МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Чорноморський національний університет
імені Петра Могили
Факультет комп'ютерних наук
Кафедра комп'ютерної інженерії

ДОПУЩЕНО ДО ЗАХИСТУ

Завідувач кафедри,
д-р техн. наук, проф.

_____ Ірина ЖУРАВСЬКА

« __ » _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

Розвиток систем Інтернету речей для інтеграції з Індустрією 4.0 та виробничими процесами

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія»

Здобувач _____Андрій СТРЕЛЬБИЦЬКИЙ
підпис
«__» _____ 202__ р.

Керівник д-р техн. наук, проф. _____ Ірина ЖУРАВСЬКА
підпис
«__» _____ 202__ р.

Миколаїв – 2024

Факультет	Комп’ютерних наук
Кафедра	Комп’ютерної інженерії
Рівень вищої освіти	Другий (магістерський)
Освітній ступінь	Магістр
Спеціальність	123 Комп’ютерна інженерія
Освітня програма	Комп’ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри комп’ютерної інженерії
_____ Ірина ЖУРАВСЬКА

«_____» _____ 2024 р.

ЗАВДАННЯ
на кваліфікаційну роботу здобувача

_____Стрельбицькому Андрію Андрійовичу_____
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи
__Розвиток систем Інтернету речей для інтеграції з Індустрією 4.0 та виробничими процесами_____

Затверджена наказом по ЧНУ ім. Петра Могили від 16.09.2024 № 236.

2. Строк представлення кваліфікаційної роботи «____» _____ 20__ р.

3. Очікуваний результат роботи та початкові дані, якщо такі потрібні
___Очікуваним результатом роботи є розробка інтегрованої IoT-системи для виробничих процесів, яка забезпечить ефективний обмін даними та підвищення продуктивності в контексті Індустрії 4.0. Передбачено створення прототипу такої системи з алгоритмами аналізу даних для оптимізації роботи обладнання та ресурсів._____

4. Перелік питань, що підлягають розробці:
1) Проведення аналіз сучасних технологій Інтернету речей (IoT);
2) вивчення основних принципів та концепцій Індустрії 4.0;
3) оцінка викликів та ризиків, пов'язаних з впровадженням IoT у виробничу сферу;
4) побудувати структурні моделі (просторові та часові) інтеграції IoT-систем у виробничі процеси.
5) розробити ПЗ для випуску карток для вузлів СКУД як IoT-підсистем.

5. Перелік графічних матеріалів

_слайди презентації_____

6. Завдання до спеціальної частини _

7. Консультанти:

Консультант	Кафедра (організація)	Частина роботи

Керівник роботи _____ _Ірина ЖУРАВСЬКА_

Особистий підпис *Власне ім'я ПРІЗВИЩЕ*

Здобувач _____ _Андрій СТРЕЛЬБИЦЬКИЙ_

Особистий підпис *Власне ім'я ПРІЗВИЩЕ*

Дата видачі завдання «____» _____ 20_____ р.

КАЛЕНДАРНИЙ ПЛАН
виконання кваліфікаційної магістерської роботи

Тема:_ Розвиток систем Інтернету речей для інтеграції з Індустрією 4.0 та виробничими процесами

№	Найменування роботи	Початок	Закінчення	Примітки
1.	Розробка та затвердження завдання на виконання КМР	01.09.2024	16.09.2024	*Виконано*
2.	Огляд літератури за темою роботи	17.09.2024	30.09.2024	*Виконано*
3.	Складання календарного плану КМР	01.10.2024	08.10.2024	*Виконано*
4.	Аналіз предметної області	09.10.2024	13.10.2024	*Виконано*
5.	Розробка проєктних рішень	14.10.2024	23.10.2024	*Виконано*
6.	Моделювання	24.10.2024	28.10.2024	*Виконано*
7.	Конструювання АПК	29.10.2024	01.11.2024	*Виконано*
8.	Перевірка працездатності, тестування та апробація розробленого АПК	02.11.2024	08.11.2024	*Виконано*
9.	Аналіз результатів тестування	09.11.2024	13.11.2024	*Виконано*
10.	Розробка керівництва користувача	14.11.2024	17.11.2024	*Виконано*
11.	Відгук керівника КМР	18.11.2024	21.11.2024	*Виконано*
12.	Оформлення КМР та презентації	22.11.2024	27.11.2024	*Виконано*
13.	Попередній захист	28.11.2024	28.11.2024	*Виконано*
14.	Рецензування	10.12.2024	13.12.2024	*Виконано*
15.	Захист кваліфікаційної роботи	19.12.2024	20.12.2024	*Виконано*

Керівник роботи _____ _Ірина ЖУРАВСЬКА_
Особистий підпис *Власне ім'я ПРІЗВИЩЕ*

Здобувач _____ _Андрій СТРЕЛЬБИЦЬКИЙ_
Особистий підпис *Власне ім'я ПРІЗВИЩЕ*

АНОТАЦІЯ

до кваліфікаційної магістерської роботи

«Розвиток систем Інтернету речей для інтеграції з Індустрією 4.0 та виробничими процесами»

Здобувач гр. 605м Стрельбицький Андрій Андрійович

Керівник: д-р техн. наук, професор Журавська Ірина Миколаївна

Актуальність теми кваліфікаційної роботи полягає у тому, що IoT в промисловості використовується буквально всюди, де є виробництво. Так, Центр керування IoT Jasper (Cisco) від Київстар може використовуватися: на фермах – датчики контролюють наявність і якість води та корму у тварин; на заводах – щоб моніторити стан обладнання й запобігати поломкам або простоям; в енергетиці – щоб автоматично збирати дані лічильників та ін.

У веденні успішного бізнесу автоматизація процесів займає важливе місце. Зазвичай першими автоматизують рутинні операції, які можна чітко описати через алгоритми: визначення необхідних параметрів для перевірки, передача результатів, контроль за граничними відхиленнями та реагування на певні події. Одним з ключових елементів цієї автоматизації є використання Інтернету речей (IoT), який стає невід'ємною частиною сучасних бізнес-процесів.

Об'єкт дослідження: методи обміну даними, автоматизації та оптимізації виробничих процесів з впровадженим апаратним та програмним забезпеченням Інтернету речей (IoT).

Предмет дослідження (розробки): системи Інтернету речей (IoT) та їх технологічні рішення, що використовуються для інтеграції з виробничими процесами та Індустрією 4.0, а також вплив цих систем на ефективність компаній у різних галузях.

Мета: аналіз сучасного стану систем Інтернету речей (IoT) та їх інтеграції з виробничими процесами та Індустрією 4.0, а також імплементація окремих вузлів систем контролю та управління доступом (СКУД) як систем IoT у промислових середовищах.

Для досягнення поставленої мети було поставлено такі завдання:

1) провести аналіз сучасних технологій Інтернету речей (IoT), їхньої архітектури та основних компонентів, що використовуються для інтеграції з виробничими процесами, а також оцінити вплив IoT на ефективність та продуктивність;

2) вивчити основні принципи та концепції Індустрії 4.0, зокрема «розумне виробництво», автоматизацію та кіберфізичні системи;

3) оцінити виклики та ризики, пов'язані з впровадженням IoT у виробничу сферу, а також розробити рекомендації щодо їх подолання;

4) побудувати структурні моделі (просторові та часові) інтеграції вузлів СКУД як складових IoT-систем у виробничі процеси, що включають етапи збору, обробки та аналізу даних;

5) розробити ПЗ для випуску карток для підсистем СКУД від компанії Hikvision.

Кваліфікаційна робота містить: перелік скорочень, вступ, чотири розділи, висновки, перелік джерел посилання та три додатки.

Вступ містить основні обґрунтування актуальності розробки обраної теми, об’єкт, предмет дослідження, мету та завдання які необхідно виконати для досягнення поставленої мети.

В першому розділі проведено аналіз Інтернету речей (IoT) їх основні компоненти та можливості, Індустрії 4.0 її принципи та ключові технології.

Другий розділ містить опис апаратного забезпечення, використаного у практичній частині роботи.

Третій розділ містить опис та результати проєктування програмної частини.

У четвертому розділі проведено пояснення розробленої системи та виконано аналіз результатів.

У висновку описано результати виконання кваліфікаційної роботи.

Додатки містять код програми та апробацію

Кваліфікаційна робота містить 91 сторінок (без додатків), 53 рисунки, 30 джерел посилання, 2 додатки.

Ключові слова: *IoT, СКУД, Industry 4.0, Hikvision, інтеграція у виробничі процеси, контроль часу*

ABSTRACT

of the Master's Thesis

" Development of Internet of Things Systems for Integration with Industry 4.0 and Manufacturing Processes"

Applicant: Strelbytskyi Andrii Andriiovych

Supervisor: D.Sc. (Techn.), Professor Zhuravska Iryna Mykolaivna

The relevance of the topic of qualified work lies in the fact that IoT is used literally everywhere in industries, including manufacturing. For example, Kyivstar's IoT management center Jasper (Cisco) can be used in the following locations: farms – where sensors monitor the availability and quality of water and feed for animals; factories – to monitor the condition of equipment and prevent breakdowns and downtime; to automatically collect energy meter data, etc.

Automated processes play a key role in making your business successful. The routine process is mainly automated and can be described by a simple action algorithm. You need to check which parameters need to be checked, where to send the results, where to check for boundary deviations, and what to do if a particular occurrence occurs. In particular, the Internet of Things has become an integral part of this process.

Research Subjects: hardware and software analysis of IoT, data exchange methods, automation and optimization of production processes, and the study of the effects of these systems on the efficiency of companies in different industries.

Research Theme (Development): IoT systems and their technical solutions for manufacturing processes and integration with Industry 4.0.

Purpose: to analyze the current state of Internet of Things (IoT) systems and their integration with manufacturing processes and Industry 4.0 and to develop recommendations for further development and effective use of IoT systems in industrial environments.

To achieve the set goals, the following tasks were set:

1) Analyze the latest IoT technologies, their architecture, and the key components used to integrate with the manufacturing process;
2) The main principles and concepts of Industry 4.0, in particular, "smart manufacturing", automation, cyber-physical systems;
3) Analyze existing examples of IoT implementations in manufacturing processes across different industries to assess their impact on efficiency and productivity;
4) Assess the challenges and risks associated with IoT adoption in the manufacturing industry and develop recommendations to overcome them;
5) Build structural models (spatial and temporal) to integrate ACS (Access Control System) modules as IoT systems' components into the manufacturing process, including the stages of data collection, processing, and analysis;
6) Develop software for issuing cards for ACS subsystems of Hikvision company.

The qualification work includes a list of abbreviations, introductions, 4 chapters, conclusions, a list of references, and 3 appendices.

The introduction includes the relevance of the selected topic, the purpose and subject of the study, the goals, and the primary basis for the tasks that must be performed to achieve the goal.

The first chapter analyzes the Internet of Things (IoT), its key components and functions, Industry 4.0, its principles, and key technologies.

The second chapter describes the hardware used in the practical part of the work.

The third chapter contains a description and results of the design of the software components.

The fourth chapter provides a description of the developed system and an analysis of the results.

The conclusion describes the results of the qualification work.

Appendices contain software code and information on the approval of the qualification work.

The qualification work contains 91 pages (without appendices), 53 figures, 30 reference sources, 2 appendices.

Keywords: *IoT, Industry 4.0, Access Control System, Hikvision, integration into production processes, hour control.*

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АППА – Асоціація підприємств промислової автоматизації України
ІТ – інформаційні технології
ІС – інформаційна система
МСП – мале та середнє підприємництво
СКУД – система контролю та управління доступом (англ. ACS)
ШІ – штучний інтелект (англ. AI)

ACS – Access Control System
AI – Artificial intelligence
AIoT – Artificial Intelligence of Things
AR – Augmented Reality
CPS – Cyber-physical system
ERP – Enterprise Resource Planning
IoT – Internet of Things
IIoT – Industrial Internet of Things
JIPDEC – Japan Institute for Promotion of Digital Economy and Community
M2M – Machine-to-Machine

ВСТУП

Інтернет речей (IoT) забезпечує інтелектуальну взаємодію між пристроями, обладнанням і системами, дозволяючи збирати, аналізувати та використовувати дані в режимі реального часу. Це підвищує гнучкість виробничих процесів, покращує управління ресурсами, знижує витрати і підвищує якість продукції. Впровадження Інтернету речей у виробництво стає невід'ємною частиною новітньої концепції «розумної фабрики», де мають місце нові рівні взаємодії між людьми, машинами і системами.

У веденні успішного бізнесу чималу роль відіграють процеси автоматизації. У першу чергу, зазвичай, автоматизують рутинні процеси, які можна описати простими алгоритмами дій: які параметри потрібно перевірити, куди передати результат, де перевірити граничні відхилення та що зробити в разі настання певної події.

Індустрія 4.0, характеризується широким впровадженням цифрових технологій в усі аспекти виробництва та економіки. Одним з ключових компонентів цього підходу є використання систем Інтернету речей (IoT), які дозволяють інтегрувати фізичні об'єкти з цифровими платформами для підвищення ефективності та автоматизації процесів.

Інтеграція Інтернету речей та Індустрії 4.0 сприяє створенню інноваційних бізнес-моделей і відкриває нові можливості для оптимізації процесів. При цьому виникають не лише технічні, але й економічні питання, що потребують поглиблених досліджень та розробки нових підходів до проєктування, впровадження та управління такими системами.

Дослідження в цій галузі є надзвичайно важливими, оскільки вони не лише сприяють технологічному розвитку, але й впливають на глобальні економічні процеси та створюють нові можливості для розвитку виробництва в умовах цифрової трансформації.

Мета роботи: аналіз сучасного стану систем Інтернету речей (IoT)та їх інтеграції з виробничими процесами та Індустрією 4.0, а також імплементація окремих вузлів систем IoT у промислових середовищах.

Об'єкт дослідження: програмно-технічні засоби комп’ютерної системи контролю та управління доступом (СКУД) як системи Інтернету речей (IoT); інтерфейси та протоколи взаємодії компонентів СКУД.

Предмет дослідження: системи Інтернету речей (IoT) та їх технологічні рішення, що використовуються для інтеграції з виробничими процесами та Індустрією 4.0, а також вплив цих систем на ефективність компаній у різних галузях.

Завдання роботи:

1) провести аналіз сучасних технологій Інтернету речей (IoT), їхньої архітектури та основних компонентів, що використовуються для інтеграції з виробничими процесами у різних галузях промисловості, а також оцінити вплив IoT на ефективність та продуктивність;

2) вивчити основні принципи та концепції Індустрії 4.0, зокрема «розумне виробництво», автоматизацію та кіберфізичні системи;

3) оцінити виклики та ризики, пов'язані з впровадженням IoT у виробничу сферу, а також розробити рекомендації щодо їх подолання;

4) побудувати структурні моделі (просторові та часові) інтеграції підсистем СКУД у якості IoT-систем у виробничі процеси, що включають етапи збору, обробки та аналізу даних;

5) розробити ПЗ для випуску карток для підсистем СКУД.

Практичне значення роботи: дослідження може бути використане для оптимізації виробничих процесів на підприємствах, що використовують системи IoT: розроблені підходи та рекомендації щодо інтеграції IoT з концепціями Індустрії 4.0 та виробничими процесами можуть бути застосовані для підвищення ефективності виробництва, автоматизації операцій та покращення управління ресурсами. Корисність. Запропонована інтегрована модель може допомогти компаніям знизити витрати, підвищити якість продукції та скоротити час виробничого циклу.

Результати цього дослідження будуть корисними не лише для інженерів, керівників виробництва та розробників систем Інтернету речей, а й для компаній, які прагнуть рухатися в напрямку цифрової трансформації.

Дана кваліфікаційна робота була апробована на XXI Міжнародній науковій конференції «Ольвійський форум – 2024: Стратегії країн Причорноморського регіону в геополітичному просторі». Матеріали доповіді опубліковані у збірнику конференції [27].

1 АНАЛІЗ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ ТА ІНДУСТРІЇ 4.0

Інтернет речей (IoT) та Індустрія 4.0 є двома взаємопов'язаними концепціями, що активно впливають на трансформацію виробничих процесів і промисловість загалом. Їхній розвиток дозволяє створювати інноваційні моделі управління, забезпечуючи гнучкість, автоматизацію та взаємодію між фізичними і цифровими системами.

В основі Інтернету речей лежать такі технології:

Засоби ідентифікації

Усі об'єкти у фізичному світі, які беруть участь в Інтернеті речей, повинні мати унікальні ідентифікатори, навіть якщо вони не підключені до мережі. Автоматична ідентифікація об'єктів включає в себе радіочастотні, оптичні (штрих-код, Матриця даних, QR-код), інфрачервоні мітки і т.д., коли до кожного об'єкта прикріплюються радіочастотні мітки. Ви можете використовувати різні існуючі системи. Однак для забезпечення унікальності різних типів ідентифікаторів необхідно провести роботу по їх стандартизації.

Засоби Вимірювання

Завданням приладу є надійне перетворення інформації про зовнішнє середовище в дані, придатні для передачі в засоби обробки. Це можуть бути як окремі датчики, такі як температура, освітлення, так і складовою вимірювальний комплекс. Для досягнення автономності вимірювального приладу бажано подавати живлення на датчик за рахунок альтернативної енергії (сонячні батареї і т. д.), щоб не витрачати час і гроші на підзарядку акумулятора або заміну батарейки.

Засоби передачі даних

Для передачі даних може бути використано будь-який з відомих пристроїв. При використанні бездротових мереж особлива увага приділяється підвищенню надійності передачі даних. При використанні кабельної мережі використовується безліч «дрібниць» (торгові автомати, банкомати і т. д.), тому

активно використовується технологія передачі даних по лініях електропередач.Підключається до електромережі.

Засоби обробки даних

Понад 30 мільярдів пристроїв, які, за прогнозами, будуть підключені до Інтернету в 2020 році, генеруватимуть 440 мільярдів терабайт даних. Це приблизно в 7 разів перевищує обсяг оцифрованої інформації в світі в 2010 році. Тому Microsoft вважає, що основною частиною Інтернету речей є не датчики або засоби передачі даних, а хмарна система, яка забезпечує високу пропускну здатність і може швидко реагувати на певні ситуації (наприклад, за показаннями датчиків видно, що в будинку нікого не було протягом 5 хвилин, і т. д.). що вхідні двері залишалися відкритими). (Ви можете дізнатися, як ним користуватися.) Fog computing також не конкурує з хмарними обчисленнями, але допомагає впоратися з величезним потоком інформації, яка ефективно доповнює їх.

Виконуючі пристрої

Це пристрої, які можуть перетворювати цифрові електричні сигнали з інформаційних систем (ІС) у дії. Наприклад, щоб включити систему опалення будинку через смартфон, потрібно відповідний пристрій. Виконавчі механізми часто конструктивно поєднуються з датчиками.

1.1 Інтернет речей (IoT): основні компоненти та можливості

Термін «Інтернет речей» (IoT) був введений у 1999 році Кевіном Ештоном, одним із засновників Центру автоматичної ідентифікації Массачусетського університету (Auto-ID Center). Існує кілька варіантів його визначення, але жодне з них не є повністю точним. Ми будемо використовувати визначення від компанії Gartner, яка також є автором терміну ERP: «Інтернет речей – це мережа фізичних об'єктів, що мають вбудовані технології для взаємодії з навколишнім середовищем, передачі інформації про свій стан і отримання даних ззовні».

Інтернет речей, як і звичайний Інтернет, складається з великої кількості взаємопов'язаних мереж. Кожна з цих мереж працює за різними стандартами і вирішує свої завдання. Він управляє кондиціонером, регулює опалення, автоматично регулює освітлення, відстежує пульс під час тренування і відстежує сигнал у разі перевантаження.

Для того, щоб всі ці різноманітні мережі об'єдналися в одну, використовується 1-ша версія протоколу IP – Ipv4. Ця версія дозволяє використовувати понад 40 мільярдів IP-адрес. Однак у зв'язку з тим, що обсяг Інтернету речей зростає настільки швидко, що до 2020 року, за прогнозами, буде від 300 до 500 мільярдів підключених до мережі пристроїв, яким потрібна власна IP-адреса або унікальний ідентифікатор, вони впроваджують 6-у версію протоколу – Ipv6. Це дозволить всім жителям планети використовувати більше 4 мільйонів IP-адрес.

Пристрої Інтернету речей в окремій мережі можуть налаштовувати, дозволяти або забороняти доступ до даних. Але в цілому вони працюють незалежно в режимі реального часу. Система Інтернету речей включає в себе набір інтелектуальних пристроїв, підключених до мережі, і хмарну платформу для зберігання даних. Пристрої найчастіше підключаються один до одного за допомогою хмарного сховища даних за допомогою Wi-Fi, Bluetooth або мобільного зв'язку.

Основними компонентами IoT є:

1. Пристрої та сенсори:

Пристрій – це фізичний об'єкт, який може підключатися до Інтернету та виконувати певні функції. Це можуть бути інтелектуальні термостати, освітлення, автомобілі, побутова техніка та інші пристрої.

Датчики– це спеціалізовані пристрої, які збирають дані про навколишнє середовище (температурі, вологості, тиску, руху, освітленості і т. д.). Датчик може вимірювати різні параметри та передавати ці дані в систему для подальшої обробки та аналізу.

2. Комунікаційна мережа:

Передача даних: після того, як дані зібрані датчиком, інформація повинна бути відправлена на центральну платформу або сервер для обробки. Використовуються різні комунікаційні технології, включаючи Wi-Fi, Bluetooth, Zigbee, LPWAN (глобальна мережа з низьким енергоспоживанням) і 5G.

Протоколи передачі: це правила, що регулюють передачу даних між пристроями. Наприклад, передача телеметрії в черзі повідомлень (MQTT), HTTP та CoAP.

3. Обробка даних:

Дані, зібрані датчиком, повинні бути оброблені для подальшого аналізу. Це може відбуватися на різних рівнях: локальна обробка (на пристрої або шлюзі) або централізована обробка (на сервері або в хмарі).

Обчислювальна платформа: ви можете використовувати потужний сервер або хмарну платформу для обробки великих обсягів даних та застосування технологій обробки даних, аналітики, штучного інтелекту та машинного навчання.

4. Аналіз та зберігання даних:

Після обробки дані зазвичай зберігаються для подальшого аналізу та прогнозування. Це включає виявлення тенденцій, виведення звітів та їх зберігання в базі даних, яка використовується для створення аналітичних моделей.

Технології великих даних часто використовуються для обробки великих обсягів даних, отриманих з пристроїв IoT.

5. Інтерфейс користувача:

Платформа IoT надає користувачам можливість відстежувати дані та контролювати пристрої через спеціалізований інтерфейс. Це веб-або мобільні застосунки, які дозволяють отримувати інформацію в режимі реального часу, налаштовувати налаштування пристрою або отримувати сповіщення про події.

6. Безпека:

Безпека є одним з ключових компонентів, оскільки системи IoT часто обробляють конфіденційну інформацію та взаємодіють з критичною

інфраструктурою. Це включає захист даних, аутентифікацію пристроїв, шифрування переданих даних та захист від кібератак.

Можливості IoT:

1. Моніторинг в режимі реального часу:

Інтернет речей дозволяє постійно відстежувати стан різних систем і процесів в режимі реального часу. Наприклад, у виробничому середовищі ви можете відстежувати стан обладнання, температуру або рівень споживання енергії. Це дозволяє швидко реагувати на проблеми і знижувати ризики.

2. Автоматизація процесів:

IoT автоматизацію багатьох рутинних завдань. Наприклад, в розумному будинку датчик може автоматично регулювати освітлення і температуру в залежності від часу доби або присутності людини. У промисловості це може включати автоматизоване регулювання виробничих процесів та управління запасами.

3. Ефективність використання ресурсів:

IoT може допомогти оптимізувати використання таких ресурсів, як енергія, вода та матеріали. За допомогою датчиків та аналітики даних ви можете зменшити витрати, підвищити ефективність та досягти сталого розвитку.

4. Профілактичне обслуговування:

Відстежуючи стан обладнання та аналізуючи дані, можна прогнозувати поломки або зниження продуктивності до того, як це станеться. Це знижує витрати на технічне обслуговування і дозволяє уникнути непередбачених відключень.

5. Розширена аналітика та прийняття рішень:

IoT дозволяє збирати великі обсяги даних, які використовуються для побудови аналітичних моделей, прогнозів та прийняття обґрунтованих рішень на всіх рівнях бізнесу та виробництва.

6. Покращена взаємодія між пристроями:

IoT дозволяє різним пристроям взаємодіяти один з одним без втручання людини. Це створює можливість для створення більш інтегрованої та

ефективної системи, в якій пристрої можуть автоматично налаштовуватися один з одним або обмінюватися даними для досягнення оптимальних результатів.

Складовою частиною Інтернету речей є Індустріальний (або Промисловий) Інтернет речей (Industrial Internet of Things, IIoT).

Технології для бездротової передачі даних розрізняються за дальністю передачі на такі: Proximity, Short Range та Long Range. Деякі з цих технологій потребують ліцензування, усі інші називаються відкритими (рис. 1.1–1.3).

