

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ
СІКОРСЬКОГО"**

Факультет електроніки

(повна назва інституту/факультету)

Кафедра акустичних та мультимедійних електронних систем

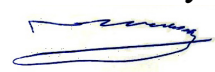
(повна назва кафедри)

"На правах рукопису"

УДК 621.396.9:021

"До захисту допущено"

Завідувач кафедри

 С.А. Найда
(ініціали, прізвище)

" 16 " грудня 2021 р

Магістерська дисертація

зі спеціальності (спеціалізації) 171 Електроніка

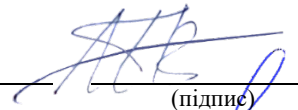
(код і назва)

на тему: "Система контролю промислового підприємства на основі технології радіочастотної ідентифікації"

Виконав: студент II курсу, групи ДВ-01мп
(шифр групи)

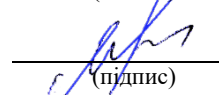
Байдюк Анастасія Владиславівна

(прізвище, ім'я, по батькові)


(підпис)

Керівник доцент, к.т.н., с.н.с. Макаренко В. В.

(посада, вчене звання, науковий ступінь, прізвище, ініціали)


(підпис)

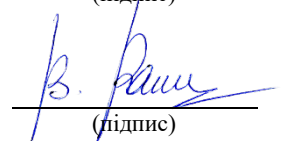
Консультант

(посада, науковий ступінь, вчене звання, прізвище, ініціали)

(підпис)

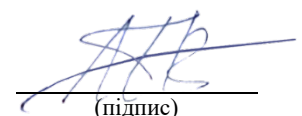
Рецензент зав. відділом і-ту Кібернетики НАН України,
професор, д.т.н., Романов В.А.

(посада, вчене звання, науковий ступінь, прізвище, ініціали)


(підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент


(підпис)

Київ – 2021 року

**Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"**

Інститут (факультет) _____ Факультет електроніки
(повна назва)

Кафедра _____ Акустичних та мультимедійних електронних систем
(повна назва)

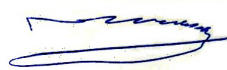
Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою;

Спеціальність (освітня програма) _____ 171 Електроніка (Електронні системи
мультимедіа та засоби Інтернету речей)

(код і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри

 С.А. Найда
(ініціали, прізвище)

"10" вересня 2021 р.

**ЗАВДАННЯ
на магістерську дисертацію студенту**

_____ Байдюк Анастасії Владиславівні

(прізвище, ім'я, по батькові)

1. Тема роботи Система контролю промислового підприємства на основі технології радіочастотної ідентифікації

науковий керівник дисертації Макаренко Володимир Васильович, доцент, с.н.с.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від "03" листопада 2021 р. № 3666-с

2. Срок подання студентом роботи 10.12.2021

3. Об'єкт дослідження Автоматизація промислового підприємства на основі технології радіочастотної ідентифікації

4. Предмет дослідження Система радіочастотної ідентифікації для контролю промислового підприємства

5. Перелік завдань, які потрібно розробити 1. Аналітичний аналіз апаратних та програмних компонентів систем радіочастотної ідентифікації та можливостей застосування систем для автоматизації виробництва. 2. Розробка структурної та функціональної схеми системи радіочастотної ідентифікації. 3. Вибір пристроїв для реалізації системи. 4. Розробка стартап-проекту.

6. Перелік графічного (ілюстративного) матеріалу Креслення плану об'єкту для контролю та автоматизації, функціональна схема системи контролю та управління доступом, функціональна система системи управління складом, розміщення пристроїв на плані об'єкту

7. Орієнтовний перелік публікацій _____

8. Консультанти розділів дисертації*

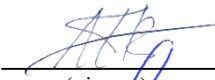
Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Написання першого розділу	29.09.2021	Виконано
2	Написання другого розділу	25.10.2021	Виконано
3	Написання третього розділу	25.11.2021	Виконано
4	Написання четвертого розділу	30.11.2021	Виконано

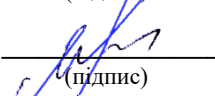
Студент


(підпис)

Анастасія БАЙДЮК

(ініціали, прізвище)

Науковий керівник дисертації


(підпис)

Володимир МАКАРЕНКО

(ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника

УДК 621.396.9:021

РЕФЕРАТ

Байдюк А.В. Система контролю промислового підприємства на основі технології радіочастотної ідентифікації: магістерська дис.: 171 Електроніка / Байдюк Анастасія Владиславівна. – Київ, 2021. – 120 с.

Ключові слова: радіочастотна ідентифікація, транспондер, зчитувач, промисловість, склад, система, автоматизація, антена.

Актуальність дослідження. Автоматизація – це один із головних напрямів розвитку виробництва, оскільки цей процес збільшує точність та швидкість роботи з обладнанням та виключає людський фактор. Технологія радіочастотної ідентифікації може забезпечити автоматизацію багатьох виробничих процесів, зокрема моніторинг, інвентаризація, контроль доступу до приміщень, охорона праці та забезпечення ланцюжка поставок.

Метою дослідження є створення системи контролю виробничих процесів на основі технології радіочастотної ідентифікації.

Об'єкт дослідження – автоматизація промислового підприємства на основі технології радіочастотної ідентифікації.

Предмет дослідження – система радіочастотної ідентифікації.

Методи дослідження – розробка системи радіочастотної ідентифікації та аналіз компонентів для реалізації системи.

Наукова новизна одержаних результатів: запропонована система автоматизація складу з використанням технології радіочастотної ідентифікації.

Практичне значення одержаних результатів: У результаті виконання дипломної роботи було розроблено систему автоматизації для складу. Проведено аналіз компонентів для використання у створеному рішенні. Отримані результати досліджень можуть бути використані компаніями для автоматизації складської логістики.

Апробація результатів дисертації: проектування системи контролю складу.

ABSTRACT

Baidiuk A.V. Control system of an industrial enterprise on the basis of radio frequency identification technology: master's dis: 171 Electronics / Baidiuk Anastasiia. – Kyiv, 2021. – 120 p.

Keywords: radio frequency identification, transponder, reader, industry, composition, system, automation, antenna.

This paper describes the development of a warehouse automation system. This first section provides an analytical analysis of RFID systems. The basic principles of radio frequency identification, hardware and software components are considered. The security and confidentiality of these systems play an important role in RFID solutions. Therefore, the paper examines the means of protection against potential attacks. Radio frequency identification is becoming widely used in the enterprise. Areas of application at the enterprise such as monitoring of production processes, access control systems to the premises, labor protection, as well as supply chain provision were considered. The issue of peculiarities of application of radio frequency identification technology at the enterprise is also covered.

The second section provides the development of warehouse automation system, which includes WMS-system, Access control and management system and protection system for employees. Initially, a drawing of the object and a concept of the system were developed. Next, the structural and functional scheme of this system was designed. The third section provides the choice of devices for system implementation is substantiated. Readers, antennas, transponders and software were selected.

The fourth section provides startup project. The essence of the startup is to automate the work of the library. Introduction of passive ultra-high frequency (UHF) radio frequency identification system. This technology is regulated by the ISO 18000-6-c standard and operates in the 860-960 MHz band.

ЗМІСТ

Скорочення та умовні позначення.....	8
Вступ.....	10
1 Аналітичний огляд	11
1.1 Основні засади технології радіочастотної ідентифікації.....	11
1.2 Аналіз компонентів RFID-системи	15
1.2.1 Апаратні компоненти	15
1.2.2 Програмні компоненти	21
1.3 Безпека та конфіденційність у системах RFID	24
1.4 Особливості застосування технології радіочастотної ідентифікації на підприємстві	27
1.5 Огляд систем радіочастотної ідентифікації для автоматизація виробництва.....	30
1.5.1 Моніторинг виробничих процесів	30
1.5.2 Системи контролю та управління доступом	32
1.5.3 Охорона праці	34
1.5.4 Забезпечення ланцюжка поставок	35
Висновки до розділу	36
2 Розробка структурної та функціональної схем системи	38
2.1 Розробка плану об'єкту контролю та автоматизації	38
2.2 Опис системи радіочастотної ідентифікації	39
2.3 Функціональна схема системи радіочастотної ідентифікації	41
Висновки до розділу	46
3 Обґрунтування вибору пристроїв для реалізації системи	48
3.1 Вибір зчитувачів	48
3.2 Вибір антен	52
3.3 Вибір транспондерів	76
3.4 Вибір програмного забезпечення	79
3.5 Вибір додаткових компонентів	82

3.6 Розрахунок вартості системи контролю та управління складом	88
Висновки до розділу	89
4 Розробка стартап проекту	91
4.1 Опис ідеї проекту	91
4.2 Технологічний аудит ідеї проекту	92
4.3 Аналіз ринкових можливостей запуску стартап-проекту	93
4.4 Розроблення ринкової стратегії проекту	96
4.5 Розроблення маркетингової програми стартап-проекту.....	97
4.6 Фінансово-економічний аналіз.....	97
Висновки до розділу	98
Висновки	100
Перелік джерел посилання	101
Додаток А Abstract	103
Додаток Б Технічне завдання.....	108
Додаток В План об'єкту	112
Додаток Г Функціональна схема системи контролю та управління доступом	114
Додаток Д Функціональна схема системи управління складом.....	116
Додаток Е Розміщення обладнання на плані об'єкту.....	118

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

АЦП	– аналогово-цифровий перетворювач;
ВЧ	– високочастотний;
ІС	– інтегральна схема;
НВЧ	– надвисокочастотний;
ПВХ	– Полівінілхлорид;
ПЗ	– програмне забезпечення;
РЧ	– радіочастотний;
СКУД	– системи контролю та управління доступом;
АМ	– Amplitude Modulation (амплітудна модуляція);
API	– Application Programming Interface (Прикладний програмний інтерфейс);
AUX	– auxiliary channels (допоміжні канали);
CMOS	– Complementary Metal–Oxide–Semiconductor (комплементарна структура метал-оксид-напівпровідник);
DHCP	– Dynamic Host Configuration Protocol (протокол динамічної конфігурації вузла);
DOS	– Disk Operating System (дисксова операційна система);
EEPROM	– Electrically Erasable Programmable Read-Only Memory (Електрично видаляема програмована пам'ять лише для читання);
ERP	– Enterprise Resource Planning System (Система планування ресурсів підприємства);
FM	– Frequency Modulation (фазова модуляція);
FOD	– Foreign Object Damage (пошкодження стороннім об'єктом);
IEEE	– Institute of Electrical and Electronics Engineers (Інститут інженерів з електротехніки та електроніки);

ISO	– International Organization for Standardization (Міжнародна організація зі стандартизації);
IoT	– Internet of Things (Інтернет речей);
MAC	– Media Access Control (Управління доступом до середовища);
MAS	– Master Accounting Series (серія програм для бухгалтерського обліку);
NRZ	– Non Return to Zero (код без повернення до нуля);
PCB	– printed circuit board (друкована плата);
PIE	– Pulse-Interval Encoding (Імпульсно-інтервальне кодування);
PM	– Phase Modulation (фазова модуляція);
RFID	– Radio Frequency Identification (радіочастотна ідентифікація);
RO	– Read-Only (тільки для читання);
RTLS	– Real-time Locating Systems (система позиціонування в режимі реального часу);
SCM	– Supply Chain Management (управління ланцюгом поставок);
SMA	– sub-miniature version A (субмініатюрна версія A);
TCP/IP	– Transmission Control Protocol / Internet Protocol (протокол керування передаванням / міжмережевий протокол);
USB	– Universal Serial Bus (універсальна послідовна шина);
UWB	– Ultra Wide Band (надширокосмуговий);
Wi-Fi	– Wireless Fidelity (безпроводна точність);
WORM	– Write Once Read Many (однин запис і багаторазове зчитування інформації);
WMS	– Warehouse Management System (Система управління складом);

ВСТУП

Технології автоматичного збору даних та ідентифікації стають все більш важливими в управлінні ланцюгом поставок, управлінні виробничими потоками, відстеження мобільних активів, управління запасами, складами та будь-якими додатками, де важливо знати точне місцезнаходження об'єктів.

Радіочастотна ідентифікація (RFID) – це безпроводова технологія для ідентифікації об'єктів, яка використовується для реалізації систем автоматизації у різних сферах. RFID використовує електромагнітні хвилі для передачі та отримання інформації, що зберігається в транспондері, до та від зчитувача. Ця технологія має ряд переваг у порівнянні зі звичайними способами ідентифікації, таких як більша дальність зчитування, швидша передача даних, відсутність вимоги до прямої видимості та здатність зчитувати велику кількість тегів одночасно.

Технологія радіочастотної ідентифікації найбільш повно відповідає всім вимогам комп'ютерної системи управління, де потрібне розпізнавання і реєстрація об'єктів і прав користувачів у реальному масштабі часу. Тому систему автоматизації складу було розроблено на основі цієї технології. Система включає моніторинг об'єктів на складі, систему контролю та управління доступом, а також систему безпеки для роботи з транспортними засобами.

