НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
(повна назва інституту/факультету)

Кафедра акустичних та мультимедійних електронних систем
(повна назва кафедри)

«На правах рукопису»
УДК 621.397

«До захисту допущено»
Завідувач кафедри
Сергій НАЙДА
(ініціали, прізвище)
"1" грудня 2020 р.

Магістерська дисертація

зі спеціальності (спеціалізації) 171 Електроніка (Електронні системи мультимедіа та засоби Інтернету-речей)
(код і назва спеціальності)

на тему: «Технічні особливості реалізації системи охорони об'єкта із застосуванням технології Інтернету речей».

Виконав студент ІІ курсу, групи ДВ-92мп
(шифр групи)

Переверзєв Олексій Андрійович _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник к.т.н., доц. Трапезон К.О. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент доц. кафедри ЕПС доц., к.т.н. Михайлов С.Р. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент Переверзєв О.А _____.

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут (факультет) Факультет електроніки
(повна назва)

Кафедра акустичних та мультимедійних електронних систем
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (освітня програма) 171 Електроніка

(Електронні системи мультимедіа та засоби Інтернету речей)
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Сергій НАЙДА
(підпис) (ініціали, прізвище)
«1» грудня 2020 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Переверзєву Олексію Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема дисертації «Технічні особливості реалізації системи охорони об'єкта із застосуванням технології Інтернету речей».

Науковий керівник дисертації к.т.н., доц. Трапезон Кирило Олександрович .
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

затверджені наказом по університету від «05» листопада 2020 р. № 3241-с

2. Строк подання студентом дисертації 01.12.2020 р.

3. Об'єкт дослідження: система охорони приміщення із застосуванням технічних рішень технології Інтернету речей .

4. Предмет дослідження (Вхідні дані – для магістерської дисертації за освітньо-професійною програмою): наявність системи контролю та управління доступом – так; базова технологія для розгортання IP-відеоспостереження – PoE; види камер для системи відеоспостереження – корпусні, поворотні, безпроводові; підтримка технології безпроводового зв'язку Jeweller - так.

5. Перелік завдань, які потрібно розробити: проаналізувати можливі технічні рішення з проектування системи контролю доступу в складі системи охорони об'єкта; дослідити особливості впровадження технології M2M в концепції IoT; визначити основні компоненти для створення системи охорони об'єкту; розробити схему розташування обладнання для реалізації системи охорони об'єкта із застосуванням технології Інтернету речей.
6. Перелік графічного (ілюстративного) матеріалу: 15 слайдів презентації, основними назвами плакатів якої є сформульовані завдання, мета, постановка проблеми, особливості створення системи охорони об'єкту на основі використання систем aCaaS, технології LoRaWAN з підтримкою Cloud-сервісу.
7. Орієнтовний перелік публікацій: 1) Дослідження особливостей створення системи безпеки будинку на основі концепції Інтернету речей // Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки – 2020. – Том.31 (70). – №1. - С. 36-41.; 2) Дослідження особливостей використання технології LPWAN у сучасних системах охорони житлових будинків // Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки – 2020. – Том.31 (70). – №3. - С. 71-76.
8. Дата видачі завдання 1. 09. 2020 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Розгляд ключових особливостей впровадження системи контролю та управління доступом при реалізації системи охорони об'єкта.	1.09.2020 – 1.10.2020	Виконано
2	Аналіз передових технологій в концепції Інтернету речей та їх вибір при створенні системи відеонагляду приміщення. Дослідження рішень з вибору видів камер для системи відеонагляду	2.10.2018 – 30.10.2020	Виконано
3	Вибір обладнання та розроблення плану схеми системи охорони об'єкта з підтримкою технології Інтернету речей	31.10.2020 – 1.12.2020	Виконано
4	Підготовка матеріалів до друку та оформлення пояснювальної записки	02.12.2020 – 05.12.2020	Виконано
5	Підготовка та оформлення презентації для доповіді	06.12.2020 – 12.12.2020	Виконано

Студент _____ Олексій ПЕРЕВЕРЗЄВ
(підпис) (ініціали, прізвище)

Науковий керівник _____ Кирило ТРАПЕЗОН
(підпис) (ініціали, прізвище)

УДК 621.397

РЕФЕРАТ

Переверзєв О.А. Технічні особливості реалізації системи охорони об’єкта із застосуванням технології Інтернету речей: магістерська дис. : 171 Електроніка. Київ, КПІ ім. Ігоря Сікорського, 2020. 63 с.

Магістерська дисертація: 63 с., 19 рис., 19 табл., 1 дод., 13 джерел.

Ключові слова: камера, інтернет речей, технологія cloud-сервіс, power over ethernet, мережа, контроль доступу, модуль, сервер, електроніка.

Актуальність дослідження. Розвиток Інтернету речей в даний час є одним з пріоритетних напрямків в технологічному розвитку людства. В процес створення IoT-систем залучено сьогодні безліч стартапів, інтеграторів, розробників програмного забезпечення. Речі, об'єкти Інтернету речей, функціонують вже як окремі модулі, які зареєстровані в системі, і які пов'язані спільним алгоритмом роботи та мають доступ в Інтернет. Можна відмітити, що в системі IoT реєструються і взаємодіють в єдиному інформаційному просторі наступні різнопланові електронні компоненти і системи: датчики положення, тиску, температури, руху, диму; цифрові відеокамери і мікрофони; різні вузли знаходяться: реле, лампи, обігрівачі, мотори та ін.; інтерфейси людино-машинного взаємодії, тобто пристрої введення виведення інформації, пульти дистанційного керування і т. д. І створення на основі існуючих рішень та обладнання комплексної системи охорони на основі Інтернету речей є однією з передових задач, оскільки в такому випадку у власників такої системи відкриваються додаткові можливості контролю та управління даною системою охорони без прив’язки до географічного місця знаходження. До того ж, в при такій реалізації значно спрощується сам процес збору та аналізу даних системи охорони.

Мета дослідження полягає у розробленні технічних рішень та рекомендацій зі створення системи охорони приміщення на основі засобів та компонентів технології Інтернету речей.

Завдання для досягнення мети: проаналізувати можливі технічні рішення з проектування системи контролю доступу в складі системи охорони об’єкта; дослідити особливості впровадження технології M2M в концепції IoT; визначити основні компоненти для створення системи охорони об’єкту; розробити схему розташування обладнання для реалізації системи охорони об’єкта із застосуванням технології Інтернету речей.

Об’єкт дослідження: система охорони приміщення із застосуванням технічних рішень технології Інтернету речей.

Предмет дослідження: електронне обладнання та компоненти, які утворюють систему охорони об’єкту.

Методи дослідження: алгоритми та методи, які визначені в основі функціонування систем та технологій в рамках концепції Інтернету речей, технології та алгоритми роботи мережевої структури системи безпеки за рівнями.

Наукова новизна отриманих результатів: 1) запропоновані варіанти реалізації системи охорони об’єкту на основі вибору сучасних електронних засобів з підтримкою технології Інтернету речей; 2) запропоновано послідовний

алгоритм зі створення плану розташування елементів системи охорони для певного приміщення, основним призначенням якого є робота з фінансовими активами та матеріальними цінностями компанії.

Практичне значення одержаних результатів: результати роботи можуть бути використані при створенні аналогічних систем охорони в банківських структурах України.

Апробація результатів дисертації: опублікування двох статей у фаховому журналі з технічних наук (категорія “Б”) за проблематикою дисертації.

SUMMARY

Master's dissertation: 63 p., 19 fig., 19 tabl., 1 supplements, 13 sources.

Keywords: camera, internet of things, cloud service technology, power over ethernet, network, access control, module, server, electronics.

Relevance of research. The development of the Internet of Things is currently one of the priority areas in the technological development of mankind. Many startups, integrators, software developers are involved in the process of creating IoT-systems today. Things, objects of the Internet of Things, already function as separate modules that are registered in the system, and which are connected by a common algorithm and have access to the Internet. It can be noted that in the IoT system the following various electronic components and systems are registered and interact in a single information space: position, pressure, temperature, motion, smoke sensors; digital video cameras and microphones; various units are: relays, lamps, heaters, motors, etc .; human-machine interfaces, ie input-output devices, remote controls, etc. And the creation of a comprehensive Internet-based security system based on existing solutions and equipment is one of the best tasks, because in this case the owners of such a system open additional opportunities to control and manage this security system without reference to the geographical location. In addition, this implementation greatly simplifies the process of collecting and analyzing data from the security system.

The purpose of the study is to develop technical solutions and recommendations for the creation of a security system based on the means and components of Internet of Things technology.

Objectives to achieve the goal: to analyze possible technical solutions for designing an access control system as part of the object security system; explore the features of the introduction of M2M technology in the concept of IoT; identify the main components for creating a system of protection of the object; develop a layout of equipment for the implementation of the security system of the object with the use of Internet of Things technology.

Object of study: room security system with the use of technical solutions of the Internet of Things technology.

Subject of study: electronic equipment and components that make up the security system of the facility.

Research methods: algorithms and methods that are defined in the basis of the functioning of systems and technologies within the concept of the Internet of Things, technologies and algorithms of the network structure of the security system by levels.

Scientific novelty of the obtained results: 1) the offered options of realization of system of protection of object on the basis of a choice of modern electronic means with support of technology of the Internet of things; 2) a consistent algorithm for creating a plan for the location of security system elements for a particular room, the main purpose of which is to work with financial assets and tangible assets of the company.

The practical implications of the findings: the results of the work can be used in the creation of similar security systems in the banking structures of Ukraine.

Testing the results of the thesis: publication of two articles in a professional journal of technical sciences (category "B") on the dissertation.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ

CMOS	-	Complementary Metal-Oxide-Semiconductor;
IaaS	-	Infrastructure as a Service;
IoT	-	Internet of Things;
GSM	-	Global System for Mobile Communications;
MTU	-	Maximum Transmission Unit;
PER	-	Packet of Error;
PTZ	-	Pan-tilt-zoom;
RFID	-	Radio Frequency IDentification;
SaaS	-	Software as a Service;
СКУД	-	Система Контролю та Управління Доступу.

ВСТУП

Стрімкий розвиток та поширення технологій Інтернету речей в різних аспектах існування сучасного людства змушує розробників відповідного електронного обладнання шукати нові шляхи застосування IoT. Одним з таких перспективних напрямків можна вважати і галузь проектування систем безпеки приміщень. Справа у тому, що класичні схеми створення систем охорони будинків залежать в переважній більшості від зовнішніх факторів – умови живлення пристроїв, електромагнітна сумісність, природні явища. І в цьому сенсі говорити про достатній рівень надійності таких систем вже не приходиться. Альтернативою можуть стати гібридні системи безпеки, які забезпечують базові послуги з охорони об’єктів з певним рівнем резервування. Тобто, поруч з традиційною схемною реалізацією систем безпеки наявні ще і системи на основі технології Інтернету речей. Важливість такого підходу значно підвищується, коли мова йде про приміщення, наприклад, банківського сектору. Саме питанням технічної реалізації системи охорони для такого роду будівель і присвячена дана дисертація. При цьому основна увага в комплексі охорони буде прикута системі відеонагляду, системі сигналізації та системи контролю та управлінням доступу в приміщення. Останню з перелічених систем і розглянемо далі.

1 СИСТЕМА КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ

Термін "контроль доступу" описує будь-які процеси, які пов'зані з контролем проходу відвідувача в будь-яку зону або з неї. Стандартний замок, де для відкриття використовується металевий ключ можна розглядати як спрощену форму "системи контролю доступу". Натомість надійність такої системи може викликати певні сумніви і тому з роками системи контролю доступу стають дедалі складнішими. Сьогодні термін "система контролю та управління доступом" найчастіше асоціюється з комп'ютерною електронною системою контролю доступу. Електронна система контролю доступу використовує спеціальну "пластикову картку входу, з чипом", а не металевий ключ, щоб дозволити доступ у захищену зону.

