ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

“Засоби захисту інформації для Інтернету речей”

зі спеціальності 125 Кібербезпека

(код, найменування спеціальності)

освітньо-професійної програми Інформаційна та кібернетична безпека

(назва програми)

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

_____ Віктор ТАРАН

(підпис)

Виконав: здобувач вищої освіти групи
БСД-44 ТАРАН Віктор

(прізвище, ім’я)

Керівник доцент ЗИБІН Сергій

(науковий ступінь, вчене звання, прізвище, ім’я)

Рецензент _____

(науковий ступінь, вчене звання, прізвище, ім’я)

Київ 2025

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

Кафедра Систем та технологій кібербезпеки

Ступінь вищої освіти Бакалавр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“__” _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Тарану Віктору Дмитровичу

(прізвище, ім’я)

1. Тема кваліфікаційної роботи: Засоби захисту інформації для Інтернету речей
   керівник кваліфікаційної роботи Зибін Сергій, доцент
   (прізвище, ім’я, науковий ступінь, вчене звання)
   затверджені наказом Державного університету інформаційно-комунікаційних технологій від “__” _____ 2025 року №___.
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2025 р.
3. Вихідні дані до кваліфікаційної роботи _____
   IoT-системи підприємства;
   технічні та організаційні заходи захисту інформації IoT;
   наукова та технічна література, експлуатаційна документація, нормативні документи;
4. Зміст розрахунково-пояснювальної записки (перелік питань які потрібно розробити) ___
   Дослідження архітектури та специфіки IoT-систем з точки зору інформаційної безпеки.
   Дослідження існуючих загроз і вразливостей, характерних для IoT.
   Аналіз сучасних методів та засобів захисту в IoT.
   Розроблення рекомендацій та варіант практичної реалізації системи захисту інформації в IoT.
5. Перелік графічного матеріалу
   Презентація PowerPoint.
6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту IoT пристроїв організації.	04.04.2025 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	10.04.2025 р.	
3.	Аналіз сучасних загроз для IoT	17.04.2025 р.	
4.	Аналіз сучасних методів та засобів захисту для IoT.	22.04.2025 р.	
5.	Визначення вимог до захисту інформації в IoT-системах підприємства.	02.05.2025 р.	
6.	Практична реалізація варіанту захисту IoT-систем підприємства.	10.05.2025 р.	
7.	Розроблення рекомендацій щодо подальшого розвитку кіберзахисту підприємства.	15.05.2025 р.	
8.	Оформлення результатів роботи.	20.05.2025 р.	
9.	Підготовка доповіді до захисту.	06.06.2025 р.	

Здобувач вищої освіти _____ Віктор ТАРАН

(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Сергій ЗИБІН

(підпис) *(ім'я, прізвищ*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу

здобувача ТАРАНА Віктора
на тему: "Засоби захисту інформації для Інтернету речей"

Актуальність: Забезпечення безпеки інформації для Інтернету речей є надзвичайно важливим у сучасних умовах цифрової трансформації та стрімкого зростання кількості підключених пристроїв. Підвищена залежність від IoT створює нові вектори атак, які не охоплюються традиційними засобами захисту. Відсутність оновлень, використання стандартних паролів, відсутність шифрування та фізичний доступ до пристроїв підсилюють ризики. Через слабкий рівень захисту IoT-пристрої часто стають ціллю атак, що може призвести до витоку даних, збоїв у роботі або несанкціонованого доступу до об'єктів. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено актуальні загрози інформаційної безпеки в IoT-системах підприємств, сформульовано мету дослідження, його завдання та структуру системи захисту.
2. Досліджено підходи та засоби забезпечення безпеки інформації для IoT-середовищ на базі сучасних технологій захисту інформації.
3. Запропоновано варіант системи захисту інформації в IoT-інфраструктурі виробничого підприємства на базі сучасних технологій захисту інформації та рекомендації щодо покращення системи кіберзахисту в цілому.
4. Текст викладено послідовно та достатньо грамотно. Сформульовано змістовні та чіткі висновки. Графічний матеріал оформлено достатньо якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі доцільно було б провести аналіз ефективності обраних заходів захисту інформації на прикладі конкретного підприємства.
2. Запропоновану систему заходів захисту бажано було б продемонструвати на прикладі конкретного підприємства.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"добре"**, а здобувач(ка) **ТАРАН Віктор** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Рецензент: _____ _____ _____

(науковий ступінь, вчене звання) *(підпис)* *(ім'я, прізвище)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач ТАРАН Віктор до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: "Засоби захисту інформації для Інтернету речей"
Кваліфікаційна робота і рецензія додаються.
Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач **ТАРАН Віктор** обрав тему роботи, метою якої було дослідити засоби захисту інформації для Інтернету речей та розробка рекомендацій щодо їх реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи **ТАРАН Віктор** показав добру 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 ШАТАЛОВА Дмитра на оцінку "добре" та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Сергій ЗИБІН
(підпис) *(ім'я, прізвище)*
"___" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ТАРАН Віктор** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.
Завідувач кафедри Систем та технологій кібербезпеки
(ім'я, прізвище)

_____ Галина ГАЙДУР
(підпис) (ім'я, прізвище)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 57 сторінки, 15 рисунків, 24 джерел.

Об'єкт дослідження - захист IoT-систем підприємства.

Предмет дослідження - Методи та засоби забезпечення захисту інформації в IoT-середовищах на базі сучасних технологій захисту.

Мета роботи розробити варіант системи на базі сучасних рішень захисту та рекомендації щодо подальшого покращення кіберзахисту підприємства вцілому.

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

Захист інформації в Інтернеті речей є необхідною складовою забезпечення кіберстійкості сучасних підприємств. Через слабкий рівень вбудованого захисту IoT-пристроїв вони часто стають ціллю атак, що може призвести до компрометації даних або порушення безперервності бізнес-процесів.

У роботі досліджено проблему захисту інформації в IoT-системах підприємства, визначено типові загрози та причини їх виникнення. Проведено аналіз існуючих підходів до забезпечення безпеки та обґрунтовано доцільність впровадження технічних і організаційних заходів захисту.

На основі досліджень проведених в роботі запропоновано комплексну систему захисту, адаптовану до особливостей IoT-інфраструктури підприємства, а також проведено оцінку доцільністі впровадження запропонованих рішень та додаткових інструментів безпеки. Сформульовано рекомендації щодо подальшого розвитку системи кіберзахисту з урахуванням поточних викликів і обмежень.

Галузь використання - кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, ІОТ-ПРИСТРОЇ, ЗАХИСТ ІОТ-ПРИСТРОЇВ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІОТ-ПРИСТРОЇВ ПІДПРИЄМСТВА

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT - Internet of Things

GDPR - General Data Protection Regulation

AIoT - Artificial Intelligence of Things

IIoT - Industrial Internet of Things

IoMT - Internet of Medical Things

OWASP - Open Worldwide Application Security Project

MitM - Man in the Middle

AES - Advanced Encryption Standard

ECC - Elliptic Curve Cryptography

SHA - Secure Hash Algorithm

2FA - Two-factor Authentication

VLAN - Virtual Local Area Network

SDN - Software-defined Networking

VPN - Virtual Private Network

IDS/IPS - Intrusion Detection System, Intrusion Prevention System

ZTA - Zero Trust Architecture

SIEM - Security information and event management

СКУД - Система контролю управління доступом

PoE - Power over Ethernet

SOC - Security Operations Center

NAC - Network access control

SSL/TLS - Secure Sockets Layer, Transport Layer Security

OTP - One Time Password

ВСТУП

Актуальність дослідження. Стрімке зростання використання технологій Інтернету речей у корпоративному середовищі призвело до появи нових загроз для інформаційної безпеки. IoT-пристрої, які взаємодіють з мережею підприємства, часто мають обмежені обчислювальні ресурси, працюють на нестандартному програмному забезпеченні та не підтримують базові засоби захисту. Це створює суттєві ризики, пов’язані з несанкціонованим доступом, підміною даних, атакою на конфіденційність, цілісність і доступність інформації.

Пристрої IoT здебільшого виконують спеціалізовані функції — моніторинг параметрів навколишнього середовища, контроль доступу, відеоспостереження, дистанційне керування обладнанням тощо. Через це вони працюють у режимі реального часу та обмінюються даними з іншими системами, що робить їх вразливими до атак типу «людина посередині», DDoS-атак, проникнення через незахищені шлюзи та експлуатації відомих вразливостей. Компрометація навіть одного пристрою може дати зловмиснику змогу проникнути в інші сегменти мережі, оскільки багато IoT-систем не мають належної ізоляції або контролю доступу.

Проблема ускладнюється тим, що в багатьох організаціях не реалізовано жодних засобів для підвищення безпеки IoT-інфраструктури, а персонал не має достатнього рівня обізнаності щодо безпечного поводження з такими пристроями. У результаті, навіть у захищених середовищах з’являються «слабкі місця», через які можуть бути скомпрометовані критичні системи підприємства.

З огляду на зазначене, тема цієї кваліфікаційної роботи є актуальною. Вона спрямована на аналіз загроз, пов’язаних з IoT, оцінку вразливостей пристроїв та розробку варіанта комплексної системи захисту з урахуванням сучасних підходів до шифрування трафіку, автентифікації доступу, сегментації мережі, централізованого та організаційних заходів. Реалізація такої системи дозволить суттєво знизити ризики кібератак та забезпечити безпечну інтеграцію IoT в інфраструктуру підприємств.

Об’єкт дослідження - захист IoT-систем підприємства.

Предмет дослідження - Методи та засоби забезпечення захисту інформації в IoT-середовищах на базі сучасних технологій захисту.

Мета роботи розробити варіант системи на базі сучасних рішень захисту та рекомендації щодо подальшого покращення кіберзахисту підприємства вцілому.

Наукові завдання:

дослідження архітектури та специфіки IoT-систем з точки зору інформаційної безпеки;

дослідження існуючих загроз і вразливостей, характерних для IoT;

аналіз сучасних методів та засобів захисту в IoT;

Розроблення рекомендацій та варіант практичної реалізації системи захисту інформації в IoT.

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

Практичне значення одержаних результатів: розроблено рекомендації

щодо застосування методів та засобів захисту IoT-інфраструктури підприємства, а також розроблено рекомендації щодо покращення кіберзахисту підприємства вцілому.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науково-практичній конференції «Цифрова трансформація кібербезпеки», яка відбулася 24 квітня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Сутність та архітектура Інтернету речей

Завдяки розвитку сучасних технологій пристрої Інтернету речей присутні майже в кожній сфері нашого життя, відіграючи свою особливу роль. Інтернет речей — це концепція, що передбачає об’єднання в мережу фізичних об’єктів, які здатні самостійно збирати, передавати та обробляти дані без безпосередньої участі людини. Ці об’єкти можуть включати в себе різні датчики, виконавчі пристрої, контролери, розумну побутову техніку, промислове обладнання тощо. Ключова особливість IoT полягає в тому, що «речі» виступають активними елементами інформаційного простору, здатними взаємодіяти між собою через мережеву інфраструктуру [1]. Важливо зазначити, що IoT-пристрої, особливо у сфері інформаційної безпеки підприємств, чаще за все відіграють роль «цифрових датчиків» у загальній системі безпеки, дозволяючи вчасно отримувати актуальну інформацію про стани різних систем або брати на себе функцію фізичного захисту. В той же час потрібно враховувати, що особливості технічних характеристик (рисунок 1.1) роблять ці пристрої вразливими до потенційних атак з боку зловмисників.

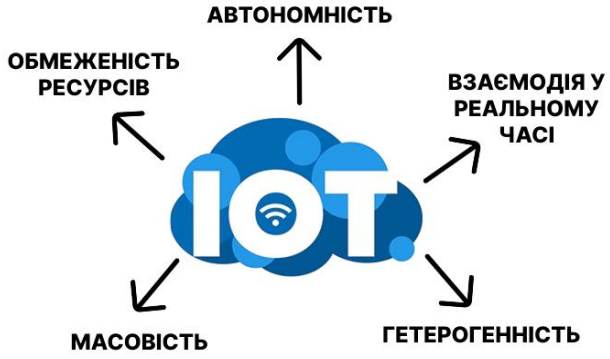

Рис. 1.1 Характеристики IoT пристроїв

В більшості випадків пристрої IoT мають наступні характеристики, деякі з них суттєво впливають на інформаційну безпеку [2]:

обмеженість ресурсів, через яку більшість IoT-пристроїв мають низьку обчислювальну потужність, обмежену оперативну пам’ять і батарею, що впливає на можливості реалізації захисту;

автономність, через що багато пристроїв працюють роками без зовнішнього обслуговування;

взаємодія у реальному часі, через що пристрої повинні реагувати на зміни оточення без затримки;

масовість, через що великі обсяги пристроїв вимагають централізованого керування та безпечної масштабованості;

гетерогенність, що створює широкий спектр виробників і протоколів комунікації створює виклики щодо сумісності;

Рівні архітектури та моделі розгортання IoT-систем

В основі IoT лежить ідея перетворення будь-якого пристрою на джерело даних, що працює в реальному часі. Згідно з даними Міжнародного союзу електрозв’язку, реалізація концепції IoT має на меті забезпечення "всеохопного з’єднання", що є логічним продовженням розвитку мереж наступного покоління [1]. Базова архітектура IoT, зазвичай, поділяється три логічних рівня: фізичний, мережевий і рівень обробки даних (рисунок 1.2) [1].

