговують на увагу. Проте ці підходи використовують до роботи в централізованих управлінських мережах. Водночас це непросто керувати послугами ідентифікації та стандартизацією у розподілених топологіях, і це стосується архітектури авторизації віддалених кінцевих користувачів за допомогою розподілених розумних шлюзів, які є на основі протоколу рукостискання Datagram Transport Layer Security (DTLS). Крім того, атаки на IIoT компрометують авторизований доступ до промислових систем, а також в результаті одна така проблема безпеки може погіршити пов’язані служби програми-вимагачі також призводить до несправності пристроїв IIoT і краде конфіденційну інформацію користувачів даних. Крім того, якщо багато інтелектуальних пристроїв IIoT не можуть шифрувати дані користувача, зловмисне програмне забезпечення зможе

їх викрадати. Пристрої IIoT використовують мережу, яка не перетворює дані на код, щоб запобігти несанкціонований доступ до пристрою.

2. Локалізація та відстеження. Це безпосередньо пов’язано з концепцією конфіденційності розташування [8]. Галузь може вибирати місця, які вона обирає для виконання своїх економічних функцій на вибір відповідного місця впливає кілька факторів, особливо природа та характеристики промислової діяльності, яку здійснює підприємство (наприклад, видобуток сировини або вирощування, виробництво проміжної або кінцевої продукції, надання послуги) і пов'язані з цим витрати на виробництво, збалансовані з собівартістю фізичної дистрибуції на цільових ринках і важливості близькості до споживачів як основи для встановлення конкурентних переваг над конкуруючими постачальниками. Деякі місця можуть бути кращими через їхні виробничі переваги, наприклад, через нижчу вартість робочої сили, наявність інвестиційних субсидій, забезпечення кваліфікованою робочою силою та паралельний доступ до відповідних об'єктів. Подібним чином необхідно розташувати багато видів діяльності з обслуговування у зонах знаходження клієнта та навколо нього. У той же час деякі постачальники можуть бути зацікавленими в роботі разом зі своїми основними клієнтами для синхронізації виробництва вхідні вимоги краще.

З іншого боку, висока ціна роздачі, особливо у випадку великогабаритної продукції з низькою доданою вартістю або міжнародному контексті, встановлення тарифів і квот на імпорт, створюють істотні вимоги для відповідної продукції орієнтованої на ринок.

Середовище IoT було запропоновано в [27] шляхом вбудовування програмного забезпечення конфіденційності в пристрої GPS, яке гарантує, що пристрої IoT та їхні адміністратори мають детальну інформацію та контроль за зміною своєї позиції. Крім того, безпека даних, отриманих із багато пристроїв IIoT безпосередньо пов’язані з іншими проблемами безпеки та конфіденційності даних від незахищених хмарних інфраструктур, веб-додатків і мобільних середовищ. Як в результаті необхідно дотримуватися правил безпеки

передачі даних у кожному домені, що існують заходи для визначення шляху, з пристрою якого передається дані. Також важливо видалити нерелевантні дані та дані, які не мають відношення до фактичної операції. Хоча дотримання численних регуляторних структур стає складним, коли накопичується багато даних, інфраструктура повинна бути перенесена з окремими службами для керування даними, пов'язаними з взаємопов'язаними пристроями і середовища [28].

3. Профілювання. Загроза полягає в порушенні конфіденційності та моніторингу осіб у зв'язку з конкретними промисловими процесами. Відповідно, це може стосуватися ідентифікації, збір та обробка інформації, отриманої від послуг або еталонних моделей, яка може становити промислову таємницю. Характерними рисами постійного занепокоєння щодо захисту пристроїв IoT від загроз профілювання є спроби посилити конфіденційність у пристроях RFID, сенсорних системах, бездротовій мережі і технології управління ідентифікацією для підвищення конфіденційності або шифрування технології [29].

4. Життєвий цикл обладнання. Промислові пристрої в більшості випадків переробляються та використовуються повторно. Тому конфіденційна інформація, журнали пристроїв і дані зберігаються в пам'яті або сховищі медіа ймовірно потраплять у чужі руки з непередбачуваними наслідками. Для конкретних загроз, галузь повинна розробити та реалізувати єдину політику для управління промисловим устаткуванням, а також застосовувати методику за видалення даних локально або в розподілених системах обробки інформації які включають перший і другий сайти, які можуть складатися з відповідної інформації виробничих дільниць. Крім того, апаратне забезпечення IIoT забезпечує безпеку та конфіденційність загрози через неадекватне тестування та відсутність процесів оновлення [28]. Виробники пристроїв IIoT, бажаючи випускати різноманітні пристрої, не враховують безпеки і проблеми з оновленням зазначених пристроїв, оскільки вони потребують ретельного тестування та, отже, додаткові витрати. Ці несправності підвищують

можливість безпеки та атаки на конфіденційність під час випуску в реальну промислову інфраструктуру [29].

5. Атака на інвентаризацію. Напади на інвентаризацію – це незаконне отримання інформації про наявність і атрибути обладнання. Крім того, з впровадженням машин для машинного, зору інтелектуальні пристрої можуть бути піддані сумніву щодо їх енергії, швидкість зв'язку, час реакції та інші відмінні характеристики, які можуть бути використані для ідентифікації їх типу та моделі з урахуванням накладених обмежень легальними або імовірно легальними організаціями. Таким чином, злі особи, які порушують конфіденційність можуть скласти перелік гаджетів у певній будівлі чи заводі, а також інформацію про те, як працює кожен пристрій. Також були запропоновані криптографічні рішення для механізмів агрегації. Безпечний протокол агрегації відповідає вимогам IoT. Він оцінює свою ефективність у світлі різних конфігурацій системи, вплив бездротового каналу на частоту помилок пакетів і методи приватного спілкування.

6. Зв'язок. Ця загроза полягає у з’єднанні різних раніше розділених систем що поєднують дані і джерела. Крім того, для забезпечення безперебійної роботи, для пристроїв IIoT важливо мати однорівневу мережу, яка дозволить їм функціонувати ефективно. Для цього важливо мати високоякісну відкриту мережеву систему. Цей конкретний фактор у мережах IIoT створює бар’єр безпеки. Тому промислові підприємства повинні ретельно оцінити свою політику безпеки, щоб визначити, що пристрої IIoT не вразливі до загроз. Крім того, провайдери повинні розуміти важливість належного налаштування мережевого пристрою та послуг щодо конфіденційності даних, які передбачають різні процеси, наприклад ефективне видалення конфіденційних даних інформація через сегрегацію даних [30].

На рисунку 2.1 зображено архітектуру, яка успішно прогнозує та оцінює умови, пов’язані з загрозами, у промисловій екосистемі, забезпечуючи при цьому конфіденційність і секретність

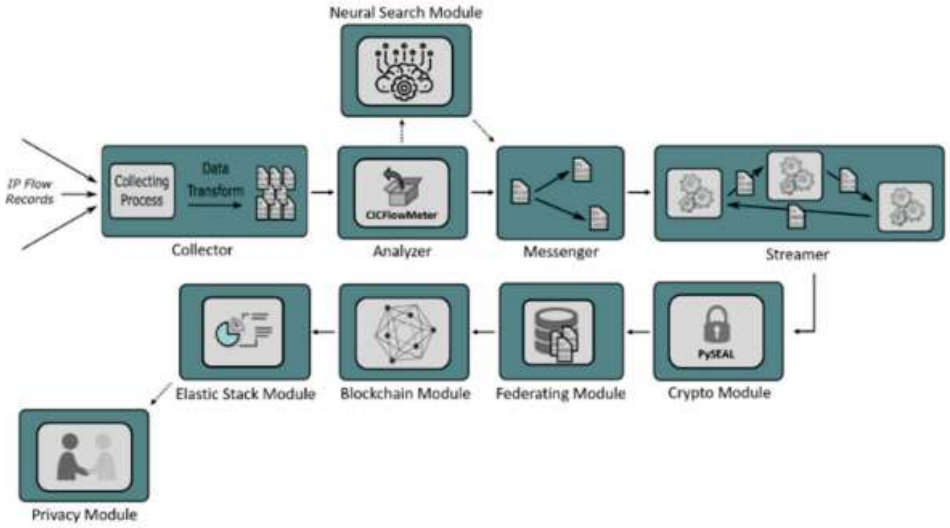


Рисунок 2.1 – Структура промислової системи IoT

Наведена вище високорівнева архітектура конкретної промислової системи запроваджує інтелектуальний механізм контролю для виявлення аномалій у галузі 4.0. Комунікаційна мережа, заснована на трьох основних принципах. Конфіденційні дані – не передаються через канали зв'язку або зберігається в центральній точці атаки, і алгоритми навчання постійно оновлюють свою прогностичну здатність. Пр. цьому значна частина відповідальності за захист належить виробникам обладнання. Часто механізми і стандарти сумісності, що стосуються безпеки пристроїв IioT або розглядаються як другорядний чинник [30]. Зазвичай це пов’язано з вимогою до коротких термінів впровадження пристрою IoT, спрощення конструкції механізмів його роботи, і зменшення його загальної вартості. Тому ті, хто бере участь у процесах доставки IIoT, повинні враховувати конфіденційність і розробляти інтерфейси керування конфіденційністю, вбудовані в кінцеву точку та Інтернет.

Інтерфейс продукту або послуги. Ця технологія повинна дозволити галузі користувачів розуміти, які функції конфіденційності використовуються екосистемою, які умови обслуговування є, і чи можливо дезактивувати розкриття цієї інформації бізнес-партнерів або конкурентів. Система управління інформацією забезпечить користувачам, які мають право та

здатність регулювати інформацію, яку вони розкривають про себе та їхнє фізичне оточення.

