Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Кривчака Вадима Ігоровича

на здобуття ступеня вищої освіти Бакалавра

Система забезпечення фізичної безпеки приміщення на основі технології Інтернету речей

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

КРБКБ.2102151.21.02.30 ПЗ

Виконав студент 4 курсу, група КБ-21-2 10.06.25 Вадим КРИВЧАК
Підпис, дата Ініціали, прізвище

Керівник докт. техн. наук Михайло КАСЯНЧУК
Науковий ступінь, вчене звання Підпис, дата Ініціали, прізвище

Нормоконтролер старший викладач 16.06.25 Сергій МОСТОВИЙ
Науковий ступінь, вчене звання Підпис, дата Ініціали, прізвище

До захисту допускаю:

Зав. кафедри кібербезпеки _____ Юрій КЛЬОЦ
Підпис, дата Ініціали, прізвище

16 06 2025р.

Хмельницький, 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кривчака Вадима Ігоровича

1 Тема роботи Система забезпечення фізичної безпеки приміщення на основі технології Інтернету речей.

Керівник роботи докт. техн. наук Михайло КАСЯНЧУК

Затверджено наказом ректора університету від 7 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру _____

3 Вихідні дані до роботи Проаналізувати існуючі рішення безпеки IoT. Визначити основні компоненти для створення системи охорони об'єкту. Розробити схему розташування обладнання для реалізації системи охорони об'єкта із застосуванням технології Інтернету речей. Порівняння з вже існуючими рішеннями.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) (перелік питань, які потрібно розробити) Вступ. Теоретична частина. Аналіз систем. Розробка схеми. Висновки

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Схема розташування інвентаря. Схеми підключень.

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 16 лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	+
Ознайомлення з предметною областю	Лютий	+
Дослідження існуючих рішень	Лютий	+
Постановка задачі	Березень	+
Визначення загальних принципів рішення задачі	Березень	+
Деталізація принципів рішення задачі	Квітень	+
Розробка проєктних рішень	Квітень	+
Тестування ефективності реалізовних рішень	Травень	+
Оформлення пояснювальної записки згідно вимог	Травень	+
Оформлення графічної частини	Червень	+
Захист КР	Червень	+

Студент _____ Вадим КРИВЧАК

Керівник кваліфікаційної роботи _____ Михайло КАСЯНЧУК

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система забезпечення фізичної безпеки приміщення на основі технології Інтернету речей».

Автор роботи: студент групи КБ-21-2 Кривчак Вадим Ігорович.

Керівник роботи: докт. техн. наук Касянчук Михайло Миколайович.

Пояснювальна записка: 66 с, 1 додаток, 1 таблиць, , 32 рис, 40 джерел.

Графічна частина: 9 презентаційних слайдів.

Ключові слова: IOT, фізична безпека, датчики, моделі систем, машинне навчання.

Кваліфікаційна робота бакалавра присвячена розробці забезпечення фізичної безпеки приміщення на основі технології Інтернету речей.

В роботі проаналізовано та розглядаються сучасні виклики проектування систем безпеки приміщень, зокрема банківських відділень, через завищені вимоги до надійності та безвідмовності обладнання. Запропоновано інтеграцію технологій Інтернету речей (IoT) для удосконалення систем відеонагляду, сигналізації та контролю доступу. На основі проведеного дослідження визначено принципи роботи систем контролю доступу з акцентом на комбіновану ідентифікацію особи, включаючи біометричні методи

10.06.25

ABSTRACT

Subject of qualification work: End-device malware detection system.

Author: student of CS-21-2 Kryvchak Vadym Igorovych.

Head of work: Doctor of Technical Sciences Kasyanchuk Mykhailo Mykolayovych.

Explanatory note: p 66, appendices 1, figures 32, tables 1, sources 40

Graphic part: presentation slides 9.

Key words: IOT, physical security, sensors, system models, machine learning.

The bachelor's qualification work is devoted to the development of ensuring physical security of premises based on Internet of Things technology.

The work analyzes and considers modern challenges in designing security systems for premises, in particular bank branches, due to high requirements for reliability and reliability of equipment. The integration of Internet of Things (IoT) technologies is proposed to improve video surveillance, alarm and access control systems. Based on the research conducted, the principles of access control systems with an emphasis on combined personal identification, including biometric methods, are determined.

10.06.25

ЗМІСТ

Зм.	Арк.	№ докум.	Підпис	Дата	КРБКБ.2102151.21.02.30 ПЗ		
Виконав		Кривчак В. І		10.06	Система забезпечення фізичної безпеки приміщення на основі технології Інтернету речей Пояснювальна записка	Літера	Аркуш 6 / Аркушів 66
Перевір.		Касянчук М.М					
Н.контр.		Мостовий С.В		16.06.25		ХНУ, КБ-21-2	
Затвер.		Кльоц Ю.П		16.0825			

ВСТУП

У сучасному світі, де інформаційні та цифрові технології активно інтегруються в усі сфери життєдіяльності, питання забезпечення безпеки набуває нового змісту та складності. Фізична безпека об’єктів – одна з головних складових національної та персональної безпеки – нині реалізується не лише за допомогою традиційних охоронних засобів, а й через інтелектуальні рішення, побудовані на базі сучасних технологій. Одним із таких інноваційних напрямів є використання Інтернету речей (Internet of Things, IoT), який відкриває широкі можливості для моніторингу, контролю та реагування на фізичні загрози в реальному часі.

Інтернет речей передбачає інтеграцію великої кількості пристроїв, які взаємодіють між собою без участі людини, передаючи та аналізуючи дані, що надходять із сенсорів, камер, контролерів тощо. Застосування цієї концепції у сфері фізичної безпеки приміщень дозволяє побудувати адаптивні, ефективні й автоматизовані системи, здатні не лише реагувати на загрози, але й запобігати їм за рахунок прогнозування та аналітики поведінкових моделей. Зокрема, завдяки IoT стало можливим створення так званих «розумних» систем охорони, які забезпечують інтеграцію відеоспостереження, сенсорів руху, пристроїв контролю доступу та аналітичних модулів в єдину архітектуру.

Актуальність теми обумовлена зростаючою кількістю загроз, що виникають як з боку зовнішніх чинників (несанкціоноване проникнення, вандалізм, пожежі), так і внаслідок внутрішніх недоліків традиційних систем охорони (людський фактор, обмеження у швидкості реагування, фрагментарність даних). У цьому контексті системи на базі IoT є відповіддю на виклики часу, оскільки вони дозволяють оперативно виявляти загрози, забезпечувати точну локалізацію подій, адаптувати сценарії реагування відповідно до контексту, а також забезпечують централізоване управління великою кількістю точок контролю.

Разом із тим, незважаючи на стрімкий розвиток IoT, залишається низка питань, що потребують ґрунтовного аналізу. Йдеться не лише про вибір оптимальних технічних засобів, протоколів передачі даних чи топології побудови системи, а й про інформаційну безпеку самої інфраструктури.

1 ДОСЛІДЖЕННЯ СИСТЕМ ФІЗИЧНОЇ БЕЗПЕКИ ПРИМІЩЕНЬ І СФЕРИ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Аналіз сучасних загроз фізичній безпеці приміщень

Фізична безпека приміщень є одним із чи не головних елементів системи загального захисту об’єкта і в широкому значенні охоплює сукупність заходів, що спрямовані на попередження, виявлення, обмеження або ліквідацію впливу загроз, які мають матеріальний характер і можуть призвести до завдання шкоди матеріальним цінностям, інфраструктурі чи життю і здоров’ю осіб, що перебувають у приміщенні. Інакше кажучи, загрозу фізичній безпеці можна трактувати як потенційний або реальний вплив певного об’єкта, суб’єкта чи події, який у разі його реалізації може спричинити негативні наслідки для фізичного стану середовища, об’єктів матеріальної інфраструктури або осіб, які знаходяться в зоні ураження. Така загроза може виникати як із зовнішнього середовища (наприклад, внаслідок несанкціонованого вторгнення, стихійного лиха чи терористичного акту), так і зсередини системи (наприклад, через людський фактор, недбалість чи технічну несправність) [1].

У сучасному контексті, зважаючи на стрімкий розвиток технологій, урбанізацію та зростання інформаційної взаємопов’язаності, питання фізичної безпеки набуває додаткового змісту та вимагає глибшого переосмислення. На відміну від минулих десятиліть, сьогоднішні загрози часто мають комбінований характер, що проявляється у взаємодії фізичних чинників із цифровими. Наприклад, проникнення до будівлі може супроводжуватись одночасним втручанням у системи відеоспостереження або блокуванням сигналу охоронних пристроїв, що свідчить про зміну природи самої загрози – від простої механічної до високотехнологічної [2].

Актуальність аналізу сучасних загроз полягає ще й у тому, що багато організацій і установ, зокрема ті, що функціонують у сфері охорони здоров’я, освіти, енергетики, державного управління, залишаються вразливими до широкого спектру ризиків, пов’язаних із фізичними вторгненнями, саботажем, порушенням контролю доступу та відмовою систем життєзабезпечення. Традиційні системи

безпеки, засновані на використанні окремих охоронців, камер або сигналізаційних пристроїв, дедалі частіше не відповідають вимогам до реагування в реальному часі, масштабованості та автоматичної адаптації до змін середовища.

Під поняттям загроз фізичній безпеці, перш за все, слід розуміти ймовірність подій, що можуть призвести до фізичного пошкодження або знищення об'єкта, устаткування, інфраструктури, або завдати шкоди людям. Зміст цих загроз є багатогранним і охоплює широкий спектр потенційних сценаріїв: від класичного несанкціонованого доступу до критичних зон або приміщень, до дій, що мають на меті приховане порушення роботи інфраструктури через блокування входу/виходу, підпал або вплив на системи електропостачання. Особливо небезпечними є сценарії, в яких зовнішнє втручання поєднується з внутрішніми уразливостями – наприклад, недостатньо захищеними маршрутами евакуації, відсутністю резервного живлення для охоронних систем чи відсутністю контролю за рухом співробітників і відвідувачів [3].

На сучасному етапі загрози фізичній безпеці слід також розглядати у взаємозв'язку з інформаційними ризиками. Це зумовлено тим, що багато фізичних елементів захисту управляються або контролюються за допомогою цифрових протоколів і пристроїв. Таким чином, зовнішній нападник може, наприклад, отримати доступ до системи контролю доступу або камери спостереження шляхом атаки на бездротову мережу або центральний сервер. В результаті, порушення фізичної безпеки може стати не лише наслідком фізичної присутності зловмисника, але й проявом комплексної кібератаки, орієнтованої на фізичну інфраструктуру.

Додатковим вектором ризику стає людський фактор. Навіть найбільш досконалі технічні засоби захисту залишаються вразливими до випадків недбалості, помилок, халатного ставлення до інструкцій безпеки, чи навіть навмисних дій з боку працівників організації. Такі випадки мають особливо небезпечний характер, оскільки важко піддаються автоматизованому моніторингу, а отже – вимагають поєднання технологічних та організаційних заходів у межах єдиної стратегії безпеки.

Крім людського чинника та зовнішніх загроз, не варто ігнорувати ризики, пов'язані з природними явищами. Пожежі, затоплення, перепади температури,

сейсмічна активність – усе це може призвести до пошкодження обладнання, виведення з ладу систем охорони або навіть до неможливості евакуації осіб з небезпечної зони. Примітно, що більшість таких явищ не є повністю непередбачуваними – сучасні засоби моніторингу дають змогу відстежувати зміну умов навколишнього середовища та попереджати про критичні відхилення параметрів. Проте для цього потрібна цілісна система, яка здатна інтегрувати дані з різних сенсорів, виявляти закономірності та автоматично формувати сигнали тривоги [4].

Отже, спектр сучасних загроз фізичній безпеці значно ширший, ніж той, що фіксувався у класичних моделях охоронної діяльності. Нині важливо враховувати гібридний характер загроз, в якому поєднуються фізичні, цифрові та організаційні чинники. Оцінка ризиків більше не може базуватись виключно на статистичних даних про інциденти – вона має охоплювати прогнозування поведінкових сценаріїв, аналіз структурних вразливостей, оцінку резервів адаптації системи до надзвичайних ситуацій.

У зв’язку з цим, зростає потреба у використанні комплексних підходів, що поєднують технологічні можливості Інтернету речей з аналітичними засобами виявлення відхилень у поведінці об’єктів, а також забезпечують швидке, автономне і гнучке реагування на загрози. Саме такі підходи дозволяють трансформувати концепцію фізичної безпеки з пасивної моделі, яка реагує постфактум, у проактивну систему, здатну попереджати інциденти, а не лише реєструвати їх наслідки.

1.2 Огляд технологій Інтернету речей, застосовуваних для забезпечення фізичної безпеки

Поняття «Інтернет речей» (Internet of Things, IoT) стало однією з головних категорій сучасної інформаційної епохи. Його поява є результатом тривалого розвитку мережевих технологій, мікроелектроніки, телекомунікацій та автоматизованих систем обробки даних [5]. У загальному значенні Інтернет речей

– це концепція, яка передбачає об’єднання фізичних об’єктів у єдину мережу через засоби зв’язку, що дозволяє цим об’єктам збирати, обмінювати та аналізувати інформацію без необхідності прямої участі людини [26].

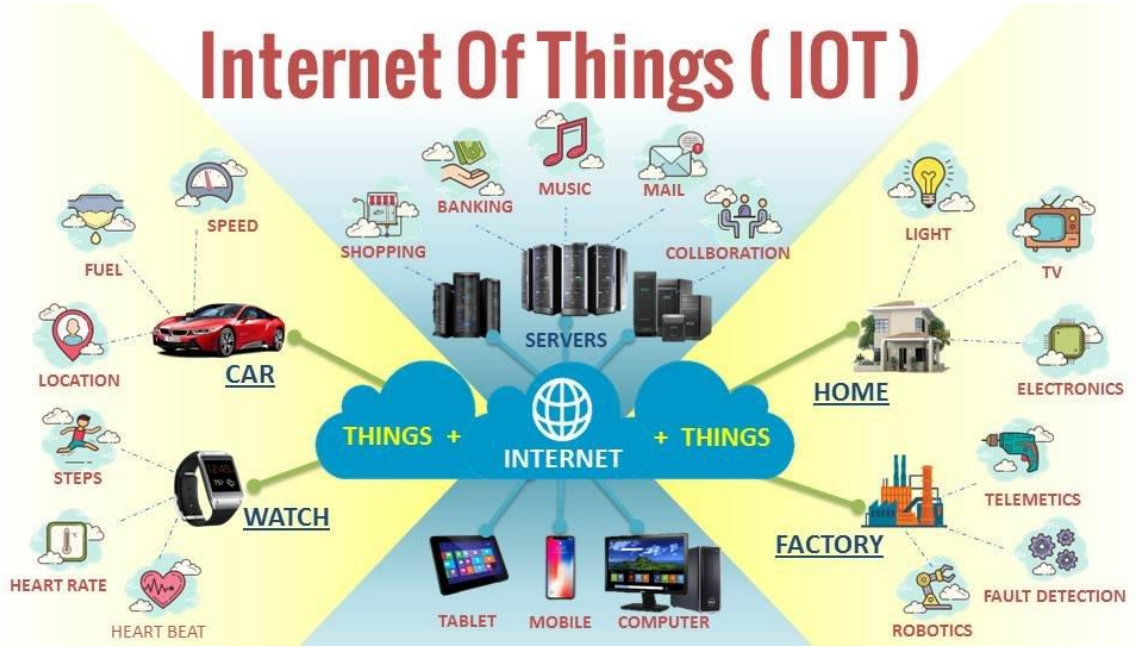


Рисунок 1.1 – Принцип Internet of Things, IoT

Ідея створення взаємопов’язаної системи об’єктів, які мають здатність «відчувати» навколишнє середовище, реагувати на події та передавати зібрані дані, бере свій початок ще у 1980-х роках. Одним із перших прикладів практичного втілення подібної концепції вважається проєкт автоматичного моніторингу запасів напоїв у торговому автоматі, який здійснювався за допомогою підключення пристрою до комп’ютерної мережі університету. Однак справжній розвиток Інтернету речей почався у 1999 році, коли дослідник з Массачусетського технологічного інституту Кевін Ештон уперше використав цей термін у контексті ідентифікації товарів за допомогою RFID-міток. Відтоді концепція еволюціонувала, охоплюючи дедалі ширше коло застосувань – від промислової автоматизації до інфраструктури «розумного міста», охорони здоров’я, агросектору та безпеки.

Інтернет речей не є самодостатньою технологією, а являє собою комплексну платформу, в яку входять апаратні засоби (сенсори, мікроконтролери, пристрої

збору та передачі інформації), програмне забезпечення (включаючи прошивки, протоколи зв'язку, платформи обробки даних) та системи управління, які інтегрують отриману інформацію в дію. Технічно IoT-пристрій – це будь-який об'єкт, здатний до самостійного підключення до мережі з метою надсилання або приймання даних. Особливість цієї концепції полягає у принципі децентралізації – інформація не зосереджена в одному центрі, а збирається та обробляється розподілено, часто на місці її виникнення, що дозволяє забезпечити швидкість реагування та адаптивність систем [6].