Призначення системи контролю доступу полягає у забезпеченні швидкого та зручного доступу для тих осіб, які мають дозвіл, і водночас необхідно надійно обмежити доступ сторонніх осіб.

Система контролю та управління доступом (СКУД) - це ряд програмного і апаратного забезпечення, який забезпечує порядок, контроль і реєстрацію пересування осіб по території, яка контролюється системою. Серед функцій таої системи варто відзначити наступні: обмеження доступу сторонніх на площу, що знаходиться під наглядом системи; обмеження свободи пересування відвідувачів відповідно до їх прав доступу. На рисунку 1.1 наведена типова система СКУД, яка на основі чисел пояснює послідовність функціонування цієї системи [1].

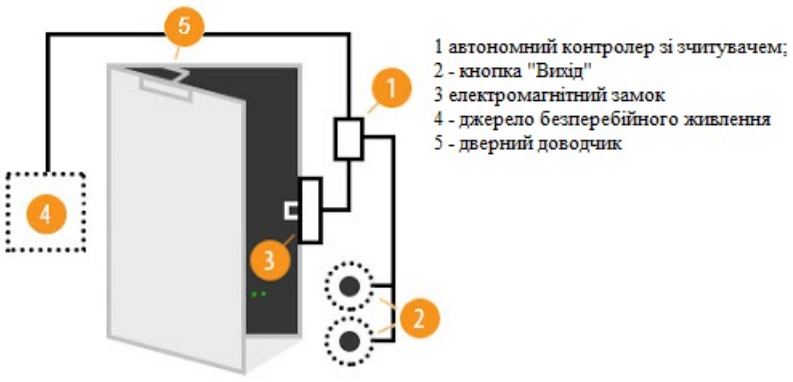

Рисунок 1.1 – Типова система контролю доступу

1.1 Принципи функціонування СКУД

СКУД на основі безконтактних пластикових карток в якості пропуску призначені для вирішення проблем підвищення безпеки об’єктів та забезпечення трудової дисципліни та порядку на підприємстві. Автоматизований пункт пропуску, що базується на турнікетах-штативах із використанням безконтактних карток при проходженні, значно підвищує рівень контролю доступу до підприємства. Система організовує пропуск працівників на територію, ідентифікуючи за допомогою безконтактних електронних карток за принципом "свій або чужий" і фіксуючи час проходження. Система дозволяє стежити за усіма подіями в точках доступу та видавати повідомлення оператору або охоронцеві про події тривоги (злам замків, порушення режиму контролю доступу тощо). Оператор може швидко керувати системними пристроями - дистанційно блокувати замки або, навпаки, відкривати їх, наприклад, у випадку пожежі.

Системне програмне забезпечення надає можливість вести базу даних персоналу (ім’я, посада, відділ, номер персоналу, режим роботи, фото, паспортні дані, пропуск, права доступу), а також безконтактні картки як значки.

Рисунок 1.2 – Пристрої для отримання доступу у приміщення

1.2 Основні складові системи контролю доступу

Системи контролю доступу відрізняються за типом та складністю. Однак більшість систем контролю доступу до карток складаються щонайменше з таких основних компонентів [2]:

- Картка доступу. Картку доступу можна сприймати як електронний "ключ". Картка доступу використовується особами для доступу через двері, захищені системою контролю доступу. Кожна картка доступу має унікальне кодування. Більшість карток доступу мають приблизно такий самий розмір, як і стандартна кредитна картка, і їх можна легко носити в гаманці або сумочці.
- Картрідери. Зчитувачі карток - це пристрої, що використовуються для електронного "зчитування" картки доступу. Зчитувачі карток можуть бути за типом "вставки" (що вимагає вставки картки у зчитувач), або можуть бути за типом зчитування на близькій відстані (тобто, для яких потрібно лише, щоб картка трималася в безпосередній близькості від 3 до 6 см. Зчитувачі карток зазвичай встановлюються на зовнішній (незахищеній) стороні дверей, яку вони контролюють.

Обладнання для електричних замків - обладнання, яке використовується для електричного блокування та розблокування дверей, які контролюються системою контролю доступу. Існує широкий вибір різних типів обладнання для електричних замків. До таких видів можна віднести електричні замки, електромагнітні замки, електричні пристрої виходу та багато інших. Конкретний тип та розташування фурнітури, що застосовуватиметься для кожних дверей, визначається виходячи з умов конструкції дверей.

Серверний комп'ютер контролю доступу - це "мозок" системи контролю доступу. Серверний комп'ютер контролю доступу виконує функції центральної бази даних та файлового менеджера для системи контролю доступу і відповідає за запис системної діяльності. Зазвичай, для управління великою кількістю дверей, що контролюються пристроєм зчитування карток, може

використовуватися єдиний серверний комп'ютер контролю доступу. Серверний комп'ютер контролю доступу - це, як правило, стандартний комп'ютер, на якому працює спеціальне прикладне програмне забезпечення системи контролю доступу.

У деяких випадках можна віддалено керувати СКУД. Це можна реалізувати кількома способами. По-перше, можливо встановити програмне забезпечення "клієнтського" контролю доступу на інші персональні комп'ютери компанії. І вони використають мережу для зв’язку з серверним комп’ютером і виконання всіх системних функцій.

По-друге, багато систем дозволяють використовувати стандартний інтерфейс веб-браузера для підключення до серверу. Уповноважені користувачі можуть увійти в систему за допомогою веб-браузера на будь-якому комп’ютері для виконання основних функцій.

Нарешті, деякі системи контролю доступу пропонують мобільні програми, які дозволяють керувати системою за допомогою смартфона.

1.3 ACaaS

Система контролю доступу запобігає несанкціонований доступ і дозволяє керівництву компанії встановлювати обмеження на доступ персоналу до приміщень в залежності від їх ролі в компанії. Незалежно від того, чи ми говоримо про складські комплекси, банківські установи, автостоянки, гаражі, готелі, навчальні заклади або бізнес-центри, у всіх них реалізований контроль доступу. Турнікети, зчитувальні карти, відеодомофони і системи сигналізації складають частину контролю доступу [3-6].

Разом з тим, за спостереженням розвитку цифрових технологій підходи AcaaS виводять безпеку сьогодні на новий рівень. AcaaS розшифровується як контроль доступу у формі послуги послуга. Він застосовує технологію «Програмне забезпечення як послугу» (SaaS) і, таким чином, є хмарним. Поки все обладнання для контролю доступу залишається на місці, програмне

забезпечення та сервери видаляються з приміщень компанії і зберігаються в потужних віддалених центрах обробки даних (рис.1.3).

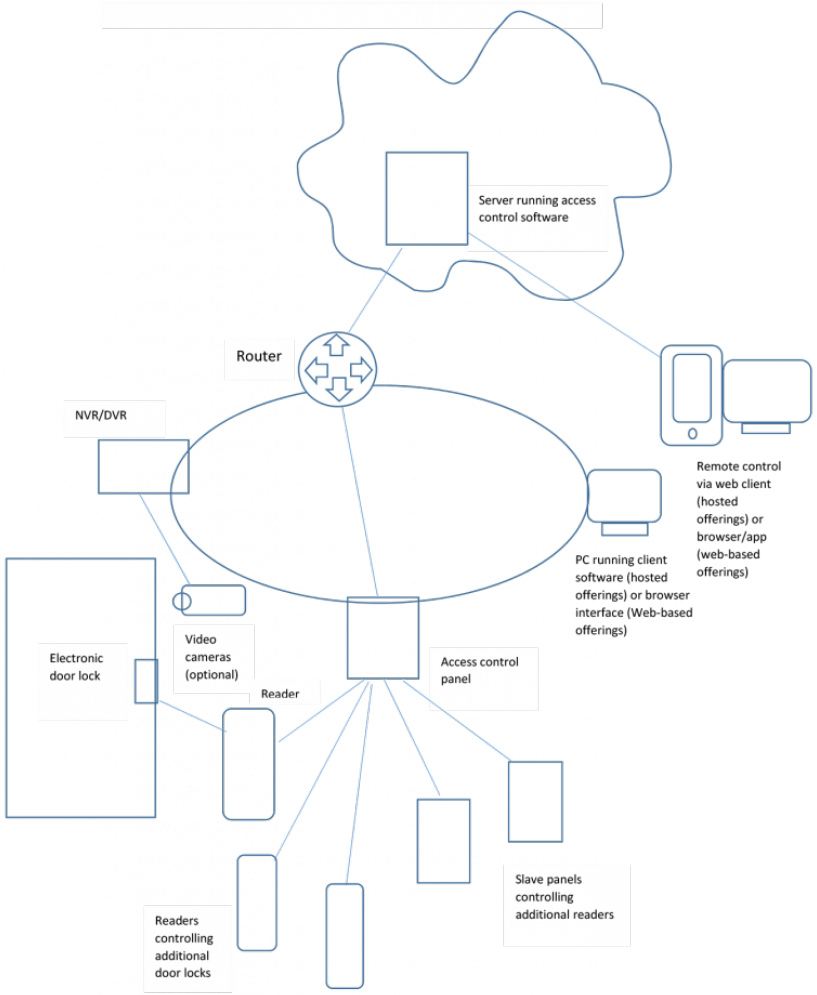

Рисунок 1.3 – Приклад інтегрованого контролю доступу як послуги

У порівнянні з традиційним контролем доступу, “контроль доступу як послуга” має ряд переваг:

1. Через те, що вся інформація зберігається на віддалених серверах, то немає необхідності встановлювати сервер в установі безпосередньо.
2. Є можливість управляти контролем доступу з будь-якого куточка світу, якщо є доступ до Інтернету.
3. Інформація, отримана з усіх об'єктів та всіх філій, зберігається в одному місці, і надається цілодобовий доступ до цієї інформації.
4. Доступність системи цілодобово підтримується технічним персоналом, і навряд чи який-небудь малий бізнес може похвалитися

цілодобовим присутністю підтримки на місці в разі традиційного контролю доступу.

5. Реалізація хмарної безпеки як послуги, дозволяє за необхідності змінювати конфігурацію контролю доступу - можна додати більше дверей, призначити власникам карт різні рівні доступу без необхідності заміни обладнання або придбання додаткового програмного забезпечення.
6. AcaaS використовує безпечне шифрування, і отже не потрібно турбуватись про злам СКУД.
7. Деякі AcaaS практично не потребують апаратного забезпечення. Співробітники отримують доступ до певних об'єктів, скачавши лише мобільний додаток. Завдяки мобільним обліковим даним, які відправляють сигнал контролеру двері, співробітники можуть увійти в офіс, в який їм дозволено.
8. Контроль доступу як послуга дозволяє отримати і включити комплексну безпеку як послугу. Тобто при цьому можна інтегрувати і систему сигналізації, відеоспостереження, виявлення вторгнень, тощо.

1.4 Sim-Cloud

Розвиток Інтернету речей в даний час є одним з пріоритетних напрямків технологічного розвитку. Адже в процес створення IoT-систем залучено безліч стартапів, інтеграторів, розробників програмного забезпечення.

Речі, об'єкти Інтернету речей, і окремі модулі, що зареєстровані в системі, пов'язані спільним алгоритмом роботи і мають доступ в Інтернет. Завдання логічного об'єднання їх в мережу в хмарі вирішується в SIM-Cloud з урахуванням індивідуальних умов кожного проекту.