У світлі згаданого вище IIoT створює унікальні проблеми конфіденційності та загрози через велику кількість даних, що генеруються, зберігаються та обробляються в промислових середовищ.

## 2.2 Основні вимоги та рекомендації для забезпечення конфіденційності промисловому IoT

Деякі з найпоширеніших загроз конфіденційності в IoT включають витік даних, кібератаки, внутрішні загрози, відсутність прозорості та незахищені комунікації. Щоб усунути ці загрози конфіденційності, IIoT має впроваджувати відповідні технічні та організаційні заходи для забезпечення захисту конфіденційної та особистої інформацій. Ці заходи можуть включати шифрування, контроль доступу, регулярне навчання працівників, оцінки вразливості та постійний моніторинг систем і пристроїв IIoT. Впроваджуючи ці заходи, системи IIoT можуть краще захиститися від загроз конфіденційності та забезпечити цілісність, конфіденційність та доступність секретної інформації.

Вимоги конфіденційності передбачають дотримання відповідних законів про конфіденційність, галузевої політики, повідомлення та договірні зобов’язання, пов’язані зі збором, записом, використанням, зберіганням, обробкою, спільним використанням, охороною, безпекою (технічною, фізичною та адміністративною), видаленням, знищення, розкриття або передача конфіденційних персональних даних [8].

Основні вимоги та рекомендації, яких слід дотримуватися в промисловому середовищі для забезпечення конфіденційності.

1. В ідеалі заходи щодо захисту конфіденційності мають бути сплановані та реалізовані у процесі проектування товарів, послуг або систем Інтернету речей.

2. Оцінювання. Оцінка впливу на конфіденційність має допомогти забезпечити безпечний метод аналізу того, як особиста інформація збирається, зберігається, захищається, передається, поводження та утилізація, регулюється цим розділом.

3. Відповідність законодавству. Для моніторингу відповідності слід оцінити відповідні законодавчі або нормативні вимоги.

4. Обмеження використання. Слід передбачити необхідну роботу для забезпечення доступу до необхідної фізичної чи електронної системи безпеки обмежено лише авторизованим особам і для цілком дозволених цілей [18].

5. Заходи безпеки при зберіганні. Сховища, озера даних і бази даних, де збирається та зберігається персональна інформація, повинні бути захищені з точки зору фізичної та логічної безпеки.

6. Безпечний зв'язок. Дані, що передаються між системами або компонентами, і загалом, комунікації в середовищі IoT слід захищати від несанкціонованого розголошення або доступу.

7. Прозорість. Особи, особиста інформація яких може бути зібрана, повинні бути повідомлені про причину збору та спосіб використання цієї інформації. Там також повинні бути механізми, які можуть виявити можливі витоки персональних даних.

8. Політика збереження даних. Має бути політика, яка визначає період зберігання персональних даних, способи знищення таких даних та порядок забезпечення, що видалена інформація не підлягає відновленню [20].

Щоб усунути загрози конфіденційності в IoT, важливо встановити чіткі вимоги до конфіденційності та впровадити відповідні заходи для забезпечення відповідності застосовуваним законам та правила захисту даних. Вимоги щодо конфіденційності та пропозиції щодо реалізації IoT повинні включати: оцінка впливу на захист даних, конфіденційність за проектом, шифрування та контроль доступу та інші.

1. Оцінка впливу на захист даних (DPIA). Організація DPIA може допомогти визначити потенційні ризики конфіденційності та переконатися, що вжито необхідних заходів для їх пом’якшення.

2. Конфіденційність за проектом. Реалізація принципів конфіденційності за проектом може допомогти забезпечити конфіденційність інтегровану в розробку систем і пристроїв IIoT з самого початку.

3. Шифрування та контроль доступу. Шифрування та контроль доступу можуть допомогти захистити конфіденційну інформацію та персональні дані від несанкціонованого доступу чи розголошення.

4. Регулярні оцінки вразливості. Регулярні оцінки можуть допомогти виявити та усунути вразливості безпеки та конфіденційності в системах і пристроях IoT.

5. Навчання співробітників. Забезпечення того, щоб співробітники були навчені вимогам конфіденційності та найкращим практикам можуть допомогти мінімізувати ризик внутрішніх загроз і покращити загальну ситуацію з конфіденційністю організації.

6. Відповідність законам і нормам про захист даних. Відповідність із законами та правилами захисту даних, такими як GDPR [23] у Європейського Союзу, має важливе значення для захисту прав на конфіденційність окремих осіб і організації, що беруть участь в операціях IIoT.

7. Регулярний перегляд політики та процедур конфіденційності. Регулярний перегляд та оновлення політик і процедур конфіденційності може допомогти переконатися, що вони актуальні та ефективний у вирішенні нових загроз і ризиків.

Впроваджуючи ці вимоги та пропозиції щодо конфіденційності, впровадження IIoT може краще захистити від загроз конфіденційності та забезпечити безпечне та відповідальне використання технології та даних в промислових умовах. Крім того, промислові партнери запропонують проривні бізнес-моделі для персоналізації та повної автоматизації безпечних і приватних процесів.

Прийняття безпечного та конфіденційного промислового Інтернету речей у рішеннях Industry 4.0 створює певні проблеми для компаній, що прагнуть плавно інтегрувати новітні технології у свої виробничі процеси. Цей виклик головним чином обертається навколо готовності та зрілості компаній до інкорпорації технології безпеки в межах їхньої виробничої інфраструктури, що охоплює як безпечну структуру, так і служби збереження конфіденційності, завдяки успішному застосуванню принципу збереження конфіденційності.

Технології IIoT, можуть створити основу для гнучкого виробництва, дозволяючи їм оперативно реагувати на динамічні зміни та вимоги ринку. Результати дослідження пропонують комплексний аналіз IIoT та його інтеграції з інтелектуальними системами в екосистемі Industry 4.0. Це проливає світло на поширені проблеми безпеки, з якими стикаються розгортання IIoT, підкреслюючи вкрай важливу потребу захисту конфіденційності в цих системах.

В підсумку, можна сказати, що розуміння потреб у конфіденційності та ризиків екосистеми Інтернету речей, є важливим для організацій, щоб зрозуміти та розробити правила, інструкції та стратегії, які забезпечують безпеку та конфіденційність технологій та його кінцевих користувачів.

## 2.3 Безпечне підключення в промисловому IoT

Для забезпечення безпечного зв'язку в промисловому Інтернеті речей потрібна злагоджена робота численних протоколів безпеки, апаратного забезпечення та інших компонентів. Вимоги до безпечного підключення, визначені в IIC (Industrial Internet Consortium) та OpenFog Consortium, мають багато спільного, що дозволяє використовувати обидва стандарти як взаємодоповнюючі джерела для розробки стратегії безпечного підключення для IIoT. Значний ступінь збігу спостерігається як у вимогах, так і в технологіях впровадження. Використання подібних або ідентичних технологій для

гарантування послуг безпеки для периферійних пристроїв і забезпечення безпеки з'єднань підкреслює, що безпека підключення є розширенням безпеки пристроїв на периферії. Це також обґрунтовує необхідність забезпечення сильної безпеки периферійних пристроїв з моменту створення мережі IIoT.

Розширення цих технологій впровадження також дозволяє розподіляти навантаження щодо виконання вимог безпеки між двома зонами мережі, створюючи резервні механізми захисту на випадок порушення безпеки.

1. Аутентифікація. Фреймворки IIC та OpenFog Consortium рекомендують створення кореня довіри (root of trust), з якого можуть генеруватися облікові дані для аутентифікації, перевірки цілісності та непідробності. Корінь довіри забезпечує початкову впевненість у роботі системи, що згодом сприяє впевненості у тому, що особи, які запитують доступ до мережі, є авторизованими і не можуть отримати доступ до ресурсів, бо не мають права.

Корінь довіри також сприяє забезпеченню цілісності мережі, встановлюючи базові критерії для виявлення та запобігання спробам несанкціонованого доступу. Механізми аутентифікації, засновані на фізичній близькості сутностей, також пропонуються для IIoT.

Для створення безпечного мережевого кореня довіри фреймворк рекомендує використання апаратного кореня довіри (HRoT), такого як апаратний модуль безпеки (HSM) або модуль довірчої платформи (TPM).

HSM – це системи-на-кристалі (SoC), які забезпечують базові криптографічні функції, такі як шифрування, розшифрування, генерація ключів, цифровий підпис та хешування, а також забезпечують фізичну стійкість до втручання і ізоляцію криптографічних функцій.

Активні дослідження в цій галузі включають розробку обладнання, стійкого до втручань, шифрованих прошивок для ПЛІС, фізично неклонованих функцій (PUF) і апаратних баз довірених обчислень (TCB) для вбудованих пристроїв з низьким енергоспоживанням.

Як і у випадку з безпекою периферійних пристроїв, використання апаратних чипів безпеки як єдиного рішення може скоротити ефективний

термін служби захищеної мережі. Це зумовлено тим, що групи стандартів постійно оновлюють існуючі стандарти. Оскільки мікросхеми інтегровані в периферійні вузли, їх заміна є складною, а для великих мереж таких операцій вимагається значні витрати, що робить їх економічно недоцільними.

Вибір відповідного механізму фізичного захисту та протоколу комунікації між чіпами стає критично важливим, адже потрібно забезпечити захист шляхів комунікації між MCU (мікроконтролер) та криптографічним акселератором, щоб уникнути витоку конфіденційної інформації.