У сфері фізичної безпеки застосування Інтернету речей має доволі велике значення, оскільки дозволяє реалізовувати функції виявлення загроз, реагування на події, контролю доступу, моніторингу стану об'єктів та підтримки прийняття рішень в режимі реального часу. Використання IoT у безпеці означає побудову інфраструктури, у якій сенсорні модулі взаємодіють з камерами, системами оповіщення, виконавчими механізмами (наприклад, замками, турнікетами), а також з аналітичними сервісами, що забезпечують інтерпретацію даних.

Типовими елементами IoT-систем у сфері безпеки є сенсори руху, детектори вібрацій, магнітні контакти, інфрачервоні приймачі, камери відеоспостереження з модулем обробки зображення, мікрофони для виявлення шумів або звуків розбитого скла, а також системи контролю доступу, які працюють на основі RFID, NFC, Bluetooth або біометричних параметрів. Кожен із цих пристроїв виконує вузькоспеціалізовану функцію, але об'єднання їх у єдину систему дозволяє досягти синергетичного ефекту. Наприклад, камера відеоспостереження фіксує рух, який супроводжується відповідним сигналом від інфрачервоного сенсора, після чого автоматично надсилається сповіщення адміністратору або вмикається сирена [7].

Важливою особливістю застосування IoT у фізичній безпеці є можливість віддаленого керування та моніторингу. Користувач або охоронний персонал має змогу в будь-який момент переглянути статус системи, отримати сповіщення про події, налаштувати параметри безпеки або навіть активувати певні дії без необхідності фізичної присутності на об'єкті. Така гнучкість має вирішальне значення у сучасних умовах мобільності та децентралізації робочих процесів [8].

Окремо слід зазначити, що технології IoT у сфері безпеки базуються на

використанні різних протоколів обміну даними, кожен з яких має свої переваги та обмеження. Серед найпоширеніших слід згадати такі, як MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), HTTP/HTTPS, а також протоколи ближнього зв'язку – Zigbee, Z-Wave, Bluetooth Low Energy, LoRaWAN та інші. Вибір конкретного протоколу залежить від потреб системи: наприклад, Zigbee та Z-Wave мають низьке енергоспоживання і добре підходять для автономних сенсорів, тоді як MQTT забезпечує високу ефективність передавання повідомлень у мережах з обмеженою пропускною здатністю [9].

Не менш важливим компонентом IoT-систем безпеки є платформи керування. Йдеться про програмні середовища, які приймають дані з пристроїв, здійснюють їх попередню обробку, зберігають історію подій та забезпечують інтерфейс користувача для взаємодії з системою. Прикладами таких платформ можуть слугувати Home Assistant, Domoticz, OpenHAB, а також комерційні рішення, інтегровані в екосистеми відомих виробників, як-от Bosch Security Systems, Hikvision, Ajax Systems. Зазначені платформи здатні працювати у гібридному режимі, поєднуючи локальну обробку з хмарними сервісами, що даєзмогу мінімізувати затримки при реагуванні та одночасно зберігати історичні дані для подальшого аналізу [11].

Іншою перевагою впровадження IoT у фізичну безпеку є можливість інтеграції зі сторонніми інформаційними системами. Сучасні підходи до проєктування передбачають відкритість архітектури, що дозволяє підключати IoT-систему до систем відеоаналітики, баз даних доступу, аналітичних модулів прогнозування, систем керування будівлею (BMS) та інших цифрових середовищ. У результаті формується єдина інформаційно-безпекова екосистема, здатна до самоадаптації, аналізу ризиків у динаміці та визначення сценаріїв реагування залежно від контексту [11].

Проте, поряд із зазначеними перевагами, широке впровадження IoT у сферу фізичної безпеки супроводжується низкою викликів. Зокрема, актуальним є питання захисту самих IoT-пристроїв від несанкціонованого доступу. Через обмежені апаратні ресурси сенсорні пристрої часто мають слабкий рівень криптографічного захисту або взагалі не підтримують його, що створює потенційні

вектори атак. Крім того, необхідно забезпечити цілісність переданих даних, автентифікацію пристроїв у мережі, захист від підміни чи блокування інформації, а також дотримання норм конфіденційності щодо збереження відео- та аудіозаписів, журналів подій тощо [12].

Отже, використання Інтернету речей у сфері фізичної безпеки приміщень є багатогранним і перспективним напрямом, який поєднує апаратні інновації, програмну інженерію та аналітику у рамках єдиного інтегрованого підходу. Реалізація таких систем вимагає врахування широкого спектру факторів – від енергетичної автономності сенсорів до вибору протоколів, каналів зв'язку та методів обробки інформації. Незважаючи на виклики, що постають перед розробниками та впроваджувачами, очевидно, що саме технології IoT стануть основою нової парадигми у забезпеченні фізичної безпеки – адаптивної, інтелектуальної та передбачуваної.

1.3 Аналіз існуючих IoT-систем фізичної безпеки приміщень

Зі зростанням потреб у забезпеченні захисту об'єктів нерухомості, виробничих і житлових приміщень, системи фізичної безпеки, побудовані на базі технологій Інтернету речей, стали активно впроваджуватись як у приватному секторі, так і в корпоративному та державному середовищі. Сучасний ринок пропонує широке різноманіття рішень, які відрізняються за функціональними можливостями, архітектурними підходами, протоколами передачі даних, ступенем інтеграції з іншими системами та навіть географічною специфікою застосування.

Однією з найвідоміших українських розробок, що набула широкого визнання на міжнародному ринку, є система безпеки Ajax Systems, головна сторінка компанії зображена на рисунку 1.2.

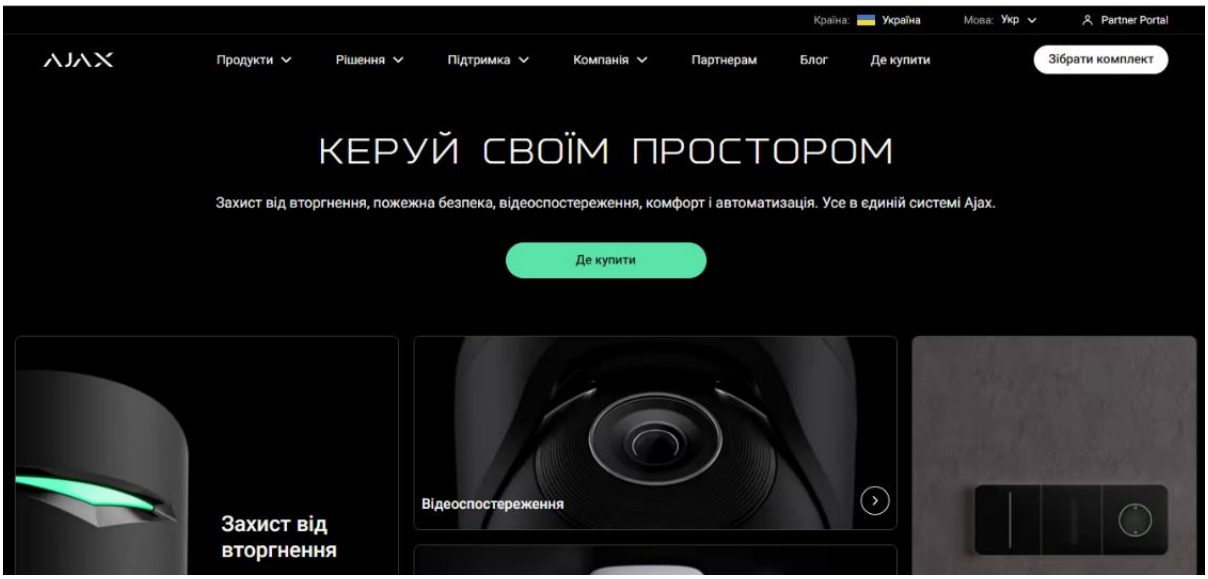


Рисунок 1.2 – Головна сторінка Ajax Systems

Ця система є прикладом повноцінної IoT-платформи, яка поєднує у собі бездротові детектори руху, відкриття, розбиття скла, димові сенсори, клавіатури, контролери реле, відеоспостереження та інтелектуальне хмарне керування. Високий рівень інтеграції, власна розробка радіопротоколу Jeweller, шифрування на основі AES, а також можливість адаптації до різних об’єктів робить цю систему прикладом ефективного поєднання апаратної надійності та гнучкого програмного середовища (рисунок 1.3).

Рисунок 1.3 -Пристрої бездротової системи безпеки Ajax

У реальних умовах система успішно використовується як у приватних оселях, так і в банківських відділеннях, комерційних центрах, офісах державних

установ. Її архітектура дозволяє адаптацію до об’єктів різного масштабу – від однокімнатної квартири до великих логістичних комплексів [13].

Іншим прикладом, що набув поширення в Європі, США та поступово виходить на ринки України, є екосистема Google Nest Secure. У цьому рішенні акцент зроблено на інтеграції з іншими продуктами компанії, включаючи Google Home, камери Nest Cam, відеодомофони Nest Hello та системи автоматизації освітлення і клімату.

Рисунок 1.4 – екосистема Google Nest Secure

Ця платформа дозволяє реалізацію сценаріїв, у яких фізична безпека тісно поєднана з функціями комфорту. Наприклад, коли фіксується рух біля дверей, вмикається освітлення у коридорі, надсилається сповіщення на смартфон власника і починається запис з камери. Таке поєднання функцій, орієнтоване на кінцевого споживача, підвищує привабливість систем для житлових будинків і квартир [14].

З-поміж локалізованих рішень, що реалізуються на рівні невеликих підприємств, варто відзначити використання розподілених сенсорних систем на базі Raspberry Pi (рисунок 1.5) та мікроконтролерів ESP32 (рисунок 1.6) [15, 16].

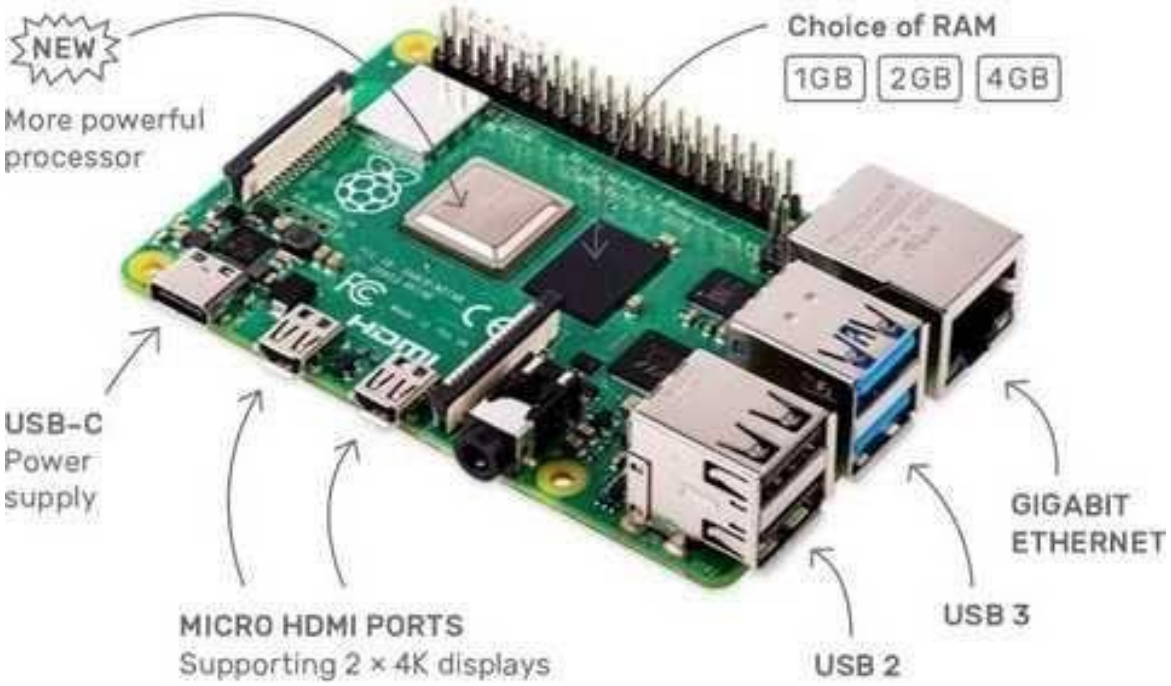


Рисунок 1.5 – Мікрокомп’ютер Raspberry Pi

Рисунок 1.6 – Мікроконтролерів ESP32

Подібні проєкти дедалі частіше реалізовуються в навчальних закладах, закладах охорони здоров’я та малих бізнесах в Україні як більш доступна альтернатива комерційним системам. Пристрої встановлюються на вікнах, дверях,

у коридорах, та виконують функції детекції руху, контролю температури, вологості, відкриття, з можливістю миттєвого реагування через Telegram-боти або SMS-інтерфейси. Незважаючи на обмежений функціонал порівняно з промисловими системами, такі рішення дозволяють досягти базового рівня безпеки при мінімальних витратах і високій гнучкості конфігурації.

З-поміж систем, що орієнтовані на комерційний і промисловий сектор, важливу роль відіграють рішення таких виробників, як Bosch Security Systems, Hikvision, Dahua. Вони пропонують модульні платформи з підтримкою IP-камер, термодетекторів, модулів розпізнавання обличчя, керування турнікетами та шлюзами. Такі системи зазвичай реалізуються на об’єктах критичної інфраструктури – в енергетичних підприємствах, аеропортах, вокзалах, складах зі спеціальними умовами зберігання. Наприклад, система Bosch з можливістю інтеграції пожежних та охоронних датчиків дозволяє створити єдиний центр моніторингу подій на об’єкті, де сигнал від сенсора негайно активує сценарій тривоги, блокує доступ до небезпечної зони та повідомляє черговий персонал.

Заслуговують на увагу й інтелектуальні платформи типу Verkada, що поєднують у собі хмарне зберігання відео, аналітику за допомогою штучного інтелекту, автоматичне розпізнавання облич та номерних знаків. Такі системи активно впроваджуються у школах, університетах, бізнес-центрах, де важливе не лише виявлення інциденту, а й можливість його аналізу, побудови звітів та дій на основі поведінкових моделей. Наприклад, в одному з американських університетів було реалізовано систему, яка у разі накопичення підозрілих дій (довге перебування в одній точці, часте відкривання дверей) попереджає службу безпеки про потенційну загрозу ще до її фактичного настання [17].

Особливим випадком застосування IoT-систем безпеки в Україні стали рішення, впроваджені в контексті воєнного часу. На об’єктах критичної інфраструктури, школах, укриттях використовуються автономні сенсорні комплекси для фіксації присутності, витоку газу, задимлення, температурних коливань.

Таблиця 1.1 – Порівняння поширених IoT-систем фізичної безпеки

Назва системи	Походження	Типова архітектура	Захищеність каналів зв’язку	Інтеграція з іншими системами	Приклади використання
Ajax Systems	Україна	Хаб + сенсори + хмара	AES-128, Jeweller	Часткова (через API)	Приватні будинки, банки, школи
Google Nest Secure	США	Хмара + IoT-пристрої	HTTPS, TLS	Повна (через Google Home)	Квартири, смарт-будинки
Bosch Security	Німеччина	Централізована, IP-зв’язок	Промислові стандарти	Повна (включно з BMS)	Аеропорти, логістичні хаби
Raspberry/ESP32 DIY	Відкриті рішення	Децентралізована, локальна	Залежить від реалізації	Можлива через MQTT/HTTP	ОСББ, лабораторії, малі офіси
Verkada	США	Хмара + AI-аналітика	AES-256, сертифікати	Висока, з AI-обробкою	Університети, офіси, кампуси

На основі таблиці 1.1 можна дійти висновку, що найбільш універсальними за функціоналом є системи типу Ajax та Bosch, які поєднують надійність, достатню гнучкість налаштувань та можливість інтеграції з іншими платформами. У той час, як Google Nest надає пріоритет кінцевому користувачу і має простий інтерфейс, вона не завжди підходить для масштабних об’єктів із підвищеним рівнем ризику. Своєю чергою, відкриті DIY-рішення демонструють високу гнучкість, проте

потребують технічної обізнаності, що обмежує їхню масову реалізацію. Системи з аналітичною надбудовою, такі як Verkada, демонструють новий тренд – інтеграцію ШІ для прогнозування і реагування, проте потребують значних інвестицій.

Але, варто зазначити, що не існує універсальної системи, яка могла б однаково ефективно вирішувати задачі безпеки на об'єктах різного типу. Наприклад, для житлового будинку достатньо інтеграції сенсорів відкриття та руху з IP-камерою, тоді як для промислового об'єкта з великим периметром потрібні багаторівневі бар'єри: датчики вібрацій ґрунту, лазерні перешкоди, контролери з криптографічною автентифікацією тощо. Водночас, гнучкість архітектури IoT дозволяє масштабувати систему, комбінуючи модулі та адаптуючи її до змін умов.

