Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та безпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

РОЗРОБКА АРХІТЕКТУРИ МЕРЕЖІ СИСТЕМ БЕЗПЕКИ НА ОСНОВІ AJAX HUB

DEVELOPMENT OF A SECURITY SYSTEM NETWORK ARCHITECTURE BASED ON AJAX HUB

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-41
Столенко Ігор Олексійович

(підпис)

Керівник:
к.т.н., доцент
Терлецький Тарас Володимирович

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 10 » червня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т. Терлецький
« 10 » 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Столенку Ігорю Олексійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Розробка архітектури мережі систем безпеки на основі Ajax Hub*
Керівник роботи *к.т.н., доцент Терлецький Тарас Володимирович*

затверджені наказом закладу вищої освіти від «04» січня 2025 року № 11/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 10.06.2025р.

3. Вихідні дані до роботи *джерелом дослідження є офіційна технічна документація Ajax Hub, аналітичні матеріали у сфері системи безпеки, наукові публікації, галузеві стандарти, довідкові ресурси, онлайн-платформа технічного спрямування та результати практичного впровадження аналогічних систем.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Сучасні системи безпеки та особливості Ajax Hub
Проєктування архітектура мережі системи безпеки
Функціональне моделювання та аналіз рішення
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Схема розташування пристроїв
Логічна схема обміну даними між елементами системи
Приклад інтерфейсу Ajax PRO Desktop

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Сучасні системи безпеки та особливості Ajax Hub	*Терлецький Т.В., доцент*		
Проєктування архітектура мережі системи безпеки	*Терлецький Т.В., доцент*		
Функціональне моделювання та аналіз рішення	*Терлецький Т.В., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І.,ст.викладач*		

7. Дата видачі завдання 10.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень*	до 10.02.2025 р.	Виконано
2.	*Сучасні системи безпеки та особливості Ajax Hub*	до 02.03.2025 р.	Виконано
3.	*Проєктування архітектури мережі системи безпеки, функціональне моделювання та аналіз рішення*	до 02.04.2025 р.	Виконано
4.	*Висновки та пропозиції*	до 10.04.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 15.04.2025 р.	Виконано
	Формування додатків	до 02.05.2025 р.	
6.	*Оформлення ілюстративного матеріалу*	до 05.05.2025 р.	Виконано
8.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 10.05.2025 р.	Виконано
9.	*Нормоконтроль*	до 15.05.2025 р.	Виконано
10.	*Інструментальна перевірка на академічний плагіат*	до 30.05.2025 р	Виконано
11.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 10.06.2025 р.	Виконано

Здобувач вищої освіти _____ Столенко І.О.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Терлецький Т.В..
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Столенко І. Розробка архітектури мережі систем безпеки на основі Ajax Hub.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел та додатків.

У першому розділі розглянуто класифікацію сучасних систем безпеки, проаналізовано можливості бездротових охоронних рішень та охарактеризовано особливості роботи Ajax Hub і пристроїв екосистеми Ajax Systems.

У другому розділі здійснено проєктування архітектури мережі системи безпеки: визначено вимоги до мережі, обрано апаратні та програмні засоби, розроблено структуру підключення, схеми з'єднань та механізми обміну даними.

У третьому розділі змодельовано розміщення пристроїв на об'єкті, проведено функціональний аналіз обраної архітектури, розглянуто варіанти резервування каналів зв'язку, живлення та методи забезпечення стабільності сигналу.

Ключові слова: Ajax Hub, система безпеки, архітектура мережі, бездротові технології, датчики, відеоспостереження, PRO Desktop.

ANNOTATION

Stolenko I. Development of a security system network architecture based on Ajax Hub.

Qualification work of a bachelor of EP «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

The qualification work consists of an introduction, three sections, conclusions, a list of references, and appendices.

The first section provides an overview of modern security systems, analyzes the capabilities of wireless solutions, and describes the functionality of Ajax Hub and related devices from the Ajax Systems ecosystem.

The second section is devoted to the architectural design of the security system network: the system requirements are defined, hardware and software components are selected, and connection schemes and data exchange mechanisms are developed.

The third section presents a functional model of device placement at the facility, analyzes the performance of the proposed architecture, and considers redundancy options for power supply and communication channels as well as methods for maintaining signal stability.

Keywords: Ajax Hub, security system, network architecture, wireless technologies, sensors, video surveillance, PRO Desktop.

ЗМІСТ

ВСТУП

Забезпечення безпеки об’єктів різного призначення вимагає системного підходу до проєктування охоронної інфраструктури. Системи безпеки повинні забезпечувати контроль доступу, моніторинг стану об’єкта, фіксацію несанкціонованих дій, а також мати можливість централізованого управління та обробки інформації в реальному часі. Для цього необхідно використовувати комплекс апаратних та програмних засобів, об’єднаних у єдину мережу з визначеною структурою, каналами зв’язку та резервуванням.

Ajax Hub це центральний елемент системи безпеки, що координує роботу датчиків, реле, сирен, відеокамер та інших пристроїв. Він підтримує бездротові протоколи зв’язку, багатоканальне підключення до інтернету, можливість резервного живлення, а також інтеграцію з програмним забезпеченням для віддаленого керування. Завдяки поєднанню цих функцій, Ajax Hub дозволяє створити масштабовану та гнучку архітектуру системи безпеки.

Мета роботи полягає у розробці архітектури мережі системи безпеки на основі Ajax Hub, що забезпечує інтеграцію пристроїв охорони, відеоспостереження, стабільне підключення до інтернету, централізоване керування та надійне живлення.

Для досягнення поставленої мети у роботі розв’язуються наступні завдання:

– проаналізувати сучасні підходи до побудови систем безпеки;

– дослідити функціональні можливості обладнання Ajax Systems;

– визначити вимоги до архітектури системи безпеки;

– обґрунтувати вибір апаратних і програмних складових;

– розробити структурну схему побудови мережі з урахуванням

– підключення, живлення та передачі даних;

– запропонувати рішення для стабільності з’єднань і резервування.

Об’єктом дослідження є мережа системи безпеки на основі бездротових технологій.

Предмет дослідження – архітектура мережі, що забезпечує взаємодію пристроїв Ajax, централізоване керування та надійність функціонування системи. У процесі дослідження використано аналітичні та порівняльні методи, методи моделювання, системний підхід, аналіз технічної документації, стандартів і практик проєктування охоронних систем.

РОЗДІЛ 1
СУЧАСНІ СИСТЕМИ БЕЗПЕКИ ТА ОСОБЛИВОСТІ AJAX HUB

1.1 Загальні поняття та класифікація систем безпеки

Системи безпеки є критично важливими елементами сучасної інфраструктури, оскільки вони забезпечують контроль за подіями, які можуть загрожувати матеріальним цінностям, інформаційним ресурсам або життю людей. Основна ідея полягає у створенні керованого середовища, яке дозволяє фіксувати відхилення від заданої норми, швидко реагувати на них, а також запобігати розвитку небезпечних ситуацій. На практиці це означає виявлення несанкціонованого доступу, пожежі, затоплення, втрати зв’язку чи електроживлення, а також зберігання інформації про ці події для подальшого аналізу.

Будь-яка система безпеки об’єднує декілька ключових компонентів: пристрої виявлення загроз, засоби керування, виконавчі механізми реагування, а також інтерфейс моніторингу та адміністрування. Взаємодія між цими елементами відбувається за допомогою комунікаційних каналів – дротових або бездротових, залежно від особливостей інфраструктури об’єкта.

У структурному плані системи безпеки поділяють за функціональним призначенням на охоронні, протипожежні, відеонаглядові комплекси та системи контролю доступу. У реальних умовах ці елементи часто інтегруються в єдину архітектуру для досягнення кращої керованості та зменшення дублювання функцій. Наприклад, відеокамери не лише фіксують зображення, а й взаємодіють із сигналізацією для підтвердження подій або активації додаткових дій.

Крім традиційних засобів реагування, сучасні системи безпеки все частіше інтегруються з аналітичними інструментами, які дозволяють виявляти відхилення на ранніх етапах. До таких інструментів відносять аналіз поведінкових патернів, виявлення аномалій, прогнозування загроз на основі попередньо зібраних даних. Це перетворює систему з реактивного засобу у проактивний інструмент управління ризиками.

Технічна реалізація систем передбачає використання численних сенсорних пристроїв – як-от датчики руху, температури, диму, відкривання або вібрації. Вони передають інформацію на центральний контролер, який приймає рішення про подальші дії. У ролі виконавчих механізмів зазвичай виступають сирени, реле, керовані замки, світлові або звукові індикатори. За потреби до системи підключаються відеореєстратори, мережеві накопичувачі, керовані модулі живлення або інші пристрої, що забезпечують повноцінне функціонування комплексу.

Оскільки системи безпеки проєктуються під конкретні задачі, важливо враховувати специфіку об’єкта – його розміри, тип приміщення, кількість користувачів, рівень потенційних загроз та можливість модернізації. Саме на основі цих параметрів обираються не тільки компоненти, а й тип архітектури – централізована чи розподілена, з пріоритетом на автономність або інтеграцію з загальними системами управління об’єктом.

1.2 Бездротові технології у системах охорони

У минулому більшість систем охоронного призначення реалізовувалась на основі дротових з’єднань, що вимагало складної та дорогої інфраструктури. Прокладання кабельних трас, дотримання норм вогнестійкості, необхідність використання захисних коробів – усе це створювало суттєві обмеження для модернізації вже існуючих об’єктів. З появою бездротових технологій з’явилась можливість відмовитися від більшості цих обмежень без втрати надійності чи функціональності.

Бездротові системи безпеки вирізняються гнучкістю розгортання та зручністю масштабування. Їх монтаж не потребує складного втручання в архітектуру будівлі – датчики можуть бути встановлені на будь-яких поверхнях, не змінюючи внутрішній інтер’єр і не порушуючи існуючу електромережу. Це особливо актуально для історичних або вже відремонтованих приміщень, де кабельна інфраструктура або заборонена, або є вкрай небажаною.

Фундаментом бездротового обміну в сучасних охоронних системах є спеціалізовані радіопротоколи, які адаптовані до умов перешкод, забезпечують шифрування даних і мають низьке енергоспоживання. На відміну від класичних протоколів Wi-Fi або Bluetooth, що використовуються в побутовій електроніці, охоронні протоколи розробляються з акцентом на стабільність сигналу, захищеність та тривалий автономний режим роботи. Це дає змогу живити більшість пристроїв батарейками протягом кількох років без потреби їх обслуговування.

Особливістю бездротових технологій є наявність механізмів постійного моніторингу каналу зв’язку. Кожен пристрій періодично надсилає сигнали життєдіяльності, які дозволяють центральному хабу відстежувати його наявність у мережі, рівень сигналу та заряд елемента живлення. При виявленні втрати зв’язку або втручання в роботу передавача користувач одразу отримує сповіщення, що дозволяє оперативно зреагувати на ситуацію.

Сучасні бездротові системи охорони також підтримують реалізацію автоматизованих сценаріїв, які залежать від взаємодії між різними пристроями. Наприклад, при виявленні руху в нічний час система може не лише активувати сирену, а й автоматично увімкнути зовнішнє освітлення, розпочати запис відео на камеру, повідомити користувача через мобільний застосунок і заблокувати електронні замки на виходах. Це дозволяє створювати комплексні сценарії безпеки без необхідності додаткових фізичних з’єднань між пристроями.

Завдяки використанню бездротових технологій значно знижується вартість встановлення системи та її адаптація до змін у конфігурації об’єкта. Це робить такі рішення не лише технічно зручними, але й економічно доцільними для більшості типів об’єктів – від малих офісів до розгалужених виробничих або житлових комплексів.

1.3 Доцільність використання Ajax Hub у побудові мережі безпеки

Вибір Ajax Hub як основного елемента в архітектурі мережі безпеки зумовлений поєднанням його функціональності, гнучкості та технічної надійності. При побудові сучасної системи захисту об’єкта важливо не лише забезпечити оперативну обробку подій, а й гарантувати безперебійну роботу всіх пристроїв навіть у разі втрати зв’язку або живлення. Саме ці характеристики реалізовані в Ajax Hub, що робить його ефективним інструментом для реалізації комплексних рішень без прокладання значних кабельних інфраструктур.