Інтернет речей - це не те ж саме, що автоматизація. Він відрізняється як способом зв'язку через Інтернет по протоколу IP, так і реалізацією SIM-Cloud

обробки інформації, зібраної з периферійних модулів, передачі результатів цієї аналітики користувачам, розробки рекомендацій та прогнозів на їх основі.

Як правило, речі підключаються до SIM-Cloud IaaS через шлюз, який накопичує метрики від самих різних мережевих пристроїв IoT, що використовують різні протоколи передачі даних - Bluetooth, WiFi, MQTT, CoAP, DDS, NFC, Cellular, AMQP, RFID, Z-Wave , HTTPs, Rest API, ZigBee, тощо (рис.1.4).

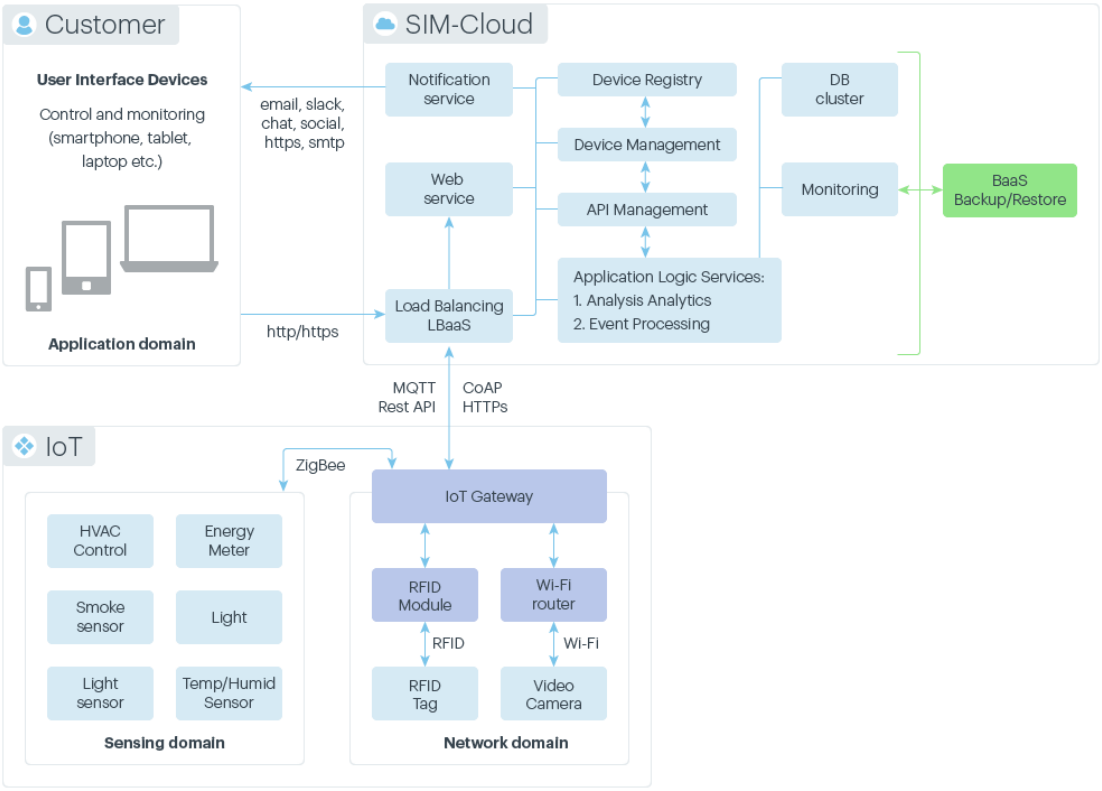

Рисунок 1.4 – Схема проекту IoT в SIM-Cloud

Якщо інтернет-з'єднання переривається на короткий час, модулі IoT продовжують працювати автономно. Після відновлення підключення до системи пристрої передають оновлену інформацію про свій стан в “хмарне” середовище. При цьому всі дані синхронізуються і оновлюються в базі даних.

Хмарна реалізація рішення для системи Інтернету речей забезпечує більш надійний захист від кібератак, які вводять шкідливий код безпосередньо в оперативну пам'ять сервера [7-9]. Кластерна організація хмарної IaaS і

масштабування ресурсів за запитом підвищують ефективність захисних заходів, дозволяючи підключати високопродуктивні обчислювальні технології для виявлення процесів, які виявляють «підозрілу поведінку» - надмірний трафік, несанкціонований доступ до ресурсів, в тому числі через Інтернет, тощо.

Висновки до розділу 1.

СКУД - це механізм відстеження входу і виходу в приміщення відвідувачів за допомогою ідентифікаторів. Основні складові системи: загороджуючий пристрій (турнікет), ідентифікатор, зчитувач і контролер. Залежно від комплектуючих і діапазону функцій, системи діляться на три групи: автономні, мережні і біометричні. В системах безпеки доцільно поєднувати ці три групи, що підвищує рівень контролю доступу в приміщення.

2 ОСОБЛИВОСТІ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Технологія LoRAWAN

Створення систем безпеки об’єктів з залученням підходів, алгоритмів та ідей технологій Інетрнету речей вимагає від розробників враховувати при розробці певні технічні особливості останніх. Найбільш поширеною технологією, на основі якої функціонують різні “розумні” пристрої є на сьогодні технологія LoRaWAN. Розглянемо далі певні особливості цієї технології у розрізі IoT [3].

LoRaWAN - це фактично мережний протокол багато крапкового зв'язку, в якому використовується схема модуляції LoRa від компанії Semtech. Справа не тільки в радіохвилях; мова йде про те, як радіохвилі зв'язуються зі шлюзами LoRaWAN, щоб робити такі речі, як шифрування і ідентифікація. Він також включає хмарний компонент, до якого підключаються кілька шлюзів. На самому фундаментальному рівні протоколи радіозв'язку, такі як LoRaWAN, досить прості. Ось як це виглядає на практиці. Припустимо, у вас чотири шлюзи і один вузол. Вузол передає дані в радіочастотний спектр наосліп, і будь-який шлюз, якому пощастить почути передачу, може прийняти її і відправити в хмару. Можливо, що всі чотири шлюзи почують це повідомлення і відправлять його. Після того, як повідомлення доставлено, немає підтвердження отримання. Однак вузли в LoRaWAN можуть і запитувати підтвердження. Проблема полягає в наступному: коли цей шлюз передає назад на вузол, він перестає “слухати” все інше.

На рисунку 2.1 показано, як працює LoRaWAN. Верхня смуга вказує, передає шлюз чи ні. Якщо помаранчевий, значить, йде передача; якщо синій, то ні. Смуга внизу показує канали приймача. Майже всі системи LPWAN, включаючи LoRaWAN, мають кілька каналів прийому, і більшість систем LoRaWAN можуть приймати вісім повідомлень одночасно по будь-якій кількості частотних каналів.

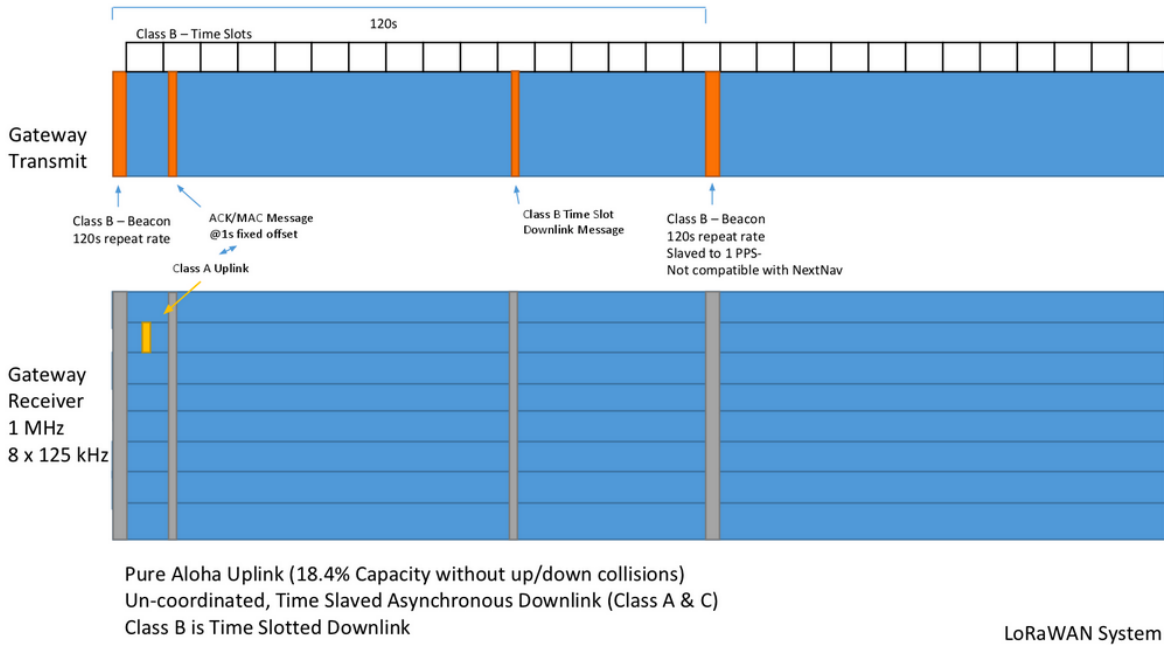

Рисунок 2.1 – Принцип функціонування LoRaWAN

LoRaWAN має три класи, які працюють одночасно. Клас А є чисто асинхронним, і це те, що називається “чистою” системою ALOHA. Це означає, що кінцеві вузли не чекають певного часу, щоб поговорити зі шлюзом - вони просто передають дані, коли їм потрібно, і до тих пір залишаються в режимі спокою. Якщо у вас є ідеально скоординована система з вісьмома каналами, ви можете заповнити кожен часовий інтервал повідомленням. Як тільки один вузол завершує передачу, негайно запускається інший. Без будь-яких перерв у комунікації теоретична максимальна ємність чистою мережі ALOHA становить близько 18,4% від цього максимуму. Це відбувається в основному через колізії, через те що, якщо один вузол передає, а інший прокидається і вирішує передавати на тому ж частотному каналі з тими ж налаштуваннями радіозв'язку, вони зіткнуться, тобто відбудеться колізія.

Клас В дозволяє відправляти повідомлення на вузли з автономними джерелами живлення. Кожні 128 секунд шлюз передає мітку. Всім вузлам класу В призначається часовий інтервал в межах 128-секундного циклу, і їм повідомляється, коли слід слухати. Ви можете, наприклад, сказати вузлу, щоб він слухав кожен десятий часовий інтервал, і коли він з'являється, він дозволяє передавати повідомлення спадного каналу.

Клас С дозволяє вузлам постійно слухати, і повідомлення спадного каналу може бути відправлено у будь-який час. Це використовується в основному для додатків з живленням від змінного струму, тому що потрібно багато енергії, для того щоб підтримувати активну роботу вузла при постійному включенні приймача.

LoRaWAN - це асинхронний протокол на основі ALOHA, в якому часто зустрічаються помилки пакетів (PER), що перевищують 50 відсотків. Це нормально для деяких додатків для зчитування показань лічильників, але для промислових або корпоративних сенсорних мереж або систем управління потрібно забезпечити 0 відсотків PER.

Більшість розробників вирішують цю проблему, вибираючи найменший доступний MTU при найвищому коефіцієнті розширення, який може призначити мережу, і який в більшості випадків дуже малий, часто менш 12 байт. Таким чином, вузли LoRaWAN, яким необхідно відправляти великі обсяги даних, наприклад 300 байт, повинні будуть відправляти їх в 30 10-байтових повідомленнях, тому що вони можуть зіткнутися з ситуацією, коли їм призначається невеликий MTU. В результаті ці вузли передають набагато більше, ніж необхідно, через складні змін програмного забезпечення, які будуть потрібні для обробки цих змінюються значень MTU.