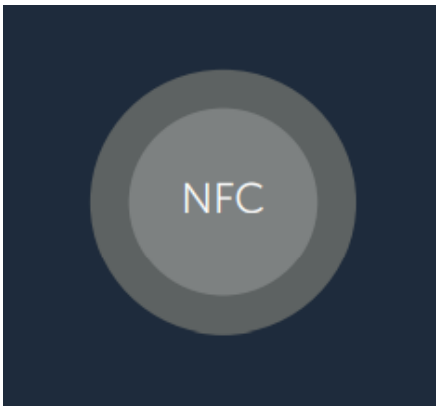

Рисунок 1.1 – Технологія щільного контакту [25]

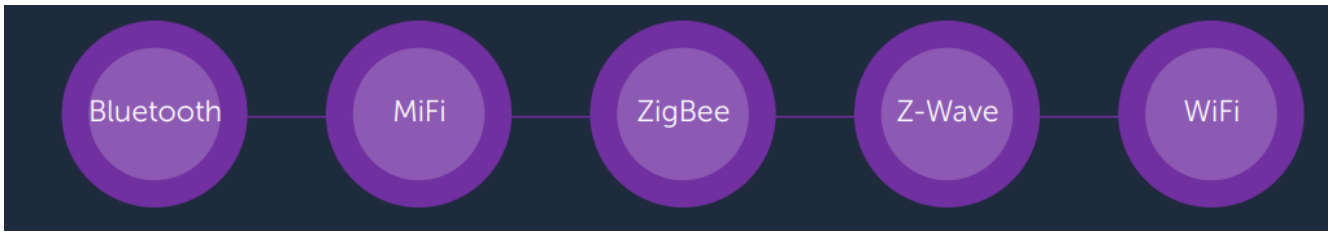

Рисунок 1.2 – Технологія короткого діапазону [25]

Рисунок 1.3 – Технологія дальнього діапазону [25]

При виборі технології для автоматизації бізнес-процесів важливо врахувати кілька ключових факторів:

– Чи будуть пристрої пересувними або стаціонарними?
– Яка відстань між пристроями та точкою збору даних?
– Чи передбачено електроживлення для пристроїв?
– Який обсяг даних планується передавати?
– З якою частотою потрібно збирати дані з пристроїв?
– У яких умовах будуть працювати пристрої — на вулиці, в приміщеннях із залізобетону, в підвалі чи на вищих поверхах?
– Наскільки критичні перешкоди при передачі сигналу?
– Які додаткові канали зв’язку можуть бути необхідні для пристроїв?

Відповіді на ці питання допоможуть вибрати технологію, що забезпечить ефективну роботу пристроїв та їх інтеграцію в автоматизовані бізнес-процеси.

1.2 M2M та IoT

Багато виробників продукції використовують технологію M2M для вдосконалення своїх товарів і надання кінцевим споживачам додаткових сервісів та можливостей. Технології, що розширюють функціональність пристроїв через M2M, отримали назву Інтернет речей (IoT).

Для дистанційного збору показників та їх передачі необхідно забезпечити канал зв’язку між пристроями, щоб вони могли «спілкуватися» один з одним. Раніше цей зв’язок був можливий лише через кабелі, однак завдяки розвитку стільникового зв’язку і новітніх технологій, пріоритет тепер віддається бездротовим способам передачі даних.

Це дозволяє використовувати дистанційне вимірювання на віддалених об’єктах або в мобільних механізмах. Таку технологію, де машини взаємодіють між собою, називають Machine-to-Machine (M2M).

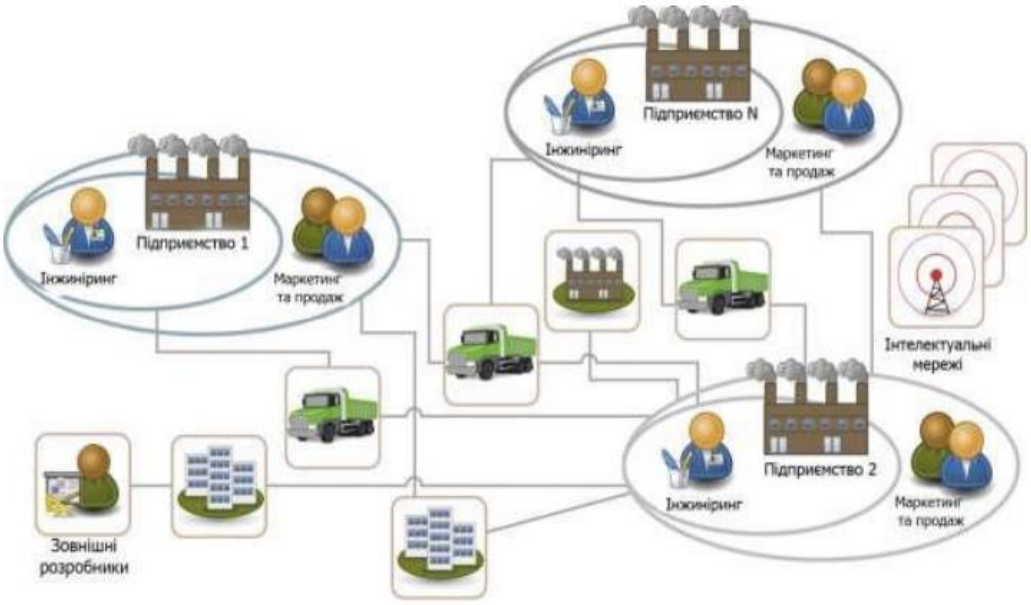

Рисунок 1.4 – Smart City [26]

Використання технологій M2M та IoT є вкрай важливим і необхідним у сферах, де потрібно автоматизувати процеси. Особливо активно IoT розвивається в аграрному секторі, логістиці, Smart City (рис. 1.4) – усюди, де потрібно прискіпливо моніторити стан об’єктів або збирати великі масиви даних задля подальшого аналізу. IoT дає змогу економити на обслуговуванні обладнання: датчики збирають інформацію про його стан, тому техобслуговування і ремонт здійснюють вчасно.

1.3 Керування великою кількістю SIM-карток M2M

На поточний момент деякі з операторів стільникового зв’язку України надають послуги «Центр керування IoT», що дозволяють споживачам послуг M2M скористатися наступними можливостями:

- налаштування власних правил роботи SIM-карток та їх автоматизованого керування;
- активація та деактивація SIM-карток за потреби;
- контроль використання послуг за всіма SIM-картками M2M;
- блокування й активація послуг;

- визначення лімітів використання трафіку та параметрів оповіщення по досягненні лімітів;
- створення груп SIM-карток M2M для масового налаштування та керування;
- захист SIM-карток від нецільового використання та шахрайства;
- зміна тарифних планів SIM-карток;
- перегляд статистики використання послуг за M2M-номерами;
- створення та керування доступами додаткових адміністраторів і користувачів;
- моніторинг поведінки пристроїв;
- авторизація доступу до пристрою;
- відстеження прийнятих і відправлених SMS-повідомлень;
- відправка й отримання SMS-повідомлень на платформу послуги та з неї;
- перегляд параметрів, з якими SIM-картки здійснювали доступ до мережі інтернет;
- відстеження активних сесій інтернет-з’єднання за їхніми параметрами: обсяг прийнятої та переданої інформації, тривалість тощо;
- можливість перегляду дій адміністраторів і користувачів в системі;
- можливість перегляду звіту спрацьовувань автоматичних налаштувань і правил;
- встановлення налаштувань для блокування SIM-карток при зміні IMEI пристрою;
- створення списку «білих» (дозволених) IMEI;
- перегляд звітів тощо.

Перший клієнт, який скористався технологією M2M у компанії «Київстар», з'явився наприкінці 2002 року. Це була охоронна компанія, для якої були розроблені перші два тарифні плани для охорони стаціонарних та рухомих об'єктів. SIM-карти вже тоді встановлювались в системи сигналізації. На той

момент це виглядало як інновація, оскільки навіть мобільні телефони були не в кожного, – згадує Євген Берус, менеджер з маркетингу «Київстар».

Згідно з підрахунками асоціації GSMA Intelligence, у II кварталі 2017 року в Україні було майже 2,14 млн активних SIM-карт для телематики. Протягом останніх восьми років їхня кількість зростала в середньому на 50% щорічно (рис. 1.5).

Рисунок 1.5 – Динаміка кількості SIM-карт M2M [30]

Зараз 55 % ринку M2M займає компанія «Київстар», але інші оператори також активно розширюють свою базу. «Приріст кількості M2M-підключень цього року на 50 % більший, ніж у попередньому», — зазначає Олена Підгірна, начальник відділу бізнес-послуг «Vodafone Україна».

У прес-службі lifecell пояснюють, що M2M є одним з найбільш швидкозростаючих сегментів. Вони зазначають, що з 2015 року цей бізнес збільшується вдвічі кожного року. [30].

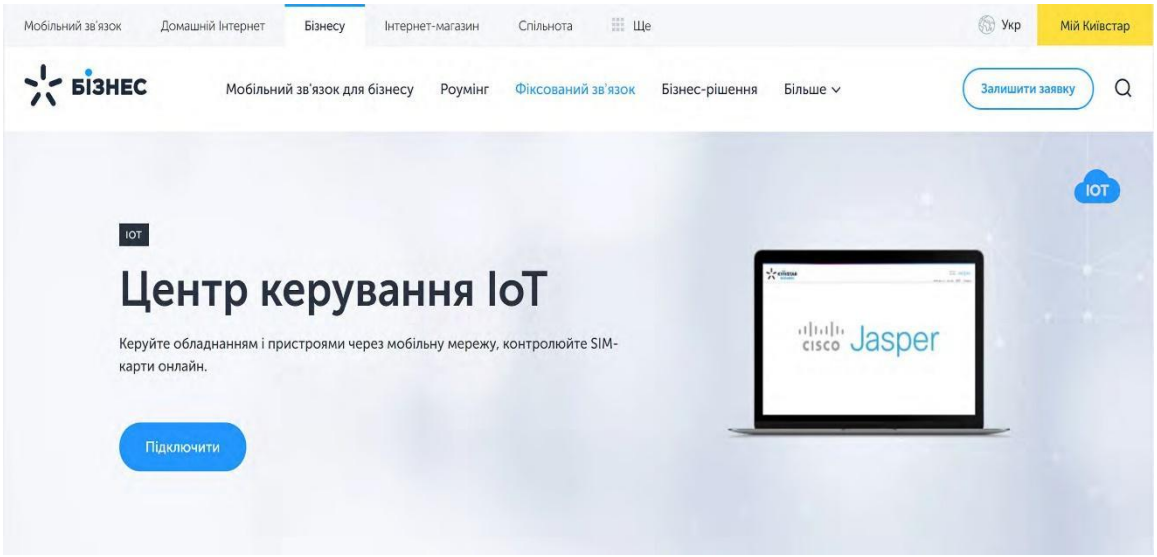

Рисунок 1.6 – Вебінтерфейс центру керування IoT

Доступ до керування SIM-картками можливий у вебінтерфейсі або за допомогою API без збільшення вартості послуги. Послуга «Центр керування IoT» доступна як для нових M2M підключень, так і для існуючих M2M-номерів і вже включена у вартість багатьох тарифних планів лінійки «IoT» (рис. 1.6).

Індустріальний IoT (IIoT) – це датчики на промислових об’єктах, які об’єднані між собою та підключені до комп’ютерних мереж. За допомогою програмного забезпечення можна збирати дані та обмінюватися ними, дистанційно контролювати роботу датчиків та управляти ними без участі людини. У підсумку стає можливим детальний збір об’єктивних і точних даних про стан виробництва.

Впровадження технології Інтернету речей для промислових підприємств (IIoT) дозволяє створити автоматизовану систему, яка контролює процеси виробництва, моніторить стан вузлів та агрегатів, а також оцінює якість продукції. Застосування таких технологій знижує ймовірність несанкціонованих зупинок обладнання.

Основні переваги промислового Інтернету речей включають:

– досягнення високої енергоефективності;
– прискорення виробничих процесів;
– підвищення якості продукції.

На першому етапі впровадження IIoT на обладнання встановлюються датчики, контролери, виконавчі механізми та інтерфейси для взаємодії з користувачем. Це дозволяє збирати точну інформацію про стан виробництва, яку передають усім підрозділам підприємства для покращення взаємодії та прийняття обґрунтованих рішень.

Інформація, що надходить з датчиків, може використовуватись для запобігання поломкам, зменшення часу на позапланове обслуговування та збоїв в управлінні ланцюгами постачання, що сприяє більш ефективному функціонуванню підприємства. Оскільки дані, що надходять від датчиків, часто є неструктурованими, важливим є їх належна фільтрація та інтерпретація. Для цього використовуються передові аналітичні платформи, що дозволяють обробляти дані в реальному часі.

Завдяки IIoT виробничі підприємства стають більш гнучкими, ощадливими та ефективними. Бездротові пристрої з підтримкою IP-протоколу, включаючи смартфони, планшети та датчики, активно використовуються в промисловості, а найближчим часом кабельні мережі датчиків будуть доповнені бездротовими, що розширить можливості систем моніторингу та управління на підприємствах.

Наступним етапом буде збільшення інтеграції інформаційних і операційних технологій, що дозволить підприємствам перейти від ізольованих систем до відкритих цифрових екосистем, де управління виробничими процесами здійснюватиметься через хмарні сервіси. Це трансформує мету підприємств: від випуску продукції до надання послуг кінцевим споживачам.

1.4 Індустрія 4.0: принципи та ключові технології

Індустрія 4.0 (Industry 4.0) – провідний тренд «Четвертої промислової революції», яка відбувається безпосередньо у теперішній час (рис. 1.7).

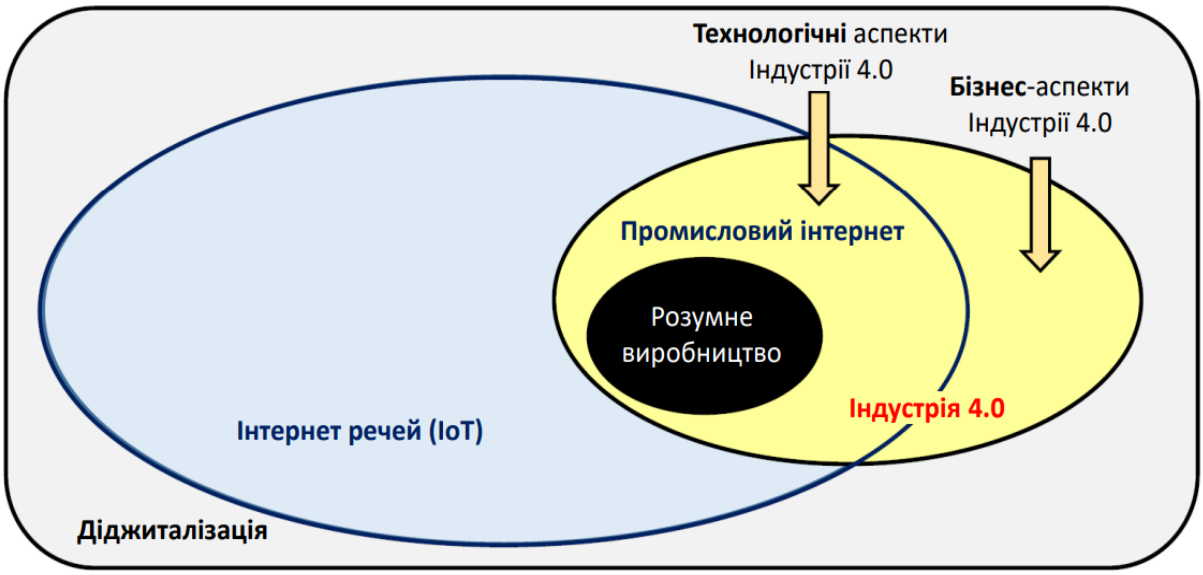

Рисунок 1.7 – Зв'язок між діджиталізацією, Інтернетом речей та Індустрією 4.0

Історія промислової революції охоплює століття, і кожен період відзначений значним технологічним прогресом.

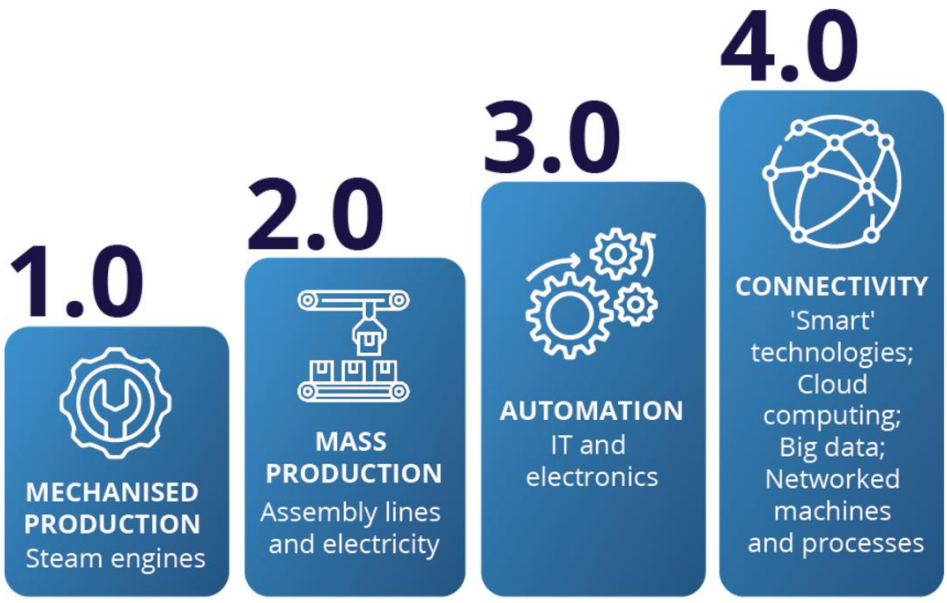

Рисунок 1.8 – Історія промислової революції [3]

Індустрія 1.0

Перша промислова революція, також відома як Індустрія 1.0, почалася у 18 столітті з впровадженням машинного виробництва, яке замінило ручну

працю машинами з паровим двигуном. Це призвело до зростання продуктивності, зростання заводів і масового виробництва.

Індустрія 2.0

Наприкінці 19-го та на початку 20-го століть друга промислова революція, або Індустрія 2.0, була спровокована розвитком електрики та двигуна внутрішнього згоряння. У цей період у будівництві широко використовувалися сталь і бетон, а Генрі Форд відіграв значну роль у встановленні високих стандартів продуктивності для автомобільної промисловості. Хімічне виробництво також збільшило свою продуктивність за менших витрат протягом цього періоду.

Індустрія 3.0

Третя промислова революція, або Індустрія 3.0, почалася наприкінці 20 століття з цифрової революції. Розвиток комп’ютерів, засобів керування з програмованою пам’яттю та Інтернету відзначили цей період. У виробничих процесах почали використовувати автоматизацію, коли роботи виконують запрограмовані послідовності без втручання людини.

Індустрія 4.0

Індустрія 4.0 є сучасним періодом технологічного розвитку і відноситься до четвертої промислової революції. Ця революція характеризується інтеграцією передових технологій, таких як штучний інтелект (AI), машинне навчання, Інтернет речей (IoT) і робототехніка в промислові процеси. Індустрія 4.0 створює «розумні фабрики», які є високоавтоматизованими, керованими даними та повністю підключеними до ланцюгів постачання. Ця революція значно підвищила ефективність і продуктивність виробничих операцій, а впровадження структурованого, гнучкого та спільного підходу стає все більш важливим [3].

Зараз ми переживаємо етап завершення третьої, цифрової революції, яка почалася в другій половині XX століття. Її основні риси – розвиток інформаційно-комунікаційних технологій, автоматизація та роботизація виробничих процесів.

Проте, діджиталізація, яка охоплює впровадження цифрових технологій, автоматизації та IT у всі сфери життя і економіки, почалася ще в минулому столітті і отримала назву технологічного укладу 3.0. Це триває й сьогодні. Проте останніми роками західні країни, зокрема Німеччина та США, запропонували новий погляд на те, як компанії ведуть бізнес. Завдяки горизонтальній та вертикальній інтеграції IT, поєднанню різних технологій, створенню кіберсистем і штучного інтелекту бізнес-моделі змінюються. Це відображається в змінах у світових рейтингах компаній, де з 2015 року серед найбагатших почали домінувати програмні та сервісні компанії, а не традиційні нафтові, газові чи металургійні компанії.

З цієї причини виникла концепція «4-ї промислової революції», яка відзначає зміни бізнес-моделей завдяки новим технологіям. З часом цей термін став більш загальним і почав охоплювати не тільки промисловість, а й міську інфраструктуру (Smart City), освіту, охорону здоров’я та інші сфери. До того ж, до спектра технологій додалися нові, такі як 3D-друк, нано-, біо- та енергоефективні технології.

Таким чином, зміни у всіх сферах життя почали називати «4-ю промисловою революцією», оскільки ці технології створюють новий етап розвитку суспільства, який значно відрізняється від попередніх. Відповідно, термін Industry 4.0 фокусується на нових технологіях і моделях виробництва, зокрема на таких платформах, як у Німеччині, що включають чотири ключові області змін: Інтернет речей (IoT), аналітику великих даних (Big Data), підключені машини і штучний інтелект.

Індустрія 4.0 стала можливою завдяки ряду технологій, які радикально змінили традиційні виробничі процеси, забезпечуючи швидке прийняття рішень та підвищення ефективності й продуктивності в різних секторах промисловості.

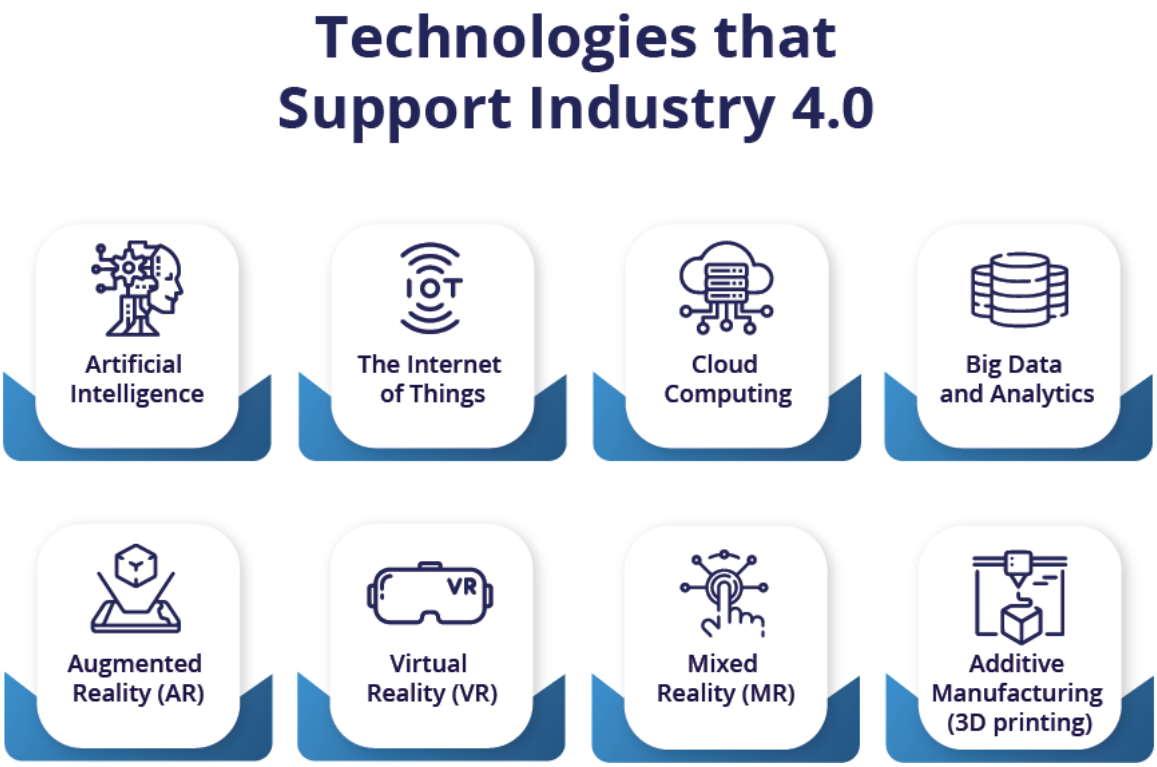

Рисунок 1.9 – Технології, що підтримують Індустрію 4.0 [3]

Індустрія 4.0 характеризується повною автоматизацією виробничих процесів, де управління здійснюється в реальному часі з урахуванням змінюваних зовнішніх умов. Кіберфізичні системи створюють віртуальні моделі фізичних об'єктів, здійснюють контроль за фізичними процесами та приймають децентралізовані рішення. Вони здатні взаємодіяти в реальному часі, самонастроюватися і самонавчатися. Важливу роль у цьому процесі відіграють інтернет-технології, що забезпечують зв'язок між людьми та машинами. Завдяки таким системам підприємства можуть виробляти продукцію, що відповідає вимогам конкретних замовників, оптимізуючи при цьому витрати на виробництво.