Одним з ключових чинників доцільності є підтримка кількох каналів зв’язку. Ajax Hub оснащений модулями Ethernet, Wi-Fi та GSM, що дає змогу зберігати зв’язок навіть у разі виходу з ладу одного або кількох каналів одночасно. Такий підхід особливо важливий у проєктуванні архітектур для об’єктів з нестабільним інтернет-з’єднанням або в регіонах із перебоями в електропостачанні.

Ще одним важливим аспектом є простота інсталяції та масштабування системи. Ajax Hub підтримує автоматичне підключення нових пристроїв без складних налаштувань, що дозволяє гнучко змінювати конфігурацію системи без зупинки її роботи. Це критично важливо для об’єктів, які можуть зазнавати змін у плануванні або розширювати свою площу. До того ж, оскільки пристрої взаємодіють із хабом через зашифрований бездротовий зв’язок, зникає потреба в додатковому монтажі кабелів, що значно знижує вартість реалізації проєкту.

Варто також відзначити енергоефективність пристроїв системи Ajax. Завдяки оптимізації протоколів зв’язку і низькому енергоспоживанню більшість датчиків можуть працювати на батарейках упродовж кількох років. Це не лише спрощує обслуговування, а й дозволяє використовувати систему в об’єктах, де постійне живлення недоступне.

Ajax Hub інтегрується з фірмовими програмними засобами, що забезпечують централізоване керування, ведення журналу подій, налаштування сценаріїв автоматизації та сповіщення користувача в реальному часі. Такі

можливості є особливо важливими при побудові мережевої архітектури, яка має бути не лише технічно стійкою, а й зручною в адмініструванні.

Загалом, Ajax Hub поєднує в собі технологічну гнучкість, надійність і простоту впровадження, що дозволяє рекомендувати його як базовий модуль при проєктуванні мереж систем безпеки з розподіленою структурою, потребою в бездротовій інтеграції та високим рівнем вимог до автономності роботи.

1.4 Технології та протоколи, які використовуються в Ajax Systems

У основі роботи Ajax Systems лежить застосування сучасних захищених протоколів зв’язку, які забезпечують ефективну комунікацію між усіма компонентами системи безпеки. Центральне місце у структурі радіозв’язку займає власний протокол Jeweller, який функціонує на частоті 868 МГц. Цей протокол розроблений спеціально для охоронних систем і забезпечує стабільне двостороннє з’єднання між хабом і датчиками [1]. Jeweller підтримує шифрування даних, а також регулярне опитування пристроїв для виявлення втрати сигналу або спроби глушіння. Завдяки оптимізації протоколу досягається висока енергоефективність – автономна робота датчиків на одному заряді батареї може тривати до 7 років.

Передача візуальної інформації у системі реалізована через протокол Wings. Він призначений для надсилання фото при тривозі з детекторів, оснащених камерами [2]. Wings працює паралельно з Jeweller, не перевантажуючи основний канал зв’язку, і забезпечує швидке доставлення зображень без втрати якості. Усі дані передаються у зашифрованому вигляді, що гарантує безпеку конфіденційної інформації.

У контексті мережевих підключень Ajax Hub використовує захищене TLS-шифрування, а доступ до облікового запису – двофакторну автентифікацію.

Відеоінформація зберігається на сторонніх пристроях – наприклад, мережевих відеореєстраторах або хмарних сервісах. Система дозволяє синхронізувати відео з подіями в системі безпеки для підвищення ефективності

реагування. Завдяки використанню окремих, оптимізованих протоколів для кожного типу даних досягається баланс між швидкістю, надійністю та безпекою обміну інформацією.

Таким чином, набір технологій, що використовується в Ajax Systems, забезпечує гнучке, стабільне й захищене функціонування системи у найрізноманітніших умовах експлуатації – від малих офісів до великих промислових об’єктів.

РОЗДІЛ 2
ПРОЄКТУВАННЯ АРХІТЕКТУРИ МЕРЕЖІ СИСТЕМИ БЕЗПЕКИ

2.1 Методологічні підходи до архітектурного проєктування

Архітектура мережі системи безпеки визначає логіку, структуру та спосіб взаємодії між її апаратними й програмними компонентами. Від правильності побудови цієї архітектури залежить ефективність функціонування всієї системи – її здатність до масштабування, стійкість до збоїв, надійність передачі даних, а також зручність керування. Методологія проєктування, що застосовується при цьому, має враховувати технічні можливості обладнання, особливості об’єкта впровадження та вимоги до рівня захисту.

Одним із базових принципів при проєктуванні систем безпеки є модульність. Кожен пристрій або програмний компонент має бути функціонально незалежним і взаємодіяти з іншими елементами через чітко визначені інтерфейси. Такий підхід дозволяє гнучко розширювати систему, замінювати окремі модулі без впливу на решту архітектури, а також підвищує ремонтопридатність та адаптивність до нових технологічних рішень.

Іншим ключовим принципом є централізація управління. Незважаючи на те, що сучасні охоронні пристрої можуть працювати автономно, централізований хаб забезпечує логічну обробку всіх подій, прийняття рішень про реакцію системи, ведення журналу подій, а також забезпечує доступ користувача до стану системи в реальному часі. Саме через хаб реалізується сценарна логіка – автоматизовані дії у відповідь на події.

Системний підхід до проєктування також передбачає аналіз зовнішніх і внутрішніх впливів, визначення граничних умов і ризиків. Зокрема, слід передбачити можливість резервування каналів зв’язку – дротового інтернету, мобільного зв’язку через SIM-карту, а також дублювання джерел живлення. Комбінація живлення від електромережі, акумуляторної батареї та блоку безперебійного живлення дозволяє гарантувати роботу системи навіть у разі аварії. Для стабілізації напруги в умовах нестабільної мережі використовуються

автоматичні регулятори напруги, які захищають обладнання від стрибків електроживлення.

Окрему увагу при проєктуванні архітектури слід приділити топології мережі. Тип розміщення обладнання залежить від геометрії об’єкта: наприклад, для компактних офісних приміщень підходить зіркова топологія, де всі пристрої підключаються до центрального хаба без посередників. У великих виробничих або логістичних комплексах, де сигнал може бути ослаблений стінами або перекриттями, доцільно передбачити використання ретрансляторів сигналу та поетапне розгортання покриття. Топологія повинна враховувати і розміщення зон з підвищеним ризиком – склади, вхідні групи, серверні приміщення – саме там першочергово розміщуються ключові охоронні сенсори.

Проєктування повинно базуватися на принципах відмовостійкості. Усі критично важливі вузли системи повинні мати резервування – як на рівні каналів зв’язку, так і на рівні живлення [3]. Застосування акумуляторних батарей, блоків безперебійного живлення та стабілізаторів напруги дозволяє гарантувати функціонування системи навіть у разі зовнішніх аварій.

Таким чином, методологія архітектурного проєктування системи безпеки включає в себе модульність, централізацію управління, гнучкість до змін топології об’єкта, передбачення ризиків і резервування критичних елементів. Вона формує основу для технічно ефективної та надійної реалізації системи, адаптованої до специфіки конкретного об’єкта.

2.2 Визначення вимог до системи з урахуванням характеристик об’єкта

Успішне проєктування архітектури мережі системи безпеки неможливе без детального аналізу об’єкта, для якого ця система впроваджується. Конкретні технічні й функціональні вимоги формуються залежно від типу приміщення, його призначення, планувальних особливостей, кількості охоронюваних зон, очікуваного рівня загроз, а також умов експлуатації. У випадку проєктування

мережі на базі Ajax Hub усі ці фактори мають безпосередній вплив на вибір обладнання, способи його розміщення, типи зв’язку та підходи до резервування.

Першим і ключовим етапом формування вимог є визначення площі об’єкта, поверховості та конструктивних матеріалів. Наприклад, будівля з бетонними перекриттями та металевими дверима створює більше перешкод для бездротового сигналу, ніж конструкції з гіпсокартону чи дерева. Це означає, що при розробці архітектури потрібно враховувати втрати потужності сигналу та, за необхідності, включати до проєкту ретранслятори для забезпечення стабільного з’єднання між хабом і датчиками.

Далі визначаються зони підвищеного ризику. Це можуть бути входи, вікна, склади, архіви, серверні кімнати, приміщення з дорогим обладнанням або критично важливою інформацією. Для таких ділянок слід передбачити використання комбінацій датчиків – наприклад, одночасне застосування сенсорів руху, відкривання, розбиття скла та датчиків температури. У вологих приміщеннях або технічних зонах: бойлерні, санвузли, машинні відділення. Необхідно встановлювати датчики протікання води з можливістю автоматичного відключення подачі через кероване реле.

Особливої уваги вимагає система живлення. Якщо на об’єкті часто виникають перебої з електроенергією, слід передбачити використання зовнішнього блоку безперебійного живлення для центрального хаба, а також джерел резервного живлення для відеореєстраторів, комутаторів і маршрутизаторів. Враховуючи важливість надійного енергопостачання, у технічному завданні окремо зазначається необхідність стабілізації напруги.

Ще одним критичним елементом є вимоги до типів зв’язку. Якщо в об’єкті є можливість підключення дротового інтернету, хаб налаштовується на роботу через Ethernet, а GSM-модуль використовується як резервний канал. У разі нестабільного інтернет-з’єднання мобільний канал може виступати як основний.

Окремо формуються вимоги до відеоспостереження. Якщо необхідно здійснювати постійний моніторинг у реальному часі або запис подій із затримкою не більше кількох секунд, у проєкті передбачається встановлення

камер з підтримкою запису на мережевий відеореєстратор, локальне сховище або хмарний архів. У залежності від розміру об’єкта, кількості камер і тривалості збереження архіву прораховується об’єм накопичувачів, параметри доступу, потужність комутаторів, а також вимоги до пропускної здатності мережі.

Таким чином, технічні та функціональні вимоги до системи безпеки повинні формуватися на основі реального аналізу об’єкта, з урахуванням усіх критичних факторів – від конструктивних особливостей і зон ризику до стабільності енергопостачання та зв’язку. Це дозволяє створити систему, яка не лише відповідає формальним критеріям, а й ефективно виконує свої завдання в конкретному середовищі.

2.3 Вибір апаратної складової системи

Фізична реалізація системи безпеки неможлива без відповідної апаратної основи. Пристрої, що використовуються в таких системах, не лише забезпечують фіксацію подій чи передачу сигналів, а й формують архітектурний каркас усієї мережі. Надійність, швидкість реакції, точність спрацювань, можливість резервування й адаптації до умов конкретного об’єкта – усе це залежить від правильного добору технічних засобів. Саме з їх допомогою система перетворюється з абстрактної моделі в реальний механізм контролю, моніторингу та захисту.

Центральне місце в архітектурі мережі безпеки займає Hub 2 Plus Jeweller – розумний контрольний пристрій, який виконує функцію головного комунікаційного та логічного вузла системи. Саме цей елемент приймає всі сигнали від сенсорів, камер, клавіатур, реле та інших модулів, аналізує їх і формує відповідні команди на основі заздалегідь визначених сценаріїв. Його присутність дозволяє системі функціонувати не як набір розрізнених пристроїв, а як єдиний цілісний механізм реагування (рис. 2.1).

Рисунок 2.1 – AJAX HUB 2 PLUS [4]

Однією з ключових переваг Hub 2 Plus Jeweller є підтримка двох власних протоколів зв’язку: Jeweller – для передачі команд і станів сенсорів, та Wings – для надсилання фото з пристроїв, що мають функцію верифікації тривоги за зображенням. Радіус стабільного зв’язку при цьому досягає 2000 метрів у відкритому просторі, що робить цей хаб ефективним навіть у великих складських приміщеннях чи офісних комплексах.

Мережеве підключення до інтернету реалізовано через Ethernet, дві SIM-картки формату nanoSIM, а також через Wi-Fi. Така комбінація гарантує безперервну роботу, навіть якщо окремі канали зв’язку будуть тимчасово недоступні. У разі втрати інтернету на основному каналі, система автоматично переключається на резервний, не припиняючи зв’язку із застосунками користувачів і сервісними платформами.

Hub 2 Plus Jeweller підтримує підключення до 200 пристроїв, включаючи датчики, реле, клавіатури, камери тощо. Крім того, він здатен обслуговувати до 100 користувачів і до 25 сценаріїв автоматизації, що дозволяє реалізувати складні логіки реагування – наприклад, відкрити замки під час пожежі або увімкнути сирени і світло при тривозі.