2. Контроль доступу. Механізми контролю доступу є необхідними для захисту систем IIoT. Дослідники нещодавно визнали, що контроль доступу має бути адаптований до специфічних особливостей IoT. Наприклад, дослідники розробили платформу на основі системи моніторингу транспортних засобів Open Vehicle Monitoring System (OVMS), яка дозволяє отримати незаконний доступ до внутрішньої мережі електромобіля.

Крім того, відповідно до досліджень, зловмисники успішно отримали доступ до мільйонів вузлів IoT, використовуючи їх як ботнет-зомбі для здійснення DDoS-атаки на DNS-сервери компанії Dyn Inc.

Методи впровадження контролю доступу, сегментації мережі, ізоляції даних і комунікацій в IIoT залишаються переважно науковими розробками. Вони мають багато недоліків, які слід розв’язувати в майбутньому, і бракують єдиного стандартного підходу для забезпечення безпеки у загальних мережевих застосунках.

Шифрувальні механізми, засновані на CP-ABE (атрибутно-базоване шифрування), можуть також використовуватись для реалізації правил контролю доступу. Групуючи та налаштовуючи пристрої у різні групи доступу, дані можна шифрувати таким чином, щоб лише пристрої з певними правами доступу могли їх розшифрувати. Такі схеми дозволяють досягти кількох цілей одночасно, зокрема забезпечити конфіденційність даних та виконання правил контролю доступу.

3. Управління ідентифікацією. Рішення для управління ідентифікацією необхідні для розв'язання проблем, пов'язаних із іменуванням, адресацією та пошуком пристроїв IIoT. Управління ідентифікацією в IIoT набуває особливого значення, оскільки зловмисний пристрій може змусити систему виконувати небезпечні дії. Ця проблема багатогранна й охоплює такі аспекти:

- використання коректних механізмів іменування та адресації;
- визначення ідентичності сутностей;
- зберігання релевантної інформації про сутності;
- визначення інтерфейсів для доступу до сутностей;
- визначення ролей та зв’язків між сутностями.

Однією з основних проблем є величезна кількість пристроїв IIoT, що ускладнює використання традиційних схем адресації та іменування, таких як IP-адреси або доменні імена. Інші фактори, що ускладнюють ситуацію, включають мобільність пристроїв (зміна імені чи адреси), крадіжку ідентичності та необхідність масштабованого механізму пошуку пристроїв.

Існує безліч рішень для управління ідентифікацією, наприклад, OpenID для управління ідентифікацією та Library Alliance для управління довірою. Майбутні рішення повинні вирішувати проблеми управління ідентифікацією пристроїв у пропрієтарних мережах, створення масштабованих механізмів іменування та адресації для постійно зростаючої кількості пристроїв, а також швидкого пошуку пристроїв для задоволення строгих вимог часу в додатках IIoT.

Комплексні рішення для управління ідентифікацією, які зберігають конфіденційність та враховують питання анонімності, доказів із нульовим розголошенням і автентифікації, вже були запропоновані. Розробка схожих рішень, адаптованих для конкретних розгортань та вимог IIoT, є бажаною для створення безпечного та конфіденційного середовища.

4. Управління ключами. Захищений обмін і зберігання ключів є проблемою, яка виникає на різних рівнях протоколів зв’язку, де криптографічні

механізми забезпечують безпеку. Це завдання ускладнюється через обмежені ресурси пристроїв IIoT і їхню фізичну доступність для зловмисників.

Рішення для управління ключами, засновані на публічній криптографії, є неприйнятними для IIoT через складні обчислення, властиві публічній криптографії.

Для подолання проблем обмежених обчислювальних ресурсів пристроїв IIoT було запропоновано рішення, засновані на легковаговій криптографії. Проте підтримання певного рівня безпеки та забезпечення того, щоб примітиви управління ключами були обчислювально ефективними навіть для найменших пристроїв, є складним завданням.

Фізична доступність пристроїв також створює нові виклики безпеці, які не характерні для звичайного Інтернету, де комп'ютери зазвичай недоступні фізично для зловмисників.

Схема управління ключами повинна включати механізми захисту від втручання, а також механізми виявлення і відновлення після успішних атак.

5. Конфіденційність потоку даних. Використання криптографії в архітектурі зв'язку дозволяє шифрувати дані сенсорів, які генеруються та передаються з периферії мережі. Криптографічні послуги для забезпечення конфіденційності даних і комунікацій можуть реалізовуватися як у програмному забезпеченні, так і в апаратному забезпеченні, із використанням протоколів зв'язку, які вже підтримують конкретні криптографічні алгоритми.

Згідно з вимогами, запропонованими OpenFog Consortium, пристрої та протоколи зв'язку, призначені для індустріальних інтернет-мереж з підтримкою туману, повинні підтримувати різноманітні відкриті й перевірені криптографічні алгоритми. Залежно від терпимості мережі до затримок і обмежень розміру пристрою можуть використовуватися програмні, апаратні або гібридні рішення для реалізації криптографічних послуг.

6. Ізоляція даних для комунікацій IIoT. Методи ізоляції можуть бути використані для захисту частин мережі IIoT з метою запобігання каскадному поширенню небажаних наслідків через відмову окремих частин мережі. Фізичні

методи ізоляції також можуть забезпечити безпеку окремо від операційних пристроїв, використовуючи спеціальний пристрій, присвячений питанням безпеки.

Наприклад, у рамках безпекової архітектури IIC пропонується використання спеціального шлюзу для забезпечення безпеки комунікацій між застарілими системами та ширшою мережею IIoT. Ізоляція може бути досягнута за допомогою:

1) операційної системи для відокремлення бізнес-процесів і операційних процесів від процесів безпеки наприклад, ізоляція процесів;

2) використання меж, визначених апаратним або програмним забезпеченням чи їх комбінацією (ізоляція контейнерів);

3) гіпервізора, налаштованого на ізоляцію кожного запущеного екземпляра на кінцевому пристрої (віртуальна ізоляція).

Практики ізоляції вже реалізовані в деяких рішеннях. Наприклад, апаратний модуль безпеки (HSM) забезпечує фізичну ізоляцію процесів безпеки.

Наразі технології на базі гіпервізорів і контейнерів переважно зосереджені на забезпеченні безпеки традиційних ICT-технологій та операційних систем. Рішення для IIoT поступово з'являються, зокрема реалізації, спрямовані на розробку контейнерних технологій для хмарних сервісів IoT або вбудованих операційних систем на базі Linux, які підтримують функції шлюзів.

7. Фільтрація та контроль доступу в IIoT. Для IIoT запропоновано три основні моделі контролю доступу.

1. Централізована модель. Фільтрування виконується відповідно до визначених політик безпеки та авторизації, причому кінцеві пристрої виступають лише як постачальники інформації.

Недоліком є єдина точка відмови, низька ефективність, вузькі місця в потоці зв'язку, залежність від своєчасного отримання контекстної інформації.

2. Гібридна модель. Центральний сервер приймає запити від користувачів, оцінює поточний стан середовища на основі інформації, одержпної від кінцевих пристроїв, та приймає рішення про надання чи заборону доступу.

Недоліки такі ж, як у централізованій моделі.

3. Розподілена модель. Кінцеві пристрої є "розумними" ресурсами, які отримують, обробляють і поширюють інформацію про доступ. Авторизація базується на локальній інформації, отриманій від сусідніх вузлів.

Популярною моделлю є CapBAC (контроль доступу на основі можливостей). У цій моделі пристрій пред'являє токен, що надає дозвіл на доступ до ресурсу. Однак вона має кілька недоліків: вразливість до атак повторного використання, недостатній контроль над забороною несанкціонованих інформаційних потоків, недоліки у вираженні політик доступу.

Покращення запропоновано у моделі ICAP, яка використовує ідентифікаційно-засновану систему можливостей, але ця модель також не вирішує проблеми створення політик безпеки й ефективної взаємодії в мережі.

4. Використання MUD. Модель Manufacturer Usage Description (MUD) застосовується для обмеження поверхні атак системи шляхом встановлення специфічних політик або механізмів контролю доступу.

MUD розроблено IETF для захисту IoT-мереж від атак на відмову в обслуговуванні (DoS) і для обмеження взаємодії пристроїв. Модель орієнтована на IoT-пристрої з конкретною або вузькою функціональністю, що полегшує виявлення стандартних моделей їхньої роботи.

Національний інститут стандартів і технологій (NIST) рекомендує MUD для зменшення загроз, пов'язаних із розподіленими атаками.

5. Програмно-визначені мережі (SDN) і віртуалізація функцій мережі (NFV). Підходи SDN та NFV забезпечують організаційні функції безпеки в IoT-системах. NFV дозволяє розгортати віртуальні апарати на периферії та у віддалених дата-центрах.

SDN інтегрує нові віртуалізовані послуги для запровадження заходів протидії кіберзагрозам.

Архітектури хмари, туману та периферії все частіше використовуються завдяки зростанню популярності IIoT-додатків.

Для забезпечення безпеки потрібні три основні фактори:

- аутентифікація;
- доступ;
- авторизація (AAA).

Рішення на базі SDN/NFV, такі як віртуальний AAA та захист каналу, пропонують динамічне управління доступом до мережі IoT-вузлів і підвищують рівень захисту під час початкового завантаження пристроїв.

## 2.4 Конфіденційність в промислових IoT

Додатки IIoT базуються на пристроях, які генерують, обробляють і обмінюються великими обсягами даних. Якщо цей процес не є безпечним, це може поставити під загрозу приватність користувачів та конкурентну перевагу організацій. Забезпечення приватності є складним завданням, яке включає соціальні, правові та технічні виклики.

