ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Інтегрована система моніторингу безпеки IoT-пристроїв на базі технології AJAX»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

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

_____ *Олександр НЕЧАЙ*

Виконав:
здобувач вищої освіти
група ІСД-42
Олександр НЕЧАЙ

Керівник:
науковий ступінь, вчене звання
Оксана ТКАЛЕНКО
к.т.н., доцент

Рецензент:
науковий ступінь, вчене звання
_____
Ім’я, ПРІЗВИЩЕ

Київ – 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інформаційних систем та технологій

Ступінь вищої освіти Бакалавр

Спеціальність Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІСТ

_____Каміла СТОРЧАК
«____» _____20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ СТУДЕНТУ
Нечай Олександру Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: «Інтегрована система моніторингу безпеки IoT-пристроїв на базі технології AJAX»

керівник кваліфікаційної роботи Оксана ТКАЛЕНКО, к.т.н., доцент
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від «24» лютого 2025 року № 56.

2. Строк подання кваліфікаційної роботи: 12 травня 2025 року.

3. Вихідні дані до кваліфікаційної роботи: моніторинг безпеки IoT-пристроїв на базі технології AJAX;
науково-технічна література з питань.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Поставновка завдання: визначення потреби, загроз та розроблення інтегрованої системи моніторингу;
2. Архітектура системи: вибір системи Ajax, апаратне та програмне забезпечення;
3. Реалізація та тестування: збірка, тестування, аналіз.

5. Перелік ілюстративного матеріалу: *презентація*
   1. Основні сфери застосування IoT.
   2. Пристрої системи безпеки Ajax.
   3. Аналіз аналогів Ajax.
   4. Процес налаштування Ajax Hub.
   5. Процес налаштування Ajax Hub.
   6. Збірка та налаштування компонентів контролера.

6. Дата видачі завдання: 24 лютого 2025 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	20.02 – 11.03.25	
2	Сутність проблеми технології IoT.	11.03 – 12.04.25	
3	Огляд та порівняння та наліз технологій.	12.04 – 21.04.25	
4	Рекомендації щодо розроблення інтегрованої системи моніторингу	21.04 – 09.05.25	
5	Збір і аналіз результатів тестування.	09.05 – 13.05.25	
7	Оформлення роботи: вступ, висновки, реферат	13.05 – 23.05.25	
8	Розробка демонстраційних матеріалів	23.05. – 25.05.25	

Здобувач вищої освіти _____ Олександр НЕЧАЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи
кваліфікаційної роботи _____ Оксана ТКАЛЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 65 стор., 20 рис., 7 табл., 18 джерел.

Мета роботи – – розробка рекомендацій щодо створення інтегрованої системи моніторингу безпеки IoT-пристроїв на базі AJAX для ефективного контролю, захисту та відстеження даних у реальному часі.

Об'єкт дослідження – інтегровані системи моніторингу безпеки для IoT-пристроїв.

Предмет дослідження – особливості розроблення, впровадження та захисту інтегрованої системи моніторингу IoT-пристроїв на основі технології AJAX.

Короткий зміст роботи: присвячена розробці інтегрованої системи моніторингу безпеки IoT-пристроїв з використанням технології AJAX. У дослідженні проаналізовано сучасні загрози, пов’язані з Інтернетом речей, зокрема несанкціонований доступ, витоки даних, DDoS-атаки, та запропоновано архітектуру системи, що дозволяє ефективно виявляти та запобігати цим загрозам у реальному часі. Підвищений акцент зроблено на використанні технології AJAX для асинхронного обміну даними, що забезпечує високу швидкість реакції системи, інтерактивність та зручність моніторингу. У роботі також порівнюються AJAX із альтернативними рішеннями, аналізується його практичне застосування в системах безпеки Ajax Systems, та наводяться рекомендації щодо впровадження, масштабування і захисту інтегрованих IoT-систем.

КЛЮЧОВІ СЛОВА: AJAX ТЕХНОЛОГІЯ, БЕЗПЕКА ІОТ-ПРИСТРОЇВ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ТЕХНОЛОГІЇ ЗАХИСТУ, ІОТ-БЕЗПЕКА, МОНІТОРИНГ КІБЕРЗАГРОЗ, СИСТЕМА УПРАВЛІННЯ БЕЗПЕКОЮ, КОНТРОЛЬ ДОСТУПУ, АВТОМАТИЗОВАНЕ РЕАГУВАННЯ, АУТЕНТИФІКАЦІЯ ІОТ-ПРИСТРОЇВ.

ЗМІСТ

ВСТУП

Актуальність дослідження. Сучасний розвиток Інтернету речей (IoT) значно вплинув на багато сфер діяльності, зокрема промисловість, медицину, транспорт, а також на повсякденне життя людей. IoT-пристрої забезпечують обмін даними між об'єктами без необхідності прямої участі людини, що відкриває нові можливості для автоматизації та підвищення ефективності процесів. Однак, водночас з ростом популярності IoT постають питання безпеки: зокрема, захисту даних, забезпечення приватності користувачів і надійності передачі інформації в умовах загроз з боку кіберзлочинців.

Безпека IoT-пристроїв стає критично важливим завданням, оскільки вразливості цих пристроїв можуть бути використані для несанкціонованого доступу, розкрадання особистих і комерційних даних, а також для здійснення атак на інші мережі. У зв'язку з цим виникає потреба в інтегрованих системах моніторингу, які забезпечували б постійний контроль за станом IoT-пристроїв та негайно реагували б на потенційні загрози.

Використання технології AJAX для створення інтегрованої системи моніторингу безпеки дозволяє здійснювати асинхронний обмін даними з IoT-пристроями в режимі реального часу. Це забезпечує ефективність у відстеженні й аналізі даних, швидке реагування на інциденти безпеки та значне зменшення навантаження на мережу. Дослідження технологічних можливостей AJAX для моніторингу та розробка на її основі захищеної інтегрованої системи актуальні для створення надійної інфраструктури безпеки в мережах IoT, що відповідає сучасним вимогам безпеки.

Метою роботи розроблення рекомендацій щодо створення інтегрованої системи моніторингу безпеки IoT-пристроїв на базі технології AJAX, що дозволить забезпечити ефективний контроль, захист та відстеження даних у режимі реального часу.

Для досягнення поставленої мети необхідно виконати наступні *завдання*:

– вивчити особливості технології IoT та основні загрози безпеки,

пов’язані з IoT-пристроями;

– провести огляд та аналіз технології AJAX і можливостей її використання для моніторингу даних у реальному часі;

– порівняти технологію AJAX з аналогами для вибору оптимального рішення для моніторингу IoT-пристроїв;

– запропонувати методи захисту даних у системі моніторингу, що забезпечать безпечну передачу та зберігання інформації;

– розробити рекомендації щодо інтегрованої системи моніторингу безпеки IoT-пристроїв на базі технології AJAX.

Об'єкт дослідження - процес інтегрованої системи моніторингу безпеки для IoT-пристроїв.

Предметом дослідження є особливості розроблення, впровадження та захисту інтегрованої системи моніторингу IoT-пристроїв на основі технології AJAX.

Методи дослідження: аналіз літературних джерел та наукових публікацій з питань безпеки та використання AJAX; порівняння технологія для визначення оптимальних рішень щодо моніторингу й захисту; тестування системи на предмет продуктивності та захищеності

Наукова новизна отриманих результатів: розроблено концепцію інтегрованої системи моніторингу безпеки IoT-пристроїв на основі технології AJAX, що дозволяє забезпечити асинхронний обмін даними у режимі реального часу. В роботі вперше систематизовано підходи до поєднання AJAX-технологій із архітектурою IoT-систем для підвищення ефективності моніторингу кіберзагроз та оперативного реагування.

Практична значущість кваліфікаційної бакалаврської роботи. Результати дослідження можуть бути використані при впровадженні систем захисту IoT-пристроїв у розумних будинках, промислових об'єктах, медичних установах тощо. Запропоновану архітектуру можна адаптувати для реальних рішень у сфері інформаційної безпеки. Крім того, матеріали роботи можуть слугувати навчальною базою для студентів та фахівців у галузі IoT, AJAX-технологій та кібербезпеки.

Апробація результатів бакалаврської роботи:

1. Нечай О.С. «Застосування технологій іот для "розумного будинку" та "розумного міста"». Тези доповіді на ІІ Всеукраїнській науково-технічній конференції «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу» Київ, 18 листопада 2024 року.

1 АНАЛІЗ ОСНОВ БЕЗПЕКИ IoT-ПРИСТРОЇВ І ТЕХНОЛОГІЇ AJAX

1.1 Сутність та особливості технології IoT

Internet of Things (IoT), або Інтернет речей – це концепція, яка передбачає підключення фізичних пристроїв до інтернету, щоб вони могли взаємодіяти один з одним, збирати, обробляти та обмінюватися даними без участі людини. Це може включати різні пристрої, такі як датчики, побутова техніка, транспортні засоби, камери спостереження, розумні годинники.

Основним аспектом IoT є підключення пристроїв, які можуть взаємодіяти між собою через Інтернет або локальні мережі. Завдяки сенсорам і мережевим модулям ці пристрої здатні збирати дані про навколишнє середовище, передавати їх на сервери або в хмару, де вони обробляються для прийняття рішень.

Автоматизація є ще одним важливим аспектом IoT. Пристрої можуть виконувати певні завдання самостійно, без втручання людини, базуючись на заданих алгоритмах. Інтеграція є ключовим фактором, який дозволяє об’єднувати різні пристрої в єдину екосистему, наприклад, у розумному домі чи на виробництві. Це забезпечує централізоване управління всіма пристроями через одну платформу.

IoT також забезпечує аналітику великих обсягів даних. Зібрана інформація аналізується за допомогою штучного інтелекту та інших алгоритмів, що дозволяє пристроям приймати рішення в реальному часі. Масштабованість IoT-систем дає змогу легко розширювати їх, додаючи нові пристрої або функції [1].

Безпека і конфіденційність даних є критично важливими аспектами, оскільки пристрої IoT часто працюють з чутливою інформацією. Використання шифрування та механізмів автентифікації допомагає зменшити ризики. Гнучкість IoT дозволяє застосовувати його в різних сферах, таких як медицина, сільське господарство, транспорт чи промисловість. При цьому технології, що лежать в основі IoT, зазвичай енергоефективні, що робить їх ідеальними для автономної роботи.

IoT відкриває бізнесу нові можливості для оптимізації внутрішніх процесів, усуваючи потребу у виконанні рутинних завдань вручну. Завдяки зібраним даним

компанії можуть проводити більш точний аналіз роботи обладнання, виявляти потенційні несправності та своєчасно їх усувати. Це зменшує ризик простоїв, знижує витрати на ремонт і обслуговування, а також позитивно впливає на якість продукції чи послуг. Автоматизація процесів за допомогою IoT значно підвищує ефективність роботи підприємства (рис. 1.1).

Однією з ключових переваг IoT є можливість детального аналізу поведінки клієнтів та їхніх уподобань. Пристрої IoT фіксують взаємодію користувачів із продуктами чи послугами, дозволяючи компаніям створювати більш персоналізовані пропозиції. Це сприяє покращенню клієнтського досвіду, підвищує лояльність і, в кінцевому результаті, збільшує продажі. Глибше розуміння потреб споживачів допомагає адаптувати бізнес до змін на ринку.

IoT забезпечує можливість віддаленого моніторингу бізнес-процесів у реальному часі. Це дозволяє контролювати виробничі лінії, керувати транспортними потоками або відстежувати складські запаси з будь-якої точки світу. Такий підхід підвищує прозорість операцій, забезпечує точність управління і дозволяє приймати оперативні рішення для усунення проблем. Бізнес отримує змогу бути більш гнучким та ефективним у своїй роботі [2].

Інтеграція IoT-систем сприяє зменшенню витрат на використання ресурсів, таких як енергія, вода або сировина. Розумні пристрої можуть автоматично налаштовувати параметри, наприклад, регулювати освітлення чи підтримувати оптимальну температуру в приміщенні, що допомагає знизити споживання енергії. Це не лише сприяє економії, але й відповідає сучасним екологічним стандартам.

На виробництві IoT дає змогу впроваджувати превентивне обслуговування обладнання. Завдяки сенсорам, які збирають дані про стан техніки, компанії можуть прогнозувати збої ще до того, як вони стануть критичними. Це зменшує ризик аварій, підвищує надійність обладнання та скорочує непередбачені витрати.

IoT також створює умови для появи нових бізнес-моделей. Компанії можуть запроваджувати послуги за принципом "оплата за використання" або "продукт як послуга", що розширює можливості для доходу. Це дозволяє бізнесу краще

адаптуватися до змін у споживчих звичках і знаходити інноваційні способи залучення клієнтів.

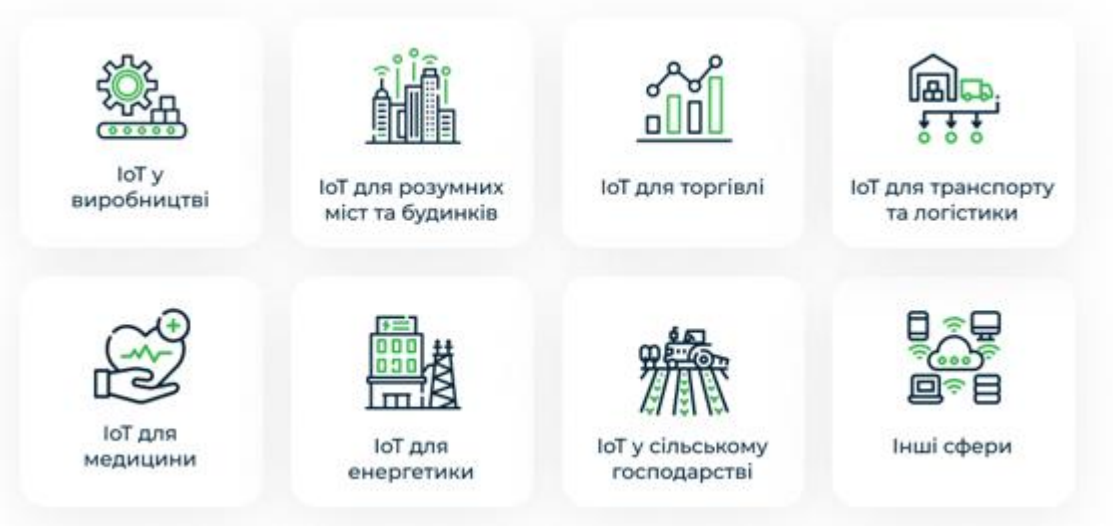


Рис. 1.1 Сфери, в яких використовується Інтернет речей

Основні характеристики IoT

– підключеність – IoT-пристрої підключені до Інтернету або локальних мереж через Wi-Fi, мобільні мережі, Bluetooth чи інші технології;

– сенсори та дані – пристрої оснащені сенсорами, які збирають інформацію про навколишнє середовище (температура, вологість, рух, рівень освітлення тощо);

– аналіз та обробка – дані передаються на сервери або хмарні платформи, де вони аналізуються для прийняття рішень;

– автоматизація – IoT дозволяє пристроям виконувати завдання на основі отриманих даних, наприклад, регулювати температуру в приміщенні або відправляти повідомлення про несправність [3];

Вплив IoT на сучасні технології:

– розумні будинки та міста – IoT трансформує наш побут і міста. Розумні будинки оснащені пристроями для автоматизації освітлення, опалення, систем безпеки та управління побутовою технікою. У розумних містах IoT використовується для управління транспортом, освітленням вулиць, збором сміття і моніторингу навколишнього середовища;

– промисловість 4.0 – IoT є основою Індустрії 4.0, яка спрямована на автоматизацію виробництва. Завдяки IoT виробничі процеси стають більш ефективними, передбачуваними і менш залежними від людського втручання;

– медицина – У сфері охорони здоров'я IoT дозволяє створювати пристрої для моніторингу здоров'я в режимі реального часу. Наприклад, носимі пристрої можуть вимірювати серцевий ритм, рівень цукру в крові або якість сну;

– сільське господарство – IoT допомагає оптимізувати зрошення, моніторинг стану ґрунту і кліматичних умов, що сприяє підвищенню врожайності і зменшенню витрат;

– транспорт і логістика – IoT використовується для управління транспортними засобами, моніторингу вантажів і маршрутизації в реальному часі. Це значно покращує ефективність логістики і зменшує витрати [4].

Переваги IoT для сучасних технологій:

– автоматизація та зниження витрат;

– збільшення ефективності та продуктивності;

– поліпшення якості обслуговування;

– вдосконалення процесів збору і аналізу даних;

– інтеграція фізичних пристроїв у цифрове середовище.

