ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ ТА ЗАСОБИ ЗАПОБІГАННЮ ПОШИРЕННЮ ЗАГРОЗ В ПРОМИСЛОВІЙ МЕРЕЖІ ІОТ ІЗ ВИКОРИСТАННЯМ КОНЦЕПЦІЇ «INDUSTRIAL TREAT DEFENCE»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
(код, найменування спеціальності)
освітньо-професійної програми Інформаційна та кібернетична безпека
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Ілля БАСЮК

Виконав: здобувач вищої освіти групи БСДМ-61
БАСЮК Ілля
(ПРІЗВИЩЕ, Ім'я)

Керівник: БОРСУКОВСЬКИЙ Юрій
к.т.н, доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: ТУРОВСЬКИЙ Олександр
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Басюку Іллі Богдановичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія та засоби запобіганню поширенню загроз в промисловій мережі IoT із використанням концепції «Industrial Treat Defence»
керівник кваліфікаційної роботи: БОРСУКОВСЬКИЙ Юрій, к.т.н., доцент,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
Технологія та засоби запобіганню поширенню загроз в промисловій мережі IoT зі використанням концепції «Industrial Treat Defence»;
Наукова та технічна література, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Сучасний стан безпеки промислових мереж IoT.
2. Аналіз можливих загроз.
3. Розробка системи захисту промислової мережі IoT.

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми захисту промислових мереж IoT.	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз загроз промисловим мережам IoT.	27.10. 2023р.	
4.	Методи та засоби управління безпекою промислових мереж IoT.	03.11.2023 р.	
5.	Розробка системи захисту промислових мереж IoT.	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату.	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач вищої освіти _____ Ілля БАСЮК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій Борсуковський
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Басюк І.Б. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія та засоби запобіганню поширенню загроз в промисловій мережі IoT із використанням концепції «Industrial Treat Defence».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***БАСЮК Ілля*** обрав тему роботи, метою якої було дослідити зміст технології контролю та засобу запобіганню до промислової мережі IoT. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***БАСЮК Ілля*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***БАСЮКА Іллі*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач ***БАСЮК Ілля*** допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

студента Басюка Іллі Богдановича

на тему: «Технологія та засоби запобіганню поширенню загроз в промисловій мережі IoT із використанням концепції «Industrial Treat Defence»

Актуальність:

Промислові мережі IoT («інтернет речей») отримують все більше розповсюдження. Постійно зростаючий попит на автоматизацію та просту передачу даних змушує розробників створювати все більш досконалі, швидші та безпечніші мережі. На жаль, із зростанням популярності також зростає ризик витоку конфіденційних даних, збільшуються загрози та підвищується ймовірність несанкціонованого доступу. Постійно розробляються засоби, які унеможливлюють реалізацію подібних небезпечних сценаріїв. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу в роботі встановлено мінімальні вимоги як щодо безпеки промислових мереж IoT, так і щодо унеможливлення втручання до обладнання користувача.

2. Досліджено комбінація варіантів які дозволяють добре розподілити, де і як користувач матиме доступ до захищеної промислової мережі IoT.

3. Розроблено рекомендації щодо застосування концепції «Industrial Treat Defence» для запобігання негативного впливу загроз.

Недоліки:

1. У кваліфікаційній роботі доцільно було б провести аналіз застосування апаратних методів захисту промислових мереж IoT.

2. Бажано було розглянути ситуацію, яка складається з комбінованими загрозами в промислових мережах IoT.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **БАСЮК Ілля** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: _____ Олександр ТУРОВСЬКИЙ

д.т.н., професор *підпис* *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи и на здобуття освітнього ступеня магістра : 84 сторінок., 8 рисунків., 3 таблиці., 42 джерела.

Об'єкт дослідження – засоби та методи безпеки в промислових мережах IoT.

Предмет дослідження – технології та методи, що застосовуються для запобігання поширенню загроз в промисловій мережі IoT.

Мета роботи – розробка рекомендацій щодо запобігання поширенню загроз в промисловій мережі IoT.

Методи дослідження – опрацювання літератури, присвяченої промисловим мережам IoT та запобіганню поширення загроз в цих мережах, вивчення та аналіз експлуатаційної документації, стандартів та проведення їх порівняння.

В роботі наведена основна інформація щодо промислових мереж IoT, приведенні основні поняття та описана структура даних мереж, описані існуючі системи захисту та пропонуються нові подібні системи.

Описані можливості застосування засобів Industrial Treat Defence для запобігання розповсюдженню загроз.

Представлені компоненти захищеної мережі IT, описані основні складові компоненти такої мережі.

Досліджені методи протоколів та алгоритми розроблюваної системи, обґрунтовані способи їх застосування.

Галузь використання – кібербезпека промислової мережі.

КЛЮЧОВІ СЛОВА: IOT, ПРОМИСЛОВИЙ ЗАХИСТ, КІБЕРБЕЗПЕКА, ПРОМИСЛОВА МЕРЕЖА IoT, ЗАХИСТ СИСТЕМ, ВІДДАЛЕНИЙ КОРИСТУВАЧ, ПРОТОКОЛИ ПЕРЕДАЧІ ДАНИХ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, СЕРВЕР, ШИФРУВАННЯ ДАНИХ, КОНТРОЛЬ ДОСТУПУ ДО МЕРЕЖІ.

ABSTRACT

Text part of the master's qualification work : 84 pages, 8 pictures, 3 table, 42 sources.

The purpose of the work is to develop recommendations for preventing the spread of threats in the industrial IoT network.

Object of research - security tools and methods in industrial IoT networks.

Subject of research - the methods and means of ensuring the security of the development of recommendations for preventing threats in industrial IoT networks.

Research methods - elaboration of literature on this topic, analysis of operational documentation, international standards and their comparison, conducting an experiment.

Basic information over is in-process brought about industrial IoT networks, including key concepts and a description of network data structures, relevant algorithms are detailed in the study.

Possibility of application facilities of Industrial Treat Defence tools for preventing threat proliferation are described thoroughly.

The components of the secured IoT network are presented, elucidating the core elements of such a network.

The possibilities components of a secure IoT network encompass a detailed description of its fundamental elements.

The method of protocols and algorithms are justified and their applications explained comprehensively.

The field of use is cyber security of the industrial network.

KEYWORDS: IOT (INTERNET OF THINGS), INDUSTRIAL THREAT DEFENSE, CYBERSECURITY, INDUSTRIAL IOT NETWORK, SYSTEM PROTECTION, REMOTE USER, DATA TRANSMISSION PROTOCOLS, SOFTWARE SOLUTIONS, SERVER, DATA ENCRYPTION, NETWORK ACCESS CONTROL.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT – Internet of Things (Інтернет речей)

IIoT – Industrial Internet of Things (промисловий Internet речей)

Industrial Threat Defence – захист від промислових загроз

DoS – Denial of Service (відмова в обслуговуванні)

DDoS – Distributed Denial of Service (розподілена відмова в обслуговуванні)

SIEM – Security information and event management (інформація про безпеку та управління подіями)

SOC – Security Operation Center (операційний центр безпеки)

Trusted Platform Module – модуль надійної платформи

ПЗ – програмне забезпечення

ВСТУП

Актуальність дослідження. В даний час велике поширення набув «Інтернет речей» (IoT) та його промислова реінкарнація «промисловий інтернет речей» (IIoT). Це система об'єднаних комп'ютерних мереж та підключених промислових (виробничих) об'єктів із вбудованими датчиками та ПЗ для збору та обміну даними, з можливістю віддаленого контролю та управління в автоматизованому режимі, без участі людини.

У міру автоматизації та поширення «безлюдних» заводів кількість подібних мереж зростає в геометричній прогресії. З одного боку це добре, але з іншого боку подібні мережі ґрунтуються на технології бездротової передачі даних, яка характеризується підвищеною вразливістю. У зв'язку з цим зростає ризик витоку конфіденційних даних, збільшується ризик несанкціонованого доступу до пристроїв, що входять до мережі.

На сучасних автоматизованих підприємствах використовуються не лише локальні та глобальні мережі, а також й промислові мережі IoT. Такі мережі є беспровідними, тому вони більш чутливі до зовнішніх перешкод і більш чутливі до небезпек та звонішніх вторгнень. Тому перед автором постає завдання розробити рішення, яке було б достатньо безпечним, надійним і водночас легким у налаштуванні з боку користувача.

Враховуючи вищезазначене, доцільним є дослідження структури промислової мережі (IoT), що базується на використанні мережевих пристроїв компанії Cisco, яка спеціалізується на реалізації та експлуатації мережевих пристроїв та засобів. Завдяки цьому забезпечується сумісність та можливість використання по максимуму функціоналу, який пропонується технологіями наведеної компанії. Завдяки цьому з’являються додаткові можливості полегшення розробки рішень для віддаленого безпечного доступу співробітників, а також гарантується безпека інформації, яка розповсюджується в промислових мережах IoT.

Об’єкт дослідження – промислава мережа IoT.

Предмет дослідження – методи та засоби забезпечення безпеки промислової мережі IoT.

Мета роботи – розробити рекомендації щодо забезпечення безпеки в промислових мережах IoT.

Наукові завдання:

– ознайомитися с основними загрозами в промислових мережах IoT;

– проаналізувати основні аспекти безпечного підключення користувачів до мереж IoT;

– дослідити умови уникнення необхідності застосування ускладненої конфігурації технічного обладнання, що реалізує роботу промислової мережі IoT;

– виокремити можливі конфігурації і способи розгортання промислової мережі IoT, та вибір найбільш раціонального варіанту;

– дослідити можливості застосування мережевих ресурсів для розробки структури промислової мережі IoT;

– провести досліджень протоколів і алгоритмів, які використовуються в промислових мереджах IoT.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

Практичне значення одержаних результатів: полягає в дослідженнях які можуть розширити перелік ефективних рішень у напрямку проектування структур промислових мереж IoT. Ці рішення можуть досить ефективно застосовуватися до різних груп користувачів. Їх поєднання є основою для отримання оптимальних результатів, у відповідності до потреб адміністраторів.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 ПРОБЛЕМАТИКА ЗАХИСТУ ПРОМИСЛОВИХ МЕРЕЖ ІОТ

1.1 Аналіз сучасного стану безпеки промислових мереж

1.1.1 Основні поняття та структура захищених промислових мереж

Структура та принцип роботи промислового інтернету речей. Принцип роботи технології полягає в наступному: спочатку встановлюються датчики, виконавчі механізми, контролери та людино-машинні інтерфейси на ключові частини обладнання, після чого здійснюється збір інформації, яка згодом дозволяє компанії придбати об'єктивні та точні дані про стан підприємства. Оброблені дані доставляють у всі відділи підприємства, що допомагає налагодити взаємодію між співробітниками різних підрозділів та приймати обґрунтовані рішення [2].

Крім цього, компанії можуть замінити паперову документацію, що швидко застаріває, а також акумулювати експертні знання фахівців [1].

Отримана інформація може бути використана для запобігання позаплановим простоям, виходу з ладу обладнання, скорочення позапланового техобслуговування та збоїв в управлінні ланцюжками постачання, тим самим дозволяючи підприємству діяти більш ефективно.

Під час обробки величезного масиву неструктурованих даних їх фільтрація та адекватна інтерпретація є пріоритетним завданням для підприємств. У даному контексті особливої значущості набуває коректне подання інформації у зрозумілому користувачеві вигляді, для чого сьогодні на ринку представлені передові аналітичні платформи, призначені для збору, зберігання та аналізу даних про технологічні процеси та події в реальному часі.

Згідно з дослідженням консалтингової компанії IDC [4], у 2011 році людством було згенеровано 1,8 зеттабайт інформації. У 2012 році обсяг цінних даних збільшився майже вдвічі і становив 2,8 зеттабайт. До 2020 року ця цифра вже сягнула 40 зеттабайт. Такі великі обсяги даних вимагають обробки, щоб бути використаними в процесі прийняття рішень.

Щоб уникнути простоїв та для дотримання безпеки на підприємстві, необхідно впровадження технологій, що дозволяють виявляти та прогнозувати ризики. Безперервний проактивний моніторинг ключових показників дає можливість визначити проблему та вжити необхідних заходів для її вирішення. Для зручності операторів сучасні системи дозволяють візуалізувати умови протікання технологічних процесів і виявляти фактори, що впливають на них, за допомогою будь-якого веб-браузера. Оперативний аналіз допомагає користувачам швидше знаходити причини несправностей.

Завдяки таким рішенням виробничі дані перетворюються на корисну інформацію, яка необхідна для безпечного та раціонального управління підприємством.

Впровадження таких технологій дає змогу підприємствам із різних галузей економіки отримати певні переваги: збільшити ефективність використання виробничих активів на 10% за рахунок скорочення кількості незапланованих простоїв; знизити витрати на технічне обслуговування на 10%, удосконаливши процедури прогнозування та запобігання катастрофічним відмовам обладнання та виявляючи неефективні операції; підвищити продуктивність на 10%, збільшити рівень енергоефективності та скоротити експлуатаційні витрати на 10% за рахунок більш ефективного використання енергії [5].

Таким чином, нові технології дозволяють підприємствам різних галузей промисловості досягти суттєвих конкурентних переваг.

Як промисловий інтернет речей трансформує економіку:

Промисловий інтернет речей кардинально змінює всю економічну модель взаємодії «постачальник – споживач». Це дозволяє виконувати наступне:

- автоматизувати процес моніторингу та управління життєвим циклом обладнання;
- організувати ефективні ланцюжки, що самооптимізуються, від підприємств – постачальників до компаній – кінцевих споживачів;
- перейти до моделей «економіки спільного використання» та багато іншого.

У найбільш розвинених випадках промисловий Інтернет речей дозволяє не тільки підвищити якість технічної підтримки обладнання з використанням розвинених засобів телеметрії, а й забезпечити перехід до нової бізнес-моделі його експлуатації, коли обладнання оплачується замовником за фактом використання його функцій.

Впровадження мережевої взаємодії між машинами, обладнанням, будинками та інформаційними системами, можливість здійснювати моніторинг та аналіз навколишнього середовища, процесу виробництва та власного стану в режимі реального часу, передавача функції управління та прийняття рішень інтелектуальним системам призводять до зміни «парадигми» технологічного розвитку, яка також називається «четвертою промисловою революцією».

Зарубіжні експерти визнають Інтернет речей технологією, яка вносить незворотну трансформацію в організацію сучасних виробничих та бізнес-процесів та породжує нові бізнес-моделі.

Проведений консультантами J`Son&Partners Consulting аналіз досвіду впровадження Інтернету речей у світі показує, що перехід на концепцію IIoT відбувається за рахунок формування крос-індустріальних відкритих (по горизонталі та вертикалі) виробничо-сервісних екосистем, що поєднують безліч різних інформаційних систем управління різних підприємств та задіють безліч різних пристроїв [6].

Такий підхід дозволяє реалізувати у віртуальному просторі як завгодно складні наскрізні бізнес-процеси, які здатні в автоматичному режимі здійснювати оптимізаційне управління (наскрізний інжиніринг) різноманітних ресурсів через весь ланцюжок поставок і створення вартості продукції - від розробки ідеї, дизайну, проектування до виробництва, експлуатації та утилізації.

Для реалізації такого підходу потрібно, щоб вся необхідна інформація про фактичний стан ресурсів (сировина та матеріали, електроенергія, верстати та промислове обладнання, транспортні засоби, виробництво, маркетинг, продажі) як усередині одного, так і на різних підприємствах була доступна

автоматизованим системам управління різних рівнів (приводи та сенсори, контроль, управління виробництвом, реалізацією та плануванням).