Індустрія 4.0 принесла революційні зміни у промисловість. Це дозволило виробникам підвищити ефективність, продуктивність і точність, одночасно зменшивши час простою та кількість помилок. Однак МСП часто стикаються з кількома проблемами, пов’язаними з цими новими технологіями. Деякі з найважливіших проблем, з якими стикаються МСП в Індустрії 4.0:

Кібербезпека

Оскільки МСП все більше покладаються на цифрові технології, вони стають більш вразливими до кібератак. Багатьом малим і середнім підприємствам бракує ресурсів, щоб інвестувати в комплексні заходи кібербезпеки, що робить їх особливо вразливими до витоків даних, атак програм-вимагачів та інших загроз кібербезпеці.

Навчання робочої сили

Швидкі темпи технологічних змін в Індустрії 4.0 вимагають від малих і середніх підприємств інвестувати в навчання співробітників, щоб підтримувати їхню робочу силу в курсі найновіших технологій. Однак багато малих і середніх підприємств можуть не мати ресурсів для проведення такого типу навчання.

Управління даними

Зі збільшенням кількості цифрових даних, створених технологіями Industry 4.0, малим і середнім підприємствам необхідно інвестувати в рішення для управління даними, щоб зберігати, аналізувати та ефективно використовувати ці дані. Однак багато малих і середніх підприємств можуть не мати ресурсів або досвіду для керування цими даними.

Інтеграція нових технологій

Інтеграція нових технологій у існуючу діяльність може стати проблемою для МСП. Це вимагає інвестицій у нове обладнання, програмне забезпечення та навчання, що може бути дорогим і трудомістким.

Управління ланцюгом поставок

Технології Industry 4.0 можуть забезпечити кращу видимість і ефективність ланцюжка поставок. Однак малим і середнім підприємствам може бути важко впровадити ці технології через брак ресурсів або співпраці з іншими підприємствами в ланцюжку постачання.

За прогнозами Всесвітнього Економічного Форуму, більшість технологій Четвертої революції стане повсякденністю вже в 2027 році. А це означає, що з'являться не тільки розумні будинки, а й розумні міста, безпілотні автомобілі на вулицях, штучний інтелект в офісах і суперкомп'ютери в кишенях.

Революція завершується успішно тільки в тому випадку, якщо вона:

а) добре організована;

б) щедро профінансована.

Подбати про це повинні ті, кому революція може принести найбільші дивіденди. Головні переваги при переході до нового технологічного укладу отримають ті підприємства, корпорації та навіть держави, які раніше інших впровадять не окремі компоненти, перераховані вище (і супутні їм), але, значною мірою, їх усі.

Тільки на перший етап цієї програми (підготовка бази для запуску процесу) урядом Німеччини було асигновано 200 млн євро, ще 300 млн виділив бізнес. Передбачалося, однак, що в подальшому бізнес буде працювати за цією програмою самостійно і до 2020 року в технології, що відносяться до Індустрії 4.0, щорічно буде інвестуватися 30-40 млрд євро. В цілому європейські інвестиції можуть скласти 140 млрд євро на рік.

В Японії створено Національний інститут просування цифрової економіки і цифрового суспільства (Japan Institute for Promotion of Digital Economy and Community, JIPDEC).

Найбільші компанії США – AT&T, Cisco, GE, IBM і Intel – в 2014 році створили Консорціум промислового Інтернету (Industrial Internet ConsortiumTM, IIC), відкриту некомерційну групу, яка за станом на початок 2017 року об'єднувала вже 250 компаній з 30 країн. Основне завдання Консорціуму – створення екосистеми компаній, наукових центрів і державних структур, сприятливою для впровадження індустріального Інтернету.

Згідно з прогнозом компанії McKinsey, до 2025 року сукупний економічний ефект від впровадження тільки промислового інтернету складе до 11 трлн доларів на рік. Значить, ті компанії, які вже сьогодні беруть активну участь у Четвертій промислової революції, отримають відчутні конкурентні переваги вже завтра.

В Україні в існуючих реаліях бізнес на допомогу держави навряд чи може розраховувати. Проте щось у напрямку переходу до Індустрії 4.0 все ж

робиться. Створено рух «Індустрія 4.0 в Україні», велику увагу цим питанням приділяє АППА (Асоціація підприємств промислової автоматизації України). На згаданій промисловій виставці в Ганновері представники компанії IT-Enterprise із задоволенням відзначили, що модуль «Виробництво» та інші модулі ERP-системи IT-Enterprise вже вирішують завдання Індустрії 4.0, причому роблять це результативніше, ніж аналогічні системи конкурентів. А на форумі в Гонконзі в 2016 році представники 200 компаній, що займаються впровадженням технологій Індустрії 4.0, з подивом дізналися, що деякі проблеми, до яких вони тільки приступають, компанією IT-Enterprise вже вирішені і її фахівці готові повідомити про досягнуті результати.

«Індустрія 4.0» – термін, введений для опису комп’ютеризації виробництва. Він поєднує в собі три технологічні тенденції, спрямовані на підвищення продуктивності та підвищення ефективності. Наприклад, штучний інтелект і машинне навчання можуть скоротити роботу людини, автоматизуючи завдання та дозволяючи людям-операторам зосередитися на системах моніторингу. Це може збільшити прибуток і продуктивність. Це також може зменшити капітальні витрати, забезпечуючи прогнозне та профілактичне обслуговування.

Штучний інтелект (ШІ) вже змінює спосіб нашої взаємодії з комп’ютерами. Це може допомогти компаніям створювати кращі продукти та вдосконалювати процеси. Це також може знизити витрати та підвищити якість продукції. Ця тенденція відома як Індустрія 4.0 і є четвертою промисловою революцією. Базовими технологіями, які забезпечують Industry 4.0, є цифрові технології, такі як Інтернет речей (IoT), хмарні обчислення та аналітика.

Технології ШІ – це фактор, що нівелює чинник дешевої робочої сили. Формат Індустрії 4.0 трансформує їх від дотримування певних алгоритмів, до здатності – змінювати. Приміром, завдяки роботизації компанія «Tesla» розгорнула свої потужності у Каліфорнії. Це виявилося дешевше, аніж виробляти і транспортувати машини з Піднебесної.

У 2019-му капіталізацію глобального ринка Industry 4.0 оцінювали в $71,7 млрд. За розрахунками аналітиків «Research and Markets», до 2024-го цей показник сягатиме $156,6 млрд. Таким чином, середньорічне зростання складає майже 17 %.

З огляду на це розвинені країни підтримують згаданий концепт як довготривалий тренд. Приміром, в Ізраїлі цим опікується Агенція інновацій. Там надають підприємцям кейси практичних інструментів чи доступ до структурних фондів для інноваційних екосистем. Це заохочує їх впроваджувати інновації. Мета – досягнути конкурентних переваг на місцевих та глобальних ринках. У результаті Ізраїль посів друге місце у звіті Всесвітнього Економічного Форуму 2016-го щодо глобальної конкурентоздатності. Там створюють найбільше у світі стартапів на душу населення.

Зрештою, повернемося до українського виміру «Індустрії 4.0». На жаль, позиції України невтішні. За даними Держстату України у 2020-му частка підприємств високотехнологічного сектору у структурі доданої вартості за попередні чотири роки скоротилася з 1,9 % до 1,2 %. Це засвідчує зворотні процеси у розвитку логістики і виробничої автоматизації.

З огляду на високі військові ризики, просування в Україні «Індустрії 4.0» є стратегічним маркером з підвищення технологічності реального сектору. Для швидкого запровадження потрібна синергія трьох чинників: державного апарату, бізнесу й освітньої системи. Аналіз Асоціації підприємств промислової автоматизації свідчить про імовірність зростання виробництва на 7–10 % за умови переходу України до Індустрії 4.0.

1.5 Яку вигоду можна отримати від використання передових технологій Четвертої промислової революції (Індустрія 4.0)

Від масового налаштування та виробництва до розширеної аналітики даних і прогнозованого обслуговування, передові технології на розумних фабриках пропонують істотні переваги.

Масове виробництво та налаштування. Цифрова трансформація скорочує час виробництва та прискорює обмін даними та інформацією.

Відстеження та прогнозне технічне обслуговування. Застосування передових технологій, таких як обробка аудіо та комп’ютерне бачення, забезпечує постійний моніторинг обладнання та виробничих ліній у реальному часі. Це може допомогти відстежити шлях продукту для майбутньої оптимізації. Постійний моніторинг дозволяє виявляти аномалії в роботі обладнання та швидко реагувати, щоб уникнути збоїв і тривалих простоїв виробничої лінії.

Віртуалізація та децентралізація. Методи віртуалізації в Industry 4.0, такі як хмарні обчислення, забезпечують масштабовані обчислювальні ресурси та послуги через Інтернет. Хмарні обчислення є надійним інструментом для зберігання даних, аналітики в реальному часі, платформ для співпраці та рішень програмного забезпечення як послуги (SaaS).

Промисловий Інтернет речей (IIoT) дозволяє децентралізувати операції. Це допомагає у відстеженні активів, моніторингу в реальному часі та децентралізованому прийнятті рішень, дозволяючи пристроям спілкуватися. Він надає цінну інформацію та допомагає вам адаптуватися до мінливих ринкових змін завдяки розподіленому прийняттю рішень, які не потребують централізованого затвердження. Удосконалені адаптивні алгоритми в децентралізованих системах можуть передбачати ринкові тенденції та відповідним чином коригувати графіки виробництва, забезпечуючи точнішу відповідність пропозиції попиту.

Підвищена продуктивність і ефективність. Впровадження IoT із підтримкою ШІ може значно скоротити ручну працю та збільшити швидкість виробництва. Датчики Інтернету речей і прогнозна аналітика безперервно контролюють працездатність обладнання, передбачаючи несправності до їх виникнення та завчасно плануючи технічне обслуговування, скорочуючи час простою обладнання та подовжуючи його термін служби.

Покращена стійкість. Передові технології в Industry 4.0 дозволяють ефективніше управляти ресурсами та зменшувати відходи за рахунок автоматизації процесів і віддалених операцій. Датчики IoT сприяють економії енергії, автоматично контролюючи приціл, вмикаючи його лише за потреби. Алгоритми штучного інтелекту можуть безперервно аналізувати моделі використання енергії для оптимізації процесів і прогнозування майбутніх потреб. Інструменти розробки програмного забезпечення допомагають перейти до більш стійкого процесу проєктування та виробництва.

Оптимізоване управління ланцюгом поставок. Штучний інтелект і машинне навчання є ключовими складовими сучасної промисловості та оптимізованого ланцюжка поставок. Алгоритми забезпечують точні прогнози, оптимізують рівень запасів, покращують відносини з постачальниками та оптимізують логістичні операції. Це дозволяє краще реагувати на зміни ринку, зменшити операційні витрати та підвищити ефективність ланцюжка поставок.

Висновок до розділу 1

Одна з характерних рис Індустрії 4.0 полягає в повній автоматизації виробничих процесів, де управління усіма операціями відбувається в реальному часі з урахуванням змін, що відбуваються в зовнішньому середовищі.

Оскільки поняття «розумне виробництво» досить розпливчасте, а перехід до нього відбувається в кілька етапів, що займають не один рік, робляться спроби розділити це поняття на три. Так, Е. Філос, координатор ІКТ-проєктів в сьомій рамковій програмі Європейського Союзу з науково-технічного співробітництва, розділяє фабрики майбутнього на три основних типи – цифрові (Digital), «розумні» (Smart) і віртуальні (Virtual) [26].

Отже, важливо відзначити, що при впровадженні оцифровки на підприємстві керівникам слід спочатку чітко визначити загальні цілі компанії та стратегічні напрями її розвитку. Це дозволить сконцентрувати увагу на найбільш ефективних бізнес-процесах для здійснення діджиталізації, що забезпечить максимальний результат.

2 АПАРАТНА СКЛАДОВА ПРАКТИЧНОЇ ЧАСТИНИ

У контексті Індустрії 4.0, система безпеки відіграє важливу роль у забезпеченні цілісності виробничих процесів, захисту фізичних та цифрових активів, а також забезпечення безпеки даних та персоналу. Враховуючи впровадження новітніх технологій, таких як Інтернет речей (IoT), автоматизація, кіберфізичні системи (CPS), великі дані, штучний інтелект (AI) та робототехніка, забезпечення безпеки стає більш складним і багатогранним завданням.

Основні аспекти системи безпеки в Індустрії 4.0 та виробничих процесах включають фізичну безпеку, кібербезпеку, захист даних, автоматизацію безпеки та інтеграцію з іншими виробничими системами.

Тому практична частина була заснована на побудові та опису системи контролю та управління доступом (СКУД), системи відеоспостереження та домофонії які є одними із засобів забезпечення безпеки.

2.1 Система керування та управління доступом турнікет

СКУД-турнікет – це система безпеки, що використовує фізичні бар'єри (турнікети) разом із технологіями контролю доступу для обмеження і моніторингу доступу до певних територій або приміщень. Така система зазвичай застосовується в бізнес-центрах, промислових об'єктах, комерційних та державних установах, де важливо регулювати потік людей і забезпечувати доступ тільки авторизованим користувачам.

Для даної системи було використано наступні складові:

Турнікет (рис. 2.1)

Рисунок 2.1 – Турнікет-трипод Hikvision DS-K3G501-R/M-Dm55

Турнікет-тринога призначений для виявлення несанкціонованого входу або виходу. В ІС, де турнікет інтегрований із СКУД, особа повинна пройти автентифікацію, щоб пройти смугою, протягнувши ІС або ID-картку, відсканувавши QR-код тощо. Він широко використовується в історичних пам’ятках, на стадіонах, будівельних майданчиках, у житлових приміщеннях тощо.

Основні характеристики

- 32-бітний високошвидкісний процесор;
- мережевий зв'язок за стеком протоколів TCP/IP. Дані зв'язку спеціально зашифровані, щоб зняти занепокоєння щодо витоку приватної інформації;
- можливість вибору відкритого/закритого режиму;
- двонаправлена (вхід / вихід) смуга. Швидкість відкриття та закриття шлагбаума можна налаштувати відповідно до потоку відвідувачів;
- самовиявлення, самодіагностика та автоматична сигналізація;
- дистанційний контроль і керування;
- робота в режимі онлайн/офлайн;
- світлодіод відображає стан входу/виходу та проходу;
- при вимкненому живленні шлагбаум знаходиться у вільному стані. Люди можуть проходити через смугу в односторонньому/односторонньому та двосторонньому напрямках;
- пропуск за пожежною тривогою. У разі спрацювання пожежної сигналізації шлагбаум автоматично опускається для екстреної евакуації;
- налаштування тривалості проїзду. Система скасує дозвіл на прохід, якщо людина не пройде через смугу протягом допустимого часу проходу;
- відкриває/закриває шлагбаум відповідно до шаблону розкладу;
- можна додати до 3’000 карток відвідувачів і до 60’000 карток, крім карток відвідувачів;
- можна записати до 180’000 подій пред'явлення карток;
- регульована яскравість підсвічування стрічки.

Картка (рис. 2.2)

Рисунок 2.2 – Картка Mifare Classic 1K 13,56 MHz (ISO)

Картки, що працюють на частоті 13,56 МГц, виконані за стандартом ISO14443A та популярні завдяки наявності шифрування і можливості запису додаткової інформації у пам'ять. Кожна картка має свій унікальний UID-номер. На відміну від EM-Marine, картку Mifare практично неможливо скопіювати, що є ключовою перевагою для СКУД. Дана картка допускає нанесення текстового і графічного зображення на поверхню за технологією термодрук, офсетний друк або шовкографія.

Крім UID, картка має 1 кбайт пам'яті, для запису інформації користувача. Наприклад, ПІБ користувача, його номер облікового запису, баланс, період дії картки або навіть шаблон біометричних даних.

Основні сфери застосування безконтактних карток Mifare 1k

- верифікація прав користувача в обладнанні управління доступом
- використання як проїзних карт в транспорті
- використання для оплати послуг платних автобанів;
- плата за паркування, стоянку автомобіля;
- як балансові карти на послуги готелів, розважальних комплексів, і т. п.

Технічні характеристики білої картки Mifare 1k

- Стандарт: ISO14443A
- Пам'ять: підтримую перезапис, читання і запис

- Ємність пам'яті: 1024 байт
- Габарити: 85,4 мм x 54,0 мм x 0,8 мм
- Матеріал: ПВХ
- Допустима вологість: 95 %
- Температура експлуатації: від мінус 30 °C до + 70 °C.

Пристрій для введення карт (рис. 2.3)

Рисунок 2.3 – Hikvision USB-пристрій для введення карт DS-K1F100-D8E

DS-K1F100-D8E — це універсальний пристрій для зчитування карток, який використовується для введення пропускних карт у систему безпеки. Пристрій підключається через USB і дозволяє зберігати нові картки в існуючих охоронних системах. Основною функцією є первинна реєстрація чіпів карток у популярних форматах, таких як Mifare, EM і CPU. Після інтеграції з системою, кардридери будуть розпізнавати картки мешканців і співробітників, що використовують автоматичні термінали для входу. DS-K1F100-D8E оснащений індикацією стану, а його налаштування займають мінімум часу, що дозволяє швидко розпочати роботу без складних конфігурацій.

В рамках Індустрії 4.0 СКУД-турнікет може бути інтегрований в загальну автоматизовану систему управління підприємством. Всі процеси, від ідентифікації до реєстрації доступу, можуть бути автоматизовані та звітуватися у реальному часі. Також ця система може включати в себе контроль робочого часу та містить anti passback. Анті-пасбек (Anti-Passback) – це функція в системах контролю доступу, яка забезпечує додатковий рівень безпеки,

запобігаючи можливості передавання карток чи інших засобів ідентифікації між людьми для обходу системи безпеки.

Простими словами, анті-пасбек дозволяє гарантувати, що людина, яка вийшла з контрольованої зони через турнікет або інший контрольний пункт, не може одразу увійти знову без дотримання певних правил.

2.2 Система керування та управління доступом «двері»

СКУД «двері» (Система контролю та управління доступом дверей) – це система безпеки, яка обмежує доступ до приміщень або зон за допомогою дверей, оснащених елементами контролю доступу. Основна мета СКУД «двері» – це забезпечення безпеки та контрольованого доступу в будівлі чи на території. Ця система контролю була встановлена з використанням наступних складових:

Контролер для однієї двері (рис. 2.4)

Рисунок 2.4 – Hikvision Контролер для однієї двері DS-K2601T

DS-K2600 – це потужний і стабільний контролер доступу, що використовує логічну архітектуру. DS-K2600 оснащений мережевим інтерфейсом TCP/IP, його сигнал обробляється за допомогою спеціального шифрування і може працювати в автономному режимі. Також підтримується функція захисту від несанкціонованого доступу.

Основні характеристики:

- контролер доступу оснащений 32-бітним високошвидкісним процесором;
- підтримує TCP/IP та GPRS мережеву комунікацію, доступ до Ehome. Дані комунікації спеціально шифруються для зменшення ризику витоку приватності;

- підтримує розпізнавання та зберігання номерів карток максимальним довжиною 20 символів;
- контролер доступу може зберігати 100 тис. дійсних карток (97 тис. звичайних карток та 3 тис. карток відвідувачів) і 300 тис. записів про зчитування карток;
- підтримує функцію багатодверного зворотного зв'язку, функцію антипроходу, функцію багатокартковості, функцію відкриття першою карткою, функцію суперкарти та суперпароля, шифрування карт M1, функцію онлайн-оновлення та дистанційного керування дверима;
- підтримує сигналізацію проти несанкціонованого доступу для зчитувача карток, сигналізацію для незакритих дверей, сигналізацію при насильному відкритті дверей, сигналізацію при таймауті відкриття дверей, сигналізацію для картки та коду в умовах примусу, сигналізацію чорного списку та сигналізацію при спробах несанкціонованого зчитування карток, які досягли межі;
- вхідний сигнал контролера підтримує функцію захисту від короткого замикання та функцію захисту від різання;
- кілька методів завантаження подій: канал, група центру та прослуховування;
- 50 зв'язків подій та карток;
- виявлення конфлікту IP-адреси.
- функція протидії зворотному проходу між контролерами та внутрішня функція протидії зворотному проходу. Для протидії зворотному проходу між контролерами на основі картки необхідно з'єднати зчитувач карток через RS-485. Для протидії зворотному проходу між контролерами на основі мережі необхідно правильно з'єднати сервер та пристрій. Можна зберігати до 5’000 записів про зчитування карток на вибраному сервері;
- підтримує інтерфейс RS-485 та інтерфейс Wiegand для доступу до зчитувача карток. Інтерфейс RS-485 має двосторонній дизайн та підтримує виявлення обриву петлі та функцію резервування; інтерфейс Wiegand

підтримує W26, W34 і безперешкодно сумісний з зчитувачами карток сторонніх виробників з інтерфейсом Wiegand;

- підтримує різні типи карток: звичайні, вимкнені, чорний список, патрульні, гостьові, картки в умовах примусу, суперкарти тощо;
- різноманітні індикатори для відображення різних станів;
- підтримує синхронізацію часу через NTP, ручний або автоматичний метод;
- підтримує функцію зберігання записів під час офлайн-режиму та сигналізацію про недостатнє місце для зберігання;
- контролер доступу має резервне живлення, конструкцію з контрольним механізмом та функцію захисту від зловживань;
- пані можуть зберігатися постійно після вимкнення контролера доступу;
- підтримує зв'язки I/O та зв'язки подій;
- підтримує протокол EHome та міжмережеву комунікацію;
- 500 груп паролів у режимі автентифікації картки та пароля.

Зчитувач (рис. 2.5)

Рисунок 2.5 – Зчитувач Hikvision DS-K1109DKB-QR

Підтримує протоколи RS-485 та Wiegand (W26, W34); читання карти Desfire, карти Felica та карти M1; автентифікація по карті, паролю та QR-коду; Bluetooth-модуль; Функція захисту від несанкціонованого доступу

Електромагнітний замок (рис. 2.6)

Рисунок 2.6 – Електромагнітний замок Yli Electronic YM-280(BLED)

Електромагнітний замок Yli Electronic YM-280(BLED) призначений для підвищення безпеки різних типів дверей: металевих, пластикових, дерев'яних та скляних. Він забезпечує надійну блокування з утримувальною силою до 280 кг, що робить його ідеальним для офісів, складів та інших комерційних приміщень. Замок працює від постійного струму 12/24 В та оснащений двоколірним світлодіодним індикатором стану, а також системою моніторингу статусу блокування (NO-NC-COM).

Корпус виконаний з анодованого алюмінію, а відповідна планка – з нержавіючої сталі, що забезпечує довговічність і стійкість до корозії. Простий накладний монтаж за допомогою комплектуючих аксесуарів і монтажного куточка MBK-280UL (не входить у комплект) робить установку швидкою та ефективною.

Замок призначений для використання в приміщеннях. Компактні розміри та невелика вага роблять його зручним для установки та інтеграції в існуючі системи контролю доступу. Такі характеристики роблять його стабільним та надійним рішенням для захисту вашого об'єкта від несанкціонованого доступу.

Основні переваги:

- **Висока утримувальна сила:** Електромагнітний замок Yli Electronic YM-280(BLED) забезпечує утримувальну силу до 280 кг, що гарантує надійне блокування дверей різних типів.
- **Двоколірний світлодіодний індикатор:** Наявність світлодіодного індикатора дозволяє легко відстежувати стан замка, забезпечуючи візуальний зворотний зв'язок про стан блокування.
- **Простота установки:** Замок монтується накладним способом і постачається з повним комплектом кріпильних аксесуарів, що робить установку швидкою та зручною без необхідності в спеціалізованих інструментах.
- **Надійна конструкція:** Корпус замка виконаний з анодованого алюмінію, а відповідна планка з нержавіючої сталі, що забезпечує довговічність і стійкість до корозії, роблячи замок ідеальним для тривалого використання.

Технічні характеристики:

- монтаж: накладний на поверхню;
- моніторинг: статус блокування NO-COM-NC;
- Режим роботи: Fail-safe;
- Напруга живлення: 12/24 В постійного струму;
- Споживаний струм: 540/250 мА (12 В постійного струму) ;
- Потужність: 6,48 Вт;
- Сила утримання: 280 кг (2746 Н) ;
- Матеріал: анодований алюміній;
- Відповідна планка: нержавіюча сталь;
- Розмір замка, мм: 252,5 × 43,8 × 27,9;
- Розмір замка (з кронштейном), мм: 252,5 × 48,8 × 27,9;
- Розмір відповідної планки, мм: 180 × 38,8 × 13,2;
- Робоча температура: від мінус 10 °C до + 55 °C;
- вологість: < 90 %;
- вага брутто: 2,1 кг.