Також важливим аспектом є захищеність системи. Hub 2 Plus Jeweller використовує шифрування з динамічним ключем, а також автентифікацію пристроїв для захисту від підміни сигналу. Протоколи зв’язку побудовані таким чином, щоб неможливо було зчитати чи змінити дані ззовні.

Живлення хаба передбачене від мережі 110-240 В, з вбудованим резервним акумулятором на 15 годин автономної роботи. Це дозволяє системі функціонувати навіть при аварійному відключенні електроенергії. У разі тривалого відключення може бути підключене резервне джерело живлення через зовнішній стабілізатор або акумулятор.

Одним із базових, але водночас критично важливих елементів охоронної інфраструктури є датчик відкривання дверей DoorProtect Jeweller. Його основне завдання – фіксація моменту, коли відчиняються двері, вікна або інші об’єкти з рухомими частинами. Попри свою простоту, цей пристрій є ключовим для побудови сценаріїв реагування, які активуються ще до моменту безпосереднього проникнення на територію об’єкта (рис. 2.2).

Рисунок 2.2 – DoorProtect [5]

DoorProtect Jeweller складається з двох частин – магнітного сенсора та магніту. Один із них встановлюється безпосередньо на дверну коробку, інший – на стулку дверей. У закритому стані компоненти розташовані поруч, і система

розпізнає це як нормальний стан. При відкриванні дверей магніт віддаляється, і сенсор миттєво реагує на зміну магнітного поля, надсилаючи сигнал тривоги на центральний хаб.

Датчик використовує радіопротокол Jeweller, що забезпечує стабільну бездротову передачу сигналів на відстань до 1200 метрів у відкритому просторі. Комунікація з Hub 2 Plus Jeweller відбувається з періодичним опитуванням, що дозволяє не лише миттєво виявляти тривоги, а й контролювати працездатність самого пристрою.

Однією з переваг DoorProtect є мінімальне енергоспоживання – пристрій працює від батареї CR123A до 5 років без заміни. Це дозволяє уникнути частого технічного обслуговування, що особливо важливо у віддалених або складнодоступних місцях. Завдяки компактним розмірам та декільком кольоровим варіантам корпусу, датчик легко інтегрується в будь-який інтер’єр без погіршення естетики приміщення.

Окрім стандартного магнітного сенсора, пристрій підтримує підключення зовнішнього дротового датчика, що дає змогу реалізовувати складніші конфігурації – наприклад, одночасне спостереження за декількома точками або застосування спеціалізованих сенсорів. Це дозволяє суттєво розширити зону покриття одного пристрою.

DoorProtect Jeweller має тампер-захист – вбудований сенсор, який фіксує спробу демонтажу або відкриття корпусу. У разі таких дій система також автоматично переходить у тривожний режим, інформуючи відповідальних осіб про несанкціоноване втручання.

У межах інтегрованої архітектури система на основі DoorProtect може застосовуватись у поєднанні зі сценаріями автоматизації. Наприклад, при відкритті дверей у певному режимі (не під охороною) система може автоматично вмикати світло, запускати вентиляцію або активувати запис із відеокамери.

У системі безпеки важливою є не лише реакція на відкривання дверей, а й можливість оперативно виявляти спроби проникнення через розбите скло. Для цього використовується спеціалізований датчик розбиття скла GlassProtect

Jeweller, який дозволяє фіксувати характерні акустичні сигнали від руйнування скляних поверхонь [6]. Його використання особливо доцільне у приміщеннях зі скляними дверима, великими вікнами або вітринами.

GlassProtect Jeweller встановлюється на стіні або стелі у безпосередній видимості до скляної поверхні на відстані до 9 метрів. Він працює за двоступеневим принципом розпізнавання – спочатку фіксує удар по склу, а потім аналізує специфічний звук його руйнування. Це мінімізує ймовірність помилкових спрацювань, наприклад, від гучних голосів, ударів об меблі або падіння предметів.

Передача сигналів від датчика до Hub 2 Plus Jeweller здійснюється за допомогою радіопротоколу Jeweller, що гарантує надійний зв’язок на великій відстані – до 1000 метрів у відкритому просторі. Як і інші пристрої Ajax, датчик має захищену двосторонню комунікацію та підтримує шифрування переданих даних, що унеможливлює підміну або перехоплення сигналів.

GlassProtect має тампер-захист, що забезпечує виявлення спроб демонтажу або зламу корпусу, а також індикатор низького заряду батареї, що дозволяє заздалегідь планувати технічне обслуговування. Термін роботи від батареї досягає 7 років, що робить цей пристрій дуже автономним.

Завдяки мініатюрному розміру та сучасному дизайну GlassProtect Jeweller легко інтегрується в інтер’єр без привернення уваги. Він також дозволяє підключити зовнішній дротовий датчик, що підвищує гнучкість під час монтажу.

У загальній архітектурі безпеки GlassProtect Jeweller виконує роль першої лінії реагування в об’єктах із великою площею скління – торгових залах, офісах, складських приміщеннях з віконними отворами. У разі виявлення загрози, інформація миттєво передається на хаб, який, відповідно до налаштувань сценаріїв, може активувати сирени, блокувати доступ, увімкнути відеозапис або повідомити охоронну службу.

HomeSiren Jeweller – це компактна та потужна внутрішня сирена, яка виконує критичну роль у системі сповіщення про тривожні події. У момент активації тривоги вона генерує гучний звуковий сигнал, який не лише сповіщає

присутніх про загрозу, але й виступає психологічним фактором стримування для потенційних зловмисників (рис. 2.3).

Рисунок 2.3 – HomeSiren Jeweller [7]

Ця сирена є повністю бездротовою та працює на базі протоколу Jeweller, що забезпечує зв’язок із хабом на відстані до 2000 метрів у відкритому просторі. Завдяки цьому вона легко монтується в будь-якому місці приміщення без необхідності прокладання додаткових дротів. Живлення здійснюється від батарей, яких вистачає на до 5 років безперервної роботи, а також є можливість живлення від зовнішнього джерела 12 В, що підходить для комерційних об’єктів із резервними лініями живлення.

Гучність HomeSiren Jeweller налаштовується у діапазоні від 81 до 105 дБ – користувач або адміністратор системи може вибрати відповідний рівень, виходячи з площі приміщення та характеру об’єкта. У багатьох випадках достатньо навіть мінімального рівня гучності, щоби привернути увагу охорони або мешканців. У той же час максимальні налаштування роблять сирену чутною через кілька кімнат або через тонкі стіни.

Пристрій має вбудований світлодіод, який дозволяє візуально ідентифікувати режим роботи або тривоги навіть у темному приміщенні. Це особливо важливо у випадках, коли сирену встановлено в адміністративних будівлях, де передбачено візуальні індикатори стану охоронних зон.

Завдяки інтеграції із системними сценаріями, HomeSiren може активуватися не тільки у випадку тривоги, а й при вході користувача до об’єкта, як індикатор затримки на вихід або вхід, або ж як підтвердження успішної деактивації охоронного режиму.

HomeSiren має захист від демонтажу – при спробі зняти пристрій із поверхні система одразу надсилає сповіщення. Вона також сигналізує про низький заряд батареї, що дозволяє уникнути моменту, коли сповіщення не буде подано в критичній ситуації.

У структурі архітектури безпеки складських приміщень HomeSiren Jeweller доцільно розміщувати на стелі або у центральній частині великого залу, де її буде чути в усіх кутках. За потреби система може підтримувати кілька сирен – для окремих зон чи поверхів – що значно підвищує ефективність оповіщення на великих об’єктах.

Таким чином, HomeSiren Jeweller виступає невід’ємним компонентом не лише для оперативного інформування про загрози, а й для формування повноцінної реактивної логіки системи безпеки. Вона поєднує автономність, гнучке налаштування та простий монтаж, що робить її універсальним вибором для об’єктів будь-якого типу.

MotionProtect Jeweller – це базовий охоронний елемент, відповідальний за виявлення присутності сторонніх осіб у приміщенні. Цей пристрій використовує інфрачервоний сенсор для виявлення руху в зоні покриття. У системі безпеки він є ключовим елементом для формування сценаріїв реагування на проникнення, особливо у випадках, коли об’єкт перебуває під охороною в неробочий час.

MotionProtect Jeweller працює на основі технології пасивної інфрачервоної детекції, яка дозволяє виявляти рух теплокровних об’єктів. Завдяки високочутливому сенсору та цифровій обробці сигналів, пристрій зменшує ймовірність помилкових спрацювань, наприклад, через коливання температури, рух штор або невеликі тварини. Ігнорує тварин вагою до 20 кг та зростом до 50 см, що робить MotionProtect ефективним для використання в житлових і

комерційних приміщеннях (рис. 2.4).

Рисунок 2.4 – Motion Protect [8]

Пристрій має дальність виявлення до 12 метрів під кутом 88,5°, що дозволяє покривати значну площу з однієї точки. Завдяки цьому MotionProtect можна розміщувати на вході до кімнати, в коридорах або біля вікон. Його можна монтувати як на стіну, так і в кут, що дає гнучкість у виборі місця встановлення.

MotionProtect Jeweller передає інформацію до хаба через радіопротокол Jeweller, який забезпечує надійний зв’язок на відстані до 1700 метрів на відкритому просторі і дозволяє обмінюватися даними кожні кілька секунд. Завдяки цьому будь-яке виявлення руху миттєво обробляється системою, і залежно від сценарію, активуються відповідні механізми реагування – наприклад, ввімкнення сирени, відеозапис, блокування дверей або повідомлення охорони.

MotionProtect живиться від батареї, ресурс якої розрахований до 5-7 років автономної роботи. Це дозволяє уникнути частого обслуговування навіть у важкодоступних місцях. Пристрій також обладнаний тампером – сенсором захисту від несанкціонованого відкриття корпусу або демонтажу, що гарантує постійний контроль за його цілісністю.

Для великих об’єктів або складських приміщень доцільно використовувати кілька таких датчиків – у різних зонах, що перекривають одна

одну. Це створює систему, в якій зловмисник не зможе пересуватись непоміченим, навіть якщо уникне одного з пристроїв.

У поєднанні з іншими компонентами системи, такими як датчики відкриття, сирени та камери, MotionProtect Jeweller забезпечує повний цикл виявлення, оцінки та реагування на загрозу, формуючи основу багаторівневої безпеки об’єкта.

LifeQuality Jeweller – це високоточний сенсор, розроблений для постійного моніторингу мікроклімату всередині приміщень. На відміну від стандартних охоронних пристроїв, він не реагує на загрози безпеці напряму, проте виконує критичну функцію: контроль температури, рівня вологості та концентрації вуглекислого газу, що особливо важливо для складів, де зберігається чутлива продукція, а також для офісів, серверних та технічних приміщень (рис. 2.5).

Рисунок 2.5 – LifeQuality [9]

Пристрій обладнаний одразу кількома сенсорними модулями: високоточною термопарою для вимірювання температури в діапазоні від –10 °C до +40 °C з точністю ±0.2 °C, гігрометром для оцінки вологості з похибкою не більше 2 %, а також сенсором CO_2 на основі інфрачервоної абсорбції. Це дозволяє не тільки отримувати об’єктивну інформацію про повітря, а й оперативно реагувати на будь-які зміни умов, які можуть вплинути на збереження товару або комфорт перебування людей.

LifeQuality передає дані на центральний хаб Ajax через протокол Jeweller із регулярним оновленням значень. Ці дані відображаються в застосунках Ajax PRO Desktop та Ajax Security System у вигляді графіків і цифрових показників.

Система дозволяє встановлювати порогові значення, при перевищенні яких автоматично активуються відповідні сценарії – наприклад, запуск витяжки, відкриття вентиляційних отворів, повідомлення персоналу або навіть блокування доступу в небезпечну зону.

Завдяки підтримці сценарного керування LifeQuality Jeweller можна інтегрувати в комплексну систему реагування. Наприклад, на складі, де зберігається електроніка, перевищення рівня вологості може призвести до конденсації, що небезпечно для обладнання. У цьому випадку система може автоматично вимкнути подачу електроенергії через WallSwitch Jeweller, активувати Ajax WaterStop, якщо витік спричинений водою, або повідомити відповідального спеціаліста.