Рис. 1.2 Рівні архітектури IoT

Описати ці рівні можна наступним чином [3]:

фізичний рівень: фізичні об'єкти, що оснащені датчиками, виконавчими механізмами та модулями зв'язку. Вони збирають дані з навколишнього середовища (температуру, рух) та передають їх на наступні рівні для обробки.

мережевий рівень: відповідає за передачу даних між пристроями, шлюзами та хмарними/локальними серверами. Технології зв'язку залежать від конкретної задачі: Wi-Fi, Bluetooth, Zigbee, LoRaWAN, мобільні мережі (3G/4G/5G), Ethernet тощо.

рівень обробки даних: сервери, контролери або хмарні платформи, які аналізують, фільтрують та зберігають отриману інформацію. Також тут реалізуються правила логіки, автоматизації та прийняття рішень.

Розгортання IoT-систем може здійснюватися за централізованою або децентралізованою моделлю. У централізованій архітектурі дані збираються та обробляються на одному або кількох центральних серверах, тоді як у

децентралізованій використовуються периферійні обчислення, що дозволяє знизити затримки та зменшити навантаження на мережу. Інфраструктура IoT може бути побудована як з використанням локальних серверів, так і за допомогою хмарних рішень (наприклад, Azure IoT Hub, AWS IoT Core, Google Cloud IoT), які забезпечують масштабованість, автоматичну обробку та зберігання даних[4].

Протоколи зв'язку в IoT

Як вже згадували раніше Інтернет речей базується на широкому спектрі протоколів, адаптованих до обмежених ресурсів IoT-пристроїв. Кожен з цих протоколів має свої переваги і недоліки, тому їх вибір залежить від конкретного застосування: дальність зв'язку, споживання енергії, вимоги до безпеки, обсяг даних тощо. Серед найбільш поширених можна виділити наступні протоколи (рисунок 1.3): MQTT, CoAP, Zigbee, Z-Wave, Thread, LoRaWAN та HTTP/HTTPS [5].

Рис. 1.3 Найпоширеніші протоколи зв'язку в IoT

Важливим фактором під час розробки протоколів зв’язку IoT є особливості технічних характеристик систем, де вони застосовуються. Так для систем із низькою пропускною здатністю мережі був розроблений протокол MQTT, що являє собою легковаговий протокол публікації/підписки, який широко використовується у промислових IoT рішеннях.

Враховуючи те, що енергозбереження є необхідністю для деяких IoT пристроїв було створено протокол CoAP, який працює поверх UDP, забезпечуючи передачу даних у форматі REST та використовується в обмежених середовищах.

Для енергоефективної комунікації IoT пристроїв в межах однієї будівлі чи офісу існують протоколи ближнього радіозв’язку - Zigbee, Z-Wave, та Thread. Натомість для далекого радіозв’язку використовується протокол LoRaWAN, він дозволяє покривати великі території при мінімальних витратах енергії, але має низьку швидкість передачі даних.

Не варто також забувати про зв’язок з веб інтерфейсами та REST API, для цього хоч і не завжди ефективно, але досі використовуються протоколи HTTP/HTTPS [5].

Моделі взаємодії у IoT

У контексті архітектури IoT системи можуть функціонувати за різними моделями взаємодії. Кожна з цих моделей впливає на затримку, обсяг трафіку, вимоги до безпеки та стійкість до збоїв у мережі (рисунок 1.4).

Рис. 1.4 Моделі взаємодії IoT

Найпростіша модель, яку можна зустріти в повсякденному житті - "Пристрій-до-пристрою" (D2D) використовується для обміну даними безпосередньо між пристроями (наприклад, передача даних від смарт годинника до смартфону через Bluetooth), часто без участі централізованого серверах.

Дуже часто в промисловості зустрічається модель "Пристрій–шлюз–хмара" (D2G2C), в якій шлюз (наприклад, Raspberry Pi або маршрутизатор з прошивкою IoT, що отримує дані з датчиків та надсилає їх до системи моніторингу) виступає посередником між пристроями і хмарною платформою.

Досить розповсюдженою є модель "Пристрій–хмара" (D2C), вона реалізована таким чином, що IoT пристрій має безпосереднє підключення до хмарного сервісу через Інтернет (наприклад, розумний годинник, що надсилає дані показників життєдіяльності людини для аналізу та зберігання у хмарі) без шлюзу між ними[6].

Основні виклики реалізації IoT

Попри потенціал IoT, його практична реалізація супроводжується низкою проблем, пов’язаних з безпекою, сумісністю, масштабованістю та конфіденційністю.

Проблема безпеки виникає перш за все через обмежені обчислювальні можливості IoT-пристроїв складно впровадити стандартні механізми шифрування, автентифікації та обробки даних прямо на пристрої. Відкритість протоколів, нестача автентифікації, відсутність оновлень програмного забезпечення створюють вразливості в IoT, які активно експлуатуються у кібератаках.

Велика кількість виробників, різноманітність протоколів (MQTT, CoAP, AMQP, ZigBee) і відсутність єдиних стандартів призводить до фрагментації ринку та складнощів інтеграції пристроїв, створюючи проблему сумісності.

Попри різноманість різних рішень реалізації інфраструктури і IoT існує проблема масштабованості. Підключення великої кількості пристроїв до мережі створює значне навантаження на інфраструктуру та потребує ефективних методів управління.

Окремо від проблеми безпеки можна також виділити конфіденційність. Дані, зібрані IoT-пристроями (відео, звук, місце перебування), можуть нести конфіденційну інформацію, що потребує належного захисту відповідно до законодавства (наприклад, GDPR).

Тенденції розвитку архітектури IoT

Аналітики прогнозують стрімке зростання кількості IoT-пристроїв — понад 40 мільярдів до 2030 року[7]. Перш за все очікується подальший розвиток у напрямках Edge Computing, AIoT та децентралізованих моделях управління[2 4].

Прогнозується, що обробка даних зміститься ближче до їхнього джерела (пристрою або шлюзу), що дозволить зменшити затримки та підвищити продуктивність IoT-систем. Управління IoT-системами стане децентралізованим (наприклад, на базі блокчейну) за рахунок створення довірчих моделей між пристроями без централізованого контролера. Враховуючи швидкість розвитку

штучного інтелекту його буде інтегровано в IoT-системи для реалізації адаптивного аналізу даних та прийняття рішень на основі поведінкових моделей [4].

1.2 Класифікація пристроїв IoT та їх функціональні особливості

Інтернет речей охоплює велику різноманітність пристроїв, що об’єднані у єдину мережу для збору, обміну, обробки і реагування на дані. Класифікація таких пристроїв є необхідною для розуміння їх функціонального призначення, безпекових особливостей та ролі в загальній архітектурі. IoT-пристрої можна класифікувати за функціональним призначенням та середовищем застосування.

Класифікація пристроїв за функціональним призначенням

За функціональним призначенням пристрої IoT можна поділити на безліч видів, але з них виділяється чотири основних (рисунок 1.5): датчики, виконавчі пристрої, пристрої збору та обробки даних та інтерфейсні пристрої [8].

Рис. 1.5 Приклади пристроїв за їх функціональним призначенням

Датчики є одним з найбільш розповсюджених видів, являючи собою пристрої для збору даних з навколишнього середовища або об’єкта. Здебільшого саме вони є джерелом первинних даних, передаючи їх до центрального вузла або хмарного сервісу для обробки. Прикладами цих пристроїв є датчики температури, вологості, руху, освітлення, газів тощо.

Виконавчі пристрої за розповсюдженістю знаходяться майже на рівні датчиків і часто працюють з ними в парі, являють собою пристрої, які отримують команди від контролерів і виконують дії, як-от: відкриття замків, активація сигналізацій, включення освітлення, тощо. Прикладами цих пристроїв є сервоприводи у розумних замках, магнітні замки, сигналізація.

Більш “розумними” пристроями є IoT контролери та шлюзи (збір та обробка даних), являють собою проміжну ланку між датчиками та віддаленими сервісами та здатні здійснювати попередню обробку даних, шифрування, фільтрацію тощо. Вони також можуть надсилати команди та контролювати роботу датчиків та виконавчих пристроїв. Прикладами цих пристроїв є одноплатні комп’ютери, запрограмовані плати з модулями зв’язку тощо.

Для взаємодії користувача з IoT-системою використовуються інтерфейсні пристрої. Це можуть бути екрани, мобільні додатки та пристрої, тощо, які дозволяють користувачеві впливати, як на окремі компоненти IoT-системи, так і в цілому на всю систему, а також візуалізувати оброблені дані.

Класифікація пристроїв за середовищем застосування

На практиці архітектура IoT реалізується як на рівні окремого будинку чи підприємства, так і в масштабі міста чи держави. Основні середовища застосування IoT пристроїв [4] (рисунок 1.6):

споживчі IoT-пристрої — це «розумні» гаджети для дому, які підвищують комфорт користувача та енергоефективність побуту. До них належать камери спостереження, розумні дверні замки, термостати, лампи, побутова техніка та інші

пристрої, що реалізують автоматизоване керування освітленням, кліматом або доступом до приміщень;

Індустріальні IoT-пристрої (IIoT) використовуються у виробництві, логістиці та енергетиці й забезпечують збір, аналіз та передачу даних про стан обладнання, що дозволяє виявляти несправності на ранньому етапі, оптимізувати технологічні процеси й підвищити ефективність управління підприємствами.

IoT для охорони здоров'я (IoMT) включає медичні сенсори, браслети для моніторингу стану здоров'я, інгалятори та інші пристрої, які передають біометричні дані у реальному часі до медичних центрів для діагностики та нагляду за пацієнтом;

інфраструктурні IoT-пристрої знаходять своє застосування в концепції «розумного міста» (Smart City) — вони охоплюють системи управління транспортом, дорожнім рухом, освітленням, збором сміття, безпекою, водопостачанням тощо, забезпечуючи ефективне використання ресурсів та підвищення якості життя громадян.

Рис. 1.6 Приклади пристроїв за середовищем їх застосування

1.3 Загрози безпеці в системах IoT: сучасний стан, виклики, тенденції

Системи Інтернету речей стали важливою складовою сучасної цифрової інфраструктури, інтегруючи фізичні пристрої у єдине мережеве середовище. Однак активне впровадження IoT супроводжується значним збільшенням потенційних кіберзагроз, що зумовлює необхідність глибокого аналізу сучасного стану безпеки в цій галузі, визначення актуальних викликів і виявлення новітніх тенденцій.

Основні загрози IoT-систем, сучасний стан та виклики

На момент 2025 року більшість IoT-пристроїв все ще залишаються вразливими через низький рівень захисту, закладений на етапі проєктування. За даними звіту Unit 42 IoT Threat Report компанії Palo Alto Networks (2020), понад 98% IoT-трафіку не зашифровано, що робить його вразливим до перехоплення й аналізу. Більше того, 57% пристроїв вразливі до середньостатистичних атак, оскільки виробники часто нехтують оновленнями безпеки або ж використовують застаріле ПЗ [9]. Інша критична проблема — відсутність уніфікованих стандартів безпеки для IoT-пристроїв, що призводить до фрагментації ринку і складності інтеграції захисних рішень. Це підтверджується дослідженням від OWASP, у якому зазначено, що "небезпека IoT зумовлена саме розривом між IT-безпекою та вбудованими системами". На рисунку 1.7 зображено перелік десяти найрозповсюдженіших і найвпливовіших вразливостей IoT-систем, визначених OWASP’ом у 2024 році[10].

Рис. 1.7 OWASP IoT TOP 10

Серед найпоширеніших викликів і загроз в IoT варто виділити низку взаємопов'язаних проблем, що виникають як через технічні обмеження пристроїв, так і через недоліки в їх проєктуванні та використанні. Однією з основних є дилема між швидкістю впровадження нових рішень та безпекою. Сучасний ринок диктує виробникам необхідність якомога швидше виводити пристрої на ринок, аби зайняти нішу або задовольнити попит, через що питання захисту часто відсувається на другий план. Це створює вразливі екосистеми, де безпека розглядається не як фундаментальна складова, а як необов'язкове доповнення.

Обмеженість апаратних ресурсів - це також дуже поширений виклик: більшість IoT-пристроїв мають малу обчислювальну потужність, обмежену пам'ять і мінімальне енергоспоживання, що ускладнює реалізацію повноцінного криптографічного захисту, систем виявлення вторгнень та моніторингу. Це відкриває шлях до використання таких пристроїв як точок входу для зловмисників або навіть як інструментів DDoS-атак, яскравим прикладом чого стала атака ботнету Mirai у 2016 році [11].

Ще однією критичною проблемою є небезпечна автентифікація: багато пристроїв постачаються з типовими або слабкими паролями (наприклад, "admin",

“123456”), які легко піддаються атакам методом перебору, а іноді користувач взагалі позбавлений можливості змінити пароль. Окрім цього, значна кількість IoT-пристроїв не шифрують мережевий трафік, що створює умови для атак типу “людина посередині” (MitM), коли зловмисник може перехоплювати або змінювати передані дані.