Таким чином, можна сказати, що промисловий інтернет речей є організаційно-технологічною трансформацією виробництва, що базується на принципах «цифрової економіки», що дозволяє на рівні управління об'єднувати реальні виробничі, транспортні, людські, інженерні та інші ресурси в програмно-керовані віртуальні, що практично необмежено масштабуються. Пули ресурсів (shared economy) надають користувачеві не самі пристрої, а результати їх використання (функції пристроїв) за рахунок реалізації наскрізних виробничих та бізнес-процесів (наскрізного інжинірингу) [6].

Відмінністю екосистеми IoT від традиційних ринків є трансформація підприємств із ізольованих самодостатніх систем, усередині яких реалізовано всі необхідні для виробництва товару або послуги виробничі та бізнес-процеси, у відкриті системи інтегрованих високоавтоматизованих процесів. Такі відкриті системи реалізовані за моделлю хмарних сервісів, у яких різні учасники ринку об'єднані в єдину платформу надання послуг кінцевому споживачеві, для створення якої основними засобами виробництва виступає не персонал, а хмарні сервіси, що автоматично керують об'єднаними в пули програмно-визначними пристроями.

Іншими словами, для традиційних підприємств та їх систем (ринків) базовим ресурсом, необхідним для безпосереднього управління всіма іншими видами ресурсів, є персонал і, як наслідок, основним видом інформаційного обміну в таких системах є обмін голосовою інформацією та даними між людьми. А для екосистем IoT, які не використовують ручну працю безпосередньо при виконанні виробничих процесів, та система управління яких автоматично звертається безпосередньо до необхідних виконавчих пристроїв та сенсорів, базовим ресурсом є інформація та автоматичні засоби її обробки.

Впровадження інтернету речей потребує зміни підходів до створення та використання автоматизованих інформаційних систем управління (АСУ) та загальних підходів до управління підприємствами та організаціями. Застарілі

виробничі лінії, які з різних причин не можуть бути автоматизовані за допомогою IoT, можуть бути замінені на нове автоматизоване та роботизоване обладнання у майбутньому. Іншою перешкодою, що обмежує розвиток IoT, є відсутність або недостатньо високий розвиток традиційних корпоративних інформаційних систем управління (ERP), тоді рішення IoT будуть локальними та вирішуватимуть нішеві функції та завдання [7].

IoT може послідовно еволюціонувати від підключення окремих продуктів та об'єктів з метою їх діагностики та контролю до об'єднання різних продуктів і більш складних технологічних об'єктів управління в мережі IoT, а мережі IoT у складніші мережеві платформи та комплексні виробничі рішення (рис. 1.1).

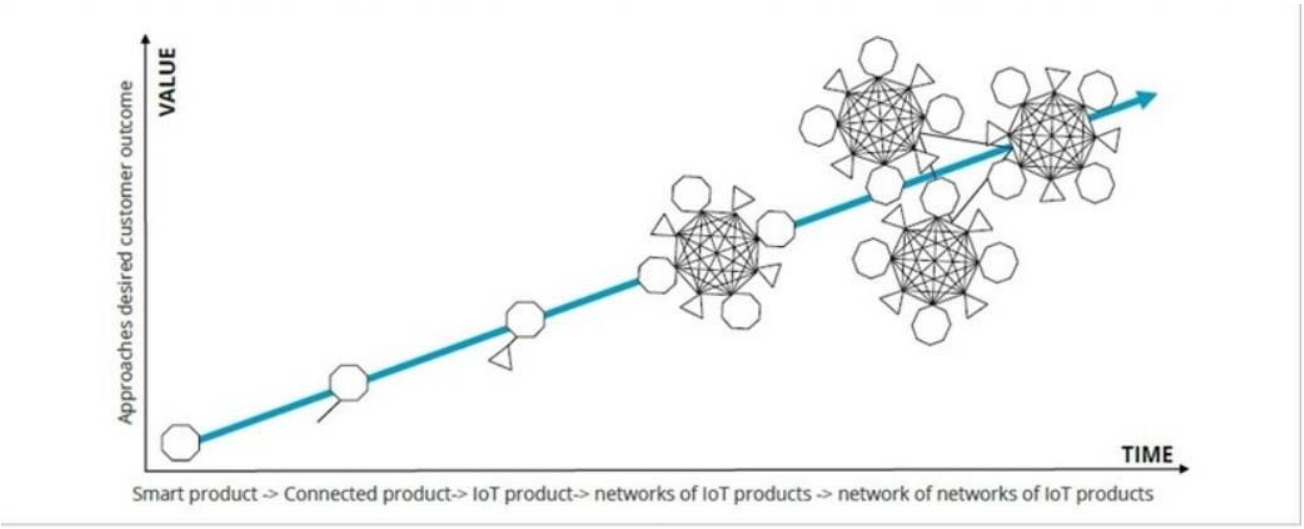

Рис. 1.1. Еволюція продуктів та рішень інтернету речей

1.1.2 Концепція Industrial Threat Defence

Завдяки концепції Cisco Industrial Threat Defence можливо побудувати промислову мережу IoT, яка відповідає наступним критеріям:

Видимість інтернету речей та виявлення загроз:

Оцінка ризиків. Захист від промислових загроз використовує вашу існуючу мережу, щоб забезпечити повну видимість, щоб ви могли виявляти загрози в масштабі та зміцнювати свою позицію промислової безпеки.

Сегментація промислової мережі

Запобігання поширенню загроз. Якщо ви будуєте свою промислову DMZ, створюєте зони та канали чи переходите на стратегію мікросегментації без довіри, Industrial Threat Defense допоможе вам [8].

Конвергентне дослідження та усунення загроз:

Використовання наявних інструментів та методів безпеки. Industrial Threat Defense додає події безпеки та контекст до вашого операційного центру безпеки (SOC), щоб ви могли створити справді конвергентну стратегію безпеки.

1.2 Аналіз загроз безпеці мереж IoT

Широке проникнення промислового інтернету речей у критично важливу інфраструктуру та виробничий сектор призвело до збільшення кількості потенційних кібератак. Про це свідчать дані дослідження, проведеного аналітиками компанії Frost & Sullivan, про що стало відомо 13 грудня 2018 [4].

На їхню думку, кібератаки лише в енергетичній та комунальній галузях обходяться в середньому в $13,2 млн щорічно. Експерти компанії Frost & Sullivan зазначають, що підвищення ризиків призводить до вироблення спільних підходів до забезпечення кібербезпеки. Свою роль відіграють посилення регулятивної ролі урядів країн світу в галузі безпеки та збільшення поінформованості про проблему і на зрілих ринках, і на молодих.

Перед розробкою та впровадженням захисних рішень проти різних атак на IoT-пристрої дуже важливо розуміти, які можливості має атакуючий і які цілі переслідує. Зловмисник може отримати фізичний доступ до простих та недорогих пристроїв, регулярний моніторинг та постійний захист яких не завжди може бути практично та фінансово здійсненний. Фізичний контроль над такими пристроями відкриває можливості для атак сторонніми каналами, включення апаратних

помилок і троянів, а також заміни підробленими пристроями. У цій статті ми розглянемо лише кібератаки, які здійснюються через програмне забезпечення та мережу. Основною метою кібератак є спотворення вихідних даних (і наступних дій через неправильні дані) пристрою, або порушення поточних процесів (відмова в обслуговуванні), або розкриття будь-якої секретної інформації, що зберігається на пристроях, такий як секретні ключі та паролі. Сучасні пристрої збирають масиви даних про своїх користувачів. Деяким із них для роботи потрібний не тільки пароль, а й ім'я користувача, його контактна інформація, відомості про біографію. Така кількість інформації потребує надійного та якісного захисту, проте на даний момент IoT не може похвалитися захищеністю. Як проілюстровано на рис. 1.2, пристрій IoT може зазнати атак наступних типів:

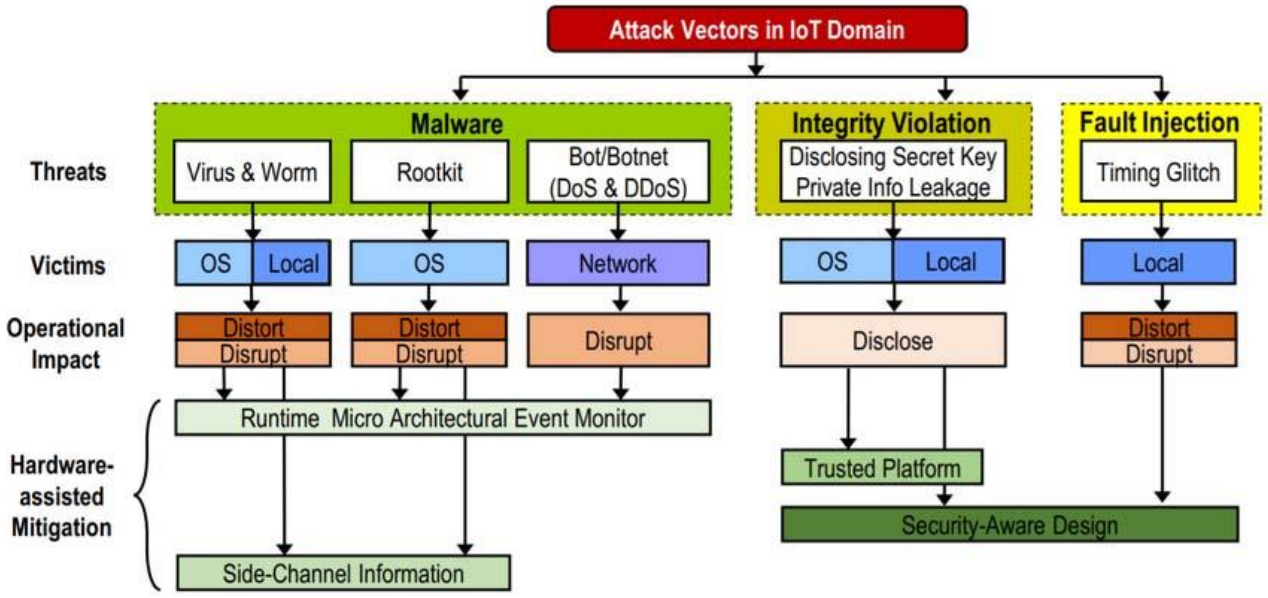

Рис. 1.2. Атаки на пристрої IoT та апаратні методи їх запобігання

Шкідливе ПЗ:

Сучасні пристрої Інтернету речей можуть бути заражені різними шкідливими програмами на різних етапах своєї роботи. У більшості випадків шкідливе ПЗ (віруси, трояни та черв'яки) зазвичай націлене на локальну експлуатацію та експлуатацію на рівні операційної системи в залежності від

складності атаки та її виконання. Основне завдання шкідливого ПЗ полягає в тому, щоб порушити поточні операції та перехопити контроль над пристроєм. Найпоширенішою зброєю зловмисників є руткіти (набори утиліт, які хакер встановлює на «зламаному» їм пристрої після отримання первісного доступу, що дозволяє хакеру закріпитися у зламаній системі та приховати сліди своєї діяльності). Таке ПЗ надає хакерам постійний привілейований доступ до системи, активно приховуючи свою присутність. Тим самим зловмисник опановує всю обчислювальну потужність і дані пристрою, а також може встановлювати невидимі користувачам драйвери і служби. Крім того, пристрої Інтернету речей можуть стати жертвою атак типу «відмова в обслуговуванні» (DoS) або розподіленої відмови в обслуговуванні (DDoS), які з кожним днем стають серйозною проблемою. Такий вразливий пристрій може працювати як бот (або «зомбі») для зараження інших допустимих пристроїв у мережі або споживати пропускну здатність мережі та обчислювальну потужність пристроїв, надаючи зловмиснику додаткові ресурси [9].

Розкриття закритого ключа:

Отримання доступу до закритого ключа (використовується для шифрування) та/або особистої інформації, що зберігається на пристрої IoT, є ласим шматочком для зловмисника, оскільки це дозволяє скомпрометувати корінь довіри систем. Це дозволяє зловмиснику отримати контроль над процесами зв'язку, захопити обчислювальні потужності пристрою, та найважливіше – конфіденційну інформацію [10].

Програмно-кероване введення збоїв:

Інший клас атак на IoT пристрої – це програмна вставка збоїв у апаратне забезпечення під час роботи пристрою. Незважаючи на те, що цей тип атак відносно складний, тому що вимагає глибоких знань апаратного забезпечення, що залежить від платформи, а також базового програмного забезпечення, засіб такої атаки дуже складно реалізувати. Оскільки цей клас атак шукає та використовує незначні вразливості в устаткуванні, марно використовувати чисто програмні захисні механізми.

Зрозуміло, існують ефективні програмні рішення для пом'якшення існуючих проблем безпеки IoT-пристроїв. Однак складні атаки та кіберзагрози не завжди можна запобігти за допомогою таких програмних методів, тому що [12]:

- Програмний механізм захисту, що використовується у пристрої IoT, сам по собі може бути вразливим для віддалених атак. Крім того, він не обов'язково має широкий захист, часто його можна обійти та зламати без відома користувача. Наприклад, атака DoubleAgent скомпрометувала багато відомих антивірусних програм, що призвело до порушення інформаційної цілісності пристроїв.
- Програмні рішення вимагають регулярних оновлень та виправлень, тоді як шкідливе ПЗ постійно розвивається та еволюціонує. До того ж, оновлення ПЗ безлічі віддалених IoT-пристроїв не завжди фізично реалізується. Тому необхідно дотримуватися концепції «поставив і забув». У цьому можуть добре зарекомендувати себе апаратні рішення.

Апаратні методи безпеки:

Апаратна безпека стала перспективною альтернативою суто програмному механізму захисту, оскільки останній сам по собі не забезпечує рівень безпеки, необхідний для сучасних IoT-пристроїв. Апаратні системи безпеки використовують апаратні модулі та можуть збирати інформацію про мікроархітектуру для аналізу переважних загроз та вразливостей на програмному рівні [13].

Використання апаратних засобів безпечного створення ключів шифрування:

Однією з основних вимог для виконання захищеної інформаційної транзакції між пристроями IoT через ненадійну мережу є використання надійної та безпечної схеми управління ключами та обробки даних на устаткуванні. У цьому відношенні добре зарекомендували себе Trusted Platform Module (TPM-назва специфікації, що описує криптопроцесор, в якому зберігаються криптографічні ключі для захисту інформації, а також узагальнене найменування реалізацій зазначеної специфікації), рис. 1.3. Такі модулі TPM дозволяють

використовувати криптографічні ключі, які можуть бути прив'язані до певних параметрів платформи та захищені від розкриття будь-яким іншим ненадійним апаратним компонентом, процесом або програмним забезпеченням. Мікросхеми з дискретним TPM (dTPM) та модулі пластикових друкованих плат можуть запропонувати більший охоплення послуг, дозволяючи спільно використовувати ресурси між кількома програмами на одній фізичній машині. Крім того, архітектури з підтримкою ARM TrustZone та Intel Software Guard Extension (SGX) додають нові функції в сучасні SoC (system on a chip), надаючи надійне та безпечне середовище для виконання критично важливих для безпеки процесів, навіть незважаючи на те, що привілейоване ядро та програмне забезпечення потенційно шкідливі. З іншого боку, криптозахищені процесори, такі як AEGIS і Ascend, використовують однокристальну архітектуру для забезпечення приватної та автентичної обробки із зашифрованим та заплутаним виконанням інструкцій. Однак такі конструкції в основному забезпечують захист від фізичних атак, таких як втручання та зондування внутрішніх компонентів, та не забезпечують захист від кіберзагроз у разі компрометації самої програми.