Аспекти приватності в IIoT. Приватність в IIoT має два основні аспекти.

1. Захист зібраних даних від несанкціонованого доступу.

Метою є уникнення атак, таких як перехоплення даних (eavesdropping) і атаки типу "людина посередині" (MitM).

Для забезпечення цього потрібне використання механізмів контролю доступу, аутентифікації, шифрування даних і захищених каналів передачі інформації.

2. Секретність місця розташування сенсорів або виконавчих пристроїв:

- розкриття такої інформації може становити загрозу безпеці;
- загрози через недоліки у забезпеченні приватності;

- ідентифікація користувача;
- відстеження користувачів;
- моніторинг ресурсів;
- контроль мережі.

Для захисту приватності на різних рівнях архітектури необхідно враховувати такі аспекти:

1) на рівні пристроїв. Реалізація контролю доступу, механізмів аутентифікації, шифрування даних, захищених каналів для боротьби з атаками (побічні канали, захоплення вузлів, вставка підроблених вузлів, повторні атаки);

2) на рівні платформи. Передбачені попередні операції з обробки даних для зменшення ризиків атак.

Технічні рішення для захисту приватності включають методи шифрування. Повністю гомоморфне шифрування ефективне в теорії, але технологія ще не досягла достатньої зрілості. Механізми шифрування від кінця до кінця (E2E) забезпечують приватність на фізичному рівні передачі, але є складними для реалізації в IIoT. Техніки підвищення приватності включають диференційну приватність і локальну диференційна приватність, яка використовуються для досягнення конфіденційності розташування.

Агрегація даних із збереженням приватності використовується в "розумних" мережах.

До новітніх підходів необхідно віднести:

- технології на базі блокчейну;
- анонімізація даних;
- захист, орієнтований на контент;
- створення приватних фреймворків;
- розподілений захист даних;
- роль нетехнічних рішень.

Вирішення проблем приватності на рівні прикладного шару також вимагає:

– навчання користувачів для зменшення ризику;

– впровадження політик управління безпекою, які мінімізації ризиків.

Забезпечення приватності в IIoT – це багатогранна задача, і жодне окреме рішення не може повністю охопити всі можливі ризики. Потрібен комплексний підхід із використанням технічних та організаційних засобів.

# 3 РОЗРОБКА ТА ДОСЛІДЖЕННЯ АЛГОРИТМІВ АВТЕНТИФІКАЦІЇ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

## 3.1 Порівняння схем автентифікації пристроїв промислового Інтернету речей

Порівняння схем автентифікації пристроїв промислового Інтернету речей (IIoT) здійснюється за низкою критеріїв, що визначають ефективність, надійність та безпеку кожної схеми. До основних критеріїв можна віднести: рівень безпеки, енергоефективність, продуктивність, Можливість роботи в умовах обмежених ресурсів, сумісність і масштабованість [31, 32].

1. Рівень безпеки.

1.1 Стійкість до атак:

– схема повинна бути стійкою до основних атак (перехоплення, атаки "людина посередині", підробка автентифікації, квантові атаки).

1.2 Використання сучасних алгоритмів:

– застосування криптографічних алгоритмів, що відповідають сучасним стандартам (наприклад, постквантова криптографія).

1.3 Захист від повторного використання даних:

– механізми запобігання атакам повторення (replay attacks), наприклад, через використання одноразових токенів або часового маркування (timestamps).

2. Енергоефективність.

2.1 Рівень споживання енергії:

– схема має бути оптимізована для пристроїв з обмеженим енергоресурсом, наприклад, датчиків або бездротових модулів.

2.2 Залежність від складності обчислень:

– Математичні обчислення для автентифікації мають бути енергоефективними.

3. Продуктивність.

3.1 Швидкість автентифікації:

− час, необхідний для встановлення автентифікації, має бути мінімальним, особливо для систем реального часу.

3.2 Сумісність із масштабованими мережами:

– схема має забезпечувати ефективну автентифікацію великої кількості пристроїв без значного зниження продуктивності.

4. Можливість роботи в умовах обмежених ресурсів.

4.1 Обмеження за пам’яттю та обчислювальною потужністю:

– схема повинна враховувати обмежені апаратні можливості пристроїв IIoT.

4.2 Легка реалізація:

– простота впровадження в пристрої з низькою потужністю.

5. Сумісність і масштабованість.

5.1 Інтеграція з існуючими протоколами:

– схема має підтримувати промислові стандарти (наприклад, MQTT, CoAP, OPC UA);

5.2 Масштабованість:

– здатність автентифікувати значну кількість пристроїв без втрати продуктивності.

6. Тип автентифікації.

6.1 Однофакторна або багатофакторна автентифікація:

– наявність підтримки багатофакторної автентифікації для критичних систем.

6.2 Метод автентифікації:

– використання сертифікатів (PKI), токенів, паролів, біометрії або комбінованих підходів.

7. Захищеність комунікаційного каналу.

7.1 Шифрування даних:

– наявність захищених каналів (наприклад, TLS/SSL) для передачі автентифікаційних даних.

7.1 Захист ключів:

– механізми зберігання та обміну ключами мають бути надійними.

8. Надійність і доступність.

8.1 Захист від збоїв:

– схема має бути стійкою до збоїв мережі чи інших факторів.

8.2 Підтримка резервного копіювання:

– механізми відновлення після збоїв (наприклад, повторні спроби автентифікації).

9. Вартість впровадження.

9.1 Ліцензійні витрати:

– чи використовує схема дорогі ліцензійні технології.

9.2 Витрати на апаратне забезпечення:

– вимоги до обладнання для підтримки схеми (наприклад, модулі TPM, HSM).

9.3 Витрати на розробку:

– складність і ресурсоємність розробки схеми.

10. Стійкість до майбутніх загроз.

10.1 Підготовленість до постквантової ери:

– використання криптографічних алгоритмів, що здатні протистояти квантовим комп’ютерам.

10.2 Модульність:

– Легкість адаптації до нових загроз і впровадження оновлень.

11. Конфіденційність і приватність.

11.1 Мінімізація даних:

– використання мінімально необхідної кількості особистих або ідентифікаційних даних пристрою.

11.2 Дотримання стандартів приватності:

– схема повинна відповідати регуляторним вимогам, таким як GDPR.

12. Зручність впровадження і використання.

12.1 Простота налаштування:

– легкість інтеграції в існуючі системи.

12.2 Автоматизація:

– можливість автоматичного управління автентифікацією для мінімізації участі людини.

Таблиця 3.1 – Порівняння схем автентифікації пристроїв

| Критерій | Сертифікатна схема (PKI) | Парольна схема | Біометрична схема |
|---|---|---|---|
| Рівень безпеки | Високий | Середній | Високий |
| Енергоефективність | Середня | Висока | Середня |
| Продуктивність | Середня | Висока | Низька |
| Сумісність | Висока | Висока | Середня |

Порівняння за цими критеріями допомагає обрати оптимальну схему автентифікації для конкретного сценарію використання в IIoT.

## 3.2 Алгоритм автентифікації для IIoT

Автентифікація для промислового Інтернету речей (IIoT) є критично важливою для забезпечення безпеки пристроїв та обміну даними. Розроблений алгоритму автентифікації базується на використанні багатофакторного підходу та протоколу SSL/TLS.

Алгоритм автентифікації складається з наступних етапів.

Етап 1. Ідентифікація пристрою. Унікальний ідентифікатор пристрою (UID).

Кожен пристрій отримує унікальний сертифікат або UID під час виробництва. UID зберігається в апаратно-захищеній зоні пристрою, наприклад, у TPM (Trusted Platform Module).

Етап 2. Встановлення захищеного з'єднання.

2.1 Ініціація з'єднання:

− пристрій надсилає запит на підключення до серверу управління;

− сервер відповідає викликом початкового протоколу (наприклад, обміну ключами через TLS).

2.2 Автентифікація на основі сертифікату:

– сервер надсилає свій сертифікат, що підписаний відповідним центром сертифікації (CA);

– пристрій перевіряє сертифікат для забезпечення справжності сервера.

2.3 Обмін ключами:

– використовується протокол Diffie-Hellman або його варіант для встановлення симетричного ключа.

Етап 3. Автентифікація пристрою.

3.1 Підтвердження UID:

– пристрій надсилає UID, підписаний своїм PKI;

– сервер перевіряє підпис за допомогою публічного ключа пристрою, збереженого в базі даних.

3.2 Верифікація параметрів:

– сервер перевіряє додаткові параметри (MAC-адресу, дані прошивки тощо) для підвищення безпеки.

Етап 4. Додаткова багатофакторна автентифікація.

4.1 OTP (One-Time Password):

– сервер генерує одноразовий пароль (OTP) і надсилає його до хмарної панелі управління;

– адміністратор або інший довірений модуль вводить OTP на пристрої для завершення автентифікації.

Етап 5. Встановлення сесії.

Захищена сесія:

– після успішної автентифікації пристрій та сервер застосовують симетричний ключ для шифрування сесії;

– обмін даними починається у зашифрованому вигляді.

Схема автентифікації.

Ідентифікація пристрою. UID → Сервер.

Перевірка сертифіката сервера. Сервер → Пристрій.

Обмін ключами (Diffie-Hellman):.Сервер ↔ Пристрій.

Перевірка UID. UID + підпис PKI → Сервер.

Багатофакторна автентифікація (OTP). Сервер ↔ Адміністратор → Пристрій.