Посилює ризики і відсутність оновлень безпеки: багато виробників не передбачають регулярного оновлення прошивки, через що знайдені вразливості можуть залишатися відкритими роками. Через компактність і просторову розосередженість IoT-пристрої часто стають легкою ціллю фізичних атак, зокрема підключення до відкритих портів, зчитування вмісту прошивки або підміни обладнання.

Не менш небезпечними є загрози соціальної інженерії, оскільки IoT-системи тісно інтегруються з мобільними додатками та хмарними сервісами, якими керують користувачі. Недостатня обізнаність останніх щодо безпеки, надання надмірних дозволів, перехід за фішинговими посиланнями або помилкова конфігурація можуть стати фатальними чинниками компрометації системи.

Тенденції розвитку безпеки IoT

Сучасні підходи до підвищення кібербезпеки в IoT-системах все більше ґрунтуються на концепції «безпека за замовчуванням» (Security by Design), яка передбачає впровадження захисних механізмів вже на ранніх етапах проєктування пристроїв, а не як додаткову опцію на фінальних стадіях. Це включає розробку архітектури з урахуванням загроз, використання безпечних компонентів і чітко визначених політик доступу. Водночас зростає роль штучного інтелекту у забезпеченні динамічного виявлення загроз: алгоритми машинного навчання здатні аналізувати трафік IoT-пристроїв у реальному часі, виявляти аномальні шаблони поведінки, що можуть свідчити про злом або інші нетипові дії, та реагувати на інциденти до того, як вони призведуть до серйозних наслідків [12].

Для створення уніфікованих вимог до безпеки активно впроваджуються стандарти, серед яких важливим є ETSI EN 303 645 — європейський документ, що

визначає мінімальні вимоги до кібербезпеки споживчих IoT-пристроїв, включаючи вимоги до безпечного оновлення програмного забезпечення, наявності унікальних облікових записів, обов'язкового шифрування трафіку тощо [13]. Окрім технічних рішень, активно розвивається і правове регулювання галузі: в Європейському Союзі ухвалено Cyber Resilience Act, а в США діє IoT Cybersecurity Improvement Act, які зобов'язують виробників дотримуватися встановлених вимог безпеки, проводити оцінку ризиків і забезпечувати оновлення протягом усього життєвого циклу пристрою. Усе це свідчить про тенденцію до більш комплексного та обов'язкового підходу до захисту IoT-екосистем на всіх рівнях.

1.4 Основні методи та підходи до захисту інформації в IoT

Захист інформації в Інтернеті речей вимагає застосування комплексного підходу, який враховує обмежені обчислювальні ресурси пристроїв, їх масовість, географічну розподіленість і високу вразливість до атак. В основі сучасних рішень лежить поєднання криптографічних методів, контролю доступу, сегментації мережі, моніторингу та безпечної розробки прошивок. На рисунку 1.8 зображено основні методи та підходи до захисту інформації в IoT.

Рис. 1.8 Методи та підходи до захисту інформації в IoT

Криптографічні методи

Криптографічні методи відіграють ключову роль у забезпеченні конфіденційності, цілісності та автентичності даних, що передаються в IoT-системах. Враховуючи обмежені обчислювальні ресурси таких пристроїв, найчастіше застосовуються полегшені алгоритми шифрування, які не потребують великої кількості пам’яті або потужного процесора.

Серед симетричних методів найбільш розповсюдженими є AES та ChaCha20 — вони використовуються для швидкого шифрування трафіку в межах локальних мереж між IoT-пристроями. Для цілей автентифікації та безпечного обміну ключами зазвичай застосовують асиметричне шифрування на основі еліптичних кривих (ECC), яке забезпечує високий рівень криптозахисту навіть при невеликому розмірі ключа, що робить його ідеальним для малопотужних пристроїв. Для перевірки цілісності даних активно використовуються геш-функції, зокрема SHA-256 і SHA-3, які дозволяють переконатися в тому, що дані не були змінені під час передавання [14].

Згідно з рекомендаціями Національного інституту стандартів і технологій США (NIST), комбінація алгоритмів ECC і AES-128 забезпечує достатній рівень захисту для більшості IoT-рішень при мінімальному впливі на продуктивність пристрою [14].

Автентифікація та авторизація

Для забезпечення надійної ідентифікації та контролю доступу в IoT-мережах кожен пристрій має бути однозначно ідентифікований і мати обмежений доступ лише до дозволених сервісів.

Одним з поширених способів ідентифікації в масштабних системах є використання цифрових сертифікатів X.509, які забезпечують автентичність пристрою та захищене з'єднання на основі криптографії з відкритим ключем. У випадках, коли IoT-пристрої взаємодіють із веб-сервісами або хмарними

платформами, застосовуються протоколи авторизації OAuth 2.0 та OpenID Connect, які дозволяють безпечно передавати облікові дані та обмежувати рівень доступу до ресурсів. Для підвищення рівня безпеки управління IoT-шлюзами все частіше використовується двофакторна автентифікація (2FA), яка додає додатковий рівень захисту при доступі до критичної інфраструктури.

Сегментація мережі та зонування

Розділення IoT-інфраструктури на ізольовані зони є ключовим підходом до мінімізації ризиків поширення кібератак у разі компрометації окремих пристроїв або сегментів мережі.

Для досягнення цього використовуються технології віртуального сегментування, зокрема VLAN , SDN та VPN, які дозволяють логічно розділяти IoT-пристрої за функціональністю чи рівнем критичності, забезпечуючи контрольований трафік між зонами. Додатковим рівнем захисту виступають міжмережеві екрани (Firewall) та системи виявлення/запобігання вторгненням (IDS/IPS), які перешкоджають несанкціонованому доступу ззовні або з корпоративної мережі до чутливої IoT-зони. Сучасною практикою також є впровадження архітектури нульової довіри (ZTA), відповідно до якої жоден пристрій чи користувач не вважається надійним за замовчуванням, навіть якщо знаходиться всередині мережі. Цей принцип забезпечує обов’язкову перевірку кожного запиту доступу на основі контексту, автентифікації та політик.

Згідно зі стандартами безпеки IEC 62443, які розроблені для промислових систем автоматизації, рекомендовано впроваджувати чітке зонування IoT-мереж із використанням шлюзів контролю доступу, що дозволяє знизити ризик горизонтального поширення атак у межах інфраструктури [15].

Захист прошивок та оновлення

Прошивки IoT-пристроїв часто становлять серйозну вразливість у системі безпеки, оскільки багато виробників не оновлюють їх належним чином або використовують старі, вже скомпрометовані версії. Для забезпечення цілісності та захисту від несанкціонованого втручання дедалі частіше впроваджуються сучасні механізми контролю.

Одним з таких є технологія Secure Boot, яка забезпечує завантаження лише автентичної прошивки, підписаної виробником. Це запобігає запуску шкідливого або модифікованого коду під час старту пристрою. Крім того, критичну роль відіграє механізм оновлення прошивки «по повітрю» (FOTA), який дозволяє безпечно отримувати оновлення через мережу з обов'язковою перевіркою цифрового підпису. Це дозволяє своєчасно закривати вразливості без фізичного втручання в пристрій. Ще одним прогресивним підходом є використання концепції Binary Transparency, яка передбачає можливість відкритої перевірки відповідності встановленого бінарного коду офіційно оприлюдненій версії. Такий підхід унеможливлює приховане внесення змін у прошивку й сприяє прозорості та довірі до виробника [16].

У сукупності ці методи істотно підвищують рівень безпеки IoT-пристроїв на рівні програмного забезпечення й захищають кінцевого користувача від потенційно катастрофічних наслідків експлуатації скомпрометованих систем.

Моніторинг та виявлення аномалій

Сучасні системи безпеки IoT повинні бути здатні до оперативного виявлення та реагування на підозрілу активність у режимі реального часу, оскільки затримки у виявленні загроз можуть мати катастрофічні наслідки для інфраструктури.

Одним із ключових компонентів є SIEM-системи, які здійснюють централізований збір, кореляцію та аналіз логів з великої кількості джерел — IoT-пристроїв, шлюзів, серверів тощо. Вони дозволяють виявляти аномалії в поведінці пристроїв, невідповідність політикам безпеки або ознаки потенційних атак. На додачу до класичних методів дедалі частіше застосовуються інтелектуальні засоби, зокрема ML-базовані IDS, які використовують алгоритми машинного навчання для

розпізнавання аномалій у трафіку та поведінці пристроїв. Вони здатні самонавчатися та адаптуватися до нових типів загроз, що особливо важливо в динамічному середовищі IoT.

Згідно з даними Cisco (2017), впровадження SIEM-систем у середовищі середніх підприємств дозволило скоротити середній час виявлення загроз до 6 годин, що свідчить про високу ефективність таких рішень у сфері кіберзахисту. Така інтеграція не лише підвищує безпеку IoT-систем, але й дозволяє проактивно запобігати інцидентам до того, як вони переростуть у серйозні атаки [17].

1.5 Аналіз нормативно-правової та стандартної бази з кібербезпеки IoT

Успішне забезпечення кібербезпеки в Інтернеті речей неможливе без наявності ефективної нормативно-правової та стандартної бази, що регламентує вимоги до захисту пристроїв, даних і каналів зв'язку. Через специфіку IoT як технології, що охоплює як споживчі, так і промислові сфери, нормативне регулювання має бути багаторівневим, адаптивним і міждисциплінарним.

Стан нормативного регулювання IoT-безпеки у світі та в Україні

На глобальному рівні функціонує низка технічних стандартів, таких як ISO/IEC 30141 (архітектура IoT), ETSI EN 303 645 (базові вимоги до захисту споживчих пристроїв), а також серія документів NIST IR 8259 (управління ризиками IoT). Вони встановлюють мінімальні вимоги до безпечного проєктування пристроїв, оновлення програмного забезпечення, захисту персональних даних і контролю доступу [18].

В Україні правове регулювання безпеки Інтернету речей перебуває на ранньому етапі розвитку. Закон «Про основні засади забезпечення кібербезпеки України» та національні стандарти, такі як ДСТУ ISO/IEC 27001:2015, визначають загальні принципи безпеки інформаційних систем, але не забезпечують спеціалізованого правового поля для IoT. Також відсутня відповідальність

виробників за незахищені IoT-пристрої, що унеможливлює контроль якості з боку держави чи споживача.

Види нормативно-правового регулювання в сфері IoT-безпеки

Нормативна база у сфері кіберзахисту IoT охоплює кілька рівнів регулювання, що доповнюють один одного для забезпечення комплексної безпеки. На міжнародному рівні ключову роль відіграють технічні стандарти, зокрема документи ISO, IEC, ETSI та NIST, які встановлюють вимоги до безпеки пристроїв, конфіденційності даних та захищеності мережевої інфраструктури. Наприклад, стандарт ISO/IEC 27030 описує практики безпеки для IoT-систем, а ETSI EN 303 645 встановлює вимоги до безпеки споживчих IoT-пристроїв [18].

Національні нормативно-правові акти формують другий рівень і включають закони, укази та стратегії з кібербезпеки, які регламентують захист критичної інфраструктури, зокрема й IoT-елементів, у межах юрисдикції конкретної держави. Третій рівень — це внутрішні нормативні документи на рівні підприємств і відомств, де визначаються політики доступу, оновлення програмного забезпечення, використання камер, замків та інших компонентів IoT-інфраструктури. Четвертий рівень становлять регуляторні ініціативи наддержавного характеру, наприклад, Cyber Resilience Act у ЄС, який передбачає обов’язкові вимоги до безпеки ще до комерційного запуску пристроїв, стимулюючи виробників вбудовувати кіберзахист у сам процес розробки [18].

Така багаторівнева система створює нормативну основу, яка охоплює весь життєвий цикл IoT-пристрою — від проєктування до виведення з експлуатації.

Основні проблеми нормативного регулювання IoT-безпеки

Стан нормативно-правового забезпечення кібербезпеки IoT в Україні характеризується низкою суттєвих проблем, які перешкоджають ефективному захисту як споживчих, так і промислових IoT-систем. Однією з ключових проблем є відсутність спеціалізованого законодавства, що прямо регламентувало б вимоги до безпеки IoT-пристроїв.

На сьогодні українські нормативно-правові акти не охоплюють специфіку IoT у достатній мірі, що створює правовий вакуум і унеможливлює системний підхід до регулювання цієї сфери. Імплементація міжнародних стандартів, таких як ISO/IEC або рекомендацій NIST, залишається на низькому рівні, особливо серед малих і середніх підприємств, які через брак ресурсів або обізнаності не дотримуються навіть базових вимог до кіберзахисту. До того ж нормативна база в Україні є фрагментованою та неузгодженою: існує розрив між державними постановами, галузевими рекомендаціями та внутрішніми політиками підприємств. Відсутність уніфікованих підходів створює нерівномірне поле безпеки в різних секторах економіки. Крім того, на сьогодні відсутній ефективний державний контроль за якістю та безпекою IoT-продукції, що надходить на український ринок. Це відкриває шлях до масового розповсюдження технічно вразливих пристроїв, які можуть бути використані зловмисниками для кібернападів або несанкціонованого збору даних.