IoT-пристрої (Internet of Things) є основою сучасної автоматизації та розумних технологій. Їх унікальна особливість полягає в тому, що вони здатні працювати автономно, без постійного втручання людини, забезпечуючи безперебійну взаємодію між фізичними об'єктами через мережу. Завдяки цим характеристикам IoT-пристрої трансформують способи взаємодії з навколишнім середовищем, підвищуючи ефективність і спрощуючи рутинні процеси [5].

Однією з ключових функцій IoT-пристроїв є автоматизація. Це означає, що пристрої можуть самостійно виконувати певні завдання, не потребуючи ручного управління. Автоматизація досягається завдяки інтегрованим сенсорам, процесорам і алгоритмам, які забезпечують аналіз даних та прийняття рішень.

– самостійне прийняття рішень – IoT-пристрої збирають дані в реальному часі та обробляють їх за допомогою програмного забезпечення.

Наприклад, розумний термостат може автоматично налаштовувати температуру в приміщенні на основі погодних умов чи уподобань користувача;

– оптимізація ресурсів – Автоматизація дозволяє зменшити споживання ресурсів, таких як електроенергія чи вода. Наприклад, розумні системи поливу активуються лише тоді, коли це дійсно необхідно, зважаючи на рівень вологості ґрунту;

– швидкість і точність – Автоматизовані IoT-пристрої виконують завдання швидше та точніше, ніж людина. Це особливо корисно у виробничих процесах, де потрібна висока продуктивність і мінімізація помилок [6].

Друга важлива особливість IoT-пристроїв — їх здатність взаємодіяти між собою без втручання людини. Це досягається через концепцію Machine-to-Machine (M2M), яка дозволяє пристроям обмінюватися даними в реальному часі, координувати дії та виконувати комплексні завдання.

– взаємодія в реальному часі – IoT-пристрої використовують мережу для передачі даних у реальному часі. Наприклад, датчики руху в системі розумного дому можуть відправляти сигнал розумним лампам, які автоматично вмикають освітлення;

– обмін даними через хмарні платформи: Пристрої передають дані в хмару, де відбувається їх обробка. Наприклад, фітнес-трекери передають інформацію про фізичну активність користувача на сервери, де аналізуються тренди для надання персоналізованих рекомендацій;

– синхронізація різних пристроїв – IoT дозволяє синхронізувати різні пристрої для спільного виконання завдань. Наприклад, автомобіль, підключений до системи розумного дому, може автоматично активувати сигналізацію, закривати двері та вимикати освітлення, коли власник залишає дім;

– мінімізація людського фактора – Завдяки автоматизації та взаємодії IoT-пристроїв, зменшується потреба в ручному втручанні, що знижує ризик людських помилок і підвищує ефективність систем.

Інтернет речей (IoT) відкриває нові горизонти для оптимізації процесів у різних галузях. Автоматизація, взаємодія пристроїв без участі людини та постійний

обмін даними є ключовими аспектами, які забезпечують підвищення ефективності, зменшення витрат і покращення управління ресурсами. Завдяки технологіям IoT компанії отримують інструменти, які дозволяють значно підвищити продуктивність і якість роботи.

У табл. 1.1 наведено основні переваги автоматизації та взаємодії без участі людини, приклади їхнього застосування в різних галузях, а також вплив цих технологій на загальну ефективність бізнесу чи побутових рішень. Ця інформація допомагає зрозуміти, як саме IoT сприяє розвитку інновацій та оптимізації процесів.

Таблиця 1.1.

Переваги та приклади застосування IoT

Переваги автоматизації та взаємодії без участі людини	**Приклади застосування**	**Вплив на ефективність**
Економія часу: автоматичне виконання завдань звільняє час для інших справ.	Розумний дім: освітлення вмикається автоматично при наявності людей у кімнаті.	Збільшує продуктивність за рахунок автоматизації рутинних завдань.
Зниження витрат: оптимізація споживання ресурсів, таких як енергія та вода.	Промисловість: роботизовані системи координують виробничі процеси.	Зменшує витрати на персонал і ресурси.
Покращення безпеки: автоматичні системи забезпечують постійний контроль.	Транспорт: автономні автомобілі обмінюються інформацією про дорожню ситуацію.	Забезпечує швидшу реакцію на позаштатні ситуації.
Масштабованість: легке інтегрування пристроїв у існуючі системи.	Медицина: носимі пристрої моніторять стан пацієнтів у реальному часі.	Підтримує масштабованість системи з ростом бізнесу.

Продовження таблиці 1.1

Підвищення точності: автоматизовані пристрої зменшують ймовірність помилок.	Сільське господарство: датчики в ґрунті оптимізують полив.	Підвищує рівень контролю над процесами.
Забезпечення безперервності: системи IoT функціонують 24/7 без втручання людини.	Роздрібна торгівля: автоматизовані системи поповнення запасів.	Допомагає уникати простоїв у роботі систем.

Інтернет речей (IoT) сьогодні активно трансформує наш світ, впроваджуючи інновації у всі сфери діяльності. Завдяки IoT пристрої здатні взаємодіяти між собою, обмінюватися даними та автоматично виконувати завдання, що раніше потребували участі людини. Ці технології стали незамінними для підвищення ефективності, економії ресурсів і створення нових можливостей як у бізнесі, так і в повсякденному житті. Нижче наведено приклади використання IoT у таких сферах, як медицина, промисловість і розумний дім, які яскраво демонструють переваги цієї технології [7].

Приклади використання IoT у різних сферах:

Медицина – Інтернет речей (IoT) активно трансформує сферу охорони здоров'я, забезпечуючи нові можливості для діагностики, моніторингу та лікування пацієнтів.

– моніторинг стану пацієнтів, носимі пристрої, такі як фітнес-трекери або кардіомонітори, дозволяють відстежувати серцевий ритм, рівень кисню в крові або якість сну в реальному часі. Це особливо корисно для пацієнтів із хронічними захворюваннями;

– розумні лікарні IoT-пристрої контролюють рівень медикаментів, моніторять стан медичного обладнання та оптимізують роботу лікарень;

– віддалена діагностика, телемедицина дозволяє лікарям аналізувати дані з пристроїв пацієнтів, надаючи консультації без необхідності фізичного візиту;

– роботи-асистенти, у лікарнях роботи IoT виконують логістичні завдання, наприклад, доставляють ліки або стерилізують приміщення.

IoT є основою Індустрії промисловості, яка спрямована на автоматизацію та оптимізацію виробничих процесів;

– превентивне обслуговування, сенсори на обладнанні моніторять його стан і прогнозують можливі поломки, дозволяючи уникнути простоїв;

– оптимізація виробничих ліній: IoT допомагає налаштовувати процеси у режимі реального часу, зменшуючи витрати на енергію та підвищуючи продуктивність;

– контроль якості, завдяки IoT пристроям дані про кожен етап виробництва збираються й аналізуються, забезпечуючи високу якість продукції;

– інтеграція роботів, розумні роботи, інтегровані з IoT, можуть координувати дії один з одним і з іншими машинами, виконуючи складні завдання.

Розумний дім IoT-технології роблять життя вдома комфортнішим, ефективнішим та безпечнішим.

– системи безпеки розумні замки, камери спостереження та датчики руху автоматично повідомляють власника про підозрілу активність;

– контроль освітлення, лампи автоматично регулюють яскравість залежно від часу доби або наявності людей у приміщенні;

– розумні термостати, пристрої IoT налаштовують температуру у будинку відповідно до уподобань користувача або погоди;

– керування технікою, ористувач може віддалено керувати побутовою технікою, наприклад, запускати пральну машину чи налаштовувати роботу духовки;

– енергоефективність, системи IoT мінімізують витрати енергії, автоматично вимикаючи пристрої, які не використовуються.

1.2 Основні загрози безпеки в середовищі IoT

Інтернет речей (IoT) відкриває широкі можливості для автоматизації, покращення ефективності та створення нових рішень у різних сферах. Проте розвиток IoT також супроводжується значними викликами, зокрема загрозами

безпеки, які можуть вплинути на роботу систем, конфіденційність даних та цілісність пристроїв. Серед основних загроз безпеки виділяють несанкціонований доступ, витік даних та кібератаки.

Однією з головних проблем безпеки IoT є ризик несанкціонованого доступу до пристроїв і мереж. Завдяки широкій кількості точок підключення (Wi-Fi, Bluetooth, мобільні мережі) зловмисники можуть отримати доступ до пристроїв, використовуючи слабкі місця в їхньому захисті.

– недостатній рівень автентифікації, багато IoT-пристроїв використовують стандартні паролі або не підтримують багатофакторну автентифікацію. Це робить їх вразливими до атак "перебору паролів" (brute force);

– відсутність оновлень програмного забезпечення, у багатьох пристроїв відсутній механізм автоматичного оновлення прошивки, що призводить до тривалого використання вразливих версій програмного забезпечення;

– ризики через відкриті порти: Деякі IoT-пристрої залишають відкритими порти для віддаленого доступу, що може бути використано хакерами для проникнення в мережу.

Приклад: Несанкціонований доступ до розумних камер спостереження може дозволити зловмисникам слідкувати за власником або навіть отримати доступ до інших пристроїв у мережі.

IoT-пристрої постійно збирають і передають величезні обсяги даних, часто чутливого характеру. Це створює високий ризик витоку інформації, якщо система не має достатнього рівня захисту.

– передача даних у незашифрованому вигляді, багато пристроїв IoT передають інформацію без шифрування, що дозволяє зловмисникам перехоплювати дані за допомогою атак "людина посередині" (Man-in-the-Middle);

– вразливі хмарні сервіси: Дані IoT часто зберігаються у хмарних сервісах. Якщо хмарна інфраструктура скомпрометована, це може призвести до масштабного витоку даних;

– низька захищеність пристроїв, через обмежені ресурси, багато IoT-пристроїв не підтримують комплексні механізми шифрування, що робить їх більш вразливими до зломів.

Приклад: Витік даних з фітнес-браслетів або розумних пристроїв може розкрити інформацію про місцезнаходження, фізичний стан або інші особисті дані користувача.

IoT-середовище є привабливою мішенню для кібератак, оскільки більшість пристроїв постійно підключені до мережі та мають слабкі механізми захисту.

– атаки типу DDoS – зловмисники можуть використовувати IoT-пристрої для здійснення розподілених атак відмови в обслуговуванні (DDoS). Зламані пристрої об'єднуються в бот-мережі (наприклад, Mirai) і паралізують роботу серверів;

– зловмисне програмне забезпечення IoT-пристрої можуть бути заражені шкідливими програмами, які крадуть дані або блокують пристрій для отримання викупу (ransomware);

– підміна даних, зловмисники можуть втручатися в процес обробки даних IoT, змінюючи їх для введення в оману користувачів або систем;

Приклад: Атака Mirai у 2016 році, коли було скомпрометовано мільйони IoT-пристроїв для здійснення масштабного DDoS-нападу, який зупинив роботу великих сайтів.

IoT-системи часто залежать від взаємодії з людьми, що робить їх вразливими до атак соціальної інженерії.

– фішингові атаки, зловмисники надсилають підроблені повідомлення від імені виробників, переконуючи користувачів надати доступ до пристроїв;

– шахрайство з техпідтримкою, хакери можуть видавати себе за технічну підтримку, щоб отримати дані для доступу до IoT-пристроїв.

Приклад: Отримання доступу до розумного дому через підроблені запити на зміну пароля.

Багато IoT-пристроїв знаходяться у відкритому доступі, що збільшує ризики їх фізичного втручання.

– несанкціонована заміна, зловмисники можуть замінити пристрій на скомпрометований аналог;

– зчитування даних з пам’яті, фізичний доступ дозволяє зловмисникам отримати ключі шифрування або конфіденційні дані.

Приклад: Фізичне проникнення в IoT-систему безпеки для отримання контролю над дверними замками.

Розвиток Інтернету речей (IoT) став справжньою революцією у сфері технологій, надавши можливість автоматизувати процеси, оптимізувати ресурси та створити новий рівень комфорту для користувачів. Однак із цими перевагами з’являються і нові виклики, зокрема загрози безпеці. IoT-пристрої часто мають обмежені можливості для захисту, що робить їх привабливою ціллю для кіберзлочинців. Відсутність стандартів безпеки, використання слабких паролів і відкриті мережеві порти значно підвищують ризики атак [8].

Однією з головних проблем є те, що IoT-пристрої, на відміну від традиційних комп’ютерів, рідко оновлюють своє програмне забезпечення. Це дозволяє хакерам використовувати відомі вразливості, залишаючи пристрої беззахисними. Крім того, через постійне підключення до мережі, ці пристрої можуть бути скомпрометовані та використані у великих масштабах для реалізації кібератак.

Найбільш поширеними формами атак є DDoS-атаки, витік конфіденційних даних і захоплення контролю над пристроями. У багатьох випадках зловмисники використовують ці методи для шантажу, економічних диверсій або створення бот-мереж для проведення масових атак. Розглянемо два реальні приклади кіберзагроз у сфері IoT, які демонструють критичну важливість підвищення рівня безпеки цих пристроїв: ботнет Mirai та злом камер спостереження.

Атака Mirai – це ботнет, який став широко відомим у 2016 році. Він був створений для пошуку вразливих IoT-пристроїв, таких як камери відеоспостереження, маршрутизатори та DVR-пристрої. Mirai використовував слабкі паролі або стандартні облікові записи, щоб проникнути в пристрої, зібрати їх у бот-мережу та здійснювати масштабні розподілені атаки типу DDoS (відмова в обслуговуванні).

Хід атаки:

– Mirai автоматично сканував мережу для пошуку пристроїв IoT з відкритими портами.

– Після проникнення в пристрій зловмисники інтегрували його до бот-мережі.

– Об’єднані пристрої надсилали масові запити до серверів, що призводило до перевантаження серверів і їхньої недоступності для користувачів.

Наслідки:

– Mirai здійснив одну з найбільших атак в історії, паралізувавши роботу популярних сервісів, таких як Twitter, Netflix, Spotify, PayPal, через атаку на сервери Dyn DNS.

– Вразливими виявилися мільйони IoT-пристроїв по всьому світу.

Злом камер спостереження – к амери спостереження часто використовуються в системах безпеки, але вони також можуть стати точкою входу для хакерів. Через слабкі механізми захисту, такі як відкриті порти та незашифровані підключення, зловмисники можуть отримати доступ до відеопотоків або навіть захопити контроль над камерами [9].

Хід атаки:

– хакери використовують інструменти для сканування мережі на наявність камер спостереження з відкритими портами;

– після виявлення пристрою вони застосовують атаки на слабкі паролі або експлойти для проникнення;

– отримавши доступ, хакери можуть:

– стежити за людьми в реальному часі;

– захоплювати відеопотоки для шантажу;

– використовувати камери як частину бот-мереж для DDoS-атак.

Приклад:

У 2021 році було розкрито інцидент, коли зловмисники отримали доступ до понад 150 000 камер, встановлених у лікарнях, школах, підприємствах і навіть у в’язницях. Причиною став злом хмарного сервісу, який керував камерами.

Наслідки:

– конфіденційність користувачів була порушена;

– уразливість хмарного сервісу поставила під загрозу безпеку об’єктів, які залежали від камер;

Злом розумних побутових приладів – побутові IoT-пристрої, такі як розумні холодильники, пральні машини або голосові асистенти, можуть бути використані для шпигунства або атак на інші пристрої.

Хід атаки:

– зловмисники отримують доступ до цих пристроїв через незахищені з’єднання;

– вони можуть відстежувати поведінку користувачів, отримувати доступ до мережі або навіть використовувати пристрої як точку входу для інших атак.

Приклад:

У 2017 році дослідники виявили, що розумні холодильники, які мали доступ до електронної пошти користувача, були використані для розсилки спаму.

Наслідки:

– витік особистих даних користувачів;

– порушення конфіденційності та безпеки.

Атака на IoT-пристрої у лікарнях – у лікарнях IoT-пристрої використовуються для моніторингу стану пацієнтів, управління медичним обладнанням та організації робочих процесів. Атаки на ці системи можуть мати серйозні наслідки для здоров’я пацієнтів [10].

Хід атаки:

– хакери зламують медичні IoT-пристрої через вразливі мережі;

– вони можуть змінювати показники пристроїв або блокувати їх роботу.

Приклад:

У 2021 році група хакерів атакувала мережу лікарні в Німеччині, заблокувавши доступ до систем управління пацієнтами та вимагаючи викуп.

Наслідки:

– порушення надання медичної допомоги;

– ризики для життя пацієнтів через неправильні або відсутні дані моніторингу.

Ці реальні приклади кіберзагроз у сфері IoT демонструють серйозність проблеми безпеки та важливість впровадження сучасних методів захисту. Унікальні паролі, регулярні оновлення, шифрування даних та підвищення обізнаності користувачів є ключовими заходами для мінімізації ризиків і забезпечення надійної роботи IoT-систем.