2.2 Технологія M2M

Машина-машина, або M2M [10], - це широке позначення, яке можна використовувати для опису будь-якої технології, що дозволяє мережевим пристроям обмінюватися інформацією і виконувати дії без ручної допомоги людини. Технологія M2M була вперше застосована на виробництві та в промислових умовах, де інші технології, такі як SCADA і віддалений моніторинг, допомогли дистанційно керувати даними з обладнання і контролювати їх. З тих пір M2M знайшов застосування в інших секторах, таких

як охорона здоров'я, бізнес і страхування. M2M також є основою Інтернету речей (IoT).

Системи межмашинної взаємодії стикаються з рядом проблем безпеки, від несанкціонованого доступу до бездротового вторгнення і злому пристроїв. Також необхідно враховувати фізичну безпеку, конфіденційність, шахрайство і розкриття критично важливих додатків.

Типові заходи безпеки M2M включають в себе, серед іншого, захист пристроїв і машин від несанкціонованого доступу, врпровадження засобів захисту в машини, забезпечення безпеки зв'язку за допомогою шифрування і захисту внутрішніх серверів. Сегментація пристроїв M2M в їх власній мережі та управління ідентифікацією пристроїв, конфіденційністю даних і доступністю пристроїв також може допомогти в боротьбі з ризиками безпеки M2M.

2.2.1 Принцип роботи M2M

Основна мета міжмашинної технології - підключення до даних датчиків і передавання їх в мережу. На відміну від SCADA або інших інструментів віддаленого моніторингу, системи M2M часто використовують загальнодоступні мережі і методи доступу, наприклад стільниковий зв'язок або Ethernet, щоб зробити їх більш рентабельними.

Основні компоненти системи M2M можуть включати датчики, RFID, Wi-Fi або стільниковий зв'язок, а також програмне забезпечення для автономних обчислень. Одним з найбільш відомих типів межмашинної взаємодії є телеметрія, яка використовувалася з початку минулого століття для передавання робочих даних.

Крім можливості віддаленого моніторингу обладнання та систем, основні переваги M2M включають:

- зниження витрат за рахунок мінімізації технічного обслуговування і простоїв обладнання;

- збільшення доходів за рахунок відкриття нових бізнес-можливостей для обслуговування продуктів на місцях; а також;
- покращене обслуговування клієнтів за рахунок активного моніторингу та обслуговування обладнання до його виходу з ладу або тільки тоді, коли це необхідно.

2.2.2 Додатки та приклади M2M

Міжмашинна взаємодія часто використовується для віддаленого моніторингу. При поповненні запасів, наприклад, торговий автомат може повідомити в мережу або автомат дистриб'ютора, коли конкретний товар закінчується, щоб відправити поповнення запасів. Забезпечуючи відстеження та моніторинг активів, M2M життєво важливий в системах управління складом (WMS) і управління ланцюгами поставок (SCM).

Системи розумного будинку також включають технологію M2M. Використання M2M в цій вбудованій системі дозволяє побутовій техніці контролювати операції в режимі реального часу, а також мати можливість віддаленого спілкування.

M2M також є важливим аспектом програмного забезпечення для дистанційного керування, робототехніки, управління рухом, безпеки, логістики, управління автопарком і автомобілебудуванням.

Відповідно до Європейського інституту телекомунікаційних стандартів (ETSI), вимоги до системи M2M включають:

- масштабованість - система M2M повинна мати можливість продовжувати працювати ефективно в міру додавання більшої кількості зв'язаних об'єктів;
- анонімність - система M2M повинна мати можливість приховувати особистість пристрої M2M за запитом відповідно до нормативних вимог;

- ведення журналу - системи M2M повинні підтримувати запис важливих подій, таких як невдалі спроби установки, непрацююча служба або поява помилкової інформації. Журнали повинні бути доступні за запитом;
- принципи взаємодії додатків M2M - системи M2M повинні забезпечувати зв'язок між додатками M2M в мережі і пристроєм або шлюзом M2M з використанням таких методів зв'язку, як служба коротких повідомлень (SMS), і пристрої, підключені до IP, також повинні мати можливість зв'язуватися один з одним;
- методи доставки - система M2M повинна підтримувати одноадресні, багатоадресні і широкомовні режими зв'язку, і при цьому широкомовна передача по можливості замінюється багатоадресною для мінімізації навантаження на мережу зв'язку;
- планування передачі повідомлень - системи M2M повинні мати можливість контролювати доступ до мережі і розкладу обміну повідомленнями, а також враховувати допустиму затримку планування додатків M2M;

2.2.3 Порівняння M2M та IoT

Хоча багато хто використовує ці терміни як синоніми, M2M і IoT−це не одне і те ж. IoT потребує M2M, але M2M не потребує IoT. Обидва терміни відносяться до зв'язку підключених пристроїв, але системи M2M часто являють собою ізольоване, автономне мережеве обладнання. Системи IoT виводять M2M на новий рівень, об'єднуючи розрізнені системи в одну велику взаємопов'язану екосистему.

Системи M2M використовують двоточковий зв'язок між машинами, датчиками і устаткуванням по стільниковим або провідним мережам, у той час як системи IoT покладаються на мережі на основі IP для відправлення даних,

зібраних з пристроїв, підключених до IoT, на шлюзи, хмарні платформи або платформи проміжного програмного забезпечення.

Дані, зібрані з пристроїв M2M, використовуються додатками для управління послугами, тоді як дані Інтернету речей часто інтегруються з корпоративними системами для підвищення ефективності бізнесу в декількох групах.

2.3 Cloud-сервіси

Термін «хмарні послуги» відноситься до широкого спектру послуг, що надаються за запитом компаніям і клієнтам через Інтернет. Ці служби призначені для забезпечення простого і доступного доступу до додатків і ресурсів без необхідності у внутрішній інфраструктурі або обладнанні. Від перевірки електронної пошти до спільної роботи над документами - більшість співробітників використовують хмарні сервіси протягом робочого дня, незалежно від того, усвідомлюють вони це чи ні. Хмарні сервіси повністю управляються постачальниками хмарних обчислень і постачальниками послуг. Вони надаються клієнтам з серверів постачальників, тому компанії не потрібно розміщувати додатки на своїх власних локальних серверах. Розрізняють три основних типи хмарних сервісів [3,4]:

- Програмне забезпечення як послуга (SaaS). Найбільш широко відомий тип хмарної служби і відомий як «програмне забезпечення як послуга» або SaaS (див. п.1.3). В цю велику категорію входять різні послуги, такі як зберігання і резервне копіювання файлів, електронна пошта в Інтернеті і інструменти управління проектами. Приклади постачальників хмарних послуг SaaS включають Dropbox, G Suite, Microsoft Office 365, Slack і Citrix Content Collaboration. У кожному з цих додатків користувачі можуть отримувати доступ, спільно використовувати, зберігати і захищати інформацію в «хмарі».

- Інфраструктура як послуга (IaaS). Інфраструктура як послуга, або IaaS, надає інфраструктуру, яка потрібна багатьом постачальникам хмарних послуг для управління інструментами SaaS. Він служить повноцінною структурою центру обробки даних, усуваючи необхідність в ресурсномістких установках на місці. Прикладами IaaS є Amazon Web Services (AWS), Microsoft Azure і Google Compute Engine. Ці постачальники обслуговують всі сервери зберігання та мережеве обладнання, а також можуть запропонувати балансування навантаження, брандмауери додатків і багато іншого. Багато відомих постачальники SaaS працюють на платформах IaaS.
- Платформа як послуга (PaaS). Модель хмарного сервісу, відома як платформа як сервіс, або PaaS, служить веб-середовищем, в якій розробники можуть створювати хмарні додатки. PaaS надає базу даних, операційну систему і мова програмування, які організації можуть використовувати для розробки хмарного програмного забезпечення без необхідності обслуговування базових елементів. Багато постачальників IaaS, включаючи приклади, перераховані вище, також пропонують можливості PaaS.

Приймаючи рішення про те, як використовувати хмарні сервіси, організації також повинні вирішити, який тип середовища найкраще підходить для бізнесу: загальнодоступна “хмарна” платформа, приватне “хмарне” середовище або поєднання того й іншого.

Послуги, які постачальник надає численним клієнтам через Інтернет, називаються загальнодоступними хмарними послугами. Наведені вище приклади SaaS, IaaS і PaaS надають загальнодоступні хмарні сервіси. Найбільшою перевагою використання загальнодоступних хмарних сервісів є можливість масштабного спільного використання ресурсів, що дозволяє організаціям пропонувати співробітникам більше можливостей, ніж це було б можливо в поодинці.

Оскільки доступність хмарних сервісів продовжує розширюватися, їх застосування в корпоративному світі також будуть зростати. Незалежно від того, чи вирішить компанія розширити існуючі локальні розгортання програмного забезпечення або повністю перейти в хмару, ці послуги будуть і далі спрощувати доставку критично важливих додатків і даних співробітникам. Від спільної роботи з контентом і управління доступом для співробітників до управління доставкою програм і рішень віртуальних робочих столів для IT, а також з широким набором проміжних варіантів, хмарні сервіси змінюють те, як люди працюють, і то, як працюють компанії.

2.4 Архітектура IoT

Інтернет речей (IoT) визначається як “парадигма”, в якій об'єкти, що обладнанні датчиками, виконавчими механізмами і процесорами, взаємодіють один з одним для досягнення певної мети [7].

Датчики та виконавчі механізми - це пристрої, які допомагають взаємодіяти з фізичним середовищем. Дані, зібрані датчиками, повинні зберігатися і оброблятися “розумно”. Зберігання та обробка даних можуть виконуватися на кордоні самої мережі або на віддаленому сервері. Якщо можлива будь-яка попередня обробка даних, то вона зазвичай виконується або на датчику, або на іншому найближчому пристрої. Потім оброблені дані зазвичай відправляються на віддалений сервер. Можливості зберігання і обробки об'єкта IoT також обмежені доступними ресурсами, які часто дуже обмежені через обмеження розміру, енергії, потужності і обчислювальних можливостей. Крім проблем зі збором і обробкою даних, існують проблеми і з комунікацією. Зв'язок між пристроями IoT в основному бездротовий, оскільки вони зазвичай встановлюються в географічно віддалених місцях. Бездротові канали часто мають високий рівень спотворень і ненадійні. У цьому сценарії надійна передача даних без занадто великої кількості повторних передач є

важливою проблемою, і, отже, комунікаційні технології є невід'ємною частиною вивчення механізмів IoT.

Датчики, виконавчі механізми, обчислювальні сервери і мережу зв'язку утворюють базову інфраструктуру Інтернету речей. Однак є багато аспектів програмного забезпечення, які необхідно враховувати. По-перше, нам потрібно проміжне програмне забезпечення, яке можна використовувати для підключення і управління всіма цими різнорідними компонентами. Для підключення безлічі різних пристроїв нам потрібна велика стандартизація.

2.4.1 Архітектури на основі “хмар” та “туману”

У деяких системних архітектурах обробка даних виконується централізовано за допомогою “хмарних” комп'ютерів. У такій архітектурі, орієнтованої на “хмару”, “хмара” знаходиться в центрі, додатки - над ним, а мережа інтелектуальних пристроїв - під ним. Хмарним обчисленням надається пріоритет, оскільки вони забезпечують більшу гнучкість і масштабованість. Розробники можуть надавати свої інструменти зберігання, програмні інструменти, інструменти інтелектуального аналізу даних і машинного навчання, а також інструменти візуалізації через хмару [7].