Охоронний точковий магнітоконтактний датчик (рис. 2.7)

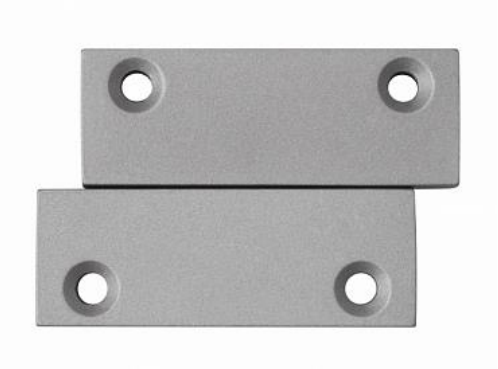

Рисунок 2.7 – HIKVISION DS-PD1-MC-MS

Охоронний точковий магнітоконтактний датчик для металевих дверей: контакти розмикаються при тривозі. Якщо відстань 40 мм і менше — контакти замкнуті, 40 мм і більше — контакти розімкнені:

- розрахунок потужності: Р-комут. 100 Вт, І-комут. 500 мА;
- температура роботи: від мінус 40 °C до + 65 °C;

- розміри: 50 мм × 18 мм × 10 мм (геркон), 50 мм × 18 мм × 10 мм (магніт) ;
- Матеріал корпусу: метал.

Бездротове реле з сухим контактом (рис. 2.8)

Рисунок 2.8 – Бездротове реле з сухим контактом Ajax Relay

Ajax Relay дозволяє автоматизувати різні процеси та дистанційно керувати пристроями через застосунок Ajax Security System. Наприклад, можна відкривати шлагбауми або ворота, автоматично закривати штори й ролети при виході з дому або налаштувати сценарій, при якому замикатимуться електрозамки під час активації охоронної системи. Також можливо віддалено перезавантажувати пристрої, наприклад, роутери, і миттєво перекрити подачу води або газу у разі спрацювання відповідного датчика.

Принцип роботи Ajax Relay полягає в тому, що він замикає й розмикає контакти через застосунок або автоматично за сценарієм при активації охоронної системи. Реле здійснює моніторинг температури та напруги в реальному часі, зокрема напруги підключених пристроїв. У разі перегріву або стрибків напруги, реле автоматично відключає контакти і надсилає тривожне повідомлення. Наприклад, при температурі понад + 65°C в приміщенні або + 85°C всередині корпусу реле, а також при порогових значеннях напруги (менше 6,5 В або більше 36,5 В), спрацьовує захист.

Після нормалізації температури або напруги реле відновлює роботу та інформує користувача.

Особливості та функції Ajax Relay

- безпотенційний сухий контакт для вмикання і вимикання приладів або пристроїв з живленням від джерела 7–24 В DC;
- бістабільний та імпульсний режими роботи;
- захищений від перегріву і перепадів напруги;
- виносна антена;
- мініатюрний корпус для зручної установки навіть всередині підрозетника.

Модуль управління (рис. 2.9)

Рисунок 2.9 – Hikvision Модуль управління DS-K2M061

DS-K2M061 Secure Door Control Unit – це проміжний пристрій між терміналом контролю доступу та замком, який включає магніт для дверей, замок, кнопку виходу тощо. Він може використовуватися для забезпечення закриття дверей у разі їх пошкодження;

- спілкується з терміналом контролю доступу через RS-485 для виконання команд, таких як відкриття дверей, закриття дверей, нормально відкритий та нормально закритий режим;
- збирає сигнал від магніту дверей, сигнал кнопки виходу та сигнал захисту від несанкціонованого доступу, передаючи їх на термінал контролю доступу;
- підтримує сигналізацію при спробі несанкціонованого доступу;
- підтримує індикатори комунікації RS-485 для відображення статусу зв'язку;
- має 4-канальний DIP-перемикач для налаштування ID номерів;

– підтримує інтерфейс Wiegand для підключення зчитувача карт Wiegand, що дозволяє входити/виходити з терміналу контролю доступу шляхом зчитування картки;

– підключення до системи пожежної безпеки та кнопки виходу.

СКУД дверей є важливою складовою системи безпеки для забезпечення контролю доступу та захисту приміщень від несанкціонованого проникнення. Вона має широкий спектр застосувань в різних галузях і може інтегруватися в загальну систему безпеки підприємства або організації.

2.3 Домофонія

Домофонія – це система аудіо- або відео зв'язку, яка використовується для комунікації між людьми, що знаходяться всередині будівлі або приміщення, і тими, хто перебуває за її межами. Домофонія є частиною системи безпеки та контролю доступу і часто використовується в багатоквартирних будинках, офісних центрах, житлових комплексах, а також у інших місцях, де необхідно контролювати вхід та здійснювати зв'язок з відвідувачами.

Основні компоненти домофонної системи:

IP-відеодомофон (рис. 2.10).

Рисунок 2.10 – IP-відеодомофон с Android DS-KH9510-WTE1

IP-відеодомофон Hikvision DS-KH9510-WTE1 – це обладнання, призначене для контролю та управління доступом на об'єктах різного

призначення. Завдяки своїм технічним можливостям, подібне обладнання стане просто незамінним рішенням в квартирах, офісних приміщеннях, приватних будинках і на інших об'єктах. На відміну від класичного домофона, за допомогою відеодомофона ви можете не тільки почути, але і бачити, хто прийшов до вас. Це спрощує ідентифікацію гостя.

Особливості IP-видеодомофона Hikvision DS-KH9510-WTE1:

- Установлений 10-дюймовий сенсорний екран з IPS, який вражає яскравістю та чіткістю зображення;
- Розширення дисплея 1024 × 600 пікселів, що дозволяє детально розглянути, хто прийшов на об'єкт;
- В відеодомофоні є всенаправлений мікрофон, що забезпечує двосторонній голосовий зв'язок;
- Підтримка захоплення зображення під час відеозв'язку через домофон DS-KH9510-WTE1;
- В конструкції є 8 датчиків тривоги, що суттєво підвищує ефективність системи контролю та управління доступом;
- Підтримує стандарт PoE, тому монтаж займає мінімум часу – достатньо підключити тільки кабель «вита пара» ;
- Працює на базі операційної системи Android, що робить інтерфейс зручним для користування;
- Має 4 Гбайт вбудованої пам'яті та 1 Гбайт оперативної пам'яті для швидкої роботи та збереження фото/відео;
- Сенсорний екран забезпечує максимально комфортне користування домофоном;
- Є можливість підключення до інтернету через Wi-Fi або мережевий інтерфейс RJ-45, залежно від уподобань користувача;
- Призначений для внутрішньої установки, витримує температури від мінус 10 °С до +50 °С.

Індивідуальна виклична панель (рис. 2.11)

Рисунок 2.11 – Hikvision 2МП IP панель
DS-KD8003-IME1(B)/Surface/Europe BV

Індивідуальна виклична панель з механічною кнопкою, що підтримує двосторонній аудіозв'язок, PoE та нічне ІЧ-підсвічування. Оснащена вбудованою 2 Мп камерою з кутом огляду 146°. Панель призначена для накладного монтажу і може використовуватися як всередині приміщень, так і на вулиці

Модуль з картрідером (рис. 2.12)

Рисунок 2.12 – Hikvision Модуль з картрідером DS-KD-M

DS-KD-M — це розширювальний модуль-картридер, призначений для зчитування брелків і карток для доступу в контрольовані приміщення. Цей пристрій підключається до викликових терміналів та домофонних систем. Завдяки чорному інтерфейсу, модуль можна використовувати як накладний або

вмонтувати в стіну, що забезпечує додатковий захист і естетичний вигляд. Поверхня модулю оснащена чутливими датчиками, що здатні розпізнавати авторизовані ключі та реагувати на них відповідно.

DS-KD-M споживає мінімальну кількість енергії, живлячись від інших підключених модулів. Установка такого пристрою значно підвищує рівень безпеки будівлі або її окремих приміщень. Модуль має високий клас захисту, високу швидкість роботи і точність ідентифікації карток.

GSM Ключ RC-1000 (рис. 2.13)

Рисунок 2.13 – GSM Ключ RC-1000

GSM-модуль – це радіоприймач у GSM-діапазоні, який оснащений SIM-карткою мобільного оператора та контролером для обробки інформації.

Як це працює: У пам'яті модуля зберігаються телефонні номери осіб, які мають доступ до закритої території. Якщо ваш номер є в цьому списку, GSM-модуль розпізнає його і відправляє сигнал блоку управління для відкриття воріт або підняття шлагбаума, імітуючи натискання кнопки на пульті дистанційного керування.

Важливо зазначити, що, коли пристрій приймає дзвінок і відкриває ворота, з'єднання не встановлюється або обривається через кілька секунд, тому оплата за дзвінок не стягується. Це дозволяє використовувати будь-яку SIM-картку без додаткових витрат. Якщо ж номер не знаходиться в списку дозволених, дзвінок буде скинуто без реакції пристрою. Однак у деяких

моделях є функція, яка дозволяє відкрити ворота при будь-якому вхідному дзвінку, навіть без перевірки номера.

Особливості пристрою

- Максимальна кількість номерів - 1000;
- Максимальне споживання - 200 мА;
- Стандарт зв'язку 900/1800 МГц;
- Дальність роботи - не обмежена;
- Світлодіодна індикація;
- Захист від неправильного підключення.

Кнопка виходу (рис. 2.14)

Рисунок 2.14 – Кнопка виходу Yli Electronic YKS-850M Yli Electronic 17211

YKS-850M — це кнопка контактного типу, призначена для відкриття дверей у місцях з великою кількістю людей, таких як проходи. Кожен користувач має унікальний ключ для посилення безпеки доступу. Кнопка витримує до 500,000 натискань, що гарантує її надійність і довговічність. Виходи NO/NC/COM дозволяють підключати відеодомофон, контролер, клямку або електрозамок для забезпечення зручного та безпечного доступу.

Домофонія є важливою складовою систем безпеки, яка дозволяє ефективно контролювати доступ до будівель, підвищує рівень комфорту та знижує ризик несанкціонованого проникнення. Її використання є популярним у різних сферах і сприяє покращенню безпеки в житлових та комерційних приміщеннях.

2.4 Система відеоспостереження

Система відеоспостереження (CCTV) – це технологічна система, що використовує камери для моніторингу, запису та трансляції відео з метою забезпечення безпеки та контролю за певною територією або об'єктами. Відеоспостереження є важливою складовою системи безпеки, що дозволяє фіксувати події, здійснювати моніторинг ситуації в реальному часі та виявляти порушення або небезпечні ситуації. В нашому випадку ця система включає розпізнавання обличчя та створення подій.

Hikvision DS-2CD2087G2H-LIU(eF) – камера з високою роздільною здатністю 8МП та вбудованим мікрофоном (рис. 2.15). Оснащена подвійним підсвічуванням ColorVu для кольорового нічного бачення та технологією Smart Hybrid Light для запису кольорового відео при виявленні руху.

Рисунок 2.15 – Hikvision 8 МП ColorVu Smart Hybrid Light DS-2CD2087G2H-LIU(2,8мм)(eF)

Особливості камери Hikvision DS-2CD2087G2H-LIU(eF)

Камера з роздільною здатністю 8 МП (3840 × 2160) надає деталізоване зображення, що дозволяє бачити найдрібніші деталі навіть на великих відстанях. Завдяки об'єктиву з фокусною відстанню 2,8 мм досягається широкий огляд 105,1° по горизонталі, охоплюючи територію великої площі. Технологія WDR 130 дБ забезпечує чітке зображення навіть за яскравого контрового освітлення.

Технологія ColorVu гарантує якісне зображення як вдень, так і вночі. ІЧ-підсвічування та біле світло з радіусом дії до 40 метрів забезпечують відмінну видимість навіть у повній темряві. А технологія Smart Hybrid Light дозволяє отримати повнокольорове відео при виявленні руху автоматично включаючи LED-підсвічування.

Камера оснащена вбудованим датчиком руху та здатна класифікувати цілі, такі як людина та транспортний засіб. Вона виявляє рух, перетин лінії, вторгнення, забезпечуючи високий рівень безпеки. А вбудований мікрофон додає ще один рівень контролю.

Корпус камери водо- та пиленепроникний (IP67), що дозволяє встановити її поза приміщенням та гарантує якісне відеоспостереження за будь-яких погодних умов.

Технологія стиснення H.265+ заощаджує пропускну здатність мережі та місце у сховищі без втрати якості зображення. Вбудований слот для карти пам'яті обсягом до 512 Гбайт дозволяє зберігати записи безпосередньо на пристрої без використання додаткового мережевого сховища.

Технологія PoE дозволяє передавати дані та живлення по одному кабелю, що робить процес встановлення швидким та простим.

Рисунок 2.16 – Hikvision мікрофон для систем відеоспостереження DS-2FP2020

IP камера Hikvision DS-2CD2T63G2-4I призначена для встановлення на вулиці, відрізняється міцним алюмінієвим корпусом та ступенем захисту IP67, що забезпечує стійкість до несприятливих погодних умов (рис. 2.17).

Рисунок 2.17 – 6Мп AcuSense IP камера Hikvision DS-2CD2T63G2-4I

Основні характеристики

Камера оснащена 1/2.8-дюймовою CMOS-матрицею з роздільною здатністю 6 Мп (3200 × 1800) і підтримкою зйомки зі швидкістю 20 кадрів в секунду. з фокусною відстанню 2,8 мм. Камера підтримує сучасні кодеки H.265/H.264, а також їх удосконалені версії H.264+ та H.265+.

Додаткові функції та особливості

Пристрій обладнано ІЧ-підсвічуванням з дальністю до 80 метрів. Підтримуються функції повороту зображення, WDR, 3D DNR, HLC та BLC для покращення якості відео. слотом для microSD карт обсягом до 256 Гбайт, підтримує живлення через PoE має порт RJ45 10 M/100 M.

8Мп Acusense IP камера Hikvision DS-2CD2383G2-LI2U (2,8 мм) – рішення для відеоспостереження з високою якістю зображення і роздільною здатністю 8 Мп (рис. 2.18). Вона оснащена технологією Acusense, яка фокусується на класифікації людей і транспортних засобів на основі глибокого навчання, забезпечуючи точне і надійне виявлення рухомих об'єктів.

Рисунок 2.18 – Hikvision 8 Мп Acusense Smart Hybrid Light
з мікро DS-2CD2383G2-LI2U

Технологія Smart Hybrid Light інтегрує інфрачервоні та білі світла, забезпечуючи чітке зображення в будь-який час доби. Камера також оснащена вбудованими двома мікрофонами для високоякісного аудіо-контролю в реальному часі. Зображення залишається чітким навіть за сильного підсвічування завдяки технології 120 дБ істинного широкого динамічного діапазону (WDR). Ефективна технологія стиснення H.265+ допомагає оптимізувати використання простору для зберігання відеоматеріалів. Камера має клас захисту IP67 від води та пилу, що забезпечує надійну роботу в різних умовах експлуатації. Камера оснащена слотом для карти пам'яті, підтримуваний обсяг до 512 Гбайт.

DS-2CD2343G2-IU – 4 Мп мережева вулична відеокамера із вбудованим мікрофоном (рис. 2.19). Підтримує технологію AcuSense (інтелектуальний фільтр хибних тривог 2-ге покоління (реакція вторгнення в зону або перетин лінії тільки на авто або людини). Об'єктив монофокальний (2,8 мм). Можливість запису відео на карту пам'яті. Оснащена вбудованою EXIR-підсвічуванням (до 30 м).

Рисунок 2.19 – 4 MP AcuSense Turret IP DS-2CD2343G2-IU

Відеореєстратор NVR DS-7716NXI-K4/16P має 16 каналів (рис. 2.20). Кодаки H.265/H.265+/H.264+/H.264. Декодування: макс. 12 каналів × 1080p. Вхідний потік 160 Мбіт/с. Аналітика за рахунок NVR: розпізнавання облич, захист периметра (2 канали 4Мп), виявлення руху 2.0 (усі канали 4Мп).

Рисунок 2.20 – Hikvision 16-канальний 1.5U 16 POE K Series AcuSense 4K NVR DS-7716NXI-K4/16P

Аналітика за рахунок камери: розпізнавання облич, захист периметра (2 канали 4Мп), викидання предметів із будівлі, виявлення руху 2.0 (усі канали), ANPR, VCA. 4 HDD до 10 Тбайт.

Також для поставленої задачі було використано різні маршрутизатори, а саме:

- MikroTik RouterBOARD 3011UiAS (RB3011UiAS-RM);
- MikroTik CRS328-24P-4S+RM;
- MikroTik RB4011iGS+RM.

Система відеоспостереження з функцією розпізнавання обличчя та створення подій є потужним інструментом для забезпечення безпеки та контролю, який має значний потенціал для застосування в різних сферах, від комерційних об'єктів до громадських місць. СКУД – це не просто система, що контролює доступ до об'єктів, а інтегрований елемент в масштабні автоматизовані й цифрові екосистеми, який допомагає оптимізувати управління безпекою, підвищити ефективність і забезпечити високий рівень захисту.

В даному розділі були описані більша частина апаратної складової, і всі ці компоненти працюють разом, забезпечуючи високий рівень безпеки та ефективний моніторинг.

Висновок до розділу 2

У контексті Індустрії 4.0 апаратна складова системи безпеки є ключовим елементом, що забезпечує надійність, масштабованість та інтеграцію сучасних технологій. Використання розумних сенсорів, контролерів, пристроїв інтернету речей (IoT) та спеціалізованих обчислювальних платформ дозволяє створити ефективну систему моніторингу, управління ризиками та автоматизації процесів.

Інтеграція таких апаратних рішень із хмарними технологіями, великими даними (Big Data) та штучним інтелектом дозволяє не лише підвищити рівень безпеки, а й зменшити людський фактор, який часто є джерелом помилок. У результаті, правильно організована апаратна складова стає основою для впровадження комплексних систем безпеки, що відповідають вимогам сучасного виробництва та стандартам Індустрії 4.0.

Таким чином, апаратна частина не тільки підтримує базову функціональність системи, а й сприяє її адаптивності та довговічності в умовах швидких технологічних змін.

3 ФУНКЦІОНАЛЬНА АРХІТЕКТУРА ТА ПРОГРАМНА СКЛАДОВА

Для реалізації проєкту було використане обладнання китайської компанії Hikvision. Повне найменування – Hangzhou Hikvision Digital Technology Co., Ltd. Штаб-квартира компанії розташована в Ханчжоу. Hikvision – найбільший у світі постачальник продуктів для відеоспостереження та готових рішень з відеоспостереження. Будучи заснованою в 2001 році, компанія Hikvision сьогодні забезпечує роботу понад 60’000 співробітників, включаючи науково-дослідний штат в 40’000 чоловік.

Компанія Hikvision прагне обслуговувати різні галузі за допомогою передових технологій машинного розвитку, штучного інтелекту та великих даних, будучи лідером у сфері інтернету:

- за допомогою комплексних технологій машинного сприйняття прагнуть допомогти людям краще взаємодіяти з навколишнім світом;
- завдяки великій кількості інтелектуальних продуктів прагнуть виявити різноманітні потреби, які надають відповідну інформацію;
- інноваційні застосунки ринку AIoT (Artificial Intelligence of Things) дозволяють кожній людині насолоджуватись кращим майбутнім, створити більш зручний, ефективний і безпечний інтелектуальний світ.

Hikvision пропонує широкий спектр продуктів фізичної безпеки, що охоплюють системи відеобезпеки, контролю доступу та сигналізації. Вони також надають інтегровані рішення для забезпечення безпеки на базі технологій, які допомагають кінцевим користувачам отримувати нові застосункі та можливості для управління безпекою, в тому числі бізнес-аналітику. За останні кілька років поглибили свої знання та досвід у задоволенні потреб клієнтів на різних вертикальних ринках за допомогою професійних та інтелектуальних рішень, включаючи «розумне місто», транспорт, роздрібну торгівлю, логістику, енергетику та освіту. Крім того, Hikvision розширює свій бізнес до багатьох будинків, робототехніки, автомобільної електроніки, інтелектуального зберігання, пожежної безпеки, інфрачервоного виявлення,

рентгенівського виявлення та медичної візуалізації, щоб дослідити нові канали для підтримки довгострокового розвитку.

Компанія Hikvision створила одну з найбільш обширних маркетингових мереж у галузі, що складається з 72 дочірніх компаній і філій у всьому світі, щоб забезпечити швидке реагування на потреби клієнтів, користувачів і партнерів. Продукція Hikvision обслуговує широкий спектр вертикальних ринків, що охоплюють понад 150 сторінок.

Технологічна компанія Hikvision прагне обслуговувати різні галузі промисловості за допомогою передових машинних технологій, штучного інтелекту та великих даних, керуючи сферою AIoT, за допомогою комплексних технологій машинних технологій, допомагають людям краще взаємодіяти з навколишнім світом; за допомогою безлічі інтелектуальних продуктів, прагнуть виявити і задовольнити різноманітні потреби за допомогою інноваційних застосунків AIoT, також дати кожній людині можливість насолодитися кращим майбутнім, створити більш зручний інтелектуальний світ в умовах безпеки.

Маючи великий науково-технічний потенціал, Hikvision виробляє повний набір комплексних продуктів і рішень для широкого спектру вертикальних ринків. Доповнюючи сферу безпеки, останнім часом Hikvision розширює свою присутність на ринках обладнання та технологій для розумного дому, промислової автоматизації та автомобільної електроніки.

Саме з за допомогою продукції Hikvision було створено системи, які описані у даній роботі.

3.1 Структурні схеми

Система керування та управління доступом через турнікет (рис. 3.1)

Впровадження СКУД дозволяє організувати безпеку та контроль об’єктів без залучення великої кількості працівників охорони та стабільну роботу автоматизованих систем у режимі 24/7.

Централізовані системи, де контролери інтегруються в єдину мережу та підключаються до комп'ютера для централізованого управління, є складовою частиною існуючих рішень, таких як відеоспостереження, пожежна та охоронна сигналізація.

Такі системи зазвичай встановлюють на великих офісних і промислових об’єктах із значною кількістю працівників та відвідувачів. Вони забезпечують одночасне управління великою кількістю пунктів пропуску, дозволяють швидко вносити зміни до налаштувань програми та додавати нові функції.

На рис. 3.1 показана СКУД, яка включає в себе зчитувач карт (перепусток) в якості одного з ключових компонентів.

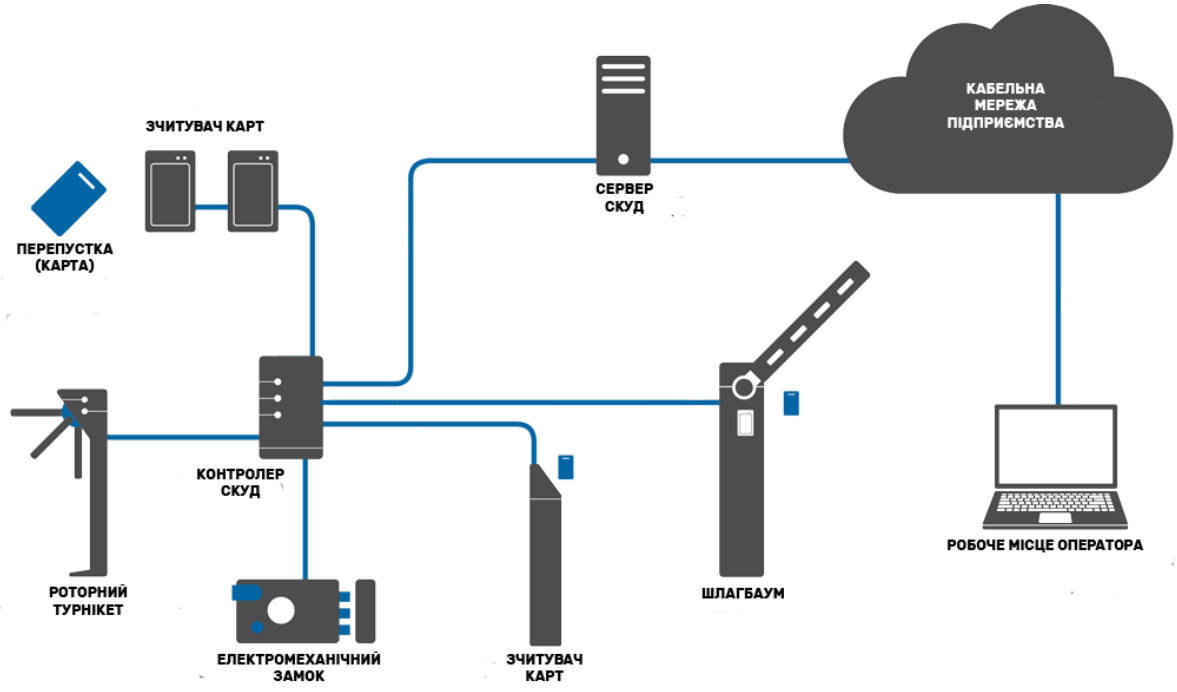

Рисунок 3.1 – Структурна модель СКУД «турнікет»

Основні компоненти схеми.

Пристрій для зчитування карт використовується для ідентифікації користувача за допомогою спеціальної карти доступу.

Процес роботи:

– Користувач підносить картку до зчитувального пристрою.

– Зчитувач надсилає дані картки на сервер для перевірки.

– Сервер порівнює отриману інформацію з базою даних.

Як тільки картка схвалена, видається дозвіл на прохід (шлагбаум або турнікет відкриваються).