1.3 Архітектура інтегрованих систем моніторингу безпеки IoT

Архітектура інтегрованих систем моніторингу безпеки IoT складається з багатьох компонентів, які забезпечують ефективний збір, аналіз і реагування на дані з IoT-пристроїв. Основна мета такої архітектури – створити цілісну систему, яка може виявляти загрози, мінімізувати ризики і забезпечувати стабільну роботу пристроїв. Розглянемо основні компоненти архітектури системи моніторингу [11].

Датчики (Sensors)

Датчики є ключовим компонентом IoT-систем, відповідальним за збір даних з фізичного світу. Вони забезпечують перетворення реальних показників у цифрові сигнали, які можуть бути оброблені системою.

Типи датчиків:

– датчики температури, вологості, тиску;

– датчики руху, освітлення;

– камери спостереження та мікрофони;

– біометричні датчики для розпізнавання осіб чи відбитків пальців.

Роль датчиків у моніторингу:

– фіксація змін у навколишньому середовищі;

– виявлення аномалій, таких як несанкціонований рух або підвищення температури.

Приклад: У системах розумного дому датчики руху можуть виявляти присутність і активувати системи сигналізації.

Обробка даних (Data Processing) є етапом у роботі інтегрованих систем моніторингу. Цей компонент забезпечує аналіз інформації, отриманої з датчиків, і перетворення її на зрозумілу та корисну форму.

Обробка даних у рамках інтегрованої системи моніторингу безпеки IoT-пристроїв включає кілька основних етапів. Спочатку проводиться фільтрація, що передбачає видалення зайвого шуму та помилкових сигналів, які можуть впливати на точність аналізу. Далі здійснюється аналіз, у процесі якого застосовуються алгоритми машинного навчання або предиктивної аналітики для виявлення потенційних загроз. Отримані результати проходять стадію візуалізації, яка передбачає створення графіків, звітів або інтерфейсів для ефективного моніторингу та інтерпретації отриманих даних.

Для обробки інформації використовуються два основні методи. Перший – локальна обробка на пристроях (Edge Computing), що забезпечує швидку реакцію на потенційні загрози без необхідності передавання даних у хмару. Другий – обробка в хмарі, яка застосовується для більш складних аналітичних завдань, що потребують значних обчислювальних ресурсів та масштабованості.

Приклад: у системах безпеки IoT аналітичні алгоритми можуть ідентифікувати підозрілі звуки або рухи, повідомляючи про це користувача через мобільний додаток.

Сервери та хмарна інфраструктура (Servers and Cloud Infrastructure) – сервери є центральною частиною системи, яка зберігає, обробляє та аналізує дані. Вони забезпечують масштабованість і доступність системи.

Сервери виконують низку ключових функцій у системі моніторингу безпеки IoT-пристроїв. Однією з основних функцій є зберігання даних, що передбачає використання центральної бази даних для накопичення та обробки всієї отриманої інформації. Крім того, сервери здійснюють координацію пристроїв, забезпечуючи ефективну взаємодію між датчиками, пристроями обробки даних та користувацькими інтерфейсами. Ще однією важливою функцією є реагування на загрози – у разі виявлення небезпеки сервери автоматично надсилають сповіщення користувачам або активують відповідні заходи захисту.

Хмарна інфраструктура відіграє ключову роль у забезпеченні масштабованості та продуктивності системи. Вона дає можливість обробляти великі обсяги даних у реальному часі, що критично важливо для швидкого реагування на події. Завдяки хмарним технологіям система залишається доступною з будь-якої точки світу, що забезпечує зручність керування та моніторингу. Додатково, хмарні сервери гарантують резервне копіювання даних, що дозволяє уникнути їхньої втрати у разі технічних збоїв або кібератак.Приклад: у розумних містах сервери збирають дані з транспортних датчиків, аналізують завантаженість доріг і коригують роботу світлофорів у реальному часі.

Інтерфейси користувача (User Interfaces), хоча інтерфейси не є центральним компонентом архітектури, вони забезпечують зручний доступ до даних і можливість управління системою.

У системі моніторингу безпеки IoT-пристроїв користувачі можуть отримувати доступ до інформації та керувати налаштуваннями за допомогою різних інтерфейсів. Мобільні додатки забезпечують швидке отримання сповіщень про потенційні загрози та дозволяють переглядати звіти про стан системи в реальному часі. Для розширеного керування передбачені веб-інтерфейси, які надають повний доступ до налаштувань, історії роботи системи та детального аналізу даних.

Інтегрована архітектура такої системи має низку важливих переваг. По-перше, вона забезпечує швидке виявлення загроз завдяки ефективній взаємодії між датчиками, модулями обробки даних та серверами. По-друге, система є масштабованою, що дозволяє легко додавати нові пристрої без зниження її продуктивності. Також важливою характеристикою є гнучкість, оскільки система підтримує різні типи пристроїв і протоколи зв’язку, що робить її універсальною. Останньою, але не менш важливою перевагою є надійність, яка досягається завдяки резервному зберіганню даних та багаторівневим механізмам захисту від загроз.

Сучасні системи Інтернету речей (IoT) пропонують безпрецедентні можливості для автоматизації та оптимізації процесів, але водночас вони стикаються з численними загрозами безпеки. Інтегровані системи моніторингу

покликані вирішувати ці виклики, забезпечуючи ефективний захист даних, пристроїв та користувачів. Завдяки поєднанню апаратних та програмних компонентів, такі системи забезпечують повний цикл моніторингу – від збору даних до автоматичного реагування на загрози.

Основна мета інтегрованих систем полягає в створенні надійної інфраструктури, яка дозволяє своєчасно виявляти та нейтралізувати загрози, забезпечуючи безперебійну роботу IoT-мереж. Використання датчиків, серверів та алгоритмів обробки даних дозволяє досягти високого рівня точності у виявленні потенційних атак і мінімізації їхнього впливу [12].

У табл. 1.2 представлені ключові функції інтегрованих систем моніторингу безпеки IoT, їх опис та приклади застосування у реальних сценаріях. Це дозволяє зрозуміти, як сучасні технології допомагають забезпечити безпеку пристроїв і даних, сприяючи розвитку IoT-середовища.

Таблиця 1.2

Інтегровані системи допомагають забезпечити безпеку IoT

Функція	**Опис**	**Приклад**
Постійний моніторинг та виявлення загроз	Система цілодобово моніторить підключені пристрої, аналізує дані та виявляє аномалії.	Датчики руху у розумному домі виявляють проникнення та активують сигналізацію.
Захист даних	Використовуються шифрування, автентифікація та резервне копіювання для захисту інформації.	Медичні IoT-системи шифрують дані пацієнтів для забезпечення конфіденційності.
Превентивне обслуговування	Система аналізує стан обладнання та попереджає про можливі несправності.	У промисловості сенсори моніторять вібрації для прогнозування поломок.
Автоматичне реагування	Система автоматично блокує доступ, вмикає сигналізацію або виконує інші дії у разі загрози.	IoT-система у транспорті автоматично блокує двері вагонів під час пожежі.

Продовження таблиці 1.2

Централізоване управління	Усі пристрої об’єднані у єдину мережу для зручного управління та моніторингу.	Дашборди у розумних містах дозволяють контролювати освітлення та транспорт.
Інтеграція з іншими системами	IoT інтегрується зі штучним інтелектом та блокчейном для покращення роботи систем.	У фінансах блокчейн гарантує безпечний обмін даними між пристроями.
Масштабованість та адаптивність	Система легко адаптується до нових потреб та дозволяє додавати нові пристрої.	У сільському господарстві додаються нові сенсори для моніторингу клімату.

Технологія Asynchronous JavaScript and XML (AJAX) відіграє важливу роль у моніторингу даних у реальному часі завдяки її здатності забезпечувати швидкий і ефективний обмін інформацією між клієнтом та сервером без необхідності перезавантаження сторінки. Це робить AJAX ідеальним інструментом для роботи з великими обсягами динамічних даних, що часто є критичним у системах моніторингу IoT.

Сучасні IoT-системи вимагають комплексного підходу до забезпечення безпеки, оскільки вони об'єднують безліч пристроїв, що взаємодіють між собою. Архітектура інтегрованих систем моніторингу безпеки IoT складається з кількох ключових компонентів, таких як датчики, сервери, модулі обробки даних та користувацькі інтерфейси. Кожен із цих компонентів відіграє важливу роль у виявленні, аналізі та реагуванні на потенційні загрози.

Таблиця 1.3 ілюструє структуру архітектури інтегрованих систем моніторингу та демонструє, як кожен елемент сприяє загальній функціональності системи. Датчики забезпечують постійний збір даних з фізичного середовища, сервери займаються зберіганням і аналізом інформації, а інтерфейси дозволяють користувачам отримувати актуальні сповіщення та управляти пристроями. Такий підхід дозволяє створити цілісну, масштабовану та надійну систему для моніторингу і забезпечення безпеки IoT [13].

Таблиця 1.3

Використання AJAX для ефективного моніторингу даних у реальному часі

Компонент	Опис	Приклад використання
Асинхронні запити	Клієнт надсилає запити до сервера у фоновому режимі, отримуючи дані без перезавантаження сторінки.	Моніторинг датчиків температури та вологості у розумному домі.
Передача даних	AJAX підтримує різні формати передачі даних, такі як JSON, XML або текст.	Передача інформації від IoT-пристроїв до серверів для обробки.
Обробка на клієнтській стороні	Отримані дані обробляються JavaScript і відображаються у вигляді графіків або повідомлень.	Графічний інтерфейс для моніторингу стану обладнання на виробництві.
Оновлення в реальному часі	Інформація оновлюється миттєво, без потреби оновлення сторінки.	Медичний моніторинг життєвих показників пацієнтів у лікарні.
Оптимізація ресурсів	Оновлюються лише потрібні дані, зменшуючи навантаження на сервер.	Системи трафіку, які оновлюють дані про затори у реальному часі.
Інтерактивність	Користувацький інтерфейс стає динамічним і зручним для роботи з даними.	Відображення активності безпекових систем у реальному часі.
Масштабованість	Можливість легко інтегрувати нові пристрої до існуючої системи.	Додання нових сенсорів у розумному місті для моніторингу якості повітря.

Розвиток Інтернету речей (IoT) відкриває нові можливості для автоматизації, оптимізації процесів і створення інноваційних рішень у різних сферах. Разом з тим, зростає потреба в забезпеченні надійності та безпеки таких систем, що обумовлює актуальність дослідження загроз і способів їхнього запобігання.

Розглянуто сутність та особливості технології IoT, яка дозволяє інтегрувати фізичні об’єкти в єдину мережу для обміну даними та виконання завдань без участі людини. Особливості IoT, такі як автоматизація та постійна підключеність, створюють передумови для підвищення ефективності, але водночас стають точками вразливості для кібератак.

Проаналізовано основні загрози безпеки в середовищі IoT, зокрема несанкціонований доступ, витік даних і розподілені атаки. Ці загрози підкреслюють необхідність впровадження багаторівневих систем захисту, таких як шифрування, автентифікація та регулярні оновлення.

Розгляд архітектури інтегрованих систем моніторингу безпеки IoT дозволив окреслити ключові компоненти таких систем, включаючи датчики, сервери та механізми обробки даних. Ці елементи забезпечують цілісний підхід до моніторингу, аналізу даних та автоматичного реагування на потенційні загрози.

2 ПОРІВНЯННЯ ТЕХНОЛОГІЇ AJAX З АНАЛОГАМИ ДЛЯ МОЖЛИВОСТІ МОНІТОРИНГУ

2.1 Огляд технології AJAX: принципи роботи та особливості

Системи безпеки Ajax — це сучасні інтелектуальні охоронні системи, які забезпечують безпеку житлових, офісних та промислових об'єктів. Вони створені українською компанією Ajax Systems і відомі своєю надійністю, стильним дизайном, простотою установки і використання.

Система складається з різних пристроїв, які взаємодіють через захищені бездротові протоколи і можуть інтегруватися з мобільними додатками для управління в реальному часі.

Центральний блок системи безпеки Ajax, також відомий як Hub, є ключовим елементом інтелектуальної охоронної системи (рис. 2.1). Це головний пристрій, який об'єднує всі компоненти системи безпеки: датчики, сирени, камери та інші пристрої. Hub працює як своєрідний "мозок", забезпечуючи безперебійний зв'язок між пристроями, обробку отриманих сигналів і миттєве інформування користувача про будь-які події. Завдяки сучасним алгоритмам і використанню безпечних протоколів передачі даних, Hub гарантує надійність і швидкість реакції системи навіть у складних умовах.

Рис. 2.1 Hub – центральний блок системи безпеки Ajax

Особливістю Hub є використання бездротового протоколу Jeweller, який забезпечує стабільний зв'язок із датчиками на відстані до 2000 метрів на відкритій місцевості. Цей протокол має високий рівень захисту від перешкод і спроб глушіння сигналу, що робить систему безпеки максимально надійною. У разі втрати зв’язку або спроби саботажу Hub миттєво сповіщає власника та охоронну службу. Додатково, пристрій підтримує резервне живлення, що дозволяє йому функціонувати навіть при перебоях з електроенергією протягом кількох годин.

Ще однією важливою перевагою центрального блоку є його можливість працювати через кілька каналів зв'язку. Hub підтримує підключення до мережі через Ethernet, Wi-Fi та мобільні мережі (2G/3G/4G, залежно від моделі). Це означає, що система залишається активною навіть у разі збоїв на основному каналі зв’язку. У разі виявлення загрози Hub швидко передає сигнал на мобільний додаток користувача, надсилає SMS або дзвінок, а також повідомляє пульт охоронної компанії. Така багатоканальна архітектура забезпечує високу стійкість і надійність системи. [14]

Окрім своїх технічних характеристик, Hub відзначається стильним дизайном, який гармонійно вписується в сучасний інтер'єр. Він компактний, легко монтується і налаштовується без допомоги спеціалістів. Усі операції керуються через інтуїтивно зрозумілий мобільний додаток, що дозволяє власнику системи перевіряти статус пристроїв, отримувати сповіщення і змінювати налаштування. Центральний блок є серцем екосистеми Ajax, забезпечуючи інтеграцію з додатковими пристроями, такими як відеокамери або розумні розетки, що робить його незамінним для створення інтелектуального та безпечного простору.

Датчики руху – це ключові елементи системи безпеки, які відповідають за виявлення присутності або руху людей у захищеному просторі. Вони використовуються для моніторингу приміщень та активації системи у разі несанкціонованого проникнення (рис. 2.2). У системах Ajax датчики руху вирізняються високою точністю, швидкою реакцією та стійкістю до хибних спрацьовувань. Вони аналізують зміни в середовищі, використовуючи

інфрачервоні сенсори для виявлення теплового випромінювання тіла людини. Це дозволяє їм розрізняти людей та інші джерела руху, наприклад, тварин або побутові прилади [15].

Рис. 2.2 Датчики руху Ajax

Однією з головних переваг датчиків руху Ajax є їхня здатність адаптуватися до різних умов середовища. Вони використовують алгоритми цифрової обробки сигналів, що мінімізує ймовірність хибного спрацьовування через тіні, протяги або зміну температури. Завдяки інтелектуальним технологіям, датчики можуть ігнорувати рух домашніх тварин вагою до 20-25 кг, що робить їх ідеальними для використання в домогосподарствах із тваринами. Крім того, вони мають стильний та компактний дизайн, що дозволяє легко інтегрувати їх у будь-який інтер’єр без порушення естетики простору.

Сучасні датчики руху Ajax підтримують бездротову технологію зв'язку Jeweller, що забезпечує стабільний зв’язок із центральним блоком (Hub) на відстані до 1700 метрів на відкритій місцевості. Вони мають вбудовані механізми захисту від саботажу, включаючи функцію виявлення розкриття корпусу та спроб глушіння сигналу. Завдяки автономному живленню, датчики можуть працювати до 7 років

від однієї батареї, що робить їх надзвичайно економічними у використанні. У разі розрядження батареї система заздалегідь повідомляє користувача, щоб уникнути перебоїв у роботі.

Інтеграція датчиків руху Ajax із мобільним додатком дозволяє користувачам отримувати сповіщення про будь-який рух у реальному часі. Це дає можливість миттєво реагувати на загрозу, включаючи активацію сирени або повідомлення охоронної служби. Датчики також можуть працювати у сценаріях автоматизації, наприклад, вмикати світло при виявленні руху [16]. Їх легко встановлювати самостійно без спеціальних знань: датчики поставляються з комплектом кріплень і налаштовуються через додаток за кілька хвилин. Завдяки таким характеристикам датчики руху є незамінною частиною системи безпеки, що забезпечує надійний контроль над простором і спокій власника.