1 АНАЛІТИЧНИЙ ОГЛЯД

1.1 Основні засади технології радіочастотної ідентифікації

Радіочастотна ідентифікація (RFID) – загальний термін для технологій, що використовують радіочастоти для передачі даних. У найбільш простій реалізації система RFID складається з мітки-ідентифікатора, яка прикріплена до об'єкта, і зчитувача, який може опитувати тег, для того, щоб ідентифікувати мітку та отримати інформацію, записану на мітці (рис. 1.1). Технологія набуває широкого розповсюдження завдяки зростанню кількості можливих областей застосування: від безконтактної картки проїзду до автоматизації виробничих процесів.

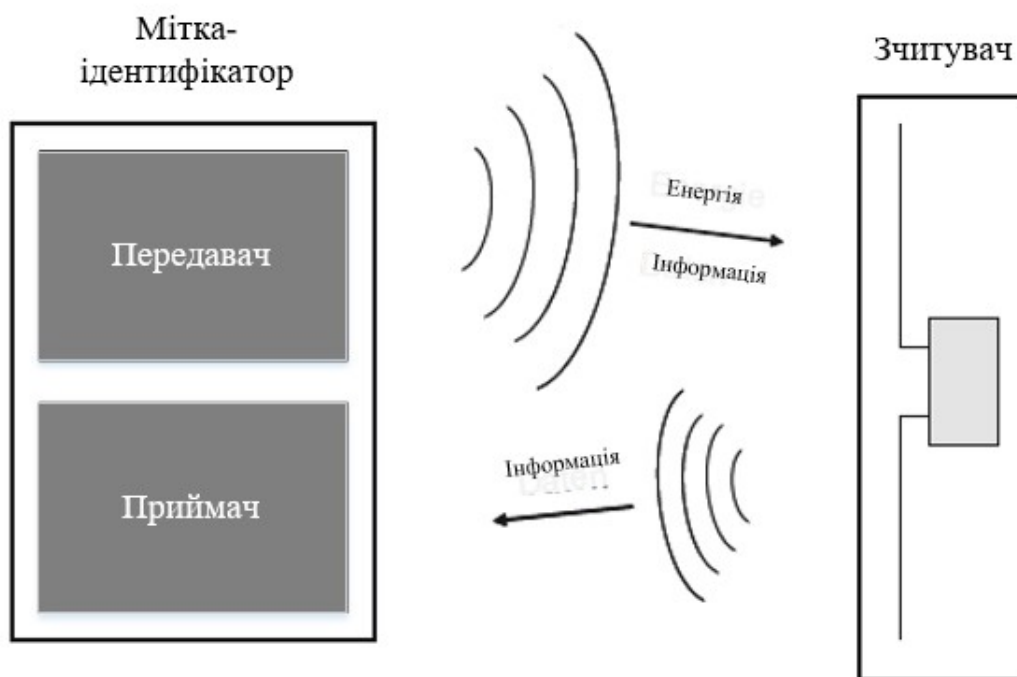


Рисунок 1.1 – Найпростіша RFID-система

Тег призначений для зберігання певної інформації, розмір якої коливається від 32 бітів до 32 000 байт. Теги можуть бути як пасивними, так і активними. Зчитувач RFID діє як ведучий для тегу і підлеглий для хосту програми. Ця концепція ведучий-підлеглий (master-slave) зображена на рис. 1.2.

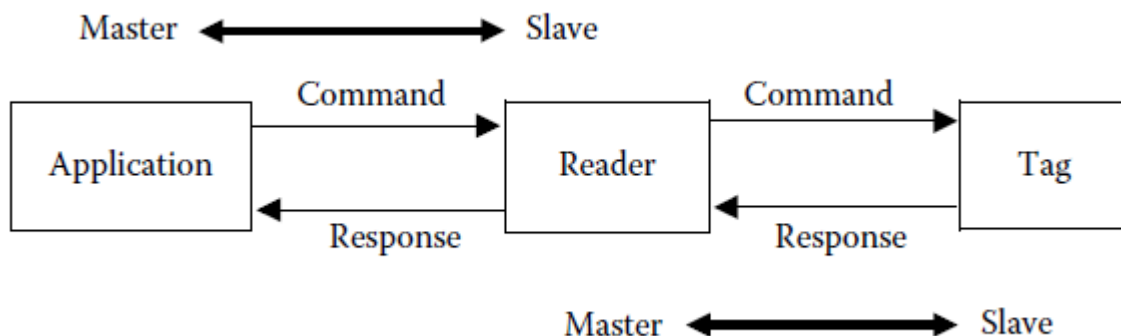


Рисунок 1.2 – Архітектура «ведучий-підлеглий» (master-slave) RFID-системи

У свою чергу теги знаходяться у зоні зчитування цього зчитувача. Зона зчитування – це фізична відстань, на якій сила електромагнітних хвиль, що генерується зчитувачем, здатна жити теги, приймати сигнали тегів і успішно їх декодувати. У будь-який момент зчитувач може прочитати лише один тег у межах своєї зони опитування, а тег може бути прочитаним лише одним зчитувачем.

Найпоширенішим методом передавання сигналу у радіочастотних системах є передавання сигналу за допомогою амплітудної модуляції.

Згідно з загальновідомим законом (1) на радіосигнал впливає амплітуда (A), кутова частота (ω), а також фаза (φ) сигналу. Відповідно до цього закону існують такі типи модуляції як амплітудна (AM), частотна (FM) і фазова (PM).

$$s(t) = A(t) \cdot \cos [\omega t + \varphi(t)] \quad (1)$$

Амплітудна модуляція проблематична для систем з різними втратами каналу. Частотна модуляція збільшує вимоги до частотного діапазону у якому працює система. Фазова модуляція обмежена можливостями обладнання. Всі ці методи можна комбінувати задля зменшення недоліків кожного способу та досягнення кращої якості передавання сигналу.

Система радіочастотної ідентифікації (RFID) має багато переваг перед іншими системами ідентифікації, включаючи системи штрих-кодів, оптичні

системи розпізнавання символів, розумні картки та біометричні дані (голос, відбитки пальців, сканування сітківки), оскільки вона не вимагає прямої видимості, підтримує суворі фізичні умови, підтримує стійку та енергоефективну роботу та дозволяє одночасно ідентифікувати велику кількість тегів.

Важливо також враховувати обмеження технології. У середовищах з великої кількістю металевих предметів або ж робота у несприятливих умовах (висока температура, підвищена вологість тощо) варто обирати системи, які мають найвищу відмовостійкість у заданих умовах, наприклад низькочастотні системи.

Як і інші радіосистеми, система RFID вимагає протоколів середнього контролю доступу (MAC) для обходу різних типів зіткнень, оскільки вони витрачають ресурси мережі та уповільнюють процедуру зчитування. Потрібна додаткова ефективність у випадку RFID через обмежені можливості тегів з точки зору обробки та пам'яті.

Стандарти RFID традиційно розроблялися за допомогою процесу Міжнародної організації стандартизації. Наприклад, ISO розробила такі стандарти як ISO 18000-6A та 18000-6B для діапазону НВЧ, які використовуються у всьому світі. Кодування даних відноситься до обробки даних з моменту, коли сигнал надходить до RFID-мітки і повертається назад до зчитувача.

Для RFID було визначено кілька алгоритмів кодування даних; вибір впливає на вартість впровадження, відновлення помилок та надійність даних. Крім того, було розроблено кілька типів алгоритмів кодування даних. Перелік можливостей синхронізації кодування та інші аспекти методів проектування систем RFID були встановлені стандартами RFID, такими як ISO 14443, ISO 15693, ISO 18000-6. Нижче наведено перелік методів кодування використовується для індуктивних та/або ємнісних систем RFID [1]:

1. NRZ (пряме). У цьому методі двійковий біт 1 представлений однією значущою умовою (логічний високий рівень), а двійковий 0 представлений іншим (логічний низький рівень) [1].

2. Манчестерське кодування. Цей механізм кодування, також називають розділеним фазовим кодуванням, не вимагає ніякої додаткової інформації про

тактовий сигнал передачі. Зміна рівню завжди відбувається у середині тактового циклу. 0 перетворюється на перехід від низького до високого (від 0 до 1), а 1 перетворюється на перехід від високого до низького (від 1 до 0) [1].

3. Кодування Міллера. У цьому кодуванні двійкове значення 1 представлено переходом (від низького до високого або від високого до низького) посередині тактового циклу. Двійкове число 0 представлено продовженням логічного стану 1 протягом наступного тактового циклу. Якщо відбувається послідовність двійкових нулів, перехід відбувається на початку тактового циклу. Більш того, послідовність Міллера може складатися з двох, чотирьох або восьми циклів/біт [1].

4. Модифіковане кодування Міллера. У цьому механізмі кожен перехід замінюється коротким негативним імпульсом [1].

5. Кодування FM0. Також відоме як двофазне кодування, тут перехід відбувається на початку кожного тактового циклу. Двійковий 0 представлений додатковим переходом у середині тактового циклу, а двійкова 1 представлена відсутністю переходу в середині тактового циклу [1].

6. Уніполярне кодування. У цьому методі двійкова 1 відповідає високому логічному рівню протягом першої половини тактового циклу та двійкове значення 0 представлено низьким логічним рівнем протягом тривалості тактового циклу [1].

7. Диференційне кодування. При диференційному кодуванні двійкове значення 1 змінює логічний рівень, а двійковий 0 не викликає змін на логічному рівні [1].

8. Диференційне двофазне кодування. У цьому механізмі зміна рівня відбувається в середині тактового циклу. А 1 відображається зміною рівня на початку годинника, а 0 - відсутністю зміни рівня на початку годинника [1].

9. Імпульсно-інтервальне кодування (PIE). Також називається кодуванням з імпульсною паузою, тут двійкове значення 1 представлено паузою тривалістю $2T$ перед наступним імпульсом, а двійкове значення 0 представлено паузою тривалості T перед наступним імпульсом [1].

1.2 Аналіз компонентів RFID-системи

1.2.1 Апаратні компоненти

Система RFID складається з зчитувача, мітки та програмного забезпечення. Зчитувач містить модуль радіочастотного приймача (передавач і приймач), процесор сигналу та блок керування, з'єднувальний елемент (антену) та послідовний інтерфейс даних (RS232, RS485) до головної системи.

Мітка виконує функцію програмованого пристрою для передачі даних і складається з елемента зв'язку (резонансна налаштована схема) та малопотужної CMOS-мікросхеми. Мікросхема містить аналоговий радіочастотний інтерфейс, конденсатор для налаштування антени, випрямляючу систему, цифрове управління та програмовану пам'ять лише для читання (EEPROM) та схеми модуляції даних. RFID передбачає безконтактне зчитування та запис даних у енергонезалежну пам'ять мітки через радіосигнал. Теги RFID бувають різних розмірів і можуть бути призначені для використання в різних видах середовища (рис. 1.3).



Рисунок 1.3 – Різні типи RFID-міток

Зчитувач видає радіочастотний сигнал, і обмінюється даними, коли тег наближається до сигналу зчитувача. Теги можна класифікувати таким чином:

- активна мітка, яка має акумулятор, що забезпечує живлення всіх функцій;

- напівактивна мітка, яка має акумулятор, який використовується тільки для живлення мікросхеми мітки, а не для зв'язку;
- пасивна мітка, яка не має батареї, відсутність джерела живлення робить пасивні мітки більш дешевшими та надійними, ніж активні.

Інтегральна схема – головний елемент мітки RFID. Це кремнієвий чіп з розмірами зазвичай менше, ніж 1×1 мм (рис. 1.4). Мікросхема мітки працює як мікропроцесор. Мікросхема має єдине основне призначення – передати унікальний ідентифікатор тегу. Унікальний ідентифікатор зберігається в пам'яті мікросхеми. Коли мікросхема живиться від енергії, що надходить від антени тегів, її логічна схема отримує ідентифікаційний номер, що зберігається в пам'яті, а потім модулює сигнал зворотного розсіювання для передачі цієї інформації. Залежно від типу та призначення тегу, мікросхема може мати додаткову пам'ять, на яку користувач може записати додаткову інформацію за допомогою зчитувача [2].

Мітки в основному працюють на високочастотних (ВЧ) або надвисоких частотах (НВЧ). ВЧ-мітки, як правило, обмежені в діапазонах, що вимірюються в дюймах. Це надає ВЧ-міткам перевагу у застосуванні для інвентаризації, де товари знаходяться в безпосередній близькості один від одного та в безпосередній близькості до читача.

Мітки також класифікують за типом пам'яті:

- тільки для читання (RO);
- WORM (записати можна тільки один раз, зчитувати – багато разів);
- RW (багаторазове зчитування/запис);
- енергозалежне сховище (для виконання розрахунків після включення).

В основі інтегральних схем радіочастотної мітки лежать транзистори, що використовуються для їх побудови. Основна функція транзистора – забезпечити підсилення сигналу. Призначення антени пасивної мітки – отримувати живлення від зчитувача і після цього передавати свій ідентифікатор у відповідь.