Якщо картка не авторизована, доступ буде заблоковано.

Турнікет:

– Працює спільно з пристроєм зчитування карт;

– Забезпечує фізичний контроль за проходом людей;

– Відкривається тільки після отримання сигналу від сервера.

Камера

Допоміжний пристрій, здатний виконувати функції відеоспостереження або розпізнавання осіб/транспортних засобів.

Сервер

Центральний елемент для обробки даних, що надходять від зчитувачів карт, камер, турнікетів та інших пристроїв.

Визначає, чи слід надавати доступ користувачам, на основі отриманих ними даних.

Корпоративна кабельна мережа (хмарне підключення)

Відповідає за передачу даних між усіма компонентами системи.

Комп'ютер адміністратора

Використовується для моніторингу системи та управління нею.

Ви можете переглядати журнали доступу, змінювати налаштування та керувати доступом.

Принцип дії.

1) Користувач підходить до турнікету і прикладає ідентифікатор до зчитувального пристрою.

2) Система перевіряє, чи має користувач право входити в даний момент і в цю зону.

3) Коли доступ буде надано, турнікет відкриється (або ви побачите зелений сигнал).

4) Якщо в доступі буде відмовлено, турнікет залишиться заблокованим (або з'явиться червоний сигнал).

Додаткові функції.

– Інтеграція з системою відеоспостереження;

– Статистика відвідувань (хто проходив, коли і скільки разів);

– Режим захисту від паніки призначений для надання вам безкоштовного доступу в разі надзвичайної ситуації;

– Облік робочого часу — поєднання з HR-системами.

Перевага.

– Підвищить рівень безпеки;

– Зручний контроль доступу до об'єктів;

– Скоротіть витрати на охорону;

– Ефективне управління потоком людей.

Одна з основних функцій даної системи була реалізована уданому проєкті а саме **облік робочого часу**.

Облік робочого часу – це серйозна і складна задача, існують різні методології з елементами універсальності, які, навпаки, підкреслюють галузеві деталі організації виробничого процесу.

Але вирішення цієї проблеми можливо тільки в тому випадку, якщо всі заходи щодо підвищення ефективності праці адаптовані до природного виробничого процесу підприємства і адекватно відображають залученість співробітників.

Організація обліку робочого часу співробітників визнає, що це лише один з таких численних заходів, тому в даному розділі немає необхідності всебічно аналізувати проблеми підвищення ефективності роботи підприємства і характерні «підводні камені».

Впровадження додаткової системи обліку на будь-якому підприємстві завжди викликає постійну реакцію співробітників на нововведення, і діапазон реакцій може бути дуже широким. Від інерційного сприйняття співробітниками

нових правил до звільнення частини персоналу, якому нововведення не подобається.

У зв'язку з цим керівництво компанії неминуче стикається з деякими проблемами при впровадженні системи обліку робочого часу, вирішення яких визначає вектор подальшого розвитку компанії, і найважливішою з них є не вибір постачальника системи, а людський фактор і його реакція на правила мене знайомлять. .

Саме виникнення проблеми необхідності організації обліку робочого часу зазвичай пов'язане з еволюційним процесом розвитку компанії, якщо, з одного боку, відправною точкою є історично ліберальний внутрішній порядок, з іншого боку, ризик втрати контролю над виробничим процесом, тим самим неможливість впровадження нових технологій роботи, неможливість подальшого зростання розмірів компанії.

У цьому випадку працівники повинні розуміти, що вони, як правило, усвідомлюють використання систем обліку робочого часу, інтегрованих з ACS, а також використання ACS та відповідних політик безпеки. В іншому випадку співробітник просто отримує додаткові правила роботи, а в першому випадку, разом з регламентами, і додаткові механізми дисциплінарної відповідальності. Навряд чи це сподобається будь-кому, навіть найвідповідальнішим співробітникам.

Система керування та управління доступом двері

Система контролю доступу до дверей-це система, яка дозволяє обмежити доступ в певне приміщення або зону за допомогою електронного ключа або карти. Такі системи використовуються в офісах, школах, готелях, аеропортах, медичних установах та інших місцях, де необхідно забезпечити контроль доступу і безпеку.

Основними компонентами системи контролю доступу до дверей є:

Електронний замок – це пристрій, який дозволяє відкривати двері за допомогою електронного ключа або карти.

Контролер доступу – це пристрій, який керує електронним замком і зчитує дані з електронного ключа або картки;

Електронний ключ або картка – це засіб ідентифікації, що використовується для доступу до дверей.

Програмне забезпечення – програма, що керує роботою системи контролю доступу до дверей, збирає інформацію про доступ і статистику.

Система моніторингу – це система, яка дозволяє відстежувати пересування людей у приміщенні, виявляти ненормальні дії та повідомляти про них.

Система контролю доступу до дверей дозволяє забезпечити безпеку і контроль доступу в приміщення або зони. Вони можуть бути налаштовані для використання різних методів ідентифікації, включаючи біометричні, і можуть бути інтегровані з іншими системами безпеки.

Система контролю доступу (СКУД) має ряд переваг:

– Підвищена безпека. СКУД дозволяє обмежити доступ в певні приміщення і зони тільки для уповноважених осіб, що підвищує рівень безпеки;

– Ефективне Управління персоналом. СКУД дозволяє не тільки вести облік робочого часу співробітників, а й відстежувати їх переміщення по території підприємства;

– Зниження витрат. СКУД знижує витрати на забезпечення безпеки, оскільки не вимагає присутності охоронців на всіх контрольно-пропускних пунктах;

– Зручність і швидкість. СКУД дозволяє швидко і зручно контролювати доступ. Це особливо важливо для великих компаній з великою кількістю співробітників;

– Простота управління. СКУД може бути легко налаштована і управлятися за допомогою програмного забезпечення, яке дозволяє дистанційно керувати системою з будь-якого місця, де є доступ в інтернет;

– Інтеграція з іншими системами безпеки. СКУД може легко інтегруватися з іншими системами безпеки, такими як системи відеоспостереження, щоб дати вам більш повне уявлення про ситуацію з безпекою вашого підприємства.

Для більшого розуміння, як працює дана система, представлено структурну схему на рис. 3.2.

Рисунок 3.2 – Структурна модель СКУД «двері»

На схемі зображена структурна модель СКУД з поясненням підключення її основних компонентів.

Термінал контролю доступу:

– це головний пристрій системи, який виконує роль контролера;

– підключення до інших компонентів здійснюється через інтерфейс **RS-485**, який забезпечує надійну передачу даних між пристроями.

Блок управління дверима:

Виконує функцію фізичного контролю доступу до дверей.

Основні підключення:

– З’єднаний із терміналом контролю доступу через **RS-485** для отримання команд;

– Підключений до **зчитувача карт** через протокол **Wiegand**, який використовується для передачі даних про ідентифікацію;

– Управляє роботою електрозамка (електричний замок) та кнопки виходу.

Зчитувач карт Wiegand:

– Зчитує інформацію з RFID-карт або кодів доступу;

– Передає ідентифікаційні дані до блоку управління дверима через **Wiegand-протокол**.

Електричний замок:

– Елемент, що відповідає за фізичне блокування або розблокування дверей;

– Отримує команди на відкриття або закриття від блоку управління дверима.

Кнопка виходу:

– Використовується для ручного відкриття дверей з внутрішньої сторони приміщення;

– Підключена до блоку управління дверима, який обробляє сигнал від кнопки.

Підключення:

– **RS-485**: Використовується для передачі даних між терміналом контролю доступу та блоком управління дверима;

– **Wiegand**: Протокол, який з’єднує зчитувач карт із блоком управління дверима, передаючи дані про користувача;

– Електричний замок і кнопка виходу безпосередньо керуються блоком управління дверима, забезпечуючи швидке відкриття чи закриття дверей.

Ця система дозволяє організувати автоматизований контроль доступу, забезпечуючи безпеку та простоту використання.

Домофонія

IP - домофонія – це сучасний напрямок у сфері домофонних систем, який стрімко набирає популярність завдяки використанню цифрових каналів зв’язку.

IP - домофони підключаються до локальної мережі з доступом до Інтернету, що дозволяє отримувати якісне зображення з камери викличної панелі. Власник може бачити відвідувача, спілкуватися з ним, а також дистанційно відкривати двері, перебуваючи як удома, так і поза його межами. Система також надає низку додаткових функцій.

IP - домофонія підключається до локальної мережі як провідним способом через провід «кручена пара» (Ethernet) або бездротовим – через Wi-Fi. Для живлення часто використовується технологія PoE (Power over Ethernet), що дозволяє передавати електричну енергію і дані через один Ethernet-кабель, знижуючи кількість необхідних кабелів і спрощуючи монтаж.

Особливості пристроїв безпеки:

– Вбудований Wi-Fi: Більшість моделей IP-домофонів оснащені вбудованим Wi-Fi-модулем, що дозволяє уникнути прокладання додаткових проводів і значно спрощує процес встановлення;

– Двосторонній зв'язок: Через смартфон за допомогою простого застосунку можна підтримувати зв'язок з відвідувачем, що зручно і швидко;

– Охоронна функція: Якщо до домофона підключені датчики тривоги, система автоматично виконує функцію охорони, сигналізуючи про порушення безпеки;

– Стабільність роботи: Домофонія працює стабільно та без збоїв, що робить її однією з найпопулярніших на ринку;

– Віддалене керування електронними замками: Можливість відкривати двері віддалено, що особливо зручно для власників бізнесу чи користувачів, що часто перебувають поза домом;

– Підтримка SD-карт: Це дозволяє зберігати фотографії абонентів, які звертаються до домофона, на SD-карті для подальшого перегляду чи архівування.

Завдяки цим характеристикам, домофонія є зручним і надійним рішенням для сучасних систем безпеки.

На рис. 3.3 представлена схема роботи системи IP-домофонії, що включає різні компоненти, підключені через IP-мережу.

Рисунок 3.3 – Структурна модель домофонії

IP - відеодомофон: Це основний пристрій системи, який дозволяє здійснювати відеозв'язок між відвідувачем та власником або охороною. Домофон підключений до IP-мережі, що дає змогу передавати відео та аудіо сигнал через мережу.

IP - камера: Камера також підключена до тієї ж IP-мережі та може бути використана для додаткового відеоспостереження або для надання більш чіткого зображення під час взаємодії з відвідувачами.

Додаткові динаміки для двостороннього зв'язку: Ці динаміки дозволяють забезпечити двосторонній аудіозв'язок між користувачем та відвідувачем, що є важливою функцією для спілкування та перевірки, хто знаходиться біля дверей.

Мережеве сховище: Мережеве сховище використовується для збереження відео та аудіо записів, зроблених системою, таких як записи відео з камери або аудіозаписи розмови. Це дозволяє зберігати історію відвідувань та забезпечує додатковий рівень безпеки.

Персональний комп'ютер і мобільний пристрій: Користувач може отримувати доступ до відео та аудіо через свій комп'ютер або мобільний телефон, що дає можливість контролювати доступ до приміщення навіть за межами дому.

Ця схема демонструє, як через IP-мережу всі компоненти системи взаємодіють між собою, надаючи користувачам зручний доступ до функцій відеоспостереження, зв'язку та безпеки.

3.2 Програмне забезпечення

Серія ПЗ HikCentral Professional від Hikvison надає модульну платформу для основних варіантів застосування, а саме відеоспостереження, контролю доступу, УРВ та багатьох інших. Маючі унікальні функціональні можливості, ці застосунки здатні задовольнити потреби широкого спектру користувальницьких сценаріїв. Усі застосунки мають однаковий дизайн інтерфейсу, що значно скорочує час навчання при розширенні діапазону обслуговуваного обладнання.

HikCentral – програмне забезпечення для керування безпекою Hikvision – допомагає професіоналам долати різні перешкоди безпеки на одній платформі.

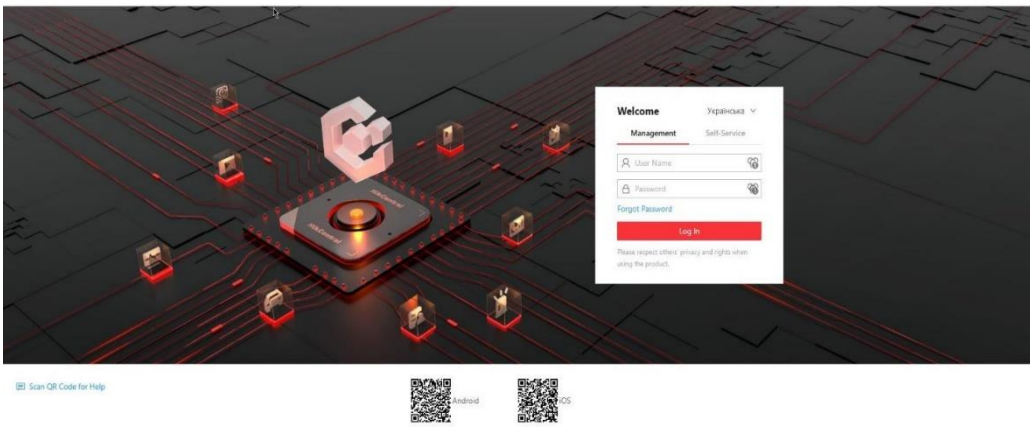

Рисунок 3.4 – Стартове вікно ПЗ

ПЗ HikCentral дозволяє з легкістю керувати окремими системами, такими як відео, контроль доступу, виявлення тривоги тощо. HikCentral Professional призначено для оптимізації повсякденних операцій безпеки для різноманітних сценаріїв.

Різноманітні бізнес-застосунки на вибір

Всі основні потреби в безпеці покриваються за допомогою різноманітних модулів безпеки, включаючи відео, контроль доступу, відвідувачів, облік часу та відвідуваності, паркування, бортовий моніторинг, виявлення сигналізації, інтелектуальний аналіз, комерційний дисплей та багато іншого (рис. 3.5).

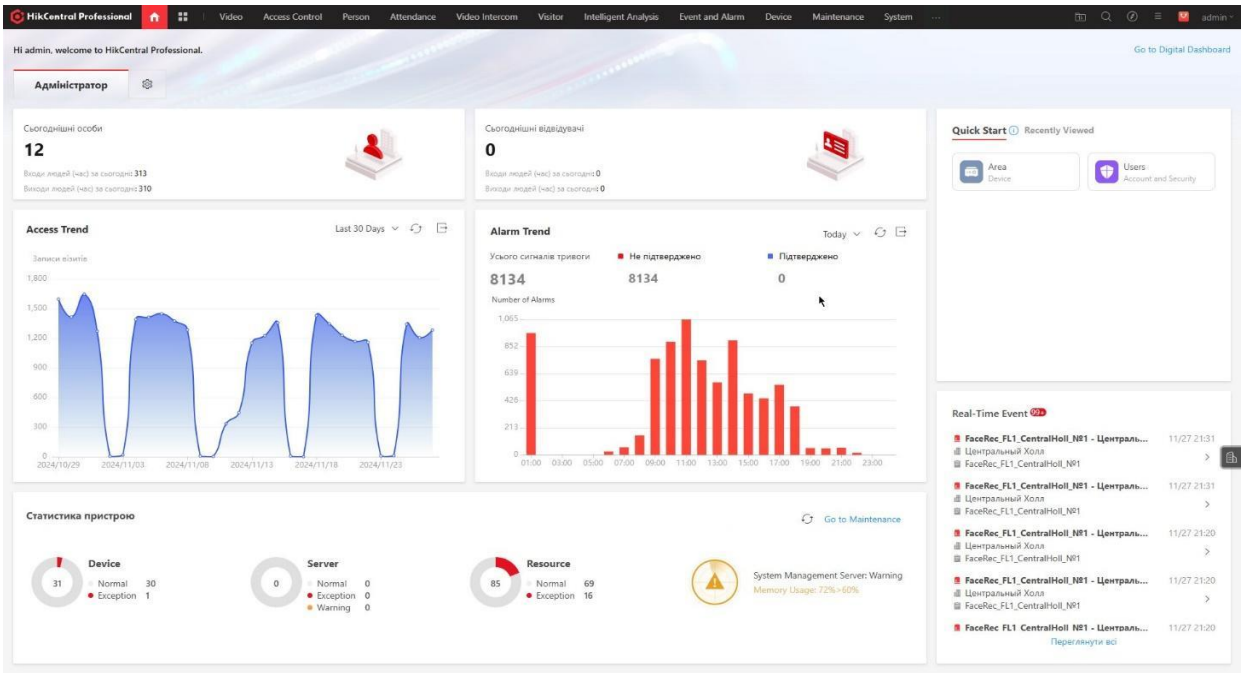

Рисунок 3.5 – Вікно статистики

Єдина система безпеки, що підвищує ефективність управлінських операцій.

HikCentral Professional об'єднує широкий спектр застосунків і надає безперебійне рішення для бізнесу, від базових до розширених потреб – наприклад, охоронна сигналізація плюс контроль доступу в поєднанні з відео верифікацією, або, можливо, доступ відвідувачів з попередньою реєстрацією транспортних засобів тощо (рис. 3.6).

Централізоване управління багаторівневими ролями надає користувачам оптимізовану ефективність.

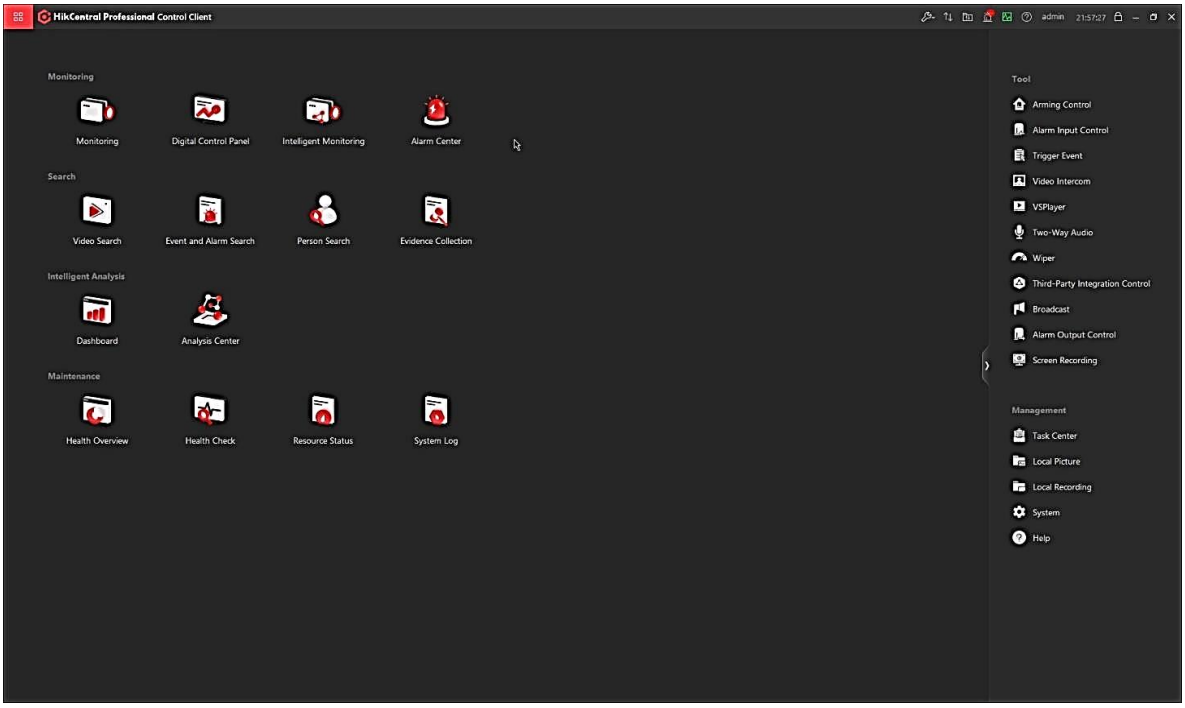

Рисунок 3.6 – Модулі HikCentral Professional

Легкі рішення для різноманітних сценаріїв

HikCentral Professional пропонує готові рішення для конкретних сценаріїв, таких як магазини, логістичні парки, автостанції тощо, покращуючи їх повсякденну безпеку та роботу за допомогою аналізу даних та уніфікованого управління.

Ефективна та всеосяжна відеобезпека

Швидко зберігайте сцени та ефективно виконуйте щоденний моніторинг. Користувачі можуть налаштувати власний вигляд, щоб мати голографічне сприйняття всіх відео, карт і даних (рис. 3.7). Зазначені подання можна відкрити за одну хвилину для швидкого попереднього перегляду та відтворення.

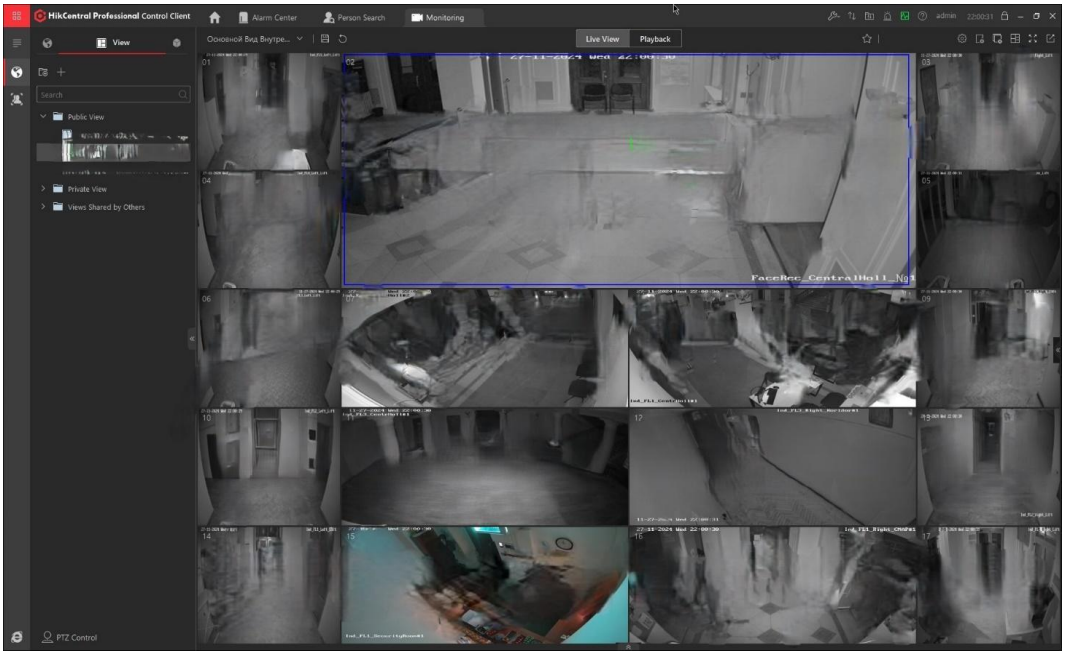

Рисунок 3.7 – Мережа відеокамер

Швидкий та зручний пошук та відтворення

Користувачам сподобається швидкий пошук інцидентів та визначення місцезнаходження за допомогою мініатюр, підтримка відтворення з підпотоком, перекодуванням та вилученням кадрів.

Зручний пошук подій ґрунтується на аналізі тегів та пошуку СВУ, а також ключових атрибутів транспортних засобів та осіб.

Швидкий перегляд відео на основі типів подій знижує потенційні ризики, знаходячи високочастотні події в критичних зонах.

Адаптивність мережі з низькою пропускною здатністю.

Плавна потокова передача автоматично регулює бітрейт і роздільну здатність між клієнтами та відео реєстраторами або мережевими камерами відповідно до умов мережі в реальному часі.

Гнучке автоматичне патрулювання.

Користувачі можуть налаштувати запланований план зйомки на основі реальних сценаріїв або потреб, і зняті знімки будуть надіслані користувачам автоматично.

Універсальна аудіотрансляція.

Поєднуючи досвід відеобезпеки з можливостями розумного аудіо, мережева колонка Hikvision пропонує передове рішення для зв'язку аудіо та відео.

Централізовано керуйте кількома аудіо пристроями та транслюйте прямі або попередньо записані голосові повідомлення в режимі реального часу в кілька зон.

Кілька режимів трансляції, таких як запланований, підключення сигналізації та аварійний збір, що забезпечує точну та своєчасну доставку важливої інформації.

Комплексне та гнучке управління доступом.

Отримайте гнучкі, налаштовані та комплексні системи контролю доступу для співробітників і відвідувачів із різноманітними обліковими даними, включаючи обличчя, райдужну оболонку ока, відбиток пальця, картку, динамічний QR-код, PIN-код, мобільні облікові дані, включаючи Bluetooth, автентифікацію 512 і 5 стратегій доступу на вибір для сотень сценаріїв.

Легке і зручне управління персоналом.

За допомогою HikCentral Professional HR та менеджери можуть легко призначати різні групи людей.

Маючи різні повноваження з покроковими інструкціями, легко керуйте процедурами прийому на роботу та звільнення співробітників тощо.

Вони отримають дозвіл на доступ миттєво.