Усі наведені приклади свідчать про те, що існуючі IoT-системи фізичної безпеки демонструють як технічну зрілість, так і широкий спектр реалізованих функцій. Проте основною тенденцією, яка визначає розвиток цієї галузі, є перехід від простого виявлення до предиктивної безпеки, де основним стає не лише фіксація події, а й прогнозування її ймовірності, розрахунок ризиків та оптимізація дій у межах динамічної адаптивної стратегії. У цьому контексті важливим напрямом удосконалення залишається підвищення надійності взаємодії між пристроями, захист даних, мінімізація хибних спрацювань та зменшення залежності від людини як ланки реагування.

1.4 Визначення вимог до системи фізичної безпеки на базі технології Інтернету речей

У процесі створення ефективної системи фізичної безпеки приміщення, побудованої на основі технології Інтернету речей, головним етапом є формулювання чітких вимог до її функціональної, апаратної, програмної та експлуатаційної частини. Ці вимоги мають ґрунтуватися на результатах попереднього аналізу загроз, технічних можливостей сучасних рішень, а також з урахуванням специфіки об'єкта, на якому передбачається впровадження системи.

Передусім, будь-яка система безпеки, реалізована з використанням IoT-

компонентів, повинна бути здатною до цілодобового моніторингу ситуації в реальному часі. Це означає, що всі сенсори, виконавчі пристрої та контролери повинні безперервно функціонувати в мережі, забезпечуючи оперативне надходження інформації про зміну стану об’єкта. Відповідно, архітектура системи має бути побудована так, щоб унеможливити втрату даних через розриви зв’язку або вихід з ладу окремих елементів. Це передбачає не лише резервування каналів зв’язку, але й здатність до автономної роботи щонайменше базового рівня (локального спрацювання сирени, запису подій на внутрішній носій тощо) [18].

Дуже важливою вимогою є наявність можливості інтеграції з іншими підсистемами та програмними сервісами. Сучасне приміщення, що має високі вимоги до безпеки, зазвичай оснащується системами пожежного оповіщення, контролю клімату, автоматичного освітлення, контролю доступу та відеоспостереження. Система фізичної безпеки, що ґрунтується на технології Інтернету речей, повинна забезпечувати єдиний інтерфейс взаємодії з цими модулями, синхронізуючи роботу різнорідних пристроїв. Це досягається за рахунок використання відкритих або адаптивних протоколів зв’язку, таких як MQTT, HTTPS, Zigbee або Modbus TCP/IP.

Функціональна частина системи повинна передбачати не лише виявлення події, але й логіку реагування. Наприклад, якщо сенсор руху виявив присутність у забороненій зоні, система має автоматично ініціювати серію дій: фіксацію відеозапису, блокування доступу до певних приміщень, відправку сповіщення адміністратору або відповідальному працівнику. Така багаторівнева реакція дозволяє оперативно локалізувати потенційну загрозу без участі людини на початковому етапі. В ідеалі, налаштування подібних сценаріїв має здійснюватися без написання коду, через візуальні інтерфейси або веб-додатки, що суттєво розширює коло осіб, здатних здійснювати керування системою.

Ще одним доволі важливим моментом є інформаційна безпека самої системи. Усі канали зв’язку мають бути захищеними від несанкціонованого перехоплення даних. Пристрої, які передають або отримують інформацію, повинні автентифікуватися перед початком обміну. Бажаною є підтримка шифрування переданих даних за сучасними стандартами, наприклад AES-256. Крім того,

важливою є реалізація захисту від атак типу «відмова в обслуговуванні» (DoS), які можуть бути спрямовані на виведення з ладу основних вузлів мережі. У цьому контексті, необхідно забезпечити можливість оновлення прошивок пристроїв без фізичного втручання, тобто реалізувати функцію OTA (over-the-air update), що дозволяє швидко усувати вразливості.

Суттєве значення має також аспект масштабованості. У разі зміни конфігурації об’єкта, додавання нових зон, датчиків або функціоналу, система повинна легко адаптуватися до нових умов без повної реконструкції. Це досягається за рахунок модульної побудови, коли кожен компонент системи – це окремий елемент, який можна підключити до централізованої системи управління. Зручність додавання нових пристроїв, автоматичне розпізнавання їх типу, можливість дистанційного налаштування параметрів – усі ці властивості мають бути передбачені на етапі проєктування.

Не менш важливою вимогою є стабільність роботи пристроїв за різних умов зовнішнього середовища. Багато IoT-рішень використовуються на об’єктах, де температура, вологість або пил можуть впливати на роботу електроніки. Отже, пристрої повинні відповідати промисловим стандартам стійкості, мати відповідний ступінь захисту корпусу (наприклад, IP65 або вище), а також працювати у розширених температурних діапазонах.

Особливе місце серед вимог займає питання зручності користувача. Незалежно від рівня складності внутрішньої архітектури системи, кінцевий користувач повинен мати доступ до простого та інтуїтивно зрозумілого інтерфейсу. Це може бути веб-додаток, мобільний застосунок або спеціальний контрольний модуль. Основні функції – перегляд подій, управління доступом, перегляд записів, налаштування профілів – мають бути доступними без потреби в спеціальній технічній підготовці. Інтерфейс має підтримувати українську мову, адаптуватися до різних типів пристроїв (ПК, смартфони, планшети), а також забезпечувати доступ через автентифікацію з багатофакторною перевіркою.

Визначення вимог до системи фізичної безпеки, побудованої на IoT – це не лише перелік функцій, які система повинна виконувати, але й опис її здатності адаптуватися, розширюватися, взаємодіяти з іншими системами та гарантувати

збереження інформації. Усі ці вимоги мають бути реалізовані з урахуванням можливостей сучасного технологічного середовища, а також відповідати стандартам безпеки, надійності та ергономіки.

1.5 Постановка задачі

Об’єктом дослідження цієї дипломної роботи є процес побудови систем фізичної безпеки приміщень. Предметом – використання технологій Інтернету речей як основи для розробки таких систем.

Метою роботи є теоретичне обґрунтування концепції, структури, функціональних можливостей та перспектив розвитку систем фізичної безпеки, які реалізуються на базі технологій IoT.

У процесі дослідження було поставлено наступні завдання:

– здійснити аналіз існуючих загроз фізичній безпеці приміщень та методів їх нейтралізації;

– провести огляд сучасних IoT-рішень, що застосовуються у сфері охоронних систем;

– сформулювати вимоги до системи фізичної безпеки з використанням IoT;

– запропонувати концептуальну модель архітектури системи безпеки;

– окреслити підходи до оцінки ефективності та можливості розвитку таких систем.

Структурно дипломна робота складається з трьох розділів. У першому розділі досліджено загрози фізичній безпеці, наведено огляд технологій Інтернету речей, а також проаналізовано наявні рішення на ринку. У другому розділі сформовано концептуальну архітектуру системи, описано її функціональні компоненти та засоби взаємодії. Третій розділ присвячено аналізу ефективності запропонованого підходу, висвітленню проблем реалізації та визначенню перспектив розвитку IoT-систем безпеки.

Запропонована тема не лише є актуальною з практичної точки зору, але й

становить науковий інтерес у контексті подальшого розвитку комплексних захисних технологій у цифрову епоху. Результати дослідження можуть бути корисними для фахівців у сфері інформаційної та фізичної безпеки, розробників IoT-рішень, а також для проєктантів інтелектуальних систем охорони будівель, офісів, навчальних закладів та інших приміщень.

2 ПРОЄКТУВАННЯ СИСТЕМИ ФІЗИЧНОЇ БЕЗПЕКИ НА ОСНОВІ ТЕХНОЛОГІЙ IoT

2.1 Концептуальна модель системи фізичної безпеки

Формування концептуальної моделі є етапом у проєктуванні будь-якої інформаційно-технічної системи, оскільки вона дозволяє уніфіковано представити загальну логіку її функціонування, визначити основні підсистеми, їхню взаємодію, а також сформулювати принципи, на яких базується організація роботи. У випадку системи фізичної безпеки, побудованої з використанням технологій Інтернету речей, концептуальна модель повинна описувати загальний обсяг даних, типи пристроїв, канали передачі інформації та логіку реагування на події.

На відміну від традиційних охоронних рішень, які найчастіше базуються на централізованому управлінні та обмеженій кількості точок моніторингу, системи на базі IoT мають розподілений характер. Це означає, що кожен окремий сенсор чи модуль не лише виконує пасивну роль, а й може ініціювати обробку подій, взаємодіяти з іншими пристроями напряму, без участі центрального контролера. У свою чергу, центральна частина системи не лише фіксує інциденти, але й виконує функції аналітики, прогнозування та адаптації під змінні умови.

Концептуальна модель теоретичної системи фізичної безпеки може бути представлена як багаторівнева структура, що охоплює чотири умовні рівні: сенсорний, комунікаційний, аналітичний та рівень керування (рисунок 2.1).

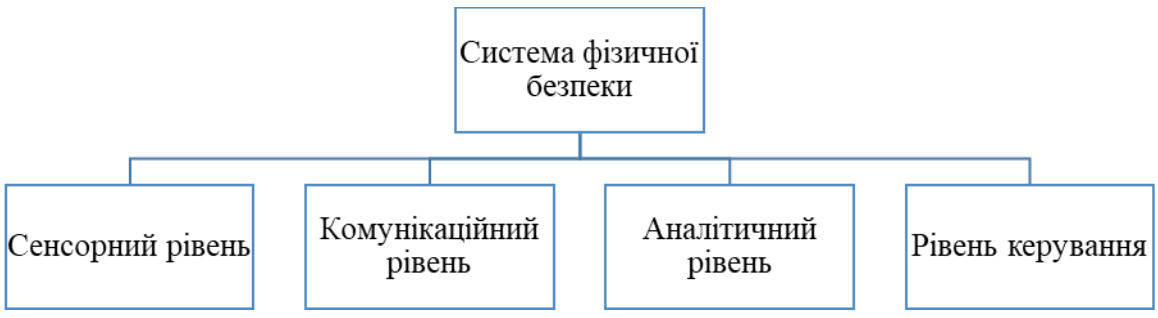


Рисунок 2.1 – Рівні системи фізичної безпеки

На сенсорному рівні функціонують усі первинні пристрої збору даних. Сюди відносяться датчики руху, відкриття, диму, звуку, температури, відеокамери,

детектори вібрації та інші пристрої, що безперервно фіксують стан фізичного середовища у межах об’єкта. Особливістю цього рівня є велика кількість вузлів, які розміщуються по периметру охоронюваного об’єкта або всередині будівлі й працюють у реальному часі.

Комунікаційний рівень забезпечує обмін інформацією між елементами системи. Це можуть бути бездротові протоколи ближнього радіусу дії (рисунок 2.2), мобільний зв’язок (2G/3G/4G), або дротові канали (Ethernet, RS-485) [19].

Рисунок 2.2 – Протоколи ближнього радіусу дії

У рамках концепції Інтернету речей особливої уваги набуває забезпечення надійності, низького енергоспоживання та захищеності переданих даних. Саме на цьому рівні визначається маршрутизація повідомлень, час доставки тривожного сигналу, а також синхронізація між пристроями.

Аналітичний рівень відповідає за обробку отриманих даних. Це ядро системи, де відбувається виявлення відхилень, класифікація подій, візуалізація стану об’єкта, а в деяких випадках – побудова прогнозів щодо потенційних загроз. На цьому етапі важливою складовою є програмне забезпечення, що реалізує логіку безпеки, а також алгоритми прийняття рішень. У теоретичному варіанті можна передбачити наявність модулів машинного навчання, які з часом адаптуються до поведінкових шаблонів середовища та вдосконалюють точність реагування.

Нарешті, рівень керування виконує функцію взаємодії з користувачем або автоматизованими виконавчими пристроями. Сюди входять мобільні застосунки, веб-інтерфейси, системи оповіщення (звукові, світлові), а також фізичні пристрої управління – замки, бар’єри, штори, тощо. В ідеалі цей рівень має бути

максимально гнучким: користувач повинен мати змогу як вручну втрутитися у процес, так і дозволити системі діяти автономно відповідно до заданих сценаріїв.

Важливо зазначити, що запропонована концепція не є фіксованою схемою, а скоріше – узагальненим теоретичним шаблоном, який може застосовуватись для аналізу або удосконалення реальних систем. Так, наприклад, в системах Ajax присутні усі зазначені рівні, хоча аналітична частина реалізується переважно у хмарі. У системах типу DIY (на базі ESP32) аналітичний рівень часто спрощений або відсутній, що знижує адаптивність, але підвищує автономність. У промислових рішеннях на кшталт Bosch чи Verkada кожен із рівнів має модульну реалізацію та підтримує масштабування.

Побудова концептуальної моделі дозволяє не лише сформувати уявлення про структуру майбутньої системи, а й виділити основні точки вразливості, визначити можливості для інтеграції та запропонувати напрями удосконалення. У подальших підрозділах ці аспекти будуть розглянуті з позиції апаратного і програмного наповнення, мережевої взаємодії та варіантів модернізації на основі аналізу реальних рішень.

2.2 Структура апаратного та програмного забезпечення системи

Формуючи цілісну теоретичну концепцію системи фізичної безпеки на основі технологій Інтернету речей, важливо визначити основні компоненти, що складають її апаратну та програмну структуру. Така структура є не лише інженерною картою функціональних зв’язків, а й логічним відображенням принципів побудови взаємодії між сенсорними пристроями, каналами зв’язку, процесорами даних та інтерфейсами керування. В умовах зростаючої складності безпекових викликів і підвищених вимог до автономності, масштабованості й надійності систем, структура їхніх компонентів має бути гнучкою, взаємозамінною та відкритою до модернізації.

У контексті апаратної частини загальна структура IoT-системи фізичної безпеки охоплює кілька головних типів пристроїв: датчики, контролери, виконавчі

елементи та комунікаційні модулі. Датчики, або сенсорні пристрої, є першоджерелом інформації про стан середовища. Серед них – детектори руху, вібраційні сенсори, датчики відкриття дверей та вікон, сенсори температури, диму, газу, а також камери відеоспостереження. Кожен з цих пристроїв виконує свою локальну функцію, генеруючи події при зміні стану параметра або при фіксації аномалії [20].

До найбільш уживаних фізичних сенсорних пристроїв належать інфрачервоні (PIR) датчики руху (рисунок 2.3), які фіксують зміну теплового випромінювання в зоні охоплення; мікрохвильові сенсори, що реагують на рух завдяки доплерівському ефекту; а також комбіновані модулі, які поєднують обидві технології для зменшення кількості хибних спрацювань.

Рисунок 2.3 –Датчики руху PIR

Датчики відкриття (магнітоконтактні) працюють за принципом розімкнення магнітного кола та використовуються для контролю стану дверей і вікон (рисунок 2.4).

Рисунок 2.4 – Магнітоконтактний датчик відкриття дверей/вікна Satel S-4

Сенсори розбиття скла аналізують акустичні хвилі, які характерні для ударів і тріщин, тоді як вібраційні сенсори – чутливі до механічних коливань, що супроводжують спроби проникнення.

Рисунок 2.5 – Датчик розбиття скла

В окрему категорію виділяються газові, температурні й димові сенсори, які виконують функцію екологічного моніторингу – зокрема, попереджають про загоряння або витоки токсичних речовин. Камери відеоспостереження, інтегровані в систему, не лише передають зображення в реальному часі, але й можуть виконувати аналітичні функції, такі як виявлення руху, розпізнавання облич або ідентифікація подій за заданими сценаріями.

Контролери, які часто реалізуються на основі вбудованих мікропроцесорів або мікроконтролерів (наприклад, ESP32, STM32, Raspberry Pi), відповідають за приймання сигналів від сенсорів, первинну обробку даних і передачу їх до центральної системи. У більш складних реалізаціях контролери здатні виконувати локальну логіку прийняття рішень, наприклад – заблокувати двері у відповідь на тривожне сповіщення без участі центрального сервера. При цьому важливо, щоби обробка здійснювалася в реальному часі або з мінімально можливою затримкою.

Виконавчі пристрої у системі фізичної безпеки реалізують дію у фізичному середовищі, вони замикають контури живлення, активують звукові та світлові сигнали, блокують замки, надсилають аварійні повідомлення або керують інженерними системами будівлі. Ці пристрої мають бути безпечними, надійними та здатними функціонувати навіть у разі втрати зв’язку з центральним вузлом.

До головних фізичних виконавчих пристроїв належать електросирени, що сигналізують про тривогу високим звуковим тиском і світловими ефектами; електромеханічні замки та засувки, які керуються дистанційно або автоматично та забезпечують блокування входу в приміщення при спрацюванні сенсорів; а також інтелектуальні реле, що дозволяють перемикати лінії живлення або активувати зовнішні пристрої. Часто такі пристрої мають функцію пріоритетного живлення або автономної роботи за рахунок вбудованого джерела енергії.