Останнім часом спостерігається перехід до іншої системної архітектурі, а саме до туманним обчислень, де датчики і мережеві шлюзи виконують частину обробки даних. Архітектура “туману” представляє собою багаторівневий підхід, який встановлює рівні моніторингу, попередньої обробки, зберігання та безпеки між фізичним і транспортним рівнями. Рівень моніторингу відслідковує потужність, ресурси, відповіді та послуги. Рівень попередньої обробки виконує фільтрацію, обробку даних датчиків. Рівень тимчасового зберігання забезпечує такі функції зберігання, як реплікація, поширення та зберігання даних. Нарешті, рівень безпеки виконує шифрування / дешифрування і забезпечує цілісність і конфіденційність даних. Моніторинг і

попередня обробка виконуються на кордоні мережі перед відправкою даних в хмару.

Часто терміни «туманні обчислення» і «периферійні обчислення» використовуються як синоніми. Останній термін передує першому і вважається більш загальним. Під “туманними” обчисленнями, спочатку названими Cisco, розуміються інтелектуальні шлюзи і інтелектуальні датчики, тоді як периферійні обчислення за своєю природою дещо інші. Ця парадигма передбачає додавання інтелектуальних можливостей до попередньої обробки даних з фізичних пристроїв, таких як, наприклад, двигуни, насоси або ліхтарі.

Більшість архітектур, пропонованих для SIoT, мають архітектуру на стороні сервера. Сервер підключається до всіх взаємопов'язаним компонентів, агрегує (становлює) служби і діє як єдина точка обслуговування для користувачів.

Архітектура на стороні сервера зазвичай складається з трьох рівнів. Перший - це базовий рівень, що містить базу даних, в якій зберігаються відомості про всі пристрої, їх атрибути, метаінформацію та їхні відносини за обміном інформацією. Другий рівень (рівень компонентів) містить код для взаємодії з пристроями, запиту їх статусу і використання їх підмножини для надання послуги. Самий верхній рівень - це рівень додатків, який надає користувачам послуги.

Висновки до розділу 2

Системи міжмашинної взаємодії стикаються з рядом проблем безпеки, від несанкціонованого доступу до бездротового вторгнення і злому пристроїв. Також необхідно враховувати фізичну безпеку, конфіденційність, шахрайство і розкриття критично важливих додатків.

Типові заходи безпеки M2M включають в себе, серед іншого, захист пристроїв і машин від несанкціонованого доступу, вбудовування засобів захисту в машини, забезпечення безпеки зв'язку за допомогою шифрування і захисту внутрішніх серверів. Сегментування пристроїв M2M в їх власній

мережі та управління ідентифікацією пристроїв, конфіденційністю даних і доступністю пристроїв також може допомогти в боротьбі з ризиками безпеки M2M.

3 ТЕХНІЧНІ ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ СИСТЕМИ ОХОРОНИ ОБ'ЄКТА НА ОСНОВІ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

В якості об'єкту, який необхідно обладнати системою безпеки з підвищеним рівнем надійності було обрано районне відділення банку "Credit Agricole" в місті Києві загальною площею 380 м^2. При цьому слід зауважити, що за вимогою замовника необхідно все приміщення поділити на 2 зони – кімната загального облсговування клієнтів банку (велика зала типу фойє відділення банку), та певні кімнати (VIP-приміщення), де передбачаються операції фінансового плану і де зберігаються певні матеріальні цінності як клієнтів банку так і самого банку (грошові цінності, дорогоцінні метали, тощо). Поруч з наявним сейфом в цих кімнатах за завданням замовника необхідно обладнати ці приміщення з підвищеним рівнем безпеки. Визначення технічних особливостей проектування такої системи побудуємо окремо за розглядом складових на основі наступного складу: система відеонагляду, система контрою та управління доступом, система фіксації руху, система сигналізації. Поруч з цим визначимо, що система освітлення в цих приміщеннях теж має основи технології Інтернету речей. Тобто, системи освітлення в кімнатах відділення можуть управлятись як механічно, так і на основі панелі управління, яка підключена до загального серверу безпеки.

3.1 Вихідні дані до проектування

Передбачається що площа відділення банку, окрім зазначених видів приміщень буде мати ще і дві технічні апаратні, де поруч з елементами моніторингу камер систем знаходиться обладнання, функціонування якої відповідає технології LoRAWAN, а також наявні елементи, які стсоуються безпроводової системи сигналізації фірми Ajax.

За умовою від замовника необхідно забезпечити повний комплекс безпеки в основній залі відділення і передбачити підвищений рівень безпеки

(створення гібридної системи безпеки на основі використання технології Інтернету речей) у трьох VIP-кімнатах відділення банку. Загальний план будівлі банку, де показано вже розгорнуту системи освітлення (блок живлення не показано, адже щит електроживлення виведено за межі наведеного плану) наведено на рисунку 3.1.

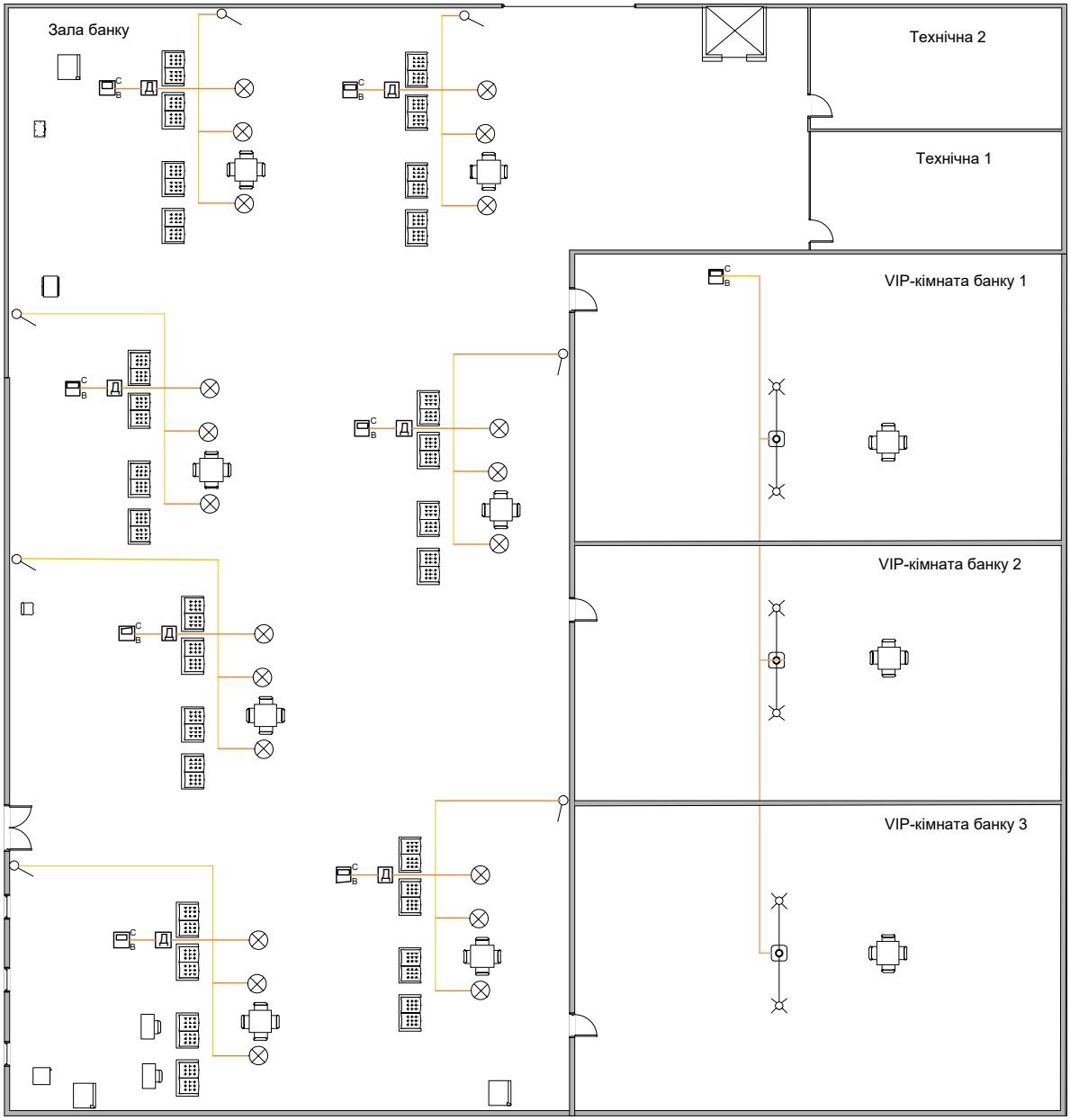

Рисунок 3.1 – План приміщення до розміщення устаткування

Система освітлення поділена на два типи – освітення за областю і освітлення загальне для VIP-кімнат. Кожне приміщення має двері, а просторова

зала має ще і вікна. Окремо показано ліфт та аксесуари меблів. Зазначимо що в комплексі аріхтектрної будівлі для входу в основну залу є ще двобічні двері.

З рисунку 3.1 варто відмітити, що світильники, які розташовані у великій залі відділення банку підключені до джерела живлення і керуються на основі драйвера та контролера освітлення (електронний діммер). Схематично це показано на рисунку 3.2.

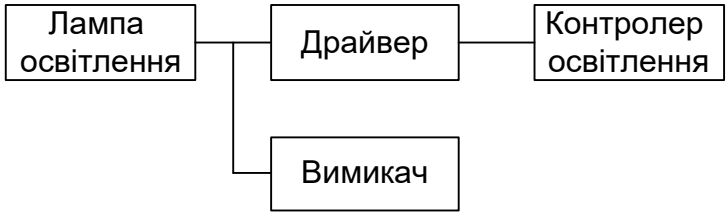

Рисунок 3.2 – Схема підключення ламп освітлення в залі відділення (блок живлення не показано)

Додатково для частини освітлення показано механічні вимикачі, які за роводкою електричних ліній виведено у бік архітектурного каркасу будівлі.

3.2 Система відеонагляду

За конструктивними особливостями визначимо наступні види камер відеоспостереження, які використаємо при проектуванні:

- поворотні (PTZ) - призначені для спостереження за великими територіями і об'єктами, що рухаються, забезпечені поворотним механізмом за рахунок чого функціонал їх застосування досить різноманітний;
- купольні - мають півсферичний (куполоподібний) корпус, який вміщує в себе швидкісний поворотний пристрій, саму камеру з трансфокатором, а також приймачем телеметрії, завдяки широкому куту огляду і високій швидкості роботи дозволяють отримувати якісну панорамну картинку для ведення спостереження за великою територією і динамічними об'єктами ;

Найбільш оптимальним рішенням за параметрами ціна / якість є камери виробництва компанії Axis. В наборі купольних можна використати камери Axis M3004-V (рис.3.3).

Рисунок 3.3 – Axis M3004-V

Основні технічні характеристики камери Axis M3004-V:

- тип корпусу - купольна (DOME);
- тип матриці - CMOS; - розмір матриці – 1/4";
- загальна кількість пікселів, 1 Мп;
- максимальна роздільність зображення - 1280×800;
- 30 кадрів в секунду при максимальній роздільній здатності
- мінімальне освітлення - 1.5 люкс;
- фокусна відстань об'єктива, мм - 2.8;
- горизонтальний кут огляду - 80º;
- підтримка відеокодеків - H.264, Motion JPEG;
- детекція руху - аналіз змін в кадрі;
- роз'єми 10BASE-T / 100BASE-TX;
- підтримка мережевих протоколів IPv4 / v6, TCP, HTTP, HTTPS, UpnP, RTSP, RTP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, SNMP, ICMP, UDP, ARP, Bonjour, QoS;

В якості PTZ-камери для осистеми охорони в будівлі можна обрати камеру Axis M5014-V (див. рисунок 3.4).