Пристрій підтримує автономну роботу від батареї з тривалим терміном служби – до 3 років без заміни. Додатково передбачено можливість встановлення на стіну або стелю з урахуванням оптимальної зони вимірювання – в центрі кімнати або поблизу потенційного джерела проблеми

LeaksProtect Jeweller – це компактний сенсор, призначений для виявлення витоку рідини в місцях із підвищеним ризиком затоплення.

Його використання дозволяє мінімізувати збитки, пов’язані з проривами труб, недбалою експлуатацією водопостачання чи несправністю сантехнічного обладнання. У складі загальної архітектури системи безпеки пристрій виконує важливу роль у запобіганні аварійних ситуацій, які можуть порушити роботу об’єкта або зіпсувати матеріальні цінності.

Принцип дії сенсора базується на замиканні електричних контактів, розташованих на його нижній поверхні. Коли LeaksProtect Jeweller виявляє навіть мінімальну кількість води – всього кілька крапель, – він миттєво передає сигнал тривоги на центральний хаб Hub 2 Plus Jeweller за допомогою радіопротоколу Jeweller. Це забезпечує надзвичайно швидку реакцію системи – зазвичай у межах 0,15 секунди.

Особливість пристрою полягає в тому, що він не потребує монтажу – достатньо просто розмістити його на підлозі в зоні ризику: під трубами, біля

пральної машини, посудомийної машини, бойлера або в технічному приміщенні (рис. 2.6).

Рисунок 2.6 – LeaksProtect [10]

Сенсор має антикорозійне покриття контактів, тому здатен зберігати працездатність у складних умовах експлуатації. Живлення забезпечується від вбудованої батареї CR2032, ресурсу якої вистачає приблизно на 5 років автономної роботи.

У системі безпеки пристрій може бути пов’язаний із реле Ajax WaterStop, що дозволяє реалізувати повністю автоматичне перекриття подачі води в разі аварійної ситуації. Такий сценарій є надзвичайно ефективним для складських приміщень, де зберігається техніка, паперова продукція або інші матеріали, чутливі до вологи. Додатково система може надіслати сповіщення відповідальному персоналу та активувати інші сценарії – наприклад, знеструмлення об’єкта або запуск сигналізації.

LeaksProtect Jeweller можна інтегрувати в кілька сценаріїв одночасно – наприклад, одночасне перекриття води, запуск оповіщення, зупинка насосів чи активація резервної системи водовідведення. Завдяки цьому пристрій є не лише засобом виявлення витоку, а й ключовим елементом системи автоматизації у сфері техногенної безпеки.

Ajax WaterStop є одним із ключових пристроїв у системі управління водопостачанням, що забезпечує своєчасне перекриття води в разі виникнення

аварійних ситуацій. Його впровадження дозволяє реалізувати ефективні механізми запобігання затопленням, зменшити людський фактор у процесі реагування на витоки, а також інтегрувати систему контролю води в загальну архітектуру охорони об’єкта (рис. 2.7).

Рисунок 2.7 – WaterStop [11]

Пристрій поєднує в собі електропривід та клапан, який встановлюється безпосередньо на трубопровід водопостачання. Управління здійснюється дистанційно – через Hub 2 Plus Jeweller, до якого WaterStop передає інформацію та приймає команди за допомогою зашифрованого радіопротоколу Jeweller. Це дозволяє в режимі реального часу реагувати на сигнали від сенсорів витоку води, зокрема LeaksProtect Jeweller, і без участі людини перекривати подачу води.

Ajax WaterStop сумісний із трубами стандартного діаметра, що робить його універсальним для більшості побутових і комерційних об’єктів. Клапан має поворотну конструкцію з електроприводом, який відкриває або закриває прохід води в трубі. Привід працює від батареї або може бути підключений до зовнішнього джерела живлення, забезпечуючи надійність і автономність роботи в разі зникнення основного живлення.

Один із головних переваг Ajax WaterStop – можливість роботи в автоматизованому режимі. Наприклад, у разі спрацювання LeaksProtect Jeweller,

хаб миттєво надсилає команду WaterStop на перекриття води. Цей сценарій дозволяє уникнути затоплення та звести до мінімуму можливі збитки. Крім того, керування може здійснюватися вручну – з мобільного застосунку Ajax, через веб-інтерфейс Ajax PRO Desktop або безпосередньо з клавіатури на об'єкті.

У системі об'єктової безпеки Ajax WaterStop виконує функцію захисту не лише від витоку, а й як елемент протипожежного сценарію. У разі виявлення загрози займання пристрій може припинити подачу води в зони, де вона не потрібна, або навпаки – дозволити роботу пожежогасіння, якщо система цього вимагає.

Монтаж WaterStop є доволі простим: його встановлюють на трубу перед запірною арматурою або замість неї. Підключення до хаба не потребує прокладання кабелів, що є важливою перевагою для об'єктів з уже завершеним ремонтом або складним плануванням.

У великих приміщеннях, таких як складські комплекси, логістичні центри чи промислові об'єкти, сигнал від центрального хаба може не охоплювати всі зони об'єкта, особливо якщо існує багато перешкод у вигляді товстих бетонних стін або металевих перегородок. Саме тому важливим компонентом системи безпеки стає Ajax ReX 2 – ретранслятор сигналу, призначений для збільшення зони покриття бездротової мережі пристроїв Ajax [12].

ReX 2 виконує роль посередника між хабом і підключеними до нього пристроями. Він приймає сигнали від хаба, підсилює їх і передає далі до кінцевих пристроїв, а також у зворотному напрямку. Це дозволяє суттєво збільшити радіус дії системи без потреби у прокладанні додаткових кабелів або встановленні кількох хабів. Один ретранслятор здатен розширити мережу на площу до 35 км² відкритого простору, а також значно покращити зв'язок у складних приміщеннях з щільними перегородками.

Підтримуються до 99 пристроїв одночасно, включаючи датчики, реле, клавіатури та сирени. Це робить його ефективним рішенням для розгалужених систем, де необхідна координація великої кількості приладів. Важливо й те, що ретранслятор зберігає усі задані сценарії, логіку роботи та навіть резервні копії

налаштувань у випадку втрати зв’язку з хабом. Завдяки цьому він здатен забезпечити автономну роботу частини системи навіть у критичних умовах.

ReX 2 оснащений двома радіомодулями: один для приймання даних від хаба, другий – для передавання сигналу до пристроїв. Це зменшує затримки, підвищує швидкість реакції системи та гарантує цілісність передачі даних. Передача відбувається за допомогою фірмового протоколу Jeweller, який забезпечує захищене шифрування та перевірку справжності кожного сигналу.

Окремою перевагою ReX 2 є можливість передачі фото по тривозі від датчиків руху з фотопідтвердженням. Це дає змогу отримати візуальні дані навіть з найбільш віддалених ділянок об’єкта, де встановлені відповідні пристрої.

Установка ReX 2 не потребує втручання в існуючу інфраструктуру – достатньо підключити його до живлення і зареєструвати в системі. Завдяки сучасному дизайну та бездротовому зв’язку його можна встановити навіть у важкодоступних місцях.

Для забезпечення повного контролю над подіями на об’єкті безпеки надзвичайно важливим є не лише сповіщення, а й можливість візуального підтвердження ситуації. Саме тому у загальну архітектуру мережі інтегрується Ajax NVR 8-CH – мережевий відеореєстратор нового покоління, створений спеціально для сумісності з екосистемою Ajax (рис. 2.8).

Рисунок 2.8 – NVR 8-CH [13]

Цей пристрій виконує функцію центрального вузла для зберігання, керування та перегляду відео з підключених IP-камер. Він підтримує одночасне підключення до 8 каналів, що дозволяє формувати комплексну систему відеоспостереження з покриттям всіх важливих зон: входів і виходів, складу, технічних приміщень, підсобок тощо. Сумісність з відеокамерами, що передають потік у форматі RTSP, забезпечує гнучкість у виборі моделей – від стандартних TurretCam до тепловізійних або поворотних камер, залежно від потреб об’єкта.

Ajax NVR 8-CH інтегрується з мобільними застосунками, що дозволяє переглядати відео в режимі реального часу, відтворювати записи за часом або подіями, а також синхронізувати ці записи з сигналами тривог, що надходять із хаба. Завдяки цьому можна миттєво отримати візуальне підтвердження вторгнення, витоку, спрацювання пожежного сенсора або будь-якого іншого інциденту.

Однією з головних переваг Ajax NVR є інтелектуальна система збереження відео, яка дозволяє створювати профілі запису: постійний, за розкладом або лише за подіями. Це суттєво оптимізує обсяг зайнятого місця на жорсткому диску та спрощує пошук важливих фрагментів. Для зберігання використовується стандартний жорсткий диск SATA до 10 ТБ, якого зазвичай достатньо для зберігання тижневого архіву з усіх 8 камер у високій якості.

Систему захищено від несанкціонованого доступу – передача даних шифрується, доступ до налаштувань обмежується лише для авторизованих користувачів, а сам пристрій можна фізично ізолювати або зафіксувати у закритій серверній зоні.

Для підключення камер та самого реєстратора до мережі використовується комутатор з підтримкою PoE, що дозволяє подавати живлення та дані одним кабелем. Це знижує витрати на прокладання інфраструктури, особливо у великих приміщеннях, та спрощує монтаж.

Контроль доступу до приміщень є одним із базових елементів сучасної системи безпеки. Одним з ефективних рішень у цьому напрямку є Ajax KeyPad TouchScreen Jeweller – сенсорна клавіатура з розширеним функціоналом, яка

забезпечує ідентифікацію користувачів і керування охоронними сценаріями (рис. 2.9).

Рисунок 2.9 – TouchScreen [14]

KeyPad TouchScreen Jeweller дозволяє здійснювати авторизацію за допомогою трьох типів засобів: персонального PIN-коду, безконтактної карти або брелока. Для шифрування зчитування використовується протокол DESFire, який забезпечує захист даних на рівні банківських систем. Це дає змогу не лише керувати охоронними режимами, а й відкривати електрозамки, підключені до системи через WallSwitch Jeweller або інші виконавчі механізми.

Клавіатура має інтуїтивно зрозумілий сенсорний інтерфейс, що дозволяє швидко взаємодіяти з системою. У залежності від налаштувань, на екрані відображаються назви зон, їх поточний статус, а також доступні дії – активація охорони, зняття з охорони, часткове блокування тощо. Це зручно як для щоденних користувачів, так і для персоналу охорони, який може швидко оцінити стан об’єкта.

Пристрій також підтримує групову конфігурацію доступу – можна створити до 200 унікальних користувачів, кожному з яких присвоюється індивідуальний рівень доступу та графік активності. Система фіксує всі події у журналі такі, як вхід, зміни режиму охорони, спроби несанкціонованого доступу. Ці дані синхронізуються з хмарною платформою та доступні в застосунку Ajax PRO Desktop для адміністраторів.

У контексті побудови комплексної системи безпеки клавіатура відіграє не лише роль контролера доступу, а й дозволяє активувати або деактивувати автоматизовані сценарії. Наприклад, за допомогою KeyPad можна вручну запустити евакуаційний сценарій, якщо неможливо це зробити через основну панель або мобільний додаток.

Конструктивно Ajax KeyPad TouchScreen Jeweller має захист від вандалізму – у разі спроби демонтажу або фізичного впливу пристрій автоматично надсилає сигнал тривоги до хаба. Клавіатура також може працювати в умовах обмеженого освітлення завдяки вбудованому підсвічуванню, а автономність забезпечується за допомогою внутрішнього джерела живлення, яке може функціонувати до декількох місяців без підзарядки.

Ajax WallSwitch Jeweller – це бездротове реле, яке дозволяє керувати живленням електроприладів у системі безпеки Ajax (рис. 2.10).

Рисунок 2.10 – WallSwitch [15]

Пристрій встановлюється в розподільчий щиток або за стандартну розетку й підключається до мережі 230 В. Його основне призначення – дистанційне вмикання та вимикання побутових приладів, освітлення, електрозамків, насосів або інших електричних пристроїв.