Комунікаційні модулі забезпечують взаємодію всіх вищезазначених компонентів між собою. У сучасних системах фізичної безпеки найчастіше застосовуються бездротові технології, що забезпечують оптимальний баланс між енергоспоживанням, дальністю зв’язку та швидкістю передачі даних. Прикладами є Wi-Fi, Zigbee, Bluetooth Low Energy, LoRaWAN. Для резервного підключення можуть застосовуватись дротові технології типу Ethernet або RS-485. У теоретичній моделі також передбачається підтримка мультиканальної передачі для підвищення стійкості системи до збоїв.

Важливо зазначити також роль шлюзів (IoT-хабів), які об’єднують усі пристрої в одну локальну мережу, забезпечуючи маршрутизацію даних між фізичними сенсорами та хмарними сервісами. Вони можуть підтримувати одразу кілька типів протоколів, а деякі – навіть виконувати частину аналітичних функцій

у режимі edge computing.

Структура програмного забезпечення системи формується з урахуванням необхідності обробки подій, зберігання історичних даних, забезпечення візуалізації, а також інтеграції з іншими сервісами або платформами. Програмна частина умовно поділяється на прошивки пристроїв (низькорівневе програмування), програмні модулі обробки (логіка подій, бази даних) і призначений для користувача інтерфейс.

Прошивки сенсорів і контролерів відповідають за базову логіку взаємодії пристроїв із середовищем: реакцію на сигнали, активацію передачі, переходи у стан енергозбереження тощо. У теоретичній моделі важливо передбачити, що така прошивка повинна бути відкрита до оновлення, підтримувати захищене підключення і автентифікацію.

На рівні обробки подій реалізуються сценарії дій, аналітичні модулі, зберігання логів, обробка даних з камер та сенсорів. Це можуть бути як локальні рішення, розгорнуті на гейтах або серверах локальної мережі, так і хмарні сервіси, які приймають інформацію з пристроїв і забезпечують масштабну обробку. У контексті сучасних тенденцій актуальним є поєднання обох підходів – так зване гібридне опрацювання даних (edge + cloud processing), коли основні реакції відбуваються локально, а глибока аналітика здійснюється віддалено.

Інтерфейс користувача – ще один важливий елемент, що визначає зручність і практичність системи. Він може реалізовуватися через веб-додатки, мобільні застосунки, персональні панелі керування. Залежно від цільової аудиторії інтерфейс може бути адаптований для кінцевого користувача (власника житла) або адміністратора системи безпеки (у разі об’єктів інфраструктури). Його головні функції – перегляд статусу пристроїв, повідомлення про події, управління сценаріями дій та аналіз історії подій.

Отже, структура апаратного та програмного забезпечення системи фізичної безпеки, реалізованої на основі технологій Інтернету речей, є результатом поєднання спеціалізованих пристроїв, протоколів зв’язку, алгоритмів обробки даних та засобів візуалізації. Її ефективність визначається не лише кількістю або точністю сенсорів, а й загальною узгодженістю роботи всіх рівнів – від датчика до

прийняття рішення. Усі ці компоненти повинні функціонувати як єдине ціле, забезпечуючи стабільність, безперервність і здатність до адаптації в умовах динамічного змінного середовища.

2.3 Протоколи взаємодії пристроїв Інтернету речей у системах фізичної безпеки

Однією з технічних складових будь-якої IoT-системи, зокрема і у сфері фізичної безпеки, є механізм обміну даними між пристроями. Така взаємодія реалізується за допомогою спеціалізованих протоколів, які визначають спосіб передавання повідомлень, структуру пакетів, механізми ідентифікації, автентифікації та маршрутизації. У контексті безпеки, де критичним є час реакції, енергоефективність, стійкість до перешкод та гарантована доставка, вибір протоколу має безпосередній вплив на загальну ефективність і надійність усієї системи.

Протоколи, що використовуються в IoT-середовищі, умовно поділяються на дві категорії: прикладні (application layer) та канальні/фізичні (low-power wireless communication). Кожен з рівнів виконує свою специфічну функцію: перший відповідає за логіку обміну повідомленнями між застосунками, другий – за фізичну передачу сигналу в середовищі.

Серед прикладних протоколів, які набули найбільшого поширення у системах фізичної безпеки, можна відзначити MQTT (Message Queuing Telemetry Transport). Його головною перевагою є надзвичайно мала вага протоколу, що дозволяє ефективно працювати у мережах із низькою пропускною здатністю або високою затримкою. MQTT працює за принципом публікації-підписки, що дозволяє будь-якому пристрою, який підписався на певну тему (topic), отримувати відповідні повідомлення (рисунок 2.6).

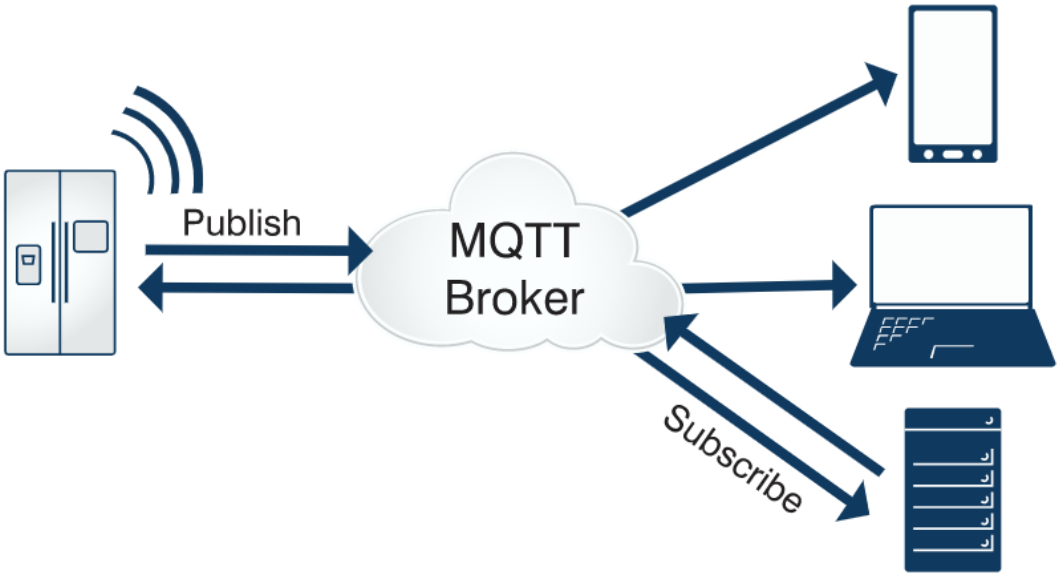


Рисунок 2.6 – Принцип роботи MQTT брокера

Це значно спрощує організацію масштабованих систем безпеки, у яких велика кількість сенсорів взаємодіє з кількома централізованими вузлами. Крім того, MQTT передбачає можливість реалізації зворотного каналу зв'язку, що дозволяє надсилати команди від сервера до пристроїв.

Ще одним прикладним протоколом є CoAP (Constrained Application Protocol), створений спеціально для пристроїв з обмеженими ресурсами. CoAP побудований на основі протоколу UDP і за своєю логікою схожий на HTTP, що робить його зручним для розробників. Його відмінною рисою є можливість використання мультикасту, що особливо корисно для масової передачі команд або сповіщень, наприклад, при надходженні сигналу тривоги на кілька точок одночасно [22]. На рисунку 2.7 наведено порівняння саме протоколу CoAP з MQTT.

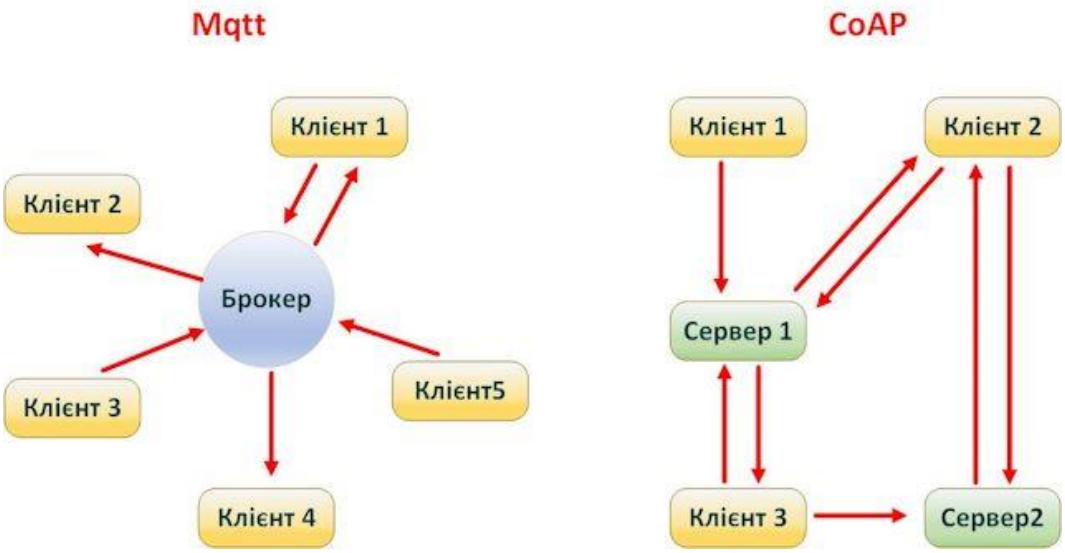


Рисунок 2.7 – Порівнння принципу роботи протоколів CoAP та MQTT

У питанні безпеки важливим є також протокол HTTPS, що базується на класичному HTTP, але із додаванням рівня шифрування TLS/SSL. Його застосування доречне для передачі конфіденційних даних або автентифікації користувачів через веб-інтерфейси керування системою. Проте через відносно велику вагу пакету та затримку у встановленні з'єднання, HTTPS рідше використовується для безпосередньої взаємодії між сенсорами (рисунок 2.8) [23].

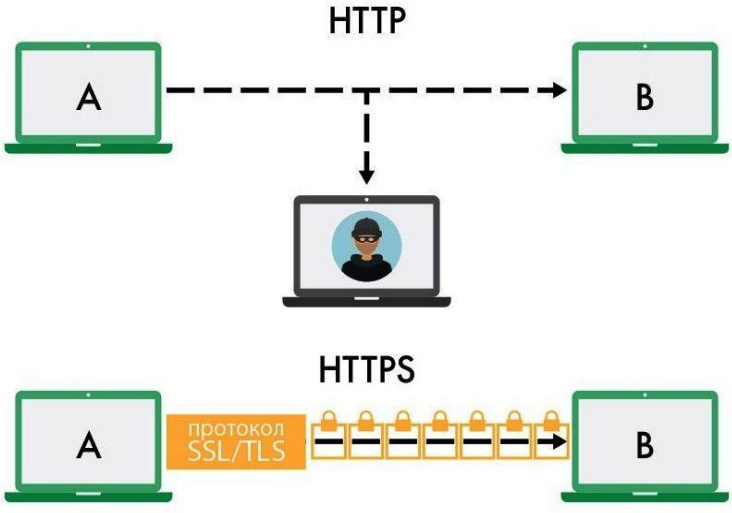


Рисунок 2.8 – Відмінність між протоколами HTTPS та HTTP

У низькорівневому сегменті найбільш поширеними є протоколи Zigbee, Z-Wave, Bluetooth Low Energy (BLE), LoRaWAN та Wi-Fi. Кожен із них має свої

переваги та обмеження, що визначають сферу їхнього доцільного застосування.

Zigbee – це протокол з низьким енергоспоживанням, який підтримує мережеву топологію типу mesh (рисунок 2.9).

Рисунок 2.9 – Структура протоколу Zigbee

Завдяки цьому пристрої можуть взаємодіяти не лише з центральним хабом, а й один з одним, що значно підвищує стійкість до втрати сигналу. Цей протокол часто використовується у системах контролю доступу, сигналізації, а також для керування освітленням.

Z-Wave, подібно до Zigbee, також використовує топологію mesh, але працює на іншій частоті (близько 900 МГц), що зменшує ймовірність перешкод з боку Wi-Fi пристроїв. Його головною перевагою є високий рівень сумісності пристроїв від різних виробників, оскільки протокол стандартизований на рівні альянсу Z-Wave Alliance [24].

Bluetooth Low Energy переважно застосовується у невеликих приміщеннях або в мобільних пристроях, де важливе значення має мінімальне енергоспоживання. У системах безпеки його часто використовують для

автентифікації користувача за допомогою смартфона або для передачі сигналу між замком і мобільним додатком [25].

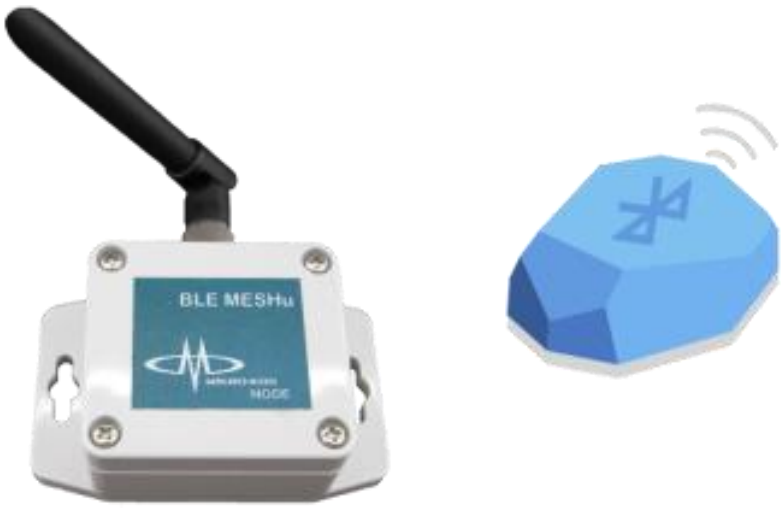


Рисунок 2.10 – Пристрій Bluetooth Low Energy

LoRaWAN забезпечує дальню передачу даних (до 10 км у відкритій місцевості) при надзвичайно низькому енергоспоживанні. Хоча цей протокол не підходить для передавання відео чи аудіо, його перевага – ідеальна придатність для передачі простих подій типу «виявлено рух», особливо в умовах, де немає стабільного доступу до дротового зв’язку або Wi-Fi (рисунок 2.11).

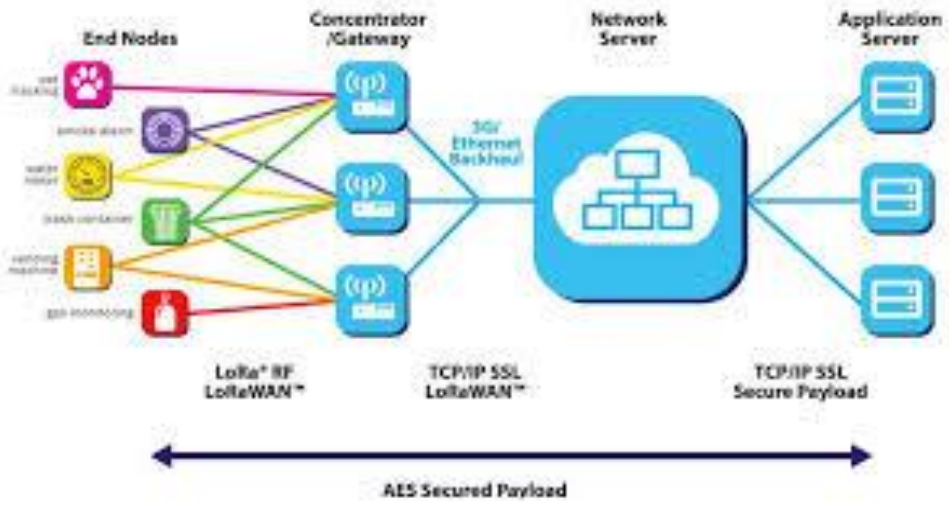


Рисунок 2.11 – Технологія LoRaWAN

Wi-Fi залишається найпоширенішим варіантом підключення, особливо у побутових умовах. Його перевагою є висока швидкість передачі даних, що робить його придатним для камер відеоспостереження, проте споживання енергії є суттєвим обмеженням для автономних сенсорів [24].

У реальних реалізаціях систем фізичної безпеки часто застосовується комбінація кількох протоколів: наприклад, сенсори можуть передавати дані на хаб через Zigbee, після чого хаб взаємодіє з хмарним сервером через MQTT або HTTPS. Такий підхід дозволяє поєднувати переваги локальної обробки та хмарної масштабованості.

Усі зазначені протоколи також мають свої механізми шифрування, автентифікації, верифікації достовірності даних. Проте важливо розуміти, що навіть наявність криптографічного захисту не гарантує безпеку, якщо він реалізований некоректно. Тому при формуванні вимог до системи доцільно передбачати підтримку оновлення прошивок, сертифікатів безпеки, а також логування спроб підключення або несанкціонованого доступу.