Напрями вдосконалення нормативної та стандартної бази

Подолання нормативно-правових прогалин у сфері кібербезпеки IoT в Україні потребує розробки національного технічного регламенту, який би чітко визначав обов’язкові вимоги до автентифікації, шифрування, оновлення програмного забезпечення та захисту даних у пристроях Інтернету речей. Такий документ має стати основою для стандартизації безпеки пристроїв на всіх етапах їх життєвого циклу. Важливою умовою удосконалення нормативної бази є імплементація європейських ініціатив, зокрема Cyber Resilience Act та принципів ENISA — Європейського агентства з кібербезпеки, які передбачають сертифікацію IoT-пристроїв щодо кіберстійкості ще до їх появи на ринку. Також необхідно підвищити прозорість і відповідальність виробників шляхом запровадження механізмів маркування пристроїв за рівнем безпеки, що дозволить споживачам свідомо обирати більш захищені рішення.

З огляду на критичну роль IoT у системах національного значення, доцільним є включення вимог до безпеки IoT у нормативи щодо захисту критичної

інфраструктури. Крім того, держава має запровадити обов’язкові стандарти використання безпечних IoT-рішень у державних установах та комунальних підприємствах, які працюють з персональними або службовими даними. Незважаючи на часткове впровадження міжнародних стандартів і існування загальних нормативів, правова база в Україні залишається фрагментарною, неуніфікованою та недостатньо адаптованою до реалій сучасної IoT-екосистеми. Тому її подальший розвиток має ґрунтуватися на комплексному підході, що враховує кращі практики ЄС і США та орієнтується на забезпечення безпеки як для кінцевих користувачів, так і для критичних систем.

2 ПРОЕКТУВАННЯ ІОТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА З УРАХУВАННЯМ ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Визначення загальної архітектури IoT-інфраструктури підприємства

В умовах сучасних виробничих підприємств, впровадження систем Інтернету речей дозволяє не лише підвищити ефективність технологічних процесів, але й забезпечити їхню безпеку за рахунок контролю за ключовими параметрами, моніторингу критичних зон та своєчасного реагування на можливі загрози. Для демонстрації використане підприємство, яке знаходиться на стадії проекту, з розгалуженою архітектурою IoT, яка охоплює зону виробництва, офісні приміщення та має зв’язок з віддаленим головним офісом. Такий підхід дозволяє продемонструвати реалізацію цілісного комплексу інформаційної безпеки, що охоплює всі критичні елементи IoT. Архітектура IoT підприємства передбачає використання кількох IoT-систем, кожна з яких реалізує окремі функції збору, обробки та передачі даних. Далі ми розглянемо кожну з них окремо.

Система моніторингу температури та вологості

У виробничій зоні підприємства реалізовано систему моніторингу температури та вологості (рисунок 2.1), яка забезпечує контроль за оптимальними умовами зберігання сировини та виробництва продукції. Основними компонентами цієї системи є датчики температури та вологості (DHT22 і SHT31), які розміщуються як у виробничих приміщеннях, так і у зонах зберігання. Зібрані дані з датчиків надходять до IoT-шлюзу на базі ESP32 через фізичне з’єднання, який далі забезпечує передачу інформації на локальний сервер за допомогою Wi-Fi. На сервері здійснюється обробка даних та їх зберігання для подальшого аналізу та формування звітності.

Для візуалізації зібраної інформації використовується система Grafana, яка надає можливість у реальному часі контролювати показники температури та вологості, а також виявляти відхилення від встановлених норм.

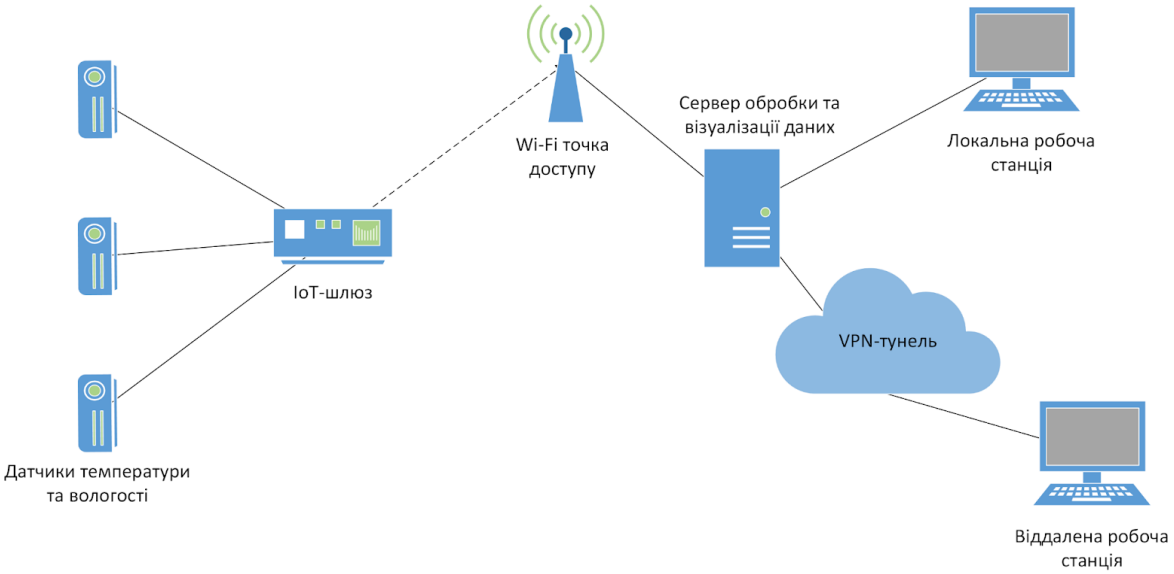

Рис. 2.1 Схема системи моніторингу температури і вологості повітря

Система відеоспостереження та контролю якості

Система відеоспостереження на підприємстві впроваджена для контролю якості виробничих процесів (рисунок 2.2), моніторингу території та забезпечення безпеки співробітників. Основними компонентами цієї системи є IP-камери Hikvision DS-2CD2347G1-LU з підтримкою PoE, що дозволяє спростити підключення та знизити витрати на прокладку кабелів. Камери встановлюються у виробничих зонах, офісних приміщеннях та на периметрі об’єкта.

Відеопотоки з камер надходять до мережевого відеореєстратора (NVR) Hikvision, який виступає в ролі IoT-шлюзу та забезпечує збір, обробку та зберігання даних. З’єднання між камерами та NVR здійснюється за протоколом RTSP, що дозволяє передавати відео у режимі реального часу. Зібрані дані передаються на сервер відеозапису, де вони зберігаються для подальшого аналізу та перегляду у разі виникнення інцидентів.

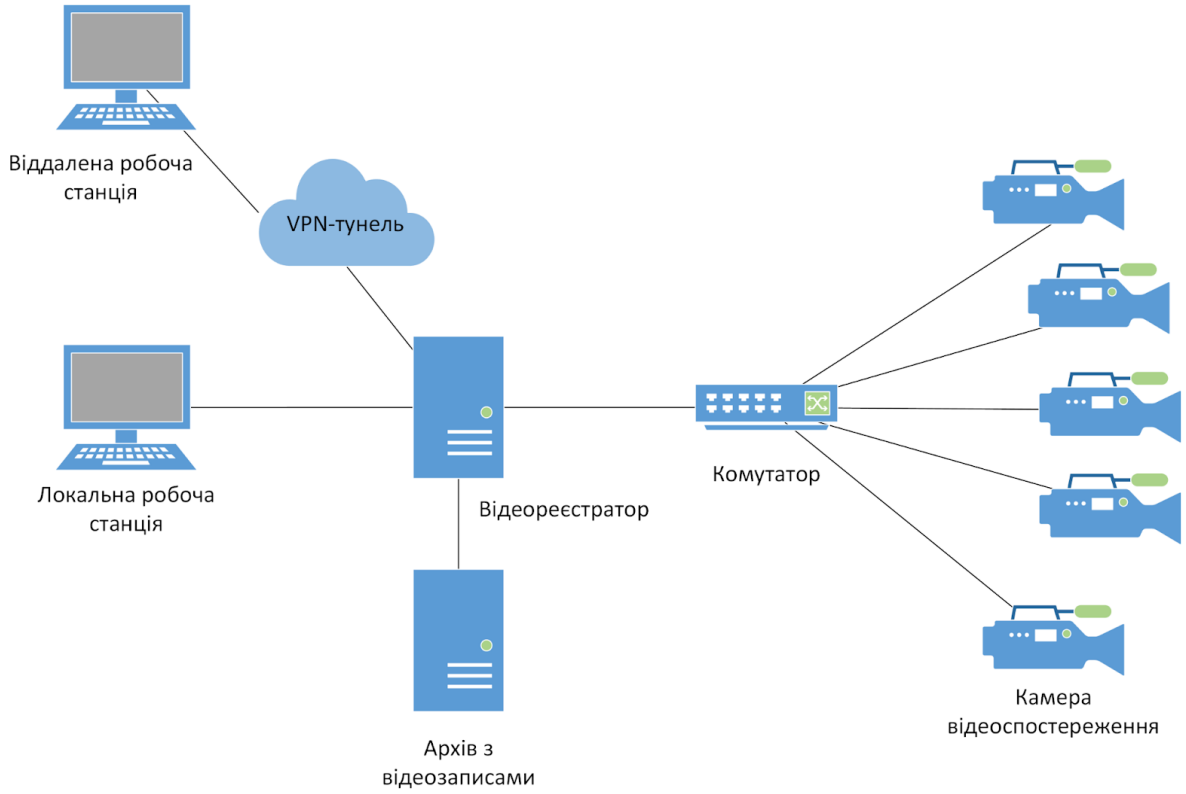

Рис 2.2 Схема системи відеоспостереження

Система контролю управління доступом

Система контролю управління доступом (рисунок 2.3) впроваджена на підприємстві для обмеження фізичного доступу до критичних зон, таких як окремі ділянки виробничого цеху, серверна кімната та офісні приміщення. Основними компонентами системи є контролери HID VertX V1000, що підтримують живлення через PoE, а також зчитувачі ключ-карток HID Edge EVO, які забезпечують ідентифікацію користувачів та фіксацію подій доступу.

Зібрані дані про доступ обробляються локальними контролерами СКУД, які виступають у ролі проміжних шлюзів і забезпечують передачу інформації до центрального шлюзу СКУД. Цей шлюз виконує функції збору, зберігання та обробки подій доступу, синхронізуючи їх із сервером СКУД, де здійснюється централізоване зберігання даних та формування звітів про дії користувачів.

Для з’єднання між замками, зчитувачами та контролерами використовується PoE Ethernet, що дозволяє передавати дані і одночасно здійснювати електроживлення. Передача даних від контролерів до центрального шлюзу здійснюється через

Ethernet. У разі відмови центрального шлюзу контролери автоматично переходять у автономний режим, зберігаючи події доступу локально. Після відновлення шлюзу усі накопичені дані синхронізуються із сервером, забезпечуючи збереження журналів доступу та відновлення цілісності інформації.

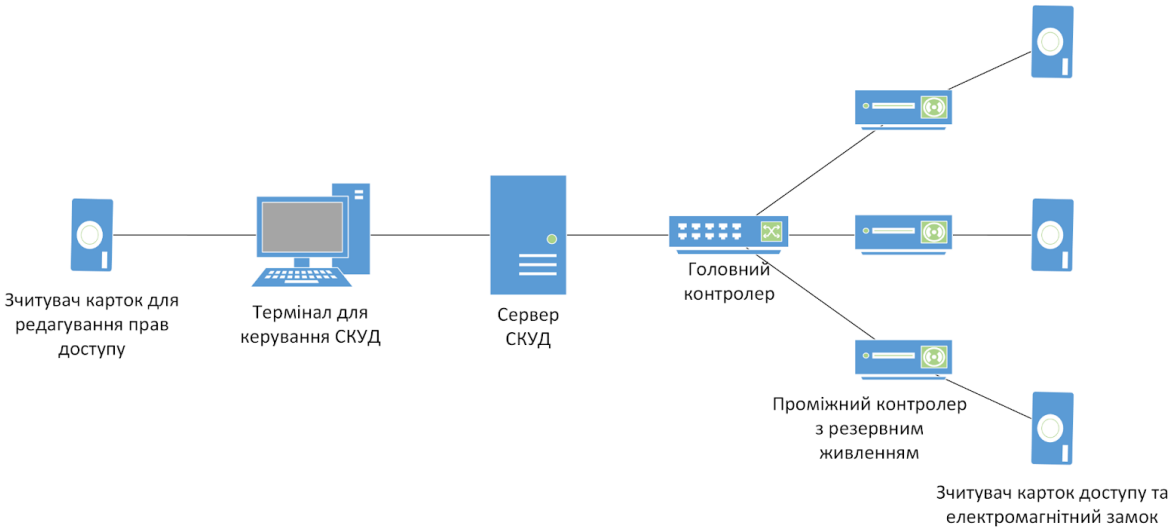

Рис. 2.3 Схема системи контролю управління доступом

Система повідомлень про помилки у технологічних процесах та обладнанні

У виробничій зоні підприємства реалізовано систему моніторингу помилок у технологічних процесах та обладнанні (рисунок 2.4), яка забезпечує контроль за стабільністю роботи критичних вузлів та своєчасне виявлення збоїв. Основними компонентами цієї системи є датчики помилок та несправностей (наприклад, AM2301 та DS18B20), які розміщуються на ключових етапах виробництва для збору інформації про відхилення у роботі обладнання. Зібрані дані з датчиків надходять до IoT-шлюзу на базі Raspberry Pi, який підключається до локального сервера через Ethernet. Шлюз виконує функції агрегації даних та їх попередньої обробки. Далі зібрана інформація передається на локальний сервер для зберігання та аналізу.