Датчики відкриття дверей/вікон – це важливі компоненти сучасних систем безпеки, які забезпечують контроль доступу до приміщень (рис. 2.3). У системах Ajax ці датчики виконують функцію миттєвого сповіщення про відкриття дверей або вікон, що є ключовим для попередження несанкціонованого проникнення. Вони складаються з двох частин: магнітного сенсора та магніту, які фіксують положення одне відносно одного. Коли магніт і сенсор розходяться через відкриття дверей або вікна, датчик автоматично передає сигнал на центральний блок (Hub), активуючи тривогу. Завдяки високій чутливості та точності, ці пристрої забезпечують ефективний контроль безпеки навіть у найскладніших умовах.

Рис. 2.3 Датчики відкриття дверей/вікон DoorProtect

Датчики відкриття Ajax вирізняються своєю універсальністю та простотою встановлення. Їх можна закріпити на будь-якому типі дверей або вікон, включаючи металеві, пластикові та дерев'яні конструкції. Крім стандартного використання, датчики також можуть слугувати для інших завдань, таких як контроль доступу до шаф із цінностями або технічних приміщень. Пристрої сумісні з широким спектром сценаріїв автоматизації. Наприклад, при відкритті дверей можна налаштувати автоматичне ввімкнення освітлення або активацію системи вентиляції.

Ключовою особливістю датчиків відкриття Ajax є їхній бездротовий дизайн та підтримка захищеного протоколу зв'язку Jeweller, який забезпечує стабільну роботу на відстані до 1200 метрів від центрального блоку. Вони стійкі до спроб глушіння сигналу та саботажу завдяки вбудованим системам захисту. Датчики живляться від батареї, яка може працювати до 7 років без заміни, що мінімізує необхідність у регулярному обслуговуванні. Крім того, пристрої мають функцію температурного моніторингу, яка дозволяє виявляти зміну кліматичних умов, таких як різке падіння або підвищення температури в приміщенні.

Інтеграція датчиків відкриття дверей/вікон із мобільним додатком Ajax дає змогу користувачеві отримувати сповіщення про кожну подію в реальному часі, незалежно від його місцезнаходження. Датчики також можуть передавати сигнал на пульт охоронної компанії, забезпечуючи швидке реагування на потенційні загрози. Простий і стильний дизайн датчиків дозволяє їм гармонійно вписуватися в інтер'єр, не порушуючи естетики приміщення. Завдяки таким характеристикам ці датчики є незамінним елементом комплексної системи безпеки, який забезпечує спокій і контроль над доступом до вашого простору.

Датчики розбиття скла Ajax – це сучасні пристрої, розроблені для забезпечення надійного захисту віконних конструкцій та швидкого виявлення спроб проникнення через скло (рис. 2.4). Ці датчики призначені для миттєвого реагування на розбиття вікон чи скляних дверей, що часто є однією з перших дій зловмисників при несанкціонованому доступі. Вони здатні визначати характерний звук розбитого скла завдяки вбудованим мікрофонам і аналізаторам звуку, які розпізнають специфічну комбінацію низькочастотного удару та високочастотного

дзвону битого скла. Це забезпечує точність спрацювання та зменшує ризик хибних тривог.

Рис. 2.4 Датчики розбиття скла GlassProtect

Особливістю датчиків розбиття скла Ajax є їхня здатність працювати на відстані до 9 метрів, що дозволяє захищати одразу кілька вікон у кімнаті чи офісі. Вони підходять для використання у різних приміщеннях: від квартир і приватних будинків до офісів, магазинів чи складських приміщень. Завдяки бездротовій технології Jeweller, датчики забезпечують стабільний зв’язок із центральним блоком (Hub) на відстані до 2000 метрів на відкритій місцевості, а також мають захист від глушіння сигналу та саботажу. Пристрій працює автономно від батареї до 7 років, що робить його зручним у використанні та обслуговуванні.

Щоб уникнути хибних спрацювань, датчики Ajax оснащені інтелектуальними алгоритмами обробки звуку, які виключають реакцію на схожі шуми, наприклад, дзвін ключів або брязкіт посуду. Це особливо важливо для приміщень з активним життям, де можливі побутові звуки. Простота встановлення також є однією з переваг датчиків. Їх можна легко закріпити на стіні або стелі біля

вікна, а налаштування здійснюється через мобільний додаток Ajax за кілька хвилин.

Датчики розбиття скла Ajax інтегруються з іншими компонентами системи безпеки, дозволяючи створювати комплексний захист вашого приміщення. У разі виявлення загрози пристрій миттєво надсилає сигнал на центральний блок, який активує сирену, сповіщає користувача через мобільний додаток і передає тривогу на пульт охоронної компанії. Завдяки своєму сучасному дизайну, високій чутливості та зручності використання, датчики розбиття скла Ajax є важливим елементом для захисту будь-якого приміщення.

Датчики диму, газу та затоплення Ajax – це спеціалізовані пристрої, які забезпечують моніторинг стану навколишнього середовища та попереджають про потенційні небезпеки, пов’язані з пожежею, витоком газу чи води (рис. 2.5). Вони є важливою частиною системи безпеки, спрямованою на захист життя та майна від різних аварійних ситуацій. Завдяки чутливим сенсорам і передовим технологіям, ці датчики можуть виявляти небезпеку на ранніх стадіях, що дозволяє вчасно реагувати і мінімізувати можливі збитки.

Рис. 2.5 Датчик проти затоплення LeaksProtect

Датчики диму Ajax виявляють навіть найменші концентрації диму в повітрі, що є ознакою початкової стадії займання (рис. 2.6). Багато моделей також оснащені температурними сенсорами, які реагують на раптове підвищення температури, навіть якщо диму немає. Датчики газу реагують на витік небезпечних газів, таких як метан чи чадний газ (CO), і сповіщають про небезпеку до того, як концентрація досягне критичного рівня. Датчики затоплення активуються при контакті з водою, попереджаючи про витоки чи затоплення в приміщенні.

Рис. 2.6 Датчик диму FireProtect

Усі ці пристрої працюють автономно і оснащені бездротовою технологією Jeweller, яка забезпечує стабільний зв'язок із центральним блоком (Hub). Вони мають тривалий термін роботи від батареї (до 7 років) та стійкі до зовнішніх перешкод. Інтеграція з мобільним додатком Ajax дозволяє користувачам отримувати сповіщення про небезпеку в реальному часі, а також контролювати стан датчиків і налаштовувати їх параметри.

Сирени Ajax — це пристрої, які створюють гучний звуковий та/або світловий сигнал у разі виявлення загрози (рис. 2.7). Вони можуть бути встановлені всередині приміщення або на фасаді будівлі, привертаючи увагу до потенційної небезпеки. Сирени не лише лякають зловмисників, а й попереджають власників та сусідів про інцидент. Їх можна налаштовувати через мобільний додаток для регулювання гучності та тривалості сигналу.

Рис. 2.7 Сирени Ajax

Ретранслятори Ajax призначені для розширення зони дії системи безпеки, забезпечуючи стабільний зв'язок між центральним блоком (Hub) і пристроями, які знаходяться на значній відстані або в умовах, де є перешкоди. Вони підтримують бездротовий зв'язок із захистом від глушіння сигналу, що забезпечує надійну роботу системи навіть у великих приміщеннях чи багатоповерхових будівлях.

Застосунок Ajax Security System є центральним інструментом для керування всіма пристроями екосистеми Ajax, включаючи датчики, сирени, ретранслятори та розумні пристрої. Це мобільний додаток, доступний для платформ iOS та Android, який забезпечує інтуїтивно зрозумілий і зручний інтерфейс для моніторингу та управління системою безпеки в реальному часі. Крім того, застосунок доступний і у веб-версії, що дозволяє користуватися ним з комп’ютера.

Застосунок Ajax Security System забезпечує зручний контроль за безпекою приміщень у режимі реального часу та має широкий функціонал для користувачів.

Одна з ключових можливостей – моніторинг у реальному часі, що дозволяє стежити за станом усіх підключених пристроїв, перевіряти активність датчиків,

рівень заряду батарей та якість підключення. У разі виявлення загрози, такої як злом, затоплення або пожежа, система надсилає миттєві сповіщення у вигляді push-нотифікацій, SMS або телефонного дзвінка відповідно до налаштувань користувача.

Додаток також дає змогу керувати режимами охорони, дозволяючи активувати або деактивувати систему, а також вмикати захист для окремих зон, наприклад, лише для певної кімнати або поверху. Ще однією корисною функцією є налаштування сценаріїв автоматизації, що дозволяє створювати правила для розумних пристроїв, наприклад, автоматичне ввімкнення світла чи відключення електрики за певних умов.

Для зручного користування система підтримує можливість додавання додаткових користувачів, надаючи членам родини або колегам доступ до управління з різними рівнями прав. Крім того, застосунок передбачає інтеграцію з охоронними компаніями, що дозволяє підключити систему до пульта моніторингу та контролювати передачу сигналів тривоги у разі небезпеки.

Переваги застосунку:

– усі функції системи доступні в одному місці, без необхідності використовувати додаткові програми чи пристрої;

– простий інтерфейс забезпечує легкий доступ до всіх налаштувань навіть для тих, хто не має технічного досвіду;

– передача даних здійснюється через зашифровані канали, що забезпечує конфіденційність і захист інформації;

– керування системою з будь-якої точки світу, де є доступ до Інтернету.

Додаток Ajax Security System робить систему безпеки максимально доступною, зрозумілою та ефективною, що дозволяє користувачам не лише забезпечити захист своїх приміщень, а й автоматизувати повсякденні процеси, підвищуючи комфорт життя.

Інтегрована система моніторингу безпеки з IoT-пристроями Ajax пропонує унікальне поєднання простоти використання, інноваційних технологій і комплексного захисту. Ці пристрої створені для того, щоб забезпечити

максимальну безпеку вашого дому чи офісу, роблячи це з мінімальними зусиллями з боку користувача. Всі елементи системи взаємодіють через захищений бездротовий протокол Jeweller, що гарантує надійний зв'язок та швидке реагування.

Користь від використання IoT-пристроїв Ajax в інтегрованій системі:

– комплексний захист, система Ajax дозволяє інтегрувати різноманітні пристрої – датчики руху, диму, затоплення, відкриття, сирени та розумні пристрої. Це дає змогу забезпечити багаторівневий захист від проникнень, пожеж, затоплень і техногенних аварій;

– миттєве сповіщення, завдяки мобільному додатку користувач отримує інформацію про будь-яку загрозу в реальному часі, незалежно від свого місцезнаходження.

– ефективність автоматизації, система підтримує налаштування сценаріїв автоматизації, які підвищують комфорт і безпеку. Наприклад, система може автоматично вимкнути подачу електрики в разі затоплення або ввімкнути сирену при виявленні руху.

– економія часу та ресурсів, завдяки простоті монтажу та мінімальному обслуговуванню, Ajax пристрої дозволяють уникнути додаткових витрат на професійне встановлення чи регулярне технічне обслуговування.

Легкість використання Ajax IoT-пристроїв:

– усі пристрої Ajax мають бездротовий дизайн і кріпляться на поверхню за допомогою спеціальних тримачів. Монтаж займає лише кілька хвилин і не вимагає спеціальних навичок;

– система контролюється через мобільний додаток, який має зрозумілий інтерфейс і підтримує різні мови. Навіть новачок швидко освоїть основи керування;

– пристрої працюють від батарей з тривалим терміном служби (до 7 років), що зводить до мінімуму необхідність регулярного обслуговування;

– Ajax легко адаптується до змін і дозволяє додавати нові пристрої до існуючої системи через QR-код у додатку;

– користувач може керувати всією системою, налаштовувати режими роботи та отримувати сповіщення зі смартфона, що робить систему доступною навіть для тих, хто не перебуває вдома.

2.2 Порівняння AJAX із іншими технологіями для моніторингу IoT-пристроїв

Охоронні системи моніторингу, що використовують технологію AJAX, базуються на механізмі асинхронного обміну даними між клієнтом і сервером. Їх принцип роботи полягає у використанні HTTP-запитів для отримання даних від IoT-пристроїв, таких як камери спостереження, датчики руху та тривожні сигнали, через веб-інтерфейс. Дані можуть оновлюватися періодично за допомогою опитування сервера або отримуватися асинхронно, що забезпечує зручний доступ до інформації без необхідності перезавантаження сторінки.

Основною перевагою таких систем є їхня доступність через веб-браузер, що дозволяє користувачам керувати охоронною системою без встановлення спеціального програмного забезпечення. Крім того, вони підтримують стандартні протоколи зв’язку, такі як HTTP і HTTPS, що спрощує інтеграцію з іншими веб-системами, зокрема з аналітичними платформами та журналами подій. Гнучкість технології дозволяє застосовувати її для взаємодії з широким спектром IoT-пристроїв і забезпечувати централізований моніторинг безпеки.

Водночас використання AJAX у моніторингових системах має певні недоліки. Постійне опитування серверів може створювати додаткове навантаження на мережу та серверні ресурси, особливо при обробці великої кількості пристроїв. Це може призводити до затримок у передаванні критичних даних, що робить технологію менш ефективною для обробки подій у реальному часі. Крім того, масштабованість таких систем обмежена – зі збільшенням кількості підключених пристроїв продуктивність може знижуватися, що потребує додаткової оптимізації або використання альтернативних технологій передачі даних.

Моніторингові системи, що використовують WebSockets, забезпечують постійний двосторонній зв’язок між клієнтом і сервером, що дозволяє миттєво отримувати сповіщення про тривоги, відеопотоки та інші критичні дані. Завдяки цьому технологія ідеально підходить для обробки подій у реальному часі, наприклад, моментального реагування на сигнали тривоги. Основною перевагою WebSockets є висока ефективність, оскільки використовується єдиний постійний канал зв’язку замість численних запитів, що зменшує навантаження на сервери. Також ця технологія добре підходить для стримінгу відео та аудіо з камер спостереження.

Водночас налаштування WebSockets потребує певних технічних ресурсів, оскільки серверам необхідно підтримувати постійні з'єднання з клієнтами. Крім того, робота системи сильно залежить від стабільності інтернет-з'єднання, адже в разі втрати зв’язку передача даних миттєво припиняється.

Ще однією ефективною технологією для моніторингу є MQTT, що працює за моделлю публікації/підписки. У такій системі пристрої публікують дані, а сервери розповсюджують їх серед підписників, зокрема охоронних систем. Головною перевагою є оптимізація для мереж із низькою пропускною здатністю, що дозволяє ефективно працювати навіть у складних умовах. MQTT також забезпечує масштабованість, оскільки легко підтримує велику кількість IoT-пристроїв. Додатковою перевагою є можливість використання різних рівнів надійності, що гарантує доставку повідомлень навіть при нестабільному з’єднанні.

Попри свої переваги, MQTT має певні обмеження. Оскільки браузери не підтримують цю технологію безпосередньо, для інтеграції з веб-інтерфейсами необхідні додаткові шлюзи. Крім того, система потребує MQTT-брокера, який виступає посередником у передачі даних, що додає рівень складності при налаштуванні.

Системи моніторингу на основі CoAP (Constrained Application Protocol) працюють за принципом легкого протоколу на основі REST, який дозволяє пристроям передавати інформацію як за запитом, так і асинхронно. Основною перевагою CoAP є його енергоефективність, оскільки протокол оптимізовано для

роботи на пристроях з обмеженими ресурсами. Це робить його ідеальним вибором для IoT-пристроїв, які не підтримують важчі протоколи, такі як HTTP або MQTT. Проте, CoAP має і свої недоліки. Зокрема, обмежена підтримка браузерами вимагає використання додаткових шлюзів для інтеграції з веб-інтерфейсами. Крім того, протокол менш популярний у порівнянні з іншими стандартами, тому його екосистема і підтримка розробниками є значно меншою.

Ще одним підходом для організації систем моніторингу є використання Server-Sent Events (SSE), які забезпечують серверу можливість надсилати дані в реальному часі безпосередньо клієнту через звичайне HTTP-з'єднання. Це дозволяє створювати ефективні рішення для передачі даних з охоронних систем у режимі стримінгу. Головною перевагою SSE є простота впровадження, оскільки технологія забезпечує односпрямований зв'язок (сервер → клієнт) без необхідності складних налаштувань, як у випадку з WebSockets. Проте саме односпрямованість з'єднання може бути обмеженням, особливо якщо система потребує двосторонньої комунікації. Крім того, масштабованість SSE обмежена, і при великій кількості клієнтів ефективність передачі даних може знижуватися.