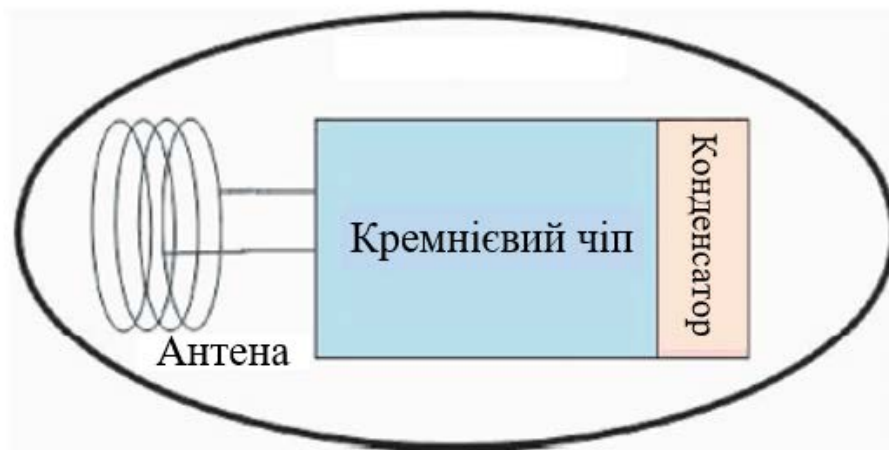


Рисунок 1.4 – Будова RFID-мітки

Розмір антени тегу визначає розмір тегу, оскільки він є найбільшим компонентом тегу. Антена відповідає за передачу і прийом радіохвиль, отже, забезпечує зв'язок. Для пасивних міток RFID антена також діє як трансформатор енергії для живлення мікросхеми тегу від енергії, отриманої від випромінювання антеною зчитувача. Антена мітки збирає енергію, що надходить на її клеми за допомогою механізму зв'язку, і подає її до випрямляча всередині мікросхеми, щоб перетворити її в постійну потужність. У залежності від конкретного застосування, антена тегу може мати багато різних конфігурацій [2].

На відміну від більшості інших радіочастотних систем, у яких антени розроблені переважно для навантажень 50 Ом або 75 Ом, антену з RFID-міткою потрібно безпосередньо узгоджувати з мікросхемою мітки, яка в першу чергу має великий вхідний опір. Цей крок є важливим для забезпечення максимальної передачі потужності від антени до мікросхеми і, отже, оптимізації роботи транспондера. Тому техніка узгодження імпедансу відіграє важливу роль в успішній розробці RFID-мітки.

Еквівалентна схема підключення антени показана на рис. 1.5. Напруга V_s формується від приймального сигналу. Антена має комплексний вхідний опір Z_{ANT} . Чіп також має опір навантаження Z_{LOAD} , який залежить від частоти. Опір навантаження специфічний для конструкції мікросхеми мітки і його можна

виміряти. Для того, щоб забезпечити максимальну передачу потужності від антени до навантаження, вхідний опір антени повинен бути спільно узгоджений з опором мікросхеми на робочій частоті мітки. Тобто, реальна частина вхідного опору антени повинна дорівнювати дійсній частині імпедансу навантаження, а уявна частина вхідного опору антени повинна дорівнювати протилежності уявної частини імпедансу навантаження.

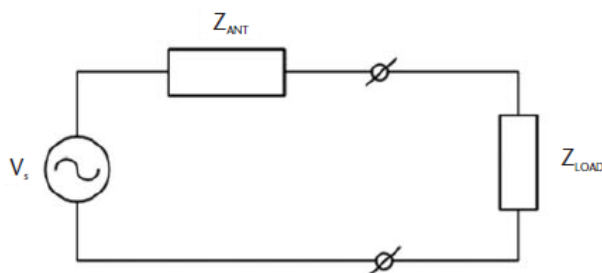


Рисунок 1.5 – Еквівалентна схема RFID-мітки

Субстрат – це матеріал, який утримує усі елементи мітки разом. Підкладка може бути жорсткою або гнучкою у залежності від застосування, а також може бути виготовлений з декількох різних типів матеріалів. Наприклад, при використанні контрольних RFID-міток у шинах автомобіля, для моніторингу стану автомобільних шин. Коли машина працює, внутрішня частина шини нагрівається до дуже високої температури, і вона знаходиться під високим тиском. Це суворе середовище накладає кілька обмежень на підкладку тегів, і тег повинен бути розміщений всередині захисної капсули для захисту антени та мікросхеми. В іншому прикладі, для RFID-тегів, що використовуються як для відстеження документів, потрібна гнучка підкладка, щоб RFID -мітки могли згинатись так само, як папір, до якого він прикріплений. У деяких особливих випадках середовище для розміщення міток дуже суворе, і розміри тегів стають основною проблемою. Спеціально розроблені підкладки, такі як гнучка магнітна композитна підкладка, можуть допомогти зменшити форм-фактор антени, одночасно зменшуючи вартість мітки.

В історії проектування RFID існували два принципово різні підходи до проектування для передачі енергії від зчитувача до тегу: магнітна індукція та

захоплення електромагнітних хвиль. Ці дві конструкції використовують електромагнітні властивості, пов'язані з радіочастотною антеною; ближнє поле і дальнє поле. Якщо через котушку пропускати змінний струм, він створюватиме змінне магнітне поле у самій котушці, і це називається ближнім полем. Ця схема також призведе до розповсюдження електромагнітних хвиль у просторі, це називається дальнім полем і є принципом радіопередачі. Обидві властивості радіоприймача можуть бути використані для передачі достатньої потужності віддаленому тегу для підтримки його роботи, як правило, від 10 мкВт до 1 мВт залежно від типу мітки, а також за допомогою модуляції можуть передавати та приймати дані [3].

Використання зв'язку ближнього поля між зчитувачем і тегом можна описати з точки зору принципу магнітної індукції Фарадея. Зчитувач пропускає великий змінний струм через котушку зчитувача, у результаті чого в ній виникає змінне магнітне поле. Якщо в цьому полі розмістити мітку, що містить котушку меншого розміру, на ній з'явиться змінна напруга, а якщо котушку з'єднати з конденсатором, відбудеться накопичення заряду, який можна використовувати для живлення чіпу мітки. Теги, які використовують зв'язок ближнього поля, надсилають дані до читача за допомогою модуляції навантаження.

Оскільки будь-який струм, що генерується котушкою мітки, породжує її власне магнітне поле, яке буде протидіяти полю зчитувача, це можна виявити на котушці зчитувача як невелике збільшення струму, що протікає через нього. Цей струм пропорційний навантаженню на котушку мітки, і це той самий принцип, який використовується в силових трансформаторах, хоча зазвичай первинна та вторинна обмотки трансформатора намотані щільно для забезпечення ефективної передачі енергії. Таким чином, якщо електроніка мітки накладає навантаження на свою котушку антени і змінює її з плином часу, може бути створений сигнал, який кодує ідентифікатор мітки, і зчитувач може відновити цей сигнал, відстежуючи зміну струму через котушку зчитувача. Можливі різноманітні модуляції у залежності від кількості необхідних бітів ідентифікатора, швидкості передачі

даних та додаткових надлишкових бітів, розміщених у коді для усунення помилок, спричинених шумом у каналі зв'язку.

Зчитувач – це пристрій, який виконує роль ведучого (master), забезпечує енергію мітки і запускає сигнали зв'язку, щоб змусити мітку виконати запитувану дію. Управління зчитувачем може здійснюватися за допомогою комп'ютерного терміналу або автоматичного виконання сценаріїв програми. Стаціонарні зчитувачі підключаються до ліній електроживлення та зв'язку, тоді як мобільні ручні зчитувачі не підключені до електромережі або зв'язку (рис. 1.6). Для подальшого обміну даними зчитувач може бути підключений до головного комп'ютера або бази даних.



Рисунок 1.6 – Стаціонарний та мобільний зчитувач

Зчитувач складається з блоку управління та радіочастотного блоку, що містить передавальні та приймальні модулі. У блоці управління вбудоване програмне та апаратне забезпечення відповідає за управління зчитувачем, зв'язком з головним комп'ютером та тегоми, а також за обробку даних. Передавач генерує радіочастотний сигнал (частоту та рівень потужності). Він підключений до резонансної схеми антени. Приймальна частина приймає радіочастотний сигнал, генерований тегом, демодулює та декодує дані та надсилає двійкові дані на блок управління для подальшої обробки [4].

1.2.2 Програмні компоненти

Будь-яка RFID система управляється деяким спеціальним програмним забезпеченням (ПЗ), яке може бути вбудовано в контролер або бути більш складним, на керуючих комп'ютерах або серверах, аж до глобальних територіально-розподілених систем [5].

Порівнюючи програмне забезпечення RFID з апаратними компонентами RFID, необхідно враховувати деякі відмінності. Використання зчитувача може бути досить простим і, як правило, його можна придбати та використовувати за низьку вартість. При інтеграції програмного забезпечення RFID необхідний більший рівень обізнаності про середовище його використання. Оскільки дані об'єднуються з іншими процесами у сценарії, тому, програмне забезпечення має бути адаптоване відповідно до задач у яких його будуть застосовувати. Один і той же тип зчитувачів в одному приміщенні можна використовувати по-різному. Ретельне визначення, проектування та планування необхідні для ефективного розгортання RFID.

Перенесення даних RFID у програмне забезпечення вимагає зберігання даних у загальному місці. Дані та пов'язані з ними атрибути потім можна отримати для подальшого використання. Інформація, така як фізичне розташування елементів, пов'язані властивості предмета або його контейнер, надає динамічні дані для прийняття рішень у реальному часі. Рішення щодо програмного забезпечення засновані на передбачуваності. Наприклад, кардіостимулятор з маркуванням RFID протікає через лінію виробництва медичних виробів, шлях процесу, який він дотримується, записується та зберігається для подальшого пошуку. Конкретний шлях або маршрут можна заново відтворити та за необхідності заново створити. Якщо в кардіостимуляторі виявлено дефект, наступні кардіостимулятори, які виконали ті ж дії, можуть бути ідентифіковані для подальшого тестування у пошуках помилки виробництва.

Це звичайний сценарій. Програмне забезпечення стає ще більш ефективним, коли під час процесу виникає ненормальна активність. Аномалія може бути такою простою, як помилка читання або запису. Це може бути контейнер або предмет з маркуванням, що надходить до зчитувача, або складніша несподівана умова, яка розпізнається програмною системою.

Розглянемо функції та можливості найбільш розповсюджених програмних продуктів для RFID-систем. Radio Frequency Maestro – це найновіша система автоматизації доставки та отримання, доступна для MAS 90, MAS 200 та MAS 200 SQL. Забезпечує керування даними в будь-який час і в будь-якому місці за допомогою інструменту, який легко переміщається від торгового залу до складського приміщення. Radio Frequency Maestro легко модифікується для задоволення потреб будь-якої дистриб'юторської компанії, яка прагне підвищити ефективність свого складу [6].

STP Source Tagging Platform – це гнучка платформа, спеціально розроблена та оптимізована для створення високопродуктивних систем кодування та перевірки. ПЗ забезпечує необмежену пропускну здатність RFID: швидкість кодування до 9500 тегів/хв і перевірка швидкості до 15000 тегів/хв, а також гнучкі параметри керування даними тегів.

BSI RFID Inventory – це рішення для управління запасами для автоматизованого відстеження RFID. Реалізує повне рішення щодо управління запасами з підтримкою численних функцій інвентаризації: планування та підрахунки ABC або Full Physicals; імпортування електронних таблиць тегів RFID для елементів або їх сканування; відстеження та повідомлення про зміни ціни та кількості запасів; інтегрування фінансових операцій з ERP (Enterprise Resource Planning System – Система планування ресурсів підприємства) [5].

rTooltrack – програмне забезпечення для управління засобами RFID, розроблене Supply Insight Inc. Відстеження інструментів, виробничих інструментів та спеціалізованого устаткування є трудомістким процесом, особливо у виробництві. rTooltrack використовує технологію пасивної радіочастотної ідентифікації (RFID), що мінімізує час, витрачений на інвентаризацію та пошук

відсутніх елементів. З моменту свого впровадження у 2012 році rTooltrack був доступний як окремий застосунок, який використовується для виконання завдань на одному пристрої або як корпоративний застосунок, що підтримує повністю зашифрований процес синхронізації між усіма вашими пристроями та базою даних корпоративного класу.

eTurns TrackStock – це просте програмне забезпечення для інвентаризації, засноване на хмарному сховищі, яке автоматизує поповнення залежно від потреби та забезпечує видимість інвентарю в реальному часі у віддалених сховищах. Використовуючи сканери штрих-коду, смартфони, датчики ваги IoT та RFID, eTurns TrackStock управляє товарно-матеріальними запасами в момент використання, щоб збільшити рівень продажів та послуг, оптимізувати запаси та усунути збитки. eTurns TrackStock RFID – дозволяє робити транзакції, одне сканування для замовлення/використання/отримання. Галузі обслуговування: промислові дистриб'ютори, виробники з кількома локаціями, підрядники з вантажними автомобілями, медичні клініки/лікарні [5].