Рис. 1.3. Модуль TPM

Хоча TPM та інші системи криптографічної стійкості пропонують надійне середовище для додатків, чутливих до безпеки, таке обладнання зазвичай дороге, енергоємне і не підходить для легких і недорогих IoT-пристроїв. Крім того, шкідливі програми, такі як віруси, трояни та боти, можуть непомітно заражати пристрої в обхід таких систем, якщо мережа недостатньо захищена. Безпосередньо після зараження дуже складно виявити шкідливе програмне забезпечення, оскільки воно може обійти антивірусні програми на пристрої. У таких випадках може допомогти апаратний моніторинг подій мікроархітектури та SIEM-системи (Security information and event management). Він пропонує тонку фільтрацію для окремих запусків, може збирати багатовимірну інформацію та забезпечує швидший відгук, ніж програмні аналоги для захисту від шкідливих програм [14].

Мікроархітектурний моніторинг подій

Хоча TPM та інші системи криптографічної стійкості пропонують надійне середовище для додатків, чутливих до безпеки, таке обладнання, як правило, дороге, енергоємне та не підходить для легких та недорогих IoT пристроїв. Крім того, шкідливі програми, такі як віруси, трояни та боти, можуть непомітно заражати пристрої в обхід таких систем, якщо мережа недостатньо захищена. Безпосередньо після зараження дуже складно виявити шкідливе програмне забезпечення, оскільки воно може обійти антивірусні програми на пристрої. У таких випадках може допомогти апаратний моніторинг подій мікроархітектури та SIEM-системи (Security information and event management). Він пропонує тонку фільтрацію для окремих запусків, може збирати багатовимірну інформацію та забезпечує швидший відгук, ніж програмні аналоги для захисту від шкідливих програм.

Ядром таких апаратних моніторів є блоки моніторингу продуктивності (PMU), доступні в сучасних процесорах та SoC. Основна мета PMU – надати уявлення про продуктивність ЦП шляхом реєстрації набору мікроархітектурних подій та відповідних підрахунків за допомогою вбудованих апаратних лічильників продуктивності (HPC). Наприклад, один або кілька HPC в PMU

можуть визначати, скільки разів заздалегідь певна подія (дозволена відповідною архітектурою), така як промахи кешу, відбувається під час виконання програми, що служить для оцінки продуктивності системи, що тестується. PMU в архітектурах ARM та Intel x86 можна керувати через програмні модулі, такі як Linux Perf tool. Він надає зворотний зв'язок у режимі реального часу для діагностики помилок або виявлення вузьких місць у програмному забезпеченні. Спочатку PMU був розроблений для моніторингу продуктивності, але його також розумно використовувати в SIEM-системах, що суттєво прискорює обробку інцидентів, пов'язаних з інформаційною безпекою, а також допомагає виявляти атаки та інші загрози елементам інфраструктури. Ще одна перевага полягає в тому, що, будучи інтегрованою частиною обладнання, PMU працює прозоро для будь-якого програмного забезпечення, запущеного на процесорі, і не може бути обманутим зовнішнім шкідливим ПЗ. Тобто апаратний монітор не звертає уваги на процеси. Оскільки будь-яке шкідливе програмне забезпечення або навіть модифікована прошивка або руткіт повинні виконувати певні дії, моніторинг подій PMU потенційно здатний виявляти такі шкідливі дії.

Розробники з NYU Polytechnic School of Engineering, Brooklyn, New York, USA [15] запропонували засновану на хості структуру виявлення DDoS-атак під назвою BRAIN (BehavioR based Adaptive Intrusion detection in Networks). Він використовує апаратні функції для моделювання безпечної поведінки та DDoS-атак. Щоб виявити DDoS-атаки, він використовує методи машинного навчання для моделювання поведінки додатків та мережевої статистики. Оскільки кореляція між статистикою мережі та програмами з даними HPC нетривіальна, необхідно вибирати апаратні події з високою точністю. Автори запропонували реалізувати інтегрований механізм виявлення DDoS-атак (DDoSDE), який відстежує поведінку як устаткування, і мережі. Інтерфейс запобігання DDoS-атак (DDoSPI) реагує на будь-яку виявлену атаку, заносячи IP-адреси до чорного списку (і видаляючи при необхідності) на основі динамічної мережі та порогового значення на основі HPC, тим самим заважаючи зловмиснику вивчити критерії та політики безпеки пристроїв.

Підвищення безпеки за допомогою методів машинного навчання

Однією з основних перешкод для використання моніторингу подій мікроархітектури є те, що одна і та сама подія мікроархітектури може відбуватися аналогічним чином (тобто підрахунок частоти та профіль події) під час допустимої операції і, отже, це може не бути очевидним індикатором для позначення конкретного софту як шкідливого. Для вирішення цієї проблеми дослідники розробили різні методи машинного навчання, що дозволяють вивчати та розрізняти такі події, а також ідентифікувати будь-який вид аномалії з більш високою точністю виявлення та меншою кількістю помилок. Дві основні вимоги до таких методів:

- вибір високоточних мікроархітектурних функцій для збору подій за допомогою високопродуктивних обчислень;
- вибір ефективних методів машинного навчання для завдань класифікації та регресії.

Для задоволення цих вимог необхідно розробити архітектуру, яка аналізує дані щодо поведінки системи, отриманих від HPC. Ключові спостереження для побудови такої структури полягають у наступному. По-перше, семантика програми істотно не змінюється, навіть якщо зловмисник спробує її реструктурувати. По-друге, під час виконання тієї чи іншої завдання існують підзавдання, які не можна радикально змінювати. Ґрунтуючись на цих припущеннях, блок виявлення аномалій на основі машинного навчання повинен виконувати такі завдання (див. рис. 1.4).

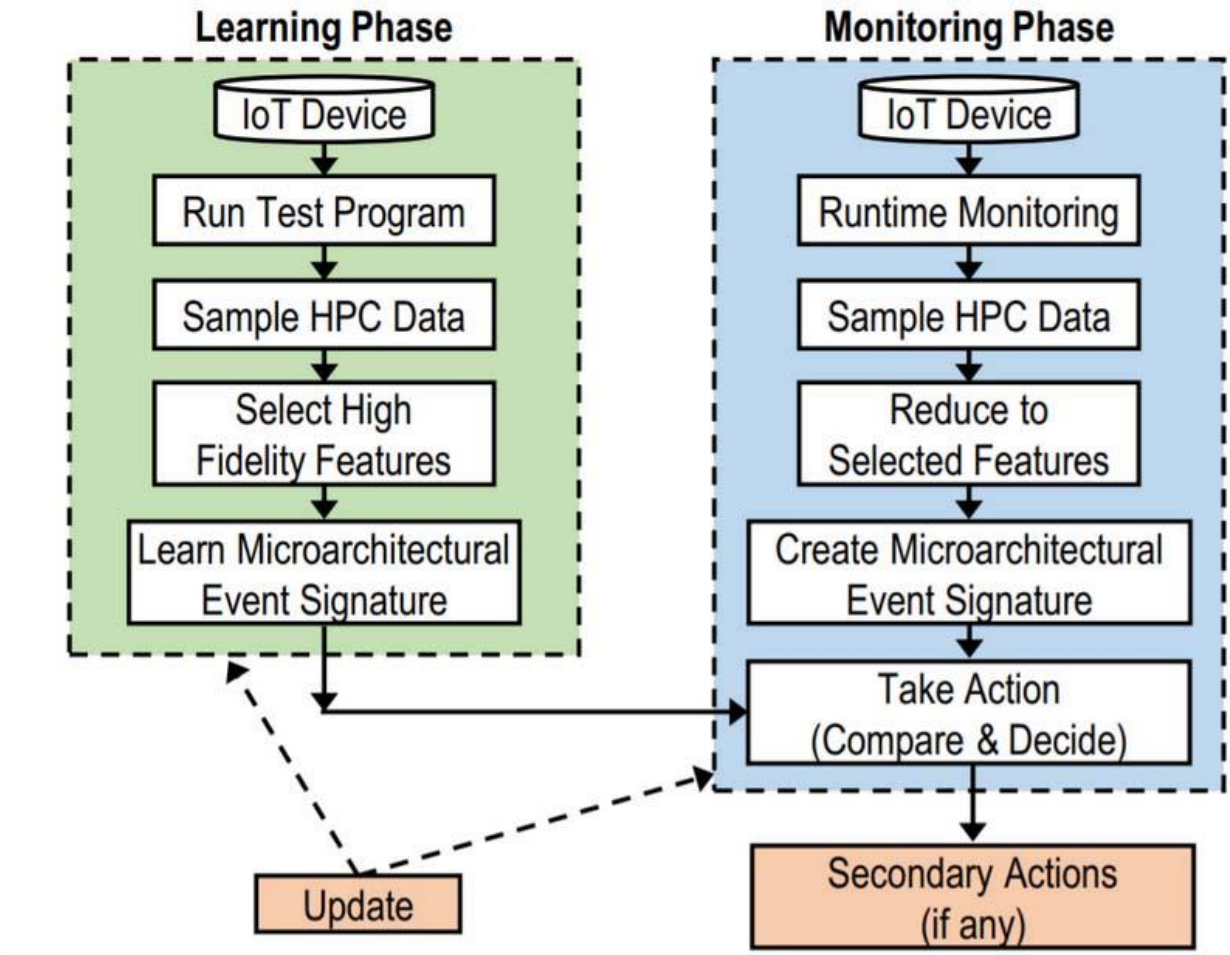

Рис. 1.4. Блок виявлення аномалій на основі машинного навчання

1. *Збір даних*

На цьому етапі алгоритм вирішує, які дані про мікроархітектурні події необхідно зібрати і як механізм виявлення повинен зберігати та обробляти зібрану інформацію.

2. *Аналіз даних*

Цей етап визначає шкідливу поведінку (якщо така є) шляхом аналізу даних. Класифікатори машинного навчання використовуються для навчання, тестування та перевірки кореляції між зібраними даними та ненадійною поведінкою.

3. *Прийняття рішення*

На цьому етапі вживаються заходи щодо виявлення загрози. Це може бути повідомлення користувачу про потенційну загрозу, завершення підозрілих

процесів, або більш критичне події, наприклад, відключення всього пристрою для захисту даних і системи.

Модуль виявлення вразливостей періодично отримує інформацію HPC від цільового модуля, у якому працює ненадійна програма чи шкідливе ПО. Архітектура системи повинна дозволяти модулю виявлення працювати з найвищим рівнем привілеїв та незалежно від будь-якої іншої програми. Крім того, вона повинна надавати доступ до фізичної пам'яті для зберігання даних HPC і мати ізольовану пам'ять, щоб модуль виявлення не був пошкоджений. Об'єм пам'яті, необхідний для зберігання даних машинного навчання, сильно різниться залежно від типу класифікатора, що використовується для аналізу, що потребує додаткового місця у пам'яті та обчислювальної потужності. Як можна зрозуміти, точність використовуваного методу машинного навчання та детальний дозвіл дискретизованих даних HPC для вибраних подій відіграють життєво важливу роль для підвищення точності та продуктивності всієї системи виявлення.

З метою підвищення ефективності зв'язки HPC +ML було проведено всебічний аналіз з використанням інформації про високопродуктивні обчислення під час їх виконання. Він показує, що програмна реалізація різних методів машинного навчання на рівні ядра ОС є надзвичайно повільною, в діапазоні мілісекунд, що досить велике в порівнянні з часом виконання шкідливого програмного забезпечення та вибірки даних на апаратному рівні. Очевидно, що методи класифікації на рівні програмного забезпечення недостатньо підходять для збору даних та виявлення аномалій з високим ступенем впевненості. Отже, для нижчої затримки та вищої точності потрібна апаратна реалізація методу машинного навчання. Для цього ML фахівці надали свої рішення на апаратних платформах, таких як Virtex 7 для порівняльного аналізу. Було виявлено, що метод OneR був найбільш ефективним класифікатором доброякісних та шкідливих програм з найвищою точністю та найменшим використанням обчислювальної потужності, а загальний успіх виявлення становив близько 81%.

Дизассемблери рівня інструкцій на основі побічних каналів

Застосування дизассемблера різноманітне - його можна використовувати для відстеження та реконструкції коду, зворотного проектування вихідного, спільної атестації апаратно-програмного забезпечення та, що найбільш важливо, для перевірки цілісності програмного забезпечення, що працює на пристрої IoT.

Широко відомий такий клас кіберзагроз, як атака сторонніми каналами. Такі атаки порушують конфіденційність криптосистем, використовуючи інформацію про фізичні процеси в пристрої, що протікають, наприклад вимірюючи час виконання операції, вольт-амперні характеристики, електромагнітне випромінювання пристрою і так далі. Зловмисники, збираючи достатньо статистичних даних, після певного аналізу можуть припустити, який алгоритм використовується в криптосистемі, отримати доступ до секретних ключів або внести зміни в алгоритм. Таким чином, зловмисник легко обходить захист і опановує IoT-пристроєм. Але чому б не використати цю вразливість на благо? З тим самим успіхом можна виявити, чи виконує IoT пристрій підозрілі інструкції, є він «зараженим» чи ні. Достатньо лише зафіксувати якесь фізичне відхилення в поведінці пристрою (рис. 1.5).

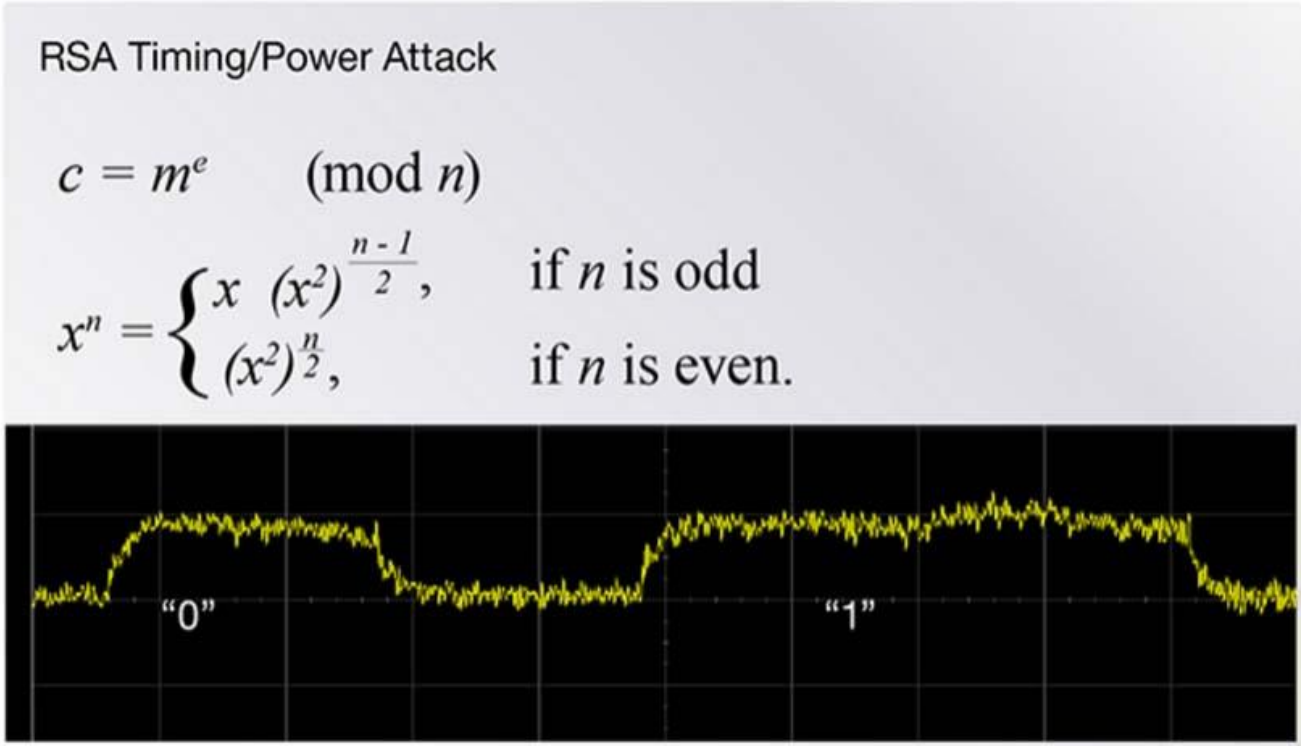

Рис. 1.5. Виявлення відхилень в поведінці пристроя IoT

Дослідження показали, що більшість шкідливих програм може бути виявлено за допомогою збоїв харчування по побічним каналам. Пропонована ними система контролює енергоспоживання пристрою та використовує метод машинного навчання для виявлення потенційної аномальної поведінки. Такі методи можуть використовуватися для атестації та аутентифікації пристроїв IoT у ненадійній мережі.