Охоронні системи моніторингу IoT-пристроїв є компонентом сучасної безпеки, забезпечуючи контроль за станом об'єктів та миттєву реакцію на загрози. Для реалізації таких систем використовуються різноманітні технології передачі даних, які впливають на швидкість, ефективність і стабільність роботи системи. Однією з найбільш розповсюджених підходів є використання AJAX – технології, що дозволяє асинхронно запитувати дані без перезавантаження сторінки [17].

Однак, з розвитком технологій з'явилися альтернативи, які краще підходять для роботи з реальним часом та масштабованими IoT-системами. У цьому порівнянні розглянуто основні технології, які застосовуються в охоронних системах моніторингу, включаючи AJAX, WebSockets, MQTT, CoAP і Server-Sent Events (SSE). Кожна з них має свої переваги та недоліки залежно від вимог до системи, як-от обробка сигналів тривоги, відеостримінг чи масштабованість.

В табл. 2.1 наведено, що порівнює ці технології за ключовими параметрами: реальний час, масштабованість, складність впровадження, ресурсоємність та сумісність із веб-технологіями.

Таблиця 2.1

Порівняння технологій моніторингу IoT-пристроїв в охоронних системах

Критерій	**AJAX (Охоронні системи)**	**WebSockets**	**MQTT**	**CoAP**	**SSE**
Реальний час	Середньо	Високо	Високо	Середньо	Високо
Масштабованість	Середньо	Високо	Високо	Високо	Середньо
Складність впровадження	Низька	Середня	Середня	Середня	Низька
Ресурсоємність	Висока	Середня	Низька	Низька	Середня
Сумісність із веб	Висока	Висока	Низька	Низька	Висока

2.3 Аналіз аналогів систем моніторингу безпеки IoT-пристроїв

Охоронні системи моніторингу IoT-пристроїв стали важливим компонентом сучасних інфраструктур безпеки. Вони дозволяють контролювати стан об'єктів, аналізувати події та своєчасно реагувати на потенційні загрози. Завдяки широкому вибору платформ, таких як AWS IoT Core, Google IoT Core, Microsoft Azure IoT Hub та інші, організації отримують інструменти для підключення, управління та моніторингу пристроїв у реальному часі. Кожна з цих платформ пропонує унікальні можливості та функціонал, що задовольняє різні потреби користувачів.

Різні платформи відрізняються не лише функціональністю, але й підходами до забезпечення безпеки. У сучасному світі, де обсяг даних постійно зростає, а кількість пристроїв IoT може досягати мільйонів, критично важливим є забезпечення надійного захисту даних та стабільної роботи системи. Такі платформи, як AWS IoT Core, зосереджуються на інтеграції з хмарними сервісами та аналітичними інструментами, тоді як Google IoT Core і Microsoft Azure IoT Hub надають додаткові можливості для обробки даних на периферії та аналізу великих масивів інформації.

У цьому контексті важливим є порівняння платформ з точки зору їхніх ключових особливостей, функціоналу, рівня безпеки, а також можливостей інтеграції з сучасними технологіями, такими як AJAX. В табл. 2.2, що узагальнює основні характеристики популярних систем моніторингу IoT-пристроїв.

Таблиця 2.2

Характеристики популярних систем моніторингу IoT-пристроїв

Платформа	Ключові особливості	Переваги	Недоліки
AWS IoT Core	- MQTT, WebSockets, HTTP - IoT Device Defender - Інтеграція з AWS Lambda, SageMaker	- Масштабованість - Надійні інструменти безпеки - Широка екосистема	- Висока складність для початківців - Можливі значні витрати при великих масштабах
Google IoT Core	- MQTT, HTTP - BigQuery, DataFlow - TensorFlow для ML	- Легка інтеграція з екосистемою Google Cloud - Потужна аналітика великих даних	- Обмежені інструменти безпеки - Висока залежність від хмар Google
Microsoft Azure IoT Hub	- Двостороння комунікація - IoT Edge для обробки на периферії - Підтримка сертифікатів	- Підтримка периферійних пристроїв - Гнучкі інструменти обробки даних - Інтеграція з Power BI	- Складність налаштування - Висока ціна для великих проектів
IBM Watson IoT	- Реальний час - AI та ML інтеграція - Підтримка різних протоколів	- Потужна аналітика та прогнозування - Розвинені AI-інструменти - Надійна безпека	- Складна система ліцензування - Менш популярна порівняно з AWS чи Google Cloud

Продовження таблиці 2.2

ThingsBoard (Open-source)	- Інтеграція з різними пристроями - Гнучкі інструменти налаштування - Dashboards	- Безкоштовне використання - Повна гнучкість - Активна спільнота розробників	- Відповідальність за підтримку - Обмежена офіційна підтримка
Node-RED (Open-source)	- Гнучка інтеграція IoT-пристроїв - Інтуїтивний візуальний інтерфейс	- Простота налаштування - Легка адаптація для невеликих проектів - Безкоштовний доступ	- Вимагає ручного налаштування - Менш ефективний для великих проектів

Функціонал платформ для моніторингу IoT-пристроїв варіюється залежно від їхніх основних завдань та орієнтації на різні категорії користувачів. Наприклад, AWS IoT Core надає широкий набір можливостей для моніторингу та обробки даних у режимі реального часу завдяки підтримці протоколів MQTT, WebSockets і HTTP. Google IoT Core зосереджується на інтеграції з інструментами аналітики великих даних, такими як BigQuery, та на можливостях машинного навчання через TensorFlow. Microsoft Azure IoT Hub забезпечує високий рівень безпеки завдяки підтримці сертифікатів, шифруванню та інтеграції з периферійними пристроями через Azure IoT Edge [18].

Рівень захисту також відрізняється. AWS IoT Core вирізняється потужними інструментами безпеки, такими як IoT Device Defender, що дозволяє виявляти аномалії та захищати пристрої від атак. Azure IoT Hub пропонує подібні можливості із захистом даних на всіх рівнях комунікації. Google IoT Core, хоча й забезпечує базові функції захисту, трохи поступається за глибиною інструментів. Відкриті платформи, такі як ThingsBoard, пропонують базові можливості безпеки, але потребують додаткового налаштування та ресурсів для захисту від потенційних загроз.

AJAX, як технологія для асинхронного обміну даними між клієнтськими пристроями та сервером, може бути інтегрований у більшість платформ моніторингу IoT для створення зручного веб-інтерфейсу. У системах, таких як

AWS IoT Core та Google IoT Core, AJAX може використовуватися для отримання та відображення даних від IoT-пристроїв без перезавантаження веб-сторінки, що дозволяє створити зручні дашборди для користувачів [19].

У контексті Microsoft Azure IoT Hub AJAX може застосовуватися для асинхронного запиту стану пристроїв або подій, інтегруючись із API хмарної платформи. У відкритих платформах, таких як ThingsBoard, AJAX використовується для побудови веб-інтерфейсів із графіками, таблицями та динамічними даними. Незважаючи на універсальність AJAX, для роботи з великою кількістю пристроїв або обробки подій у реальному часі краще застосовувати WebSockets або інші сучасні протоколи для забезпечення більшої ефективності.

3 РОЗРОБЛЕННЯ ІНТЕГРОВАНОЇ СИСТЕМИ МОНІТОРИНГУ БЕЗПЕКИ IOT-ПРИСТРОЇВ НА БАЗІ ТЕХНОЛОГІЇ AJAX

3.1 Вибір архітектури системи моніторингу

Архітектура системи моніторингу безпеки IoT-пристроїв є основою для забезпечення ефективного та безперебійного контролю за станом підключених пристроїв і їх захисту від потенційних загроз. Основна мета цієї архітектури полягає у створенні інтегрованої системи, яка здатна забезпечувати збір, обробку та аналіз даних у режимі реального часу, водночас зберігаючи високу продуктивність, надійність і масштабованість.

На етапі розробки архітектури потрібно врахувати вибір апаратних компонентів, таких як датчики, які мають збирати інформацію про фізичний стан об’єктів чи середовища. Ці пристрої мають бути високочутливими, енергоефективними та адаптованими до роботи у складних умовах. Для зменшення витрат і підвищення надійності, важливо обирати датчики з довгим терміном служби та підтримкою сучасних протоколів зв’язку.

Центральний елемент архітектури – сервер або хаб, що відповідає за обробку отриманих даних. Цей компонент повинен забезпечувати централізовану координацію роботи системи, обробляти великий обсяг інформації та надсилати результати аналізу до користувача або інших модулів системи. Для забезпечення ефективної роботи системи необхідно використовувати сервери з високою обчислювальною потужністю, які підтримують паралельну обробку запитів. Крім того, важливо інтегрувати технології для резервного копіювання та відновлення даних, щоб уникнути втрат у разі збоїв.

У сучасних системах розумного будинку вибір апаратного забезпечення відіграє ключову роль у забезпеченні їхньої надійності, ефективності та інтеграції з іншими елементами. Відповідне обладнання дозволяє не лише виконувати базові функції моніторингу та управління, але й створювати комплексні автоматизовані сценарії, що підвищують комфорт і безпеку користувачів. У табл. 3.1 наведено

основні типи апаратного забезпечення, зокрема датчики, сервери та пристрої обробки даних, які забезпечують стабільну роботу розумного будинку. Особливу увагу приділено пристроям компанії Ajax, які поєднують високу якість, надійність і зручність використання.

Таблиця 3.1

Апаратне забезпечення

Категорія обладнання	**Модель Ajax**	**Функція**	**Особливості для надійності**
Ajax Hub	Ajax Hub	Управління всією системою безпеки, обробка сигналів від датчиків, передача тривожних повідомлень	Двосторонній захищений протокол Jeweller, резервне живлення до 16 годин, захист від саботажу
Датчики руху	Ajax MotionProtect	Виявлення руху в приміщеннях	Стійкість до тварин (вагою до 20 кг), захист від фальшивих спрацьовувань, тривалий час роботи батареї (до 7 років)
Датчики відкриття дверей/вікон	Ajax DoorProtect	Виявлення відкриття дверей або вікон	Захист від саботажу, компактний дизайн, підтримка різних типів дверей/вікон
	Ajax DoorProtect Plus	Додатково фіксує нахил або удар по вікну чи дверям	Ідеально підходить для вікон, які можуть залишатися відкритими для провітрювання
Інтерфейси управління	Ajax SpaceControl	Бездротовий пульт для управління	Компактний дизайн, можливість активації режиму тривоги з одного натискання

Система безпеки Ajax Systems працює на базі бездротового зв’язку за допомогою протоколу Jeweller, який забезпечує стабільний захист та шифрування переданих даних. Всі датчики з'єднуються з Ajax Hub або його розширеною версією

Ajax Hub 2 Plus, яка підтримує більшу кількість пристроїв і має резервні канали зв’язку.

Підключення здійснюється через мобільний додаток Ajax Security System:

1. Відкриття додатка та вибір центрального блоку Ajax Hub.
2. Сканування QR-коду датчика, який знаходиться на корпусі пристрою.
3. Додавання пристрою в систему та налаштування його параметрів.
4. Тестування сигналу для визначення оптимального розташування датчика.

Після підключення датчики працюють у режимі реального часу, передаючи сигнали на Ajax Hub, який обробляє їх і активує відповідні сценарії або надсилає повідомлення користувачам. Характеристики моделей Ajax Hub для інтеграції в систему моніторингу, наведені в табл. 3.2.

Таблиця 3.2

Характеристики моделей Ajax Hub для інтеграції в систему моніторингу

Модель	**Кількість пристроїв**	**Дальність зв’язку (м)**	**Типи підключення**	**Додаткові функції**
Ajax Hub	До 100	До 2000	Ethernet	Базова модель
Ajax Hub 2	До 150	До 2000	Ethernet + 2 SIM (2G)	Фотофіксація руху
Ajax Hub 2 Plus	До 200	До 2000	Ethernet + Wi-Fi + 2 SIM (LTE)	Інтеграція IP-камер, підтримка Fibra

Ajax Hub – підходить для невеликих об’єктів (квартири, офіси, невеликі будинки).

Ajax Hub 2 – оптимальний для середніх об'єктів (будинки, магазини), підтримує датчики з фотофіксацією.

Ajax Hub 2 Plus – ідеальний для великих комерційних об’єктів, заводів, складів, має розширені можливості зв’язку та інтеграцію з камерами.

3.2 Захист даних та забезпечення безпеки

Система безпеки Ajax Systems забезпечує високий рівень захисту даних та стійкість до кібератак завдяки впровадженню сучасних технологій шифрування та автентифікації. Ці методи гарантують захищений обмін даними між пристроями, запобігають несанкціонованому доступу до системи та забезпечують конфіденційність інформації.

Для безпечного обміну інформацією між пристроями та центральним хабом використовується протокол Jeweller. Основні характеристики захисту протоколу Jeweller:

1. Шифрування даних Jeweller використовує шифрування за алгоритмом AES-128, який забезпечує захищений обмін інформацією між пристроями та хабом. Цей алгоритм є одним із найбільш стійких до злому, оскільки дані кодуються унікальними ключами, що виключає можливість їх перехоплення або модифікації сторонніми особами.

2. Захист від глушіння сигналу Jeweller постійно моніторить радіочастотний діапазон, у якому працюють пристрої, для виявлення спроб глушіння. У разі виявлення таких дій система миттєво надсилає сповіщення користувачу та переходить на резервний канал зв’язку, наприклад, мобільну мережу через SIM-карту. Це забезпечує безперервну роботу системи навіть у разі інтенсивних перешкод.

3. Автентифікація пристроїв Кожен пристрій, підключений до хаба, має свій унікальний ідентифікатор. Jeweller перевіряє автентичність кожного сигналу, що надходить від пристроїв, щоб виключити можливість підключення підроблених чи несанкціонованих пристроїв до системи. Це гарантує, що тільки сертифіковані датчики Ajax можуть бути частиною екосистеми.

4. Енергоефективність Jeweller оптимізовано для мінімального споживання енергії. Завдяки цьому датчики можуть працювати від однієї батареї до 7 років, що є важливою перевагою для автономних систем безпеки.

5. Дальність з’єднання Протокол забезпечує зв’язок на відстані до 2000 метрів у відкритому просторі. Це дозволяє використовувати систему Ajax у великих приміщеннях, таких як склади, офіси чи приватні будинки, без втрати якості зв’язку.

6. Швидкість передачі даних Jeweller дозволяє пристроям передавати тривожні сигнали до хаба за 0,15 секунди. Така швидкість забезпечує миттєве реагування системи на будь-які події, наприклад, відкриття дверей, рух чи задимлення.

Ajax Systems має вбудовані механізми, що забезпечують стійкість до глушіння бездротового сигналу:

– Постійний моніторинг частотного спектра для виявлення спроб глушіння.

– Автоматичний перехід на резервний канал зв’язку (наприклад, з Wi-Fi на мобільну мережу), якщо основний канал блокується.

– Надсилання сповіщень про спроби глушіння до мобільного додатка користувача.

Щоб уникнути втрати даних у разі кібератаки або збоїв системи, Ajax Systems підтримує резервне копіювання даних:

– Хмарне збереження даних на сервері Ajax Cloud, що забезпечує резервну копію інформації про всі пристрої та події.

– Локальне збереження подій у пам’яті хаба, що дозволяє зберігати до 250 подій, навіть якщо немає з’єднання з хмарою.

Стійкість до фізичних втручань:

– Всі пристрої Ajax мають захист від саботажу. У разі спроби розкриття корпусу або демонтажу датчика система миттєво повідомляє користувача.

– Хаб обладнаний резервним джерелом живлення, яке дозволяє йому працювати до 16 годин у разі відключення електроенергії.

3.3 Процес налаштування Ajax Hub

Для початку налаштування Ajax Hub його необхідно підключити до електромережі. Це забезпечить стабільну роботу пристрою та безперервний зв’язок із датчиками та іншими елементами системи. Вибравши відповідне місце для встановлення, слід підключити адаптер живлення до роз’єму DC 12V, що розташований на задній панелі хаба. Потім адаптер вставляється у стандартну розетку 110-240V. Якщо підключення виконано правильно, на корпусі хаба загориться індикатор живлення, що свідчить про успішну активацію пристрою. У разі відключення електроенергії Ajax Hub продовжить працювати за рахунок вбудованого резервного акумулятора, що забезпечує автономність роботи на кілька годин.

Після підключення живлення необхідно забезпечити з’єднання хаба з інтернетом. Це потрібно для синхронізації з мобільним додатком та віддаленого керування системою. Існує кілька варіантів підключення, і вибір залежить від моделі пристрою та доступних засобів зв’язку. Для дротового підключення використовується Ethernet-кабель, який вставляється у відповідний роз’єм на корпусі хаба, після чого пристрій автоматично отримає мережеві параметри.