Встановлення захищеної сесії. Симетричний ключ → Обмін даними.

Серед переваг даного алгоритму є те, що безпека імплементована на рівні апаратного забезпечення, так як UID зберігається у захищеній зоні.

Використання стандартів SSL/TLS для шифрування і PKI для автентифікації.

Багатофакторність додає рівень безпеки за допомогою OTP.

Розроблений алгоритм легко адаптується до різних сценаріїв промислового Інтернету речей, включаючи розподілені системи та хмарні обчислення.

### 3.2.1 Алгоритм автентифікація на основі сертифікату

Алгоритм автентифікації на основі сертифікату складається з наступних етапів: ініціалізація, встановлення зв’язку, перевірка автентичності, встановлення захищеного каналу.

1. Ініціалізація:

- генерація ключів. Кожен пристрій створює пару ключів (відкритий і закритий);
- запит сертифікату (CSR). Пристрій формує запит на сертифікат, який включає його відкритий ключ і метаінформацію (ідентифікатор пристрою, організацію, термін дії тощо).
- підпис сертифікату центром сертифікації (CA). Центр сертифікації (Certificate Authority, CA) перевіряє інформацію в CSR і створює цифровий сертифікат, підписуючи його своїм закритим ключем.

2. Встановлення зв’язку:

– запит на підключення. Пристрій-ініціатор (IoT-устрій) відправляє запит серверу або іншому пристрою IoT;

– обмін сертифікатами. Сервер або пристрій відповідає сертифікатом, підписаним довіреним CA.

3. Перевірка автентичності.

− валідація сертифікату. Перевіряється підпис сертифікату за допомогою відкритого ключа довіреного CA. Перевіряються такі параметри: термін дії сертифікату; відповідність метаінформації (наприклад, ідентифікатор пристрою) та відкликані сертифікати (через CRL або OCSP);

− перевірка відкритого ключа. Переконуємося, що відкритий ключ сертифіката відповідає заявленому пристрою.

4. Встановлення захищеного каналу.

– створення сесійного ключа. Пристрої використовують свої ключі для узгодження сесійного ключа через протоколи, такі як TLS;

– шифрування каналу. Встановлюється захищений канал для обміну даними.

### 3.2.2 Протокол обміну ключами

Протокол обміну ключами Diffie-Hellman (DH) дозволяє двом пристроям спільно створити секретний ключ для безпечного зв’язку через незахищений канал, без необхідності попереднього обміну секретною інформацією.

У контексті IIoT, протокол DH використовується для автентифікації пристроїв і встановлення захищених каналів між ними, наприклад, для передачі конфіденційних даних.

Основні поняття протоколу:

1. Параметри протоколу:
   - просте число p: велике просте число, загальновідоме.
   - основа $g$: первісний корінь за модулем p, також загальновідома.
   - $p$ і $g$ можуть бути спільними для всіх пристроїв в IoT-системі.

2. Приватні та публічні ключі. Кожен пристрій генерує приватний ключ ($a$ або $b$) – випадкове ціле число.

На основі приватного ключа обчислюється публічний ключ:

$$A = g^a \ (mod\ p),$$

$$B = g^b \ (mod\ p).$$

3. Обмін ключами. Пристрої обмінюються публічними ключами.

4. Обчислення спільного секретного ключа. Кожен пристрій використовує отриманий публічний ключ іншого пристрою для обчислення спільного секретного ключа: $K = B^a \ (mod\ p) = A^b (mod\ p)$

Цей ключ $K$ однаковий для обох пристроїв, але недоступний для третіх сторін, навіть якщо вони перехоплять публічні ключі.

Етапи протоколу для IIoT.

1. Ініціалізація. Централізований сервер або система надає параметри p і g усім пристроям.

2. Генерація ключів. Пристрій 1 генерує приватний ключ $a$ і публічний ключ $A = g^a \ (mod\ p)$.

Пристрій 2 генерує приватний ключ $b$ і публічний ключ $B = g^b \ (mod\ p)$ .

3. Обмін публічними ключами:

Пристрій 1 надсилає А пристрою 2, і навпаки.

4. Обчислення спільного секретного ключа:

Пристрій 1 обчислює:

$$K = B^a \ (mod\ p).$$

Пристрій 2 обчислює:

$$K = A^b \ (mod\ p).$$

Отриманий ключ *K* використовується як сесійний ключ для шифрування подальшої комунікації (рисунок 3.1).

Код програми автентифікації двох пристроїв IIoT з використанням протоколу обміну ключами Diffie-Hellman приведений в додатку А. Програма працює наступним чином.

Кожен пристрій генерує свої приватний та публічний ключі, використовуючи спільні параметри: базу (g) та модуль (просте число p).

Пристрої обмінюються публічними ключами і обчислюють спільний секретний ключ за допомогою свого приватного ключа та публічного ключа іншого пристрою.

Спільний секретний ключ використовується для автентифікації та може бути застосований для подальшого шифрування даних між пристроями.

```
Спільний модуль (p): 57
Спільна база (g): 23

Пристрій A:
  Приватний ключ (a): 9979
  Публічний ключ (A): 44

Пристрій B:
  Приватний ключ (b): 6608
  Публічний ключ (B): 16

Спільний секрет (обчислений пристроєм A): 55
Спільний секрет (обчислений пристроєм B): 55

Автентифікація успішна: спільні секрети збігаються!
```

Рисунок 3.1 – Вивід результатів програми обміну ключами

Просте число **(**p**)** та база **(**g**)**. Ці параметри є загальнодоступними та відомі обом пристроям. Їх вибір має бути безпечним для забезпечення криптографічної стійкості.

Приватний ключ. Кожен пристрій генерує випадковий приватний ключ, який зберігається у таємниці.

Публічний ключ. Обчислюється на основі приватного ключа та передається на інший пристрій.

Спільний секретний ключ. Обидва пристрої незалежно обчислюють однаковий секретний ключ, що гарантує конфіденційність та аутентифікацію.

5. Автентифікація пристроїв.

Для підтвердження автентичності публічні ключі можуть супроводжуватися цифровими сертифікатами, підписаними довіреним центром сертифікації (CA).

Захист протоколу Diffie-Hellman.

1. Безпека алгоритму. Захищений протокол базується на складності обчислення дискретного логарифма. Треті сторони, які перехоплюють $A$ і $B$, не можуть обчислити $K$ без знання $a$ або $b$.

2. Ризики. Атака “людина посередині” (MITM): зловмисник може перехопити обмін ключами. Щоб уникнути цього, використовуються цифрові підписи та сертифікати.

Приклад сценарію для IoT.

1. Сенсор і шлюз:

1) сенсор генерує свої $a$ та $A$, шлюз – $b$ та $B$;

2) сенсор і шлюз обмінюються $A$ та $B$;

3) Використовують спільний ключ $K$ для захисту переданих даних.

2. Хмарний сервер і IoT-пристрій.

Хмарний сервер використовує DH для встановлення сесійного ключа з кожним підключеним пристроєм, забезпечуючи захищений зв’язок у масштабованій мережі.

Переваги протоколу Diffie-Hellman для IoT:

1) мінімальна залежність від попередньо встановлених ключів;

2) можливість роботи в динамічних системах з великою кількістю пристроїв;

3) підтримка інтеграції з цифровими сертифікатами для автентифікації.

Diffie-Hellman є основою для багатьох сучасних IoT-протоколів, таких як TLS та інші системи, орієнтовані на безпеку.

### 3.2.3 Автентифікація пристрою

Автентифікація пристрою – це ключовий етап у встановленні довіреного зв'язку між пристроєм та сервером в промисловому Інтернеті речей (IoT). На цьому етапі відбувається перевірка унікального ідентифікатора пристрою (UID), що підтверджує його автентичність.

Підтвердження UID (унікального ідентифікатора) відбувається в такій послідовності.

Крок 1. Пристрій генерує підпис для UID.

UID (Unique Identifier) – це унікальний ідентифікатор пристрою, який може бути серійним номером, MAC-адресою або іншим ідентифікатором, специфічним для пристрою. UID підтверджує індивідуальність пристрою в системі.

Пристрій має власний приватний ключ (згенерований під час початкового налаштування або встановлений виробником).

За допомогою криптографії з відкритим ключем (PKI) пристрій підписує UID:

$$\text{Підпис} = Sign(UID, \text{Приватний ключ пристрою}).$$

Функція підпису гарантує, що UID неможливо підробити без приватного ключа пристрою.

Крок 2. Пристрій надсилає дані серверу.

Пристрій надсилає серверу.

1. UID – унікальний ідентифікатор.
2. Підпис – результат підписання UID приватним ключем.

Крок 3. Сервер перевіряє підпис.

Сервер має доступ до публічного ключа пристрою, збереженого в базі даних (це забезпечується попередньою реєстрацією пристрою в системі).

Сервер перевіряє UID, використовуючи публічний ключ пристрою:

$$\text{Результат перевірки} = Verify(UID, \text{Підпис}, \text{Публічний ключ пристрою}).$$

Якщо підпис дійсний, сервер впевнений, що UID дійсно було згенеровано конкретним пристроєм, власником приватного ключа.

Крок 4. Підтвердження автентичності.

Якщо перевірка підпису успішна, тоді:

– сервер підтверджує автентичність пристрою;

– переходить до наступного етапу встановлення захищеного зв'язку (наприклад, обмін сесійними ключами).

Якщо перевірка підпису неуспішна:

– сервер відхиляє автентифікацію.

– генерує повідомлення про відмову в доступі.