Реле підтримує навантаження до 3 кВт і може вимикатися автоматично у разі перевантаження, перегріву чи короткого замикання. Завдяки захищеному бездротовому протоколу Jeweller, WallSwitch передає інформацію на хаб на відстані до 1000 метрів на відкритому просторі. Окрім основної функції

комутації, реле також вимірює параметри енергоспоживання – напругу, силу струму та загальне споживання електроенергії, що дозволяє здійснювати моніторинг у мобільному застосунку Ajax.

У складі системи безпеки Ajax, WallSwitch може використовуватись для автоматизації сценаріїв: відкривання замків після авторизації на клавіатурі, вимкнення світла при активації охорони, зупинка приладів під час пожежної тривоги або запуск вентиляції у разі підвищеної вологості. Пристрій забезпечує стабільну роботу навіть без доступу до інтернету, завдяки логіці сценаріїв, закладених у сам хаб.

Для забезпечення фізичного контролю доступу до окремих зон об’єкта безпеки до складу архітектури системи включено електромеханічний замок YLI YB-500B. Цей пристрій забезпечує надійну фіксацію дверей у зачиненому стані та здатен інтегруватися з охоронними сценаріями, передбаченими системою Ajax (рис. 2.11).

Рисунок 2.11 – YLI YB-500B [16]

YLI YB-500B є електроригельним замком накладного типу, що встановлюється переважно на дерев’яні, металеві або скляні двері. Він підтримує режим нормально відкритий, тобто у разі знеструмлення автоматично розблоковується, забезпечуючи евакуацію з приміщення. Це критично важливо для сценаріїв протипожежного захисту.

Замок має корпус із нержавіючої сталі, що забезпечує стійкість до механічних пошкоджень, та підтримує керування через реле, зокрема Ajax WallSwitch. В цьому випадку відкривання замка може здійснюватися

автоматично після авторизації користувача на KeyPad TouchScreen Jeweller, або у відповідь на сигнали від центрального хаба під час активації тривожного сценарію.

Монтаж замка передбачає встановлення на раму дверей зі збереженням прихованого кабелю живлення, що під’єднується до джерела 12V DC. Завдяки низькому енергоспоживанню близько 0.9 А при активному утриманні, YLI YB-500B може працювати в складі автономної системи з резервним живленням.

У проєктованій мережі системи безпеки замки такого типу встановлюються на вхідні двері до складу, а також на окремі приміщення з обмеженим доступом в серверні кімнати або сейфові зони.

TurretCam – це сучасна мережева відеокамера, розроблена спеціально для інтеграції з екосистемою Ajax Systems. Вона забезпечує високоякісне відеоспостереження та є важливою складовою системи безпеки, яка доповнює роботу сенсорів, сирен і інших охоронних пристроїв (рис. 2.12).

Рисунок 2.12 – TurretCam [17]

Камера підтримує роздільну здатність до 1920x1080, що дозволяє отримувати чітке та деталізоване зображення в реальному часі. Завдяки інфрачервоному підсвічуванню, TurretCam може працювати в умовах повної темряви, забезпечуючи контроль об’єкта незалежно від освітлення. Вбудований об’єктив з широким кутом огляду дозволяє охопити значну частину приміщення або території.

TurretCam підтримує живлення через PoE (Power over Ethernet), що суттєво спрощує монтаж – передача даних і живлення здійснюється одним кабелем. Це зменшує кількість проводки на об’єкті та покращує естетичний вигляд установки. Підключення до мережі здійснюється через PoE-комутатор, який живить камери й об’єднує їх з реєстратором.

Для зберігання відео TurretCam використовує Ajax NVR, який забезпечує централізований запис і архівацію зображень із кількох камер одночасно. Це дозволяє організувати локальний архів і забезпечити доступ до записів через мобільний застосунок або десктоп-програму Ajax PRO.

FireProtect Jeweller – це бездротовий пожежний сповіщувач від Ajax Systems, який забезпечує раннє виявлення диму, підвищення температури та, в деяких моделях, чадного газу. Він є критично важливим елементом безпеки об’єкта, що доповнює охоронну систему функціональністю пожежного моніторингу [18].

Основним завданням FireProtect є виявлення пожежі на ранніх стадіях, навіть до появи відкритого вогню. У приладі використовується фотоелектричний сенсор, який фіксує наявність диму в повітрі, а також термодатчик, що реагує на раптове або тривале підвищення температури. Такий подвійний підхід дозволяє уникати помилкових спрацювань і підвищує точність сповіщення.

FireProtect Jeweller працює на вбудованій батареї, що забезпечує до 4-5 років автономної роботи. Це дозволяє легко монтувати пристрій у будь-якому приміщенні без прокладання проводів, зберігаючи інтер’єр та спрощуючи обслуговування.

Завдяки бездротовому протоколу Jeweller, пристрій має зону дії до 1300 метрів на відкритому просторі та забезпечує стабільний захищений зв’язок із хабом. Пристрій постійно передає сигнали про свій стан, заряд батареї, а також проходить регулярне опитування для підтвердження працездатності.

У разі спрацювання FireProtect видає гучний звуковий сигнал (до 85 дБ), який допомагає оперативно попередити людей у приміщенні про небезпеку.

Одночасно з цим надсилається сповіщення до мобільного додатку користувача та, при налаштуванні, до пульта охорони.

Додатковою функцією є взаємна синхронізація сповіщувачів: якщо один FireProtect виявляє дим чи перегрів, інші в мережі також активують тривожний сигнал, що підвищує охоплення й ефективність оповіщення на великих об’єктах.

FireProtect Jeweller відповідає сучасним стандартам пожежної безпеки й може бути встановлений як в офісах, так і на промислових чи житлових об’єктах.

2.4 Топологія мережі та організація з’єднань

Проєктування ефективної мережі системи безпеки вимагає детального опрацювання топології, конфігурації зв’язків між компонентами, каналів передачі інформації, типів живлення та їх резервування [19]. У системі, побудованій на основі Ajax Systems, реалізовано гібридну архітектуру з підтримкою бездротового зв’язку між більшістю пристроїв і централізованим комутаційним центром для дротових елементів, як-от відеоспостереження та мережеве обладнання.

Центральним вузлом усієї структури є контролер Hub 2 Plus Jeweller, який монтується в технічно захищеному приміщенні, звідки доступна більшість зон покриття. Розташування контролера визначається з урахуванням геометрії об’єкта, наявності металевих чи бетонних перекриттів і радіусу дії сигнальних модулів. Для розширення зони впевненого прийому в умовах складного планування або великої площі використовуються ретранслятори ReX 2, які посилюють та дублюють сигнали між хабом і сенсорами.

Уся бездротова взаємодія між основним хабом і датчиками, сиренами, реле та іншими периферійними елементами здійснюється через захищений протокол Jeweller, розроблений Ajax. Він забезпечує високу енергоефективність, низьку затримку передачі даних і надійність зв’язку з періодичними перевірками стану кожного пристрою. Для передачі мультимедійного контенту – наприклад, фотознімків із датчиків зображення – застосовується протокол Wings.

Для зовнішнього з’єднання системи з мережею Інтернет контролер Hub 2 Plus використовує Ethernet-з’єднання з пропускною здатністю до 1 Гбіт/с. Кабель передбачено категорії 5e або вище, прокладається в захисних гофрах або кабель-каналах відповідно до норм безпеки. У якості резервних каналів використовуються два незалежні слоти для SIM-карт з LTE-підтримкою, що забезпечує безперервну передачу даних у разі втрати дротового інтернету. Додатково підтримується Wi-Fi як третій резервний канал.

Система відеоспостереження базується на камерах TurretCam, які підключаються до мережі через PoE-комутатор Tenda TEG1110P-8-150W. Цей пристрій забезпечує передачу живлення та даних через один кабель, що значно спрощує інсталяцію та зменшує витрати на інфраструктуру. Усі відеопотоки надходять до Ajax NVR 8-CH – мережевого відеореєстратора, який синхронізується з подіями системи безпеки та надає віддалений доступ до архіву.

Електроживлення системи реалізовано у комбінованій схемі. Більшість сенсорів працює автономно – від батарей, термін служби яких сягає 5-7 років. Камери, комутатори, хаб, реєстратор та маршрутизатор живляться від основної електромережі через стабілізатор напруги. Додатково передбачене підключення до джерела резервного живлення для забезпечення безперервної роботи в разі аварійного відключення енергії.

Загальна схема мережі реалізована за топологією «зірка», де всі дротові вузли зосереджені у комутаційному центрі, а бездротові пристрої взаємодіють із хабом напряму або через ретранслятори. Такий підхід гарантує легке масштабування, модернізацію системи та її адаптацію під особливості будь-якого об’єкта.

Таким чином, логічна та фізична структура побудованої мережі забезпечує оптимальний баланс між продуктивністю, резервуванням і адаптивністю, що є важливим фактором для об’єктів із підвищеними вимогами до безпеки.

2.5 Механізми зберігання даних та обробки сигналів

Один із ключових аспектів побудови ефективної системи безпеки – це забезпечення надійного зберігання подій та їх коректної обробки в реальному часі. У системі, що базується на Ajax, ці процеси реалізуються через взаємодію центрального контролера, хмарного сервера, відеореєстратора та локальних пристроїв пам’яті.

Усі сигнали, що надходять від сенсорів – спрацювання датчика руху, відкриття дверей, виявлення диму чи води – обробляються у хабі Ajax Hub 2 Plus. Цей пристрій виконує функцію первинної фільтрації подій, класифікації сигналів, верифікації достовірності інформації, а також реєстрації їх у внутрішньому журналі. Усі записи мають чіткі атрибути часу, ID пристрою, статуси до та після події, що дає змогу відтворити повну картину подій на об’єкті в будь-який момент.

Хаб автоматично передає копії подій до хмарного середовища Ajax Cloud, що гарантує збереження навіть у разі фізичної втрати або пошкодження обладнання на об’єкті. Обробка подій у хмарі відбувається практично миттєво, із подальшим розсиланням push-повідомлень, SMS або дзвінків користувачам, а також створенням системних сповіщень у програмному забезпеченні Ajax PRO Desktop.

Дані з відеокамер Ajax TurretCam передаються на мережевий відеореєстратор Ajax NVR, де зберігаються у вигляді високоякісного відеоархіву. Запис може відбуватися безперервно, за розкладом або лише у випадках тривог, що знижує навантаження на диски та зменшує обсяг даних. Збереження відео здійснюється на вбудовані жорсткі диски обсягом до шістнадцяти терабайтів, що забезпечує кілька тижнів безперервного архівування.

Відеореєстратор дозволяє здійснювати фільтрацію подій за датою, типом пристрою, конкретним інцидентом або місцем спрацювання. Це значно пришвидшує пошук у архіві, особливо у випадках проведення службових

розслідувань або передачі інформації до правоохоронних органів. Передавання даних з камер до відеореєстратора здійснюється за внутрішнім протоколом Ajax, оптимізованим для швидкої синхронізації подій із відео.

Інтеграція подієвих сигналів та відеопотоків – це ще один важливий елемент системи. У момент спрацювання будь-якого датчика система автоматично пов’язує цю подію з відповідним фрагментом відео. Такий підхід дозволяє не лише отримувати миттєві візуальні підтвердження, а й зменшує кількість хибних тривог, оскільки користувач або охоронна служба можуть перевірити, що саме спричинило сигнал.

Керування всіма механізмами зберігання даних здійснюється через єдиний інтерфейс, доступний у мобільному застосунку або на платформі Ajax PRO Desktop. Це забезпечує зручність адміністрування, швидкий доступ до архівів, контроль використання простору на дисках, а також можливість експорту потрібних фрагментів для збереження або передачі.

Окремо варто відзначити високий рівень захисту даних. Усі події, передані в Ajax Cloud, проходять через зашифровані канали з використанням сучасних криптографічних протоколів. Доступ до архівів обмежується системою прав і рівнів доступу, а додатковим рівнем безпеки виступає двофакторна автентифікація при вході в систему.

Таким чином, побудована система забезпечує надійне, захищене та структуроване зберігання інформації, а також швидкий і зручний доступ до неї в будь-який момент. Це дозволяє максимально підвищити оперативність реагування на події, мінімізувати час на аналіз ситуацій і забезпечити повну інформаційну прозорість роботи всієї архітектури безпеки.