Virtual Asset Tracker – програмне забезпечення для управління активами RFID, розроблене компанією Radiant RFID. Відстежує очікувані та точні місця розташування всіх видів активів. Забезпечує надійну звітність та аналітику, які інтегруються з популярними системами ERP. Має простий у використанні налаштований інтерфейс з головним екраном у стилі приладової панелі для зручного огляду активів. Підтримує пасивні та активні теги RFID. Працює зі стаціонарними та мобільними портативними RFID-сканерами та смартфонами. Працює зі штрих -кодами, щоб клієнти могли самостійно переходити на RFID. Пропонує відстеження та оновлення за допомогою мобільного супутнього додатка для пристроїв iOS та Android.

RedBeam RFID Asset Tracking – програмне забезпечення для відстеження комп'ютерів, обладнання, меблів, транспортних засобів та інших цінних активів. Переваги RedBeam RFID: просте розгортання та використання програмного забезпечення для відстеження RFID; кодування тегів; гнучкі зони зчитування, визначені користувачем; можливість додавати нотатки та записи технічного

обслуговування; надійна звітність з можливостями застосування та сортування; історія придбання та розрахунки амортизації; імпорт та експорт за допомогою Microsoft Excel; надійна база даних SQL; одно- або багатокористувацька мережева версія програмного забезпечення RFID [5].

1.3 Безпека та конфіденційність у системах RFID

Загалом, порушення конфіденційності може мати дві форми: витік інформації та відстеження місцезнаходження. Перша форма стосується прямої інформації, отриманої з мітки, яка може допомогти визначити уподобання власника та його фізичний стан. Наприклад, інформація про ліки може вказувати на певну хворобу, інформація про одяг може розкривати певний спосіб життя тощо. Одне з головних занепокоєнь прихильників конфіденційності полягає в тому, що придбані позначені товари пов'язують покупців із цими конкретними товарами в центральних базах даних. Тоді маркетологи могли б використовувати цю інформацію для створення особистих профілів та націлювання на окремих осіб із спеціалізованими пропозиціями щодо продажу. Однак, навіть якщо відповіді тегів не прив'язані до певного товару, статичні дані можуть допомогти відстежити місцезнаходження людини. Ця друга форма порушення конфіденційності може бути досягнута шляхом співвіднесення "спостережень" тегів від кількох читачів у фіксованих місцях. Таким чином, людей можна відстежувати за тегами, які вони носять.

Нижче наведено набір загальних цілей безпеки, які мають відповідати будь-якому протоколу RFID:

1. **Захист конфіденційності.** Ніяка секретна інформація не повинна витікати з тегу, що може допомогти в ідентифікації вмісту тегу або носія тегу. Поточні теги RFID мають на меті бути дешевими, тому вони випромінюють постійні ідентифікатори, які можуть розкривати особисту та конфіденційну інформацію. Приклади включають гроші, ліки (які можуть бути пов'язані з певною хворобою), книги (які можуть вказувати на певні політичні уподобання) тощо [4].

2. Захист від відстеження. Оскільки теги можна читати з гаманців, рюкзаків, валіз тощо, а зчитувачі можуть бути скрізь (приховані в стінах, під'їздах тощо ...), поточні розгортання RFID можна використовувати для відстеження людей за тегамі, які вони носять. Крім того, колекція позначених об'єктів може точно визначити конкретну особу, навіть якщо особиста особа не пов'язана з тегамі. Щоб вирішити цю проблему, теги не повинні видавати фіксовані ідентифікатори [4].

Оцінюючи та впроваджуючи безпеку навколо RFID, важливо пам'ятати, що деякі фізичні активи важливіші за фактичні дані. Дані можуть ніколи не постраждати, хоча організація все ще може зазнати величезних втрат. Щоб визначити тип атаки, потрібно зрозуміти цілі цієї атаки, що потім допоможе визначити можливий характер нападу.

З точки зору радіочастотних атак, теги та зчитувачі розглядаються як одне ціле. Навіть незважаючи на те, що вони виконують протилежні функції, вони по суті є різними гранями однієї і тієї ж частини радіочастотної системи. Інтернет-інтерфейс для тегів і зчитувачів зазвичай підлягає одному з чотирьох типів атак: підробка, вставка, повтор і відмова в обслуговуванні (DOS).

Атаки можуть бути комбінаційними. Різні атаки, що зустрічаються на противагу системам RFID, також були здійснені проти окремих підсистем. Однак підвищена кмітливість тих, хто атакує системи RFID, ймовірно, призведе до змішаних атак. Зловмисник може атакувати радіочастотний інтерфейс роздрібного продавця за допомогою власного тегу вірусу, який потім може проходити через посереднє програмне забезпечення, в кінцевому підсумку викликаючи бекенд для скидання номерів кредитних карт на невідомий веб-сайт через анонімний сервер.

Для застосування плану щодо запобігання атак на систему радіочастотної ідентифікації, перше, що потрібно зробити, це визначити свої потреби безпеки. Розглянемо наступний сценарій. Склад має систему відстеження цінностей, де зчитувач RFID встановлюється на порталі над конвеєром. Коли піддони проходять по конвеєрній стрічці, вони проходять через портал, антени зчитувача активують теги на кожному піддоні, теги зчитуються, а зчитувач передає інформацію до бази даних.

У цій ситуації, потенційні зловмисники можуть збирати інформацію з радіохвиль, що випромінюються станцією зчитування RFID, і тегами, тому слід обмежити випромінювання радіохвильових хвиль за межі безпосередньої зони читача. Найпростіший спосіб – зменшити потужність передачі зчитувача до абсолютного мінімуму для зчитування тегів.

Якщо це рішення не працює або недоступне, інші варіанти можуть включати зміну положення чи орієнтації зчитувальних антен на порталі або побудову клітки Фарадея навколо зчитувача.

Надійне управління проміжним програмним забезпеченням гарантує, що дані будуть коректними під час переміщення по системі. Отримання текстового рядка замість числового може вказувати на те, що зловмисник намагається впровадити в систему команду із шахрайством. Контрольні суми – також поширений спосіб перевірки даних.

Керування безпекою проміжного програмного забезпечення зазвичай передбачає використання шифрування для захисту даних, і в цьому випадку потрібно враховувати термін служби інформації з урахуванням того, скільки часу знадобиться зловмиснику, щоб зламати шифрування. Однак не варто забувати, що збільшення обчислювальної потужності та нові техніки шифрування постійно розвиваються. Сильна техніка шифрування сьогодні може бути слабкою вже завтра.

Потрібно переконатись, що електроніка чи лінії зв'язку зчитувача не відкриті для тих, хто не має до них доступу. У цьому випадку можна розмістити обладнання (наприклад, комутаторів Ethernet) у заблокованих комунікаційних шафах або ж можна постійно переглядати вихідний код програмного забезпечення, щоб переконуватись, що буфер перевантаження не виведе з ладу зчитувач.

Також варто перевіряти цілісність своїх систем за допомогою доступу до входу та протоколу динамічної конфігурації хостів (DHCP), а також виконувати фізичні перевірки, щоб переконатися, що нові пристрої не додаються до мережі без відома користувача. Управління системою також передбачає встановлення правильної політики безпеки для користувачів цієї системи.

На додаток до вищезазначених основних вимог, наведемо перелік похідних вимог:

1. Ефективність ідентифікації. Після того, як зчитувач отримає відповідь на тег, вона пересилається до внутрішньої бази даних, яка допомагає ідентифікувати тег зі списку дійсних ідентифікаторів тегів. Оскільки ця база даних може складатися з мільйонів, навіть мільярдів елементів, і зчитувачі можуть бути використані для зчитування кількох тегів одночасно, масштабованість має бути необхідною вимогою будь-якого добре розробленого протоколу [4].

2. Захист від підробки тегів або клонування. Клонування тегів дозволяє замінити тег, або просто надіслати запит тегу і надіслати його відповідь зчитувачу поблизу. Це вводило б систему в оману, вважаючи, що продукт все ще на полиці, або ж можна було придбати дорогий товар за ціну дешевого. Ці атаки можуть мати серйозні наслідки, особливо коли RFID-мітки використовуються для контролю доступу. Одним із можливих способів захисту є розгляд методів обмеження відстані, які розроблені таким чином, щоб час затримки в обох напрямках точно вимірювався і був захищений від маніпуляцій [4].

1.4 Особливості застосування технології радіочастотної ідентифікації на підприємстві

Якщо врахувати всі фактори, які повинні бути включені до RFID-рішення, такі як апаратне забезпечення, програмне забезпечення, інженерія бізнес-процесів та управління інформацією, легко побачити, що ці проекти потребують нетривіальних обсягів капіталу, персоналу та часу. Основна відмінність від інших проектів полягає у зусиллях, необхідних на початковому етапі аналізу. Зазвичай ці зусилля вимагають ретельного дослідження даних, гарного розуміння поточних, а також майбутніх тенденцій бізнесу.

Впровадження системи RFID насправді є спробою інтегрувати фізичну точкову діяльність в окремий процес з існуючими елементами програмного

забезпечення. Ці визначені відносини необхідні для створення керованого фізичного представницького середовища для ведення бізнесу. Дані збираються та стають доступними для кращого прийняття рішень. Інформація, яку можна отримати в електронному вигляді у режимі реального часу, цінніша за дані, зібрані та збережені вручну (рис. 1.7). Вплив на ці дані на рівні компонентів дозволяє повторювані дії виконувати з більшою швидкістю та з більшою точністю. Інтеграція сценаріїв з можливістю автоматичної обробки реальних ситуацій відкриває нові можливості для економії коштів шляхом вдосконалення процесу.



Рисунок 1.7 – Стек програмних компонентів RFID

Особливість використання технології RFID у промисловості зумовлюють декілька факторів: робота в широкому діапазоні температур та вологості, наявність в оточуючому середовищі великої кількості металевих предметів, складні форми виробів, що підлягають ідентифікації [5].

Впровадження технології RFID у промисловості зіштовхнулось з погіршенням продуктивності системи при ідентифікації металевих предметів або роботі в середовищі, що містить метали. Наприклад, в автомобільній промисловості, коли RFID використовується для відстеження деталей, більшість деталей виготовляються з металу. Щоб вирішити проблему, яку спричинюють металеві предмети, і щоб заохотити повне розгортання RFID, особливо маркування на рівні елементів, були створені спеціальні RFID-мітки, так звані «on-metal tag».

Наведемо декілька типів міток, які мають конструктивні особливості і їх можна використовувати у металевих середовищах: RFID-мітки з простою прямокутною антеною, RFID-мітки з малою антеною у вигляді петлі, RFID-мітки з плоскою інвертованою антеною F-типу, RFID-мітки з патч-антеною з електромагнітним зазором.

Хоча існують різні конструкції тегів для позначення металевих предметів, і вони різняться за розмірами та характеристиками діапазону читання, усі вищезгадані теги мають спільну проблему, тобто вони мають певну значну товщину порівняно зі звичайними плоскими RFID-мітками, схожими на етикетки. Наприклад, патч-антени зазвичай мають товщину, яку вносить шар діелектричної підкладки. Для петльової антени, (петля перпендикулярна металевій поверхні), товщина обумовлена площею, охопленою петлею. Отже, насправді немає універсального вибору тегів для металевих предметів. Вибір використовуваної антени для тегів буде залежати від типу об'єкта, що підлягає ідентифікації, кількості наявного місця для ідентифікації, обмеження вартості, а також від вимоги діапазону зчитування.

Вода та інші рідини мають менший вплив на RFID-мітки ближнього поля, оскільки більші довжини хвиль систем ближнього поля менш сприйнятливі до поглинання. З іншого боку, RFID-системи далекого поля мають меншу довжину хвилі і більш сприйнятливі до поглинання рідинами. У практичному застосуванні мітки ближнього поля більше підходять для позначення контейнерів, що містять воду або рідину. Мітки далекого поля можна змусити працювати, але їх ефективна відстань читання буде різко скорочена [7].

Залежність індуктивності антени від частоти поблизу водної поверхні ілюструє рис. 1.8. Розмір моделі $250 \times 80 \times 80$ мм з такими електричними параметрами – $\epsilon_r = 77,3$, $tg = 0,048$. Видно, що вода призводить до дуже незначного зменшення індуктивності котушкової антени, навіть якщо антена котушки розміщена всередині води. Це свідчить про те, що RFID-система ближнього поля є кращою для застосувань, які вимагають прикріплення мітки до об'єктів, що містять воду або інші рідини, такі як безалкогольні напої, молоко або масло.