Більше того, з HikCentral Professional простіше, ніж будь-коли, вводити інформацію про співробітників і оформляти їх бейдж за допомогою декількох унікальних стилів і макетів на вибір. За допомогою кількох кліків керівники можуть ввести свою інформацію та роздрукувати значки співробітників з усіма необхідними дозволами доступу.

Швидке керування сигналізацією.

При виникненні інцидентів система контролю доступу буде спрацьовувати мережеві камери для зйомки зображень і запису відео.

Співробітники служби безпеки можуть перевіряти відео в режимі реального часу та вживати кілька необхідних дій.

Аномальні точки доступу можна своєчасно виявити за допомогою електронних карт, а відхилення від норми ефективно усуваються за допомогою відеоверифікації.

Забезпечують повне сприйняття панорами та деталей на відкритих просторах, таких як індустріальні парки та будівельні майданчики, використовуючи режим «Pic in Pic» для операцій на основі пальців, які імітують перебування на місці. Легкий доступ до ключових позиційних камер без втрати глобального огляду.

Ключові позиції на AR Live Map можна знайти за допомогою тегів за допомогою простих кнопок «Натисніть» та «Фільтр» (рис. 3.8).

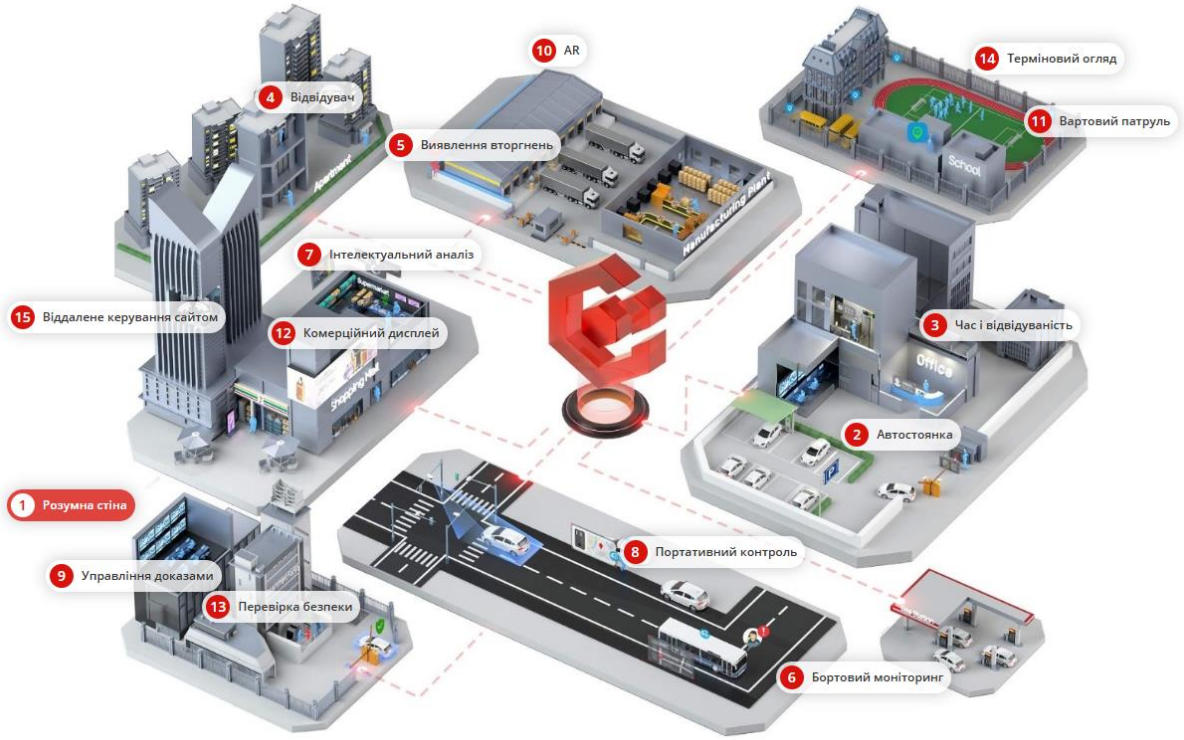

Рисунок 3.8 – Мапа AR Live Map

3D-відстеження цілі реалізовано на пристроях з доповненням AR. Спроєктуйте ефективний процес для швидкої обробки подій із замкнутим циклом від сповіщення до підтвердження.

Дозволяють додавати на дисплей різні мітки, включаючи відео, контроль доступу, сигналізацію, теги входу/виходу та інше. Також є і багато інших виробників у яких альтернативна спеціалізація.

Популярні європейські виробники систем контролю доступу

На сьогодні на європейському ринку існує велика кількість виробників систем контролю доступу. Ось кілька з них:

ASSA ABLOY – шведський виробник систем безпеки, до якого належать бренди, такі як HID Global, Yale та ABLOY. Компанія пропонує широкий асортимент рішень для контролю доступу, включаючи карткові системи, біометричні технології, електромеханічні замки та інше.

ISEO – італійський виробник, заснований у 1969 році, який спеціалізується на розробці замків, ключів та систем безпеки для різних промислових і комерційних застосувань. Серед продуктів ISEO є електронні замки, дверне обладнання, біометричні зчитувачі та програмне забезпечення для управління доступом.

Mottura – компанія, що працює з 1960 року, розробляє та виробляє різноманітні замки та системи безпеки. Вона пропонує електронні рішення для контролю доступу, включаючи використання RFID-карток та біометричних даних для ідентифікації користувачів.

Mul-T-Lock – ізраїльський виробник, заснований у 1973 році, який пропонує широкий спектр продукції для контролю доступу та безпеки. Їхня продукція включає механічні та електронні замки, системи для комерційної та житлової нерухомості, а також криптографічні системи для захисту від несанкціонованого доступу.

Siemens – німецький концерн, що займається енергетикою та автоматизацією, також розробляє системи контролю доступу для різноманітних об'єктів.

Bosch Security Systems – німецький виробник, що пропонує як бездротові, так і провідні рішення для контролю доступу.

Salto Systems – іспанська компанія, яка спеціалізується на електронних замках і системах контролю доступу, зокрема на технологіях RFID та Bluetooth.

Ці компанії є лише частиною виробників, представлених на європейському ринку систем контролю доступу. Вибір конкретного виробника залежить від ваших вимог і потреб.

Популярні китайські виробники систем контролю доступу

На європейському ринку також представлені кілька китайських виробників систем контролю доступу, серед яких:

Hikvision – один із лідерів у галузі відеоспостереження та систем контролю доступу, що пропонує продукти з сучасними технологіями, такими як розпізнавання обличчя та відбитків пальців.

ZKTeco – компанія, яка спеціалізується на біометричних та RFID-системах для контролю доступу, виготовляючи продукти високої якості за доступними цінами.

Dahua – ще один відомий виробник систем відеоспостереження та контролю доступу, з пропозицією біометричних і RFID-рішень.

Uniview – компанія, яка випускає продукцію для відеоспостереження та контролю доступу, що відповідає європейським стандартам безпеки.

Ezviz – виробник систем контролю доступу, орієнтований на біометричні технології, такі як розпізнавання обличчя та відбитків пальців.

При виборі виробника систем контролю доступу варто ретельно вивчити асортимент, порівняти різні продукти та послуги, щоб знайти оптимальне рішення для ваших потреб [26].

Висновок до розділу 3

У даному розділі компоненти Системи контролю і управління доступом (СКУД) розглядаються як частина технологій Інтернету речей (IoT). Це пояснюється тим, що ці пристрої, які використовуються для управління доступом, не просто виконують функції блокування чи відкриття дверей, а є «розумними» пристроями, здатними самостійно збирати, обробляти та передавати дані. Зокрема, вони можуть моніторити переміщення працівників, фіксувати час входу/виходу, а також інтегруватися з іншими системами для оптимізації робочих процесів.

Інтеграція компонентів СКУД у виробничі процеси має великий потенціал у рамках Індустрії 4.0. Наприклад, за допомогою таких систем можна автоматизувати облік робочого часу, здійснювати моніторинг переміщення працівників між приміщеннями, а також обчислювати чисельність людей у приміщеннях для регулювання таких систем, як кондиціонування або вентиляція. Це забезпечує не лише безпеку, але й ефективність роботи, підтримуючи оптимальні умови для працівників та ресурсів підприємства.

Компоненти СКУД, завдяки своїй здатності обробляти дані в реальному часі, є важливою частиною цифрової трансформації в рамках Індустрії 4.0. Вони не лише забезпечують безпеку, але й сприяють інтеграції інших технологій, таких як аналіз великих даних (Big Data) та штучний інтелект (AI), що дозволяє автоматично оптимізувати управлінські та виробничі процеси на підприємствах.

4 МЕХАНІЗМ ТА РЕЗУЛЬТАТИ ПРАКТИЧНОЇ ЧАСТИНИ

4.1 Програмування картки та результати роботи системи СКУД на базі HikCentral

Картка доступу – це фізичний пристрій (зазвичай у вигляді пластикової картки з вбудованим чіпом або магнітною стрічкою), який використовується для ідентифікації та надання доступу до певних зон або систем. У контексті зображення, яке ви надали, картка доступу може бути створена, призначена чи налаштована для нового користувача через програмний інтерфейс.

Програмування картки доступу за допомогою програмного забезпечення HikCentral для системи контролю доступу Hikvision включає кілька етапів, зокрема налаштування пристроїв, створення користувачів і програмування карток доступу.

На рис. 4.1–4.3 показаний інтерфейс програми для управління доступом системи відеоспостереження або контролю доступу. Це вікно додавання нового користувача ("Add Person") у програмному забезпеченні системи HikCentral Professional.

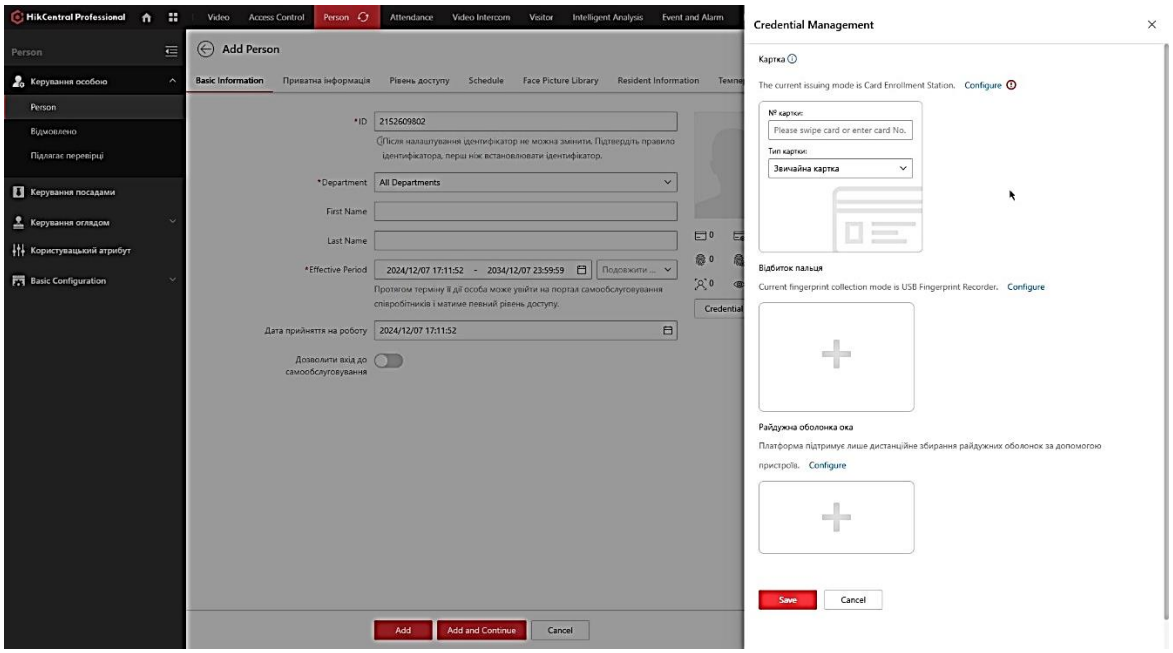

Рисунок 4.1 – Інтерфейс програми для управління доступом

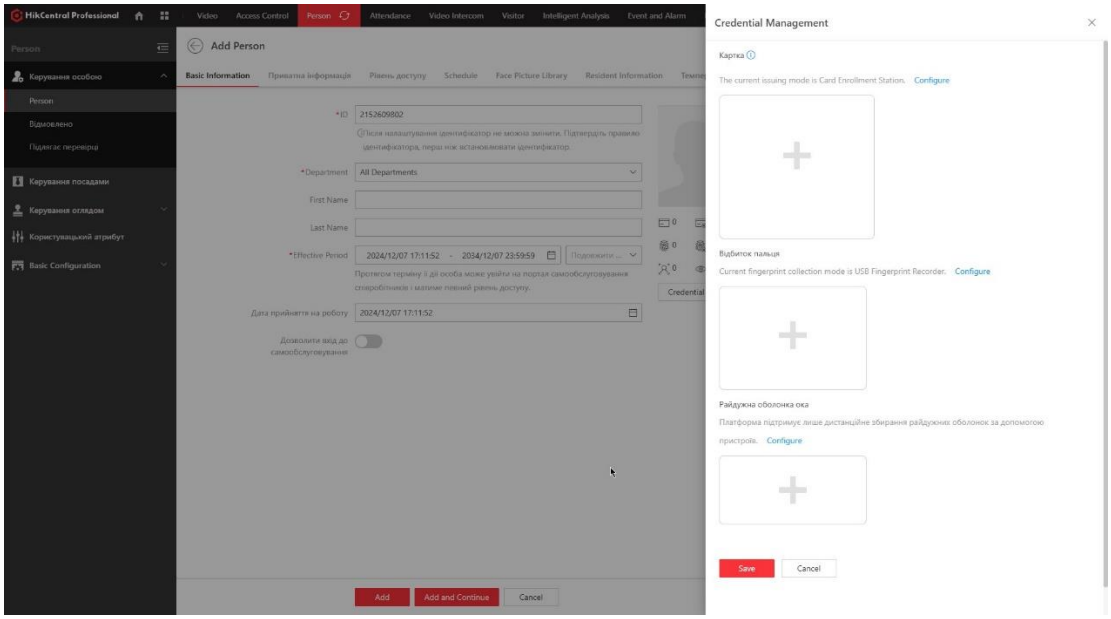

Рисунок 4.2 – Інтерфейс програми для управління доступом

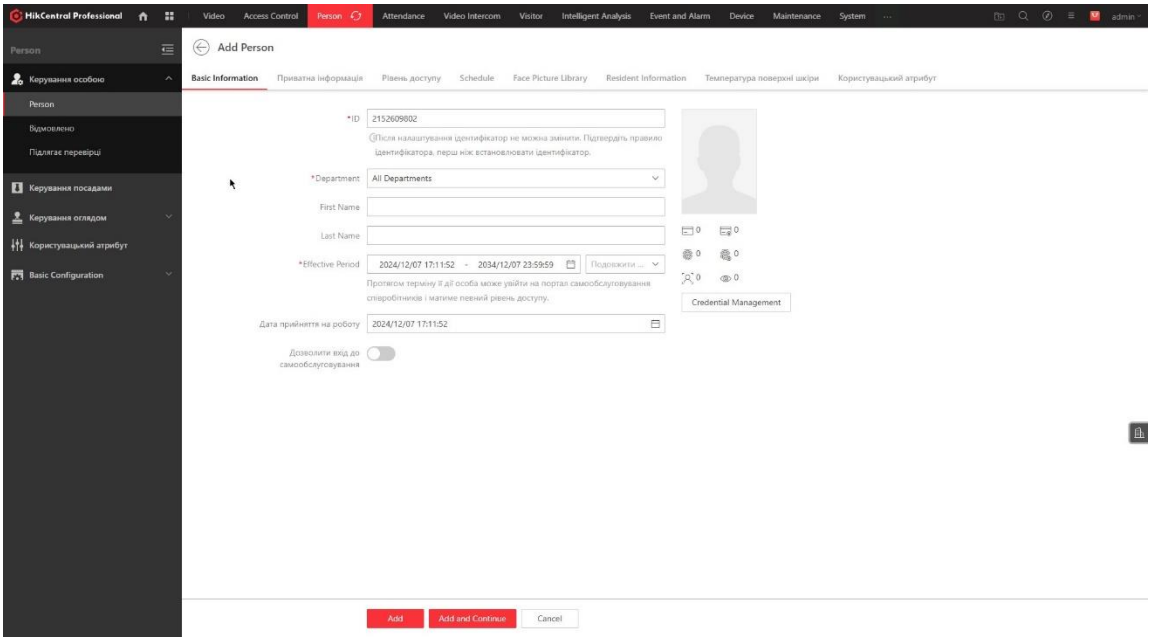

Рисунок 4.3 – Інтерфейс програми для управління доступом

Вкладка Add Person (Додавання користувача):

Містить поля для введення основної інформації про особу.

Форма для введення даних:

– ID: Унікальний ідентифікатор користувача;

– Department (Відділ): Вибір відділу зі списку;

– First Name та Last Name: Поля для введення імені та прізвища користувача;

– Effective Period (Період дії): Встановлення періоду, протягом якого доступ буде активним;

– Дата прийняття на роботу: Поле для вибору дати;

– Додаткові параметри: Чекбокс для активації або деактивації функцій, таких як самореєстрація;

Кнопки управління:

– Add (Додати).

– Add and Continue (Додати та продовжити).

– Cancel (Скасувати).

– Додаткові вкладки:

Крім **Basic Information**, є й інші вкладки, такі як **Рівень доступу**, **Розклад**, **Face Picture Library**.

Цей інтерфейс є частиною комплексного програмного забезпечення для управління доступом і моніторингу, яке використовується в організаціях для підвищення безпеки, автоматизації процесів і контролю за переміщенням співробітників чи відвідувачів. Окрім базового налаштування облікових записів користувачів, він також пропонує широкий набір функцій для управління правами доступу, інтеграції з іншими системами безпеки та аналізу даних.

На рис. 4.4–4.5 відображений інтерфейс програмного забезпечення HikCentral Professional, розділ Attendance (Відвідуваність). Він використовується для моніторингу та аналізу даних про присутність співробітників, їх графік роботи, запізнення, відсутність тощо.

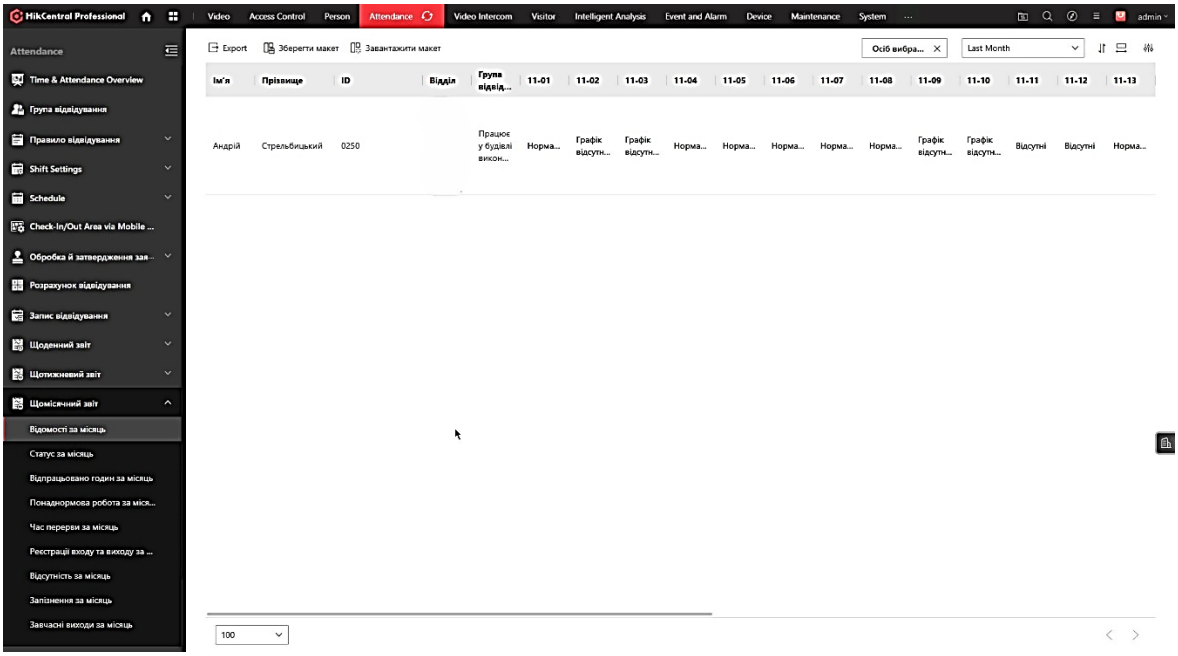

Рисунок 4.4 – Розділ Attendance

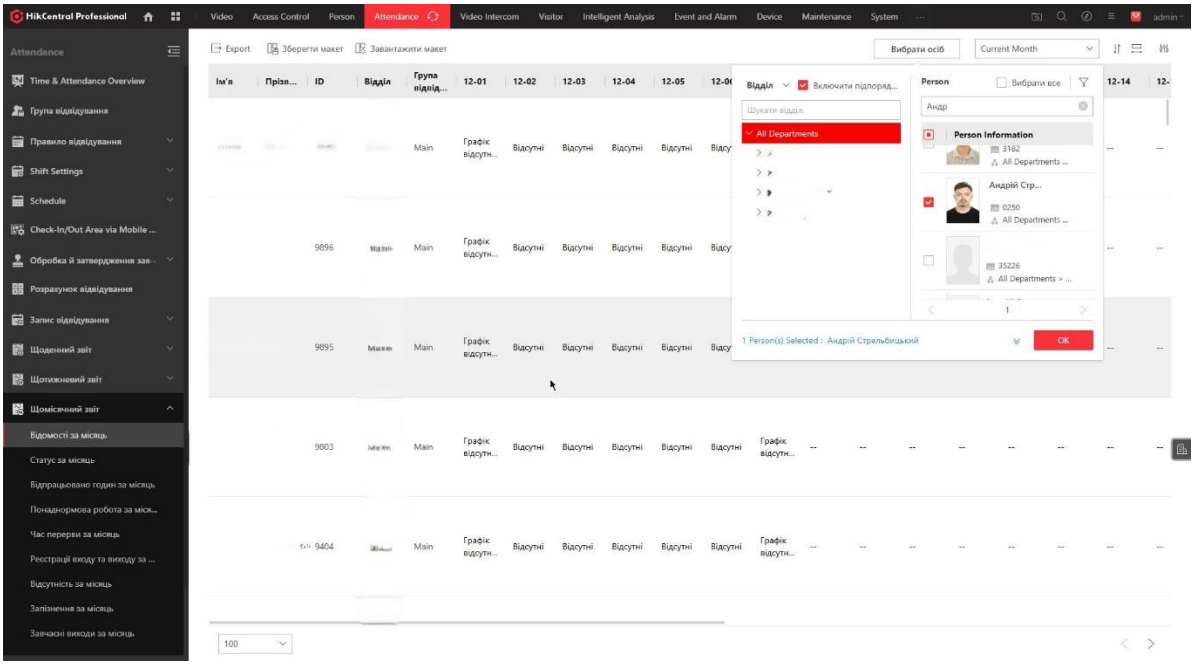

Рисунок 4.5 – Розділ Attendance

Головна таблиця преставлє собою стовпці (рис. 4.6–4.7):

– Ім'я: Ім'я співробітника (наприклад, Андрій).
– Прізвище: Прізвище користувача (наприклад, Стрельбицький).
– ID: Унікальний ідентифікатор співробітника.

– Група відвідувань: Наприклад, Працівник у будівлі чи інша інформація.

– Дати (11-01, 11-02 тощо): Відображення стану за конкретні дні, включаючи **Норма**, **Графік відсутній** чи **Відсутній**.

– Для кожного дня відображаються записи, що відображають статус присутності (норма, запізнення, відсутність).