2.6 Засоби віддаленого керування

Однією з ключових переваг сучасної системи безпеки на основі Ajax є можливість повноцінного віддаленого керування всією архітектурою через спеціалізоване програмне забезпечення. Для цього компанією Ajax Systems

розроблено дві взаємодоповнювальні платформи – Ajax PRO Desktop і Ajax Security System. Кожна з них орієнтована на свого користувача – професійного адміністратора або кінцевого власника об’єкта – але разом вони утворюють єдиний контрольний інтерфейс з високим рівнем деталізації, прозорості та гнучкості.

Ajax PRO Desktop – це професійна десктопна система керування, призначена для інженерів, монтажників, технічного персоналу та представників охоронних компаній. Основне її призначення – централізоване адміністрування декількох об’єктів одночасно. Користувач може у єдиному інтерфейсі підключити десятки або сотні об’єктів, перемикатися між ними, отримувати статуси в реальному часі, а також змінювати налаштування як окремих пристроїв, так і всієї системи на конкретному об’єкті.

Об’єкт у PRO Desktop логічно поділяється на кімнати або зони, до яких прив’язуються всі встановлені на території пристрої – датчики руху, вологи, задимлення, реле, камери, сирени. Це дозволяє не лише структуризувати інформацію, а й швидко орієнтуватися у фізичному розташуванні обладнання. Для кожного пристрою у кімнаті відображається його статус – чи він активний, чи має збої, який рівень сигналу, заряд батареї, чи не втрачено зв’язок із хабом. За потреби оператор може налаштувати інтервал пінгів, чутливість, сценарії реакції, часові рамки охорони та багато інших параметрів.

У системі доступна детальна історія подій, де фіксуються всі спрацювання, зміни статусу охорони, вмикання і вимикання пристроїв, технічні збої, втрати живлення або зв’язку. Усі ці події відображаються у хронологічному порядку з позначенням точного часу, ID пристрою та дій, що були вжиті системою або користувачем у відповідь. Це забезпечує високий рівень контролю й дозволяє оперативно виявляти несправності або ненормальні сценарії.

Ajax Security System – це мобільний застосунок, призначений для кінцевих користувачів, тобто власників об’єкта або відповідальних осіб. У ньому доступний базовий функціонал: перегляд статусу охорони, перемикання між режимами, перегляд повідомлень про тривоги, перегляд відео з камер у

реальному часі, доступ до журналу подій. Хоча цей інтерфейс не має адміністративного доступу до глибоких системних налаштувань, саме кінцевий користувач надає або відкликає права доступу для технічних спеціалістів. Це означає, що контроль над об’єктом завжди залишається за власником, і навіть охоронна компанія не може внести зміни без відповідного дозволу.

Інтеграція Ajax PRO Desktop та Ajax Security System дозволяє забезпечити чіткий розподіл ролей між адміністратором і власником об’єкта. Така модель особливо ефективна у корпоративному середовищі або при обслуговуванні великої кількості об’єктів – наприклад, офісів, складів, котеджів або філій компаній. Це дозволяє підтримувати належний рівень безпеки без постійної фізичної присутності інженера на місці, а також оперативно реагувати на зміни ситуації, спираючись на дистанційні інструменти управління.

Таким чином, архітектура керування системою Ajax забезпечує не лише зручність і оперативність, а й гнучкий рівень доступу, детальну аналітику, повний огляд усіх подій та надійний контроль над усіма компонентами безпеки – незалежно від місцезнаходження користувача чи адміністратора.

РОЗДІЛ 3
ФУНКЦІОНАЛЬНЕ МОДЕЛЮВАННЯ ТА АНАЛІЗ РІШЕННЯ

3.1 Опис умовного об’єкта та сценарії використання системи

Для практичного моделювання функціонування системи безпеки на базі Ajax Systems у межах дипломної роботи розглянуто умовний об’єкт – складське приміщення з адміністративною та технічною зоною. Такий об’єкт є типовим представником комерційної інфраструктури, яка потребує багаторівневого захисту, контролю доступу, постійного моніторингу параметрів навколишнього середовища та швидкого реагування на потенційні загрози.

Об’єкт складається з чотирьох основних приміщень: велике складське приміщення, адміністративний офіс, кімната персоналу, технічний санітарний блок та коридори, що з’єднують зони. Усі приміщення обладнані дверима з електрозамками, що керуються централізовано з використанням реле Ajax WallSwitch.

У денний час працівники отримують доступ до необхідних приміщень шляхом авторизації на клавіатурі, використовуючи персональні коди або DESFire-картки. Ці дії фіксуються системою, що дозволяє вести облік присутності та ідентифікацію дій кожного користувача. Ввечері система автоматично активує нічний режим охорони, при якому вхід дозволений лише уповноваженим особам.

Для забезпечення контролю мікроклімату в зоні зберігання продукції використовується Ajax LifeQuality – сенсор, що вимірює температуру, вологість та рівень вуглекислого газу. Якщо значення виходять за встановлені межі, система активує сценарій вентиляції або надсилає попередження відповідальним працівникам. Водночас, LeaksProtect виявляє витоки води у технічних приміщеннях і при спрацюванні активує Ajax WaterStop, перекриваючи подачу води в об’єкт.

Охоронні функції реалізовано за допомогою датчиків MotionProtect, DoorProtect, GlassProtect та сирен HomeSiren. У випадку виявлення вторгнення,

система переходить у режим тривоги: двері автоматично блокуються, вмикається освітлення, активуються всі сирени та надсилається сповіщення до користувача й охоронної компанії (рис. 3.1).

Рисунок 3.1 – Сценарій вторгнення на об’єкт

При виявленні пожежі за допомогою FireProtect, система діє за зворотним сценарієм – усі двері розблоковуються для евакуації, активується візуальне та звукове оповіщення по всьому об’єкту. Якщо передбачено, система запускає пожежогасіння через підключене реле.

Інтеграція відеоспостереження через Ajax TurretCam і відеореєстратор NVR 8-CH дозволяє здійснювати моніторинг ситуації в реальному часі та зберігати записи для подальшого аналізу. Всі події синхронізуються в хронологічному журналі, що доступний у програмі Ajax PRO Desktop.

Таким чином, реалізовані сценарії охоплюють контроль доступу, моніторинг середовища, запобігання затопленню, пожежну безпеку та відеонагляд, забезпечуючи комплексний захист умовного об’єкта в режимі реального часу.

3.2 План розміщення пристроїв та оптимізація зони дії

Правильне фізичне розташування пристроїв системи безпеки є критичним фактором для досягнення її ефективності, стабільності сигналу та оперативного реагування на події. З урахуванням особливостей умовного об’єкта – складського приміщення з прилеглими адміністративними і технічними зонами – було розроблено зональну схему розміщення обладнання, яка забезпечує як контроль периметра, так і внутрішній моніторинг та автоматизацію (рис. 3.2).

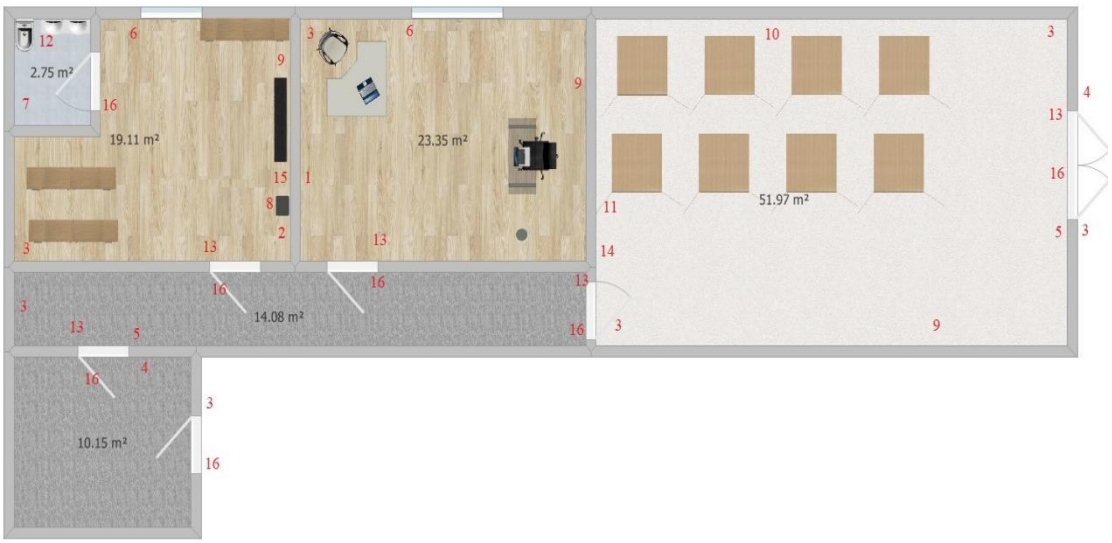

Рисунок 3.2 – Схема розміщення приладів

Позначення пристроїв на схемі:

1) Hub 2 Plus;
2) NVR;
3) TurretCam;
4) KeyPad;
5) MotionProtect;
6) GlassProtect;
7) WaterStop;

8) WallSwitch;

9) FireProtect;

10) LifeQuality;

11) ReX 2;

12) LeaksProtect;

13) DoorProtect;

14) HomeSiren;

15) Tenda TEG1110P-8-150W;

16) YLI YB-500B.

У коридорі, що з’єднує всі приміщення об’єкта, встановлено камеру TurretCam, яка забезпечує постійний візуальний контроль переміщень між зонами та фіксацію активності в умовах обмеженої видимості. Для фіксації несанкціонованого руху в нічний час або під час охоронного режиму використовується датчик MotionProtect, розташований у центрі проходу. Контроль за відкриттям дверей здійснюється двома сенсорами DoorProtect, встановленими на відповідних міжкімнатних дверях. Усі дверні прорізи в коридорі додатково обладнані чотирма електрозамками YLI YB-500B, які підключено до системи централізованого електроживлення і логіки сценарного керування доступом.

У кімнаті персоналу реалізовано локальну точку авторизації для співробітників. Безпосередньо в приміщенні встановлено сенсорну клавіатуру KeyPad TouchScreen Jeweller, яка дозволяє пройти ідентифікацію через персональний PIN-код, брелок або безконтактну карту.

На зовнішньому вході до кімнати персоналу з боку коридору встановлено камеру TurretCam, яка дозволяє в режимі реального часу контролювати підходи до дверей та фіксувати факти входу/виходу. Контроль доступу до цього входу здійснюється через електрозамок YLI YB-500B, інтегрований у загальну систему автоматизації.

У технічному санвузлі встановлено сенсор LeaksProtect, який виявляє витоки води на підлозі. У разі підтвердження витоку система автоматично

активує електромагнітний клапан Ajax WaterStop, що перекриває подачу води. Вхід до приміщення обладнано електрозамком YLI YB-500B, що також реагує на тривожні сценарії.

Технічне приміщення виконує роль центрального вузла зв’язку та електроживлення. Тут встановлено PoE-комутатор Tenda TEG1110P-8-150W, який одночасно забезпечує живлення та мережеву комунікацію для всіх семи камер TurretCam. Також у кімнаті розміщується відеореєстратор Ajax NVR 8-CH, який виконує функції зберігання відеоархіву. Окрім цього, технічна зона обладнана сенсором відкривання DoorProtect, пожежним сповіщувачем FireProtect, склосповіщувачем GlassProtect, а також реле WallSwitch Jeweller, яке керує живленням світильників, замків та інших пристроїв. Камера TurretCam забезпечує відеомоніторинг усього приміщення.

Центром усієї системи є адміністративна кімната, де встановлено головний хаб Ajax Hub 2 Plus, що забезпечує двосторонній зв’язок з усіма пристроями та виконує функції логіки, сценарного керування і синхронізації з мобільними застосунками. У цій зоні також розміщено датчик відкривання дверей DoorProtect, склосповіщувач GlassProtect, пожежний сенсор FireProtect і камера TurretCam, що покриває всю площу приміщення для загального контролю.

У складському приміщенні передбачено повноцінну охоронну, пожежну та екологічну систему моніторингу. Тут встановлено датчик руху MotionProtect, сенсор якості повітря Ajax LifeQuality, пожежний сповіщувач FireProtect і сирену HomeSiren для оперативного сповіщення персоналу про події. Для забезпечення доступу використовується клавіатура KeyPad TouchScreen Jeweller на зовнішньому вході. У приміщенні встановлено дві камери TurretCam, які забезпечують повний огляд приміщення по діагоналі, а також ретранслятор ReX 2 для стабілізації сигналу віддалених пристроїв.