Також було реалізовано систему моніторингу часу виконання, що використовує електромагнітні випромінювання (EI) як побічний канал. Вона може виявляти ненормальну поведінку під час виконання програми, таке як впровадження шкідливого програмного забезпечення або іншого коду, за допомогою контрольованих класифікаторів машинного навчання. Ця схема вимагає визначення характеристик шкідливого ПЗ. Вона використовує піки у виміряному електромагнітному спектрі під час виконання програми та порівнює їх із золотими даними фази навчання. Цей метод потенційно добре підходить для моніторингу безпеки IoT і вбудованих пристроїв, оскільки він не вимагає додаткових ресурсів на машині, що відстежується, не вимагає провідного з'єднання, як у випадку збору інформації про побічний канал живлення.

1.3 Проблеми, які вирішуються в роботі

Враховуючи вимоги до захисту сучасних корпоративних мереж IoT, можна зформулювати наступні задачі поточної роботи:

- визначення основних умов безпечної роботи користувачів в корпоративній мережі IoT;
- визначення можливих конфігурацій і способів розгортання захищеної корпоративної мережі IoT, та вибір раціонального варіанту;
- провести аналіз функціональних можливостей розроблюваної системи;
- роозробити систему контролю доступу до мережі IoT;

- скласти висновки за результатами досліджень.

1.4 Висновки до першого розділу

Досліджено основні поняття в області побудови промислових мереж (IIoT), а також структура типової промислової мережі IoT.

Проаналізовано концепцію Cisco Threat Defence, а саме структурні складові цієї концепції та їх роль в забезпеченні безпеки даних та користувачів промислових мереж IoT.

Визначені основні загрози в промислових мережах IoT на практичних прикладах. Також окреслені вразливі місця промислових мереж IoT.

Коротко розглянуті апаратні та програмі засоби, які дозволяють гарантувати безпеку даних та користувачів промислових мереж IoT.

2 МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРОМИСЛОВИХ МЕРЕЖ IOT

2.1. Засоби забезпечення безпеки промислового інтернета речей

В промисловому інтернеті речей застосовуються наступні технології забезпечення безпеки, які наведені в таблиці [15].

Таблиця 1.1

Технології, які застосовуються в індустріальному інтернеті речей

Назва технології	Опис
Кінцеві пристрої IoT	Пристрої, оснащені вбудованими технологіями збору, обробки, зберігання, передачі, інтелектуального прийняття рішень;
Міжмашинний зв'язок (M2M)	Технологія, що полегшує прямий зв'язок між пристроями у мережі без участі людини;
Аналіз Big Data	Процес вивчення величезної кількості різних типів наборів даних, відео та аудіо, згенерованих у реальному часі інтелектуальними датчиками, пристроями та журналами;
Робототехніка	Удосконалені промислові роботи, наділені для вирішення складних завдань інтелектуальними можливостями, такими як здатність вчитися на своїх помилках та підвищувати свою продуктивність;
Штучний інтелект	Алгоритми, які дозволяють комп'ютерам та обчислювальним машинам виконувати завдання, які зазвичай виконують люди;

Машинне навчання	Алгоритми, які дозволяють комп'ютерам діяти та покращувати здатність прогнозувати без явного програмування;
Прогнозне обслуговування	Рішення, які відстежують стан обладнання, прогнозуючи, коли може статися збій, для ефективного обслуговування з мінімально можливою частотою;
Моніторинг у режимі реального часу	Технології, що дозволяють збирати та об'єднувати дані про безпеку від компонентів системи, а також відстежувати та аналізувати події, що відбуваються в мережі;
Розширена аналітика збитків	Методи аналізу різних типів втрат, які можуть виникнути в середовищі, з метою їх усунення чи зменшення;
Комп'ютерні обчислення	Рішення, що забезпечують доступ до загальних наборів ресурсів, таких як мережі, сервери та програми, з мінімальними вимогами до управління та взаємодії з постачальником послуг;
Доповнена реальність	Технології, які змінюють сприйняття реального довкілля, інструмент для підвищення ефективності завдань (наприклад, ручного складання);

В промислових мережах IoT (IIoT) виникають наступні вразливості:

- *Вразливість пристроїв та систем.* Щодня кількість нових пристроїв стрімко зростає. Питання безпеки IIoT не можна вирішити ізольовано, не забезпечивши інші види безпеки, такі як інформаційна безпека, безпека операційних технологій та фізична безпека. У промислових умовах це може

представляти значну проблему, оскільки більшість систем цього типу були розроблені без урахування вимог безпеки [32], і тому вразливості у подібному устаткуванні виявляються дедалі частіше [33].

- *Складність управління процесами.* Крім великої площі атаки з урахуванням величезної кількості підключених пристроїв слід враховувати безліч складних процесів, пов'язаних з інтелектуальним виробництвом. У системах IIoT управління процесами є проблемою з погляду безпеки, оскільки функціональність і ефективність роботи пристроїв зазвичай вважаються пріоритетнішими, ніж безпека.
- *Конвергенція інформаційних та операційних технологій (IT/OT).* Промислові системи управління перестали бути ізольованими після того, як впровадження IT-компонентів у промисловість стало звичайною практикою. Конвергенція організацій за допомогою IT-мереж спростила управління складними середовищами, а також привнесла нові загрози безпеці. Супутні фактори включають небезпечні мережеві з'єднання (внутрішні та зовнішні), використання технологій з відомими вразливостями, які вносять раніше невідомі ризики в середовище OT, та недостатнє розуміння вимог серед ICS.
- *Складність ланцюжка поставок.* Компанії, які виробляють продукти або рішення, рідко можуть виробляти самостійно весь продукт цілком і зазвичай звертаються за допомогою у виробництві окремих компонентів до третіх осіб. Розробка технологічно складних продуктів призводить до надзвичайно складного ланцюжка поставок за участю великої кількості людей та організацій, що робить його надзвичайно складним з погляду управління. Нездатність відстежити кожен компонент до джерела означає неможливість забезпечити безпеку продукту. Безпека цілого продукту оцінюється за його найслабшою (з точки зору безпеки) ланкою.
- *Застарілі промислові системи управління.* Застаріле обладнання є суттєвою перешкодою для впровадження систем безпеки. Виробники встановлюють нові системи поверх застарілих, і це може призвести до

неефективності колишніх заходів захисту, а також прояву невідомих уразливостей, які були неактивними протягом багатьох років. Додавання нових пристроїв IoT до застарілого обладнання викликає обґрунтовані побоювання, оскільки може дозволити зловмисникам знайти новий спосіб злому систем.

- *Небезпечні протоколи.* Виробничі компоненти з'єднуються приватними промисловими мережами, використовуючи певні протоколи. У сучасних мережевих середовищах ці протоколи часто не забезпечують належного захисту від загроз.
- *Людський фактор.* Впровадження нових технологій означає, що робітники та інженери заводу повинні застосовувати нові способи роботи з новими типами даних, мережами та системами. Якщо вони не знатимуть про ризики, пов'язані зі збором, обробкою та аналізом даних, вони можуть стати легкою метою для зловмисників.
- *Функції, які не використовуються.* Промислова техніка, що не використовується, призначена для надання великої кількості функцій і послуг, частина яких може бути незатребуваною на окремому виробництві. У промислових середовищах машини або їх окремі компоненти часто використовують не весь доступний функціонал, при цьому функції, що не використовуються, можуть значно розширити область потенційної атаки і стати воротами для зловмисників.
- *Забезпечення безпеки продукту після його реалізації.* Безпека пристрою повинна бути предметом розгляду протягом усього життєвого циклу продукту, навіть у разі закінчення терміну служби пристрою [16].

2.2 Класифікація загроз в промислових мережах IoT

В сучасних промислових мережах IoT мають місце наступні загрози.

Відмова або вихід з ладу елементів системи:

а) збій або вихід з ладу кінцевих IoT-пристроїв виникає за умови неналежного обслуговування та недотримання посібників та інструкцій з експлуатації пристроїв [17];

б) відмова або вихід з ладу систем управління може статися, якщо не забезпечується належне обслуговування та дотримання посібників та інструкцій з експлуатації пристроїв;

в) експлуатація вразливостей програмного забезпечення стає можливою через відсутність оновлень, використання слабких паролів або паролів за промовчанням, а також неправильної конфігурації;

г) відмова або збій у постачальників послуг спричиняє порушення процесів, які залежать від сторонніх сервісів.

Зумисна дія:

а) відмова у обслуговуванні – атака цього може бути двунаправленной. З одного боку, вона може бути націлена на систему IIoT, при цьому в систему надсилається велика кількість запитів, що призводить до недоступності системи та збоїв у роботі (DoS-атака від англ. Denial of Service - «відмова в обслуговуванні»). З іншого боку, зловмисник може скористатися великою кількістю пристроїв IIoT в промисловому середовищі і створити армію бот-мереж IoT як платформу для атаки на будь-яку іншу систему (DDoS-атака від англ. Distributed Denial of Service – «розподілена атака типу «відмова» в обслуговуванні»);

б) шкідливе ПЗ проникає в IoT з метою виконання небажаних та несанкціонованих дій, які можуть завдати шкоди системі, операційним процесам та пов'язаним даним. Віруси, троянські коні та шпигунські програми є типовими прикладами цієї загрози;

в) управління програмним та апаратним забезпеченням або додатками пристроїв зловмисником є несанкціонованим і у сфері промислових систем IoT може включати маніпуляції з промисловим роботом, маніпуляції з пристроями та зміну їх конфігурації;

г) маніпулювання інформацією передбачає небажану та несанкціоновану зміну даних зловмисником. Сюди може входити компрометація ОТ або систем підтримки виробництва, таких як SCADA, MES та маніпулювання даними процесу. Можливі наслідки можуть включати недоречні рішення, що ґрунтуються на фальсифікованих даних;

д) цільова атака спрямована на конкретну організацію (або на конкретну людину в цій організації) з метою завдати шкоди організації, наприклад взяти під контроль систему за допомогою різних технічних засобів, таких як зламування ключових пристроїв і фальсифікація телеметрії, що вводить в оману необізнаних операторів. До інших небезпек відносяться заподіяння шкоди репутації або крадіжка секретів компанії. Коли метою є виробнича компанія, зловмисник може, наприклад, спробувати вкрасти формули чи рецепти та продати їх конкурентам. Зловмисник також може використовувати штучний інтелект для виконання персоналізованої атаки, призначеної для обраної групи або окремих співробітників. Ця атака відрізняється за масштабом від атак, метою яких є зараження пристроїв усієї компанії при підключенні до певного веб-сайту, підготовленого зловмисником, або використання пристрою або програмного забезпечення з певною вразливістю [18];

е) витік персональних даних може призвести до компрометації особистої інформації, що зберігається на пристроях або у хмарі. Мета зловмисника – отримати несанкціонований доступ до даних такого роду та використовувати їх у незаконний спосіб. У виробничих компаніях до подібних даних можуть належати імена та ролі користувачів системи ОТ. Виробничі дані не вважаються конфіденційними, але їх витік може створювати проблеми, якщо вони пов'язані з роботою окремих співробітників;

ж) Brute-force атака (від англ. brute force - «груба сила») означає спробу отримати несанкціонований доступ до ресурсів організації (наприклад, до даних, систем, пристроїв і т.д.), вгадавши правильний ключ або пароль за допомогою перебору всіх можливих поєднань символів. Організації, які дозволяють

використання нескладних паролів або паролів за промовчанням для промислових пристроїв та систем, особливо вразливі для таких атак.

Правове порушення:

а) порушення законодавства, норм, правил та зловживання персональними даними може призвести до юридичних проблем та фінансових втрат. Небезпека пов'язана з обробкою персональних даних, наприклад, при використанні кінцевих пристроїв IIoT без дотримання місцевих законів або норм.

б) невиконання вимог документації спричиняє порушення договірних вимог виробниками компонентів та постачальниками програмного забезпечення у разі неможливості забезпечити необхідні заходи безпеки [19].

Ненавмисне пошкодження елементів системи:

а) ненавмисна зміна даних або конфігурації в системі OT, виконана недостатньо навченим співробітником, може викликати порушення робочого процесу. Навіть із добрими намірами некваліфікований працівник, не підозрюючи про наслідки, може внести неналежні зміни до системи, особливо якщо він отримує повноваження, що перевищують необхідні;

б) некоректне використання або адміністрування пристроїв та систем IIoT недостатньо навченим співробітником може призвести до порушення робочого процесу або фізичного пошкодження пристрою;

в) збитки, завдані третьою стороною, можуть призвести до пошкодження активів IoT. Якщо стороння організація має неконтрольований доступ до системи IoT, наприклад з метою обслуговування або оновлення програмного забезпечення, порушення безпеки цією організацією можуть завдати шкоди компанії, яка отримує послугу.

Фізична атака:

а) крадіжка та вандалізм можуть призвести до незапланованих простоїв виробництва, оскільки заміна пошкодженого або вкраденого пристрою потребує часу, іноді значного;

б) саботаж, диверсія можуть бути здійснені зловмисником при отриманні фізичного доступу до пристроїв внаслідок неправильної конфігурації портів та їх

відкритості. Зловмисник також може використовувати доступ для виконання несанкціонованих дій оператора [20].

Вимкнення пристроїв:

а) відключення мережі зв'язку може виникнути через проблеми з кабельною, бездротовою або мобільною мережею;

б) відключення електроживлення може стати результатом збою в роботі або виходу з ладу будь-якого джерела живлення та, у разі відсутності аварійного джерела живлення, призвести до серйозних наслідків через раптове припинення виробничих процесів;

в) втрата послуг підтримки відбувається внаслідок збою чи несправності систем, які підтримують виробництво чи логістику.

Підслуховування, перехоплення, крадіжка інформації:

а) «людина посередині» (MitM-атака, англ. Man in the middle) - активна атака підслуховування, при якій зловмисник передає повідомлення від однієї жертви іншій, щоб змусити їх повірити, що вони розмовляють безпосередньо один з одним;

б) перехоплення протоколу IoT означає взяття під контроль існуючого сеансу зв'язку між двома елементами мережі. Зловмисник може прослуховувати цінну інформацію, зокрема паролі. У перехопленні можуть використовуватися агресивні методи, наприклад, примусове відключення або відмова в обслуговуванні;

в) перехоплення інформації включає несанкціоноване перехоплення (і іноді модифікацію) особистих повідомлень, таких як телефонні дзвінки, миттєві повідомлення, повідомлення електронної пошти;

г) мережна розвідка передбачає пасивний і активний збір внутрішньої інформації про мережу: про підключені пристрої, протокол, відкриті порти, служби, що використовуються, і т.д. за допомогою загальнодоступних даних та додатків;

д) перехоплення сеансу (англ. session hijacking) передбачає перехоплення з'єднання для передачі даних і перемикання його на новий хост замість законного для крадіжки, зміни або видалення даних, що передаються;

е) збір інформації означає пасивне отримання внутрішньої інформації про мережу: про підключені пристрої, використовуваний протокол і т.д.;

ж) повтор повідомлень використовується як атака, щоб маніпулювати цільовим пристроєм або збивати його роботу за допомогою зловмисного використання допустимої передачі даних з багаторазовим її відправленням або затримкою.