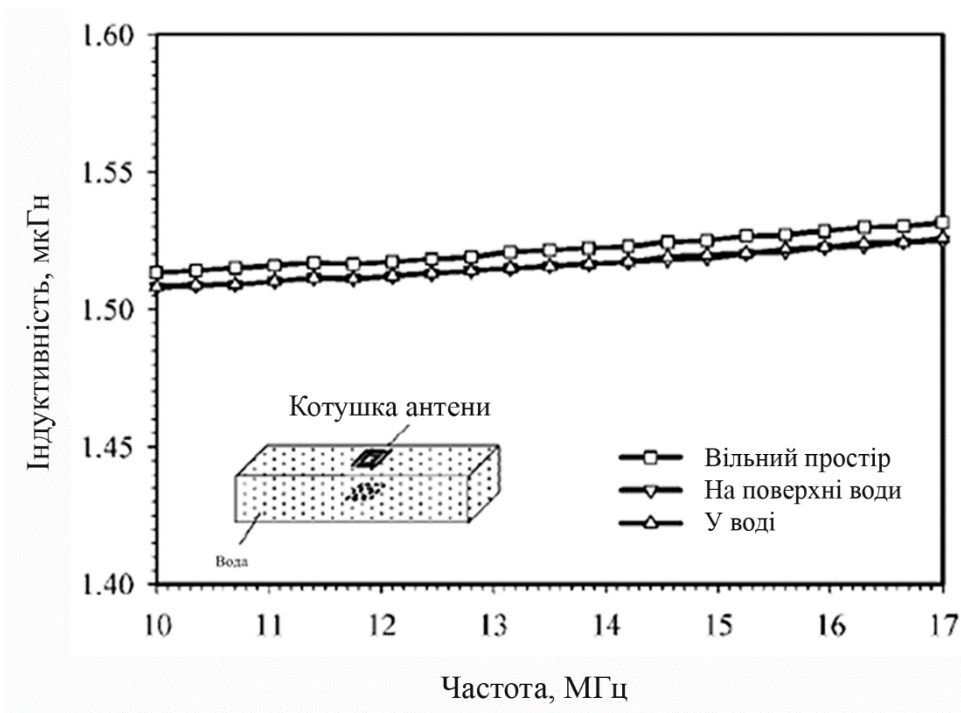


Рисунок 1.8 – Розрахована індуктивність котушкової антени з водою

1.5 Огляд систем радіочастотної ідентифікації для автоматизація виробництва

1.5.1 Моніторинг виробничих процесів

Виробничі процеси зазнали процесу безперервної раціоналізації під час розвитку промислового масового виробництва. Невдовзі це призвело до складання виробничої лінії ("виробництво конвеєрної стрічки"), причому одна і та ж стадія виробництва час від часу виконується на певному місці на конвеєрі. Поки що

виробничий процес такого типу здатний виробляти лише об'єкти, ідентичні за функціями та зовнішнім виглядом.

Виробники зацікавлені в тому, щоб краще зрозуміти операції на кожному етапі виробництва. Аналіз інформації про виробничу діяльність та вимірювання умов навколишнього середовища може допомогти виявити причини проблем з якістю та вказати на можливості покращення. Крім того, аналіз реальних даних може забезпечити швидку реакцію на проблемні процеси. Загалом, більший набір даних дозволяє краще зрозуміти процес.

Точна інформація про те, який об'єкт був виготовлений, з яких компонентів та матеріалів потрібна для ідентифікації всіх продуктів, які потенційно містять дефектні деталі. Крім того, точні та надійні записи даних можуть мати значення у судових справах. Адже на компанію можуть подати до суду, якщо продукти, що виходять з ладу, завдають шкоди. У цьому випадку записи даних важливі для доведення того, що виробництво велося таким чином, що воно відповідало сучасному рівню техніки. Тут дані датчиків можуть допомогти виявити причину виходу з ладу та ще більше звузити сферу потенційно уражених продуктів. Оцінка цих даних може дати додаткову інформацію про показники ефективності, такі як час циклу [8].

Наприклад, 03 листопада 2020 р. CribMaster, підрозділ Stanley Black & Decker, випустив оновлене, швидше та точніше рішення з підтримкою RFID, для забезпечення клієнтам-виробникам повний огляд своїх інструментів. Використання лінії Асси з пристроями з підтримкою RFID надає клієнтам CribMaster в реальному часі уявлення про стан усіх активів, починаючи від розеток і закінчуючи великими інструментами. Рішення включає в себе зчитувач RFID з чотирма антенами, а також теги, прикріплені до кожного інструменту, і програмне забезпечення для управління запасами CribMaster для управління зібраними прочитаними даними. Інформація, надана кабінетом, є надзвичайно важливою для клієнтів, оскільки цим рішенням користуються у аерокосмічній промисловості, для яких один недоречний товар може призвести до зупинки виробництва [9].

У найгіршому сценарії FOD (Foreign object damage) може спричинити катастрофічні збої. За оцінками Boeing, інциденти, пов'язані з FOD, завдають збитків у 4 мільярди доларів щорічно авіаційній промисловості. З цієї причини компанії прагнуть ретельно керувати своїми інструментами та гарантувати, що все, що є у монтажній зоні, негайно повернеться до шаф для інструментів. Автоматизуючи процес виявлення того, які інструменти знаходяться в шафі, а які ще не повернуті, рішення Асси можуть зменшити FOD та включити програми профілактики, особливо у критично важливих для FOD областях, де один предмет може бути катастрофічним. Ті самі проблеми, пов'язані з FOD, виникають у всій авіаційній промисловості, наприклад, у обслуговуванні, експлуатації та будівництві.

1.5.2 Системи контролю та управління доступом

Електронні системи контролю доступу з використанням носіїв даних використовуються для автоматичної перевірки дозволу на доступ осіб до будівель, приміщень або окремих кімнат. При проектуванні таких систем потрібно спочатку зрозуміти, що існує дві принципово різні системи з відповідними властивостями: онлайн та офлайн системи.

Онлайн-системи, як правило, використовуються там, де авторизацію доступу великої кількості людей потрібно перевіряти лише за декількома входами. Так буває, наприклад, біля головних входів в адміністративні будівлі та комерційні приміщення. У системі такого типу всі термінали з'єднані з центральним комп'ютером за допомогою мережі. Центральний комп'ютер керує базою даних, у якій кожному терміналу призначені всі носії даних, дозволені для доступу до цього терміналу. Дані авторизації, створені з бази даних, завантажуються в термінали (або в проміжний блок управління дверима) через мережу і зберігаються там у таблиці. Також можливе використання транспондерів лише для читання [10].

Офлайн-системи набули поширення насамперед у ситуаціях, коли багато окремих кімнат, до яких мають доступ лише одиниці, мають бути обладнані

електронною системою контролю доступу. Кожен термінал зберігає список ключових ідентифікаторів, доступ до якого має бути дозволений. Немає підключення до інших терміналів або до центрального комп'ютера.

Контроль доступу за допомогою безконтактних систем забезпечує набагато більшу гнучкість, оскільки транспондер повинен пройти лише невелику відстань від антени зчитувача. Перепустки можна оформляти у вигляді безконтактних смарт-карт, брелків і навіть наручних годинників.

Великою перевагою безконтактних систем контролю доступу є те, що зчитувач не потребує обслуговування та не піддається впливу пилу, бруду чи вологи. Антену можна встановити під поверхнею стіни, де вона абсолютно непомітна і захищена від вандалізму. Зчитувачі також можна вмонтувати в турнікети.

У загальному вигляді системи контролю та управління доступом (СКУД) можуть мати у своєму складі наступні елементи (рис. 1.9). По-перше, контролери СКУД – електронні мікропроцесорні модулі, що реалізують автентифікацію об'єктів доступу за допомогою пристроїв введення ідентифікаційних ознак, логіку авторизації для доступу в ті чи інші приміщення і області, управління керованими перешкоджаючими пристроями [5].

По-друге, пристрої введення ідентифікаційних ознак або зчитувачі та керовані пристрої-перешкоди. Наприклад, турнікети, двері, обладнані керованими замками, ворота, шлагбауми, шлюзи. По-третє, програмне забезпечення. Необов'язковий елемент, що дозволяє здійснювати централізоване управління контролерами СКУД з персонального комп'ютера, формування звітів, різноманітні додаткові функції.

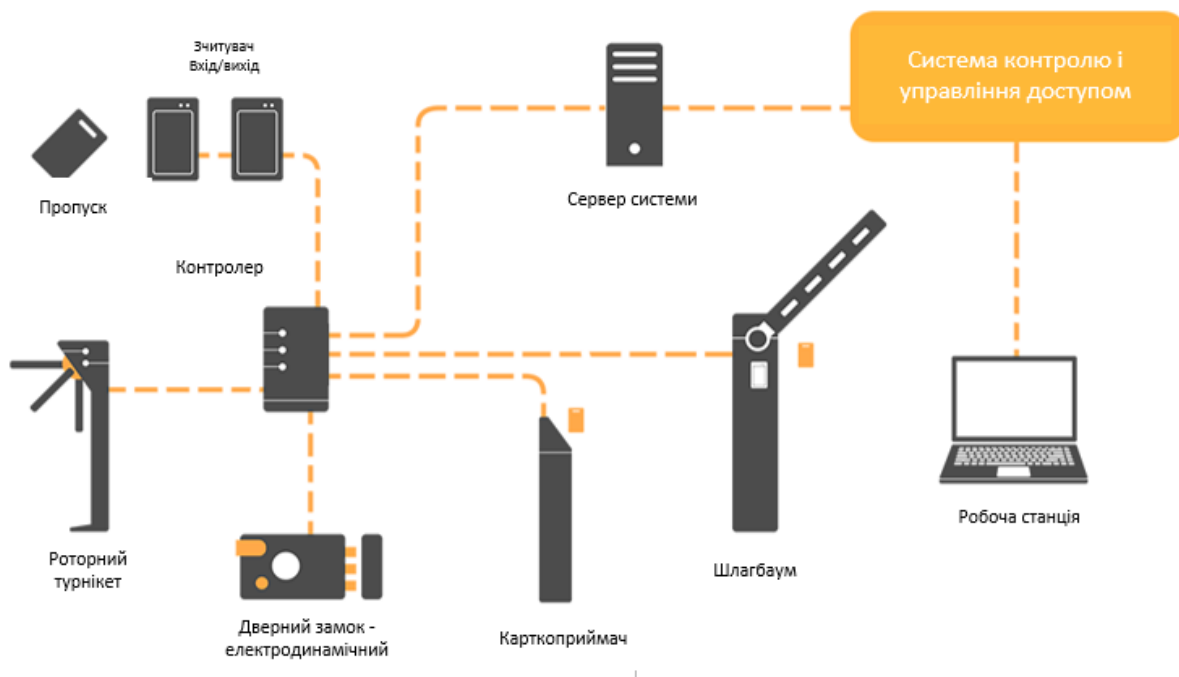


Рисунок 1.9 – Основні елементи системи контролю та управління доступом

1.5.3 Охорона праці

У промисловості існує безліч верстатів з високою швидкістю обертання та швидкістю руху. Тому ризик нещасних випадків для людини та машини дуже високий під час заміни інструменту; наприклад, небезпека може бути викликана неправильною установкою ланцюгового магазину верстата.

Цю потенційну небезпеку можна усунути, встановивши RFID-мітку у частину валу або у кріпильні болти тримача інструменту. Усі відповідні дані інструменту попередньо запрограмовані у мітку виробником інструменту. Оператор верстата вставляє інструменти з міткою у тримач верстата у будь-якому порядку. Потім машина ініціює автоматичну послідовність зчитування всіх інструментів у тримачі інструментів, під час якої інструменти спочатку впорядковуються у положення держателя інструменту, а потім усі геометричні та технічні дані для інструментів коректно передаються до системи управління інструментом блоку управління. Немає введення даних вручну, що виключає можливість людської помилки. Таким чином виключається небезпека нещасних

випадків через надмірну швидкість, неправильний вибір напрямку обертання або неправильне розташування інструменту щодо заготовки.

Що стосується безпеки робітників, які працюють зі спеціальним транспортом, наприклад, на складах чи будівельних майданчиках, то надто часто люди отримують травми через зіткнення з транспортними засобами. Завдяки застосуванню технології RFID ризик зіткнення між транспортними засобами та пішохідними працівниками можна значно зменшити. Розширені системи сигналізації, на основі технології радіочастотної ідентифікації, про наближення спеціального транспорту пропонують двостороннє рішення. Все дуже просто: пішохід може носити RFID-мітку на рукаві або ж прикріплени до каски, а всі транспортні засоби у свою чергу обладнані RFID-зчитувачем. Коли пішохід надто близько підходить до транспортного засобу, і пішохід, і водій отримують попередження.

В умовах поганої видимості стандартні засоби індивідуального захисту та навіть камери неефективні, якщо мова йде про запобігання зіткненням між пішоходами та транспортними засобами. RFID-система надає всім працівникам підприємства додатковий рівень контролю та захисту. Адже зчитувач ідентифікує теги і з-за поворотів, і на систему не впливають такі умови навколишнього середовища, як пил і дим, і погане освітлення.

1.5.4 Забезпечення ланцюжка поставок

Управління ланцюгами поставок (SCM) займається переміщенням товарів між організаціями від сировини до готового продукту. Кожен ланцюжок поставок відрізняється і відображає унікальні потреби асортименту продуктів, які підлягають переробці. Тим не менш, усі ланцюжки поставок мають спільну рису – процес має бути простим, стандартним та швидким.