Рисунок 3.4 – Axis M5014-V

Основні технічні характеристики цієї камери наступні:

- тип корпусу - купольна (DOME);
- тип матриці - CMOS;
- тип розгортки - прогресивна;
- розмір матриці - 1/4 ";
- загальна кількість пікселів - 1МП;
- максимальна роздільність зображення - 1280×720;
- максимальна кількість кадрів в секунду - 30;
- мінімальне освітлення - 1.4лк;
- тип об'єктива - фіксований;
- фокусна відстань об'єктива - 3.6 мм;
- горизонтальний кут огляду - 60 °;
- 3-х кратний цифровий зум;
- підтримка відеокодеків - H.264, Motion JPEG;
- автоекспозиція;
- роз'єми 10BASE-T / 100BASE-TX;
- підтримка мережевих протоколів IPv4 / v6, TCP, HTTP, HTTPS, UpnP, RTSP, RTP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, SNMP, ICMP, UDP, ARP, Bonjour, QoS;
- кут повороту 0 - 360 °;
- кут нахилу 0 - 90 °;

- тип монтажу - в підвісну стелю;

Таким чином, систему відеонагляду для заданого об’єкту можна визначити за особливостями розташування звичайних купольних камер та PTZ-камер. Визначимо, що звичайні камери з підтримкою та управлінням за IP-протоколом (живлення подається на основі технології Power Over Ethernet) будуть встановлені в двох технічних приміщеннях системи безпеки, а також нехай ці камери встановлені у трьох VIP-кімнатах. При цьому в кожній такій окремій VIP-кімнаті розташуємо по дві таких камер. Всього таких камер при створенні системи використано у кількості 8 одиниць. При цьому на схемі PoE-адаптер не показано, адже вважається, що цей адаптер вже використано при підключенні даної камери до мережі Ethernet. Схема підключення камери з підтримкою технології PoE наведено на рисунку 3.5.

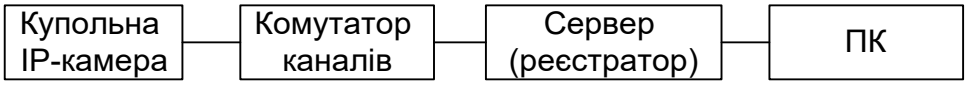

Рисунок 3.5 – Схема підключення купольної камери

PTZ-камери обраної моделі розташуємо теж у кількості 8 одиниць в основній залі відділення банку. Такий вибір при проектуванні обумовлено тим, що IP-камера Axis M5014-V забезпечена поворотним механізмом за рахунок чого функціонал їх застосування, насамперед через реальний кут огляд, досить різноманітний. Схема підключення цієї камери наведено на рисунку 3.6. В якості комутатора каналів для комутації камер відеоспостереження візьмемо Cisco WS-C2960X-24PSQ-L.

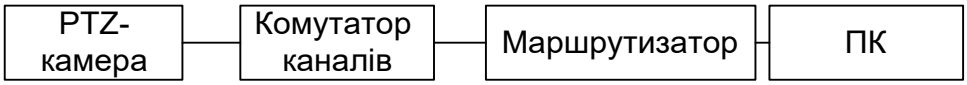

Рисунок 3.5 – Схема підключення PTZ-камери з підтримкою IP-протоколу

Реєстратор (рис.3.5) функціонує за наступним принципом: камери за логікою підключаються і передають відеозображення по лініях зв'язку. Реєстратор отримує відеотрафік, перетворює його в зображення, конвертує в необхідний формат, і, при необхідності, записує на пристрій зберігання.

Для системи безпеки можна використати реєстратор AXIS Camera Station S1048 Mk II Recorder. Цей реєстратор дозволяє підключати до 64 камер і має мність для зберігання інформації об’ємом до 24 ТБ.

Задля підвищення надійності системи безпеки запровадимо на основі технології IoT у VIP-кімнатах додаткові безпроводові камери, які мають у своєму складі Wi-Fi-модуль і підтримують взаємодію з пристроями на основі технології LoRAWAN. В якості такої камери візьмемо модель HIPER IoT Cam M2 (рис.3.6).

Рисунок 3.5 – Камера HIPER IoT Cam M2

Таких камер в системі безпеки розташуємо по 4 одиниці в кожній VIP-кімнаті. Схема підключення такої камери наведена на рисунку 3.6.

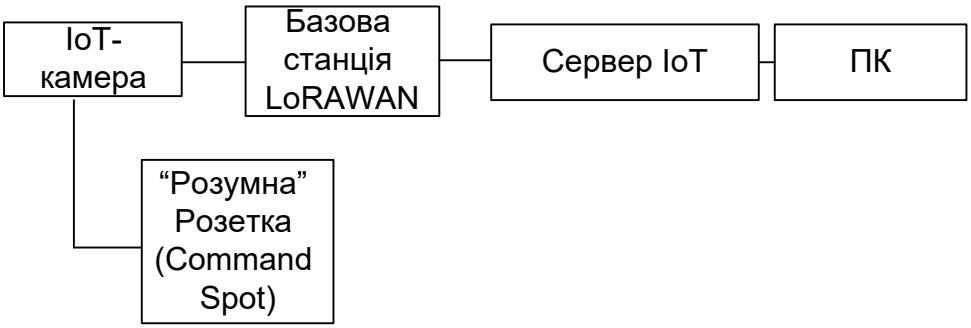

Рисунок 3.5 – Схема підключення “розумної” камери

Варто відмітити, що таке технічне рішення обумовлено тим, що гібридна система відеонагляду дозволяє підвищити загальну надійність, адже в даному випадку інформація яка зуміється з звичайної купольної камери буде резервуватись даними, які отримує системи від безпроводової камери.

3.3 Система контролю та упраління доступом та система сигналізації

Через те, що наведена площа для безпеки за периметром має особливості охорони, то необхідно забезпечити контроль та ідентифікацію осіб, які потрапляють у відділення банківської установи.

Для контролю доступу застосовано панель для зчитування карт Hikvision DS-K1101M. З внутрішньої сторони для відкриття дверей встановлено кнопку відкриття електронних замків ART-801A. Панель Hikvision DS-K1101M зображено на рис. 3.6.

Рисунок 3.6 – Панель для зчитування карт доступу Hikvision DS-K1102M

Кнопка відкриття електронних замків ART-801LED зображена на рис. 3.7.

Рисунок 3.7 – Кнопка відкриття електронних замків ART- 801LED

Для забезпечення фіксованого закриття дверей обрано електромагнітний замок TECSAR TREK EL-60 з напругою живлення 12 В. Електромагнітний замок TECSAR TREK EL-60 зображено на рис. 3.8.

Рисунок 3.8 – Електромагнітний замок TECSAR TREK EL-60

Система контролю доступу як і система відеонагляду теж доцільно зробити багаторівневою. Тобто, доступ до приміщення організуємо не лише на основі електромагнітного замка та кнопки, але й з використання карт доступу (рис.3.9).

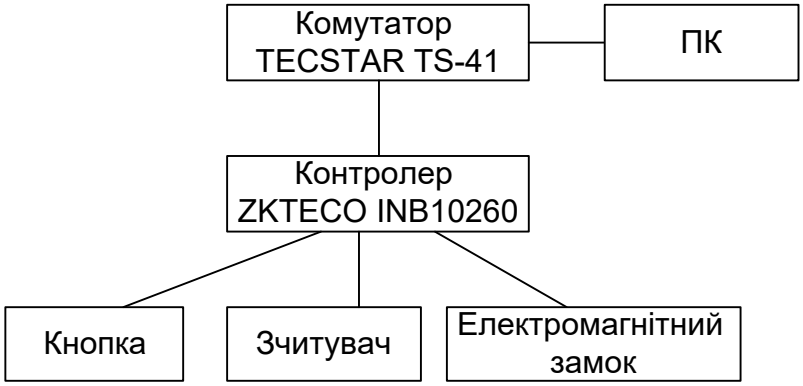

Рисунок 3.9 – Схема підключення СКУД (базовий варіант)

Крім цього, як елемент сигналізації на кожні двері і вікна встановимо датчики відкриття двері/вікна Ajax DOORPROTECT PLUS. Серед характеристик AJAX DOORPROTECT PLUS варто відзначити наступні: тип датчика – безпроводовий; поріг спрацьовування - 2 см; дальність передачі безпроводового сигналу - 2000 м; робочий діапазон частот - 868 або 915 МГц в залежності від місця розташування; потужність радіопередавача датчиків - 20 мВт; тип елемента живлення - батарея типу CR123A; термін роботи датчика від одного елемента живлення - до 7 років; робоча напруга - 3 В.

В якості датчиків руху візьмемо в усіх приміщеннях банківської установи інфрачервоний датчик руху AJAX COMBIPROTECT. Серед характеристик даного пристрою варто відзначити наступні: тип датчика – безпроводовий; тип сенсора руху – піросенсор; діяльність визначення руху – 12 метрів; горизонтальний кут детектування – 88,5 °; вертикальний кут детектування – 80 °; висота інсталяції – 2,4 м; захист від злому – є; частота передачі – 868 або 915 МГц в залежності від місця розташування; дальність зв'язку – 2000 м; потужність радіопередавача датчиків – 20 мВт; робоча напруга – 3 В. На основі аналізу площ виділення виберемо 10 датчиків з розрахунку на активну область кімнати. Дані датчики на основі системи зв’язку Jeweller підключаються до інтелектувальної централі Ajax Hub яка розташована в технічному приміщенні системи безпеки. В області входу у VIP-кімнати запроваджено задля підвищення безпеки та контролю, інтелектувальну систему на основі технічного рішення компанії Vega Smart. За цією схемою використовуються зчитувачі як за картою так і за сенсором дотику. Крім цього, є підтримка технології LoRAWAN. Схема підключення показана на рис.3.10.

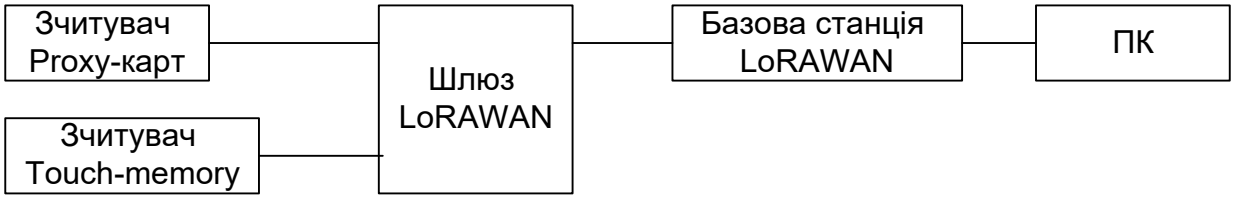

Рисунок 3.10 – Схема СКУД на основі технології IoT

У підсумку проведений вибір обладнання, аналіз основних схем підключення компонентів системи безпеки банківського відділенні дозволяє нам звести усі розглянуті складові в рамках комплексного технічного рішення зі створення системи безпеки обраного об’єкту. План-схема отриманих результатів показана на рис.3.11.