Якщо використовується мобільний зв’язок, слід встановити SIM-карту у спеціальний слот, розташований під задньою кришкою пристрою. Це дозволяє підтримувати 2G/3G/4G-з’єднання залежно від моделі хаба та оператора мобільного зв’язку. Використання SIM-карти є особливо корисним у випадку втрати дротового з’єднання, оскільки дозволяє системі залишатися на зв’язку та передавати тривожні сповіщення навіть за відсутності основного інтернет-з’єднання.

Для моделей Ajax Hub 2 Plus є можливість підключення через Wi-Fi. Щоб активувати цей режим, необхідно увійти до мобільного додатка Ajax Security System, вибрати хаб у списку пристроїв та ввести параметри бездротової мережі (SSID і пароль). Після збереження налаштувань пристрій з’єднається з інтернетом

через Wi-Fi, що дасть змогу використовувати його без необхідності прокладання дротового з’єднання.

Наступним кроком є додавання хаба в систему безпеки через мобільний додаток. Спершу потрібно завантажити застосунок Ajax Security System на смартфон або планшет через App Store чи Google Play (рис. 3.1).

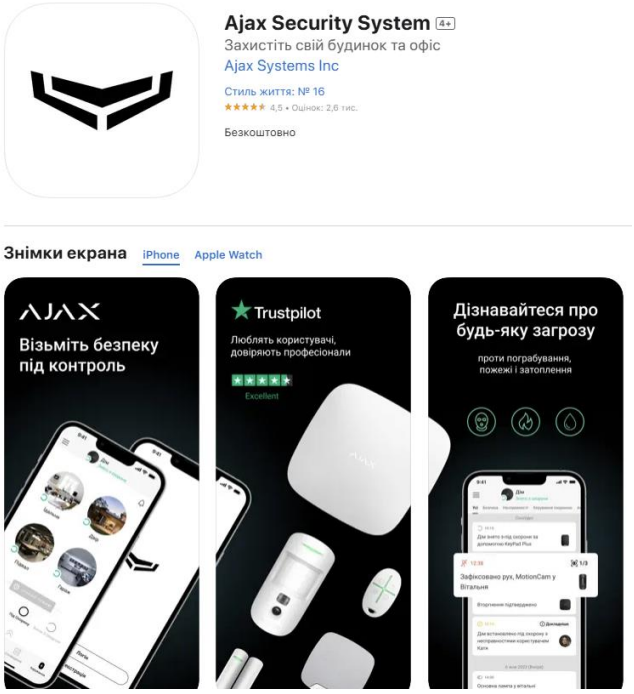


Рис. 3.1 Застосунок Ajax Security System

Після встановлення додатка необхідно створити новий обліковий запис або увійти до наявного. У головному меню вибирається опція "Додати новий хаб" (рис.3.2).

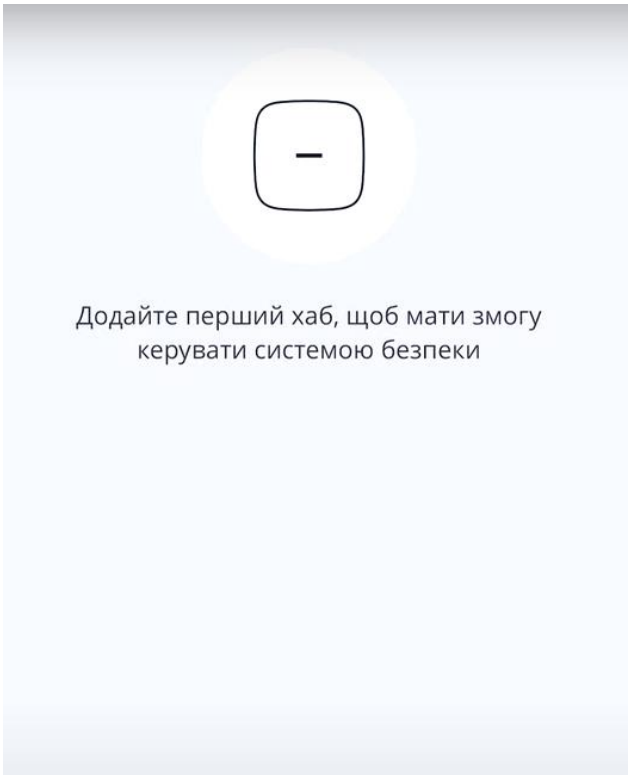


Рис. 3.2 Створення облікового запису

Після чого потрібно відсканувати QR-код, розташований на нижній панелі пристрою. Це дозволяє миттєво додати хаб до системи безпеки та синхронізувати його з мобільним додатком (рис.3.3-3.4).

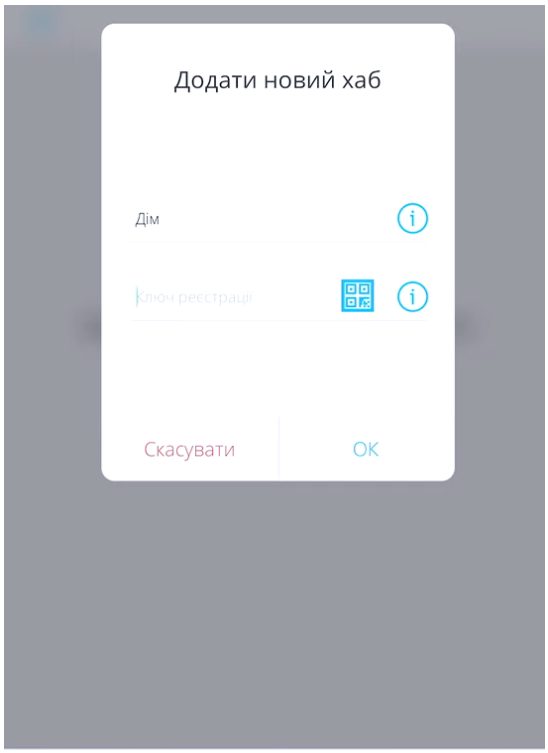


Рис. 3.3 Додавання нового пристрою, а саме Hub AJAX

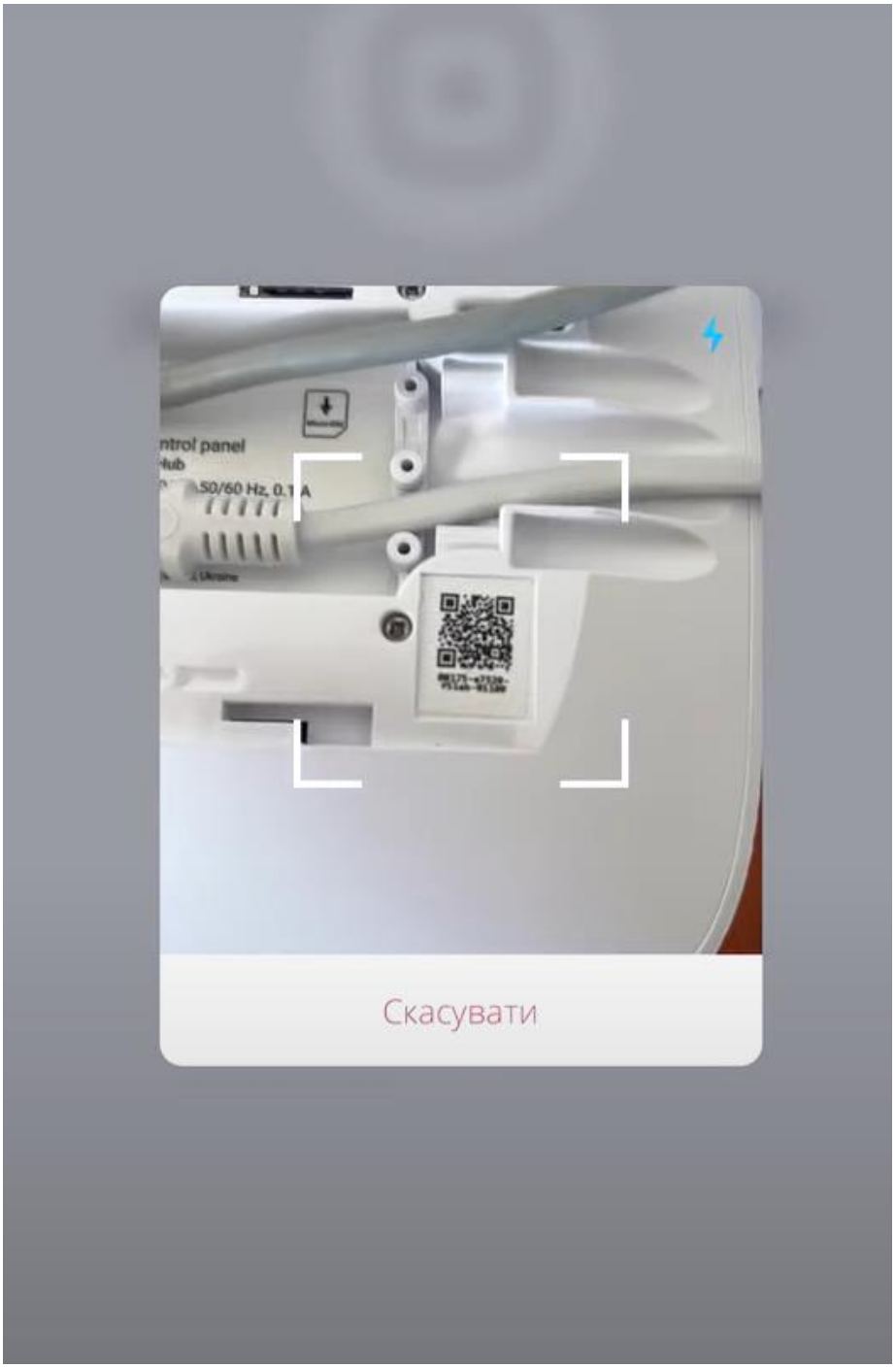


Рис. 3.4 Сканування QR-коду

Після додавання Hub, потрібно створити кімнату, наприклад Дім (рис. 3.5).

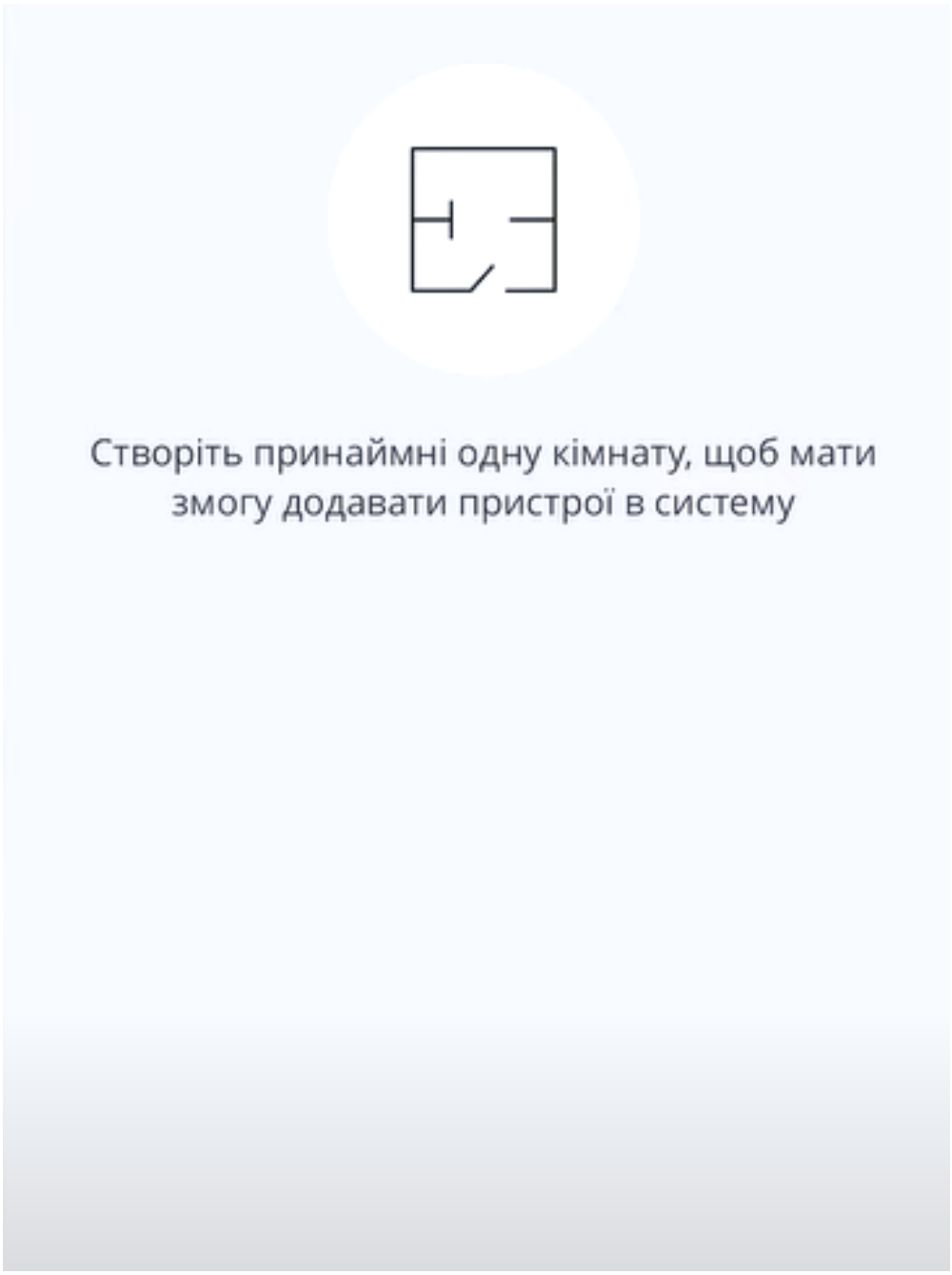


Рис. 3.5 Створення кімнати «Дім»

Після успішного підключення хаба до системи, у мобільному додатку з’являється відповідний інтерфейс, який дозволяє додавати нові пристрої та налаштовувати їх функціонал. На рис. 3.6 показано екран додатку, який відображає підключений Ajax Hub і готовність системи до подальшої інтеграції пристроїв.

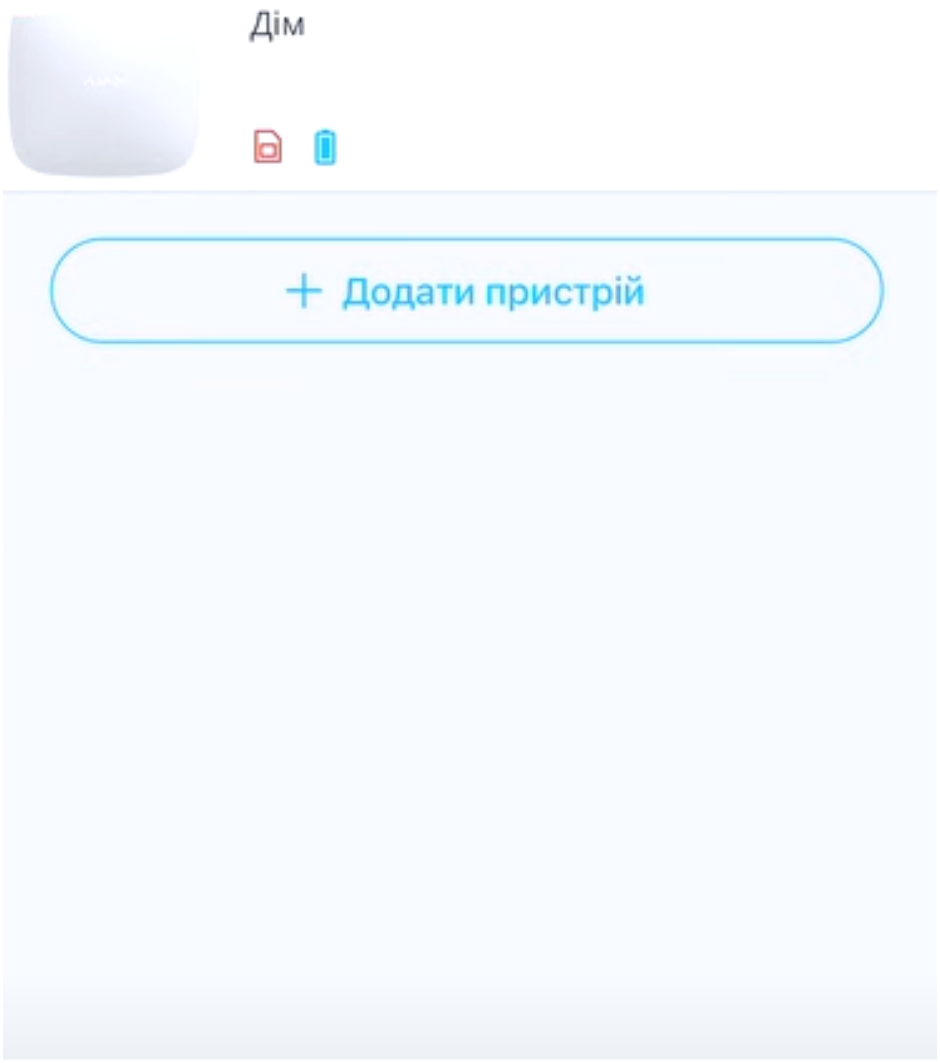


Рис. 3.6 Успішно додано Ajax Hub

Після успішного додавання пристрою до системи, на екрані з’явилася інформація про стан хаба, рівень сигналу зв’язку. З цього моменту Ajax Hub готовий до роботи, і можна почати підключати інші пристрої системи безпеки, створювати сценарії автоматизації та налаштовувати рівні доступу для інших користувачів.