Для візуалізації даних використовується система Grafana, яка дозволяє відслідковувати у режимі реального часу показники роботи обладнання та виявляти

відхилення від нормальних значень. У разі виявлення аномалій система формує сповіщення для відповідальних співробітників, що дозволяє оперативно реагувати на можливі збої.

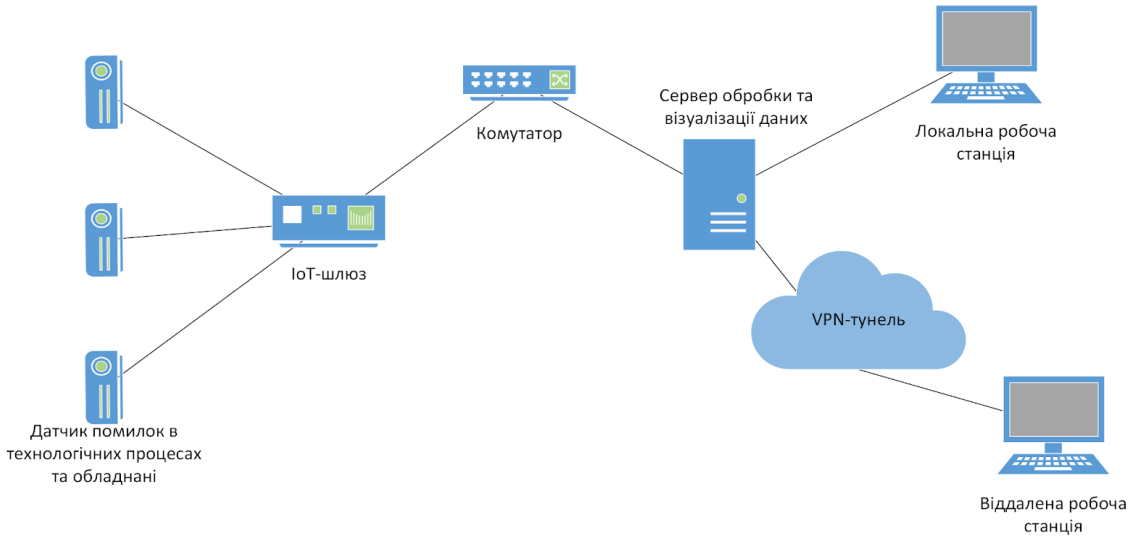

Рис. 2.4 Схема систем повідомлень про помилки у технологічних процесах та обладнанні

Система перевірки якості готової продукції

Система перевірки якості готової продукції (рисунок 2.5) впроваджена для контролю якості на фінальних етапах виробничого процесу. Основними компонентами системи є ручний датчик, який здатен визначати концентрацію певних речовин у готовій продукції, та планшет із Bluetooth-з'єднанням, що забезпечує зручний інтерфейс для перегляду та обробки зібраних даних.

Зібрані показники з датчика надходять на планшет через Bluetooth, що дозволяє оперативно отримувати дані без необхідності дротових підключень. Планшет виконує функції первинної обробки даних та їх передачі на локальний сервер через Wi-Fi, де інформація зберігається для подальшого аналізу та формування звітів.

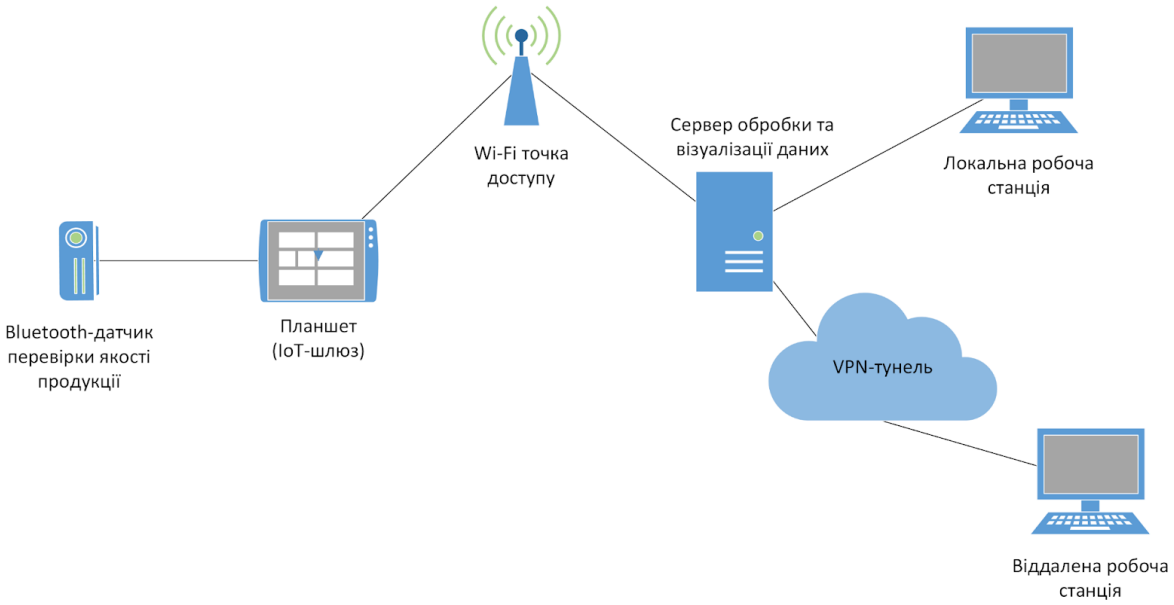

Рисунок 2.5 Система перевірки якості готової продукції

Віддалений доступ та аналітика

Віддалений доступ (рисунок 2.6) реалізований для забезпечення контролю та моніторингу IoT-систем підприємства з головного офісу через захищені канали зв'язку. Основними компонентами цієї системи є VPN-сервер, що забезпечує захищене з'єднання між виробничим середовищем та головним офісом, а також аналітична платформа Grafana та система відеоспостереження, які надають можливість оперативного доступу до даних у реальному часі. Оператор отримує доступ до аналітичних панелей Grafana та системи відеоспостереження, де він може переглядати поточні показники температури та вологості у виробничих зонах, дані про помилки в технологічних процесах та про вміст речовин у готовій продукції, відео з камер спостереження у реальному часі та архівні записи.

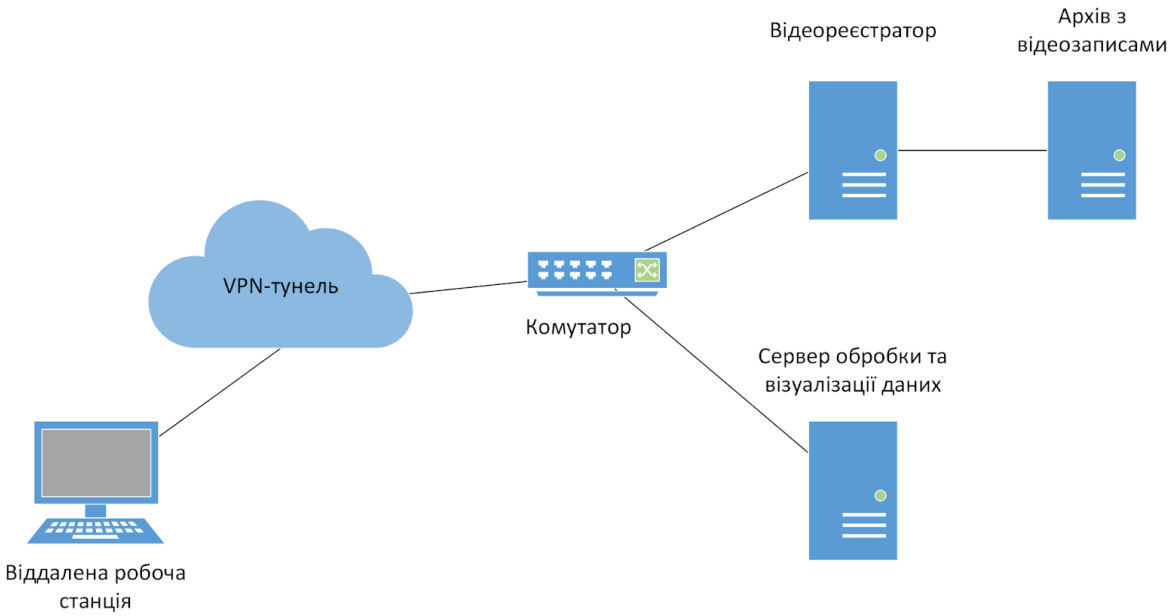

Рис. 2.6 Схема віддаленого доступу

2.2 Аналіз загроз в IoT-інфраструктурі підприємства

Аналіз загроз для IoT-систем підприємства має важливе значення для виявлення потенційних векторів атак та розробки заходів щодо їх попередження. На основі попередньо визначеної архітектури та компонентів системи можна виокремити наступні аспекти. Основною загрозою для всіх IoT-систем підприємства є інсайдерська загроза. Це пояснюється тим, що основний вектор атак спрямований на використання правомірного доступу для реалізації неправомірних дій. Водночас існують загрози несанкціонованого доступу до пристроїв з боку зовнішніх зловмисників, особливо через неналежно захищені канали зв'язку і пограничні шлюзи або фізичний доступ до пристроїв (Рис. 2.7).

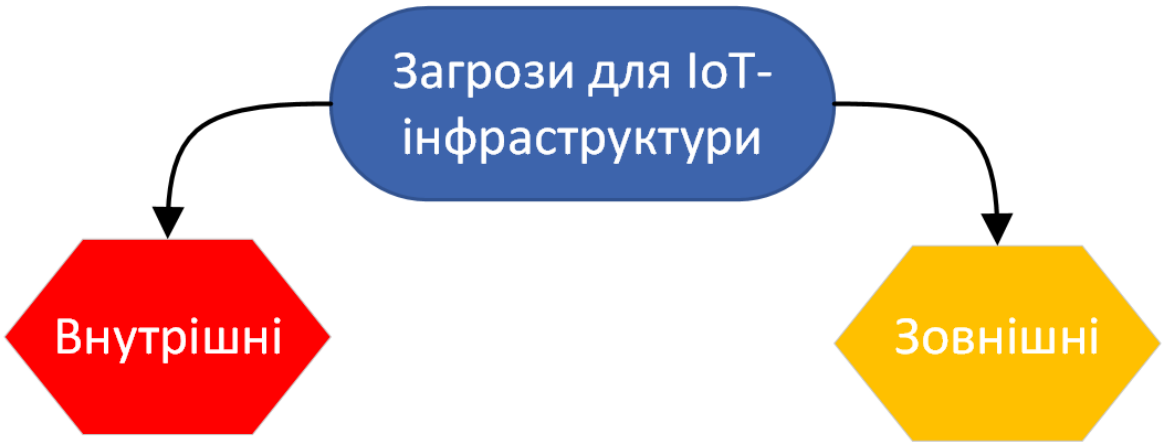

Рис. 2.7 Загрози для IoT-інфраструктури

Однією з основних загроз для всіх IoT-систем є перехоплення даних під час передачі через бездротові канали зв'язку. Вразливими є системи, що використовують Wi-Fi та Bluetooth, зокрема система моніторингу температури та вологості, система перевірки якості готової продукції та система повідомлень про помилки технічних процесів. Відсутність надійного шифрування на цих каналах дозволяє зловмисникам перехоплювати інформацію, змінювати її та підміняти справжні дані фальшивими, що може призвести до хибних реакцій на зміну параметрів середовища або до маніпуляцій з даними про якість продукції.

Ще однією значною загрозою є фізичний доступ до компонентів системи. Датчики температури та вологості, IP-камери системи відеоспостереження та ручні датчики для перевірки якості готової продукції можуть бути об'єктами фізичних атак. Зловмисники можуть пошкодити ці пристрої, змінити їхні налаштування або вимкнути їх, що призведе до втрати критичних даних або до фальсифікації показників. Наприклад, фізичний доступ до датчиків температури може дозволити фальсифікувати їх дані, щоб обійти контроль процесів виробництва, а пошкодження камер відеоспостереження може унеможливити реєстрацію інцидентів безпеки.

Компрометація шлюзів та контролерів також становить серйозну загрозу для інформаційної безпеки IoT-систем підприємства. Шлюзи, що використовуються для передачі даних від датчиків температури та вологості на сервер, можуть бути

перепрограмовані для зміни параметрів передачі даних або перенаправлення потоків на сторонні сервери. У випадку системи моніторингу технічних процесів атака на контролери може призвести до передачі фальшивих аварійних сигналів або до блокування сигналів про реальні несправності обладнання. Крім того, відсутність надійних механізмів автентифікації шлюзів збільшує ризик реалізації атак типу "людина посередині" (MitM), коли зловмисник може перехоплювати дані, що надходять до сервера, та змінювати їх на ходу.