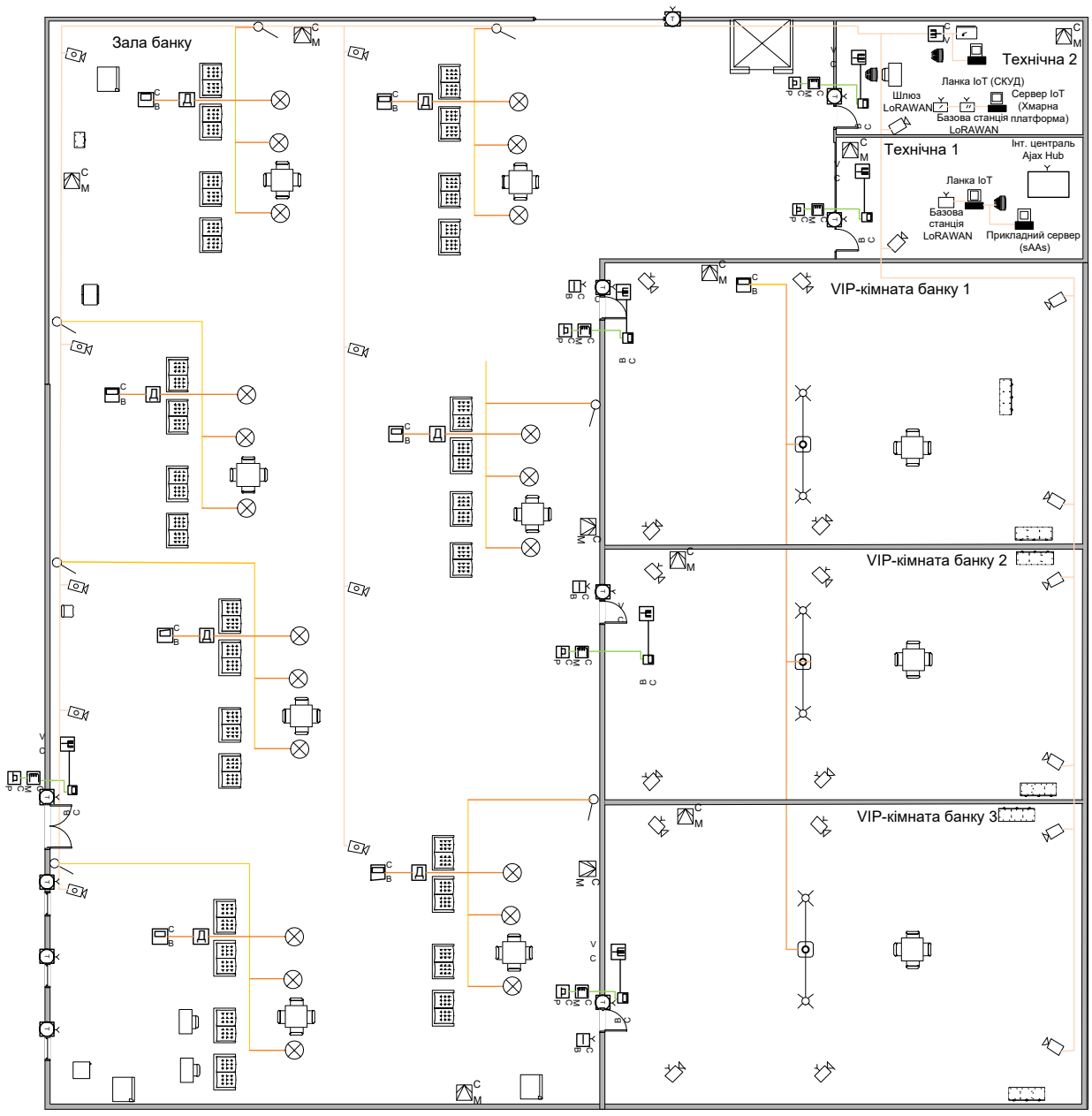

Рисунок 3.11 – План приміщення після розміщення устаткування

Висновки до розділу 3.

В межах запропонованих технічних рішень була створена гібридна система безпеки об’єкту, в якості якого обрано приміщення банкілвських установи загальною площею 380 м^2. Так, задля підвищення надійності функціонування складових такої системи були зпропоновані рішення на основі систем та технологій Інтернету речей. Зокрема, були впровадженні як звичайні камери відеонгаляду, так і камери з безпроводовим зв’язком на основі

технології LoRAWAN. Крім цього, за результатами проведеного аналізу можні підкреслити, що доступ до приміщення дозволяє забезпечити трирівневу аутентифікацію особи – за сенсором, за карточкою, на основі сканування обличчя з передаванням даних на базову станцію LoRAWAN і з подальшим пересиланням останніх на прикладний сервер системи.

4 РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

4.1 Опис ідеї проекту

Таблиця 4.1 - Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Security Control – це простий і зрозумілий пристрій та сервіс для стеження за рухомими об’єктами. Спеціальний пристрій з SIM картою та контакт-центр і онлайн навігація	1. Стеження за працівниками.	Безпека об’єктів стеження.
	2. Онлайн пошук і стеження за персоналом.	Контроль переміщення за допомогою GSM та GPS/GLONASS і онлайн системи.
	3. Онлайн пошук і стеження за документацією.	Персональний сервіс, доступний будь-якому клієнту цілодобово 24/7.

Опис до таблиці 4.2:

W – слабка сторона;

N – нейтральна сторона;

S – сильна сторона.

Таблиця 4.2 - Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характе-ристики ідеї	(потенційні) товари/концепції конкурентів				*W*	*N*	*S*
		Security Control	GPS Friend	tagg	GPSM			
1	Розмір пристрою	50×40×30 мм	52×40×23 мм	37×80×20 мм	77×51×25 мм		+	
2	Модулі	GSM/	GPS/ GSM	GPS/ GSM	GPS/ GSM			+
3	Автоном-ний час роботи	2-210 діб	48 год	2-10 діб	-			+
4	Робоча температу-ра	-35ºС +55ºС	-15ºС +55ºС	-15ºС +55ºС	-25ºС +55ºС			+
5	Водонепро никність	+	+	+	-		+	
6	Об’єкти застосува-ння	Авто, приміще ння, діти	Дом. тварини	Дом. тварини	Авто			+
7	Контакт-центр	+	+	+	+		+	
8	Вартість пристрою	50 $	35 $	99 $	120 $		+	

Продовження таблиці 4.2 - Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характе-ристики ідеї	(потенційні) товари/концепції конкурентів				*W*	*N*	*S*
		Security Control	GPS Friend	tagg	GPSM			
9	Абон.плата сервісу	12.5$/міс	3.85$/міс	7.95$/міс	4-15$/ міс			+

4.2 Технологічний аудит ідеї проекту

Таблиця 4.3 - Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Супутниковий моніторинг	GPS/GLONASS модуль	наявна	доступна
2	Мобільний моніторинг	SIM карта	наявна	доступна
3	Контакт-центр	«Контакт-центр по запросу» послуга 0-800	наявна	доступна
4	Персональний онлайн сервіс	Програмне забезпечення для ОС: Windows, Android, Mac	необхідно розробити	доступна
5	Автономне живлення	**(Ni-Cd), (Ni-MH), (Ni-MH) акумулятори**	наявна	доступна

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Таблиця 4.4 - Попередня характеристика потенційного ринку

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	5
2	Динаміка ринку (якісна оцінка)	Зростає
3	Наявність обмежень для входу (вказати характер обмежень)	відсутні
4	Специфічні вимоги до стандартизації та сертифікації	ДСТУ,СТТУ,ТУУ, ТУ
5	Середня норма рентабельності в галузі (або по ринку), %	53%

Таблиця 4.5 - Характеристика потенційних клієнтів стартап-проекту

Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
Безпека об’єктів стеження. Контроль переміщення за допомогою за дітьми, автомобілем чи домашними тваринами.	Власники автомобілів, власники домашніх тварин та сім’ї.	Залежно від цільової групи пристрій комплектується різного роду кріпленнями для зручності користування. Для продовження часу автономної роботи комплектується додатковими акумуляторними батареями. Залежно від вподобань цільових сегментів, пристрій синхронізовано з різними ОС.	- надійність - компактність - доступність - простота - зручність - екологічність - швидкість

Таблиця 4.6 - Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1	Незацікавленість клієнтів	Внаслідок невдалого маркетингу клієнт може не зацікавитись послугами	Внесення додаткових сервісних послуг тазниження цін
2	Втрата монополії	Втрата рангу єдиного гаранту якості технології	Якісне та кількісне нарощування інтенсивності

Таблиця 4.7 - Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1.Монополія	Інноваційний тип послуг	Стандартизація на високому рівні
2.Локальний	Відсутність єдиного національного постачальника послуг	Окремий підхід до кожної локальної ділянки
3.Міжгалузева	Конкуренція з іншими галузями (постачальниками апаратної частини)	Необхідність співробітництва в окремих сегментах
4.Товарно-видова	Подолання розсинхронізації відбувається за схожими технологіями, що реалізовані апаратно	За необхідності, використання приладів схожого типу

Продовження таблиці 4.7 - Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
5.Цінова	Можливість заощадити за допомогою діагностики	Гнучка політика ціни
6.Марочна	Кожна діагностика має бути стандартизованою	Отримання монополії над стандартом синхронізації

Таблиця 4.8 - Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
	Технологічні постачальники	Необхідність пошуку постачаль-ників	Залучення малопопулярних постачальників	Незалежність у прийнятті клієнтських рішень	Надання переваги більш авторите-тним технологічним рішенням
Висновки:	Незначна	Можливість виходу на ринок є	Постачальники диктують цінову політику на обладнання	Клієнти диктують вимоги до якості	Обмеження існують лише у разі відмови від діагностики

Таблиця 4.9 - Обґрунтування факторів конкурентноспроможності

№	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)
1	Раціональніший ціновий показник	Можливість більш раціонально використати ресурсів
2	Надання персональних сервісних послуг 24/7	Сервісна підтримка апаратної та програмної частини
3	Синхронізованість	Синхронізація з усіма ОС.
4	Спектр застосувань	Використання для ряду потреб користувачів.

Таблиця 4.10 - Порівняльний аналіз сильних та слабких сторін GNSS Control

№	Фактор конкуренто-спроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні						
			-3	-2	-1	0	1	2	3
1	Раціональніший ціновий коказник	13			+				
2	Надання персональних сервісних послуг 24/7	15			+				
3	Синхронізованість	20	+						
4	Спектр застосувань	17		+					

Таблиця 4.11 - SWOT-аналіз стартап-проекту

Сильні сторони:, надання персональних сервісних послуг 24/7, синхронізованість	Слабкі сторони: раціональніший ціновий показник
Можливості: використання для ряду потреб користувачів	Загрози: незацікавленість клієнтів, втрата монополії

4.4 Розроблення ринкової стратегії проекту

Таблиця 4.12 - Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Власники автомобілів	Середня	Високий	Високий	Середня
2	Власники домашніх тварин	Середня	Високий	Середній	Середня
3	Сім’ї	Середня	Висока	Низький	Середня
4	Мережі магазинів (електроніки, зоо, охорони, авто)	Висока	Висока	Середній	Середня
5	Web ресурси (сайти, клуби, соц.мережі)	Висока	Висока	Середній	Середня
Які цільові групи обрано: мережі магазинів та web ресурси					

Таблиця 4.13 - Визначення базової стратегії розвитку

№	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
1	Створення гаранту якості державного рівня	Встановлення єдиного універсального стандарту	Розробка і випуск власних пристроїв	Стратегія диференціації
2	Дешевизна проекту	Раціональніші витрати на обладнання, та послуги	Маловідомі партнери з постачання обладнання	Стратегія лідерства по витратах

Таблиця 4.14 - Визначення базової стратегії конкурентної поведінки

№	Чи є проект «першопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки
1	ні	Забирати існуючих та шукати нових	Характеристики апаратної частини	Стратегія виклику лідера

Таблиця 4.15 - Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкуренто-спроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сфо-рмувати комплексну позицію власного проекту (три ключових)
1	Висока якість послуг	Стратегія диференціації	Синхронізова-ність	Якість, надійність, сервісність
2	Мінімальні витрати	Стратегія лідерства по витратах	Широкий спектр застосування	Дешевизна, раціональність, тех. підтримка

4.5 Розроблення маркетингової програми стартап-проекту

Таблиця 4.16 - Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1	Якість	Висока якість, сервісність	сервісність
2	Дешевизна	Раціональне використання коштів	дешевизна

Таблиця 4.17 - Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові		
I. Товар за задумом	Дешевий якісний товар та послуги, стандартизована якість послуг та обладнання		
II. Товар у реальному виконанні	Властивості/характеристики:	М/Нм	Вр/Тх /Тл/Е/Ор
	1) Варстість обслуговування, 2) Кількість елементів 3) Строк безвідмовної праці 4) Технологічна собівартість товару	1) М 2) М 3) М 4) М	1)Е 2) Пр 3)Нд 4)Тх
	Якість: дерстандарт якості, високоякісні технології		
III. Товар із підкрі-пленням	До продажу – діагностика, обладнання, кріплення, дод.елементи живлення Після продажу – персональний онлайн сервіс		

Таблиця 4.18 - Визначення меж встановлення ціни

№	Рівень цін на товари замінники	Рівень цін на товарианалоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1	70-500 у.о./од	5-250 у.о./од	Високий	Н.50 у.о. – В.180 у.о.