Катастрофа:

а) стихійне лихо, таке як повінь, удар блискавки, сильний вітер, дощ або снігопад, що може завдати фізичної шкоди компонентам довкілля ОТ;

б) екологічна катастрофа, наприклад пожежа, забруднення, вибух може призвести до фізичного пошкодження компонентів навколишнього середовища [20].

Засоби забезпечсення безпеки пристроїв IoT

Нижче перелічені засоби, які допоможуть вам захистити пристрої IoT в вашому офісі або вдома.

1. Вибирайте виробника, який орієнтированний на безпеку.

Коли справа доходить до покупки IoT пристроїв для вашого бізнесу або вдома, вам слід вибрати виробника або продавця, який займається кібербезпекою.

Якщо виробник не приділяє першочергової уваги безпеці, цілком імовірно, що пристрої, що їм поставляються, матимуть недоліки безпеки, які можуть не бути усунені в оновленнях. Це може зробити пристрої та їх користувачів вразливими до атак.

2. Приняття моделі безпеки з нульовою довірою.

У традиційній моделі безпеки пристрій та користувач повинні бути перевірені та автентифіковані лише один раз при першій спробі підключення до мережі.

Але в моделі безпеки Zero Trust кожен пристрій та користувач IoT будуть перевірені та автентифіковані щоразу, коли вони намагаються підключитися до мережі інтелектуальних пристроїв. Таким чином, ви гарантуєте, що всі є тими, за кого себе видають, і кожен пристрій є справжнім.

3. Впровадьте сегментацію мережі.

Коли ви реалізуєте сегментацію мережі, ви ділите свою мережу більш дрібні частини. Ці сегменти працюють як незалежні мережі.

Таким чином, реалізація сегментації мережі для підключених IoT-пристроїв зменшує поверхню атаки та зменшує проблеми з безпекою. Це пов'язано з тим, що фрагментація мережі ускладнює для зловмисників бічне переміщення по мережі та заподіяння значної шкоди.

4. Поновлюйте свої пристрої.

Невиправлені вразливості можуть бути точкою входу для хакерів, щоб отримати доступ до пристроїв IoT. Тому встановлюйте всі оновлення вбудованого програмного забезпечення, як тільки вони стануть доступними, і обов'язково завантажуйте оновлення з веб-сайтів виробників обладнання.

Скористайтеся перевагами функції автоматичного оновлення на IoT-пристроях. Якщо пристрій не підтримує автоматичні оновлення, заплануйте щотижневу перевірку вручну.

Своєчасне оновлення пристроїв IoT допоможе запобігти використанню хакерами відомих уразливостей у пристроях IoT.

5. Змініть стандартні паролі для пристроїв.

Якщо ви не зміните паролі за промовчанням для IoT-пристроїв, ваші підключені пристрої будуть вразливі для різних IoT-атак. Хакери можуть легко вгадати ім'я користувача та пароль ваших пристроїв, і ви будете в небезпеці. Отримавши контроль над вашими пристроями, зловмисник може додати їх у ботнет Інтернету речей (бот-мережа - це величезна група (обчислювана тисячами або навіть мільйонами) зламаних через Інтернет пристроїв, кожне з яких називається ботом, який обслуговує бота-майстра).

Ось чому дуже важливо, щоб ви негайно змінили свої паролі за замовчуванням і створили непорушну фразу, яку ви можете запам'ятати.

Ви також можете почати використовувати менеджер паролів або генератор для створення та керування паролями для різних пристроїв IoT.

6. Посильте налаштування безпеки на своїх пристроях.

Ваші пристрої IoT можуть поставлятися з налаштуваннями конфіденційності та безпеки за промовчанням. Ці налаштування часто приносять більше користі виробникам пристроїв, ніж вам, особливо коли йдеться про конфіденційність.

Тому вам слід уважно перевірити налаштування конфіденційності та безпеки ваших IoT-пристроїв. Якщо ви бачите варіанти підвищення конфіденційності та безпеки, вимкніть їх.

7. Вимкніть функції, які не використовуються.

Вимкнення функцій, що не використовуються, на пристроях IoT — ще один спосіб захистити підключені пристрої від хакерів. Пристрої IoT мають безліч функцій, і ви можете не використовувати їх усі. Наприклад, деякі пристрої можуть мати веб-браузер, який не потрібний у вашому випадку використання.

Якщо ви активуєте всі функції та служби, доступні на пристроях, це розширить поверхню атаки; У зловмисників буде більше можливостей для використання вразливостей у пристроях IoT.

Візьміть за звичку періодично переглядати активні функції та послуги. Якщо ви виявите щось непотрібне для вашого варіанта використання, вимкніть його, щоб зменшити поверхню атаки.

8. Увімкніть багатофакторну автентифікацію (MFA), коли це можливо.

Багатофакторна автентифікація (MFA) — це метод автентифікації, який вимагає від користувача надання двох або більше факторів для отримання доступу до пристрою. Наприклад, замість того, щоб запросити ім'я користувача та пароль, сервер автентифікації може запросити додатковий фактор, такий як одноразовий пароль, для надання доступу до пристрою.

Якщо ваші пристрої Інтернету речей підтримують багатофакторну автентифікацію, ви повинні її реалізувати. Це додасть додатковий рівень безпеки. Але будьте обережні з атаками вигоряння, призначеними для обходу MFA, які у разі успіху можуть допомогти хакерам обійти автентифікацію.

9. Інвестуйте у рішення безпеки.

Системи Інтернету речей постійно перебувають у зору хакерів; Впровадження надійного рішення для безпеки пристроїв IoT необхідно для захисту підключених пристроїв.

Для забезпечення безпеки IoT потрібно виконати такі дії:

- Перегляньте всі пристрої IoT у вашій мережі та дізнайтеся про пов'язані з ними загрози безпеці.
- Введіть політику нульової довіри, щоб запобігти несанкціонованому доступу.
- Слідкуйте за загрозами та вразливістю.
- Запобігайте відомим і готовим атакам за допомогою віртуальних виправлень та аналізу загроз Інтернету речей у режимі реального часу. Оцініть пристрої зі слабкими обліковими даними для входу.

10. Поліпшення реальної безпеки.

Хакер йде на все, щоб отримати доступ до IoT-пристроїв, у тому числі проникнути у ваш будинок чи офіс. При захисті пристроїв IoT також необхідно враховувати фізичну безпеку цих пристроїв.

Зберігання конфіденційних пристроїв IoT у захищеному від несанкціонованого доступу стані, додавання функцій, які відключатимуть підключені пристрої, коли хтось їх відключає, та надання лише авторизованого доступу до конфіденційних пристроїв – це деякі способи підвищення фізичної безпеки пристроїв IoT.

11. Захист маршрутизатора.

Маршрутизатор Wi-Fi – це шлюз між пристроями IoT та Інтернетом. Хакери, які мають доступ до вашого маршрутизатора та мережі Wi-Fi, можуть поставити під загрозу безпеку підключених пристроїв та всієї мережі.

Таким чином, крім захисту пристроїв IoT, ви також повинні захистити свій маршрутизатор і Wi-Fi.

Ось кілька швидких порад, які допоможуть вам розпочати:

- Змініть облікові дані маршрутизатора за промовчанням.
- Змініть SSID за промовчанням, щоб хакери не вгадали виробника вашого маршрутизатора.
- Використовуйте шифрування WPA2 або WPA3.
- Увімкніть брандмауер маршрутизатора.

Крім того, слід оновити прошивку маршрутизатора.

2.3 Висновки до другого розділу

Розглянуті проблеми безпеки промислового Інтернету речей та методи, які дозволяють мінімізувати загроози.

Проаналізовані основні технології, які застосовуються для забезпечення безпеки в промислових мережах (IoT).

Класифіковані та детально розглянуті загрози, що мають місце в сучасних мережах IoT. А саме, проаналізовані загрози, викликані як людським фактором, так і стихійним лихом, наведені засоби боротьби з цими загрозами.

3 РОЗРОБКА СИСТЕМИ ЗАХИСТУ ПРОМИСЛОВОЇ МЕРЕЖІ IoT

3.1 Методи захисту пристроїв в промислових мережах IoT

В процесі аналізу було виявлено сукупність проблем безпеки IoT-пристроїв.

Відсутність єдиного підходу до забезпечення безпеки.

В даний час жодного підходу до забезпечення безпеки в IoT, ні загальної моделі безпеки, розробленої за участю всіх зацікавлених сторін, немає. Більшість компаній та виробників використовують власний підхід до забезпечення безпеки в IoT, що призводить до відсутності або, у кращому разі, уповільненого прийняття стандартів безпеки IoT. Варто враховувати і той факт, що в різних сферах застосування до технології пред'являються різні вимоги безпеки.

Має бути вирішена ще одна важлива проблема - відсутність відповідальності як моральної, так і юридичної. Її можна вирішити, змусивши виробників виконувати свої обов'язки щодо безпеки продуктів чи послуг. В даний час неможливо забезпечити ідеальну ізоляцію між різними елементами екосистеми IoT, які розробляються різними виробниками та експлуатуються різними сторонами. У зв'язку з цим необхідно уточнити відповідальність кожного учасника у разі виникнення загрози безпеці.

Недолік поінформованості та знань у користувачів

У зв'язку з масштабним переходом до підключених та взаємозалежних систем та пристроїв нестача знань відчувається особливо гостро. В ході інтерв'ю з експертами в галузі IoT було виявлено, що у фундаментальній термінології існує різниця між поняттями «безпека» та «захищеність». Експерти з безпеки зазвичай знайомі з безпекою IT-бізнесу, але не з безпекою IoT.

Загалом відсутнє розуміння необхідності забезпечення безпеки у пристроях IoT. Велику тривогу викликає відсутність знань про загрози, які наражаються на ці пристрої – більшість споживачів IoT не мають базового уявлення про свої IoT-пристрої та принципи їх безпеки. Тому пристрої не оновлюються, що може спричинити порушення безпеки [21].

Компанії повинні навчати своїх співробітників передовим методам забезпечення безпеки, усвідомлюючи, що технологічний досвід не завжди прирівнюється до досвіду безпеки. У цілому нині необхідно інформувати нове покоління споживачів, розробників, виробників тощо. про використання IoT та пов'язані з ним ризики безпеки. Багато інцидентів безпеки можна було б уникнути, якби розробники та виробники знали про ризики, з якими вони стикаються щодня.

Необхідно підвищувати рівень знань про поточні загрози та ризики, інформуючи про те, як запобігати інцидентам, захищати IoT та діяти у разі інциденту безпеки.

Небезпечне проектування та розробка:

У контексті проектування та розробки IoT видаються особливо важливими такі питання [22]:

- відсутність стратегії глибокого захисту під час проектування системи, такої як безпечний процес завантаження, ізоляція довіреної обчислювальної бази, обмеження кількості відкритих портів, самозахист тощо;
- відсутність безпеки чи конфіденційності під час проектування. У деяких випадках відбувається обмін інформацією з третьою стороною і слід переконатися, що за межі IoT-середовища експортується не більше інформації, ніж це необхідно;
- відсутність захисту зв'язку як у внутрішніх, і зовнішніх интерфейсах;
- відсутність надійної автентифікації та авторизації (немає перевірки чи підпису оновлень прошивки, оновлення програмного забезпечення без перевірки автентичності сервера та достовірності файлів, механізмів безпечного завантаження);
- відсутність захисту у прошивці (не застосовуються технології запобігання передачі даних або пом'якшення наслідків атак, публічні вразливості не виправляються, деякі сервіси відкриваються через різні точки входу, при цьому непотрібні комунікаційні порти залишаються відкритими - такі сервіси, як Telnet

або ssh, іноді прив'язані до всіх мереж інтерфейсів, використовуються слабкі паролі або стандартні паролі, залишені без змін).

Відсутність сумісності між різними пристроями та платформами IoT

Переважна більшість IoT-екосистем включають пристрої IoT, пов'язані із застарілими системами, особливо у критично важливих інформаційних інфраструктурах. Більше того, як згадувалося раніше, через відсутність єдиного підходу більшість компаній та виробників використовують власний підхід при розробці пристроїв IoT, що призводить до проблем сумісності між пристроями різних виробників, а також появи різних моделей безпеки, несумісних концепцій тощо. Тому дуже важливо розробити заходи, що забезпечують правильне та безпечне з'єднання та взаємодію між середовищем IoT та успадкованими системами, а також іншими IoT-пристроями, виготовленими сторонніми виробниками [23].

Більшість IoT-пристроїв використовують власні протоколи зв'язку, розроблені їх виробниками. Навіть якщо це не є проблемою для одного виробника, це стає проблемою при з'єднанні пристроїв різних виробників.

Необхідно розробляти та використовувати стандартні протоколи, які повинні підтримуватись усіма виробниками для забезпечення гарного рівня сумісності з найменшими втратами ефективності та безпеки. Хорошою практикою щодо цього є відмова від використання протоколів із закритим вихідним кодом, оскільки їхню безпеку неможливо перевірити. Крім протоколів, використання загальних рамок також допоможе підвищити ефективність і безпеку пристроїв при з'єднанні декількох пристроїв різних виробників.

Відсутність економічних символів

Основні виробники та постачальники IoT зазвичай вважають функціональність та зручність використання важливішими, ніж безпечне проектування та програмування. Не в їхніх економічних інтересах витрачати багато грошей на безпеку, а в деяких випадках вони взагалі не розглядають питання безпеки. Компанії не виділяють кошти на безпеку тому, що, на загальну

думку, ці кошти не повертаються, це можна пояснити складністю оцінки фінансових наслідків гіпотетичних недоліків у системі безпеки.

Ситуація посилюється відсутністю економічних стимулів, які могли б сприяти підвищенню безпеки, таких як економічні вигоди (наприклад, збільшення кількості грантів для забезпечення більшої безпеки у пристроях), ресурси, передбачувана репутація тощо.

Різні ризики, загрози та небезпеки зазвичай недооцінюються і не враховуються через бюджетні проблеми – існує тенденція вирішувати проблеми безпеки після інцидентів [24].

Відсутність належного керування життєвим циклом продукту.

Загалом заходи безпеки виявляються недостатніми, починаючи з етапу проектування та закінчуючи його подальшою розробкою. Для різних активів, що становлять це IoT-середовище, необхідно належне керування життєвим циклом продукту, оскільки пристрої та мережі взаємопов'язані і, в більшості випадків, відкриті для доступу в Інтернет, де вони можуть стати мішенню для безлічі різноманітних загроз.

IoT включає в себе таке різноманіття продуктів, що, якщо залишити їх поза увагою, вони роблять уразливим весь ланцюжок поставок. IoT розширює глобальну поверхню атаки, і кожен виробник відповідає за управління ризиками. Різні пристрої та продукти повинні будуть розвиватися безпечним способом, щоб постійно забезпечувати протягом свого життєвого циклу рішення, для якого вони були створені.

У цей процес необхідно залучити постачальників, а оскільки саме вони відповідають за проектування та розробку пристроїв, це їхня прерогатива реалізувати необхідні зміни – вони можуть кваліфіковано і з мінімальними витратами включати нові функції або характеристики безпеки. Але це залежить не тільки від виробників, які додають нові функції, але й від організацій, що приймають пов'язані з цим витрати, отже, баланс між безпекою і вартістю повинен бути збережений.