Датчики відкриття дверей або вікон дозволяють відстежувати зміни стану об'єктів і сповіщати про спроби несанкціонованого доступу. На рис. 3.7 показано екран налаштувань додавання пристрою, де можна ввести ім’я, вибрати кімнату та відсканувати QR-код для реєстрації датчика у системі.

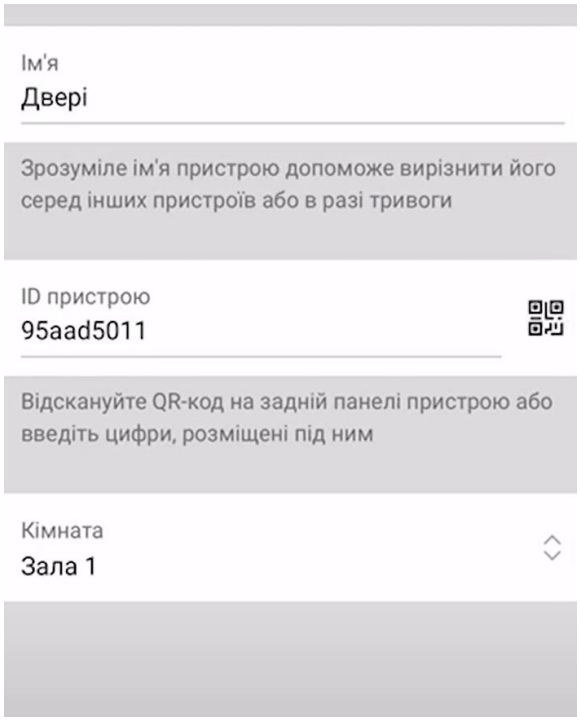


Рис. 3.7 Додавання Ajax DoorProtect

Під час підключення датчика Ajax DoorProtect до хаба пристрій передає запит на реєстрацію лише у момент увімкнення. На рис. 3.8 показано необхідність увімкнення пристрою для його реєстрації. Якщо пристрій уже увімкнено, його потрібно вимкнути, зачекати кілька секунд і увімкнути знову, щоб забезпечити правильний процес реєстрації.

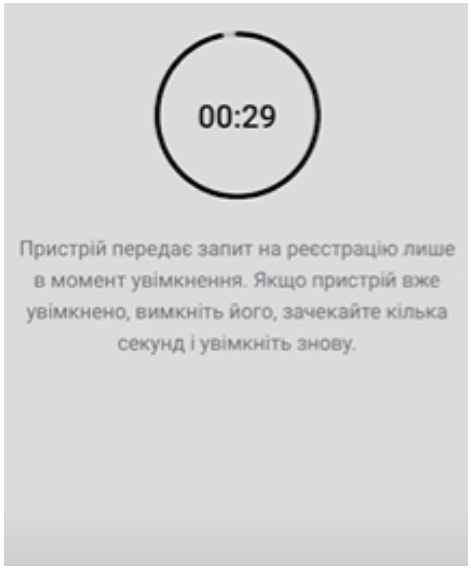


Рис. 3.8 Необхідність увімкнення пристрою

Після успішного підключення датчика Ajax DoorProtect до хаба система підтверджує його реєстрацію. На рис. 3.9 показано, що пристрій успішно зареєстровано та готовий до використання.

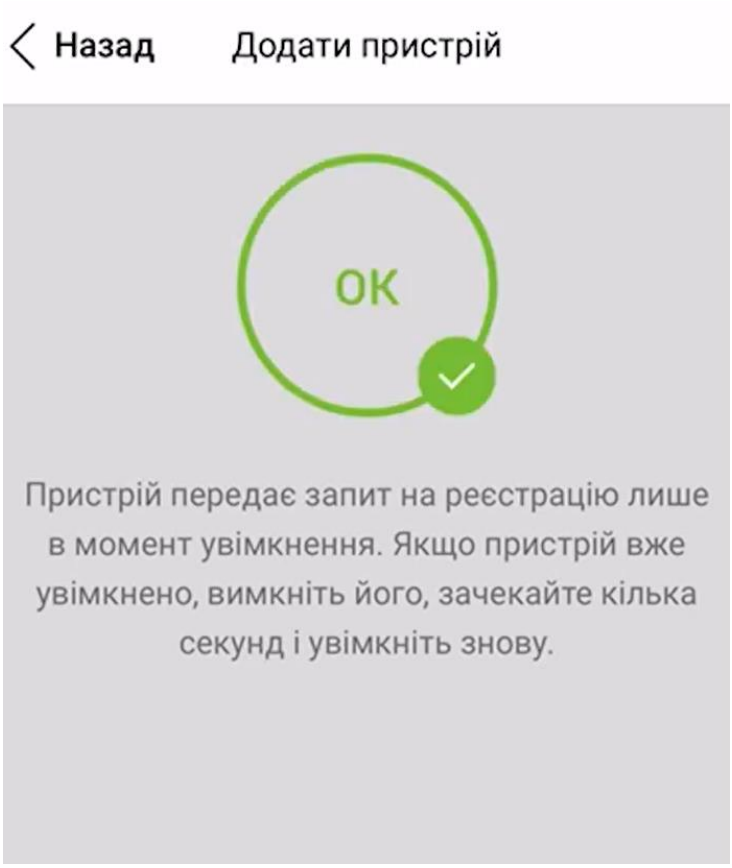


Рис. 3.9 Успішно зареєстровано DoorProtect

На рис. 3.10 показано процес налаштування датчика руху Ajax MotionProtect через мобільний додаток Ajax Security System. У цьому інтерфейсі користувач може ввести зрозуміле ім’я пристрою (наприклад, "Коридор"), прив’язати датчик до конкретної кімнати (наприклад, "Зала 1") та зареєструвати його в системі шляхом сканування QR-коду, розташованого на задній панелі датчика.

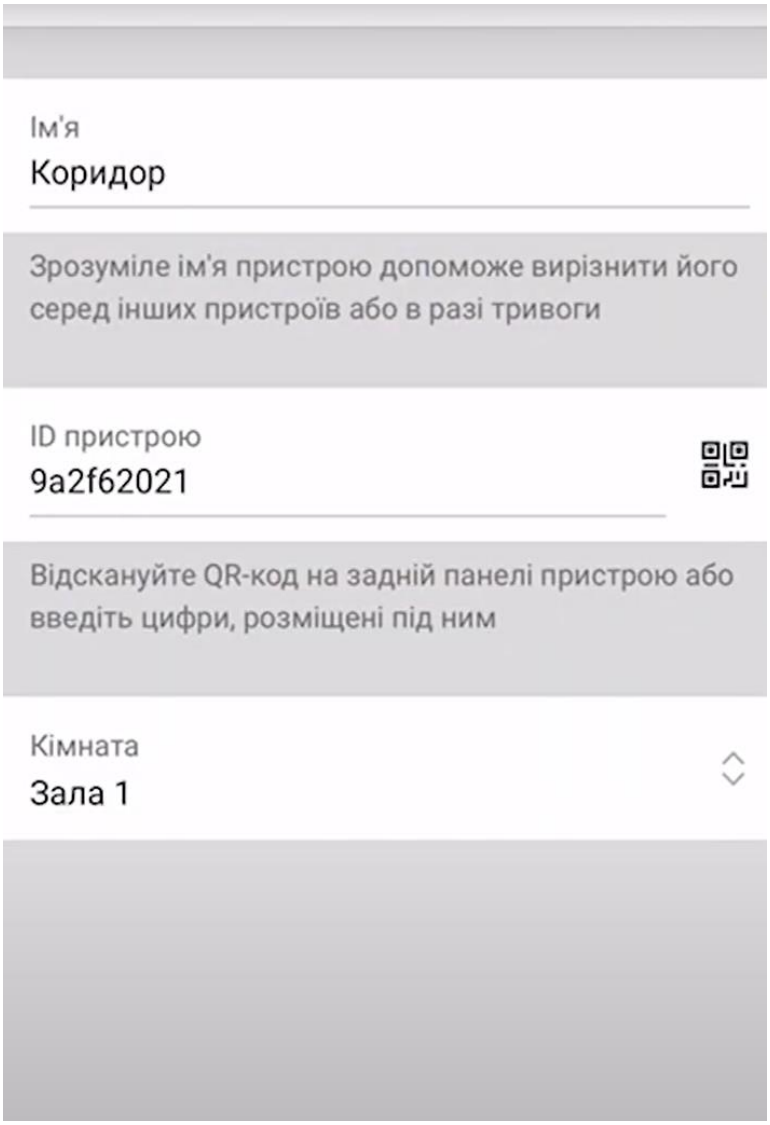


Рис. 3.10 Додавання MotionProtect

Наступний пристрій це пульт – Ajax SpaceControl White, забезпечує зручне дистанційне керування охоронною системою, включаючи активацію та деактивацію режиму охорони, а також екстрене викликання тривоги. На рис. 3.11 зображено процес налаштування пульта Ajax SpaceControl White у мобільному додатку Ajax Security System**.**

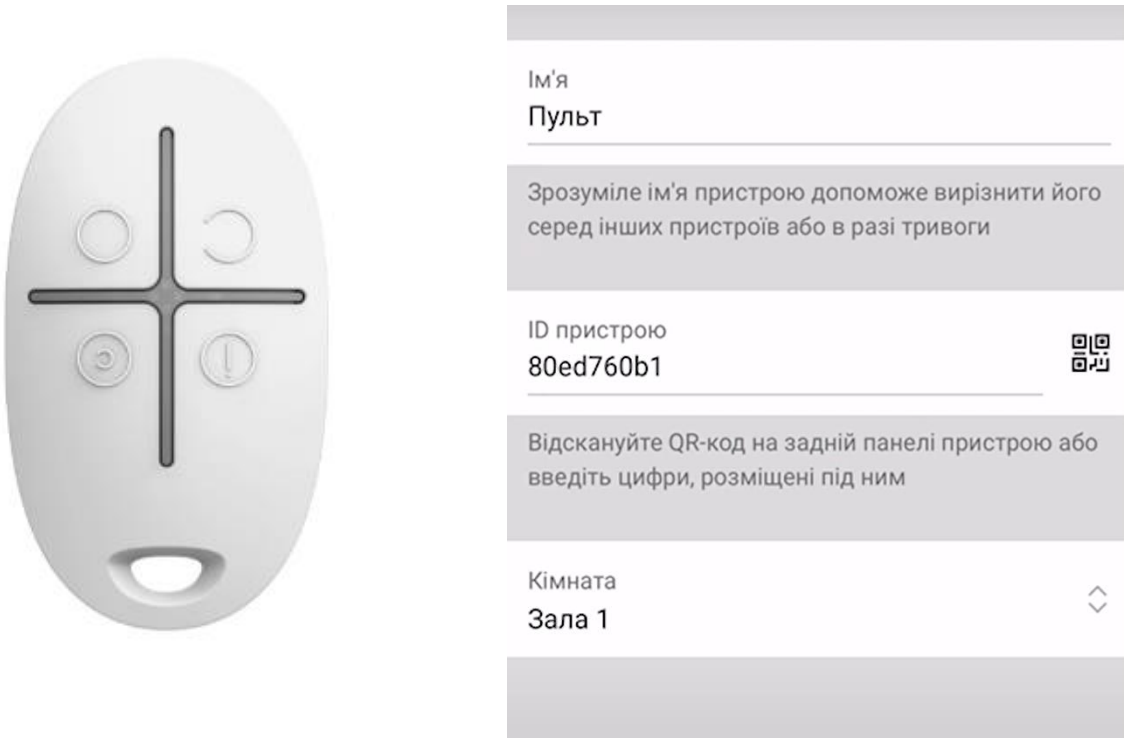


Рис. 3.11 Ajax SpaceControl White

Інтегрована система моніторингу безпеки IoT-пристроїв на базі технології AJAX готова до роботи. На рис. 3.12 представлено інтерфейс мобільного додатку Ajax Security System, який демонструє успішно підключені пристрої: хаб, датчики відкриття дверей (DoorProtect), датчик руху (MotionProtect) та пульт керування (SpaceControl). Усі пристрої функціонують у реальному часі, забезпечуючи повноцінний захист та моніторинг заданої зони. Додатково користувач має можливість підключати нові пристрої для розширення функціоналу системи.

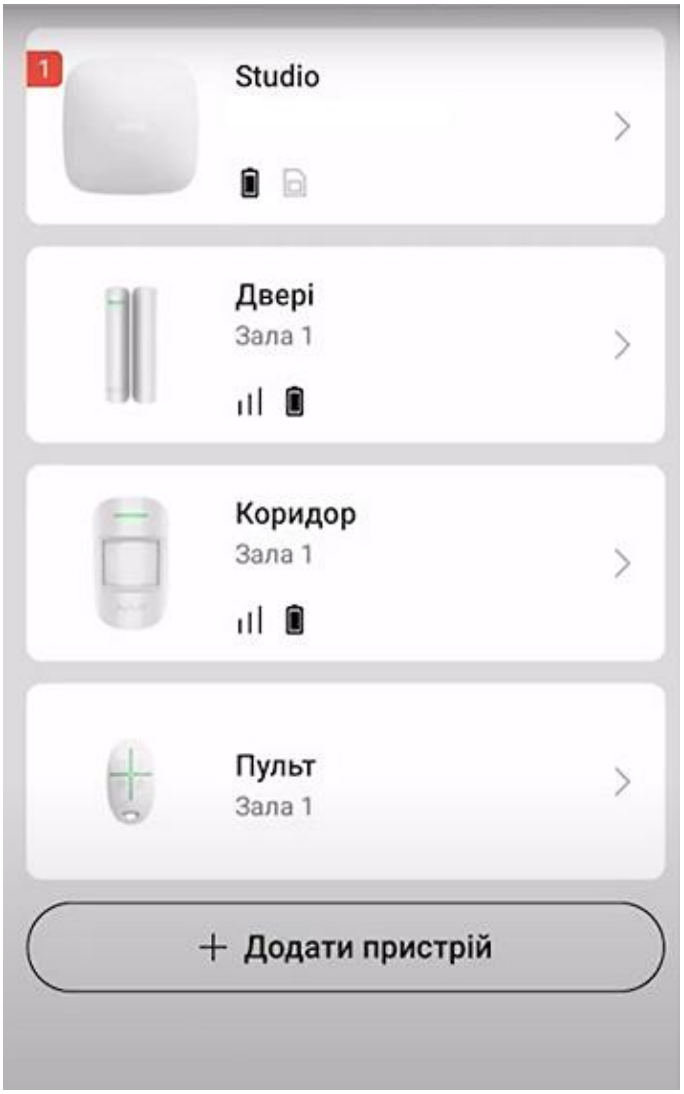


Рис. 3.12 Успішно підключені пристрої

ВИСНОВКИ

Розвиток Інтернету речей (IoT) відкриває нові можливості для автоматизації, оптимізації процесів і створення інноваційних рішень у різних сферах. Разом з тим, зростає потреба в забезпеченні надійності та безпеки таких систем, що обумовлює актуальність дослідження загроз і способів їхнього запобігання.

Розглянуто сутність та особливості технології IoT, яка дозволяє інтегрувати фізичні об’єкти в єдину мережу для обміну даними та виконання завдань без участі людини. Особливості IoT, такі як автоматизація та постійна підключеність, створюють передумови для підвищення ефективності, але водночас стають точками вразливості для кібератак.

Проаналізовано основні загрози безпеки в середовищі IoT, зокрема несанкціонований доступ, витік даних і розподілені атаки. Ці загрози підкреслюють необхідність впровадження багаторівневих систем захисту, таких як шифрування, автентифікація та регулярні оновлення.

Розгляд архітектури інтегрованих систем моніторингу безпеки IoT дозволив окреслити ключові компоненти таких систем, включаючи датчики, сервери та механізми обробки даних. Ці елементи забезпечують цілісний підхід до моніторингу, аналізу даних та автоматичного реагування на потенційні загрози.