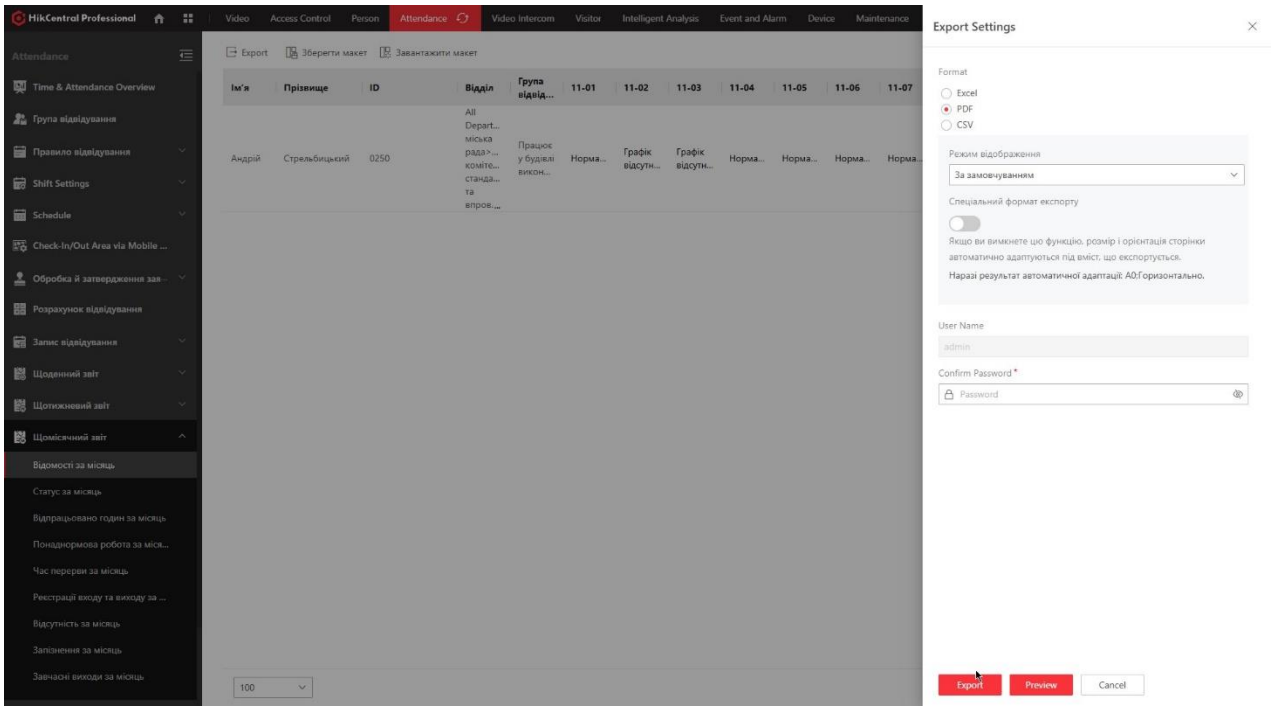

Рисунок 4.6 – Export settings

Для подальшої роботи та аналізу даних, інформацію отриману у програмі можна експортувати до файлу форматів Excel, PDF, та CSV. Ці дані допомагають забезпечити ефективне управління персоналом, контроль за виконанням трудових обов'язків та дотриманням законодавства, а також сприяють підвищенню продуктивності праці.

Відомості за місяць

Експорт часу: 2024-12-07 17:15

Оператор: admin

Період часу: 2024-11-01 - 2024-11-30

Ім’я	Прізвище	Ідентифікатор
Андрій	Стрельбицький	0250

11-01	11-02	11-03	11-04	11-05	11-06	11-07	11-08	11-09	11-10
W	NS	NS	W	W	W	W	W	NS	NS

11-11	11-12	11-13	11-14	11-15	11-16	11-17
A	A	W	W	W	NS	NS

11-18	11-19	11-20	11-21	11-22	11-23	11-24
A	W	W	W	W	NS	NS

11-25	11-26	11-27	11-28	11-29	11-30
W	W	W	W	W	NS

Рисунок 4.7 – Відомості за місяць

Отримані дані принесуть гарну користь для підприємства, а саме:

Ефективність: Автоматизація процесів зменшує навантаження на адміністративний персонал.

Прозорість: Дані є доступними для аналізу, що сприяє довірі між працівниками та керівництвом.

Оптимізація: Дає змогу краще розподіляти ресурси та уникати перевантажень.

Безпека: Інтеграція з системами доступу забезпечує контроль за перебуванням працівників на території.

Використання даних робочого часу допомагає створити ефективну та дисципліновану робочу атмосферу, підвищуючи загальну продуктивність і конкурентоспроможність підприємства.

На рис. 4.8 зображено модуль який містить конфігурацію що стосуються точок конролю відвідування та правил відвідування. Він забезпечює перегляд та обробку записів та формування звітів.

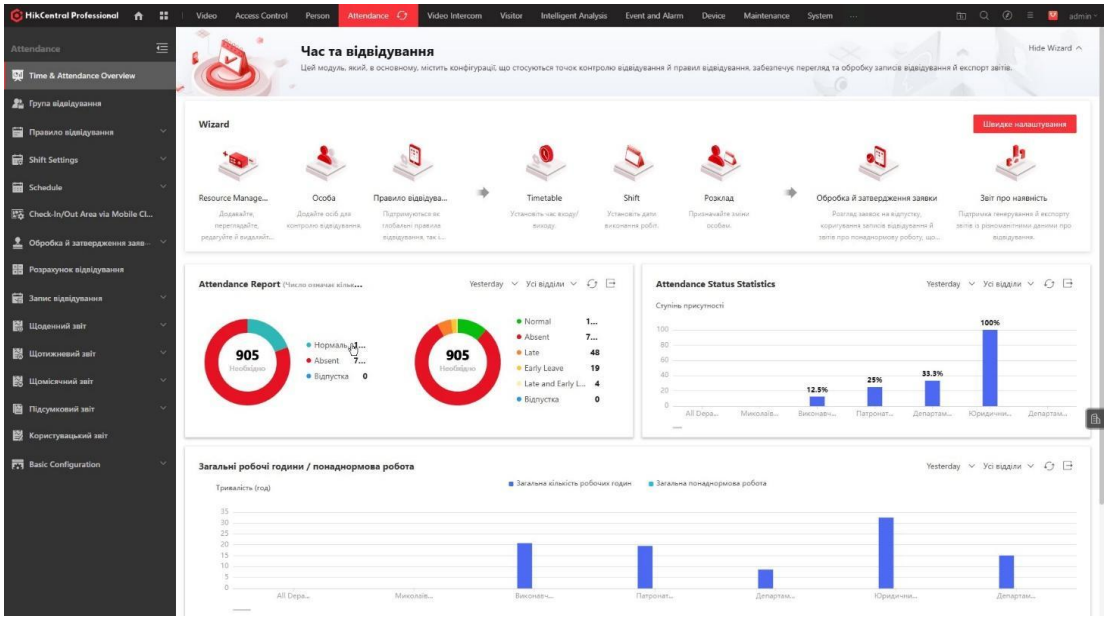

Рисунок 4.8 – Час та відвідування

На рис. 4.9–4.10 продемонстровано результат автоматично моніторигу та створенн подій на основі зафіксованих даних. Принцип роботи полягає у тому, що потрапяючи у фіксовану зону, програма автоматично фіксує подію.

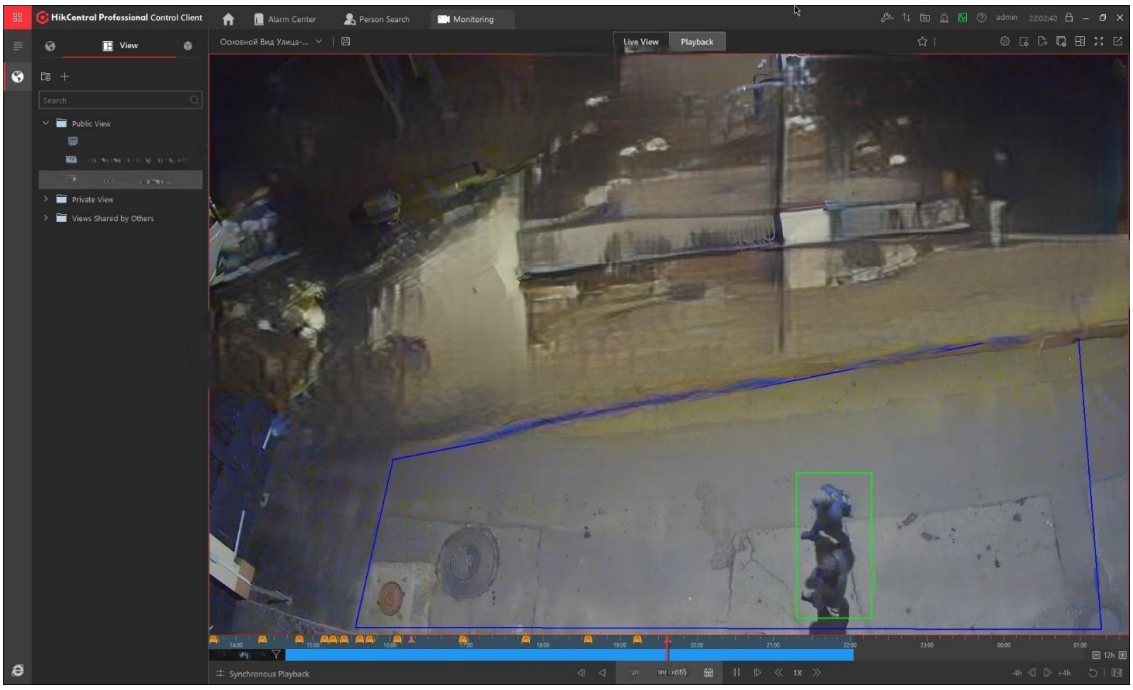

Рисунок 4.9 – Моніторинг

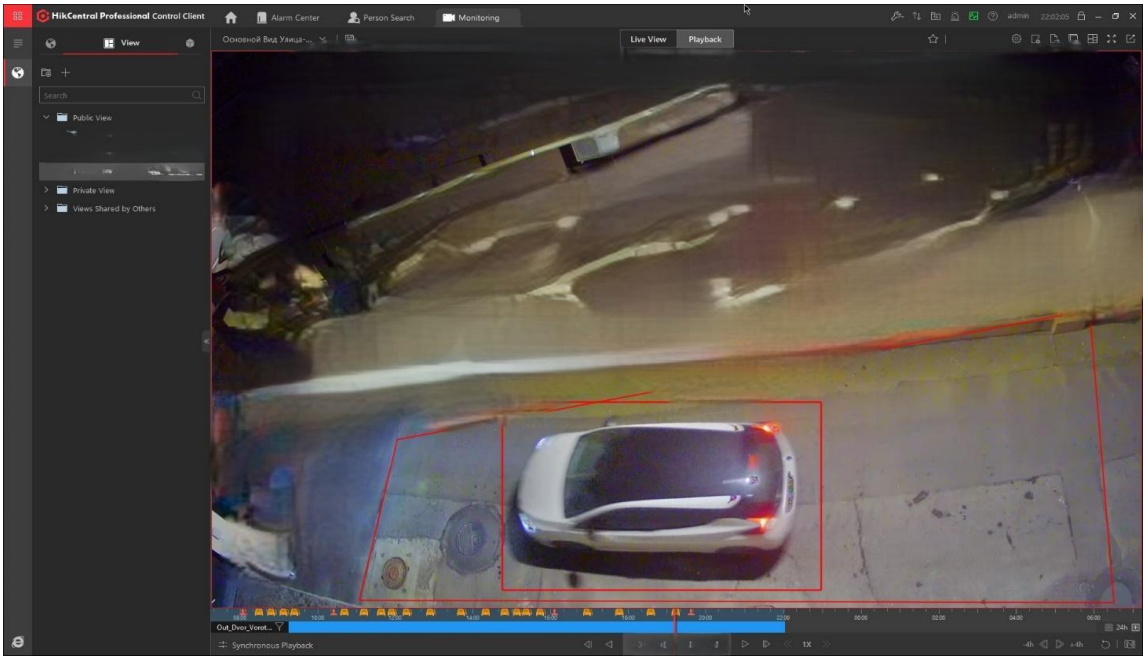

Рисунок 4.10 – Моніторинг

Далі ця поді відображається на часовому проміжку який можна побачи у нижній частині рисунка. Система також здатна роспізнавати об’єкти по типу «людина» чи «машина». Дана система спрощює роботу у системі віоспостереження та пришвидшує процес обробки інфрмації.

4.2 Зчитувач СКУД

В даному фрагменті наведено функціонал та особливості програмного забезпечення Sigur Access Framework версії 2.0.0. Це програмне забезпечення використовується у системах контролю та управління доступом (СКУД), а саме в роботі з пристроями-зчитувачами доступу.

Sigur Access Framework (SDK) – це набір програмних інструментів (Software Development Kit), створений для розробників і інтеграторів, які працюють із системами Sigur.

Версія 2.0.0 містить нові можливості для роботи із зчитувачами, які є частиною СКУД.

Основні можливості Sigur Access Framework:

– Інтеграція з обладнанням: Надає інструменти для підключення та управління зчитувачами (наприклад, RFID, біометричними чи кодовими);

– Налаштування доступу: Дозволяє програмно задавати права доступу для користувачів;

– Обробка подій: Автоматично реєструє події, такі як вхід, вихід, відхилені спроби доступу;

– Розширення функціоналу: Дає змогу інтегрувати зчитувачі з іншими системами (наприклад, відеоспостереженням, HR-системами);

– Гнучкість у розробці: Призначений для використання розробниками для створення власних рішень на основі обладнання Sigur.

Програмне забезпечення призначено для розширення можливостей СКУД для підприємств і організацій, забезпечення кастомізації системи відповідно до потреб конкретного об’єкта та підвищення рівня безпеки та автоматизації завдяки інтеграції з іншим програмним забезпеченням.

Для підключення бібліотеки до проєкту необхідно додати репозиторій Maven у файл *settings.gradle* проєкту (рис. 4.11).

```
dependencyResolutionManagement {
  // ... repositories {
    // ... maven {
      url 'https://maven.sigur.com' credentials {
        username sigurMavenUsername password
        sigurMavenPassword
      }
    }
  }
}
```

Рисунок 4.11 – Додавання репозиторія Maven у файл *settings.gradle* проєкту

Це налаштування дозволяє проєкту підключатися до приватного Maven-репозиторія https://maven.sigur.com для завантаження залежностей. Для доступу до репозиторія використовуються облікові дані (ім’я користувача та пароль), що забезпечує безпеку доступу до приватних бібліотек чи пакетів.

Далі потрібно додати залежність у файл *build.gradle* модуля (рис. 4.12).

```
dependencies {
// ...
implementation 'com.sigur.android:accessframework:2+'
}
```

Рисунок 4.12 – Додавання залежності у файл *build.gradle*

Цей фрагмент додає залежність від бібліотеки accessframework версії 2 або новішої до проєкту. Бібліотека містить компоненти для роботи з системою контролю доступу або інтеграцією з платформою SIGUR.

Щоб почати працювати з Sigur Access Framework, необхідно реалізувати інтерфейс Access.Delegate (рис. 4.13).

```
import com.sigur.android.accessframework.Access
// …
object MyDelegate : Access.Delegate { override fun
  onScanFailed(errorCode: Int) {
    // Bluetooth scan error.
    showBluetoothError(errorCode)
  }
       override fun isInForeground(): Boolean {
         // Is application currently on screen
         return mainActivity.lifecycle.currentState == Lifecycle.State.RESUMED
       }
  override fun getKey(guid: ByteArray): ByteArray? {
    // Return secret authentication key associated with the server GUID.
    // Or null, if there is no key
    return keysDao.getKeyForGuid(guid)
  }
  override fun getIdentifier(deviceInfo: Bundle): ByteArray? { if
    (isIdentificationAllowed(deviceInfo)) {
      // Return identifier. Any byte array generated by vendor. return
      USER_IDENTIFIER
    } else {
      // Or null, if identification should not be started on the device by some reason
      return null
    }
  }
  override fun onIdentificationEvent(deviceInfo: Bundle, eventCode: Int, status: Int) {
    // Callback for notifications about identification state changes. updateUi(deviceInfo,
    eventCode, status)
  }
}
```

Рисунок 4.13 – Реалізація інтерфейсу Access.Delegate

Це основна частина логіки для обробки подій у застосунку, що працює з пристроями контролю доступу, інтегрованими через Sigur Access Framework.

Цей делегат дозволяє застосунку обробляти такі події, як помилки Bluetooth, ідентифікацію пристроїв, а також управління ключами доступу.

Докладніше про методи інтерфейсу Access.Delegate:

onScanFailed(errorCode) – помилка під час запуску сканування BLE. Коди помилок описані в документації Android. Цей метод не викликається під час роботи з HCE.

isInForeground() – повертає true, якщо програма відображається на екрані. Викликається лише тоді, коли зчитувач Sigur знаходиться в режимі "коли програма на екрані".

getKey(guid) – повинен повернути 128-бітний секретний ключ для авторизації на зчитувачі, асоційований з GUID сервера Sigur. Якщо повертається null, ідентифікація не буде виконана. Цей метод не викликається, якщо зчитувач налаштований на базовий режим роботи.

getIdentifier(deviceInfo) – повертає ідентифікатор, який буде передано на зчитувач. Вся інформація про зчитувач міститься в параметрі deviceInfo, який детально описано в DeviceInfo.java. Якщо повертається null, ідентифікація не відбудеться. Зчитувачі Sigur MR підтримують максимальну довжину ідентифікатора 16 байт.

onIdentificationEvent(deviceInfo, eventCode, status) – повідомляє про зміну стану ідентифікації на конкретному зчитувачі. Інформація про зчитувач передається в параметрі deviceInfo, подія ідентифікації – в eventCode, а status містить додаткову інформацію. Наприклад, при успішній ідентифікації eventCode дорівнює Access.Delegate.EVENT_CODE_IDENTIFICATION_DONE, а status – 0. Будь-який інший статус вказує на помилку.

Для використання Access.Delegate потрібно встановити глобальне посилання на нього. Наприклад, це можна зробити під час запуску програми (рис. 4.14).

```
import android.app.Application

import com.sigur.android.accessframework.Access
// …

class App : Application() { override fun
   onCreate() {
      super.onCreate()

      Access.setDelegate(MyDelegate)
   }
}
```

Рисунок 4.14 – Встановлення глобального посилання на Access.Delegate

Цей код налаштовує делегат для роботи зі СКУД від Sigur. Він дозволяє застосунку реагувати на події, пов'язані з доступом (сканування, ідентифікація, авторизація), що можуть відбуватись протягом роботи застосунку. Використання класу *Application* забезпечує, що делегат буде налаштований тільки один раз при запуску програми, незалежно від того, скільки активностей буде відкрито.

Для роботи через NFC потрібно просто оголосити сервіс у маніфесті застосунку (рис. 4.15).

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="...">

   <!-- required permission -->
   <uses-permission android:name="android.permission.NFC" />

  <application>
     <service android:name="com.sigur.android.accessframework.AccessHostApduService"
        android:exported="true" android:permission="android.permission.BIND_NFC_SERVICE">
        <intent-filter>
           <action android:name="android.nfc.cardemulation.action.HOST_APDU_SERVICE" />
        </intent-filter>
        <meta-data android:name="android.nfc.cardemulation.host_apdu_service"
           android:resource="@xml/apduservice" />
              </service>
         </application>
<manifest />
```

Рисунок 4.15 – Оголошення сервісу NFC у маніфесті застосунку

Цей фрагмент налаштовує сервіс у застосунку для роботи з NFC-картами через APDU. Сервіс обробляє запити для емуляції карт і взаємодії з ними, дозволяючи здійснювати операції з NFC, наприклад, авторизацію або зчитування даних. Вказаний дозвіл *android.permission.NFC* дає застосунку можливість доступу до NFC, а BIND_NFC_SERVICE обмежує доступ до сервісу лише тим застосункам, які мають відповідні права.

Цей сервіс використовує метадані з XML-файлу ресурсів, в даному випадку – *apduservice.xml* (рис. 4.16).