Протягом усього життєвого циклу IoT-пристрої повинні мати можливість швидкого виправлення та оновлення, щоб забезпечити правильну роботу та усунути усі виявлені вразливості. Як згадувалося раніше, більшість користувачів не мають базових знань про IoT-пристрої та їх вплив на середовище, в результаті пристрою не оновлюються і, відповідно, залишаються вразливими до нових загроз.

Крім того, одним із важливих етапів керування життєвим циклом пристрою є етап розгортання. Можна розробити рекомендації щодо розгортання IoT. Вони включатимуть рекомендації щодо конкретних конфігурацій пристроїв та мереж [15].

3.2 Засоби безпеки для пристроїв в мережах IoT

Нижче наведено докладний список заходів щодо забезпечення безпеки, спрямованих на зниження загроз, уразливостей та ризиків, що впливають на пристрої та середовища IoT (таблиця 2) [25].

Таблиця 2

Засоби безпеки для пристроїв в мережах IoT

Засіб безпеки	Опис
Керування інформаційною безпекою та управління ризиками	Заходи безпеки щодо аналізу ризиків безпеки інформаційної системи, політики, акредитації, показників та аудиту, а також безпеки людських ресурсів
Управління екосистемами	Заходи безпеки щодо картування екосистем та відносин між екосистемами
Архітектура інформаційної безпеки	Заходи безпеки щодо конфігурації систем, управління активами, поділу систем, фільтрації трафіку та криптографії

Адміністрування інформаційної безпеки	Заходи безпеки щодо адміністративних облікових записів та адміністративних інформаційних систем
Управління ідентифікацією та доступом	Заходи безпеки щодо автентифікації, ідентифікації та прав доступу
Технічне забезпечення інформаційної безпеки	Заходи безпеки щодо процедур технічного забезпечення IT-безпеки та віддаленого доступу
Виявлення загроз	Заходи безпеки щодо виявлення, реєстрації, а також кореляції та аналізу журналу
Управління інцидентами комп'ютерної безпеки	Заходи безпеки щодо аналізу та реагування на інциденти безпеки в інформаційній системі, а також звіт про інциденти

Перераховані вище заходи безпеки класифіковані в залежності від того, до якої області IoT-екосистеми вони застосовуються.

Крім цього, кожен захід безпеки може бути віднесений до певної категорії залежно від її характеру – це може бути політика безпеки, яку необхідно враховувати під час розробки пристроїв; організаційні заходи, орієнтовані на бізнес та співробітників, які мають бути вжиті самою організацією; нарешті, технічні заходи, спрямовані зниження потенційних ризиків для пристроїв IoT та інших елементів IoT-екосистеми. Відповідно, виявлені базові заходи безпеки IoT розподілені за трьома основними категоріями, представленими в наступному списку.

Політика безпеки

Перша група заходів відноситься до політики безпеки, яка загалом спрямована на забезпечення інформаційної безпеки та покликана зробити її більш конкретною та надійною. Вона має відповідати діяльності організації та містити

добре документовану інформацію. У цьому контексті було визначено такі рекомендації щодо безпеки [26].

Варто зазначити, що коли йдеться про забезпечення безпеки та конфіденційності при проектуванні, заходи безпеки повинні відображати особливості та контекст, в якому буде розгорнутий пристрій або систему IoT. Коли справа доходить до IoT, ризик залежить від контексту (тобто ґрунтується на сценарії програми), і щодо цього заходи безпеки повинні застосовуватися з урахуванням цього фактора.

Організаційні заходи

Усі підприємства повинні мати організаційні критерії інформаційної безпеки. Дії персоналу повинні забезпечувати безпеку, управління процесами та безпечну роботу з інформацією у робочому процесі організації.

Організації повинні забезпечити відповідальність підрядників і постачальників за виконання функцій, що розглядаються. У разі інциденту безпеки організація має бути підготовлена (відповідальність, оцінка та реагування).

Технічні заходи

Заходи безпеки повинні враховувати та охоплювати технічні елементи, щоб зменшити вразливість IoT. Нижче наведено огляд необхідних технічних заходів для збереження та захисту інформації в IoT.

Апаратне забезпечення безпеки

Рекомендується використовувати обладнання, яке включає апаратні засоби безпеки для посилення захисту та цілісності пристрою: наприклад, спеціалізовані мікросхеми, які забезпечують захист на апаратному рівні (захищене зберігання даних і засобів аутентифікації, ідентифікація пристрою і захист ключів у стані спокою і в процесі використання) . Захист від локальних та фізичних атак може бути забезпечений за допомогою функціональної безпеки.

Управління довірою та цілісністю

Довіра до завантажувальної прошивки повинна бути встановлена до того, як буде встановлено довіру до будь-якого іншого програмного забезпечення.

Необхідний контроль за встановленням програмного забезпечення в операційних системах, щоб запобігти завантаженню недостовірного програмного забезпечення та файлів.

Необхідно дозволити системі повертатися до початкового безпечного стану, в якому вона перебувала до порушення безпеки. Можливість відновлення системи у випадку, якщо оновлення не було завершено коректно, також відіграє важливу роль.

Рекомендується використовувати протоколи та механізми, здатні керувати довірою.

Надійне забезпечення безпеки та конфіденційності за умовчанням

Будь-які застосовні функції безпеки повинні бути включені за замовчуванням, а будь-які функції, що не використовуються або небезпечні, – відключені.

Важливо створювати складні паролі за промовчанням для окремих пристроїв.

Захист персональних даних

Персональні дані повинні збиратися та оброблятися на підставі відповідних законів, вони ніколи не повинні збиратися та оброблятися без згоди суб'єкта даних.

Необхідно перевіряти, чи використовуються персональні дані у зазначених цілях.

Користувачі IoT повинні мати можливість контролювати інформацію, що збирається [27].

Безпека та надійність системи

Під час проектування системи важливо враховувати системні та експлуатаційні збої, не допускаючи, щоб система викликала неприйнятний ризик травмування або заподіяння фізичних збитків.

Основні функції повинні продовжувати працювати при втраті зв'язку та/або негативному впливі з боку компрометованих пристроїв або хмарних систем.

Безпечне оновлення програмного забезпечення

Слід переконатися, що програмне забезпечення пристрою, його конфігурація та його програми мають можливість оновлення по бездротовій мережі, сервер оновлень безпечний, файли оновлення передаються через захищене з'єднання і не містять конфіденційних даних, підписані авторизованим довіреним об'єктом та зашифровані з використанням прийнятих методів шифрування, Оновлення має свій цифровий підпис, сертифікат підпису та ланцюжок сертифікатів підпису.

Автоматичні оновлення прошивки не повинні змінювати налаштування уподобань, параметрів безпеки або конфіденційності без повідомлення користувача.

Автентифікація

Слід розробляти системи аутентифікації та авторизації на основі моделей загроз на рівні системи [28].

Важливо переконатися, що під час початкового встановлення паролі та імена користувачів за промовчанням, а також слабкі або недійсні паролі та імена користувачів змінені. Механізми автентифікації повинні використовувати надійні паролі або особисті ідентифікаційні номери (PIN). Доречно розглянути можливість використання двофакторної або багатофакторної аутентифікації, такої, як у смартфонах, біометричних даних і т.д.

Важливо враховувати, що облікові дані для автентифікації мають бути зашифровані.

Необхідно переконатися, що механізм відновлення або скидання пароля надійний і не надає зловмиснику інформацію, яка вказує на дійсний обліковий запис. Те саме стосується і механізмів оновлення та відновлення ключів.

Авторизація

Необхідно обмежити дії, дозволені для цієї системи, шляхом впровадження механізмів деталізованої авторизації та використання принципу найменших привілеїв: додатки повинні працювати на найнижчому рівні привілеїв.

Прошивка пристрою повинна бути розроблена таким чином, щоб ізолювати привілейований код, процеси та дані прошивки. Апаратне забезпечення пристрою

має забезпечувати ізоляцію для запобігання доступу зловмисника до чутливого до безпеки коду.

Контроль доступу – фізична безпека та безпека навколишнього середовища

Цілісність та конфіденційність даних повинні забезпечуватися засобами контролю доступу. Коли суб'єкт, який запитує доступ, авторизований для доступу до конкретних процесів, необхідно забезпечити дотримання певної політики безпеки.

Виявлення несанкціонованого доступу та реагування на апаратне втручання не повинні залежати від підключення до мережі.

Важливо, щоб пристрої були оснащені тільки зовнішніми фізичними портами, які необхідні їм для роботи.

Безпечний та надійний зв'язок

Необхідно забезпечити різні аспекти безпеки – конфіденційність, цілісність, доступність та справжність інформації, що передається по мережах, а також зберігається у додатку IoT або у хмарному сховищі.

Важливо врахувати, що безпека зв'язку забезпечується стандартними сучасними протоколами безпеки шифрування, такими як TLS.

Облікові дані не повинні передаватися у відкритому вигляді через мережу.

Щоб забезпечити надійний обмін даними від передачі до прийому, вони завжди повинні бути підписані, коли і де вони збиралися б і не зберігалися.

Необхідно відключати певні порти або мережні з'єднання для вибіркового підключення.

Також варто встановити контроль трафіку, що надсилається або одержується мережею, для зниження ризику автоматизованих атак.

Безпечні інтерфейси та мережеве обслуговування

Поділ мережевих елементів на окремі компоненти допомагає ізолювати інциденти безпеки та мінімізувати загальний ризик.

Протоколи повинні бути розроблені таким чином, щоб у разі зламування одного пристрою це не вплинуло на весь набір.

Необхідно уникати надання одного і того ж секретного ключа для всього сімейства продуктів, оскільки злому одного пристрою буде достатньо, щоб зламати інші пристрої цього сімейства [30].

Важливо впровадити інфраструктуру, що стійка до DDoS-атак і балансує навантаження.

Необхідно переконатися, що веб-інтерфейси повністю шифрують сеанс користувача – від пристрою до серверних служб – і не схильні до XSS, CSRF, SQL-ін'єкцій тощо.

Безпечна обробка введення та виведення даних

Повинна проводитися валідація даних, що вводяться (забезпечення безпеки даних перед використанням) і фільтрація виведення.

Слід впровадити систему протоколювання, яка реєструє події, пов'язані з автентифікацією користувачів, керуванням обліковими записами та правами доступу, змінами правил безпеки та функціонуванням системи. Журнали повинні зберігатися на довгострокових носіях та витягуватись через автентифіковані з'єднання.

Моніторинг та аудит

Важливо здійснювати регулярний моніторинг для перевірки поведінки пристрою, виявлення шкідливих програм та виявлення помилок цілісності. Необхідно проводити періодичні перевірки засобів контролю безпеки, щоб переконатися в їх ефективності та тестування на проникнення.

Застосування цих технічних заходів має враховувати особливості екосистеми IoT, такі як масштабованість, тобто величезна кількість задіяних пристроїв потребує вжиття певних заходів на рівні спеціалізованих компонентів архітектури [33].

Узагальнені рекомендації щодо безпеки пристроїв IoT

Нижче наведено список рекомендацій для розробників, операторів та експертів з безпеки. Рекомендовані рекомендації стосуються зацікавлених сторін, охоплюють весь спектр IoT і спрямовані на усунення проблем, визначених вище.

Створення єдиних стандартів та вимог щодо безпеки IoT Проблема фрагментації керівних принципів, ініціатив, стандартів та інших механізмів забезпечення безпеки IoT потребує вирішення. Першим кроком у цьому напрямку є визначення списку кращих практик і посібників з безпеки та конфіденційності IoT, які можна використовувати як основу для розробки та розгортання систем IoT [35].

Цікаво відзначити, що поняття стандарту високо цінується і підтримується промисловістю, але групи зацікавлених сторін мають різні ланцюжки науково-дослідної та дослідно-конструкторської роботи, що призводить до фрагментації.

В якості рекомендації щодо боротьби з фрагментацією можна запропонувати створення загального набору практик, посібників та вимог безпеки в IoT. Згодом кожна організація може зосередитись на визначенні конкретних наборів практик, посібників, вимог для власних потреб на основі конкретного контексту та факторів ризику.

Процес закупівель є ще одним способом забезпечення гармонізації базових стандартів та вимог для систем IoT. Важливо враховувати, що є безліч різних галузей, тому гармонізація має бути досягнуто спочатку у кожному секторі.

Підвищення рівня знань щодо забезпечення безпеки IoT

Безпека IoT – загальна відповідальність усіх заінтересованих сторін. Тому всі сторони повинні мати повне уявлення про пов'язані ризики та загрози, а також про засоби захисту від них. Таким чином, підвищення рівня знань має першорядне значення.

Як свідчать численні інциденти у сфері безпеки, пов'язані з IoT, розробникам та кінцевим користувачам IoT-пристроїв не вистачає знань. Щоб вирішити цю проблему, необхідно розробити конкретні рекомендації для зацікавлених сторін, а саме [37]:

- під час організації навчання з питань кібербезпеки до програми повинні бути включені матеріали про сучасний стан у цій сфері, практичні приклади, еталонні архітектури, методології та інструменти для безпечних систем IoT;

- кінцеві користувачі та споживачі повинні бути поінформовані, щоб мати можливість приймати обґрунтовані рішення під час експлуатації пристроїв та систем IoT;
- розробникам необхідно підвищити рівень знань у галузі безпеки, щоб усвідомити необхідність прийняття основних принципів безпеки для всіх сфер застосування IoT.

В останні роки в школах та університетах все частіше вводять програми навчання основам безпеки, що сприяє більш глибокому розумінню цієї проблеми в IoT серед молодого покоління.

Прийняття принципу розробки безпечного програмного та апаратного забезпечення протягом усього життєвого циклу пристроїв IoT

Розробники, виробники та постачальники продуктів та рішень IoT повинні домовитися про введення принципу, згідно з яким протягом усього життєвого циклу пристроїв IoT розроблятиметься безпечне програмне та апаратне забезпечення, і включатиме відповідні процеси у свої операції. Безпека має бути реалізована загалом, лише на рівні додатків і кожному з етапів розробки.

Тому важливо спонукати якнайбільше компаній пропонувати безпечні рішення, якими могли б скористатися і розробники, і користувачі.

Досягнення консенсусу щодо функціональної сумісності пристроїв екосистеми IoT

Проблема сумісності дуже актуальна для екосистеми IoT через зростаючу кількість пристроїв, складність ланцюжків поставок та велику кількість зацікавлених сторін. Забезпечення функціональної сумісності пристроїв, платформ та систем IoT, як і методи забезпечення безпеки є важливим елементом безпеки IoT [38].

Рекомендації щодо вирішення проблеми:

- заохочувати використання відкритих сумісних систем, що включають засоби безпеки;
- забезпечити прозорість щодо безпеки сумісних систем;

- просувати відкриті та доступні лабораторії та випробувальні стенди для забезпечення безпеки.

Створення економічних та адміністративних стимулів для забезпечення безпеки IoT

У сфері виробництва IoT конкурентна перевага в даний час полягає у швидшому виході на ринок, а не в безпеці. Цей баланс необхідно змінити так, щоб базовий рівень безпеки та конфіденційності заохочувався ще до виходу на ринок. Визначення принципів безпеки, які підтримуються базовими заходами безпеки, може стати кроком уперед у цьому напрямку.

Повинне бути розглянуто використання інших способів, таких як сертифікація та маркування, які також можуть сприяти забезпеченню безпеки IoT.

Створення безпечного керування життєвим циклом пристроїв IoT

Безпека відіграє на всіх етапах життєвого циклу продукту IoT. Ці етапи включають проектування, розробку, тестування, виробництво, розгортання, обслуговування, підтримку та закінчення терміну служби (тобто виведення з експлуатації).