Протоколи взаємодії є невід'ємним структурним елементом концепції IoT у сфері фізичної безпеки. Вони визначають не лише можливості системи щодо передачі даних, а й впливають на її надійність, масштабованість, стійкість до збоїв і гнучкість у подальшій модернізації. Ретельний вибір і комбінація протоколів надає змогу побудувати систему, яка буде не лише функціонально повною, а й технічно стійкою до загроз зовнішнього середовища.

2.4 Пропозиції щодо удосконалення функціоналу існуючих систем

Аналіз сучасного стану IoT-систем фізичної безпеки приміщень свідчить про значний поступ у напрямі автоматизації охоронних процесів, підвищення надійності виявлення загроз та зручності керування. Проте навіть найрозвинутіші комерційні платформи мають низку недоліків і обмежень, що зумовлює потребу у подальшому вдосконаленні функціоналу. Враховуючи тенденції розвитку технологій Інтернету речей та зростання складності безпекових загроз, у даному

підпункті пропонуються шляхи покращення роботи наявних систем, які можна було б теоретично інтегрувати в їхню архітектуру або алгоритми.

Насамперед, актуальним залишається питання адаптивності систем безпеки до змін у середовищі функціонування. Більшість існуючих рішень працюють на основі статичних сценаріїв, які визначають реакцію системи на заздалегідь передбачені події. Наприклад, датчик руху активує сирену або надсилає повідомлення при кожному виявленні активності. Такий підхід, хоча й ефективний у простих випадках, не враховує контекст події: час доби, звичні маршрути користувача, погодні умови, попередню історію подібних інцидентів. Теоретично доцільно було б інтегрувати в системи елементи адаптивної логіки, які здатні навчатися на основі накопичених даних, і, відповідно, коригувати сценарії реагування. Це дозволило б суттєво зменшити кількість хибних спрацювань і підвищити інформативність сповіщень.

Ще одним напрямом удосконалення є розширення взаємодії між пристроями безпосередньо на локальному рівні, без потреби у зверненні до центрального контролера або хмарного сервера. Існуючі реалізації здебільшого передбачають вертикальну архітектуру взаємодії, де всі події проходять через хаб. У теоретичній перспективі доцільно впроваджувати горизонтальні схеми, у яких пристрої взаємодіють за принципом «peer-to-peer», що дозволяє суттєво підвищити швидкість реагування, зменшити залежність від інтернет-з’єднання і реалізовувати складніші сценарії – наприклад, колективне прийняття рішення про активацію тривоги у разі одночасного спрацювання кількох сенсорів.

Окрему увагу слід звернути на проблему візуалізації стану системи і доступу до історичних даних. Багато наявних платформ не забезпечують користувача повноцінною аналітикою: записи з камер зберігаються обмежений час, немає інтерактивних діаграм подій, відсутній зручний інтерфейс аналізу спрацювань за критеріями (час, зона, тип загрози). Теоретично виправданим удосконаленням у цьому контексті може стати розробка модулів ситуаційного аналізу, які на основі історичних даних формуватимуть узагальнені картини активності, виявлятимуть «аномальні» часові вікна, дозволятимуть ранжувати ризики за зонами або типами подій. У таких системах користувач отримає не просто повідомлення про «рух в

кімнаті», а статистично обґрунтоване попередження про нетипову активність порівняно з аналогічними часовими відрізками.

Ще одним напрямом покращення є безперервність роботи систем у критичних ситуаціях. Багато сучасних рішень у разі зникнення інтернету або живлення стають малоефективними: вони не передають сповіщення, не мають резервного живлення для камер або шлюзів, не зберігають локальні копії даних. Теоретична модель удосконалення передбачає використання комбінованих джерел живлення (мережа + акумулятор + сонячна панель), локальні резервні копії відео або логів, а також дублювання каналів зв'язку (наприклад, основний Wi-Fi, резервний – GSM).

Останній, але не менш важливий аспект, пов'язаний із розширенням доступності таких систем для малих об'єктів – приватних квартир, дач, невеликих офісів. Багато сучасних платформ залишаються складними для самостійного встановлення і налаштування. Теоретичне удосконалення може полягати у створенні універсального відкритого інтерфейсу налаштування системи через мобільний додаток або голосового помічника, з можливістю автоматичної конфігурації на основі обраного шаблону (наприклад, «житловий будинок», «магазин», «офіс»). Це дозволило б зменшити поріг входу для користувачів без технічної освіти і підвищити рівень загальної захищеності населення.

Отже, навіть без створення принципово нової системи можливо сформулювати обґрунтовані теоретичні напрями вдосконалення вже існуючих рішень у сфері IoT-безпеки. Потенціал сучасних технологій дозволяє оптимізувати архітектуру охоронних систем, не вдаючись до повного переосмислення їхньої структури, а натомість зосередитись на точковому підсилення основних функціональних блоків. Серед найважливіших характеристик, які мають бути пріоритетними на наступному етапі еволюції систем фізичної безпеки, визначальне місце займає адаптивна логіка управління. Йдеться про здатність системи не лише реагувати на зовнішні стимули, а й аналізувати контекст, змінювати сценарії дій відповідно до поведінкових моделей, історії подій та змін у середовищі.

Також важливою складовою модернізації є запровадження горизонтальної взаємодії між пристроями, що дозволяє зменшити залежність від центрального

вузла, прискорити обмін інформацією та забезпечити більш гнучку реакцію в умовах непередбачуваних ситуацій. Така децентралізована архітектура значно підвищує загальну відмовостійкість системи та сприяє її масштабуванню без втрати керованості.

Окремо слід підкреслити роль аналітичної візуалізації – інструменту, що дозволяє користувачеві не просто отримувати повідомлення про події, а бачити загальну динаміку, виявляти аномалії, будувати прогнозні моделі та приймати обґрунтовані управлінські рішення. Візуальна інтерпретація інформації, підкріплена аналітикою, перетворює систему безпеки з технічного комплексу на повноцінний інструмент ситуаційного контролю.

Невід'ємною умовою ефективного функціонування IoT-систем безпеки є їхня стійкість до збоїв – як технічних (перебої живлення, втрати зв'язку), так і логічних (конфлікти між пристроями, перевантаження мережі). Здатність системи працювати у деградованому режимі, підтримка резервних каналів передачі даних, локальна обробка подій – усе це повинно стати невід'ємною частиною проєктних рішень.

Не менш важливою складовою є інтуїтивне налаштування системи, орієнтоване на користувача з базовими технічними знаннями. Спрощення інтерфейсів, автоматичне виявлення пристроїв, шаблони сценаріїв, голосове керування або адаптація на основі попередніх дій користувача – усі ці елементи сприяють підвищенню доступності технологій безпеки для широкого кола споживачів, зокрема в побутовому секторі.

Підсумовуючи, можна стверджувати, що модернізація існуючих IoT-систем безпеки не обов'язково передбачає створення нових платформ «з нуля». Натомість комплексне вдосконалення окремих функціональних елементів здатне забезпечити суттєве підвищення ефективності, надійності та адаптивності систем до викликів сучасного середовища. Саме на цих пріоритетах має будуватися подальша еволюція систем фізичної безпеки у цифрову епоху.

3 РЕАЛІЗАЦІЯ СИСТЕМИ ОХОРОНИ ОБ'ЄКТА НА ОСНОВІ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

3.1 Об'єкт проектування

Для впровадження системи безпеки з високим рівнем надійності було обрано районне вигадане відділення банку «Ascold Cred» площею 380 м². Згідно з вимогами замовника, приміщення необхідно розділити на дві зони: загальна зала для обслуговування клієнтів (фойє банку) та спеціалізовані приміщення (VIP-зони), призначені для проведення фінансових операцій та зберігання цінностей, зокрема грошей, дорогоцінних металів тощо, що належать як клієнтам, так і банку. У VIP-приміщеннях, зокрема біля сейфа, необхідно забезпечити підвищений рівень безпеки. Технічні аспекти проектування системи безпеки будуть розглянуті окремо з урахуванням таких компонентів: система відеоспостереження, система контролю доступу, система виявлення руху та система сигналізації. Крім того, система освітлення у приміщеннях базується на технології Інтернету речей, що дозволяє керувати освітленням як вручну, так і через централізовану панель управління, підключену до головного сервера безпеки.

Передбачається, що у відділенні банку, крім зазначених типів приміщень, будуть облаштовані дві технічні апаратні кімнати. У цих приміщеннях розміщено обладнання для моніторингу відеокамер, а також пристрої, що функціонують за технологією LoRaWAN, та компоненти бездротової сигналізації від компанії Ajax. Відповідно до вимог замовника, необхідно забезпечити комплексну систему безпеки в головній залі відділення та реалізувати підвищений рівень захисту у трьох VIP-приміщеннях банку. Загальний план будівлі банку, на якому зображено розгорнуту систему освітлення (без вказівки блоку живлення, оскільки електрощит розташовано поза межами плану), представлено на рисунку 3.1.

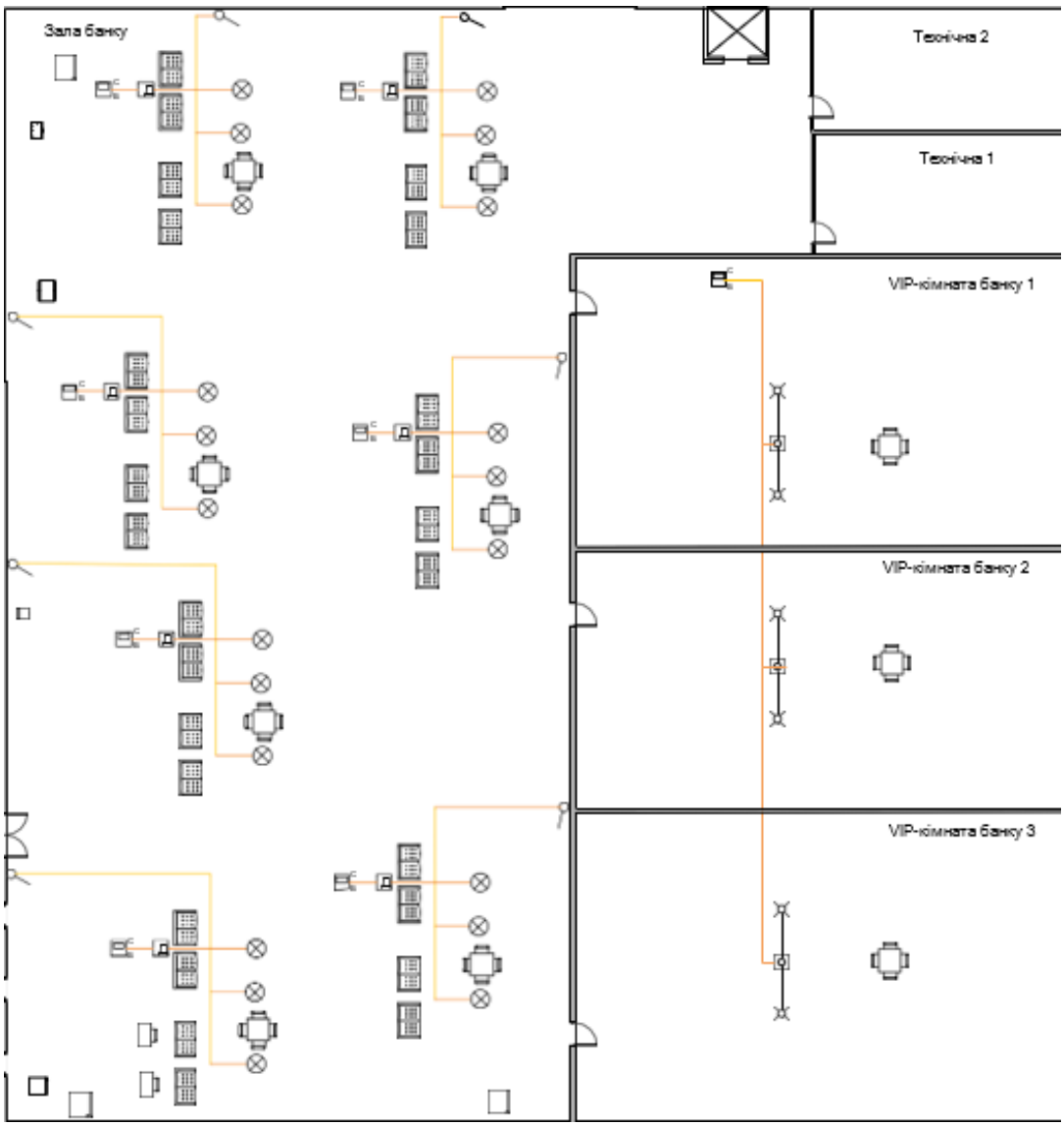


Рисунок 3.1 – Зона банку

Система освітлення поділяється на два види: зональне освітлення та загальне 7для VIP-приміщень. Усі кімнати обладнані дверима, а простора зала додатково має вікна. Окремо зображено ліфт і елементи меблевого оснащення. Важливо зазначити, що для доступу до головної зали архітектурного комплексу передбачено двостулкові двері.

Рисунок 3.2 – Схема підключення ламп освітлення у віділені банку

На рисунку 3.1 видно, що світильники у великій залі банку під’єднані до джерела живлення та керовані за допомогою драйвера й контролера освітлення (електронного діммера). Схематичне зображення цієї системи представлено на рисунку 3.2.

3.2 Системи спостереження

З урахуванням конструктивних особливостей для проектування системи відеоспостереження обрано такі типи камер: Поворотні, що призначені для моніторингу великих просторів і рухомих об’єктів, оснащені механізмом обертання, що забезпечує широкий спектр їхнього застосування і Купольні , які мають напівсферичний корпус, у якому розміщено швидкісний поворотний механізм, камеру з об’єктивом-трансфокатором і приймач телеметрії. Завдяки широкому куту огляду та високій швидкості роботи вони забезпечують якісне панорамне зображення для спостереження за великими територіями та динамічними об’єктами. Непоганим варіантом буде купольні камери виробників Hikvision рисунок 3.3

Рисунок 3.3 – Hikvision DS-2CE56D0T-IRMMF

Turbo HD відеокамера Hikvision DS-2CE56D0T-IRMMF – це купольна камера, призначена для внутрішнього використання в системах відеоспостереження. Вона підтримує технологію Turbo HD, що забезпечує високу якість зображення через коаксіальний кабель, а також сумісність із сучасними системами безпеки.

Основні технічні характеристики:

Тип камери: Купольна, аналогова (Turbo HD).

Роздільна здатність: 2 Мп (1920×1080 пікселів), Full HD.

Матриця: 2 Мп CMOS-сенсор.

Об’єктив: Фіксований, 2.8 мм, 3.6 мм або 6 мм (залежно від модифікації), кут огляду до 103° (для 2.8 мм).

Інфрачервоне підсвічування: До 20 метрів, забезпечує чітке зображення в умовах низької освітленості або повної темряви.

Режим день/ніч: Автоматичне перемикання з механічним ІЧ-фільтром (ICR).

Чутливість: 0.01 Лю

А в випадку поворотної камери візьмемо для того щоб збільшити площу спостереження та контролю, найкращим варіантом буде камера зображена на рисунку 3.4.

Рисунок 3.4 – Hikvision DS-2DE7A432IW-AEB T5

IP-камера Hikvision DS-2DE7A432IW-AEB T5 – це поворотна (PTZ) камера, призначена для використання в системах відеоспостереження з підвищеними вимогами до якості зображення та функціональності. Вона підтримує передові технології, включаючи розпізнавання об’єктів на основі штучного інтелекту, і є ідеальним рішенням для моніторингу великих територій, таких як банківські зали, офіси чи інші об’єкти з високими вимогами до безпеки.

Основні технічні характеристики:

Тип камери: Поворотна (PTZ), IP-камера.

Роздільна здатність: 4 Мп (2560×1440 пікселів).

Матриця: 1/2.8" Progressive Scan CMOS.

Об’єктив: Варіофокальний, 4.8–153.6 мм, 32-кратний оптичний зум, кут огляду від 55.6° до 2.04°.

Панорамування та нахил: Панорама 360° (безперервне обертання), нахил від -15° до 90° (автоматичний переворот).

Інфрачервоне підсвічування: До 200 метрів, забезпечує якісне зображення в умовах низької освітленості або повної темряви.

Режим день/ніч: Автоматичне перемикання з механічним ІЧ-фільтром (ICR).

Чутливість: 0.005 Люкс @(F1.2, AGC увімкнено), 0 Люкс з ІЧ-підсвічуванням.

Стандарти стиснення відео: H.265+/H.265/H.264+/H.264, MJPEG.

Частота кадрів: До 30 к/с при 4 Мп.

Систему відеоспостереження для зазначеного об’єкта можна організувати, враховуючи специфіку розміщення купольних камер і поворотніх камер. Звичайні

камери, що підтримують керування через IP-протокол і живляться за технологією (PoE), пропонується встановити в двох технічних приміщеннях системи безпеки, а також у трьох VIP-приміщеннях. У кожній VIP-кімнаті буде розміщено по дві такі камери. Загалом для створення системи використано 8 таких камер. На схемі PoE-адаптер не відображено, оскільки вважається, що він уже задіяний при підключенні камер до мережі Ethernet. Схему підключення камери з підтримкою технології PoE показано на рисунку 3.5.