Розглянемо приклад практичного застосування.

1. IIoT-термостат:

− термостат надсилає свій UID та підпис до серверу управління;

− сервер перевіряє дані, використовуючи публічний ключ термостата, і підтверджує його автентичність перед тим, як надіслати оновлення конфігурації.

2. IIoT-камери спостереження:

− камера підписує свій UID і надсилає його до хмарного сервера перед передачею відеопотоку;

− хмарний сервер перевіряє автентичність камери, щоб упевнитись, що відеопотік надходить від авторизованого пристрою.

Захист проти атак. Підробка UID. Завдяки підписанню UID приватним ключем, зловмисники не можуть створити дійсний підпис без доступу до приватного ключа пристрою.

Атака "людина посередині". Підпис гарантує цілісність UID і захищає від змін під час передачі даних.

Захист бази даних серверу. Публічні ключі пристроїв мають зберігатися у захищеній базі даних, щоб уникнути компрометації.

Автентифікація на основі UID і PKI є основою для захищених IoT-систем і дозволяє масштабувати мережі пристроїв, підтримуючи високий рівень безпеки.

### 3.2.4 Верифікація параметрів

Верифікація параметрів є додатковим етапом автентифікації, спрямованим на підвищення рівня безпеки в IIoT-системах. Цей етап передбачає перевірку специфічних характеристик пристрою, що дозволяє захистити мережу від підроблених або скомпрометованих пристроїв.

Основні етапи верифікації параметрів.

1. Отримання додаткових параметрів від пристрою. Після успішної перевірки UID сервер запитує і отримує від пристрою додаткові параметри, які характеризують його унікальні особливості:

- MAC-адресу – фізичну адресу мережевого інтерфейсу пристрою;
- версію прошивки – інформацію про поточне програмне забезпечення пристрою;
- серійний номер – унікальний номер пристрою, наданий виробником;
- стан сертифікату – для пристроїв, що використовують сертифікати (наприклад, у PKI);
- таймстамп – час генерації запиту, що дозволяє захистити від атак повтору (replay attack).

2. Верифікація MAC-адреси. MAC-адреса (Media Access Control) є апаратним ідентифікатором пристрою в мережі:

- сервер перевіряє, чи зареєстрована MAC-адреса в його базі даних;
- якщо MAC-адреса є новою або відсутньою, сервер може заблокувати доступ або вимагати додаткової перевірки.

3. Перевірка версії прошивки. Сервер порівнює версію прошивки пристрою з еталонними даними в базі:

− актуальність: чи є прошивка останньою версією? Стара прошивка може містити вразливості;

− сумісність: чи відповідає версія прошивки очікуваній для конкретного типу пристрою?

− якщо версія прошивки застаріла, сервер може рекомендувати або автоматично ініціювати оновлення.

4. Перевірка серійного номера. Серійний номер перевіряється на відповідність даним у базі серверу:

− чи належить цей номер пристрою, зареєстрованому в системі?

− серійні номери, які не проходять верифікацію, можуть сигналізувати про підробку пристрою.

5. Перевірка стану сертифікату. Якщо пристрій використовує сертифікат (наприклад, у PKI), сервер перевіряє його:

− Термін дії сертифікату: чи не минув час його використання?

− Стан сертифікату: сертифікат має бути чинним і не відозваним (revoked);

− цілісність сертифікату: перевіряється, чи не було внесено змін.

6. Аналіз таймстампу. Таймстамп застосовують для захисту при атак ах повтору:

− сервер перевіряє, чи є час запиту у межах допустимого інтервалу;

− запити з "протермінованим" таймстампом або занадто ранні запити відхиляються.

Дії у разі невідповідності. Якщо будь-який з параметрів не проходить перевірку:

− сервер відхиляє запит автентифікації;

− генерується повідомлення про помилку з поясненням причини (наприклад, "невідповідна MAC-адреса" або "застаріла прошивка");

− в окремих випадках сервер може вимагати від пристрою додаткової автентифікації або залучення адміністратора.

Захист протоколу та переваги. Перевірка MAC-адреси і серійного номера унеможливлює доступ для незареєстрованих пристроїв.

Безпека проти вразливостей. Контроль версій прошивки гарантує, що пристрій використовує безпечне та актуальне програмне забезпечення.

Додаткова довіра. Використання сертифікатів та таймстампів забезпечує глибший рівень перевірки та захисту.

Верифікація параметрів є важливим доповненням до базової автентифікації, оскільки дозволяє значно підвищити рівень безпеки в промислових IIoT-системах.

## 3.3 Багатофакторна автентифікація при автентифікації пристроїв

Багатофакторна автентифікація (MFA) надає додатковий рівень захисту до процесу автентифікації пристроїв, використовуючи незалежні канали або методи перевірки. Одним із популярних методів MFA для IIoT є використання одноразових паролів (OTP). Цей підхід підвищує безпеку, зменшуючи ризики компрометації пристрою чи мережі, навіть якщо інші автентифікаційні фактори були зламані.

Додаткова багатофакторна автентифікація за допомогою OTP складається з наступних кроків.

1. Генерація одноразового пароля (OTP). Сервер після успішного проходження базової автентифікації (наприклад, UID-перевірки) генерує одноразовий пароль.

Характеристики OTP:

− пароль є унікальним для кожної сесії автентифікації;

− має обмежений термін дії (наприклад, 60 секунд);

− генерується на основі криптографічно стійкого алгоритму, такого як TOTP (Time-based OTP) або HMAC-based OTP.

2. Передача OTP до хмарної панелі управління. Сервер передає згенерований OTP до хмарної панелі управління, яка доступна адміністратору або іншому авторизованому модулю. Для захисту каналу передачі OTP передається через захищені канали, наприклад, HTTPS або за допомогою протоколів шифрування.

3. Використання OTP адміністратором чи довіреним модулем. Адміністратор або інший довірений модуль отримує OTP із хмарної панелі управління. Відповідальна сторона вводить OTP на пристрої IoT для підтвердження завершення автентифікації.

До можливих способів введення OTP:

− через веб-інтерфейс управління пристроєм;

− через фізичний інтерфейс пристрою (наприклад, сенсорний екран);

− через мобільний додаток, інтегрований з пристроєм.

Наступним етапом є використання механізму перевірки OTP сервером.

1. Прийом OTP від пристрою. Пристрій надсилає OTP на сервер після введення його адміністратором.

2. Перевірка відповідності OTP:

− сервер порівнює отриманий OTP із тим, що було згенеровано для цієї сесії;

− OTP вважається дійсним лише за умови збігу з очікуваним значенням та

використання у межах терміну дії.

2. Підтвердження автентифікації. Якщо OTP дійсний, сервер завершить процес автентифікації і дозволить пристрою доступ до системи. У разі невідповідності або спливу терміну дії сервер блокує сесію.

Код програми автентифікації на основі одноразового пароля приведений нижче:

```
import pyotp
```

```
import time
# Генерація секретного ключа для пристрою
def generate_secret():
    return pyotp.random_base32()
def otp_authentication():
    # Крок 1. Генерація секретного ключа
    secret = generate_secret()
    print("Секретний ключ (зберігайте його у безпеці):", secret)
    # Крок 2. Генерація OTP
    totp = pyotp.TOTP(secret)
    otp = totp.now()
    print("\nСформовано OTP:", otp)
    print("OTP надіслано адміністратору.")
    # Крок 3: Перевірка OTP
    input_otp = input("\nВведіть OTP для автентифікації: ")
    if totp.verify(input_otp):
        print("Автентифікація успішна!")
    else:
        print("Помилка автентифікації: введено невірний OTP.")
# Запуск програми
if __name__ == "__main__":
    otp_authentication()
```

Програма працює наступним чином (рисунок 3.2, рисунок 3.3).

1. Кожен пристрій отримує унікальний секретний ключ, який зберігається в безпечному місці.

2. За допомогою секретного ключа програма генерує одноразовий пароль, який дійсний протягом короткого часу (наприклад, 30 секунд).

3. Пристрій вводить отриманий пароль для завершення автентифікації. Сервер перевіряє, чи відповідає введений OTP згенерованому.

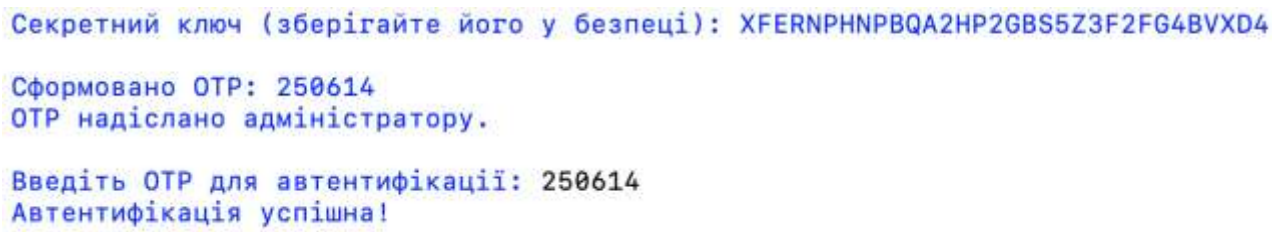


Рисунок 3.2 – Приклад успішної автентифікації на основі одноразового пароля

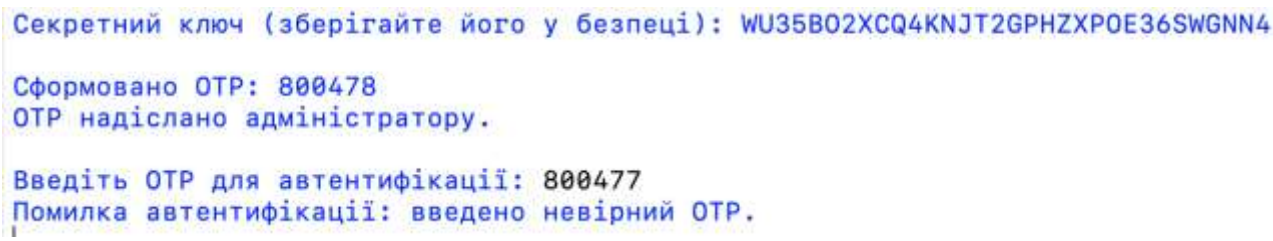


Рисунок 3.3 – Приклад не успішної автентифікації на основі одноразового пароля

Переваги використання OTP у багатофакторній автентифікації.