Рекомендується визначити конкретні безпекові процеси для всіх цих етапів.

Крім того, процеси безпеки мають бути правильно впроваджені. Для цього необхідно визначити основні вимоги безпеки кожному етапі.

Розмежування відповідальності між заінтересованими сторонами IoT

Дуже важливим питанням під час розгляду IoT є питання відповідальності.

Він має особливе значення у сфері IoT, оскільки природа IoT тісно пов'язує захищеність із безпекою. Це питання вимагає вирішення кожному з перелічених рівнів всім зацікавлених сторін [15].

3.3 Особливості реалізації запропонованої системи захисту

3.3.1 Контроль доступу до мережі

Для забезпечення контроля доступу к промисловим мережам IoT використовуються наступні методи.

Динамічна авторизація

Насамперед організаціям слід подбати про правильне конфігурування пристроїв IoT та їх захищене підключення до корпоративних мереж.

Усунення надлишкових даних

На додаток до моніторингу активності та доступу корисно скласти план дій щодо усунення надмірності даних.

«Організаціям слід спробувати домогтися того, щоб отримання, збирання та відправлення даних відбувалися одночасно, це підвищить ефективність їх передачі, - сказав Енді Сімпсон-Пірі [39], головний технолог Cyberfort Group. — Дотримуючись стратегії мінімізації даних, простіше забезпечувати інформаційну безпеку. Ви можете більш точно передбачити, що саме витягується, куди прямує і що шукати, якщо піде не так. Це як жонглювати трьома тарілками замість шести - теж непросто, але набагато легше. Створення ешелонованої оборони навколо IoT також посилить контроль доступу. За такої стратегії дані у мережі шифруються і захищаються кожному етапі, як у самому пристрої, і під час передачі чи системі одержувача. Ідея полягає у використанні на кожному етапі різних механізмів шифрування, що перетворює дані на рухому мету».

Безпека в жодному разі не є єдиним аспектом, який слід розглядати під час контролю доступу до даних IoT. Існують також проблеми наочності. А на випадок ослаблення системи безпеки потрібно мати план резервного копіювання.

На думку Роба МакНатта, головного технолога компанії Forescout [21], рішення полягає у сегментуванні мережі. «Організаціям необхідні повні видимість та контроль над усіма пристроями у своїх мережах, і їм слід відповідним чином сегментувати свої мережі, – сказав він. — Не можна захистити

дані, що надходять від пристроїв, які ви не бачите. Без видимості всіх пристроїв та їх активності в мережі неможливо домогтися, щоб лише авторизовані користувачі та пристрої отримували доступ до ваших даних. Якщо пристрій справді зламано, сегментація мережі здатна перешкодити лиходіям незаконно переміщатися по мережі і при цьому отримувати доступ до даних, яких не повинно бути».

3.3.2 Налаштування контролю доступу

Розглянемо практичний приклад, розроблений автором, - систему контролю упарвління доступа (СКУД), яка буде підраховувати кількість людей в офісі.

Вся робота виконуєтьтся на платформі Rightech IoT Cloud

Основні дані з контролера - це події, на платформу вони приходять у форматі JSON і включають поля

- eventTime - час настання події;
- eventCode – код події;
- keyNumber - номер картки співробітника (поле може бути порожнім, якщо подія викликана не карткою).

Модель пристрою виглядає наступним чином:

Можливі події:

- натиснута кнопка дзвінка;
- невідомий ключ на вході;
- невідомий ключ на виході;
- ключ знайдено у банку ключів при вході;
- ключ знайдено у банку ключів при виході;
- відкривання оператором через мережу;
- двері заблоковані оператором;
- двері залишені відчиненими після входу;
- двері залишені відчиненими після виходу;

- прохід відбувся на вхід;
- прохід відбувся на вихід;
- перезавантаження контролера.

Об'єкт:

Інтерфейс об'єкта повністю формується відповідно до розробленої моделі.

Ці підрахунки будуть відбуватися системою контролю дверима, яка працює на основі бесконтактної картки.

В якості контролера, який відповідає за обробку інформації безконтактних карток, був обраний контролер із серії GATE (рис. 3.1).

Основні переваги цього контролера:

- формирування та зберігання необходідної інформації щодо факту відкриття дверей за допомогою карти та час проходу людини в офіс;
- можливість автономної роботи та захист від збою;
- зберігання до 16 тисяч ключів та 8 тисяч подій;
- просте підключення та керування.

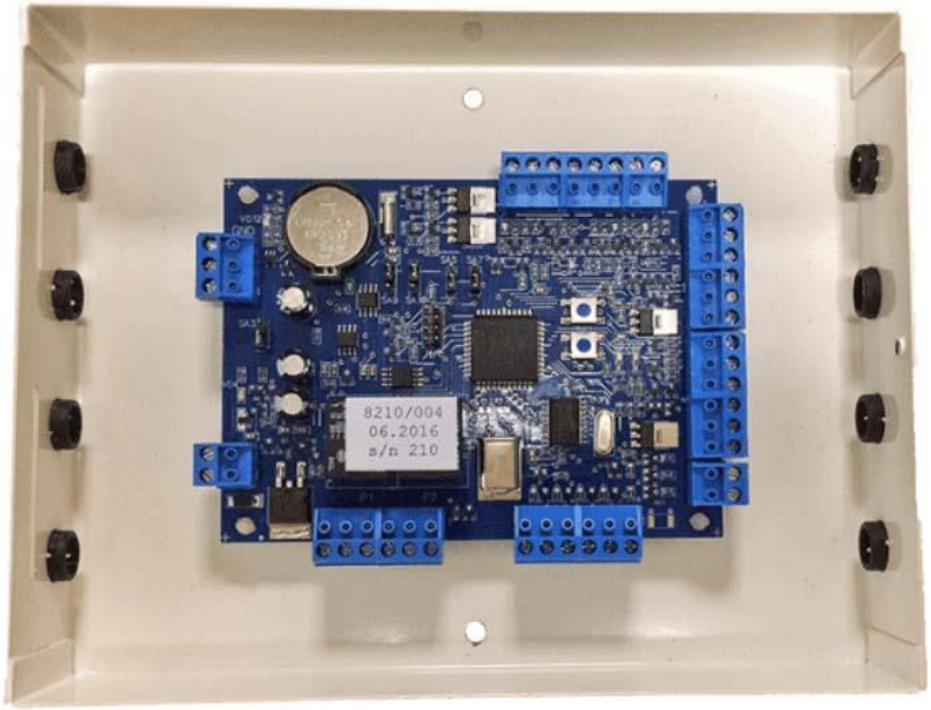

Рис. 3.1. Контролер доступу співробітників в приміщення

Технічні характеристики контролера наведені в таблиці 3.

Таблиця 3.

Технічні характеристики контролера

Напруга живлення	11,4-15,0 В
Струм, що споживається:	
в режимі очікування, не більше	30 мА
в режимі комутації, не більше	90 мА
Тип підключення	RS-485
Швидкість обміну по мережі RS-485	19200 біт/с
Максимальна кількість контролерів в одній лінії RS-485	255
Інтерфейс считувачів, які підключаються	2
Кількість реле, що керуються	2
Параметри реле:	
комутована напруга, не більше	30 В постійного струму
комутований струм, не більше	6 А

Основний принцип роботи системи, яка контролює відкриття дверей: контролер оброблює інформацію, яка передається считувачем, і з допомогою вбудованого реле комутує виконавчий пристрій - електромагнітний замок дверей.

Система взаємодії з платформою IoT:

Після того, як контролер встановили систему за загальною схемою підключення, а карти записали в пам'ять, ми вже убезпечили себе від проходу в офіс сторонніх. А далі постало питання, як підключити цей контролер до платформи Rightech ioT Cloud. Адже дуже добре мати а) графічний інтерфейс, в якому можна погортати історію всіх проходів, б) можливість відправлення команд на відкриття дверей віддалено, не відходячи від робочого місця, наприклад, для гостей або постачальника їжі.

Контролер не має виходу в Інтернет і видимої можливості підключення до платформи, до того ж всі події потрібно примусово зчитувати з його циклічного буфера. Однак він має свій протокол обміну даними з комп'ютером управління, завдяки якому можна відправляти на контролер команди, такі як рахувати з контролера, записати в контролер, відкрити/закрити замок та інші. Значить, потрібно зробити деякий програмно-апаратний прошарок між контролером і платформою - агента, який відправлятиме команди на читання подій та управління контролером.

Звертаю увагу, що в цій архітектурі функція відкриття дверей при додаванні карти не перестане виконуватися за відсутності Інтернету. За відкриття дверей та збір інформації відповідає контролер СКУД, тому в разі втрати Інтернету, єдине, що нам загрожує, - це те, що агент, який доставляє дані на платформу, не функціонуватиме, оскільки не зможе отримувати команди на читання буфера. Однак, при відновленні з'єднання всі події вважаються в повному обсязі і не загубляться, оскільки вони будуть збережені в буфері контролера СКУД.

Апаратна частина:

Для початку потрібно було вибрати пристрій, який завжди буде в активному стані з включеною програмою-агентом в безпосередній близькості від плати СКУД. З різноманіття мікрокомп'ютерів перше що потрапило під руку вибір упав на Raspberry Pi.

Далі постало питання, як під'єднати GATE до Raspberry - тобто як підключити послідовний інтерфейс RS485 від GATE до USB від мікрокомп'ютера. Розпочалися пошуки перехідника USB-RS485. Перший варіант, який ми випробували, - Espada. Надія на те, що маленький кволий китайський перехідник запрацює, була невеликою. Він і не заробив. Замість потрібних даних приходило щось схоже на вигляд і розмір, але все ж таки не те. У чому була справа: без гальванічної розв'язки, неможливо підтримувати швидкість 19200 bps або просто в неякісній елементній базі, загадка. Але після звернення до виробника GATE, ми отримали рекомендацію на більш дорогий (в 10 разів) і громіздкий (але акуратний і корпусований) перехідник Z-397, який запрацював відразу як слід (рис. 3.2).

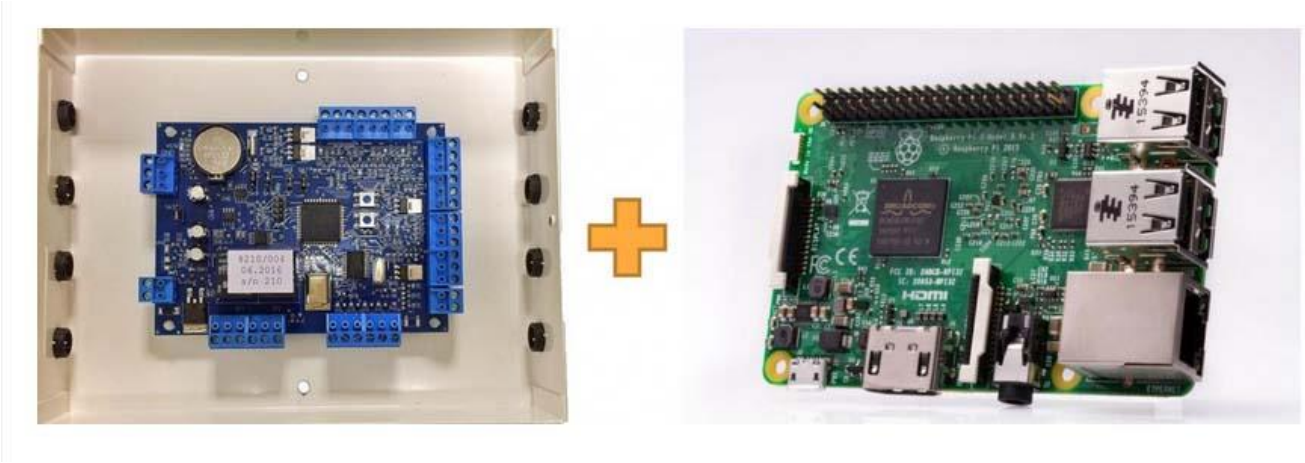

Рис. 3.2. Для нормальної роботи контролера протрібен перехідник

Програмна частина:

Починаємо розробку програми з визначення функцій, які вона має виконувати.

- Що потрібно - взаємодія з GATE для надсилання команд та отримання даних.
- Яким чином - вивчимо протокол GATE, напишемо серіалізатор та десеріалізатор даних, підключимо бібліотеку для роботи з послідовним портом.
- Що потрібно - взаємодія з платформою для отримання команд та надсилання даних.
- Як саме - виберемо для спілкування протокол MQTT, у коді скористаємося готовою бібліотекою Paho MQTT.

Отже, ми почали вивчення протоколу контролера GATE, який є закритим, тому нижче розказано лише про деякі його особливості. Він досить низькорівневий, і потрібно звертатися безпосередньо до регістрів пам'яті пристрою. У документі цього протоколу описані кадри запитів від комп'ютера контролеру і кадри відповідей контролера комп'ютера. Змінюючи поля в кадрі запиту, можна надсилати різні команди на пристрій і отримувати інформацію з регістрів.

Однією з особливостей протоколу є те, що ініціатором обміну завжди є комп'ютер. Тому застосовуються два підходи роботи з пристроєм:

- програмувати всю логіку роботи в агенті;
- використовувати зовнішні запити (від платформи).

Було обрано другий варіант і винесли логіку з кінцевого пристрою на платформу. Так її легко адаптувати та підлаштувати, при цьому код програми залишається компактним і дозволяє просто формувати команди для пристрою, а платформа, у свою чергу, координує відправку команд та їх періодичність.

Після того, як ми уважно вивчили цей протокол, формат кадрів та список команд, виникла перша складність. Команди для читання буфера, в якому містяться події про те, хто і скільки прийшов, не виявилося. Адже отримати цю інформацію – першочергове завдання. Знадобилося вивчити карту пам'яті контролера, щоб визначити адреси, якими потрібно зчитувати дані.

Наступна особливість роботи з контролером у тому, що за один цикл читання можна отримати лише 12 подій, по 8 байт на кожну. А на кожен прохід людини в офіс генерується вже дві події:

- знайдено ключ у банку ключів (банк ключів - ще один блок у розподіленій пам'яті контролера);
- відбувся прохід (якщо він, звісно, відбувся).

Нижче представлений фрагмент коду C++, що реалізує метод одного циклу читання буфера.

Приклад:

```
bool SerialPortInlet::readBufferCycle(unsigned
short& bottom, unsigned short const& top,
unsigned char& u_lowerBound,
unsigned char& l_lowerBound,
std::vector<unsigned char>& readBuffer,
std::string& result)
{
```

```
        // Підрахунок необхідної кількості байтів
  unsigned short byteCountTmp = top - bottom;
  BOOST_LOG_SEV(log_, logging::info) <<
    "Need read " << byteCountTmp << " byte";
  unsigned char byteCount;
        // За один цикл неможливо прорахувати більше 12
  // подій (96 байт)
  byteCount = byteCountTmp > 0x60 ? 0x60 :
    (unsigned char)byteCountTmp;
  BOOST_LOG_SEV(log_, logging::info) <<
    "Read " << +byteCount << " byte";
  // Описуємо тіло команди
  std::vector<unsigned char> body =
    {0x02, 0xA0, byteCount,
    u_lowerBound, l_lowerBound};
    std::vector<unsigned char> command;
  // Отримуємо повний текст команди
  generateComplexCommand(command,
    Command::BYTE_CODE_READ, body);
  // Якщо не вдалось з будь-яких причин
  // відправити команду (наприклад, кінцевий
  // пристрій не підключений), повертається false
  if (!sendCommand(command, result))
  {
  return false;
      }
// Інакше відправляємо відповідь з пристрою
// на парсинг по подіям
  SerialPortType::Answer answerEvents;
  if(!Parsers::parserAnswer(log_, result,
```

```
    answerEvents, Command::BYTE_CODE_READ))
  {
    BOOST_LOG_SEV(log_, logging::error) <<
      "Failed parse buffer reading";
    return false;
  }
  readBuffer.insert(readBuffer.end(),
  answerEvents.body.begin(),
  answerEvents.body.end());
// Зміщуємо нижню границю буфера для читання
// наступних подій
  bottom = bottom + byteCount;
  u_lowerBound = (unsigned char)(bottom >> 8) ;
  l_lowerBound = (unsigned char)bottom;
  return true;
}
```

Трохи додало клопоту те, що, нарешті витягнувши потрібні байти, на місці інформації про карту, ми побачили не номер карти, а адресу, за якою він знаходиться. Тому кожен номер ключа доводиться окремо зчитувати за адресою. Також не відразу помітили наявність байтстафінгу, його обробку ми запровадили вже після першого тестування з платою.