Таблиця 4.19 - Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Зацікавленість в якісному продукті з раціональним використанням ресурсів	Мережні ресурси	Синхронізованість з будь-якими ОС	Зацікавити у покращеннях пов'язаних із зростаючою популярністю товару та послуг	Представлення продукції відправною точкою на шляху до безпеки
2	Зацікавленість у великій кількості продукту із дотриманням умов якісності	Мережні ресурси	Широкий спектр застосування	Зацікавити у позитивних сторонах	Представлення якісної роботи з клієнтами

Висновки до розділу 4.

В розділі дисертації, який присвячений розробці стартап-проекту визначаються конкуренті спроможності мобільного гаджету, який на основі відеокамери дозволяє слідкувати за рухом відвідувачів відділення банку. Визначено сильні та слабкі сторони запропонованого рішення та проаналізовано перспективи його просування на ринку через порівняння з аналогами. Визначено стратегію позиціонування товару на ринку та виявлені шляхи його просування з виходом на міжнародний ринок, де пропонується подібна продукція.

ВИСНОВКИ

Завищені технічні вимоги за принципами та критеріями надійності і безвідмовності обладнання з боку замовників до проектування сучасних систем безпеки приміщень змушують розробників такого обладнання шукати нові шляхи до удосконалення існуючих базових схем систем відеонагляду, систем сигналізації, систем контролю та управління доступом. Одним з можливих рішень такої проблеми може стати паралельне використання в комплексі складових систем безпеки обладнання з підтримкою технологій Інтернету речей. Особливо це стає нагальним, коли необхідно забезпечити охорону найбільш важливих установ, до числа котрих можна віднести і, зокрема, банківські відділення.

За результатами проведеного дослідження можна сформулювати наступні висновки.

1. Визначено принципи функціонування системи контролю та управління доступом і на основі проведеного аналізу варто підкреслити, що за критерієм захищеності доцільним є залучення ідентифікації особи на основі комбінаційного способу. Тобто, окрім традиційного пропуску за магнітною карткою, доцільним є використання систем сканування за певними рисами фізіологічних особливостей людини.

2. У другому розділі дисертації визначено базові особливості технології LoRAWAN. Так, зокрема, відмічено, що пристрої на основі LoRAWAN можуть функціонувати за трьома класами. При цьому, клас С не рекомендується використовувати, коли пристрої системи живляться автономно. Наприклад, це може стосуватись датчиків руху в приміщенні, які мають автономне живлення.Окремо сформульовані ключові особливості технології M2M у аспекті її використання в концепції Інтернету речей.

3. В практичні частині дисертації запропоновано підхід за яким з’являється можливість поєднати традиційні реалізації створення систем безпеки об’єкту і новітні на основі технологій Інтернету речей. Так, за

результатами вибору обладнання запропоновано власну схему розташування елементів за критерієм забезпечення підвищенної захищеності та надійності. Наведені особливості з проектування системи безпеки банківського відділення можуть стати у майбутньому підґрунтям до розроблення аналогічних систем в інших сферах людської діяльності.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Ворона, В. А. Системы контроля и управления доступом.— М. : Горячая линия – Телеком, 2013 .— 272 с. : ил.
2. Ворона, В. А. Охранные подразделения.— М. : Горячая линия – Телеком, 2012 .— 211 с. : ил.
3. Ли П. Архитектура интернета вещей. Москва: "ДМК Пресс", 2019. 454 с.
4. McEwen A. Designing the Internet of Things, USA: Publishing NT, 2013. – 336 p.
5. Сети LPWAN: история и перспективы. URL: http://orion-m2m.com/ru/news/seti-lpwan-istoriia-i-perspektivy/ (дата звернення: 02.05.2020)
6. Кучерявый А. Е. Самоорганизующиеся сети. СПб.: "Любавич", 2011. 312 с.
7. Jerker D. IoT Automation: Arrowhead Framework, Great Britain: CRC Press, 2017. – 366 p.
8. Муромцев Д. И., Шматков В. Н. Интернет вещей: введение в программирование на arduino, Санкт-Петербург: "ИТМО", 2018. – 36 с.
9. Росляков И. В., Ваняшин С. В., Гребешков А. Ю. Интернет вещей: учебное пособие, Самара: ПГУТИ, 2015. – 200 с.
10. ETSI TS 102 690 «Machine-to-Machine communications (M2M); Functional architecture» [електронний ресурс], V1.1.1. – 2011. – 280 p.
11. Елементи і пристрої фізичної та електронної охорони об'єктів: Конспект лекцій / П. В. Мокренко; Нац. ун-т «Львів. політехніка». — Л. : Фенікс, 2000. — 186 с. — Бібліогр.: 27 назв.
12. Ворона, В. А. Технические системы охранной и пожарной сигнализации.— М. : Горячая линия – Телеком, 2012 .— 377 с. : ил.

13. Макаров С.Б., Певцов Н.В., Попов Е.А., Сиверс М.А. Телекоммуникационные технологии: Введение в технологии GSM — М.: Академия, 2006. — 256 с.

ДОДАТОК А

ABSTRACT

The rapid development and spread of the Internet of Things technologies in various aspects of the existence of modern humanity is forcing developers of appropriate electronic equipment to look for new ways to use IoT. One of such promising areas can be considered the field of design of premises security systems. The fact is that the classic schemes of creating home security systems depend in the vast majority on external factors - the power supply of devices, electromagnetic compatibility, natural phenomena. And in this sense, to talk about a sufficient level of reliability of such systems is no longer necessary. An alternative is hybrid security systems, which provide basic security services with a certain level of redundancy. That is, in addition to the traditional circuit implementation of security systems, there are also systems based on the technology of the Internet of Things. The importance of this approach is greatly enhanced when it comes to premises, such as the banking sector. This dissertation is devoted to the issue of technical implementation of the security system for such buildings. The main attention in the security complex will be focused on the video surveillance system, alarm system and control system and access control to the premises.

ACS based on contactless plastic cards as a pass are designed to solve problems of improving the safety of facilities and ensuring labor discipline and order in the enterprise. The automated checkpoint, based on turnstiles-tripods with the use of contactless cards when passing, significantly increases the level of access control to the enterprise. The system organizes the passage of employees to the territory, identifying with the help of contactless electronic cards on the principle of "own or someone else's" and recording the time of passage. The system allows you to monitor all events at access points and issue notifications to the operator or security guard about alarm events (breaking locks, violation of access control, etc.). The operator can quickly control system devices - remotely lock the locks or, conversely, open them, for example, in case of fire.

The system software provides the ability to maintain a database of staff (name, position, department, staff number, mode of operation, photos, passport data, pass,

access rights), as well as contactless cards as icons. Compared to traditional access control, "access control as a service" has a number of advantages:

1. Because all information is stored on remote servers, there is no need to install the server in the institution directly.

2. It is possible to control access control from anywhere in the world, if there is Internet access.

3. The information received from all objects and all branches is stored in one place, and round-the-clock access to this information is provided.

4. The availability of the system is maintained around the clock by technical staff, and hardly any small business can boast of a round-the-clock presence of on-site support in the case of traditional access control.

5. Implementation of cloud security as a service, allows you to change the configuration of access control - if necessary, you can add more doors, assign cardholders different levels of access without the need to replace equipment or purchase additional software.

6. AcaaS uses secure encryption, so you don't have to worry about ACS hacking.

7. Some AcaaS require almost no hardware. Employees gain access to certain objects by downloading only the mobile application. Thanks to mobile credentials that send a signal to the door controller, employees can enter the office where they are allowed.

8. Access control as a service allows you to get and enable comprehensive security as a service. That is, it is possible to integrate the alarm system, video surveillance, intrusion detection, etc.

The term "cloud services" refers to a wide range of services provided on request to companies and customers via the Internet. These services are designed to provide easy and accessible access to applications and resources without the need for internal infrastructure or equipment. From checking email to working together on documents, most employees use cloud services during the workday, whether they realize it or not. Cloud services are fully managed by cloud providers and service

providers. They are provided to customers from vendor servers, so companies do not need to host applications on their own local servers. There are three main types of cloud services [3,4]:

• Software as a Service (SaaS). The most widely known type of cloud service and known as "software as a service" or SaaS (see 1.3). This large category includes various services such as file storage and backup, online email and project management tools. Examples of SaaS cloud service providers include Dropbox, G Suite, Microsoft Office 365, Slack, and Citrix Content Collaboration. In each of these applications, users can access, share, store and protect information in the cloud.

• Infrastructure as a service (IaaS). Infrastructure as a service, or IaaS, provides the infrastructure that many cloud service providers need to manage SaaS tools. It serves as a full-fledged structure of the data center, eliminating the need for resource-intensive installations on site. Examples of IaaS are Amazon Web Services (AWS), Microsoft Azure and Google Compute Engine. These vendors service all storage servers and network equipment, and can offer load balancing, application firewalls, and more. Many well-known SaaS vendors operate on IaaS platforms.

• Platform as a Service (PaaS). The cloud service model, known as the platform as a service, or PaaS, serves as a web environment in which developers can create cloud applications. PaaS provides a database, operating system, and programming language that organizations can use to develop cloud software without having to maintain basic elements. Many IaaS providers, including the examples listed above, also offer PaaS capabilities.

When deciding how to use cloud services, organizations must also decide which type of environment is best for the business: a public cloud platform, a private cloud environment, or a combination of both.

The services that a provider provides to numerous customers over the Internet are called publicly available cloud services. The above examples of SaaS, IaaS and PaaS provide publicly available cloud services. The biggest advantage of using public cloud services is the ability to share resources on a large scale, which allows organizations to offer employees more opportunities than would be possible alone.

As the availability of cloud services continues to expand, their use in the corporate world will also increase. Whether the company decides to expand existing local software deployments or move entirely to the cloud, these services will continue to make it easier to deliver critical applications and data to employees. From collaborating with content and managing access for employees to managing the delivery of programs and virtual desktop solutions for IT, as well as a wide range of intermediate options, cloud services are changing the way people work and the way companies work.