Продемонстровано що забезпечення безпеки IoT-пристроїв є багатовимірним завданням, яке вимагає врахування технологічних, організаційних і соціальних аспектів. Використання технології AJAX додатково підсилює ефективність моніторингу та управління IoT-системами, забезпечуючи обробку даних у реальному часі. Це створює основу для впровадження надійних та масштабованих рішень, що відповідають викликам сучасності.

Проведено детальний аналіз технології AJAX, її принципів роботи та ключових особливостей, які роблять її потужним інструментом для моніторингу IoT-пристроїв. AJAX забезпечує асинхронний обмін даними між клієнтом і сервером, що дозволяє отримувати актуальну інформацію в реальному часі без

перезавантаження інтерфейсу. Це створює інтерактивне та зручне середовище для користувачів IoT-систем.

Аналіз аналогів систем моніторингу безпеки IoT-пристроїв дозволив визначити, що сучасні рішення часто комбінують кілька технологій для досягнення максимальної ефективності. У той час як AJAX чудово справляється з завданнями реального часу, інші технології можуть бути використані для забезпечення додаткових функцій, таких як стрімінгові дані або забезпечення низької затримки.

AJAX залишається потужним і гнучким інструментом для моніторингу IoT, особливо у випадках, коли простота та ефективність є пріоритетами. Водночас для вирішення складних задач рекомендується враховувати специфіку кожної технології та застосовувати їх у поєднанні для створення надійних та ефективних рішень.

У третьому розділі було продемонстровано процес побудови інтегрованої системи моніторингу безпеки IoT-пристроїв на базі технології Ajax. Розглянуто ключові етапи налаштування системи, включаючи підключення центрального хаба Ajax Hub, інтеграцію датчиків руху, відкриття дверей/вікон, пульта керування та інших компонентів.

Зазначено, що система Ajax забезпечує високий рівень захисту даних завдяки використанню сучасних методів шифрування та автентифікації, а також захищеного протоколу Jeweller для бездротового зв’язку. Виокремлено переваги налаштування системи через мобільний додаток Ajax Security System, який надає зручний інтерфейс для керування та моніторингу.

Розглянуто можливості розширення та автоматизації системи через сценарії, що дозволяють адаптувати її під різні вимоги користувачів. Також було зазначено, що налаштування окремих компонентів системи, таких як датчики та пульти, є інтуїтивно зрозумілим і забезпечує їх оперативне підключення до хаба.

Таким чином, у третьому розділі продемонстровано, що технологія Ajax відповідає сучасним вимогам до систем безпеки, забезпечуючи високу ефективність, надійність і гнучкість у використанні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. І. М. Сміт та ін., “RFID та інклюзивна модель для IoT”, CASAGRAS Partnership Rep., West Yorkshire, UK, Final Rep., 2009, pp. 10–12.
2. Міністерство промисловості та інформаційних технологій Китаю (2012, лютий). Національний 12-й п’ятирічний план, що включає розвиток IoT (2011–2015) [Інтернет]. Доступно: http://www.gov.cn/zwgk/2012-02/14/content 2065999.htm
3. Бортник К.Я., Ольшевський О.В., Пащук В.Ю. Інтернет речей та як він змінить наше життя у майбутньому. Комп’ютерно-інтегровані технології: освіта, наука, вир-во. 2018. № 30/31. С. 14–18.
4. Журавльов О.В., Сімасов О.А. Інтернетизація та глобальна інституціоналізація економічних систем. Статистика України. 2017. № 4. С. 39–46.
5. Коваль В.В., Замлинський В.А. Ринок послуг Інтернету речей (IoT): сучасний стан та обмеження розвитку. Трансформація економіки та права в умовах системних реформ України : зб. наук. пр. за матеріалами всеукр. наук.-практ. конф. (м. Одеса, 27 жовтня 2017 року) / МОН України, Одес. торг.-екон. ін-т [та ін.]; редкол.: Квач Я.П. [та ін.]. Одеса, 2017. С. 35–37.
6. Баранов О.А. Інтернет речей і охорона здоров’я. Інтернет речей: теоретико-методологічні основи правового регулювання : монографія. 2-ге вид. Харків, 2018. Т. 1: Сфери застосування, ризики і бар’єри, проблеми правового регулювання. С. 24–36.
7. Баранов О.А. Інтернет речей і транспорт. Інтернет речей: теоретико-методологічні основи правового регулювання : монографія. 2-ге вид. Харків, 2018. Т. 1. С. 92–96.
8. Heikki Halttula, Harri Haapasalo, Risto Silvola. Managing data flows в infrastructure projects - the lifecycle process model // Journal of Information Technology in Construction March 2020 (25) pp. 193-211 DOI: 10.36680/j.itcon.2020.012.

Сайт компанії Ajax. URL: https://ajax.systems/ua/blog/orbitands-monitoring-software/ (дата звернення 20.01.202)

9. Маліновський В.І. Аналіз ризиків кіберзагроз і захист даних в сучасних системах Інтернету речей (IoT) / В.І. Маліновський // Матеріали LI-ї Науковотехнічної конференції факультету інформаційних технологій та комп'ютерної 82 інженерії. Факультет інформаційних технологій та комп'ютерної інженерії(ФІТКІ). – 2022. 31.05.2022. – ВНТУ: URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/14999.

10. Diogenes Y. Cybersecurity: strategies of attack and defense / Y. Diogenes, E. Ozkay. — M.: DMK Press, 2020. — 326 p.

11. Cory Beard, William Stallings Wireless Communication Networks and Systems. - Pearson Education, 2015. – 672 p.

12. Kakareka, Almantas У. Vacca, John. Computer and Information Security Handbook. Morgan Kaufmann Publications. Elsevier Inc. 2009. – p. 393. ISBN 978-0-12- 374354-1.

13. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.

14. D. Evans, “The Internet of things: How the next evolution of the Internet is changing everything,”CISCO, San Jose,CA, USA,White Paper, 2011.

15. L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

16. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future Internet: The Internet of Things architecture, possible applications and key challenges,” inProc. 10th Int. Conf. FIT, 2012, pp. 257–260.

17. J. Gubbi, R. Buyya, S.Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013

18. P. Lopez, D. Fernandez, A. J. Jara, and A. F. Skarmeta, “Survey of Internet of Things technologies for clinical environments,” in Proc. 27th Int. Conf. WAINA, 2013, pp. 1349–1354.

ДЕМОНСТРАЦІЙНИЙ МАТЕРІАЛ (Презентація)

Державний університет інформаційно-комунікаційних технологій

Кафедра інформаційних систем та технологій

Кваліфікаційна робота на тему:

«Інтегрована система моніторингу безпеки IoT-пристроїв на базі технології AJAX»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Виконав: НЕЧАЙ Олександр ІСД-42
Науковий керівник роботи: ТКАЛЕНКО Оксана

КИЇВ - 2025

Актуальність теми: Використання технології AJAX для створення інтегрованої системи моніторингу безпеки дозволяє здійснювати асинхронний обмін даними з IoT-пристроями в режимі реального часу. Це забезпечує ефективність у відстеженні й аналізі даних, швидке реагування на інциденти безпеки та значне зменшення навантаження на мережу.

Мета роботи – розробка рекомендацій щодо створення інтегрованої системи моніторингу безпеки IoT-пристроїв на базі AJAX для ефективного контролю, захисту та відстеження даних у реальному часі.

Об'єкт дослідження – інтегровані системи моніторингу безпеки для IoT-пристроїв.

Предмет дослідження – особливості розроблення, впровадження та захисту інтегрованої системи моніторингу IoT-пристроїв на основі технології AJAX.

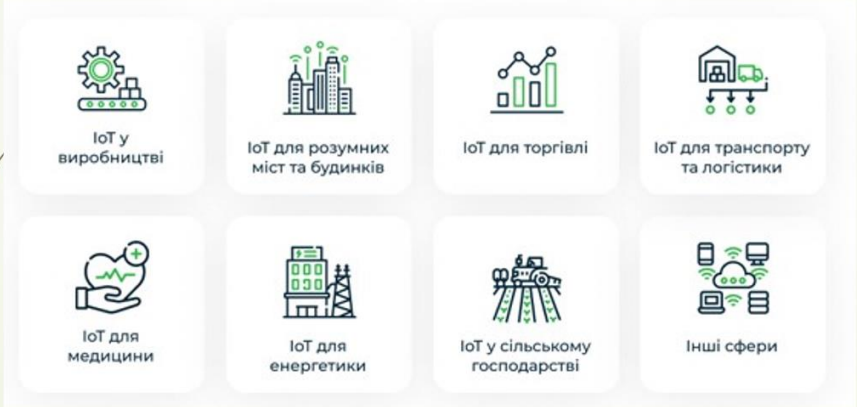
Наукові завдання:

- ❑ вивчити особливості технології IoT та основні загрози безпеки, пов'язані з IoT-пристроями;
- ❑ провести огляд та аналіз технології AJAX і можливостей її використання для моніторингу даних у реальному часі;
- ❑ порівняти технологію AJAX з аналогами для вибору оптимального рішення для моніторингу IoT-пристроїв;
- ❑ запропонувати методи захисту даних у системі моніторингу, що забезпечать безпечну передачу та зберігання інформації;
- ❑ розробити рекомендації щодо інтегрованої системи моніторингу безпеки IoT-пристроїв на базі технології AJAX.

Основні сфери застосування IoT

3

Інтернет речей (IoT) використовується у багатьох галузях для автоматизації, збору даних і підвищення ефективності.



Блок-схема 1. Сфери застосування IoT

Пристрої системи безпеки Ajax

4

Рис. 1. Hub – центральний блок системи безпеки Ajax

Рис. 2. Датчики руху

Рис. 3. Датчики відкриття дверей/вікон DoorProtect

Рис. 4. Датчик диму FireProtect

Рис. 5. Сирени Ajax

Аналіз аналогів Ajax

Рис. 6. Система «розумного будинку» Xiaomi Mijia

Рис. 7. Система «розумного будинку» Google Home

Рис. 8. Система «розумного будинку» Amazon Alexa

Процес налаштування Ajax Hub

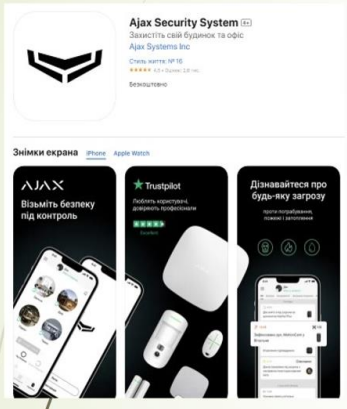


Рис. 9. Завантаження застосунку Ajax Security System

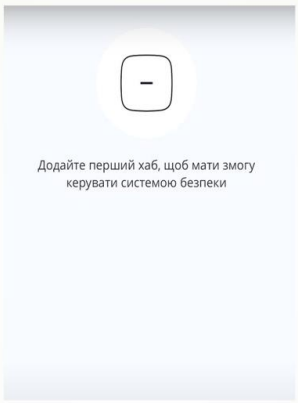


Рис. 10. Створення облікового запису

Рис. 11. Додавання нового пристрою, а саме Hub AJAX

Процес налаштування Ajax Hub

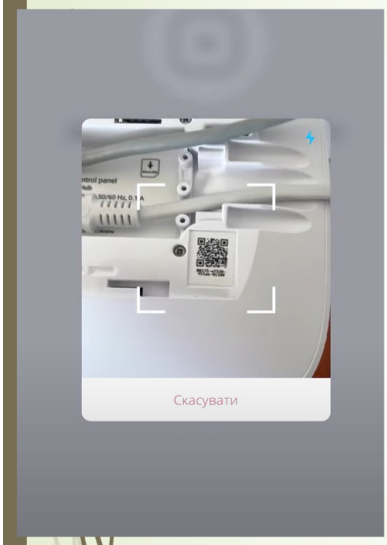


Рис. 12. Сканування QR-коду

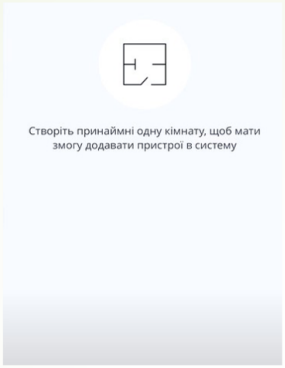


Рис. 13.
Створення кімнати «Дім»

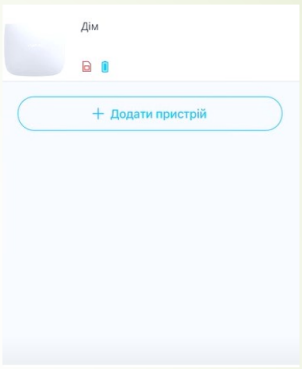


Рис. 14.
Успішно додано Ajax Hub

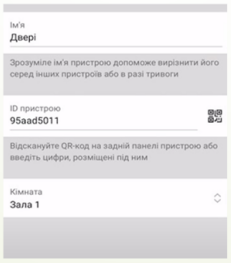


Рис. 15. Додавання Ajax DoorProtect

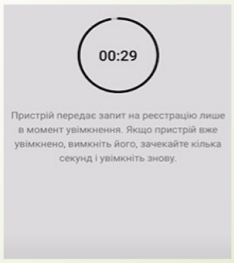


Рис. 16. Увімкнення пристрою

Збірка та налаштування компонентів контролера

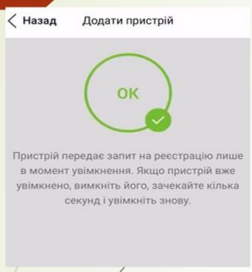


Рис. 17. Успішно
зареєстровано DoorProtect

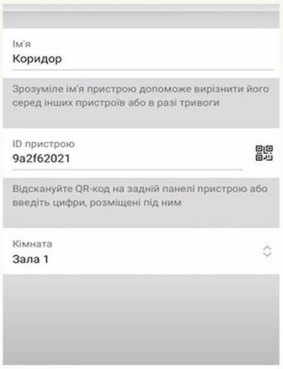


Рис. 18. Додавання MotionProtect

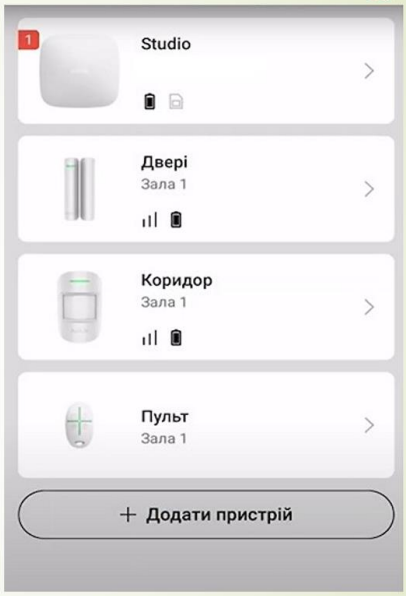


Рис. 19. Успішно підключені пристрої

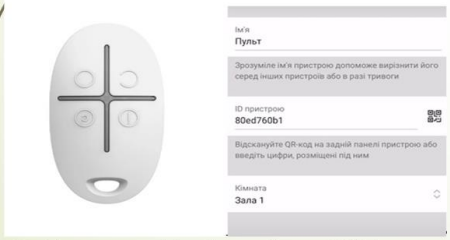


Рис. 20. Додавання Ajax SpaceControl White
для керування системою

ВИСНОВКИ

- Аналіз аналогів систем моніторингу безпеки IoT-пристроїв дозволив визначити, що сучасні рішення часто комбінують кілька технологій для досягнення максимальної ефективності. У той час як AJAX чудово справляється з завданнями реального часу, інші технології можуть бути використані для забезпечення додаткових функцій, таких як стрімінгові дані або забезпечення низької затримки.

- Продемонстровано процес побудови інтегрованої системи моніторингу безпеки IoT-пристроїв на базі технології Ajax. Розглянуто ключові етапи налаштування системи, включаючи підключення центрального хаба Ajax Hub, інтеграцію датчиків руху, відкриття дверей/вікон, пульта керування та інших компонентів.

- Зазначено, що система Ajax забезпечує високий рівень захисту даних завдяки використанню сучасних методів шифрування та автентифікації, а також захищеного протоколу Jeweller для бездротового зв'язку. Виокремлено переваги налаштування системи через мобільний додаток Ajax Security System, який надає зручний інтерфейс для керування та моніторингу.

- Розглянуто можливості розширення та автоматизації системи через сценарії, що дозволяють адаптувати її під різні вимоги користувачів. Також було зазначено, що налаштування окремих компонентів системи, таких як датчики та пульти, є інтуїтивно зрозумілим і забезпечує їх оперативне підключення до хаба.

Нечай О.С. «Застосування технологій іот для "розумного будинку" та "розумного міста"». Тези доповіді на II Всеукраїнській науково-технічній конференції «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу» Київ, 18 листопада 2024 року.

Дякую за увагу!