На зовнішньому фасаді біля головного входу до складу встановлено камеру TurretCam, що дозволяє здійснювати моніторинг підходів до об’єкта з боку вулиці. Тут також розміщено клавіатуру KeyPad TouchScreen Jeweller, яка

забезпечує авторизацію доступу персоналу у визначений час.

3.3 Налаштування системи та перевірка працездатності

Після завершення проектування системи безпеки наступним етапом є її фізичне встановлення. Монтаж має відбуватися згідно з заздалегідь розробленим планом, що враховує особливості об’єкта: розташування кімнат, тип стін, місця прокладання кабелів, та зони стабільного радіосигналу.

3.3.1 Монтаж центрального блоку та комунікаційного вузла

Встановлення починається з розміщення центрального контролера Ajax Hub 2 Plus у центральній частині об’єкта – на висоті 1.5-2 метри від підлоги, у точці, що забезпечує найкраще бездротове покриття. До хаба підключається живлення 110-230 В, дротовий Ethernet-кабель для доступу до Інтернету, а також встановлюються дві SIM-карти як резервні канали зв’язку. У разі потреби, додається джерело безперебійного живлення.

У технічному приміщенні організовується комунікаційний вузол: встановлюється PoE-комутатор Tenda TEG1110P-8-150W, що забезпечує як живлення, так і передачу відеосигналу до всіх 7 IP-камер Ajax TurretCam. Кожна камера з’єднується з комутатором через один Ethernet-кабель (тип Cat.5e або Cat.6), що значно спрощує прокладання. У цьому ж вузлі розміщується відеореєстратор Ajax NVR 8-CH, який приймає потоки з камер.

3.3.2 Первинне налаштування системи

Після встановлення обладнання налаштування здійснюється через Ajax PRO Desktop:

1) активація хаба та перевірка підключення: у розділі Ethernet обирається тип підключення (DHCP або статична IP-адреса), перевіряється наявність зв’язку через SIM-карти;

2) додавання пристроїв: кожен датчик, камера або реле вмикається та додається до системи через меню керування. У процесі відображається статус підключення, заряд батареї, рівень сигналу Jeweller, і в разі потреби – система

пропонує змінити місце встановлення або використати ReX 2 для розширення зони покриття (рис. 3.3-3.5);

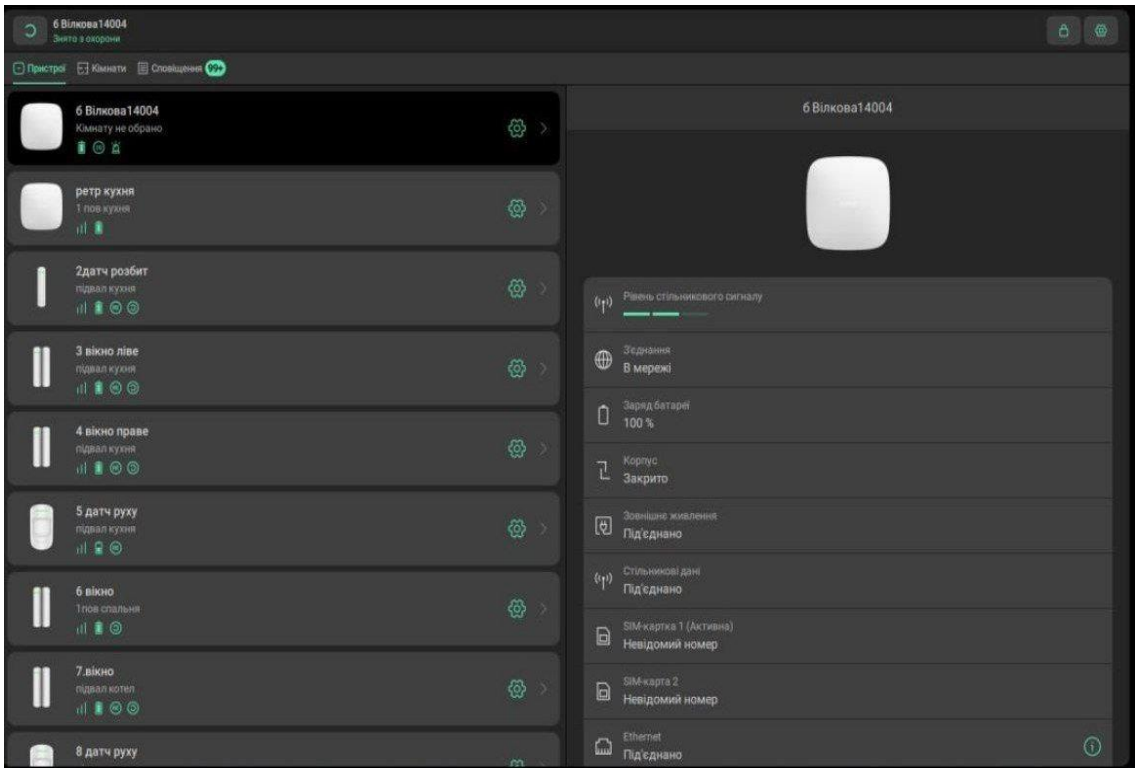

Рисунок 3.3 – Ajax Pro Desktop приклад переліку приладів впроваджених в об’єкт

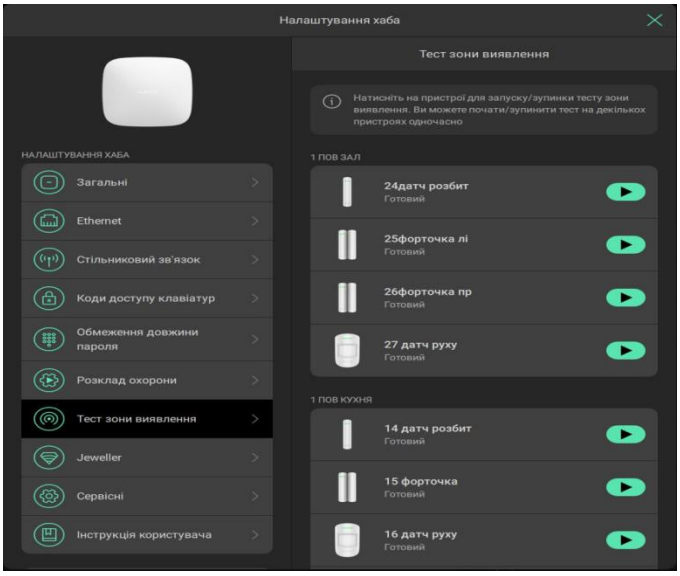

Рисунок 3.4 – Ajax Pro Desktop приклад переліку приладів підключених доконкретного хабу

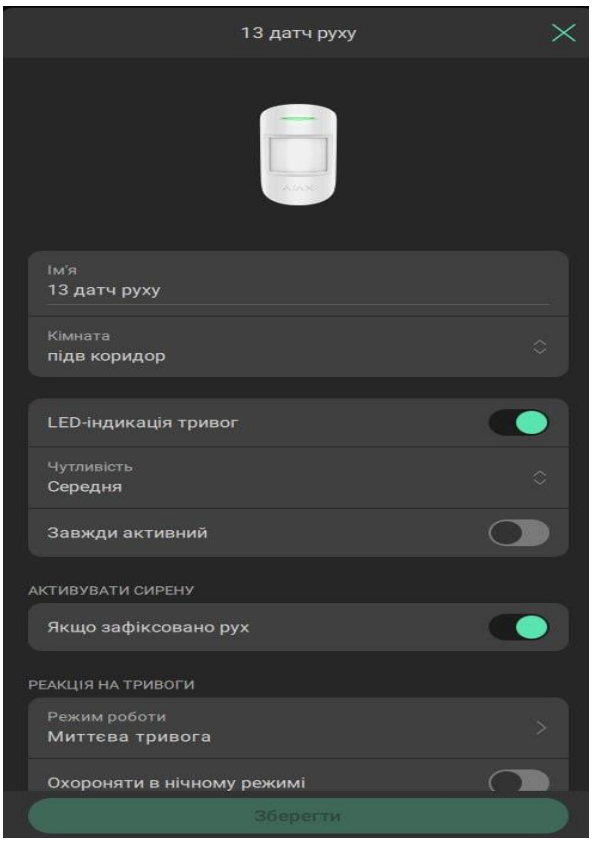

Рисунок 3.5 – Ajax Pro Desktop приклад меню налаштування прилада

3) присвоєння кімнат і сценаріїв: кожен пристрій отримує назву та прив'язується до конкретного приміщення; налаштовуються реакції на події;

4) тестування зон виявлення: у відповідному меню запускається тест виявлення руху, відкривання, вібрації тощо – для перевірки кута спостереження, чутливості, та наявності завад;

5)налаштування протоколів Jeweller та Wings: встановлюються інтервали опитування, пороги втрати зв'язку, виявлення глушіння сигналу. Протокол Wings, при наявності камер із фотозахопленням, відповідає за передачу зображень із мінімальною затримкою.

3.3.3 Перевірка інтеграції камер

У стандартному сценарії IP-камери Ajax TurretCam автоматично визначаються відеореєстратором Ajax NVR 8-CH. Відеопотік передається без необхідності додаткових налаштувань, а відео зберігається в архіві.

Проте у випадку, якщо камера не з'являється у списку пристроїв або немає відео в режимі реального часу, рекомендується перевірити мережеву видимість

пристрою. Якщо камера стороннього виробника або сумісна, але не Ajax, її можна додати вручну через підтримку протоколу ONVIF.

ONVIF (Open Network Video Interface Forum) – це відкритий стандарт, який дозволяє відеокамерам і реєстраторам різних брендів взаємодіяти між собою [20].

Він дозволяє:

– автоматично виявляти камери у локальній мережі;

– здійснювати базове управління;

– транслювати відео незалежно від виробника;

– налаштовувати передачу тривог та запис.

У випадку проблем із автоматичним додаванням TurretCam – ONVIF слугує як додатковий шлях інтеграції.

3.3.4 Завершення інсталяції

На завершення виконується повна перевірка сценаріїв – спрацьовування реле, запуск сирен, запис відео, надсилання сповіщень, а також автоматичне перекриття води. Додаються користувачі з відповідними рівнями доступу, і активується розклад охорони.

Таким чином, використання Ajax PRO Desktop дозволяє не лише виконати базове налаштування, а й перевірити стабільність, покриття та функціональність усіх пристроїв системи, з можливістю гнучкої адаптації до особливостей об’єкта.

3.4 Аналіз стабільності мережі

Стабільність мережі системи безпеки – ключовий фактор, що визначає її надійність у повсякденному використанні та в критичних ситуаціях. У проєкті, реалізованому на базі Ajax Systems, враховано усі основні виклики, пов’язані з втратами сигналу, затримками в передачі даних, залежністю від інтернет-з’єднання та електропостачання.

Усі периферійні пристрої Ajax (датчики, реле, клавіатури) працюють на базі фірмового протоколу Jeweller, який забезпечує двосторонній зв’язок,

шифрування переданих даних та автоматичне резервування каналу. Jeweller дозволяє хабу постійно контролювати стан пристроїв, отримувати зворотний зв’язок про виконання команд, а також миттєво реагувати на порушення в роботі. У разі втрати сигналу, пристрій автоматично позначається в Ajax PRO Desktop як недоступний.

Додатковий протокол Wings, застосований для передачі мультимедійного контенту (наприклад, фотопідтверджень із датчиків із камерами), дозволяє мінімізувати затримку та уникнути втрат якості зображення.

Для покриття великих площ або складних об’єктів із товстими бетонними стінами використовується ретранслятор ReX 2, який забезпечує стабільну передачу сигналу на відстанях до 1800 метрів у приміщеннях. Завдяки цьому уся бездротова мережа зберігає цілісність навіть у важкодоступних зонах.

Усі IP-камери системи з’єднані через PoE-комутатор Tenda TEG1110P-8-150W, який одночасно забезпечує живлення та передає відеопотік. Цей підхід дозволяє зменшити кількість кабелів та покращити якість зв’язку. Камери працюють стабільно за умови належного монтажу та коректного вибору типу кабелю (Cat.6 або Cat.5e).