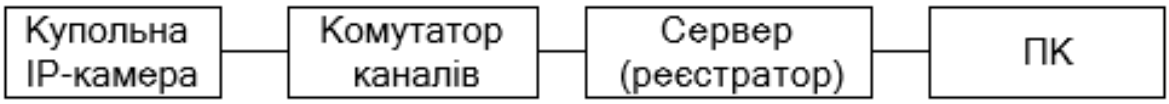


Рисунок 3.5 – Підключення куп. камери

Для основної зали відділення банку передбачено встановлення 9 поворотних камер обраної моделі. Такий вибір зумовлений особливостями IP-камери Hikvision DS-2CE56D0T-IRMMF, яка оснащена поворотним механізмом, що забезпечує широкий кут огляду та різноманітний функціонал для ефективного відіоспостереження. Схему підключення цієї камери представлено на рисунку 4.6. Для комутації відеокамер використано комутатор каналів циско.

Рисунок 3.6 – Підключення поворотної камери

Камера працює за таким принципом: камери підключаються до нього через лінії зв’язку та передають відеопотік. Реєстратор приймає відеодані, обробляє їх, перетворюючи в зображення, конвертує у потрібний формат і, за потреби, зберігає на пристрій для запису. Для системи безпеки пропонується використання реєстратора Hikvision DS-7732NI-K4. Цей пристрій підтримує підключення до 32 відеокамер і забезпечує зберігання даних на накопичувачі об’ємом до 6 ТБ.

Для підвищення надійності системи безпеки у VIP-приміщеннях пропонується впровадити додаткові бездротові камери на основі технології IoT, оснащені Wi-Fi-модулем і сумісні з пристроями, що використовують технологію LoRaWAN. Як приклад такої камери обрано модель EZVIZ C3WN

Рисунок 3.7 –EZVIZ C3WN

Таких камер в системі безпеки розташуємо по 4 одиниці в кожній VIP-кімнаті. Схема підключення такої камери наведена на рисунку 3.8.

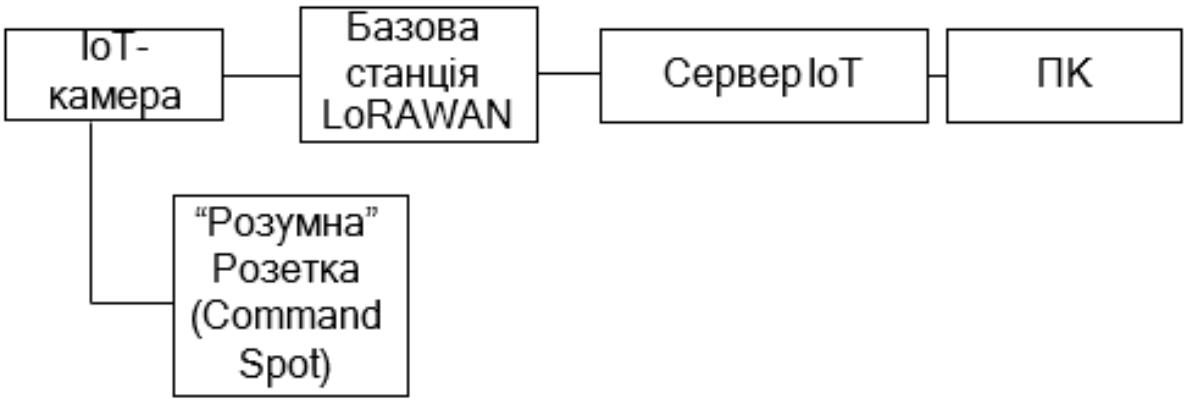


Рисунок 3.8 – Схема підключення IoT камери

Слід зазначити, що вибір такого технічного рішення зумовлений здатністю гібридної системи відеоспостереження підвищувати загальну надійність. У цьому випадку дані, отримані від звичайних Hikvision, дублюються інформацією, яку забезпечують бездротові камери.

3.3 Системи СКУД

Оскільки периметр об’єкта, що охороняється, має специфічні вимоги до безпеки, необхідно забезпечити контроль та ідентифікацію осіб, які входять до приміщення банківського відділення.

Для управління доступом використано зчитувач карт Dahua DHI-ASI1201A. А внут. боку дверей установлено кнопку для активації електронних замків ZKTeco TL-600. Dahua DHI-ASI1201A зображено на рисунку 3.9.

Рисунок 3.9 – Dahua DHI-ASI1201A

Рисунок 3.10 – ZKTeco TL-600

Для гарантії надійного замикання дверей використано електромагнітний замок Yli Electronic YM-60 з живленням 12 В.

Рисунок 3.11 – Yli Electronic YM-60

Систему контролю доступу, подібно до системи відеоспостереження, доцільно реалізувати як багаторівневу.

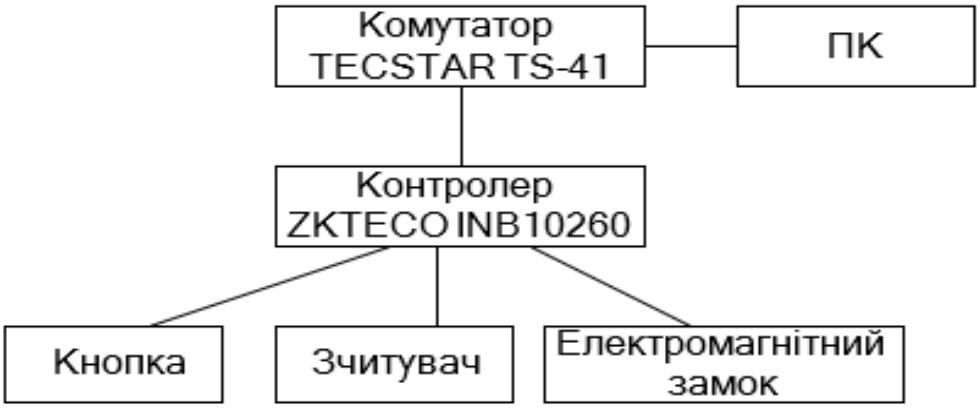


Рисунок 3.12 – СКУД

Для забезпечення сигналізації на кожні двері та вікна встановлюються бездротові датчики відкриття Satel VERSA-MCU. Основні характеристики Satel VERSA-MCU: тип датчика – бездротовий; поріг спрацьовування – 3 см; дальність передачі сигналу – до 3000 м; робочі частоти – 798 або 1025 МГц. Потужність радіопередавача – 30 мВт; елемент живлення – батарея; термін роботи від однієї батареї – 10 років; робоча напруга – 4 В.

Як датчики руху у всіх приміщеннях банківського відділення використовуються красні датчики руху Satel AQUA Plus. Основні характеристики пристрою: тип датчика – бездротовий; сенсор руху – піроелектричний; дальність виявлення руху – 22 м; горизонтальний кут огляду – 90 °; вертикальний кут огляду

– 100 °; Аналіз площі приміщень встановлюється 10 датчиків, розрахованих на активні зони кімнат. Ці датчики підключаються до централі управління Satel Perfecta через бездротову систему зв’язку, розташовану в технічному приміщенні системи безпеки. Для підвищення безпеки та контролю доступу до VIP-приміщень впроваджено інтелектуальну систему на основі рішень компанії Kerberos IoT. Ця система використовує зчитувачі, що працюють як із картами доступу, так і з сенсорами дотику, а також підтримує технологію LoRaWAN.

Інтеграція з внутрішньою мережею підприємства забезпечує централізований моніторинг і миттєве реагування на інциденти. Додатково, система дозволяє створювати гнучкі сценарії доступу залежно від ролі користувача та часу доби. У разі спроби несанкціонованого проникнення відбувається автоматичне блокування дверей і надсилання сповіщення службі безпеки. Система веде детальний журнал подій, що дозволяє аналізувати дії персоналу та швидко виявляти потенційні загрози. Завдяки використанню LoRaWAN забезпечується стабільний зв'язок навіть у складних архітектурних умовах. Система легко масштабується та може бути адаптована до специфіки різних об’єктів без значних витрат. Передбачена можливість резервного живлення гарантує безперебійну роботу навіть у разі відключення електроенергії. Завдяки модульній архітектурі можлива інтеграція з іншими захисними та аналітичними платформами.

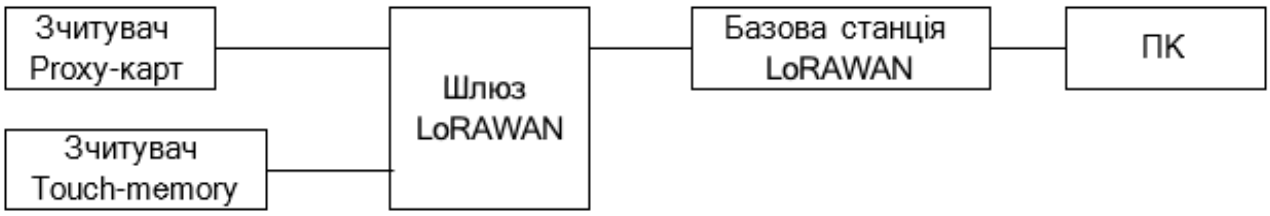


Рисунок 3.13 – СКУД на IOT

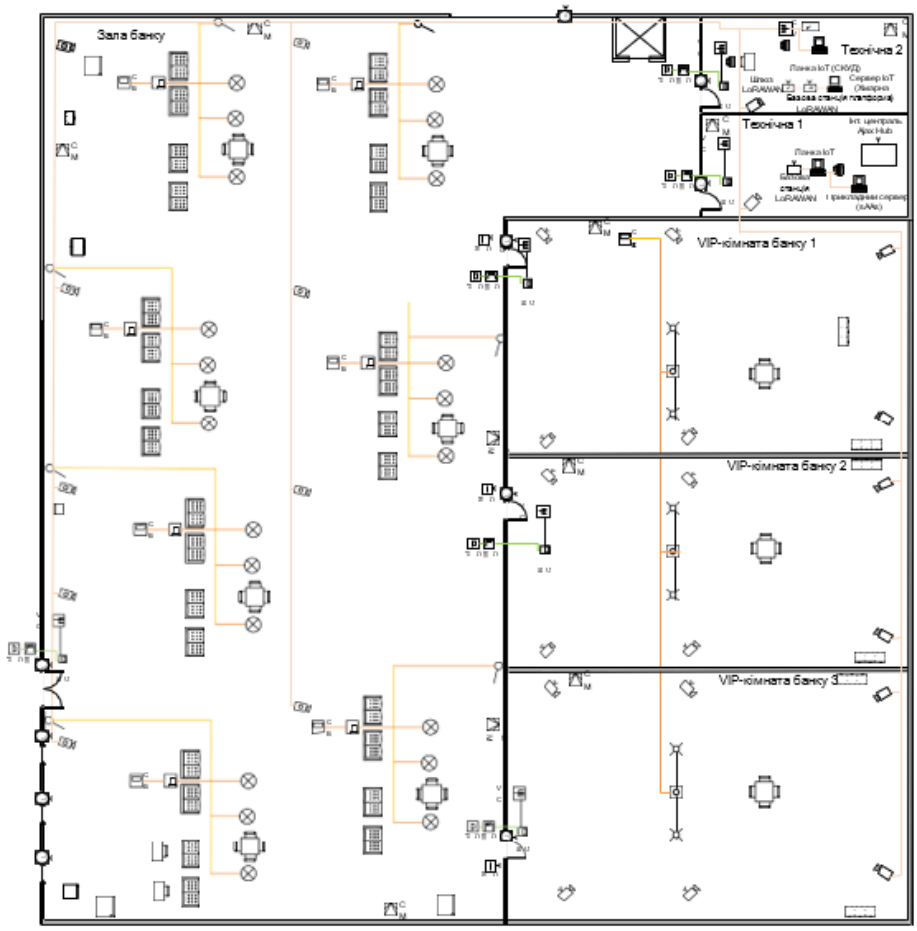


Рисунок 3.14 – Карта банку захисту

На основі проведеного підбору обладнання та аналізу схем підключення компонентів системи безпеки банківського відділення сформовано комплексне технічне рішення для забезпечення захисту обраного об’єкта.

3.4 Критерії оцінки ефективності IoT-систем фізичної безпеки

Оцінювання ефективності систем фізичної безпеки, що побудовані на базі технологій Інтернету речей, є необхідною складовою аналізу якості їх впровадження, функціонування та подальшого вдосконалення. В умовах стрімкого розвитку цифрових рішень, зокрема у сфері охоронних технологій, виникає потреба у формуванні чіткої методології, яка б дозволяла не лише зіставляти окремі системи між собою, а й встановлювати відповідність між технічними характеристиками та реальними потребами об’єктів, що підлягають охороні.

У загальному випадку ефективність системи безпеки можна трактувати як здатність системи виконувати свої функції у заданих умовах з високою точністю, стабільністю, швидкістю реакції та за мінімального втручання з боку користувача. Проте у випадку IoT-систем така оцінка ускладнюється багаторівневою структурою, наявністю розподілених вузлів, динамічністю середовища функціонування, а також інтеграцією з хмарними сервісами, штучним інтелектом та сторонніми протоколами керування.

Одним із базових критеріїв виступає надійність виявлення загроз, тобто здатність системи своєчасно і правильно реагувати на події, що потенційно можуть становити небезпеку. Надійність визначається не лише чутливістю сенсорів або точністю аналітичного модуля, а й сукупністю параметрів: стабільністю зв'язку, відсутністю конфліктів при одночасному надходженні даних з кількох пристроїв, здатністю системи відрізнити реальну загрозу від фонової активності. Теоретичною метою має бути досягнення так званої низької частоти хибних спрацювань при високій чутливості.

Наступним важливим параметром є час реакції. Під цим мається на увазі проміжок часу між моментом виникнення події (наприклад, спрацювання сенсора руху) та виконанням захисної дії (наприклад, надсилання повідомлення, блокування дверей, активація сирени). Для ефективної роботи в системах фізичної безпеки цей інтервал повинен бути мінімальним – бажано не більше однієї секунди. На практиці час реакції залежить від вибраного протоколу зв'язку, пропускної здатності мережі, навантаження на обчислювальний модуль та віддаленості користувача.

Ще одним важливим критерієм є енергоефективність системи. Більшість сенсорних пристроїв у IoT-середовищі працюють автономно, живляться від батарей або сонячних модулів. Тривалість їх функціонування без заміни джерела живлення прямо впливає на вартість обслуговування та зручність експлуатації. У системах фізичної безпеки важливо, щоб автономні компоненти працювали стабільно щонайменше протягом року, зберігаючи при цьому здатність до швидкої передачі сигналів і періодичного оновлення прошивки.

Додатковим параметром, що має суттєве значення, є масштабованість. Вона

передбачає можливість розширення системи без значного ускладнення її архітектури або необхідності повної перебудови логіки. У випадку IoT-систем масштабованість реалізується завдяки модульному підходу, коли до наявної інфраструктури можна додавати нові пристрої, зони моніторингу, типи сенсорів, не змінюючи ядра системи. Висока масштабованість є особливо важливою для об’єктів, що поступово розширюються (наприклад, виробничі комплекси або склади).

Окремо слід зупинитись на інтероперабельності, тобто здатності системи взаємодіяти з іншими програмно-апаратними комплексами. Це можуть бути системи відеонагляду, контролю доступу, автоматичного освітлення, пожежогасіння, а також платформи «розумного дому» чи будівельного моніторингу. Теоретично ефективною вважається система, яка використовує відкриті протоколи зв’язку або API та підтримує стандартизовані моделі інтеграції.

Оцінюючи IoT-систему, не можна ігнорувати інформаційну безпеку, яка полягає у здатності системи захищати дані від несанкціонованого доступу, підміни або втрати. При цьому розглядаються такі фактори, як шифрування каналів зв’язку, автентифікація пристроїв, можливість віддаленого оновлення прошивки, наявність систем журналювання подій. У теоретичній моделі ефективною вважається система, яка не лише реалізує базовий захист, але й передбачає механізми виявлення аномалій у трафіку та дій користувача.

Останнім, але не менш важливим моментом, виступає зручність користування. Система має бути інтуїтивно зрозумілою, з простими інтерфейсами, підтримкою мов локалізації, доступом з мобільних пристроїв та адаптивною реакцією на потреби користувача. У системах, орієнтованих на масове використання, зручність і швидкість навчання користувача часто відіграють вирішальну роль у тому, чи буде система ефективною в реальних умовах.

Усі зазначені критерії можуть розглядатись як взаємопов’язані, адже ефективність системи безпеки не визначається ізольованими параметрами, а формується на перетині технічних, експлуатаційних і контекстуальних характеристик. У цьому зв’язку теоретично обґрунтованою є побудова інтегральної моделі оцінки ефективності, яка враховує взаємозалежність факторів та їхній

відносний вплив на загальну продуктивність системи. Така модель передбачає застосування вагових коефіцієнтів для кожного параметра – наприклад, для часу реакції, точності детекції, рівня енергоефективності, вартості обслуговування чи зручності взаємодії з користувачем. Це дозволяє адаптувати підхід до оцінювання відповідно до специфіки об’єкта – будь то житловий комплекс, навчальний заклад, заклад охорони здоров’я чи промисловий об’єкт із підвищеним рівнем ризику.