Окремою загрозою є несанкціонований доступ до серверів зберігання даних. Якщо зловмисник отримає доступ до сервера відеозапису, він може видалити або підмінити архівні записи, що ускладнить розслідування інцидентів або дозволить приховати сліди несанкціонованих дій. Аналогічно, компрометація обробки і візуалізації даних може дозволити зловмиснику приховати аварійні події або створити фальшиві аварійні повідомлення для дезінформації операторів.

Зловживання правомірним доступом до IoT-систем також є критичним вектором атак. Компрометація облікових записів користувачів, що мають доступ до СКУД або до системи перевірки якості продукції, дозволить зловмиснику змінювати налаштування доступу, видаляти записи про переміщення співробітників або маніпулювати даними про якість готової продукції. У разі реалізації віддаленого доступу через VPN підвищується ризик використання викрадених облікових даних для отримання несанкціонованого доступу до критичних систем. Відсутність двофакторної автентифікації значно спрощує реалізацію таких атак.

2.3 Визначення вимог до безпеки та заходів захисту інформації в IoT-інфраструктурі підприємства

Для забезпечення ефективного захисту IoT-систем підприємства необхідно визначити конкретні цілі захисту для кожної категорії пристроїв, враховуючи їх функціональні особливості, канали передачі даних та потенційні загрози. Основним завданням є забезпечення конфіденційності, цілісності та доступності

даних під час їх передачі та зберігання, а також запобігання несанкціонованому доступу до компонентів системи.

Розробка цілей захисту для кожної категорії пристроїв

Для системи моніторингу температури та вологості важливо забезпечити захист даних від перехоплення під час передачі через бездротові канали зв'язку. Це досягається шляхом реалізації шифрування трафіку, що передається через Wi-Fi та Ethernet. Додатково передбачається використання окремого VLAN та прихованої мережі Wi-Fi в якості сегментації мережі, до якої підключаються шлюзи, що ускладнює її виявлення потенційними зловмисниками та зменшує ймовірність несанкціонованих підключень. Контроль доступу до мережі буде здійснюватися шляхом фільтрації MAC-адрес, дозволяючи доступ тільки визначеним пристроям. Оскільки фізичний доступ до таких датчиків може використовуватися для їх перепрограмування або пошкодження, доцільно реалізувати заходи контролю доступу до пристроїв, зокрема встановлення захисних кожухів.

Таблиця 1.1

Заходи захисту інформації для системи моніторингу температури та вологості

Ціль захисту	**Заходи реалізації**
Захистити дані від перехоплення або підміни при передачі по бездротових каналах	Використання сучасних методів шифрування
Уникнути підключення сторонніх пристроїв до мережі IoT	Сегментування мережі (окрема VLAN) Використання закритої прихованої Wi-Fi мережі Фільтрація MAC-адрес
Недопущення несанкціонованого доступу, пошкодження або маніпуляції з пристроями	Встановлення захисних кожухів Обмеження фізичного доступу

Система відеоспостереження є одним із критичних компонентів, що потребує особливої уваги з погляду захисту конфіденційності та цілісності даних. Відеопотоки, що передаються між камерами, реєстратором та сервером архіву відеозаписів, повинні бути зашифровані для запобігання їх несанкціонованому перехопленню або зміні. Крім того, для захисту від атак на сервер зберігання відеозаписів необхідно забезпечити автентифікацію користувачів, що мають доступ до системи, із впровадженням двофакторної автентифікації, що дозволить мінімізувати ризик використання викрадених облікових даних. Також передбачаються заходи з сегментації мережі, а саме використання окремого VLAN для системи. Окрему увагу слід приділити моніторингу доступу до камер та серверів з метою виявлення спроб несанкціонованого підключення або зміни налаштувань.

Таблиця 1.2

Заходи захисту інформації для системи відеоспостереження

Опис	**Заходи реалізації**
Недопущення перехоплення або перегляду відеопотоків сторонніми особами	Шифрування відеопотоків між камерами, реєстратором і сервером
Виключення можливості доступу до системи неавторизованих осіб	Запровадження автентифікації користувачів з двофакторним підтвердженням
Уникнути підключення сторонніх пристроїв до мережі IoT	Сегментування мережі (окрема VLAN)
Недопущення несанкціонованого доступу, пошкодження або маніпуляції з пристроями	Встановлення захисних кожухів Обмеження фізичного доступу

У системі контролю управління доступом основним заходом захисту є DMZ, що утворена повною ізоляцією системи на фізичному рівні, що унеможливлює доступ до неї з віддалених офісів чи зовнішніх мереж. Це рішення знижує ризик несанкціонованого доступу до критичних компонентів СКУД, залишаючи можливість управління лише з локальної мережі підприємства. Основні заходи захисту зосереджені на запобіганні компрометації зчитувачів контролерів та сервера управління доступом. Це досягається шляхом шифрування даних, що передаються між зчитувачами, контролерами та сервером СКУД, що дозволяє унеможливити перехоплення сигналів та їх підміну. Водночас, для підвищення рівня безпеки доступу до системи запроваджується двофакторна автентифікація для адміністраторів та осіб, відповідальних за управління доступом. Такий підхід зменшує ризик компрометації облікових записів, особливо у випадках використання викрадених паролів.

З метою запобігання несанкціонованому втручанню в роботу контролерів, необхідно забезпечити контроль фізичного доступу до цих компонентів. Додатково, передбачається реалізація резервного копіювання даних про переміщення осіб та події в системі контролю доступу. Це дозволить зберегти критичні журнали подій у разі збою основного сервера або втрати даних через кібератаку.

Таблиця 1.3

Заходи захисту інформації для системи контролю управління доступом

Опис	**Заходи реалізації**
Унеможливлення втручання ззовні через мережу	Фізична ізоляція СКУД від зовнішніх мереж та інтернету

Недопущення маніпуляцій з переданими даними	Шифрування сигналів між зчитувачами, проміжними та головним контролерами та сервером
Мінімізація ризику несанкціонованого входу з викраденими обліковими даними	Запровадження двофакторної автентифікації для адміністраторів
Запобігання фізичному втручанню у роботу контролерів і серверів	Обмеження фізичного доступу до контролерів і серверів
Гарантія доступності журналів подій та логів у разі аварій чи атак	Регулярне резервне копіювання даних СКУД

Система повідомлень про технічні помилки та стан обладнання також вимагає реалізації заходів захисту для запобігання маніпуляціям із переданими даними. Зокрема, для забезпечення достовірності повідомлень про аварійні ситуації буде реалізоване шифрування даних між контролерами та сервером моніторингу, що дозволить унеможливити перехоплення та модифікацію інформації під час передачі. Для запобігання несанкціонованому доступу до сервера моніторингу передбачається реалізація чітких заходів контролю доступу. Це включає використання окремого VLAN в рамках сегментації мережі та обмеження доступу до серверу лише для авторизованих осіб. Додатково, для захисту облікових записів адміністраторів планується використання двофакторної автентифікації, що дозволить знизити ризик компрометації облікових даних.

Таблиця 1.4

Заходи захисту інформації для системи повідомлень про технічні помилки та стан обладнання

Опис	**Заходи реалізації**

Унеможливлення підміни або модифікації даних про технічний стан	Шифрування трафіку між контролерами та сервером обробки даних
Запобігання несанкціонованому втручанню в роботу системи	Сегментація мережі (окремий VLAN) Доступ до серверу лише для авторизованих користувачів
Недопущення компрометації облікових даних, що дають доступ до критичних функцій	Запровадження двофакторної автентифікації

Для системи перевірки якості готової продукції, яка використовує Bluetooth-датчики, основним завданням є забезпечення конфіденційності та достовірності результатів перевірки якості. Це досягається шляхом шифрування переданих даних для унеможливлення їх підміни або перехоплення. З метою зниження ризику несанкціонованого доступу до мережі передачі даних планується використання прихованого Wi-Fi. Це рішення дозволить обмежити можливість виявлення мережі сторонніми особами та мінімізувати ризик атак на канали передачі даних. Крім того, контроль фізичного доступу до планшетів та використання двофакторної автентифікації дозволить знизити ризик їх пошкодження або несанкціонованого використання.

Таблиця 1.5

Заходи захисту інформації для системи перевірки якості готової продукції

Опис	**Заходи реалізації**
Унеможливлення підміни чи перехоплення результатів перевірки якості	Шифрування даних, що передаються через Bluetooth Шифрування трафіку між планшетом та сервером обробки даних

Мінімізація ризику несанкціонованого підключення до Wi-Fi та мережі вцілому	Використання прихованої Wi-Fi мережі для обміну даними Сегментування мережі (окрема VLAN)
Запобігання несанкціонованому використанню або пошкодженню пристроїв перевірки	Контроль фізичного доступу до планшетів Фізичне зберігання обладнання в контрольованій зоні
Зниження ризику компрометації адміністраторських або службових облікових записів	Впровадження двофакторної автентифікації на планшетах

Окремим аспектом захисту IoT-систем є забезпечення безпечного віддаленого доступу до пристроїв та серверів. Зважаючи на необхідність віддаленого моніторингу та управління компонентами системи, необхідно впровадити двофакторну автентифікацію для доступу до віддалених ресурсів. Це дозволить мінімізувати ризик використання компрометованих облікових даних для отримання несанкціонованого доступу до IoT-систем. Додатково, доцільно забезпечити шифрування трафіку віддаленого доступу через VPN з використанням сучасних криптографічних алгоритмів, а також застосувати механізми обмеження доступу за IP-адресами та зовнішніми портами для запобігання атакам з непередбачених локацій.

Таблиця 1.6

Заходи захисту інформації для віддаленого доступу

Опис	**Заходи реалізації**
Запобігання несанкціонованому доступу внаслідок викрадення логінів/паролів	Впровадження двофакторної автентифікації для доступу до віддалених ресурсів

Забезпечення конфіденційності та цілісності даних при віддаленому підключенні	Шифрування всього трафіку за допомогою VPN Використання сучасних криптографічних алгоритмів
Мінімізація ризику зовнішніх атак на віддалений інтерфейс доступу	Фільтрація за IP-адресами Обмеження відкритих портів

Також для забезпечення комплексного захисту необхідно визначити організаційні заходи, спрямовані на мінімізацію ризиків компрометації пристроїв та даних. Для цього буде запроваджено низку політик інформаційної безпеки і систематичне навчання персоналу. Впровадження парольної політики для IoT-систем має запобігти використанню стандартних паролів та встановити вимоги до їх складності, що знизить ризик несанкціонованого доступу, особливо це стосується всіх IoT-шлюзів. Політика доступу повинна розмежовувати права користувачів залежно від їхніх завдань, забезпечуючи автентифікацію для дій із критичними системами, такими як СКУД та архіви відеоспостереження. Навчання персоналу спрямоване на підвищення обізнаності щодо захисту IoT-пристроїв та реагування на потенційні загрози.

Таблиця 1.7

Організаційні заходи захисту IoT-інфраструктури

Опис	**Організаційні заходи реалізації**
Мінімізація ризику несанкціонованого доступу через скомпрометовані облікові записи або стандартні паролі	Впровадження парольної політики
Розмежування прав доступу до систем на основі ролей та повноважень користувачів	Політика розмежування прав доступу

Запобігання компрометації системи через людський фактор	Проведення регулярного навчання персоналу Ознайомлення працівників із внутрішніми вимогами та політиками ІБ

Обґрунтування доцільності впровадження обраних та додаткових заходів захисту інформації в IoT-інфраструктурі підприємства

При розробці системи захисту IoT-систем підприємства також було розглянуто кілька додаткових рішень, впровадження яких могло б суттєво підвищити загальний рівень безпеки інфраструктури. Однак, через високі фінансові витрати та організаційні обмеження, їх реалізація на даному етапі визнана недоцільною.

Одним із таких рішень є система управління подіями інформаційної безпеки. SIEM забезпечує централізований збір, аналіз та кореляцію даних з усіх компонентів IoT-системи, включаючи шлюзи, контролери, сервери відеоспостереження та систему контролю доступу. Це дозволяє виявляти аномальні активності, потенційні атаки та інші інциденти безпеки в режимі реального часу. Впровадження SIEM значно підвищило б рівень контролю за подіями в мережі та забезпечило б швидке реагування на загрози. Водночас, це рішення потребує розгортання власного SOC або залучення сторонніх провайдерів послуг моніторингу. Такий підхід є фінансово затратним та вимагає наявності висококваліфікованого персоналу для аналізу інцидентів, що на поточному етапі не відповідає можливостям підприємства.

Іншим рішенням, впровадження якого було розглянуто, є інтеграція систем виявлення та запобігання вторгненням. Вони дозволяють контролювати мережевий трафік у реальному часі, виявляти атаки на IoT-пристрої та блокувати шкідливу активність. Оскільки IoT-система підприємства має розгалужену структуру з великою кількістю кінцевих точок, IDS/IPS здатні виявляти такі загрози, як спроби експлуатації вразливостей пристроїв або передачу несанкціонованих команд через мережу. Втім, розгортання IDS/IPS потребує потужної інфраструктури для аналізу

великого обсягу даних, а також кваліфікованих фахівців для налаштування правил та моніторингу інцидентів. Враховуючи поточні ресурси підприємства, реалізація IDS/IPS не є пріоритетною, проте таке рішення може бути розглянуто на наступних етапах розвитку системи захисту.