У ланцюгах поставок складське господарство відіграє важливу роль у зберіганні готової продукції. Усі фізичні об'єкти зберігаються на складах принаймні один раз до продажу. Зберігання, обробка та транспортування товарів

включають багато процесів, які впливають на вартість та можливість надання послуг.

Наприклад, працівники узгоджують відправлення з накладними, упаковкою та списками за допомогою фізичного підрахунку та ручного введення даних. Виконання людьми цих завдань часто призводить до помилок і до уповільнення часу обробки. Потреба в точних даних у реальному часі про продукти в ланцюжку поставок особливо важливі для промисловості споживчих товарів. Промисловість переміщує великі обсяги різноманітної продукції через складні ланцюжки поставок, які часто охоплюють великі відстані. Незважаючи на успіх і широке використання штрих-кодів, стає зрозуміло, що промисловість потребує більш конкретної інформації, ніж та, яку можуть надати штрих -коди для управління потоком товарів. Додаткова інформація може включати:

- повна інформація про продукцію, додана до кожного кейсу або піддону;
- деталі виробництва, інформація про партію, завод та якість;
- технічні аспекти виробу, включаючи належне використання.

Наприклад, можна розмістити кілька зчитувачів на навантажувальних пристроях біля відсіків для вантажівок. Оскільки навантажувачі переміщують вантажі у вантажівки, зчитувачі можуть автоматично сканувати та записувати завантажену кількість. Замовлення можна миттєво перевірити, щоб переконатися, що на відправці є відповідна продукція та потрібна кількість. RFID виявляє проблему доставки неправильної одиниці або неправильної кількості товару у місці проходження, а не в кінці. Отримуючи підтвердження на кожному кроці, помилки в відправленнях виявляються по дорозі, коли їх виправлення дешевше.

Висновки до розділу

Радіочастотна ідентифікація – це безпроводна технологія для збору даних. Найпростіша система RFID складається з мітки-ідентифікатора, яка прикріплена до об'єкта, і зчитувача, який може опитувати тег, для того, щоб ідентифікувати мітку та отримати інформацію, записану на мітці.

Мітка виконує функцію програмованого пристрою для передачі даних і складається з елемента зв'язку (резонансна налаштована схема) та малопотужної CMOS-мікросхеми. Зчитувач видає радіочастотний сигнал, і обмінюється даними, коли тег наближається до сигналу зчитувача. Програмне забезпечення у системі – це інструмент для інтеграції апаратних компонентів у єдину комп'ютерну систему зі своїми функціями і базами даних.

Для безпеки та конфіденційності RFID-систем важливо дотримуватись загальних правил безпеки:

- захист конфіденційності;
- захист від відстеження;
- ефективність ідентифікації;
- захист від підробки тегів або клонування.

При виборі технології RFID для реалізації у промисловості потрібно спиратись на такі обмежуючі фактори:

- температура та вологість середовища;
- наявність в оточуючому середовищі великої кількості металевих предметів;
- складні форми виробів;
- наявність води та інших рідин.

Технологія радіочастотної ідентифікації набула широкого поширення в автоматизації таких виробничих процесів як моніторинг виробничих процесів, системи контролю доступу до приміщення (СКУД), охорона праці, забезпечення ланцюжка поставок.

2 РОЗРОБКА СТРУКТУРНОЇ ТА ФУНКЦІОНАЛЬНОЇ СХЕМ СИСТЕМИ

2.1 Розробка плану об'єкту контролю та автоматизації

Система RFID буде встановлена у вже існуючій інфраструктурі, яка містить інші системи та пристрої. Тому потрібно визначити, як ця система RFID впишеться в існуючу інфраструктуру об'єкта. З цієї причини перед фіналізацією проекту системи RFID і перед установкою системи RFID потрібно провести аналіз об'єкту. Саме для цього необхідно проаналізувати фізичну інфраструктуру об'єкту та радіочастотне середовище, щоб знайти відповідні місця для зон зчитування або позначити заплановані зони зчитування.

Об'єктом автоматизації є склад споживчих товарів (рис. 2.1). Умовно склад можна розділити на кілька основних зон. Перша зона – отримання та кінцева відправка товарів. Друга зона – основна, сховище товарів. Третя зона – фойє та приміщення для відпочинку гостей та водіїв. Четверта зона – офіс та адміністрація. П'ята зона – зона відпочинку для працівників.

Перша зона – це зона загрузки та розгрузки товару, яка має 6 воріт на в'їзд та виїзд для великогабаритного транспорту. Друга зона містить 9 стелажів з товаром, два конвеєри для доставки товару на склад з зони відвантаження та для доставки товару зі складу до зони завантаження, робоче місце пакувальників та іншу техніку доставки товару.

Третя зона – це фойє та зона відпочинку для гостей та водіїв. Також у цій зоні передбачений роздільний санвузол для чоловіків та жінок. Четверта зона – це офісні приміщення для операторів та працівників з базою даних, передбачений також кабінет директора складу. П'ята зона містить роздільний санвузол для чоловіків та жінок, а також їдальню.

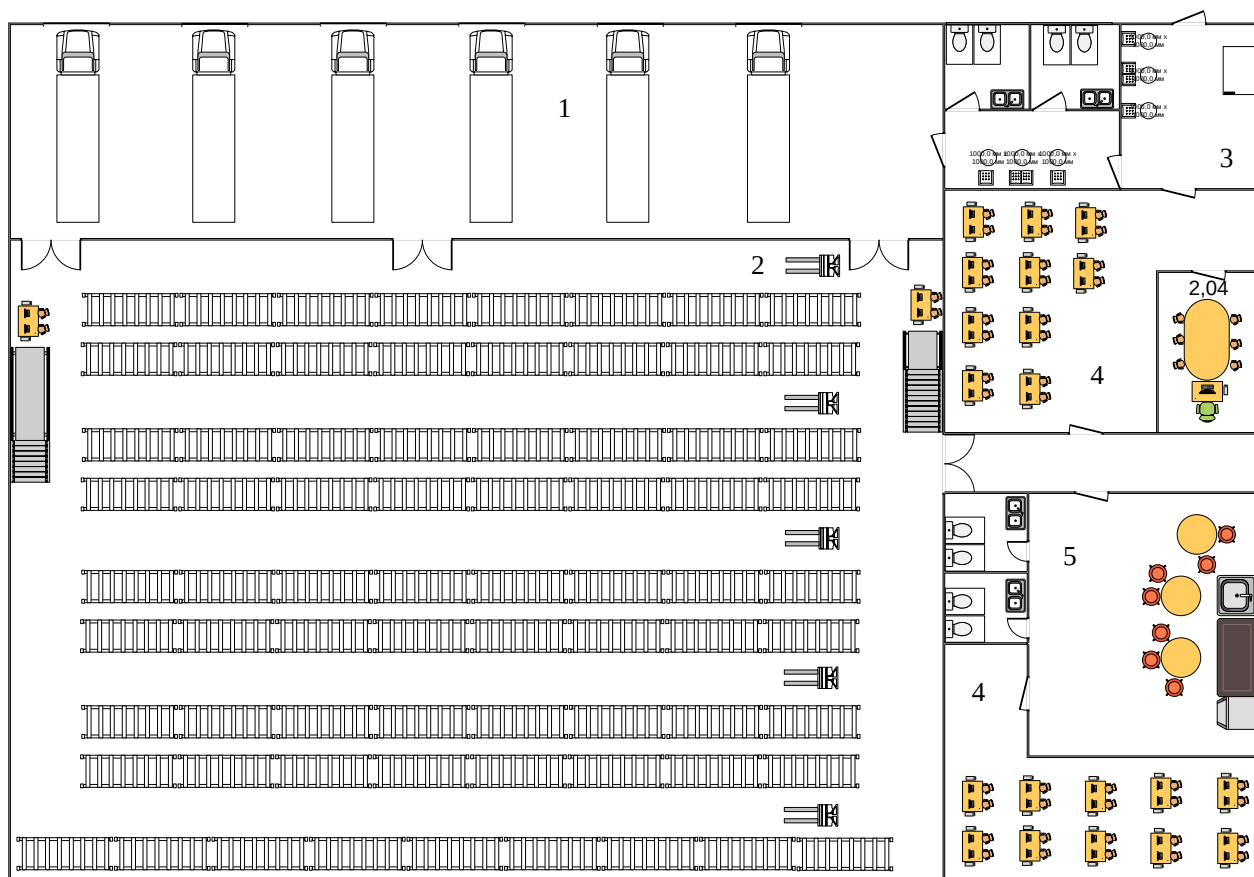


Рисунок 2.1 – План об'єкту контролю та автоматизації

Робота звичайного складу відбувається за наступним алгоритмом. Процес починається з першої зони, де сканується вручну кожен товар, ящик або палета і направляється до зони розподілення. А далі за допомогою техніки – у зону зберігання. Самі замовлення збираються вручну оператором і відправляються конвеєром до пакувальників, де знаходяться усі можливі варіанти тари для відвантаження. Далі товар направляється до зони відвантаження.

2.2 Опис системи радіочастотної ідентифікації

Шляхом впровадження RFID-системи у логістичні процеси можна контролювати дані в режимі реального часу в будь-якій точці виробничого процесу, що може виявити будь-які порушення або недоліки. Для проведення інвентаризації співробітнику достатньо лише обійти склад з ручним зчитувачем в руках на відстані 1-2 метри від товарів [5].

Система контролю переміщення та обліку товарів на складі розробляється для модернізації існуючого об'єкту. Для автоматизації роботи складу розроблено пасивну надвисокочастотну (НВЧ) систему радіочастотної ідентифікації. Ця технологія регулюється стандартом ISO 18000-6-с і працює у діапазоні 860-960 МГц. Перевагою цього протоколу є можливість використання менш дорогих тегів, висока швидкість зчитування та протидія колізіям.

Систему умовно можна розділити на три частини. Перша частина – це система управління складом або ж (WMS – Warehouse Management System). Друга частина – це система контролю доступу до приміщення (СКУД). Третя частина пов'язана з охороною праці і спрямована на безпеку працівників під час роботи з автомобільною технікою (візками тощо).

Система управління складом починається з порталних воріт, які обладнані RFID-зчитувачем. Розглянемо ситуацію, коли приїздить машина з основного підприємства – власника складу. Усі її ящики обладнані RFID-тегами, тому зчитувач без проблем передає інформацію про те, який товар надійшов, одразу до бази даних. У випадку постачання товару від сторонніх компаній потрібне втручання людини. Оскільки, до кожної коробки потрібно нанести RFID-тег. Для цього у зоні відвантаження передбачений RFID-принтер для міток, підключений до WMS-системи.

Далі всі ідентифіковані товари направляються конвеєром до складу. У цей час працівники з базою даних за допомогою програмного забезпечення віддалено заносять інформацію у теги про те, де саме має зберігатись товар. Оператори, використовуючи мобільний зчитувач, розвозять їх по потрібним стелажам.

Зворотній процес відправки товару починається із формування списку потрібних ящиків. Список містить витяг з бази даних, у якому є ідентифікаційні номери потрібних ящиків та їх місце розташування. Тому оператори, маючи список на руках швидко збирають потрібні ящики і відвозять їх у зону завантаження.

У зоні завантаження пакувальники зчитують кожен ящик за допомогою мобільного зчитувача. У базу надходить інформація про те, який саме ящик покинув зону зберігання і це забезпечить надійність комплектації замовлення.

Останнім етапом верифікації замовлення є портальний зчитувач на виїзних воротах. Тоді у базу надходить інформація про те, який саме товар покидає склад. Отже, система на кожному етапі може виявити неточність комплектування замовлення. Структурна схема системи управління складом.

Система контролю доступу до приміщення (СКУД) застосовується для доступу до самого приміщення та окремих зон складу. У кожного співробітника є тег у вигляді пластикової картки. Біля головного входу (1) розташований турнікет із вбудованим зчитувачем. При зчитуванні коректної картки співробітник зможе пройти далі.

Що стосується першої зони, то зовні туди можна потрапити через портальні ворота з електроприводом. Їх може відчинити тільки начальник складу зі свого робочого місця або ж охорона (якщо це відбувається не у робочий час). До другої зони можна потрапити з першої через три двері зі зчитувачами. При зчитуванні коректної картки (у базі даних міститься інформація про цей ідентифікатор і дозволені зони доступу) подається струм на електромагнітний замок і двері можна відчинити. Так само відбувається із доступом до інших зон.

Безпека працівників при роботі з автомобільною технікою реалізована за допомогою системи сигналізації при зближенні з транспортним засобом. Усі працівники другої зони – зони зберігання матимуть браслет з вбудованим RFID-тегом та сигналізацією у вигляді вібрації та блимання світлодіода. Транспорт у свою чергу обладнаний зчитувачем. При зближенні працівника і транспорту більше, ніж на визначену відстань, браслет потрапляє у зону зчитувача та починає сигналізувати про це пішохода. Щодо водіїв, то вони також мають носити браслети у зоні зберігання. Тому передбачена можливість вимкнення сигналізації за допомогою кнопки для безпосереднього керування транспортним засобом.