Важливо розуміти, що ефективність IoT-систем фізичної безпеки не може бути зведена лише до суто технічних показників, таких як дальність дії сенсорів або пропускна здатність каналу зв’язку. До сфери аналізу мають входити також соціальні аспекти (рівень прийняття технології користувачами, вплив на приватність), експлуатаційні (надійність у тривалому використанні, вимоги до технічного обслуговування) та інтеграційні (сумісність із іншими системами, масштабованість, відкритість до оновлень і адаптації). Наприклад, система, яка демонструє високу точність і швидкість, але викликає незручності у використанні або потребує надмірних витрат на обслуговування, навряд чи буде ефективною у реальному середовищі.

Тому лише багатофакторний підхід дозволяє дійти обґрунтованих і всебічних висновків щодо доцільності впровадження тієї чи іншої IoT-системи в конкретному середовищі. Комплексна модель оцінювання також може стати інструментом прийняття управлінських рішень, оптимізації витрат, вибору постачальника або формування вимог до нових розробок. Такий підхід сприяє об’єктивізації процесу впровадження систем фізичної безпеки, підвищуючи ймовірність успішної інтеграції технології в соціально-професійне середовище.

3.5 Проблеми та обмеження сучасних рішень

Попри значні успіхи у розвитку технологій Інтернету речей і широке впровадження IoT-систем у сфері фізичної безпеки, наявні рішення все ще характеризуються низкою проблем, які стримують їхнє повсюдне використання та знижують загальний рівень ефективності. Ці обмеження стосуються не лише

технічної сторони, а й економічних, організаційних, нормативних і психологічних аспектів, що формують цілісну картину сучасного стану галузі.

Однією з найбільш помітних проблем є високий рівень фрагментації ринку. Сьогодні спостерігається значна кількість незалежних розробників і виробників, які пропонують несумісні між собою системи. Це призводить до відсутності єдиного стандарту на рівні протоколів взаємодії, способів обробки подій, моделей конфігурації та управління. Внаслідок цього користувачі змушені або обмежуватись рішеннями одного виробника, або інвестувати додаткові ресурси у налаштування шлюзів, API та інтеграційних платформ. У теоретичному аспекті така ситуація перешкоджає створенню дійсно відкритої, інтероперабельної інфраструктури безпеки.

Іншою проблемою є високий рівень залежності від підключення до Інтернету. Багато сучасних систем передбачають надсилання тривожних сповіщень, керування сценаріями або отримання оновлень лише через хмарні сервіси. У випадку перебоїв у мережі, збоїв у роботі провайдера або кіберзагроз на рівні каналів зв’язку, система може частково або повністю втратити свою функціональність. Це особливо критично для об’єктів, які не мають постійного доступу до інтернету або розташовані у місцевостях зі слабким покриттям. В умовах воєнного часу або надзвичайних ситуацій ця проблема набуває ще більшої актуальності.

Окремим блоком обмежень виступає питання інформаційної безпеки IoT-пристроїв. Через обмежені апаратні ресурси більшість сенсорів та виконавчих механізмів не підтримують повноцінні криптографічні протоколи або складні алгоритми аутентифікації. Це відкриває можливості для атак типу перехоплення трафіку, спуфінгу, підміни даних, віддаленого вимкнення пристроїв. Часто виробники не передбачають регулярне оновлення прошивки, що унеможливлює оперативне реагування на виявлені вразливості. У довгостроковій перспективі така ситуація загрожує масштабними кіберінцидентами з фізичними наслідками.

До технічних проблем також слід віднести обмежений час автономної роботи пристроїв, особливо в тих випадках, коли системи розгортаються на об’єктах без постійного електропостачання або у важкодоступних місцях. Попри розвиток

технологій енергозбереження та використання літієвих батарей, більшість пристроїв потребує регулярного обслуговування, що не завжди можливо в оперативному режимі. Недостатня автономність знижує загальну надійність системи й підвищує витрати на експлуатацію.

Ще однією проблемою, яка має не лише технічне, але й організаційне підґрунтя, є перевантаженість користувача інформацією. Багато IoT-систем надсилають надмірну кількість сповіщень про події, включно з малозначущими або фоновими. Це призводить до ефекту «ігнорування тривог» – коли користувач перестає реагувати навіть на важливі повідомлення. Відсутність інтелектуального фільтрування та персоналізації реакцій часто є наслідком спрощеної логіки прийняття рішень і неможливості адаптації системи до реального сценарію використання.

Не менш суттєвими є й економічні обмеження. Високовартісні професійні системи недоступні для більшості приватних користувачів або невеликих підприємств. У той же час, дешевші рішення часто не відповідають базовим критеріям надійності або потребують додаткових витрат на налаштування, інтеграцію та підтримку. Відсутність системних механізмів державного стимулювання впровадження таких технологій на локальному рівні (наприклад, у школах чи муніципальних закладах) також обмежує поширення безпечних рішень у публічному секторі.

Суттєвою проблемою, особливо в українському контексті, є нестача фахівців, здатних проєктувати, впроваджувати та обслуговувати IoT-системи. Навіть наявність якісної техніки не гарантує ефективної реалізації проекту без відповідного людського ресурсу. Освітні програми лише починають включати тематику IoT у свої курси, тому професійна підготовка значно відстає від темпів технологічного розвитку.

Зрештою, окремим обмеженням, що має соціальний характер, є психологічне несприйняття або недовіра користувачів до повністю автоматизованих систем. Частина споживачів вважає, що контроль безпеки повинен залишатись у руках людини. Інші бояться втратити приватність через постійний моніторинг, камери або мікрофони, що є складовими IoT-систем. Цей чинник особливо актуальний у

Європі, де діють жорсткі нормативи захисту персональних даних (зокрема, GDPR), а в Україні – у зв’язку з низьким рівнем цифрової довіри та обізнаності.

Отже, незважаючи на стрімкий розвиток технологій та зростання інтересу до IoT-рішень у сфері безпеки, сучасні системи мають низку комплексних обмежень, які впливають на їхню ефективність, масштабованість та рівень впровадження. Усвідомлення цих обмежень є основою для формування стратегії вдосконалення – технічного, нормативного, економічного та соціального – що і стане предметом подальшого аналізу у наступному підпункті.

3.6 Перспективні напрями розвитку систем фізичної безпеки з використанням Інтернету речей

Інтенсивний розвиток технологій Інтернету речей у поєднанні зі зростанням безпекових викликів на побутовому, корпоративному та державному рівнях формує нову парадигму проєктування систем фізичної безпеки. Існуючі рішення демонструють значний потенціал, проте їхній розвиток не зупиняється – навпаки, він супроводжується постійним вдосконаленням технічної архітектури, алгоритмів аналізу даних та засобів інтеграції з іншими цифровими системами. У цьому контексті окреслюються основні перспективні напрями, які визначатимуть майбутнє цієї галузі в найближчі роки.

Одним із пріоритетних напрямів є інтеграція штучного інтелекту (ШІ) у системи фізичної безпеки. Якщо раніше IoT-рішення були переважно реактивними – тобто здійснювали дії лише у відповідь на конкретні події, – то новітні підходи передбачають проактивну логіку. Це означає, що система не лише фіксує вторгнення або зміну параметрів середовища, але й прогнозує їхню ймовірність на основі попередніх даних. Такі функції вже частково реалізовані в системах типу Verkada, які використовують відеоаналітику для розпізнавання підозрілої поведінки. У перспективі можна очікувати масового впровадження локальних моделей машинного навчання, які будуть здатні адаптуватися до конкретного середовища без надмірної залежності від хмари.

Наступним напрямом є розвиток периферійних (edge) обчислень, які дозволяють обробляти дані безпосередньо на пристроях або локальних вузлах мережі, мінімізуючи затримку та зменшуючи навантаження на центральний сервер. Це особливо актуально для систем безпеки, де швидкість реагування має вирішальне значення. Наприклад, у разі виявлення диму або відкриття дверей у заборонений час система повинна діяти негайно, навіть без підключення до інтернету. Edge-компоненти вже впроваджуються в системах, орієнтованих на промислові об’єкти та розподілену інфраструктуру, проте їхнє подальше удосконалення дозволить зробити безпеку доступнішою для широкого кола користувачів.

Ще один перспективний вектор розвитку стосується застосування багатофакторної сенсорики. Ідея полягає у поєднанні даних з кількох різних сенсорів (руху, температури, шуму, вібрації, відео) для підвищення достовірності виявлення загроз. Замість того щоб реагувати на окремий сигнал, система аналізує комплексну картину та формує ймовірнісний висновок про подію. Це значно знижує кількість хибних спрацювань і дозволяє забезпечити більш диференційовану реакцію: наприклад, увімкнення запису лише при комбінації нетипового шуму та теплового сліду. Теоретично така підсистема може стати стандартною для майбутніх IoT-рішень у багатоквартирних будинках, офісних центрах та закладах освіти.

У контексті енергоефективності та сталого розвитку все більшого значення набуває використання автономних та енергонезалежних IoT-пристроїв. Мова йде не лише про традиційне живлення від акумуляторів, а й про застосування сонячних панелей, термоелектричних генераторів та інших джерел мікроенергії. Це дозволяє розгортати охоронні системи навіть у віддалених регіонах або у тимчасових спорудах без інфраструктури. У країнах з нестабільним електропостачанням такі рішення вже зараз стають незамінними, і в майбутньому очікується поява повністю самодостатніх модулів охорони, які працюватимуть роками без заміни джерела живлення.

Також важливим напрямом розвитку є підвищення прозорості та довіри до систем через впровадження технологій блокчейн для збереження подій та логу

активності. Ідея полягає у створенні незмінного журналу безпекових подій, який не може бути підроблений або змінений заднім числом. Це особливо актуально для юридично значимих ситуацій: наприклад, у випадках правопорушень або спорів щодо доступу до приміщень. Теоретично блокчейн може застосовуватись не лише як засіб фіксації, а й як інструмент контролю доступу, з прозорими умовами авторизації користувачів.

Окремо слід зазначити перспективу державної стандартизації та масового впровадження у публічний сектор, зокрема в системи безпеки шкіл, медичних закладів, бібліотек, музеїв. Сьогодні значна частина таких об’єктів використовує застарілі рішення або взагалі не має систем охорони. Створення уніфікованих державних протоколів підключення, шаблонів проєктування та фінансових механізмів підтримки дозволить вивести системи безпеки у публічному просторі на якісно новий рівень. У цьому напрямі доцільним є вивчення досвіду країн Європейського Союзу, де вже діють відповідні програми (наприклад, Smart Building Initiative).

Не менш важливим залишається розвиток етичних, нормативних та соціально прийнятних моделей впровадження систем. Це включає захист приватності, мінімізацію ризику зловживань, роз’яснювальну роботу серед населення, забезпечення прозорості використання відеоспостереження. У майбутньому саме ті системи, що поєднуватимуть технічну ефективність із соціальною легітимністю, матимуть найкращі шанси на масове прийняття.

Таким чином, розвиток IoT-систем фізичної безпеки не обмежується лише вдосконаленням окремих пристроїв або розширенням їх технічних можливостей. Йдеться про комплексну трансформацію підходів до організації безпеки як такої – від традиційного пасивного фіксування подій до активного прогнозування потенційних загроз; від централізованої логіки обробки сигналів до розподілених і самодостатніх вузлів ухвалення рішень; від користувацької недовіри та обмеженого прийняття технологій до прозорих, етичних і соціально відповідальних моделей впровадження. Цей перехід вимагає не лише технічних інновацій, а й глибокого переосмислення ролі людини в контурі безпеки, підвищення цифрової грамотності користувачів, формування стандартів взаємодії

між платформами, а також правового врегулювання питань приватності, відповідальності та контролю.

Перспективні напрями відкривають широкі можливості як для подальших наукових досліджень у сфері кіберфізичних систем, машинного навчання, мережевої безпеки, так і для інженерних рішень, орієнтованих на створення гнучких, масштабованих і стійких до відмов платформ. Також актуальним стає міждисциплінарний підхід до інтеграції IoT-систем безпеки – на перетині інформатики, електроніки, соціології та права. Саме у такій синергії закладено потенціал подальшого впровадження новітніх безпекових рішень у загальну цифрову екосистему сучасного суспільства – екосистему, в якій технології не лише обслуговують, а й активно захищають людське життя, майно та інформацію.

З урахуванням стрімкого зростання кількості пристроїв, підключених до мережі, особливого значення набуває питання стійкості таких систем до зовнішніх впливів – як з боку зловмисників, так і з точки зору технічних збоїв. Системи безпеки повинні не лише ідентифікувати загрози в реальному часі, а й адаптуватися до змін у середовищі, що досягається шляхом впровадження самонавчальних алгоритмів. У цьому контексті все більшої ваги набуває концепція edge computing, яка дозволяє обробляти дані безпосередньо на місці їх виникнення, зменшуючи затримки та підвищуючи автономність систем. Поєднання зазначених технологічних тенденцій формує основу для побудови нової генерації інтелектуальних систем захисту, здатних ефективно функціонувати в умовах зростаючої складності цифрового середовища.

Такі рішення є основними для формування довіри до цифрових сервісів та інфраструктури. Вони сприяють зміцненню національної та корпоративної кібербезпеки. Надалі очікується активне впровадження подібних технологій у критично важливих галузях – енергетиці, транспорті, медицині та обороні.

ВИСНОВКИ

Проблематика фізичної безпеки приміщень набуває дедалі більшої ваги в умовах зростання ризиків, пов’язаних із урбанізацією, енергетичною нестабільністю, соціальною напруженістю та кіберзагрозами. У таких обставинах стає очевидним, що класичні методи охорони, засновані переважно на людському факторі та автономних елементах контролю (сигналізація, відеоспостереження, охоронці), поступово вичерпують свій потенціал. Натомість новітні технології Інтернету речей відкривають принципово нові підходи до організації систем фізичної безпеки, де ключову роль відіграє не лише детекція загроз, а й гнучке реагування, аналітика та самонавчання системи.

У рамках цього дослідження було здійснено цілісний аналіз архітектур, протоколів, апаратних і програмних складових, що формують основу сучасних IoT-систем безпеки. Обґрунтовано, що основними перевагами таких рішень є розподілена структура, здатність до автономної роботи, масштабованість, можливість інтеграції з іншими цифровими платформами, зокрема системами відеоспостереження, розумного освітлення, пожежогасіння, клімат-контролю, а також мобільними застосунками. Також підтверджено, що ефективна система має базуватись на принципах модульності, енергоефективності, багатоканальної комунікації та підтримки відкритих стандартів.

Найбільшу цінність для прикладного впровадження мають ті рішення, які поєднують декілька рівнів безпеки – фізичний, інформаційний, організаційний та поведінковий. Разом з тим, більшість систем на ринку мають обмеження: вони або занадто дорогі, або складні в інтеграції, або вимагають постійного доступу до Інтернету, що не завжди можливо в українських реаліях.

Виявлено також ряд системних проблем, які стримують ефективну реалізацію IoT-рішень у сфері фізичної безпеки. Серед них – фрагментація платформ і протоколів, вразливість до атак на рівні комунікацій, складність у налаштуванні взаємодії між компонентами, високе енергоспоживання деяких модулів, а також обмежена автономність пристроїв. Особливо актуальними залишаються питання захисту даних користувача, запобігання вторгненням у

приватне життя, забезпечення довіри до цифрових систем у публічному просторі.

Разом з тим, виявлені у дослідженні перспективи розвитку дозволяють стверджувати, що інтеграція IoT у сферу фізичної безпеки продовжить прискорюватись. Очікується масове впровадження edge-computing-пристроїв, які зможуть здійснювати обробку подій на місці без передачі в хмару, що дозволить системам працювати навіть за відсутності інтернету. Важливою тенденцією є впровадження штучного інтелекту, що дозволяє зменшити кількість хибних спрацювань, виявляти аномалії, прогнозувати потенційні загрози ще до їх реалізації. Перспективними є також енергонезалежні модулі, побудовані на основі сонячної або теплової генерації, блокчейн-реєстрація подій для гарантування цілісності логів, адаптивні сценарії поведінки на основі багатофакторної сенсорики.

Не менш важливим напрямом є розвиток національної інфраструктури безпеки в публічному секторі. Стандартизація IoT-рішень для шкіл, дитсадків, бібліотек, закладів охорони здоров'я – це крок до масштабного впровадження ефективних і доступних систем безпеки, які не лише фіксують події, а й підвищують загальний рівень захищеності соціуму. Подібні ініціативи вже реалізуються у провідних країнах світу, і мають потенціал до запровадження в Україні.