Система контролю доступу до мережі дозволяє ідентифікувати та контролювати всі пристрої, що підключаються до мережі, а також забезпечує дотримання політик безпеки на рівні кінцевих точок. У випадку IoT-інфраструктури, NAC може бути використана для автоматичної перевірки прошивок пристроїв, контролю версій програмного забезпечення та блокування підключень небезпечних пристроїв. Крім того, NAC може інтегруватися з SIEM для отримання детальної інформації про активність підключених IoT-пристроїв. Однак, враховуючи значну кількість різнорідних IoT-пристроїв та обмеженість їхніх апаратних ресурсів, реалізація NAC є складним завданням, яке потребує додаткових витрат на мережеве обладнання та спеціалізоване програмне забезпечення. Таким чином, впровадження NAC на поточному етапі є малоефективним, проте може бути реалізоване у майбутньому разом з модернізацією мережевої інфраструктури.

Централізована система управління прошивками (Firmware Management System) дозволяє своєчасно оновлювати програмне забезпечення IoT-пристроїв та забезпечувати їх відповідність актуальним вимогам безпеки. Враховуючи різнорідність використовуваних пристроїв (ESP32, Hikvision, HID Edge), інтеграція такої системи дозволила б автоматизувати процес оновлення, контролювати версії прошивок та оперативно реагувати на виявлені вразливості. Однак, розгортання такої системи потребує значних інвестицій у розробку індивідуальних модулів для кожного типу пристроїв, а також у створення централізованої бази даних оновлень. На даний момент, оновлення прошивок виконується вручну відповідальними адміністраторами, що зменшує ймовірність випадкової компрометації системи. Впровадження системи управління прошивками може бути розглянуто у довгостроковій перспективі як складова загальної стратегії кіберзахисту.

У таблиці 1.8 порівняно вартість впровадження, вартість щомісячної підтримки та вимоги до людських ресурсів в описаних засобах та заходах захисту інформації.

Таблиця 1.8

Порівняльна таблиця впроваджених та додаткових рішень з точки зору економічної доцільності

Засіб / Захід захисту	**Вартість впровадження (разово)**	**Щомісячна підтримка / ліцензія**	**Людські ресурси / супровід**
Шифрування трафіку IoT	$500–1000	$0–100	IT/ІБ-спеціаліст
Приховані Wi-Fi / VLAN-сегментація	$0-700	—	Мережевий адміністратор
Двофакторна автентифікація (2FA)	$300–1000	$0–300	IT/ІБ-спеціаліст
Контроль фізичного доступу до IoT	$500–1500	—	Охорона / технічне обслуговування обладнання
Навчання персоналу	—	—	Керівник IT/ІБ
Парольна політика / Політика розмежування прав і доступу	—	—	Керівник IT/ІБ
SIEM (аутсорсинг)	$5000–10000	$500–1500	Зовнішній SOC
IDS/IPS (мережева інфраструктура)	$1500–3000	$100–300	Аутсорсинг - впровадження та налаштування / IT/ІБ-спеціаліст - підтримка

NAC (контроль доступу до мережі)	$2000–5000	$300–700	Аутсорсинг - впровадження та налаштування / IT/ІБ-спеціаліст - підтримка
Централізована система управління IoT	$3000–6000	$300–1000	IT/ІБ-спеціаліст

**вартість вказана в доларах США*

***вартість розрахована з урахуванням поточної ситуації на ринку надання послуг з кібербезпеки*

Можна зробити висновок, що вибір поточних заходів захисту обумовлено оптимальним співвідношенням між витратами та потенційними ризиками для системи. Впровадження SIEM, IDS/IPS, NAC та централізованої системи управління прошивками є ефективними з точки зору безпеки, проте вимагає значних ресурсів на етапах розробки, впровадження та підтримки. З огляду на обмежений бюджет було прийнято рішення зосередитись на менш ресурсозатратних методах захисту, таких як моніторинг критичних компонентів, контроль доступу та резервування даних, що дозволяє підтримувати базовий рівень безпеки без додаткових витрат на складні системи моніторингу та аналізу інцидентів.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ІОТ-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

3.1 Реалізація технічних засобів захисту IoT-інфраструктури підприємства

Реалізація технічних засобів спрямована на забезпечення цілісності, конфіденційності та доступності даних, що циркулюють між IoT-пристроями, шлюзами, серверами та користувацькими станціями. До таких заходів віднесено шифрування переданих даних, мережеву сегментацію, автентифікацію доступу та налаштування міжмережевих екранів.

Система моніторингу температури та вологості

Основним завданням захисту системи моніторингу та вологості є забезпечення конфіденційності даних, їх цілісності та запобігання несанкціонованим змінам конфігурації обладнання. Для досягнення зазначених цілей було реалізовано низку технічних заходів захисту.

Першим етапом стало впровадження механізму шифрування даних. На сервері зберігання даних використовується SSL/TLS 1.3 для створення захищеного каналу передачі інформації між шлюзами та сервером. Для цього було розгорнуто внутрішній центр сертифікації, що ґрунтується на OpenSSL з використанням 4096-бітних ключів RSA.

Наступним кроком стала логічна сегментація мережі, спрямована на зниження ризику несанкціонованого доступу та перехоплення даних. Шлюзи ESP32 підключено до окремої прихованої Wi-Fi мережі з обмеженим діапазоном дії, створеної на базі маршрутизатора MikroTik hAP ax2. Цей маршрутизатор підтримує WPA3-Enterprise, що дозволяє забезпечити високий рівень шифрування даних. Крім того, для передачі даних від шлюзу до серверу обробки даних використовується окермий VLAN. Контроль доступу до мережі здійснюється шляхом фільтрації MAC-адрес за допомогою Firewall MikroTik, що обмежує

підключення лише дозволених пристроїв та знижує ймовірність несанкціонованого підключення до мережі [19, 20].

Для захисту від фізичного доступу до обладнання були вжиті додаткові заходи безпеки. Датчики DHT22 та SHT31 розміщено у герметичних корпусах з вбудованими пломбами на основі Tamper-Evident Tape, що дозволяє своєчасно виявити спроби несанкціонованого доступу до пристроїв. Крім того, шлюзи ESP32 встановлені у спеціалізованих монтажних шафах Rittal TS IT, обладнаних механічними замками, що додатково захищає обладнання від фізичного втручання.

Система відеоспостереження та контролю якості

Основним завданням захисту системи відеоспостереження є захист відеопотоків, архівів даних та серверів зберігання інформації є критично важливим завданням, яке реалізується шляхом впровадження комплексу технічних заходів.

Одним із ключових напрямів захисту є шифрування даних. Для захисту відеопотоків, що передаються між камерами Hikvision та NVR, впроваджено алгоритм AES-256 із використанням TLS 1.2. Сертифікати для реалізації TLS генеруються внутрішнім центром сертифікації, створеним на базі OpenSSL. Центр сертифікації використовує RSA-2048 для генерації ключів. Додатково, TLS 1.2 застосовується для передачі даних між NVR та сервером архіву відеозаписів, що гарантує цілісність та конфіденційність інформації навіть у випадку компрометації окремих мережевих сегментів [21].

Автентифікація користувачів є наступним важливим елементом системи захисту. Для всіх користувачів, які мають доступ до системи відеоспостереження, впроваджено двофакторну автентифікацію. Реалізація 2FA здійснюється через генерацію OTP у додатку Google Authenticator на мобільному телефоні адміністратора або іншої уповноваженої особи.

Для запобігання несанкціонованому доступу до камер та серверів системи відеоспостереження впроваджено логічну сегментацію мережі. Вся система працює в окремому VLAN’і, доступ до якого можливий лише з певних мережевих сегментів.

Фізичний захист компонентів системи відеоспостереження реалізовано за допомогою спеціалізованого обладнання та організаційних заходів. NVR та сервер архіву розміщені у серверному приміщенні, доступ до якого обмежено. Камери встановлені у захисних кожухах, що відповідають стандартам IP66 та IK10, що гарантує захист обладнання від вандалізму та несприятливих погодних умов. Доступ до серверного приміщення регламентовано відповідно до політики контролю фізичного доступу.

Система контролю управління доступом

Основним принципом побудови системи є фізична ізоляція мережевих компонентів СКУД від загальної мережі підприємства та зовнішніх підключень. Такий підхід дозволяє запобігти можливим спробам віддаленого втручання у роботу контролерів та серверів управління доступом, обмежуючи доступ виключно локальною мережею підприємства.

Одним із ключових заходів захисту є шифрування даних, що передаються між контролерами та сервером управління доступом. Для цього впроваджено алгоритм AES-256 у поєднанні з TLS 1.3. Використовуються сертифікати, згенеровані внутрішнім центром сертифікації на базі OpenSSL із RSA-2048. Таке рішення дозволяє захистити канали передачі даних від перехоплення та модифікації, що є особливо актуальним у контексті забезпечення цілісності інформації про доступ до об’єктів. Додатково, у випадку передачі даних між контролерами та зчитувачами карт застосовується симетричне шифрування AES-128, що знижує навантаження на обладнання без втрати рівня безпеки.

З метою підвищення рівня захисту доступу до системи контролю доступу для адміністраторів та осіб, відповідальних за управління доступом, запроваджено двофакторну автентифікацію. Реалізація 2FA здійснюється шляхом поєднання пароля та одноразового пароля, що генерується через мобільний додаток Google Authenticator.

Фізичний захист компонентів СКУД забезпечується за допомогою встановлення контролерів у спеціалізованій монтажній шафі Rittal AE, яка обладнана

електронним замком та сенсорам відкриття дверей. Датчики відкриття підключені до центрального пульту охорони і подають сигнал при відкритті дверей.
Для забезпечення захисту даних про переміщення осіб реалізовано резервне копіювання журналів подій. Резервні копії створюються за графіком кожні 24 години та зберігаються на окремому зашифрованому диску, до якого мають доступ тільки визначені особи.

Система повідомлень про помилки у технологічних процесах та обладнанні

Основним завданням захисту системи повідомлень про технічні помилки та стан обладнання є забезпечення цілісності і достовірності інформації, що надходить до серверу, запобігання маніпуляціям із даними та несанкціонованому доступу до критичних повідомлень.

Передача даних між контролерами та сервером моніторингу здійснюється через зашифровані канали зв’язку, що базуються на використанні AES-128 у поєднанні з TLS 1.3. Для реалізації TLS 1.3, як вже вказувалось раніше, використовується внутрішній центр сертифікації, який видає сертифікати з 2048-бітними RSA-ключами. Для адміністраторів серверу моніторингу впроваджено двофакторну автентифікацію , що ґрунтується на OTP, які генеруються за допомогою мобільного додатка Google Authenticator. В рамках сегментації мережі система розташована у окремому VLAN`і, що реалізовано можливостями коммутатора Cisco.

Система перевірки якості готової продукції

Основним завданням захисту системи перевірки якості готової продукції є забезпечення цілісності та конфіденційності даних, що збираються Bluetooth-датчиками та передаються на віповідний сервер.

Першим рівнем захисту є шифрування даних на етапі передачі інформації від Bluetooth-датчиків до планшетів. Для забезпечення конфіденційності даних підчас передачі з датчика до планшета використовується шифрування за алгоритмом AES-128. Другим рівнем захисту є передача даних від планшетів до маршрутизатора

через захищену Wi-Fi мережу. Вибір прихованої Wi-Fi мережі із застосуванням WPA3-Enterprise забезпечує високий рівень безпеки передачі даних. WPA3-Enterprise використовує шифрування AES-256 та передбачає обов'язкову автентифікацію пристроїв перед підключенням. Це дозволяє обмежити доступ до мережі лише авторизованими планшетами та мінімізувати ризик атак на канал передачі даних. В рамках сегментації мережі впроваджується окрема VLAN, що дозволить ізолювати потоки даних системи перевірки якості від інших сегментів мережі, зменшуючи ризик перехоплення даних та запобігаючи можливим атакам з інших сегментів.

Також не менш важливим є запровадження двофакторної автентифікації та контроль доступу перед використанням пристроїв, що ґрунтується на OTP, які генеруються за допомогою мобільного додатка Google Authenticator та ведення журналу використання датчиків.

Віддалений доступ та аналітика

Основним завданням захисту системи віддаленого доступу до систем відеоспостереження та моніторингу Grafana є мінімізація ризиків перехоплення трафіку, несанкціонованого доступу та компрометації даних.

Основою захисту є впровадження VPN на базі OpenVPN. OpenVPN обрано через його високу гнучкість, підтримку шифрування AES-256 та можливість використання сертифікатів для автентифікації користувачів. Для шифрування трафіку між клієнтом і сервером використовується алгоритм AES-256 у режимі GCM, який забезпечує не лише шифрування, але й вбудовану перевірку цілісності даних [22].

На рівні автентифікації використовується TLS 1.3 з підтримкою сертифікатів X.509, що видаються внутрішнім центром сертифікації підприємства на базі OpenSSL. Сертифікати генеруються для кожного користувача VPN, що дозволяє відслідковувати активність конкретних облікових записів.

Для посилення захисту реалізовано двофакторну автентифікацію на основі OTP, що генерується за допомогою мобільних додатків Google Authenticator. Для

обмеження доступу за IP-адресами та зовнішніми портами застосовується фаєрвол на основі iptables, який дозволяє доступ до VPN лише з певних IP-адрес, що належать до мережі підприємства або зареєстрованих адміністративних пристроїв і обмежує доступ до всіх портів, крім тих, що використовуються сервісами моніторингу та відеоспостереження.