1. Підвищена безпека. Навіть якщо базовий фактор автентифікації (UID або пароль) скомпрометовано, зловмисники не зможуть пройти автентифікацію без OTP.

2. Динамічність. Одноразовий пароль генерується динамічно, що робить його неактуальним для повторного використання.

3. Широкі сценарії застосування. Підходить для автентифікації як фізичних пристроїв IoT, так і користувачів у мережі.

Розширення та додаткові заходи.

1. Множинний канал доставки OTP. OTP може доставлятися не лише до хмарної панелі, а й через інші канали (наприклад, SMS, email, або мобільний додаток).

2. Інтеграція з біометрією. Для додаткової безпеки можна інтегрувати біометричну перевірку адміністратора перед отриманням OTP.

3. Використання апаратних токенів. Адміністратор може отримувати OTP через апаратний токен (наприклад, пристрої типу YubiKey).

До недоліки багатофакторна автентифікація при автентифікації пристроїв необхідно віднести.

1. Залежність від додаткового каналу. Наявність зв’язку з хмарною панеллю чи іншими сервісами є критичною.

2. Затримки доставки OTP. Можуть виникати затримки в доставці OTP, якщо інфраструктура мережі перевантажена.

3. Захист самого OTP. Зловмисники можуть спробувати перехопити OTP, тому потрібен додатковий захист каналу передачі.

Додаткова багатофакторна автентифікація з використанням OTP значно підвищує рівень безпеки в IoT-системах. Вона зменшує ризик атак, таких як викрадення пароля чи компрометація пристрою, і створює додатковий бар’єр для несанкціонованого доступу.

# ВИСНОВКИ

В кваліфікаційній роботі розв’язано актуальну задачу підвищення ефективності алгоритмів автентифікації промислових Інтернет речей. При цьому отримано наступні результати.

1. Аналіз механізмів автентифікації в промисловому Інтернеті речей показав, що через динамічну природу та масштабованість IIoT-систем їх безпека залишається важливим викликом. Недоліки існуючих стандартів і протоколів безпеки можуть призводити до серйозних загроз для конфіденційності та цілісності даних.

2. Дослідження загроз конфіденційності в IioT виявило низку критичних вразливостей, зокрема перехоплення трафіку, атаки типу "людина посередині" (MITM) та повторні атаки (Replay). Для їх мінімізації були визначені основні вимоги до конфіденційності та запропоновані рекомендації для безпечного підключення пристроїв.

3. Розроблений алгоритм автентифікації на основі сертифікатів забезпечує високий рівень безпеки за рахунок застосування інфраструктури відкритих ключів (PKI). Він дозволяє ефективно протидіяти несанкціонованому доступу до пристроїв у IIoT.

4. Протокол обміну ключами Diffie-Hellman був адаптований для середовища IIoT. Він дозволяє безпечно встановлювати спільні ключі між пристроями навіть у присутності атакуючих, що спостерігають за мережею.

5. Дослідження багатофакторної автентифікації підтвердило її ефективність для підвищення безпеки в IIoT-системах. Використання одноразових паролів (OTP) як додаткового фактора автентифікації значно знижує ризик компрометації системи.

6. Розроблені алгоритми автентифікації та механізми верифікації параметрів пристроїв IioT відповідають вимогам сучасних стандартів безпеки. Вони враховують специфіку промислових мереж, забезпечуючи захист конфіденційності, цілісності та доступності даних.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. El-hajj, M.; Chamoun, M.; Fadlallah, A.; Serhrouchni, A. Analysis of authentication techniques in Internet of Things (IoT). In Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 18–20 October 2017; pp. 1–3.

2. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. Comput. Netw. **2010**, 54, 2787–2805.

3. Ahmed, M.E.; Kim, H. DDoS Attack Mitigation in Internet of Things Using Software Defined Networking. In Proceedings of the 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService), Redwood City, CA, USA, 6–9 April 2017; pp. 271–276.

4. Liu, Y.; Hao, X.; Ren, W.; Xiong, R.; Zhu, T.; Choo, K.-K.R.; Min, G. A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things. IEEE Trans. Comput. **2023**, 72, 501–512.

5. Tanveer, M.; Badshah, A.; Khan, A.U.; Alasmary, H.; Chaudhry, S.A. CMAF-IIoT: Chaotic map-based authentication framework for Industrial Internet of Things. Internet Things **2023**, 23, 100902.

6. Zhang, Y.; He, D.; Vijayakumar, P.; Luo, M.; Huang, X. SAPFS: An Efficient Symmetric-Key Authentication Key Agreement Scheme with Perfect Forward Secrecy for Industrial Internet of Things. IEEE Internet Things J. **2023**, 10, 9716–9726.

7. Rangwani, D.; Om, H. 4F-MAKA: Four-factor mutual authentication and key agreement protocol for internet of things. Peer-Peer Netw. Appl. **2023**, 16, 35–56.

8. Bułat, R.; Ogiela, M.R. Personalized Context-Aware Authentication Protocols in IoT. Appl. Sci. 2023, 13, 4216.

9. Alsaeed, N.; Nadeem, F. A Framework for Blockchain and Fogging-based Efficient Authentication in Internet of Things. In Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT),

Tabuk, Saudi Arabia, 25–27 January 2022; pp. 409–417.

10. Ahmed, W.K.; Mohammed, R.S. Lightweight Authentication Methods in IoT: Survey. In Proceedings of the 2022 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, 14–17 March 2022; pp. 241–246.

11. Salama, M.; Bahsoon, R.; Bencomo, N. Managing Trade-offs in Self-Adaptive Software Architectures. In Managing Trade-Offs in Adaptable Software Architectures; Elsevier: Amsterdam, The Netherlands, 2017; pp. 249–297

12. Xu, H.; Hsu, C.; Harn, L.; Cui, J.; Zhao, Z.; Zhang, Z. Three-Factor Anonymous Authentication and Key Agreement Based on Fuzzy Biological Extraction for Industrial Internet of Things. IEEE Trans. Serv. Comput. **2023**, 16, 3000–3013.

13. Pu, L.; Lin, C.; Chen, B.; He, D. User-Friendly Public-Key Authenticated Encryption with Keyword Search for Industrial Internet of Things. IEEE Internet Things J. **2023**, 10, 13544–13555.

14. Dohare, I.; Singh, K.; Ahmadian, A.; Mohan, S.; Praveen Kumar Reddy, M. Certificateless Aggregated Signcryption Scheme (CLASS) for Cloud-Fog Centric Industry 4.0. IEEE Trans. Ind. Inform. **2022**, 18, 6349–6357.

15. Zhang, P.; Wang, Y.; Aujla, G.S.; Jindal, A.; Al-Otaibi, Y.D. A Blockchain-Based Authentication Scheme and Secure Architecture for IoT-Enabled Maritime Transportation Systems. IEEE Trans. Intell. Transp. Syst. **2023**, 24, 2322–2331.

16. Liu, J.; Yang, J.; Wu, W.; Huang, X.; Xiang, Y. Lightweight Authentication Scheme for Data Dissemination in Cloud-Assisted Healthcare IoT. IEEE Trans. Comput. **2023**, 72, 1384–1395

17. Tong, F.; Chen, X.; Wang, K.; Zhang, Y. CCAP: A Complete Cross-Domain Authentication Based on Blockchain for Internet of Things. IEEE Trans. Inf. Forensics Secur. **2022**, 17, 3789–3800.

18. AlQahtani, A.A.S.; Alamleh, H.; Al Smadi, B. IoT Devices Proximity Authentication. In Ad Hoc Network Environment, Proceedings of the 2022 IEEE

International IOT, Electronics and Mechatronics Conference, IEMTRONICS 2022, Toronto, ON, Canada, 1–4 June 2022; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2022; pp. 1–5.

19. Saqib, M.; Jasra, B.; Moon, A.H. A lightweight three factor authentication framework for IoT based critical applications. J. King Saud Univ. Comput. Inf. Sci. **2021**, 34, 6925–6937.

20. Nezhad, M.A.; Barati, H.; Barati, A. An Authentication-Based Secure Data Aggregation Method in Internet of Things. J. Grid Comput. **2022**, 20, 1–28.

21. Hu, B.; Tang, W.; Xie, Q. A two-factor security authentication scheme for wireless sensor networks in IoT environments. Neurocomputing **2022**, 500, 741–749.

22. Leng, Y.; Zhang, R.; Wen, W.; Wu, P.; Xia, M. Physical-layer Authentication with Watermarked Preamble for Internet of Things. In Proceedings of the International Conference on Wireless and Mobile Computing, Networking and Communications, IEEE Computer Society, Montreal, QC, Canada, 21–23 June 2023; pp. 212–217.