Відео передається до реєстратора Ajax NVR 8-CH, який підтримує до восьми каналів відеоспостереження та забезпечує збереження записів. У разі перебоїв в електропостачанні система переходить на резервне живлення (UPS), що дозволяє зберігати дані та підтримувати зв’язок.

Таким чином, побудована архітектура є багатоканальною, резервованою та адаптованою до типових загроз – від втрати інтернету до перешкод у радіосигналі. Це забезпечує високу стабільність функціонування мережі в режимі 24/7.

3.5 Порівняльна характеристика варіантів архітектурних рішень

У процесі проєктування мережевої архітектури системи безпеки на базі Ajax Systems було проаналізовано кілька можливих конфігурацій з урахуванням

потреб об’єкта, технічних обмежень, ступеня ризику та можливостей розширення. Основною метою такого аналізу було знайти оптимальний баланс між надійністю, гнучкістю, функціональністю та вартістю реалізації.

Перший базовий варіант передбачав мінімальну конфігурацію без використання ретрансляторів сигналу, без джерел резервного живлення та з єдиним каналом зв’язку – Ethernet. Датчики розташовувалися в межах прямої зони дії хаба, а відеонагляд реалізовувався за допомогою камер, що записують відео на внутрішні носії або ж на реєстратор без резервного доступу до мережі. Такий варіант є дешевим у реалізації, однак виявився найбільш вразливим до збоїв, оскільки будь-яке пошкодження мережевого кабелю чи відключення електроенергії призводило до повної втрати контролю над об’єктом.

Другий, покращений варіант включав часткове резервування. До системи додавався GSM-модуль як резервний канал зв’язку, що дозволяло підтримувати доступ до системи у випадку зникнення інтернету. Також передбачалося резервне живлення для хаба, комутатора та відеореєстратора, що забезпечувало короткострокову автономність. Камери підключалися через PoE-комутатор, що спрощувало монтаж. У цьому варіанті зростала надійність системи та її здатність продовжити функціонування в умовах локальних відмов, однак залишалася певна залежність від мобільного зв’язку.

Остаточним обраним варіантом стала розширена конфігурація, яка забезпечує повне резервування та максимальну стійкість до відмов. У цій архітектурі реалізовано три канали зв’язку – основний дротовий Ethernet, два незалежних GSM-канали та додатковий Wi-Fi як резерв. Усі критичні елементи, включаючи хаб, PoE-комутатор, NVR та маршрутизатор, підключені до джерел безперебійного живлення. Для покриття всіх приміщень з урахуванням можливих перешкод встановлено ретранслятор ReX 2. Камери Ajax TurretCam працюють через PoE-комутатор, що спрощує кабельну інфраструктуру. Вся відеоаналітика виконується на зовнішньому відеореєстраторі Ajax NVR 8-CH з можливістю збереження архіву як локально, так і в хмарі. Усі автоматизовані сценарії – контроль вологості, температури, сповіщення про вторгнення або

пожежу, перекриття води, блокування замків, контроль доступу – активні та повністю функціональні.

Порівняння трьох підходів дозволило зробити висновок, що саме останній варіант відповідає сучасним вимогам до надійної та масштабованої системи безпеки. Його гнучка структура дозволяє адаптуватися до змін у конфігурації об’єкта, додавати нові пристрої, зберігаючи при цьому централізоване керування. Така архітектура виявилася найефективнішою в умовах підвищених вимог до стабільності, автономності та швидкості реагування на інциденти.

3.6 Визначення переваг обраної архітектури та її ефективності

Результатом багаторівневого аналізу та моделювання стала архітектура мережі системи безпеки, побудована на базі пристроїв Ajax із використанням централізованого керування, бездротової комунікації та резервованих каналів зв’язку. З огляду на завдання, що ставилися перед системою, ця конфігурація дозволяє досягти балансу між гнучкістю, надійністю та енергоефективністю.

Однією з ключових переваг є високий рівень автономності пристроїв. Усі сенсори мають вбудовані джерела живлення з тривалим терміном служби, що дозволяє зменшити залежність від зовнішніх джерел електроенергії. Централізовані елементи, що потребують постійного живлення, додатково захищені джерелом безперебійного живлення, що гарантує безперервну роботу навіть у разі аварійного знеструмлення.

Друга значуща перевага – багатоканальна структура комунікації. Використання одночасно трьох каналів Ethernet, GSM і Wi-Fi забезпечує високу стійкість до втрати зв’язку. Система автоматично перемикається між каналами залежно від умов, що дозволяє зберігати стабільне з’єднання навіть при частковій втраті інфраструктури. Завдяки цьому зростає надійність передачі тривожних повідомлень і команд керування.

Сценарна логіка, яка реалізована у хабі, дозволяє автоматизувати критично важливі дії, не потребуючи постійного контролю з боку користувача. Це

стосується як охоронного реагування (автоматичне замикання дверей, вмикання світла, виклик охорони), так і пожежних ситуацій (відкриття дверей, активація сповіщень, запуск гасіння). Іншими словами, система здатна самостійно оцінювати події та виконувати задані дії без затримок.

Архітектура підтримує інтелектуальну диференціацію зон, що дає змогу поділити об’єкт на кімнати або сектори з різними рівнями доступу, індивідуальними датчиками та сценаріями реагування. Такий підхід дозволяє масштабувати систему в межах великого об’єкта, зберігаючи при цьому зрозумілу логіку адміністрування.

Окремо слід відзначити гнучкість у застосуванні технологій зберігання даних. Відео може зберігатися як на внутрішніх пристроях, так і на віддалених серверах (хмара або NAS). Це забезпечує надійність збереження критичних записів навіть при фізичному пошкодженні частини обладнання.

І, нарешті, обрана конфігурація дозволяє забезпечити інтеграцію системи у загальну концепцію «розумного об’єкта», де охоронні функції поєднуються з автоматизованим освітленням, кліматичним контролем, електропостачанням та управлінням доступом. Система є не лише реактивною, а й проактивною – вона формує безпечне, контрольоване та адаптивне середовище для експлуатації об’єкта.

Усі ці характеристики дозволяють стверджувати, що обрана архітектура є технічно обґрунтованою, економічно доцільною і готовою до подальшого масштабування або інтеграції з додатковими функціями у разі розширення потреб замовника.

ВИСНОВКИ

Сучасні системи безпеки базуються на інтеграції різних підсистем, таких як охорона, пожежна сигналізація, відеоспостереження та контроль доступу, в єдину архітектуру, що дозволяє ефективно керувати безпекою об’єкта в реальному часі. Ключовими принципами є модульність, централізоване управління, масштабованість та резервування каналів зв’язку та живлення. Використання бездротових технологій значно спрощує розгортання системи та забезпечує гнучкість її розширення.

Аналіз обладнання Ajax Systems показав, що воно відповідає сучасним вимогам до безпекових систем. Центральний контролер Hub 2 Plus забезпечує надійне управління пристроями, підтримуючи різні канали зв’язку та резервне живлення. Датчики руху, відкривання дверей, розбиття скла, витоку води та інші елементи системи працюють автономно, що зменшує залежність від зовнішніх джерел живлення. Інтеграція відеоспостереження через Ajax NVR дозволяє створювати комплексні рішення з можливістю швидкого реагування на події.

Досліджено, що архітектура системи безпеки повинна враховувати необхідність централізованого управління, бездротового зв’язку з високим рівнем захисту, резервування каналів передачі даних та живлення, а також можливість автоматизації сценаріїв реагування. Вибір апаратних та програмних компонентів на основі Ajax Systems обґрунтований їхньою надійністю, простотою інтеграції та можливістю масштабування.

Структурна схема мережі, побудована за топологією «зірка», забезпечує стабільність роботи системи завдяки централізованому керуванню через Hub 2 Plus, резервуванню каналів зв’язку (Ethernet, Wi-Fi, GSM) та використанню ретрансляторів для покращення покриття. Живлення критичних вузлів забезпечується резервними джерелами, що підвищує відмовостійкість системи.

Для підвищення стабільності роботи запропоновано багаторівневе резервування: альтернативні канали зв’язку, автономні джерела живлення,

посилення радіопокриття за допомогою ретрансляторів та захист передачі даних через шифрування. Ці заходи дозволяють мінімізувати ризики виходу системи з ладу навіть у разі часткових збоїв.

Таким чином, побудова сучасної системи безпеки на базі Ajax Systems забезпечує високий рівень захисту завдяки інтеграції різних підсистем, надійності обладнання, гнучкості архітектури та ефективним механізмам резервування, що було продемонстровано на схемі об’єкта.

Використання бездротових технологій та автоматизованих сценаріїв реагування значно підвищує ефективність роботи системи, що робить її придатною як для приватного, так і для комерційного застосування.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ajax Systems. Jeweller. Опис бездротової технології зв’язку Ajax. URL: *https://short-link.me/-lsa* (дата звернення 12.02.2025).

2. Ajax Systems. Дальність дії бездротового зв’язку. Технічні можливості протоколу Jeweller. URL: *https://short-link.me/-lsd* (дата звернення 12.02.2025).

3. Alesta. Катастрофостійкість та відмовостійкість дата-центрів. Огляд стратегій для забезпечення безперервної роботи систем. URL: *https://short-link.me/-lsg* (дата звернення 09.03.2025).

4. Ajax Systems. Хаб Hub 2 Plus. Опис функціоналу та характеристик пристрою. URL: *https://short-link.me/-lsB* (дата звернення 09.03.2025).

5. Ajax Systems. Датчик відкривання DoorProtect. Призначення та специфікація. URL: *https://short-link.me/-lsF* (дата звернення 09.03.2025).

6. Ajax Systems. Датчик розбиття скла GlassProtect. Принцип роботи і технічні параметри. URL: *https://short-link.me/-lsJ* (дата звернення 09.03.2025).

7. Ajax Systems. Внутрішня сирена HomeSiren. Технічні особливості та сценарії використання. URL: *https://short-link.me/lsT* (дата звернення 09.03.2025).

8. Ajax Systems. Датчик руху MotionProtect. Огляд та принцип роботи. URL: *https://short-link.me/-lt2* (дата звернення 11.03.2025).

9. Ajax Systems. Сенсор якості повітря LifeQuality. Моніторинг мікроклімату приміщення. URL: *https://short-link.me/-lt6* (дата звернення 12.04.2025).

10. Ajax Systems. Датчик протікання LeaksProtect. Призначення та технічні параметри. URL: *https://short-link.me/-ltv* (дата звернення 11.03.2025).

11. Ajax Systems. Клапан WaterStop. Інтелектуальне керування водопостачанням. URL: *https://short-link.me/-ltx* (дата звернення 11.03.2025).

12. Ajax Systems. Ретранслятор сигналу ReX 2. Розширення зони дії системи безпеки. URL: *https://short-link.me/-ltz* (дата звернення 11.03.2025).

13. Ajax Systems. Відеореєстратор NVR 8-CH. Огляд відеоархівування та характеристик. URL: *https://short-link.me/-ltB* (дата звернення 14.03.2025).

14. Ajax Systems. Сенсорна клавіатура KeyPad TouchScreen. Функціональність та особливості керування. URL: *https://short-link.me/13pbv* (дата звернення 14.03.2025).

15. Ajax Systems. Реле керування WallSwitch. Принцип роботи та сценарії використання. URL: *https://short-link.me/-ltK* (дата звернення 14.03.2025).

16. Rozetka. Замок електроригельний врізний YLI Electronic YB-500A. URL: *https://short-link.me/-ltN* (дата звернення: 14.03.2025).

17. Ajax Systems. Камера Ajax TurretCam. Відеоспостереження та аналітика. URL: *https://short-link.me/-ltQ* (дата звернення 17.03.2025).

18. Ajax Systems. Пожежний датчик FireProtect. Виявлення диму та температури. URL: *https://short-link.me/-ltR* (дата звернення 17.03.2025).

19. Guru99. Network Topology. Види мережевої топології та їх особливості. URL: *https://short-link.me/-ltX* (дата звернення 17.03.2025).

20. ONVIF. Open Network Video Interface Forum Стандартизація IP-відеоспостереження та протоколів сумісності. URL: *https://short-link.me/13pbO* (дата звернення 03.04.2025).