```
<host-apdu-service
xmlns:android="http://schemas.android.com/apk/res/android"
   android:description="@string/sigur_host_apdu_service_description"
   android:requireDeviceUnlock="false">
   <aid-group android:category="other"
      android:description="@string/sigur_access_aid_group_description">
      <aid-filter android:name="f4ff13c98558b8a01ea9e6329fdceb19" />
   </aid-group>
</host-apdu-service>
```

Рисунок 4.16 – Використання метаданих з XML-файлу ресурсів

Цей XML описує конфігурацію для роботи з Host APDU Service, який відповідає за взаємодію з картами через NFC за допомогою APDU. Вказані мета-дані дозволяють налаштувати сервіси для певних AID і категорій карт, а також визначають, чи потрібно розблоковувати пристрій для роботи з ними.

Параметр requireDeviceUnlock можна встановити в значення true, якщо це необхідно. Рядкові ресурси для полів description надані Sigur Access Framework, але їх можна замінити за потреби.

4.3 Останні досягнення у розвитку IoT та Індустрії 4.0

Трансформація промисловості 4.0: машинне навчання підвищує надійність обладнання, скорочуючи час простою та підвищуючи продуктивність. Спільні роботи підвищують безпеку, розсуваючи межі співпраці людини та робота. Цифрові близнюки оптимізують управління енергією та прискорюють розвиток розумних міст.

Провідні інноватори : Rockwell Automation, ICP DAS і Siemens є лідерами з передовими технологіями автоматизації та інтеграцією ШІ. Альянс Open Industry 4.0 і Digital Twin Consortium прагнуть об’єднати технології цифрових близнюків.

Розширення IoT та IIoT : зростаючий вплив на управління енергією та безпеку; очікується, що ринок IIoT стрімко зростатиме до 2028 року.

Технологічна конвергенція : інтеграція економного виробництва з IoT та AI призводить до новаторської оптимізації процесів.

Виклики та оптимізм : хоча переважає оптимізм щодо технологічного впливу, зростає потреба у кваліфікованій робочій силі та заходах кібербезпеки[19].

Передовики в області

Rockwell Automation робить значну ставку на AMR, коботів і генеративний ШІ, щоб очолити промислову автоматизацію в авангарді цієї революції. Тим часом ICP DAS представить абсолютно нові інновації в сфері автоматизації та інновації в галузі автоматизації на виставці Smart Factory Expo 2024 у Токіо.

Альянс Open Industry 4.0 і Digital Twin Consortium працюють разом над стандартизацією технологій цифрових близнюків. Siemens не відстає, включаючи генеративний штучний інтелект у свої послуги з прогнозованого обслуговування. Крім того, ринок коботів зростає завдяки представленню Universal Robots міцного 30-кілограмового кобота[19].

HSINCHU, 9 січня 2024 р. /PRNewswire/ на виставці SMART FACTORY Expo 2024, Токіо, ICP DAS (3577-TW) продемонструвала повний портфель продуктів і рішень для управління Інтернетом речей і автоматизації під темою «ESG і чисті нульові викиди». ." Дебют знаменує значну віху в участі компанії у провідних світових шоу.

Компанія пропонує ряд датчиків, модулів віддаленого вводу/виводу, промислових комунікаційних пристроїв, контролерів і програмного забезпечення для керування. На цій виставці компанія представить, як ці

продукти допомагають клієнтам будувати розумні заводи та оптимізувати управління виробничими процесами.

Виявлення проблемних точок є першим кроком до надання ідеально підібраних рішень. За допомогою цього принципу ICP DAS одного разу успішно допомогла провідному виробнику контактних лінз в управлінні вуглецевим слідом заводу та відповідності суворим екологічним стандартам, спеціально встановленим для чистих приміщень.

У цьому застосунку компанія встановила інтелектуальні лічильники електроенергії та концентратор вимірювачів електроенергії IIoT для збору та передачі даних у реальному часі про споживання електроенергії на заводі. Одночасно були розгорнуті модулі датчиків якості повітря ICP DAS для моніторингу температури, вологості та концентрації твердих частинок у чистих приміщеннях. Інтегроване рішення забезпечує відповідність виробничим стандартам, одночасно підвищуючи ефективність виробництва.

Крім того, ICP DAS створює центр керування для візуалізації даних за допомогою програмного забезпечення для керування хмарою IIoT. Проєкт реалізує моніторинг ліній продукції та виробництва в режимі реального часу, що зрештою підвищує конкурентоспроможність виробника[9].

Німеччина є лідером у сфері промислової автоматизації та інтеграції генеративного ШІ. Наприклад, Siemens розробила Industrial Engineering Copilot, що допомагає інженерам швидше генерувати код PLC для обладнання. Також компанії, як Rockwell Automation і Bosch Rexroth, активно впроваджують AI, роботи та IoT для оптимізації процесів.

США активно інвестують у рішення для штучного інтелекту та IoT для промисловості. Компанії, як SymphonyAI та Hewlett Packard Enterprise, покращують прогностичне обслуговування та застосування ШІ на периферійних пристроях, що дозволяє оптимізувати роботу і управляти даними на промислових підприємствах

Індія зосереджується на вирішенні проблем з управлінням даними та доступністю, що є важливим для масштабування промислового ШІ. Компанія

Tata Consultancy Services (TCS) працює над цією проблемою, використовуючи партнерські мережі та міжгалузевий досвід для подолання цих бар'єрів

Японія активно розвиває робототехніку та рішення для ШІ на периферії. Компанії, як Sony, розробляють платформи для комп'ютерного зору з використанням ШІ, які інтегруються з промисловими IoT пристроями для підвищення точності автоматизації

Ці країни є піонерами в інтеграції технологій, таких як ШІ, IoT та цифрові двійники, що дозволяє створювати більш розумні та ефективні промислові системи по всьому світу.

Висновок до розділу 4

У цьому розділі було розглянуто основні методи та підходи, застосовані під час проведення практичної частини дослідження, а також отримані результати. Виявлено, що впровадження нових технологій та інновацій, зокрема IoT і автоматизації, дозволяє значно підвищити ефективність процесів. Результати демонструють покращення в оперативності та точності виконання завдань, що підтверджується зростанням продуктивності та скороченням витрат. Успішно реалізовані механізми інтеграції штучного інтелекту з IoT системами також показали високу ефективність у зборі та аналізі даних в реальному часі, що сприяло прийняттю обґрунтованих рішень у процесі управління.

Отримані результати підтверджують важливість правильного застосування технологічних рішень для оптимізації робочих процесів, що відкриває нові можливості для подальших досліджень і вдосконалення існуючих систем.

ВИСНОВКИ

Під час виконання кваліфікаційної магістерської роботи були виконані всі поставлені завдання, а саме:

1) проведено аналіз сучасних технологій Інтернету речей (IoT), їхньої архітектури та основних компонентів, що використовуються для інтеграції з виробничими процесами у різних галузях промисловості, вплив IoT на ефективність та продуктивність;

2) визначено основні принципи та концепції Індустрії 4.0, зокрема «розумне виробництво», автоматизацію та кіберфізичні системи;

3) визначено виклики та ризики, пов'язані з впровадженням IoT у виробничу сферу, а також розроблено рекомендації щодо їх подолання;

4) побудовано структурні моделі інтеграції у виробничі процеси вузлів СКУД (турнікети, двері, домофони) від компанії Hikvison у якості IoT-систем, що включають крім просторового структурування ще і структурування в часі (етапи збору, обробки та аналізу даних);

5) розроблено ПЗ для випуску карток для підсистем СКУД на базі HikCentral.

Розвиток систем Інтернету речей (IoT) для інтеграції з Індустрією 4.0 є ключовим етапом цифровізації виробничих процесів. Завдяки IoT забезпечується ефективний обмін даними між обладнанням, підсистемами та працівниками, що сприяє автоматизації, раціональному використанню ресурсів і зростанню продуктивності. Впровадження сенсорів, розумних пристроїв і платформ управління дозволяє здійснювати моніторинг у реальному часі, прогнозувати поломки та адаптувати виробництво до змінюваних умов.

Такі системи стають основою для створення «розумних» фабрик, де виробничі процеси стають прозорими, інтерактивними та адаптивними. Використання аналітики великих даних, штучного інтелекту та машинного навчання в IoT допомагає покращити якість продукції, скоротити простої й оптимізувати витрати. Крім того, інтеграція IoT із системами управління,

такими як ERP, MES і SCADA, відкриває нові можливості для ефективної координації всього виробничого ланцюга.

Впровадження таких технологій має стратегічне значення для компаній, які прагнуть зберігати конкурентоспроможність у світі глобалізації та швидкого технологічного прогресу. Однак успіх впровадження IoT у виробництво залежить від подолання викликів, таких як забезпечення безпеки даних, стандартизація технологій та адаптація існуючої інфраструктури. У результаті інтеграція IoT в Індустрію 4.0 сприятиме формуванню сталого, високоефективного й інноваційного виробничого середовища.

Робота пройшла **апробацію** на XXI Міжнародній науковій конференції «Ольвійський форум – 2024: Стратегії країн Причорноморського регіону в геополітичному просторі» (червень 2024 р., Миколаїв).

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Aneesh Pradeep Integration of IoT and Industry 4.0: Revolutionizing *Industrial Processes Advanced Communication and Intelligent Systems* Серія: Технічні науки. 2023 P.85-96. DOI:10.1007/978-3-031-45124-9_7.

2. HikCentral Professional URL: https://www.hikvision.com/en/products/software/HikCentral-Professional-series/HikCentral-Professional-2-0/ (Last accessed: 18.10.2024).

3. How Industry 4.0 is Revolutionizing Manufacturing Operations? URL: https://www.smartfactorymom.com/blog/how-industry-4-0-is-revolutionizing-manufacturing-operations/ (Last accessed: 15.10.2024).

4. ICP DAS to Make Its SMART FACTORY Expo Debut in Tokyo with Innovative IIoT and ESG Solutions URL: https://www.prnewswire.com/in/news-releases/icp-das-to-make-its-smart-factory-expo-debut-in-tokyo-with-innovative-iiot-and-esg-solutions-302028070.html (Last accessed: 26.10.2024).

5. Industry 4.0. URL: https://www.it.ua/knowledge-base/technology-innovation/industry-4 (Last accessed: 30.04.2024).

6. Internet of Things, IoT URL: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot (дата звернення: 11.10.2024).

7. Internet of Things, IoT. URL: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot (дата звернення: 03.10.2024).

8. Juhi Liladhar Dawale. Rajat Rajesh Singh, Keya Shailendra Gawai, Radhika Abhay Gimonkar Industry 4.0 *International Journal of Advanced Research in Science Communication and Technology* Серія: Технічні науки. 2023. DOI:10.48175/IJARSCT-13103.

9. Jui Pattnayak, Shourav Md Hasibul Hasan, T. Ch. Anil Kumar, K.T. Thilagham IoT and Industry 4.0: Revolutionizing Manufacturing Processes and

Supply Chains *Journal of Informatics Education and Research 4(3)* Серія: Технічні науки. 2024. DOI:10.52783/jier.v4i3.1425.

10. Loso Judijanto, Agus Yulistiyono, Weda Febriyanto Bibliometric Analysis on the Application of IoT in Smart Manufacturing System in Industry 4.0 *West Science Interdisciplinary Studies* Серія: Технічні науки. 2024. 2(08):1566-1578. DOI:10.58812/wsis.v2i08.1225.

11. Manoj Gupta, Tarun Gupta, Prashant Thapliyal, Dharamvir Mangal, Don Biswas Study and Analysis of IoT (Industry 4.0) *Handbook of Smart Manufacturing* Серія: Технічні науки. 2024. P. 29-39. DOI:10.1201/9781003333760-2

12. Murali Krishna Pasupuleti Smart Industry 4.0: Transformative Innovations and Advanced Technologies *In book: Transformative Innovations in Smart Manufacturing* Серія: Технічні науки. 2024. DOI:10.62311/nesx/77691.

13. Oktafina Noor Ulfa The Role of Internet of Things (IoT) on Human Resources in Industry 4.0 *Formosa Journal of Science and Technology* Серія: Технічні науки. 2024. 3(11):2515-2526. DOI:10.55927/fjst.v3i11.12350 .

14. Rebecca Wilson Industry 4.0: skills for the future and learning development *Journal of Learning Development in Higher Education* Серія: Технічні науки. 2024. DOI:10.47408/jldhe.vi32.1462.

15. Scott Halle, Ahmad Elshennawy Evolution of technological leadership with the introduction of industry 4.0 Серія: Технічні науки. October 2024 DOI:10.62704/10057/28461.

16. Smart Factory. URL: https://www.it.ua/knowledge-base/technology-innovation/smart-factory (дата звернення: 30.04.2024).

17. Sushanta K., Paul Industry 4.0: Makes Manufacturing Factory Smatter *International Journal of Research and Innovation in Applied Science* Серія: Технічні науки. 2024. №(119-204). DOI:10.51584/IJRIAS.2024.910019.

18. Teodora Rajković Implementation of Industry 4.0: Examples from the Serbian Manufacturing Industry *Conference: 43rd International Conference on*

Organizational Science Development Серія: Технічні науки. 2024. DOI:10.18690/um.fov.3.2024.61.

19. What’s Currently Happening in Industry 4.0? URL: https://www.startus-insights.com/innovators-guide/whats-currently-happening-in-industry-4-0/#industry-4.0-transformation (Last accessed: 30.10.2024).

20. Індустрія 4.0 – Огляд та наслідки для політики. URL: https://www.beratergruppe-ukraine.de/wordpress/wp-content/uploads/2018/08/PB_06_2018_ukr.pdf (дата звернення: 30.04.2024).

21. Індустрія 4.0 – що це таке та навіщо це Україні. URL: http://surl.li/eskcsf (дата звернення: 04.10.2024).

22. Індустрія 4.0 як інноваційний тренд України. URL: https://interfax.com.ua/news/blog/799334.html (дата звернення: 03.10.2024).

23. Індустрія 4.0. Промисловий Інтернет Речей. URL: http://surl.li/hskeep (дата звернення: 30.04.2024).

24. Інтернет речей IoT. URL: https://kyivstar.ua/business/ (дата звернення 30.04.2024).

25. Київстар впроваджує платформу Cisco Jasper для керування M2M. URL: https://www.unian.ua/economics/telecom/10495674-kijivstar-vprovadzhuye-platformu-cisco-jasper-dlya-keruvannya-m2m.html (дата звернення: 03.10.2024).

26. Системи контролю доступу до дверей. Їх типи та виробники URL: https://superdveri.ua/door-access-control-systems-types-brands/?srsltid=AfmBOoocMuxR4Z0p8mR68XQ5_bQ_7JpKOaH9CsPNNMeo9gxDaVCT8pJZ (дата звернення: 22.10.2024).

27. Стрельбицький А. А., Журавська І. М. Розвиток систем Інтернету речей для інтеграції з індустрією 4.0 та виробничими процесами. *Ольвійський форум-2024: Стратегії країн Причорноморського регіону в геополітичному просторі.* Миколаїв : ЧНУ ім. Петра Могили, 2024. С. 138–141.

28. Управління процесами разом з IoT. URL: https://hub.kyivstar.ua/assets/cms/uploads/005422_whitepaper_iot_fin_4_dbb6e6729c.pdf (дата звернення: 02.10.2024).

29. Що таке Industrial 4.0? URL: https://fiberroad.com/uk/resources/new-trends/what-is-industry-4-0/ (дата звернення: 03.10.2024).

30. Як мобільні оператори заробляють на інтернеті речей. URL: https://mind.ua/publications/20176008-yak-mobilni-operatori-zaroblyayut-na-interneti-rechej (дата звернення: 03.10.2024).

ДОДАТОК А
Код програми

fakereq.asp

```
<%
Session.Timeout = 1
  Response.Buffer = true
  Response.ContentType = "text/plain"
  Response.CharSet = "UTF-8"
    set asPageErr = Server.GetLastError()
    set conFiBi = Server.CreateObject("ADODB.Connection")
    set conFbErr = conFiBi.Errors
    conFiBi.Mode = 3
    conFiBi.Open "DSN=accpoint_db"
    set sqlCmd = Server.CreateObject("ADODB.Command")
    sqlCmd.CommandText = "SELECT current_time FROM rdb$database"
    sqlCmd.CommandTimeout = 5
    sqlCmd.CommandType = 1
    sqlCmd.Prepared = False
    conFiBi.Execute sqlCmd.CommandText
'    set sqlRes = conFiBi.Execute(sqlCmd.CommandText)
'    for each x in sqlRes.Fields
'  Response.Write(CStr(x.Name) + ": " + CStr(x.Value) + "<br>")
'    next
    conFiBi.Close
  Response.Flush
Session.Abandon
%>
```

index.html

```
<!DOCTYPE html>
<html>
```

```
<title>Open Door</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="lib/w3.css">
<link rel="stylesheet" href="lib/w3-theme-theal.css">
<script src="lib/w3data.js"></script>
<body>
 <div class="w3-center">
  <div><br><h1>Відкрити двері</h1><br></div>
  <div id="idP1" class="w3-hide"><br><hr><br>{{sqlRet}}<br></div>
  <div class="w3-dropdown-click">
   <button class="w3-btn w3-red w3-xlarge" onclick="showFloors()" style="width:240px">Де ?</button>
   <div id="idDrop" class="w3-dropdown-content w3-border w3-xlarge" style="width:240px">
    <a onclick="pushMe(7)" href="#">на 7 поверсі</a>
    <a onclick="pushMe(6)" href="#">на 6 поверсі </a>
    <a onclick="pushMe(5)" href="#">на 5 поверсі </a>
    <a onclick="pushMe(4)" href="#">на 4 поверсі </a>
    <a onclick="pushMe(3)" href="#">на 3 поверсі </a>
   </div>
  </div>
 </div>
<script>
var floor;
function showFloors() {
 w3Http("fakereq.asp", function() {
  if ( this.readyState == 4 && this.status != 200 ) {
   window.alert("readyState: " + this.readyState + "\nstatus: " + this.status + "\nText: " +
this.responseText);}
  }
 );
 var o = document.getElementById("idDrop");
 if ( o.className.indexOf("w3-show") === -1 ) {
```

```
   o.className += " w3-show";
  } else {
   o.className = o.className.replace( " w3-show", "" );
  }
}
function pushMe(floor) {
  w3Http("odoor.asp?f=" + floor, function() {
   if ( this.readyState == 4 && this.status == 200 ) {
/*     w3DisplayData( "idP1" , JSON.parse('{ "sqlRet" : "' + this.responseText + '" }') ); */
   window.alert("Двері відчинено!");
   } else if ( this.readyState ==4 && this.status != 200) {
     window.alert("readyState: " + this.readyState + "\nstatus: " + this.status + "\nText: " +
this.responseText);}
   }
  );
}
</script>
</body>
</html>
```

odoor.asp

```
<%
Session.Timeout = 1
Dim fl
  fl = Request.QueryString("f")
Dim numForSec
  numForSec = "0"
Select Case fl
  Case 7
   numForSec = "1578"
  Case 6
   numForSec = "1626"
  Case 5
```

```
    numForSec = "1642"
  Case 4
    numForSec = "1658"
  Case 3
    numForSec = "1674"
  Case else
    numForSec = "-1"
End Select
  Response.Buffer = true
  Response.ContentType = "text/plain"
  Response.CharSet = "utf-8"
    set asPageErr = Server.GetLastError()
    set conFiBi = Server.CreateObject("ADODB.Connection")
    set conFbErr = conFiBi.Errors
    conFiBi.Mode = 3
'    conFiBi.Open "DSN=employee_db"
    conFiBi.Open "DSN=accpoint_db"
'  Response.Write(conFiBi.Provider + "; " + conFiBi.Version + "; " + CStr(conFiBi.State) + "; " +
CStr(conFiBi.Mode) + "; " + CStr(conFiBi.IsolationLevel) + "<br>")
    set sqlCmd = Server.CreateObject("ADODB.Command")
'    sqlCmd.CommandText = "SELECT current_time FROM rdb$database"
'    sqlCmd.CommandText = "UPDATE project SET product='other' WHERE team_leader=85"
    sqlCmd.CommandText = "INSERT INTO events
(D,T,PCARD,PUSER,PCOMPUTER,APPLICATION,EVENT,STATUS,POBJECT,PKEY,PALEVEL,PGLEVEL,COMMEN
TTYPE,COMMENT,PAZONEIN,PAZONEOUT,PVIDEO,PCARDTYPE,DFROM,DTO,PMAKET,LOBJECT)    VALUES
((select ( datediff(day from date '1-Jan-0001' to current_date) + 1 ) from rdb$database),(select
datediff(millisecond from time '0:00:00.000' to current_time) from rdb$database),0,7,13,5,127,Null," +
numForSec + ",0,0,0,133,Null,0,0,0,0,Null,Null,0,Null)"
    sqlCmd.CommandTimeout = 5
    sqlCmd.CommandType = 1
    sqlCmd.Prepared = False
'  Response.Write(sqlCmd.CommandText + "; " + CStr(sqlCmd.CommandTimeout) + "; " +
CStr(sqlCmd.CommandType) + "; " + sqlCmd.Name + "; " + CStr(CInt(sqlCmd.Prepared)) + "; " +
CStr(sqlCmd.State) + "<br><hr><br>")
    conFiBi.BeginTrans
```

```
   conFiBi.Execute("INSERT INTO evout (EVENT,POBJECT,INFO,MISC) VALUES (133," + numForSec + ",6,-
1)")
   conFiBi.Execute sqlCmd.CommandText
   conFiBi.CommitTrans
'    set sqlRes = conFiBi.Execute(sqlCmd.CommandText)
'    for each x in sqlRes.Fields
'  Response.Write(CStr(x.Name) + ": " + CStr(x.Value) + "<br>")
'    next
   conFiBi.Close
  Response.Flush
Session.Abandon
%>
```

ДОДАТОК Б

Апробація роботи

Міністерство освіти і науки України
Чорноморський національний університет імені Петра Могили
Національна академія наук України
Південний науковий центр НАН і МОН України
Інститут української археографії та джерелознавства
ім. М.С. Грушевського НАН України
Державний архів Миколаївської області
ДУ «Національний науковий центр радіаційної медицини НАМН України»
Донецький національний медичний університет
Technical University of Moldova (Moldova)
Jan Dlugosz University in Czestochowa (Poland)
Adam Mickiewicz University (Poland)
Leipzig University of Applied Sciences (Germany)
Rzeszow University of Technology (Poland)
Ca' Foscari University (Italy)

ОЛЬВІЙСЬКИЙ ФОРУМ – 2024:
стратегії країн Причорноморського регіону
в геополітичному просторі

XXI Міжнародна наукова конференція

ТЕЗИ

ТЕХНІЧНІ НАУКИ ТА ІНЖЕНЕРІЯ

20–23 червня 2024 р., м. Миколаїв, Україна

Миколаїв – 2024

домашнього використання, так і для невеликого бізнесу. Компактність, мобільність, економічність, простота установки та доступна ціна роблять його дуже привабливим вибором.

Подальше вдосконалення системи буде полягати у реалізації додаткового функціоналу клієнтського програмного забезпечення, такого, як функції розпізнавання: облич, рухомих об'єктів, видів руху.

Список використаних джерел

1. MarketsandMarkets. Video Surveillance Market Size, Forecast and Industry Trends 2030. URL: https://www.marketsandmarkets.com/Market-Reports/video-surveillance-market-645.html

2. IDC. Video Surveillance and Artificial Intelligence Video Analytics. URL: https://www.idc.com/getdoc.jsp?containerId=IDC_P39911

3. Allied Market Research. Video Surveillance Market Size, Share, Competitive Landscape and Trend Analysis Report by Component, by Enterprise Size, by System Type, by Customer Type, by Application : Global Opportunity Analysis and Industry Forecast, 2023-2032. URL: https://www.alliedmarketresearch.com/Video-Surveillance-market

4. Hangzhou Hikvision Digital Technology Co., Ltd. 2023 3rd Quarter Report. URL:https://www.hikvision.com/content/dam/hikvision/en/investor-relations/annual-quarterly-reports/2023/3Q2023-Financial-Report.PDF

УДК 004.5:33

Стрельбицький А. А.,
магістрант,
Журавська І. М.,
д-р техн. наук, професор,
ЧНУ імені Петра Могили, м. Миколаїв, Україна

РОЗВИТОК СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ІНТЕГРАЦІЇ З ІНДУСТРІЄЮ 4.0 ТА ВИРОБНИЧИМИ ПРОЦЕСАМИ

Індустрія 4.0 є домінуючою тенденцією «Четвертої промислової революції» і відбувається на наших очах.

Зараз ми живемо в епоху завершення третьої цифрової революції, що почалася в другій половині минулого століття. Характеризується розвитком інформаційно-комунікаційних технологій, автоматизацією та роботизацією виробничих процесів.

Індустрія 4.0 характеризується повністю автоматизованим виробництвом, де всі процеси управляються в режимі реального часу та

враховують мінливі зовнішні умови. Кіберфізичні системи створюють віртуальні копії об'єктів у фізичному світі, контролюють фізичні процеси та приймають децентралізовані рішення. Вони можуть інтегруватися, взаємодіяти в реальному часі, самоналаштовуватися та самонавчатися. Важливу роль відіграють Інтернет-технології, які забезпечують зв'язок між людьми та машинами. Компанія виробляє продукцію відповідно до вимог індивідуальних замовників та оптимізує витрати на виробництво.

Сьогодні більшість виробників впроваджують технології Industry 4.0 для оптимізації бізнес-процесів, для впровадження нових бізнес-моделей тощо. Враховуючи вищезазначену ситуацію та величезні масштаби ринку Індустрії 4.0, її розвиток є одним із стратегічних завдань українських підприємств та уряду, а цифровізація має бути використана для досягнення прориву від оригінальної економіки до Індустрії 4.0 (рис.1). Розумні галузі, розумні підприємства, розумні міста, розумні речі. Цей прогрес стане можливим із розвитком ключових компонентів Індустрії 4.0, таких як Інтернет речей (IoT).

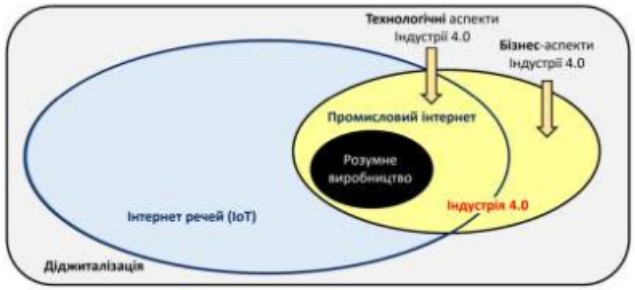

Рис.1. Зв'язок між діджиталізацією, Інтернетом речей та Індустрією 4.0

Автоматизовані процеси відіграють важливу роль в успішній роботі бізнесу. По-перше, вони часто автоматизують рутинні процеси, які можна описати простими алгоритмами дій: які параметри потрібно перевіряти, куди передавати результати, куди перевіряти граничні відхилення, що робити, коли відбувається конкретна подія.

Щоб дистанційно зчитувати будь-який індикатор і передавати цю інформацію, необхідно забезпечити канал зв'язку між пристроями, щоб допомогти їм «розмовляти» один з одним. Раніше такі канали були

можливі лише через дротове з'єднання, але завдяки прогресу стільникового зв'язку та технологій це було замінено бездротовою передачею даних. Все це дає можливість проводити дистанційні вимірювання віддалених об'єктів або індикаторів у мобільних рухомих механізмах. Ця технологія взаємодії машин називається Machine-to-Machine (скорочено M2M).

У технології M2M для передачі даних використовуються різні канали: Інтернет, SMS, CSD або голосові канали. За допомогою будь-якого з них можна організувати передачу даних «точка-точка» між двома об'єктами. Найбільш популярним і доступним є Інтернет.

Слід зазначити, що IoT є набагато складнішим явищем, ніж простий сенсор. Використання датчиків для збору та аналізу даних про різні об'єкти – будь то механізми, будівлі чи люди – існує вже давно. Промисловий Інтернет унікальний тим, що датчики об'єднані в єдину мережу з системами аналізу та контролю. Тому об'єкт має власну мережу, в якій відбувається обмін даними. Ці дані служать основою для автоматизованого прийняття рішень і дій з управління аудиторією. Так виникли елементи штучного інтелекту та принцип саморегуляції.

Технології бездротової передачі даних відрізняються за відстанню передачі: на близьку відстань, на коротку відстань і на дальню відстань. Деякі з цих технологій вимагають ліцензій, всі інші називаються відкритими.

До Proximity (технологія щільного контакту) відносять:
- NFC.

До Short Range (технологія короткого діапазону) відносять:
- Bluetooth;
- MiFi;
- ZigBee;
- Z-Wave;
- WiFi.

До Long Range (технологія дальнього діапазону) відносять:
- GSM/LTE (ліцензована);
- NB-IoT (ліцензована);
- WiMAX (ліцензована);
- SigFox (відкрита);
- LoRa (відкрита).

При виборі технології для забезпечення автоматизації бізнес-процесів слід враховувати наступні параметри:
- Яким буде пристрій – мобільним чи стаціонарним?
- Як далеко від точки збору даних працюватимуть пристрої?
- Чи є джерело живлення для пристрою?

– Який середній обсяг пакета даних, який буде передано?
– З якою періодичністю слід збирати дані пристрою?
– Де розміщуватимуться прилади – на вулиці, у приміщеннях із залізобетону чи інших матеріалів, у підвалі чи на підлозі?
– Наскільки сильні перешкоди сигналу?
– Які додаткові канали зв'язку потрібні пристрою?

Відповіді на ці питання допоможуть вибрати технологію, яка зможе забезпечити працездатність ваших пристроїв і автоматизувати їх роботу.

Використання технологій M2M та IoT є надзвичайно важливим і необхідним у сферах, де потрібна автоматизація процесів. Особливо активно IoT розвивається у сферах сільського господарства, логістики, Smart Cities – скрізь, де необхідно ретельно стежити за станом об'єктів або збирати великі масиви даних для подальшого аналізу. IoT заощаджує витрати на обслуговування обладнання: датчики збирають інформацію про стан обладнання, тому технічне обслуговування та ремонти виконуються вчасно.

Список використаних джерел

1. Industry 4.0. URL: https://www.it.ua/knowledge-base/technology-innovation/industry-4 (дата звернення 30.04.2024).
2. Індустрія 4.0 – Огляд та наслідки для політики. URL: https://www.beratergruppe-ukraine.de/wordpress/wp-content/uploads/2018/08/PB_06_2018_ukr.pdf (дата звернення 30.04.2024).
3. Інтернет речей IoT URL: https://kyivstar.ua/business/ (дата звернення 30.04.2024).

УДК 004.725.5

Тогоєв О. Р.,
викладач кафедри комп'ютерної інженерії,
ЧНУ імені Петра Могили, м. Миколаїв, Україна

ЗАСОБИ LTE-СНІФІНГУ

Сніфер LTE пасивно перехоплює бездротовий трафік абонентів базової станції 4G. Завдяки особливостям передачі трафіку LTE, будь-хто з відповідним обладнанням може перехоплювати ці сигнали. Імітуючи поведінку користувацького обладнання, такого як смартфон і