23. Yuan, S.; Phan-Huynh, R. A Lightweight Hash-Chain-Based Multi-Node Mutual Authentication Algorithm for IoT Networks. In Proceedings of the 2022 IEEE Future Networks World Forum, FNWF 2022, Montreal, QC, Canada, 10–14 October 2022; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2022; pp. 72–74.

24. Chen, F.; Xiao, Z.; Xiang, T.; Fan, J.; Truong, H.-L. A Full Lifecycle Authentication Scheme for Large-Scale Smart IoT Applications. IEEE Trans. Dependable Secur. Comput. **2023**, 20, 2221–2237.

25. Wazzeh, M.; Ould-Slimane, H.; Talhi, C.; Mourad, A.; Guizani, M. Privacy-Preserving Continuous Authentication for Mobile and IoT Systems Using Warmup-Based Federated Learning. IEEE Netw. **2022**, 37, 224–230.

26. Ismail, S.; Dawoud, D.; Reza, H. Towards A Lightweight Identity Management and Secure Authentication for IoT Using Blockchain. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022;

pp. 77–83.

27. Jin, C.; Yang, Z.; Xiang, T.; Adepu, S.; Zhou, J. HMACCE: Establishing Authenticated and Confidential Channel from Historical Data for Industrial Internet of Things. IEEE Trans. Inf. Forensics Secur. **2023**, 18, 1080–1094.

28. Al Ahmed, M.T.; Hashim, F.; Hashim, S.J.; Abdullah, A. Hierarchical blockchain structure for node authentication in IoT networks. Egypt. Inform. J. **2022**, 23, 345–361.

29. Khashan, O.A.; Khafajah, N.M. Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. J. King Saud Univ. Comput. Inf. Sci. **2023**, 35, 726–739.

30. Zhang Q, Wu J, Zhong H, He D, Cui J. Efficient Anonymous Authentication Based on Physically Unclonable Function in Industrial Internet of Things. IEEE Transactions on Information Forensics and Security 2023;18:233–47

31. Онищенко М., Тимчак А., Понедєльніков Г. Забезпечення захисту кіберфізичних систем за допомогою моніторингу. Матеріали проблемно-наукової міжгалузевої конференції «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2024), Тернопіль, 2024. – С. 46-48.

32. Онищенко М., Тимчак А., Понедєльніков Г. Захист даних у кіберфізичних системах. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. – С. 73-75.

ДОДАТОК А

Код програми автентифікації двох пристроїв IIoT з використанням протоколу обміну ключами Diffie-Hellman

```
import random
def generate_private_key():
    """Генерує приватний ключ для пристрою."""
    return random.randint(1, 10000)
def generate_public_key(private_key, g, p):
    """Генерує публічний ключ за формулою (g^private_key) % p."""
    return pow(g, private_key, p)
def compute_shared_secret(their_public_key, private_key, p):
    """Обчислює спільний секрет за формулою (their_public_key^private_key) % p."""
    return pow(their_public_key, private_key, p)
# Симуляція обміну ключами DH
def diffie_hellman_authentication():
    # Спільні параметри (відомі обом пристроям)
    p = 23  # Просте число
    g = 5   # Примітивний корінь по модулю p
    print("Спільний модуль (p):", p)
    print("Спільна база (g):", g)
    # Ключі пристрою A
    private_key_a = generate_private_key()
    public_key_a = generate_public_key(private_key_a, g, p)
    # Ключі пристрою B
    private_key_b = generate_private_key()
    public_key_b = generate_public_key(private_key_b, g, p)
    print("\nПристрій A:")
    print("  Приватний ключ (a):", private_key_a)
```

```
    print("  Публічний ключ (A):", public_key_a)
    print("\nПристрій B:")
    print("  Приватний ключ (b):", private_key_b)
    print("  Публічний ключ (B):", public_key_b)
    # Обчислення спільного секрету
    shared_secret_a = compute_shared_secret(public_key_b, private_key_a, p)
    shared_secret_b = compute_shared_secret(public_key_a, private_key_b, p)
    print("\nСпільний секрет (обчислений пристроєм A):", shared_secret_a)
    print("Спільний секрет (обчислений пристроєм B):", shared_secret_b)
    # Перевірка відповідності спільних секретів
    if shared_secret_a == shared_secret_b:
        print("\nАвтентифікація успішна: спільні секрети збігаються!")
    else:
        print("\nАвтентифікація не вдалася: спільні секрети не збігаються!")
# Запуск симуляції
if __name__ == "__main__":
    diffie_hellman_authentication()
```

ДОДАТОК Б

Копії публікацій

*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

**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.

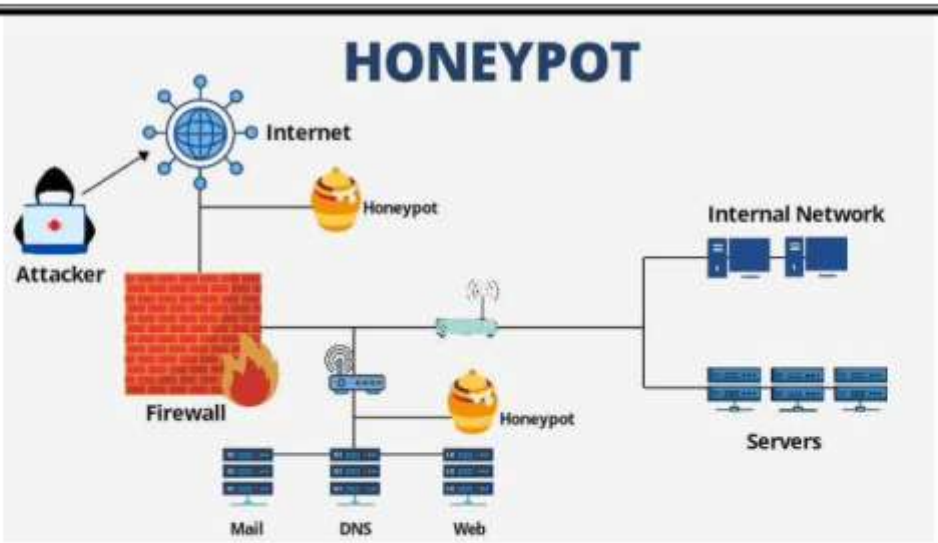


Рисунок 1 - Honeypots

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].

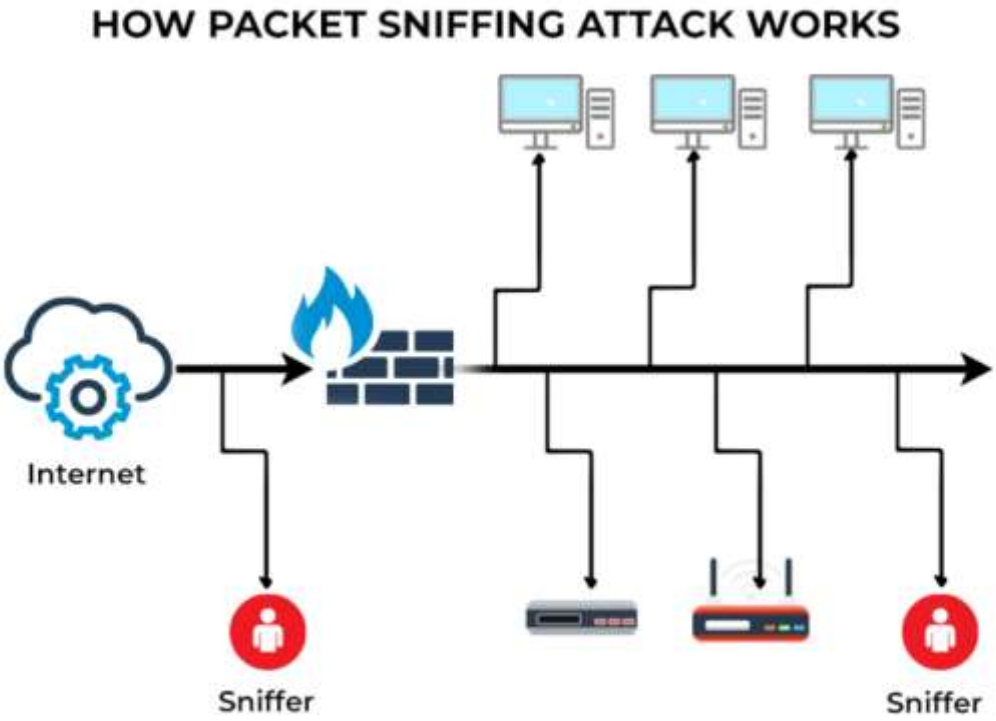


Рисунок 2 - Принцип роботи сніфера пакетів

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.

*ГРОМАДСЬКА ОРГАНІЗАЦІЯ*
*«КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»*

**Матеріали**
**науково-практичного симпозіуму**
# *«ЗАХИСТ ІНФОРМАЦІЇ»*

30 листопада 2024
Тернопіль

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.

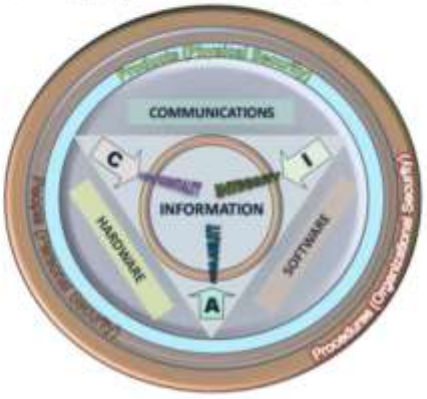


Рисунок 2 - Октет захисту інформації

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.