2.3 Функціональна схема системи радіочастотної ідентифікації

Система контролю та управління доступом передбачає сім дверей та турнікет, які керуються чотирма контролерами доступу. До трьох контролерів

підключено по два RFID-зчитувачі та по два електромагнітні замки, до четвертого під'єднано один RFID-зчитувач, один електромагнітний замок, турнікет та кнопка виходу . Самі контролери підключені до сервера через концентратор за допомогою двостороннього Ethernet-з'єднання. Що стосується живлення, то контролери, зчитувачі, замки та турнікет потребують 12 В постійного струму. Тому було використано трансформаторний перетворювач. Сервер та комутатор отримують живлення від мережі змінного струму. Структурна схема системи контролю доступом зображена на рис. 2.2.

Інфраструктура системи WMS починається з системи серверів, яка використовує спеціалізоване програмне забезпечення, щоб взаємодіяти зі зчитувачами, RFID-принтерами та проміжним програмним забезпеченням цих пристроїв.

RFID-принтери під'єднані до концентратора за допомогою Ethernet-підключення. А концентратор у свою чергу під'єднаний до сервера. Мобільні RFID-зчитувачі керуються проміжним програмним забезпеченням, яке завантажують через USB-підключення. RFID-принтери та мобільні RFID-зчитувачі мають вбудоване джерело живлення.

Портальний зчитувач складається з RFID-зчитувача та 4 антен, під'єднаних до зчитувача SMA проводом. Що стосується живлення, то ці RFID-зчитувачі для потребують 24 В постійного струму, тому було використано трансформаторний перетворювач. Сервер та комутатор отримують живлення від мережі змінного струму. Структурна схема системи управління складом зображена на рис. 2.3.

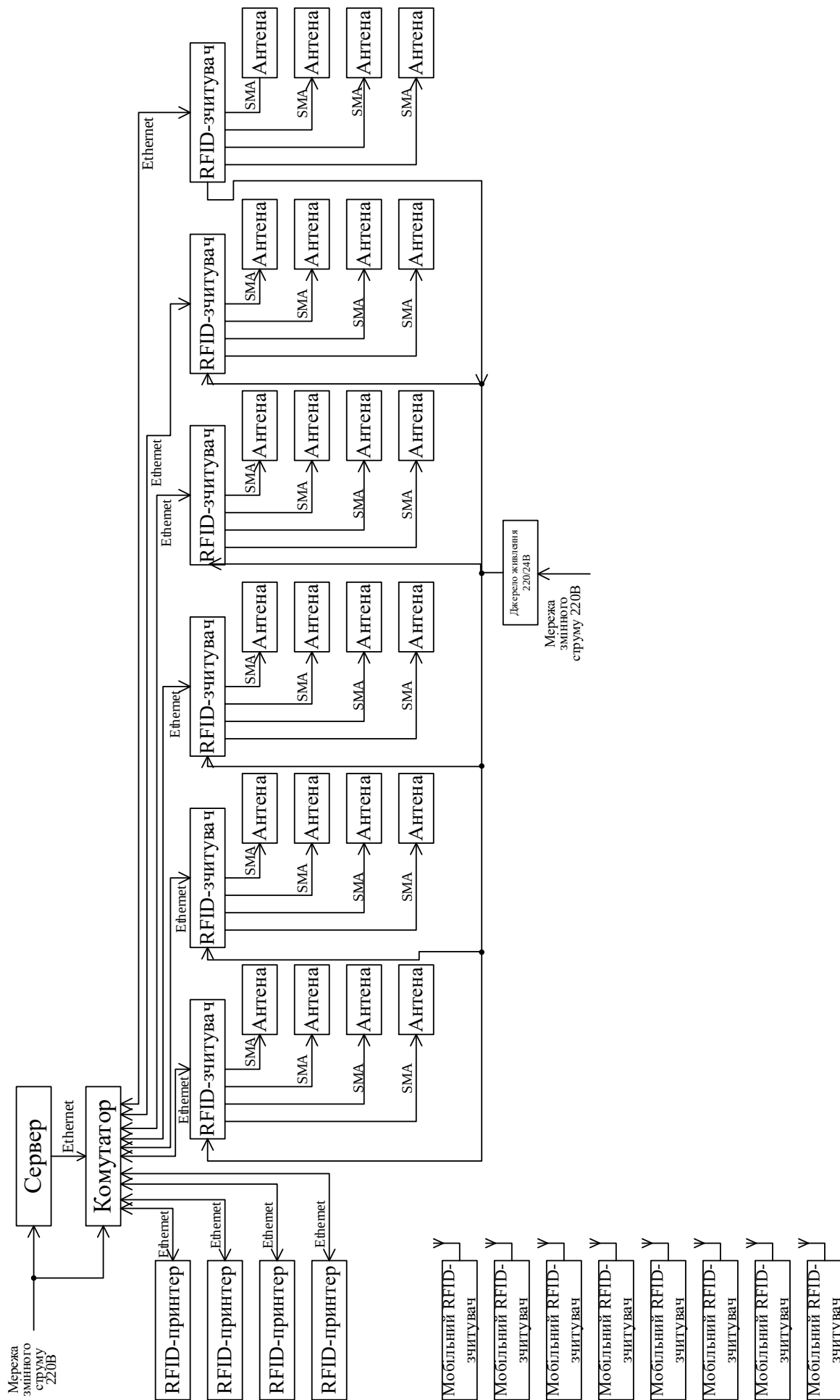


Рисунок 2.2 – Функціональна схема системи управління складом

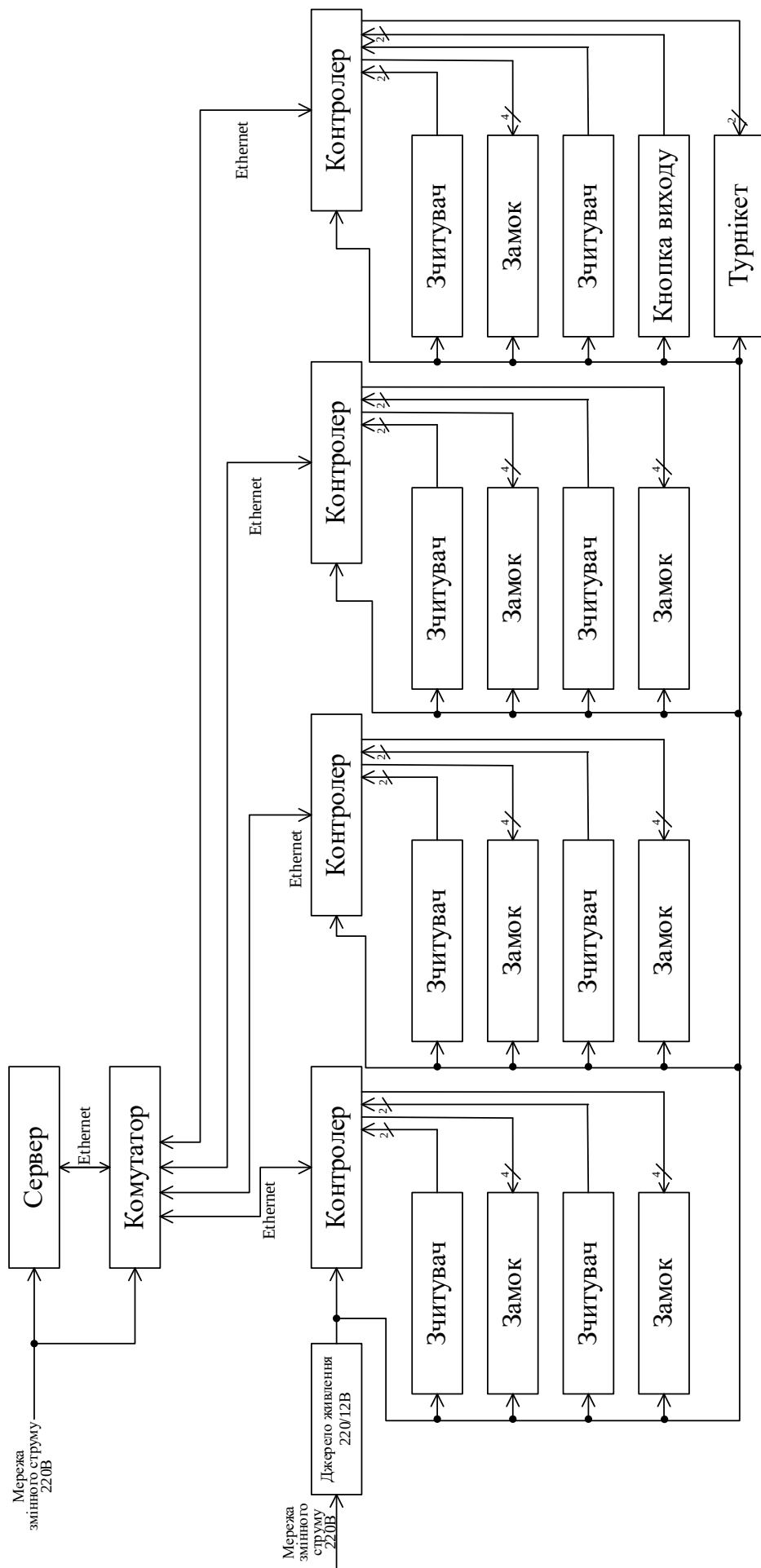
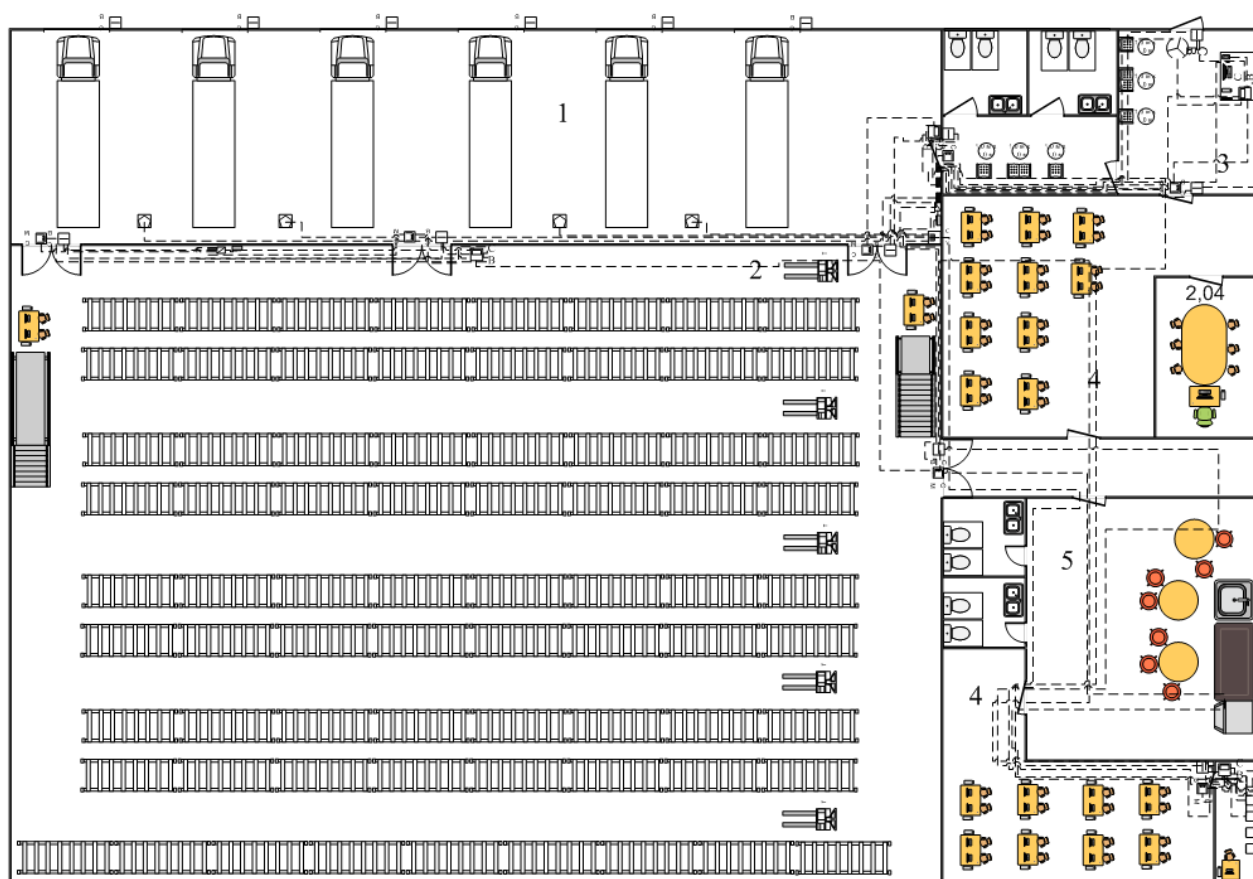


Рисунок 2.3 – Структурна схема системи контролю та управління доступом

Система сигналізації при зближенні з транспортним засобом складається лише з RFID-зчитувачів з джерелом живлення, якими обладнані транспортні засоби, транспондерів, які носять співробітники, та програмного забезпечення. Розміщення усіх пристроїв системи контролю на плані складу наведено на рис. 2.4.