Повна структурна схема розробленої системи має такий вигляд (рис. 3.3).

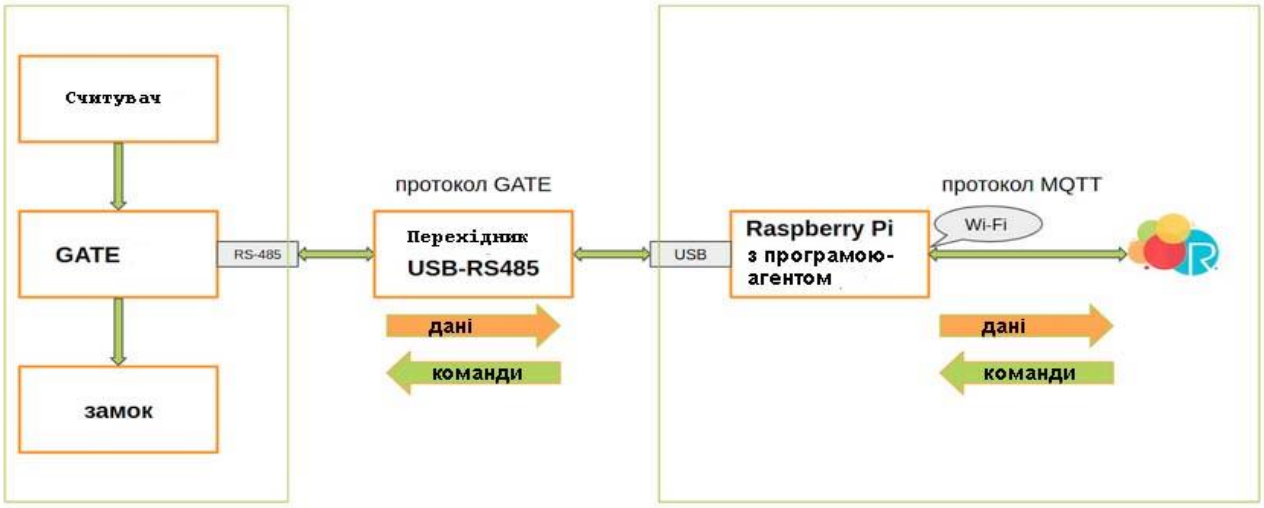

Рис. 3.3 Система конторолю доступа до приміщення

Працездатність всіх пристроїв було зручно перевіряти за допомогою графічного послідовного терміналу CuteCom. Після успішного тестування програма була поставлена на автозапуск, а Raspberry вирушила жити на стелі поряд із платою СКУДу.

Подальший розвиток систем забезпечення безпеки IoT

Незважаючи на те, що вищезазначені методи безпеки забезпечують широкий спектр засобів захисту для сучасних IoT пристроїв, існує кілька проблем та обмежень щодо ефективності виявлення та запобігання зовнішнім загрозам програмного та апаратного забезпечення.

Існуюче надійне та безпечне обладнання, таке як TPM, зазвичай вимогливе у плані енергоспоживання і складається з безлічі компонентів. Таким чином, адаптація таких пристроїв та архітектур за принципом plug-and-play не підходить для легких пристроїв IoT, де процесор менш потужний, а розмір пристрою та енерговитрати обмежені.

Методи виявлення шкідливих програм на основі контролю продуктивності пристрою багато в чому засновані на ефективних та складних методах машинного навчання, що дозволяють розрізняти допустимі та шкідливі операції. Однак такі методи зазвичай реалізуються у програмному забезпеченні, де дані HPC збираються на обладнанні та передаються в програму для обробки та виявлення в

режимі онлайн/офлайн. Це, на жаль, створює вузьке місце у схемі виявлення, оскільки програмна класифікація дуже повільна по відношенню до накопичених апаратних даних. Це змушує вибірку подій/даних виконуватися зі значно меншою частотою, підвищуючи ризик того, що шкідливі події чи виконання залишаться непоміченими. Зрештою це знижує ймовірність успіху та збільшує операційні витрати.

Більшість методів машинного навчання, що використовуються у вищезгаданих схемах, потребують великих даних для навчання, тестування та перевірки. Схема, заснована на золотому стандарті, отриманому під час її навчання, підходить лише відомих кіберзагроз, оскільки дозволяє правильно характеризувати шкідливі події етапі навчання. Отже, виявлення вразливостей нульового дня та невідомих загроз за допомогою такої схеми є досить складним завданням.

Системи моніторингу Інтернету речей та виявлення шкідливих програм на основі побічних каналів потребують додаткового обладнання для збирання та обробки даних. У цьому випадку самоконтроль може створювати перешкоди для зібраних підписів або сам блок моніторингу може бути скомпрометований. До того ж, отримання інформації про побічний канал живлення вимагає додаткового проводового підключення до контрольованого пристрою. Хоча для електромагнітного моніторингу не потрібне провідне з'єднання, вплив ЕМ-збирає антени і зовнішні перешкоди сильно впливають на якість виявлення. До того ж, розміщення додаткового обладнання для моніторингу може виявитися неприйнятним рішенням для малопотужних віддалених пристроїв Інтернету речей.

Апаратні рішення в галузі інформаційної безпеки для пристроїв IoT чудово доповнюють існуючі програмні механізми захисту. Ключовим напрямом досліджень може бути створення апаратних прискорювачів для високошвидкісних реалізацій машинного навчання на одному чіпі з іншим обладнанням. Розробка спрощених методів машинного навчання також має вирішальне значення для виявлення шкідливих програм/аномалій на основі

розпізнавання подій. На додаток до PMU для безпеки можуть використовуватися різні вбудовані датчики, такі як датчики температури, а також нові архітектури.

3.4 Висновки до третього розділу

Проаналізовано проблеми безпеки пристроїів в промислових мережах IoT.

Зроблено практичну реалізацію контролю доступу до приміщення за допомогою пристроів IoT.

Було реалізовано апаратну частину на базі контролеру GATE.

Під час реалізації програмної частини було використано протокол MQTT та готова бібліотека Paho MQTT.

Аапаратну та програмну частини було успішно протестовано.

ВИСНОВКИ

В магістерській роботі отримано наступні теоретичні та практичні результати:

1) Проаналізовано структуру промислової мережі IoT. Розглянуті проширені загрози для даних користувачів та пристроїв, підключених до промислової мережі IoT. Це дозволило краще осягнути проблематику иа зрозуміти потенціальні та існуючі загрози в промислових мережах IoT.

2) Виконано дослідження потенціальних та реальних загроз для промислових мереж IoT. Проведена детальна класифікація загроз та розглянуті методи протидії цим загрозам.

3) Підкреслено засоби забезпечення безпеки в промислових мережах IoT. Ці засоби детально проаналізовані та розглянуті на реальних прикладах.

4) Розглянуті методи та засоби забезпечення безпеки пристроїв в мережах IoT. Проведена оцінка ефективності запропонованих методів та засобів.

5) Проаналізована система забезпечення захисту пристроїв в промислових мережах IoT. Виконаний порівняльний аналіз цієї системи.

6) Запропонована власна система контролю доступа в приміщення засобами промислової мережі IoT.

7) Зроблено висновок, що під час налаштування системи контролю доступа виключена можливість несанкціонованого доступу відвідувачів в приміщення.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ ПРИ НАПИСАННІ МАГІСТЕРСЬКОЇ РОБОТИ

Характеристика джерела	Джерело
Два автори	1. Журахівський Б.Ю., Зенів І.О. Технології інтернету речей. Навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2021. – 127 с
Наукові статті в періодичних виданнях, матеріали конференцій, семінарів	2. Бондаренко Д.А. Застосування технології інтернету речей в сільскому господарстві. Державний університет телекомунікацій. Київ 3. International Journal of Open Information Technologies ISSN: 2307-8162 vol. 7, no.8, 2019 4. Basic protocols, message sequence charts, and the verification of requirements specifications / A. Letichevsky [et al.] // Computer Networks. 2005. Vol. 49, issue 5. P. 661–675. 5. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures / ENISA. Hague : European Union Agency For Network And Information Security, 2017. 103 p. doi:10.2824/03228. 16. Definition of a research and innovation policy leveraging cloud computing and IoT combination : Final report / Aguzzi S. [et al.]. European Commission, 2014. 95 p. doi:10.2759/38400. 6. Van der Meulen R. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016 // Gartner: [site]. 2017. 07 Apr. (date of access: 20.06.2021). 7. Kavis M. Making sense of IoT data with machine learning technologies // Forbes : (date of access: 20.06.2021). 8. Chui M., Löffler M., Roger R. The Internet of Things // McKinsey Quarterly : [magazine]. 2010. 01 March. (date of access: 20.06.2021). 9. Minerva R., Biru A., Rotondi D. Towards a definition of the Internet of Things (IoT). IEEE, 2015. (date of access: 20.06.2021). 10. Rayes A., Salam S. The things in IoT: Sensors and actuators // Internet of things from hype to reality. Cham : Springer, 2017. P. 57–77. 11. GSMA, “IoT Device Connection Efficiency Guidelines” Version 5.0, January 2018.

12. H., Wang W. A Game Theory Based Collaborative Security Detection Method for Internet of Things Systems // IEEE Transactions on Information Forensics and Security. 2018. Vol. 13, no. 6. P. 1432–1445. doi:10.1109/TIFS.2018.2790382.
13. Industrial Internet of Things Platform Comparison // M&S Consulting : [site]. 2016. 08 Febr.
14. The industrial internet of things (IIoT): An analysis framework / H. Boyes [et al.] // Computers in Industry. 2018. Vol. 101. P. 1–12.
15. Proposal of an automation solutions architecture for Industry 4.0 / M. Saturno [et al.] // 24th International Conference on Production Research (ICPR 2017) : proceedings. Lancaster, U.S.A. : DEStech Publications, Inc., 2017. 7 p. doi:10.12783/dtetr/icpr2017/17675.
16. S. Vitturi, C. Zunino and T. Sauter, "Industrial Communication Systems and Their Future Challenges: Next-Generation Ethernet, IIoT, and 5G," in Proceedings of the IEEE, vol. 107, no. 6, pp. 944-961, June 2019, doi: 10.1109/JPROC.2019.2913443.
17. Erguler I. A potential weakness in RFID-based Internet-of-things systems // Pervasive and Mobile Computing. 2015. Vol. 20. P. 115–126.
18. F. John Dian, R. Vahidnia and A. Rahmati, "Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey," in IEEE Access, vol. 8, pp. 69200-69211, 2020, doi: 10.1109/ACCESS.2020.2986329.
19. Zhong Ray J., Xu Xun, Klotz Eberhard, Stephen T. Newman Intellectual production in the context of Industry 4.0: Overview, Engineering 3 (2017), p.616-630.
20. Frankenfield J. Cloud Computing // computing.asp (date of access: 10.08.2021).
21. Singh D., Tripathi G., Jara A.J. A survey of Internet-of-Things: Future vision, architecture, challenges and services // 2014 IEEE World Forum on Internet of Things (WF-IoT). IEEE, 2014. P. 287–292. doi:10.1109/WF-IoT.2014.6803174. Internet of things – from research and innovation to market deployment / O. Vermesan, P. Friess (eds.). Aalborg, Denmark : River Publishers, 2014. 373 p. (River Publishers Series in Communications). (date of access: 20.06.2021).
22. Hamilton E. What is Edge Computing: The Network Edge Explained // Cloudwards : [site]. 2018.

23. Durmus M. What is Edge Computing? // AISOMA : [site]. 2019. 09 April. (date of access: 10.08.2021).
24. Chai W., Labbe M., Stedman C. Big data analytics // SearchBusinessAnalytics.com : [site]. 2021.
25. Artificial Intelligence (AI) // Techopedia : [site]. 2020. 27 March. (date of access: 10.08.2021).
26. Burns E. Machine learning // TechTarget : [site]. 2021. March. (date of access: 10.08.2021).
27. Hylving L., Schultze U. Evolving The Modular Layered Architecture in Digital Innovation: The Case of the Car's Instrument Cluster // International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design : proceedings. Milan, 2013. 17 p. (date of access: 10.08.2021).
28. F. J. Dian and R. Vahidnia, “LTE IoT Technology Enhancements and Case Studies,” in IEEE Consumer Electronics Magazine, doi: 10.1109/MCE.2020.2986834.
29. F. J. Dian, R. Vahidnia, “Formulation of BLE Throughput Based on Node and Link Parameters,” IEEE Canadian journal of Electrical and Computer Engineering, vol. 43, no. 4, pp. 261-272, Fall 2020, doi: 10.1109/CJECE.2020.2968546.
30. F. J. Dian, A. Yousefi, S. Lim, “A practical study on Bluetooth Low energy (BLE) throughput,” in IEEE IEMCON, pp. 768-771, Vancouver, Nov. 2018.
31. F. J. Dian, “Low-power Synchronized Multi-channel Data Acquisition Communication System,” in IEEE CCWC, pp. 1027-1031, Las Vegas, Jan. 2019.
32. F. J. Dian, A. Yousefi, K. Somaratne , “A study in accuracy of time synchronization of BLE devices using connection-based event,” in IEEE IEMCON, pp. 595 – 601, Vancouver, OCT. 2017.
33. F. J. Dian, A. Yousefi, K. Somaratne, “Performance evaluation of time synchronization using current consumption pattern of BLE devices,” in IEEE CCWC, pp. 906-910, Las Vegas, Jan. 2018.
34. F. J. Dian, “An analytical scheme for power consumption of battery-operated peripheral BLE nodes,” in 9th IEEE CCWC, pp. 1021-1026, Las Vegas, Jan. 2019.
35. F. J. Dian, A. Yousefi, S. Lim, “Time scheduling of central BLE for connection events,” in IEEE IEMCON, pp. 763-767, Vancouver, Nov. 2018.
36. Yousefi, F. J. Dian, K. Somaratne “Analysis of time synchronization based on current measurement for

	Bluetooth Low Energy (BLE)," in IEEE IEMCON, pp. 602 – 607, Vancouver, OCT. 2017. 37. K. Somaratne, F. J. Dian, A. Yousefi, "Accuracy analysis of time synchronization using current consumption pattern of BLE devices," in IEEE CCWC, pp. 841-844, Las Vegas, Jan. 2018.
Електронні ресурси	38. 10 Ways Machine Learning Is Revolutionizing Manufacturing: https://www.forbes.com/sites/louiscolumbus/2016/06/26/10-ways-machine-learning-is-revolutionizing-manufacturing/?sh=170b059b28c2 39. https://www.ibm.com/topics/internet-of-things 40. https://www.oracle.com/internet-of-things/what-is-iot/ 41. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT 42. Industrial internet of things // Wikipedia : [site]. 2021. https://en.wikipedia.org/wiki/Industrial_internet_of_things (date of access: 10.08.2021).