Результати цього дослідження становлять практичну цінність як для розробників IoT-систем, так і для фахівців у сфері інформаційної безпеки, проєктантів, аналітиків та осіб, відповідальних за охорону об'єктів інфраструктури. Узагальнення основних тенденцій, викликів і рішень, що представлені в роботі, дає змогу сформувати чітке бачення ефективної, гнучкої, етичної та надійної системи фізичної безпеки нового покоління. Така система повинна бути не просто реактивною, а проактивною, не лише фіксувати події, а й попереджати їх, не лише наглядати, а й захищати.

Підсумовуючи, можна впевнено констатувати, що Інтернет речей вже сьогодні змінює фундаментальні принципи фізичної безпеки приміщень, формуючи технологічно зріле середовище, здатне відповідати викликам сучасного світу.

СПИСОК ДЖЕРЕЛ ПОСИЛАННЯ

1. Шутий М. Сутність і зміст фізичного захисту підприємств та організація забезпечення фізичного захисту. Вісник Національного університету «Львівська політехніка». Львів : Видавництво Львівської політехніки, 2017. № 865. С. 362–365. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2018/jun/13391/57.pdf (дата звернення: 21.02.2025).

2. Suzanne Niles Physical Security in Mission Critical Facilities : white paper : Schneider Electric’s Data Center Science Center, 2015. Rev. 2. 22 p. URL: https://bit.ly/3N3pg4p (дата звернення: 22.02.2025).

3. John Kingsley-Hefty Physical Security Strategy and Process Playbook. 1st Edition : Elsevier, 2013. 160 p (дата звернення: 22.02.2025).

4. Bagchi, S. N., Sharma, R. Rethinking Security Paradigms in the Face of External Backlash: A Case Study in Private Security. URL: https://doi.org/10.1177/025609092412921 (дата звернення: 22.02.2025).

5. Шакуров Є. О. Поняття «Інтернет речей», способи застосування та технології побудови «Інтернету речей» / Є. О. Шакуров, О. С. Балюк // Наумовські читання : зб. тез доп. учасників XX Всеукр. наук.-метод. конф. здобувачів вищ. освіти та молодих вчених, присвяч. 300-річчю з дня народж. Г. С. Сковороди, Харків, 3–4 листоп. 2022 р. / Харків. нац. пед. ун-т ім. Г. С. Сковороди ; [за заг. ред. О. А. Жерновникової]. – Харків : [б. в.], 2022. – С. 191–193.

6. Самойленко М. Ю. Принципи застосування технології Інтернет речей у сучасному світі техніки // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. – 2020. – Т. 31, № 6(1). – DOI: https://doi.org/10.32838/TNU-2663-5941/2020.6-1/24 (дата звернення: 22.02.2025).

7. Технології інтернету речей. Навчальний посібник навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.

8. Бабенко Т. В., Лютий О. І., Петренко А. І. Поняття Інтернету речей з точки зору інформаційної безпеки // Міжнародна безпека: економіка, політика, право : зб.

наук. пр. – Київ : КНЕУ, 2023. – Вип. 1 (98). – С. 4–11. – DOI: 10.33111/mise.98.1 (дата звернення: 23.02.2025).

9. Гіль А. Промислові інтерфейси та протоколи передачі даних інтегрованих систем для автоматизованого управління в умовах Industry 4.0 / А. Гіль, О. Чала, О. Филипенко // Виробництво & Мехатронні Системи 2021 : матеріали V-ої Міжнар. конф., 21-22 жовтня 2021 р. - Харків, 2021. - С. 127-130.

10. IoT панелі управління: ключові вимоги та функції для моніторингу пристроїв. URL: https://wezom.com.ua/ua/blog/iot-paneli-upravlinnya (дата звернення: 10.03.2025).

11. Киричек Г. Г., Пестов О. Д. Система віддаленого керування об’єктами критичної інфраструктури // Системи і технології. – 2024. – Т. 68, № 2. – С. 63–70. – DOI: 10.32782/2521-6643-2024-2-68.7. – Режим доступу: https://journals.uran.ua/index.php/2521-6643 (дата звернення: 15.03.2025).

12. Stergiou C., Psannis K. E., Kim B.-G., Gupta B. Secure integration of IoT and Cloud Computing // Future Generation Computer Systems. – 2016

13. Захист від вторгнення, пожежна безпека, відеоспостереження, комфорт і автоматизація. Усе в єдиній системі Ajax. URL: https://ajax.systems/ua (дата звернення: 15.03.2025).

14. Google's Nest Secure Has Fully Shut Down: We've Got Answers if You're Worried. URL: https://www.cnet.com/home/security/googles-nest-secure-has-fully-shut-down-weve-got-answers-if-youre-worried/ (дата звернення: 20.03.2025).

15. Представлено новий мікроконтролер Raspberry Pi Pico 2 W з підтримкою Wi-Fi 2,4 ГГц та Bluetooth 5.2. URL: https://mezha.media/2024/11/25/raspberry-pi-pico-2-w-release/ (дата звернення: 27.03.2025).

16. Мікроконтролер ESP32. URL: https://itmaster.biz.ua/directory/microcontrollers/esp32.html (дата звернення: 5.04.2025).

17. ТОП-7 західних компаній альтернатив Hikvision та Dahua в Україні URL: https://kristall-systems.net.ua/ua/novosti/top_7_alternative_dahua_hikvision/ (дата звернення: 10.04.2025).

18. Sultana T., Wahid K. IoT-Guard: Event-Driven Fog-Based Video Surveillance

System for Real-Time Security Management // IEEE Access. – 2019. – Vol. 7. – P. 134558–134567. – DOI: 10.1109/ACCESS.2019.2941978 (дата звернення: 10.05.2025).

19. Mohamed K. IoT Networking and Communication Layer // The Era of Internet of Things / eds. K. S. Sree, M. V. Krishna Rao. – Cham : Springer, 2019. – DOI: 10.1007/978-3-030-18133-8_3 (дата звернення: 17.05.2025).

20. Волошко А. В., Макаренко А. О. Використання сенсорних пристроїв у поєднанні з алгоритмами комп'ютерного зору для покращення систем відслідковування руху // Наукові записки Державного університету телекомунікацій. – 2024. – № 1(5). – С. 11–18. – DOI: 10.31673/2786-8362.2024.010202 (дата звернення: 20.05.2025).

21. Lee S., Kim H., Hong D. K., Ju H. Correlation analysis of MQTT loss and delay according to QoS level // Proceedings of the 2013 IEEE International Conference on Information Networking (ICOIN). – 2013. – P. 714–717.

22. Токаренко О. В., Богомазов С. А. Розробка програмного забезпечення мережевої системи збору даних на основі протоколу CoAP // Погляд у майбутнє приладобудування : матеріали XIII Всеукр. наук.-практ. конф. студентів, аспірантів та молодих вчених, 13–14 травня 2020 р. – Київ : КПІ ім. Ігоря Сікорського, 2020. – С. 393–395.

23. Herrero R. Application Layer // Textbooks in Computer Science. – Published online: 24 June 2021. – DOI: 10.1007/1-4020-0613-6_762 (дата звернення: 01.06.2025).

24. Порівняння Zigbee, Z-wave і WiFi: що найкраще? URL: https://surl.li/rolyqg (дата звернення: 1.06.2025).

25. Ozerchuk I. Bluetooth Low Energy, as the basis of data transmission with ultra-low energy consumption / I. Ozerchuk // Computer-Integrated Technologies: Education, Science, Production. – 2023. – № 51. – С. 174–180. – DOI: https://doi.org/10.36910/6775-2524-0560-2023-51-22 (дата звернення: 5.06.2025).

26. https://ibps.iitk.ac.in/sathee-bank-exam/student-corner/ncertbooks/class-11/information-practices/chapter-02 emergingtrends/ URL:https://french.alibaba.com/g/milesight-iot.html (дата звернення: 2.06.2025).

27. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things architecture, possible applications and key challenges. 2012 10th International Conference on Frontiers of Information Technology, 257–260.

28. Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1), С.49–69.

29. Li, S., Xu, L. D., & Zhao, S. (2015). The Internet of Things: A survey. *Information Systems Frontiers*, 17(2), 243–259.

30. Елементи і пристрої фізичної та електронної охорони об'єктів: Конспект лекцій / П. В. Мокренко; Нац. ун-т «Львів. політехніка». — Л. : Фенікс, 2000. — 186 с. — Бібліогр.: 27 назв.

31. ETSI TS 102 690 «Machine-to-Machine communications (M2M); Functional architecture» [електронний ресурс], V1.1.1. – 2011. – 280 p.

32. Jerker D. IoT Automation: Arrowhead Framework, Great Britain: CRC Press, 2017. – 366 p.

33. McEwen A. Designing the Internet of Things, USA: Publishing NT, 2013.

34. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.

35. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), С. 2787–2805.

36. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), С. 1645–1660.

37. Гринишин, М. Т., & Хома, В. В. (2019). Застосування технологій Інтернету речей для забезпечення безпеки об’єктів. Наукові записки Тернопільського національного технічного університету імені Івана Пулюя, 2(54) – С. 87–94.

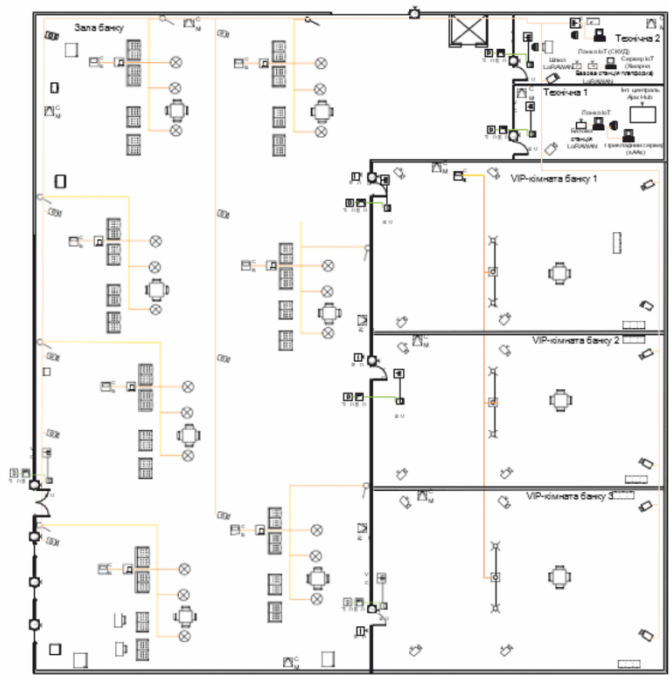
38. Кравець, П. О., & Лозинський, О. М. (2020). Інтернет речей: Технології, застосування та виклики безпеки. Вісник Національного університету "Львівська політехніка". Серія: Комп'ютерні науки та інформаційні технології, (911), 123–130.

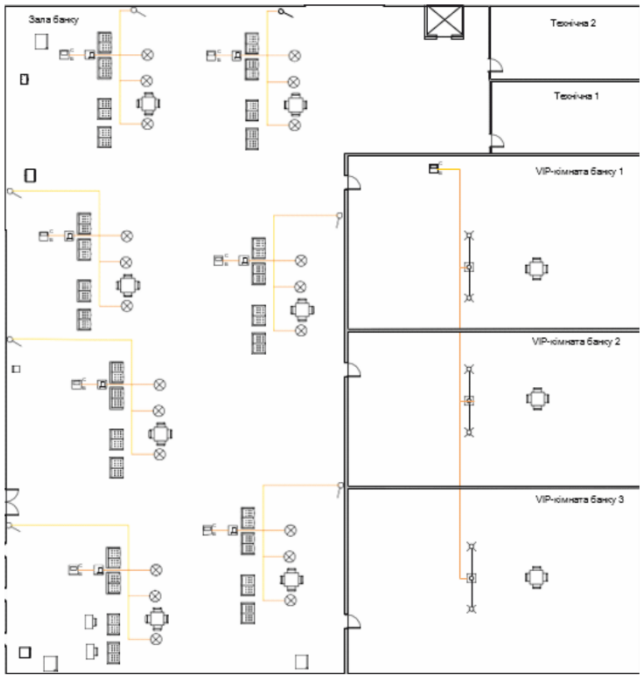
39. Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 4(1), С. 65–88.

40. Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1), С. 49–69.

ДОДАТОК А

Копії графічної частини





КРБКБ.2102151.21.02.30 Е8

					КРБКБ.2102151.21.02.30 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Система забезпечення фізичної безпеки приміщення на основі технології Інтернету речей	Літ.	Маса	Масштаб
Розроб.		Єщенко В.І.				У		
Перевір.		Єщенко М.М.						
Т.контр.					Комплексне креслення	Аркуш	Аркушів 1	
Н.контр.		Мостовий С.В.				ХНУ, КБ-21-2		
Затверд.		Ільєв Ю.П.						

Назва системи	Походження	Типова архітектура	Захищеність каналів зв'язку	Інтеграція з іншими системами	Приклади використання
Ajax Systems	Україна	Хаб + сенсори + хмара	AES-128, Jeweller	Часткова (через API)	Приватні будинки, банки, школи
Google Nest Secure	США	Хмара + IoT-пристрої	HTTPS, TLS	Повна (через Google Home)	Квартири, смарт-будинки
Bosch Security	Німеччина	Централізована, IP-зв'язок	Промислові стандарти	Повна (включно з BMS)	Аеропорти, логістичні хаби
Raspberry/ESP32 DIY	Відкриті рішення	Децентралізована, локальна	Залежить від реалізації	Можлива через MQTT/HTTP	ОСББ, лабораторії, малі офіси
Verkada	США	Хмара + AI-аналітика	AES-256, сертифікати	Висока, з AI-обробкою	Університети, офіси, кампуси

КРБКБ.2102151.21.02.30 Е8
Контролер освітлення
Драйвер
Вимикач
Лампа освітлення
ПК
СерверIoT
Базова станція LoRAWAN
IoT-камера
"Розумна" Розетка (Command Spot)
ПК
Сервер (реєстратор)
Комутатор каналів
Купольна IP-камера
ПК
Маршрутизатор
Комутатор каналів
PTZ-камера
ПК
Базова станція LoRAWAN
Шлюз LoRAWAN
Зчитувач Proxy-карт
Зчитувач Touch-memory
Комутатор TECSTAR TS-41
ПК
Контролер ZKTECO INB10260
Кнопка
Зчитувач
Електромагнітний замок
КРБКБ.2102151.21.02.30 Е8
Комплексне креслення
ХНУ, КБ-21-2

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Кривчака Вадима Ігоровича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-21-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

10.06.25
дата

підпис

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Кривчак Вадим Ігорович

Співавтор:

Назва: Система забезпечення фізичної безпеки приміщення на основі технології "Інтернет речей»

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1.6%

Коефіцієнт подібності 2:0.2%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-16 13:08:57.0

Після аналізу Звіту подібності констатую наступне:

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

16.06.2025р.

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 0.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 8%**

	Document		Sum coincidence on the DB	
ID: 246025 Title: Система забезпечення фізичної безпеки приміщення на основі технології "Інтернет речей» Added in a DB: 2025-06-16 Authors: Кривчак Вадим Ігорович Heads: Касянчук М.М. Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	79978	514	608 (1%)	7 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система забезпечення фізичної безпеки приміщення на основі технології Інтернету речей

Автор: Кривчак Вадим Ігорович

Спеціальність: 125 – Кібербезпека

Освітня програма:Кібербезпека

Науковий керівник:Михайло Касянчук, док.техн. наук

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 99%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 97,7%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Михайло КАСЯНЧУК

Гарант ОП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студента Кривчак Вадим Ігорович

Тема Система забезпечення фізичної безпеки приміщення на основі технології Інтернету речей

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 1; кількість сторінок записки 66.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі, відповідно до поставленого завдання, проведене дослідження предметної області, проаналізовано та розглядається сучасні виклики проектування систем приміщенняо. У підсумку визначено принципи роботи систем контролю доступу з акцентом на комбіновану ідентифікацю особи, включаючи біометричні методи.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі виконано завдання на достатньому рівні. Матеріали оформлені згідно вимог стандартів.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У розділі 1 було провдено аналіз фізичних загроз, які актуальні для приміщень. Особливу увагу приділено комбінованим загрозам. У розділі було запропоновано концептуальну модель IoT-системи фізичної безпеки.У 3 розіділі окреслено перелік вимог до ефективної IoT-системи безпеки.

4. Позитивні сторони роботи Робота базується на детальному аналізі вимог до безпеки IoT-системи. Кваліфікаційна робота має практичну цінність і орієнтована на вдосконалення захисту.

5. Негативні сторони роботи В роботі недостатньо уваги приділено розробці технічних характеристик автоматизованої, що підлягає захисту, та деталізації прийнятих проєктних рішень

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні сторони кваліфікаційної роботи, а також негативні сторони і загальну якість роботи, рекомендованою оцінкою є «задовільно»

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Нічепорук Андрій Олександрович
Кандидат тех. наук, доцент кафедри комп'ютерної інженерії та інформаційних систем

« 10 » 06 2025. (підпис)