Сегментація мережі реалізована через налаштування VLAN на рівні маршрутизаторів Cisco, що дозволяє ізолювати потоки даних віддалених підключень у спеціальний сегмент, окремий від основних IoT-систем підприємства. Це унеможливлює прямий доступ до критичних ресурсів без проходження етапу ідентифікації та перевірки прав доступу.

Для запобігання компрометації облікових записів у разі крадіжки пристрою або неактивності користувача, реалізовано автоматичне розірвання VPN-з'єднання після 10 хвилин бездіяльності. Додатково передбачено автоматичне блокування облікового запису після п'яти невдалих спроб входу, з можливістю розблокувати тільки звернувшись до адміністратора безпеки.

3.2 Реалізація організаційних заходів захисту IoT-інфраструктури підприємства

Водночас ефективність системи кіберзахисту неможливо забезпечити без впровадження організаційних політик, що регламентують порядок використання паролів в IoT- системах, розмежування прав доступу, а також навчання персоналу. Сукупність технічних рішень та організаційних процедур дозволила створити цілісну багаторівневу систему безпеки, здатну адаптуватись до сучасних загроз та оперативно реагувати на потенційні інциденти.

Політика управління паролями передбачає використання складних паролів для всіх шлюзів IoT, які мають довжину не менше 12 символів та містять великі й малі літери, цифри й спеціальні символи. Усі стандартні паролі постачальників були змінені при першому налаштуванні на унікальні облікові дані для кожного пристрою. Для адміністративних облікових записів СКУД, системи

відеоспостереження та систем моніторингу встановлено вимогу до складності паролів — мінімум 14 символів, для звичайних - 12. Вимога про вміст паролів (великі і малі літери, цифри і спеціальні символи) розповсюджується і тут. Також адміністративні облікові записи підлягають обов'язковому оновленню паролів кожні 90 днів. На пристроях встановлено захист від підбору паролів: обліковий запис блокується після п'яти невдалих спроб входу з можливістю бути розблокованим тільки керівником відділу ІТ/ІБ.

Політика управління доступом до IoT-систем забезпечує обмеження доступу до критичних компонентів виключно через локальну мережу підприємства. Адміністратори і оператори СКУД, системи відеоспостереження та системи моніторингу проходять автентифікацію з використанням 2FA через мобільний додаток Google Authenticator. Доступ до сервера обробки даних, сервера СКУД, відеореєстратора та архіву відеоспостереження, дозволений лише з робочих станцій із попередньо визначеними статичними IP-адресами та після проходження 2FA. Для архіву відеозаписів та системи моніторингу передбачено розмежування прав доступу: оператори можуть лише переглядати записи і показники, тоді як адміністратори мають повний доступ із можливістю видалення та експорту даних, редагування візуалізацій і т.д.

Процедура навчання та підвищення обізнаності персоналу передбачає вступне та позапланове навчання для співробітників які так чи інакше взаємодіють з IoT-інфраструктурою підприємства:

з актуальних загроз та методів захисту IoT-систем, що використовуються на підприємстві;

ознайомлення з політиками ІБ підприємства;

відповідальності за вчинення або ігнорування неправомірних дій;

Також щороку проводиться тестування персоналу щодо знання та розуміння вищеперелічених тем.

3.3 Загальні рекомендації щодо подальшого розвитку системи кіберзахисту підприємства

З метою підвищення ефективності функціонування всієї системи кібербезпеки підприємства, зокрема в частині захисту IoT-інфраструктури, доцільно розглянути впровадження додаткових технологічних і організаційних заходів. Ці заходи можуть бути реалізовані у перспективі — за умови розширення фінансових можливостей підприємства — і сприятимуть значному зміцненню здатності системи протистояти сучасним кіберзагрозам.

Одним із ключових напрямів розвитку є впровадження SIEM-системи Wazuh з інтеграцією Elastic Search, що дозволить централізовано збирати, обробляти та аналізувати події з усіх компонентів інформаційної інфраструктури, включаючи IoT-шлюзи, сервери, мережеві відеореєстратори та контролери систем контролю доступу. Wazuh забезпечує виявлення аномальної активності завдяки механізмам кореляції подій, а Elastic Search дозволяє ефективно працювати з великими обсягами даних. Візуалізація подій у Kibana та автоматичні сповіщення через Telegram-бот або інші інструменти дозволяють оперативно реагувати на інциденти безпеки [23].

Для впровадження Wazuh необхідно встановити окремий сервер з високою продуктивністю, розгорнути агентів збору логів на критичних елементах системи, налаштувати кореляційні правила виявлення загроз, а також автоматичні сповіщення про критичні події — наприклад, зміну конфігурацій, відключення пристроїв чи неуспішні спроби авторизації. Це дозволить підвищити рівень ситуаційної обізнаності IT-фахівців і забезпечити централізований контроль усіх подій безпеки.

Другим перспективним напрямом є впровадження системи виявлення та запобігання вторгненням Suricata, яка дозволяє аналізувати мережевий трафік у реальному часі, включаючи специфічні для IoT протоколи, такі як MQTT, CoAP, HTTP тощо. Suricata здатна виявляти широкий спектр атак — від DDoS до MitM — та інтегрується з SIEM-системами для комплексного аналізу подій.

Реалізація Suricata потребує окремого вузла з доступом до сегментів IoT-мережі, налаштування відповідних правил виявлення загроз (зокрема, бази

Emerging Threats), інтеграції з Wazuh і автоматизації реагування на атаки. Очікуваним результатом стане суттєве підвищення здатності підприємства виявляти та локалізовувати мережеві загрози до того, як вони спричинять шкоду.

Окрім технічних рішень, важливою складовою розвитку системи кіберзахисту є впровадження політики регулярного аналізу загроз, з урахуванням специфіки IoT-систем. На основі зібраних даних із Wazuh і Suricata варто періодично формувати аналітичні звіти щодо поточних загроз, тенденцій атак і вразливостей. Водночас доцільно розробити чітку процедуру реагування на інциденти, яка включатиме послідовність дій для ключових типів загроз — зокрема DDoS-атак, несанкціонованого доступу, компрометації пристроїв тощо [24].

У перспективі, за умови достатнього фінансування, впровадження наведених рішень дозволить суттєво підвищити рівень зрілості всієї системи кіберзахисту підприємства, забезпечивши її стійкість до сучасних загроз і адаптивність до нових викликів в сфері інформаційної безпеки.

ВИСНОВКИ

У роботі проведено дослідження проблеми забезпечення захисту інформації в IoT-системах виробничого підприємства. Визначено мету, завдання та обґрунтовано актуальність теми у зв'язку зі зростанням кількості IoT-пристроїв, збільшенням обсягів оброблюваних даних та наявністю специфічних вразливостей, притаманних Інтернету речей. Особливу увагу приділено складності захисту IoT-систем в умовах обмежених ресурсів пристроїв, широкого спектру загроз та високих вимог до доступності й надійності функціонування систем.

Проведено аналіз сучасного стану проблеми, існуючих підходів до захисту IoT та нормативно-правових документів. Здійснено моделювання типових загроз для об'єкта дослідження, ідентифіковано ключові вразливості, включаючи незашифровані канали зв'язку, слабкі паролі та низький рівень контролю фізичного доступу. Сформульовано вимоги до майбутньої системи захисту інформації на основі комплексного підходу, що поєднує технічні та організаційні заходи.

У практичній частині розроблено та реалізовано модель захисту для кожної з основних IoT-систем підприємства: системи відеоспостереження, СКУД, моніторингу технічного стану, температури та контролю якості продукції. Для кожної системи визначено цілі захисту, підібрано відповідні засоби безпеки (шифрування, двофакторна автентифікація, ізоляція сегментів тощо) та обґрунтовано вибір рішень з точки зору їх ефективності та економічної доцільності. Додатково оцінено потенціал впровадження SIEM, IDS/IPS, NAC та централізованого управління IoT-інфраструктурою. Запропоновано перелік організаційних заходів, включно з навчанням персоналу, парольною політикою та політикою доступу до критичних ресурсів.

Таким чином, реалізація комплексної системи захисту IoT-інфраструктури дозволяє істотно знизити ризики компрометації даних і пристроїв, забезпечити безперервність функціонування критичних сервісів та підвищити загальний рівень кіберзахисту підприємства. Запропонована модель захисту є універсальною,

масштабованою та може бути адаптована до інших організацій зі схожими загрозами, вимогами та архітектурою інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Recommendation ITU-T Y.2060, "Overview of the Internet of Things". *ITU*. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (Дата звернення: 23.05.2025).

2. GeeksforGeeks. Characteristics of Internet of Things - GeeksforGeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/characteristics-of-internet-of-things/ (Дата звернення: 25.05.2025).

3. Reynolds I. J. H. IOT Architecture: 3 Layers, 4 Stages Explained. *Custom Software Development Insights | Zibtek Blog*. URL: https://www.zibtek.com/blog/iot-architecture/ (Дата звернення: 25.05.2025).

4. What is the Internet of Things (IoT)?. *IBM*. URL: https://www.ibm.com/think/topics/internet-of-things (Дата звернення: 23.05.2025).

5. IoT protocols: A comprehensive guide. *A1 Digital*. URL: https://www.a1.digital/knowledge-hub/iot-protocols-a-comprehensive-guide/ (Дата звернення: 23.05.2025).

6. Explain different types of IoT Communication. *StudyX*. URL: https://studyx.ai/questions/4lkp0ne/explain-different-types-of-iot-communication-models-in-apa-format (Дата звернення: 23.05.2025).

7. IoT connections worldwide 2022-2033. *Statista*. URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (Дата звернення: 23.05.2025)

8. Networking Protocols and Standards for Internet of Things. *IEEE Internet of Things Journal*. 2015. с. 134.

9. 2020 Unit 42 IoT Threat Report. *Unit 42*. URL: https://unit42.paloaltonetworks.com/iot-threat-report-2020/ (Дата звернення: 23.05.2025).

10. OWASP Internet of Things. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: https://owasp.org/www-project-internet-of-things/ (date of access: 23.05.2025).

11. What is Mirai Botnet?. *CloudFlare*. URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/ (Дата звернення: 23.05.2025).

12. Guidelines for Securing the Internet of Things. ENISA. URL: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things (Дата звернення: 23.05.2025).

13. ETSI EN 303 645 Cybersecurity Standard for Consumer IoT Devices. *Intertek*. URL: https://www.intertek.com/iot/cybersecurity/etsi-en-303-645/ (Дата звернення: 23.05.2025).

14. SP 800-175B Rev. 1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. *NIST Computer Security Resource Center*. URL: https://csrc.nist.gov/pubs/sp/800/175/b/r1/final (Дата звернення: 24.05.2025).

15. IEC 62443-3-3:2013. *IEC*. URL: https://webstore.iec.ch/en/publication/7033 (Дата звернення: 24.05.2025).

16. Niroshan Y. Revolutionizing IoT Devices : Firmware Over-The-Air. *Medium*. URL: https://medium.com/@niroshanyi/revolutionizing-iot-devices-firmware-over-the-air-4b882ae2e776 (Дата звернення: 25.05.2025).

17. Cisco 2017 Annual Cybersecurity Report: Chief Security Officers Reveal True Cost of Breaches and the Actions Organizations are Taking. *The ChannelPro Network*. URL: https://www.channelpronetwork.com/2017/02/02/cisco-2017-annual-cybersecurity-report-chief-security-officers-reveal-true-cost-of-breaches-and-the-actions-organizations-are-taking/ (Дата звернення: 24.05.2025).

18. IoT Security Standards and Regulations: Where Are We Now?. *IoT For All*. URL: https://www.iotforall.com/iot-security-standards-and-regulations-where-are-we-now (Дата звернення: 25.05.2025).

19. ESP32 - ESP-IDF Programming Guide v4.3.3 documentation. *Espressif Systems*. URL: https://docs.espressif.com/projects/esp-idf/en/v4.3.3/esp32/api-reference/protocols/esp_tls.html (Дата звернення: 24.05.2025).

20. MikroTik hAP ax². *MikroTik Routers and Wireless*. URL: https://mikrotik.com/product/hap_ax2 (Дата звернення: 24.05.2025).

21. Hikvision White Paper on GDPR. *Hikvision Global - Leading the future of AIoT*. URL: https://www.hikvision.com/content/dam/hikvision/eu/support/cybersecurity/Hikvisions-White-Paper-on-GDPR.pdf (Дата звернення: 24.05.2025).

22. Tutorial: Change the Data-Channel Encryption Cipher. *Business VPN For Secure Networking | OpenVPN*. URL: https://openvpn.net/as-docs/tutorials/tutorial--change-encryption-cipher.html#tutorial--change-the-data-channel-encryption-cipher (Дата звернення: 25.05.2025).

23. Wazuh documentation. *Wazuh*. URL: https://documentation.wazuh.com/current/index.html (Дата звернення: 24.05.2025).

24. Suricata User Guide – Suricata 8.0.0-rc1-dev documentation. *Suricata User Guide*. URL: https://docs.suricata.io/en/latest/ (Дата звернення: 24.05.2025).