Умовні позначення

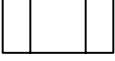
 C В	Контролер	 T	RFID-зчитувач UWB		Трансформаторний перетворювач
 C M	Електрозамок	 C В	RFID-зчитувач		Електричний щиток
 C V	Комутатор		RFID-принтер		Сервер

Рисунок 2.4 – Розміщення пристроїв системи контролю на плані складу

Висновки до розділу

У ланцюгах поставок складське господарство відіграє важливу роль у зберіганні готової продукції. Усі фізичні об'єкти зберігаються на складах принаймні один раз до продажу. Зберігання, обробка та транспортування товарів включають багато ручних процесів, які впливають на вартість та можливості надання послуг. Тому доцільно автоматизувати ці процеси для виключення помилок.

Об'єктом автоматизації обрано склад споживчих товарів. Для автоматизації роботи складу розроблено пасивну надвисокочастотну (НВЧ) систему радіочастотної ідентифікації. Ця технологія регулюється стандартом ISO 18000-6-с і працює у діапазоні 860-960 МГц.

Систему умовно можна розділити на три частини. Перша частина – це система управління складом або ж (WMS – Warehouse Management System). Друга частина – це система контролю доступу до приміщення (СКУД). Третя частина пов'язана з охороною праці і спрямована на безпеку працівників під час роботи з автомобільною технікою (візками тощо).

Система управління складом враховує кожну точку переміщення товару та замовлення по складу. Складовими елементами є портальні зчитувачі на в'їзних та виїзних воротах, RFID-принтер для товарів, які надходять без міток (зі сторонніх підприємств), мобільні зчитувачі для операторів та пакувальників, а також програмне забезпечення з базою даних, яке об'єднує усі ці елементи.

Система контролю доступу до приміщення (СКУД) застосована для доступу до самого приміщення та окремих зон складу. У кожного співробітника є тег у вигляді пластикової картки. Біля головного входу розташований турнікет із вбудованим зчитувачем. Що стосується доступу до окремих зон, то там встановлені двері зі зчитувачами. При зчитуванні коректної картки (у базі даних міститься інформація про цей ідентифікатор і дозволені зони доступу) подається струм не електромагнітний замок і двері можна відчинити.

Безпека працівників при роботі з автомобільною технікою реалізована за допомогою системи сигналізації при зближенні з транспортним засобом на основі технології радіочастотної ідентифікації. В умовах поганої видимості стандартні засоби індивідуального захисту та навіть камери неефективні, якщо мова йде про запобігання зіткненням між пішоходами та транспортними засобами. RFID-система надає всім працівникам підприємства додатковий рівень контролю та захисту. Адже зчитувач ідентифікує теги і з-за поворотів, і на систему не впливають такі умови навколишнього середовища, як пил і дим, і погане освітлення.

3 ОБГРУНТУВАННЯ ВИБОРУ ПРИСТРОЇВ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМИ

3.1 Вибір зчитувачів

Зростання використання RFID в багатьох галузях, а також збільшення використання мобільних зчитувачів RFID призводить до ситуацій, коли зчитувачі повинні працювати в безпосередній близькості одне з одним, що призводить до колізій, і це у свою чергу впливає на швидкість та коректність роботи.

Зчитувач має цілий ряд різноманітних задач, включаючи живлення транспондера, його ідентифікацію, зчитування з нього даних, запис даних і додаток (програмне забезпечення) для роботи з даними. Зчитувач складається з трьох основних вузлів:

- прийомопередавач, що забезпечує двосторонній зв'язок;
- мікроконтролер, що забезпечує шифрування та дешифрування прийнятої та переданої інформації;
- одна або декілька антен.

Також зчитувачі є джерелом енергії для пасивних міток. Зчитувач здатний одночасно обробляти дані з величезної кількості міток, що знаходяться в зоні зчитування. Уникнути помилок при одночасному зчитуванні даних з різних міток допомагає функція антиколізії [5].

У зчитувачі РЧ-сигнал перетворюється на низьку частоту за допомогою змішувача та гетеродина. На кожному етапі використовуються аналогові фільтри для розрізнення сигналу за межами смуги частот. Останнім кроком перед оцифруванням є розкладання сигналу на синфазну та квадратурну складові. Потім ці сигнали перетворюються у аналого-цифровому перетворювачі (АЦП). У діапазоні НВЧ смуга пропускання каналу складає 25 МГц, в той час як ширина спектру сигналу мітки складає 500 кГц. Це дозволяє зчитувачу обробляти сигнали 50 міток, що працюють у діапазоні частот цього каналу.

Зчитувачі доступні з багатьма різними типами апаратних інтерфейсів. Ці інтерфейси варіюються від RS232 (послідовний зв'язок) до безпроводового зв'язку 802.11B/G. Найпоширенішими інтерфейсами є RS232 для близького підключення,

RS485 для промислового підключення на середню відстань і TCP/IP через Ethernet або 802.11b/g для інсталяцій в масштабах підприємства.

Почнемо з вибору мобільних зчитувачів для операторів. Серія Zebra MC3300 RFID – це лінійка інтегрованих RFID-зчитувачів НВЧ-діапазону, які створені на базі технологій радіочастотної ідентифікації (RFID) та мобільної платформи Android. Модель MC3330xR (рис. 3.1) призначена для зчитування RFID-бірок та штрих-кодів у стандартних діапазонах на складах магазинів, готелів, медичних установ та великих постачальників.



Рисунок 3.1 – Мобільний зчитувач MC3330xR

Середовище крос-платформної розробки компанії Xamarin дозволяє розробникам використовувати свій досвід роботи та інструменти мовою C# для розробки швидких та зручних програм для пристроїв Android. Завдяки комплекту EMDK для Xamarin від Zebra усі розширені можливості пристрою MC3330xR можна легко впровадити в додатки Xamarin. Комплект розробника мобільних додатків підприємств (EMDK) спрощує проектування корпоративних додатків, що

забезпечують скорочення тривалості та підвищення економічної ефективності циклів розробки.

Перевагами цього мобільного зчитувача є вбудована кільцева антена, яка забезпечує надійну роботу незалежно від розташування транспондера. Мобільний зчитувач має вбудоване джерело живлення ємністю 7000 мАг. Також пристрій підтримує зчитування штрих-кодів, що прискорить інтеграцію існуючого рішення на підприємстві, яке використовує штрих-коди.

Зчитувачами для системи контролю доступом обрано HIKVISION DS-K1802E (рис. 3.2). Ці зчитувачі мають 8-bit процесор, клас захисту IP65, інтерфейс підключення Wiegand (w26, w34). Тип карт, які можна зчитувати – Em-Marine, робоча частота 125 кГц, а дальність 50 мм. Зчитувач потребує живлення 12 В і може працювати при температурах від -20 до +65 °С.



Рисунок 3.2 – RFID-зчитувач HIKVISION DS-K1802E

Окремим елементом СКУД є турнікет на вході у будівлю. У якості турнікету було використано готове рішення турнікет трипод EXPERT (рис. 3.3). Турнікет

забезпечує прохід не менше 20 осіб на хвилину (в режимі разового проходу). Пропуск здійснюється за допомогою пристроїв зчитування карток (125 кГц RFID-карт або 13,56 МГц Mifare карт), дистанційного керування через пульт або контролер СКУД, а також вручну.



Рисунок 3.3 – Турнікет трипод EXPERT

Основними перевагами є невеликі розміри і низький рівень енергоспоживання, обумовлений простотою конструкції. Також передбачена можливість внутрішньої установки лічильника проходів. Живлення відбувається від мережі змінного струму 100...240 В, 50/60 Гц або ж від джерела постійного струму 12 В, а споживана потужність складає 30 Вт.

Що стосується зчитувачів, якими обладнано транспортні засоби на складі, то було обрано RFID-зчитувач Zebra UWB Wand (рис. 3.4). Цей зчитувач розроблено для додатків, які потребують точності та високої швидкості оновлення розташування об'єктів у режимі реального часу. UWB використовує запатентовані технології, щоб забезпечити переваги RTLS за допомогою транспондерів, які мають надзвичайно тривалий термін служби акумулятора. Крім того, Zebra UWB є

рішенням UWB, яке відповідає новому міжнародному стандарту UWB, IEEE 802.15.4.f, а також міжнародному стандарту ISO-24730-61 Draft. Це захищає інвестиції в інфраструктуру, роблячи її сумісною не тільки з тегами UWB від Zebra, але й іншими тегами UWB, які відповідають стандартам.



Рисунок 3.4 – RFID-зчитувач Zebra UWB Wand

Перевагами цього зчитувача є висока продуктивність – працює в багатопроменевому режимі, відмінна точність визначення місцезнаходження у режимі реального часу, тривалий термін служби акумулятора – до 7 років при частоті миготіння 1 Гц, велика дальність RTLS – до 200 метрів прямої видимості, висока пропускна здатність – до 3500 транспондерів на один зчитувач одночасно.

3.2 Вибір антен

Спроекуємо прямокутну патч-антену з субстратом RO4003C для портального зчитувача. Спочатку потрібно встановити вхідні параметри та розрахувати інші, необхідні для моделювання (рис. 3.5). Вхідні параметри:

- резонансна частота: $f_r = 868$ МГц;
- товщина субстрата (наповнювача): $h = 32$ мм;
- товщина патчу: $t_1 = 35$ мкм;
- діелектрична стала субстрату (RO4003C): $\epsilon_r = 3,55$;
- швидкість розповсюдження електромагнітних хвиль: $c = 3 \cdot 10^8$;
- тангенс кута діелектричних втрат субстрату (RO4003C): $\tan \delta = 0,0021$.

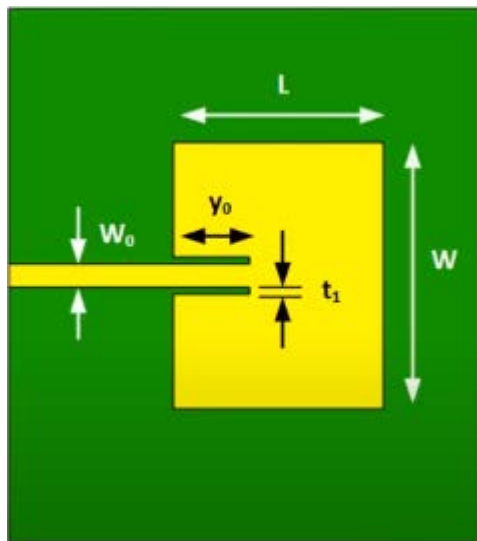


Рисунок 3.5 – Модель патч-антени

Розрахуємо ширину патчу за формулою:

$$W = \frac{c}{2 f_r} \sqrt{\frac{2}{\epsilon_r + 1}}. \quad (2)$$

Ширина патчу:

$$W = \frac{3 \cdot 10^8}{2 \cdot 868 \cdot 10^6} \sqrt{\frac{2}{3,55 + 1}} \approx 114,49 \text{ мм.}$$

Тепер розрахуємо ефективну діелектричну константу за формулою:

$$\varepsilon_{\text{reff}} = \frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2} \left[1 + 12 \frac{h}{W} \right]^{-1/2}. \quad (3)$$

Ефективна діелектрична константа:

$$\varepsilon_{\text{reff}} = \frac{3,55 + 1}{2} + \frac{3,55 - 1}{2} \left[1 + 12 \frac{0,032}{0,11449} \right]^{-1/2} \approx 2,887.$$

Далі для визначення довжини патчу розрахуємо ΔL – довжину оболонки патчу:

$$\Delta L = 0,412h \frac{(\varepsilon_{\text{reff}} + 0,3)(W/h + 0,264)}{(\varepsilon_{\text{reff}} - 0,258)(W/h + 0,8)}. \quad (4)$$

Довжина оболонки патчу:

$$\Delta L = 0,412 \cdot 0,032 \frac{(2,887 + 0,3)(0,11449/0,032 + 0,264)}{(2,887 - 0,258)(0,11449/0,032 + 0,8)} = 0,014 \text{ м.}$$

Довжину самого патчу визначимо за формулою:

$$L = \frac{c}{2f_r \sqrt{\varepsilon_{\text{reff}}}} - 2\Delta L. \quad (5)$$

Довжина патчу:

$$L = \frac{3 \cdot 10^8}{2 \cdot 868 \cdot 10^6 \sqrt{2,887}} - 2 \cdot 0,014 \approx 74 \text{ мм.}$$

Для розрахунку інших даних скористуємось калькулятором [11].

Розраховані дані:

- ширина проміжку: $t_1 = 2,75$ мм;
- ширина патчу: $W = 114,49$ мм;

- довжина патчу: $L = 74$ мм;
- ширина лінії живлення: $W_f = 1,92$ мм;
- довжина лінії живлення: $L_f = 112,25$ мм;
- відстань для узгодження з 50 Ом: $y_0 = 24,13$ мм.

У програмному забезпеченні Comsol Multiphysics (рис. 3.6) розробимо модель патч-антени.

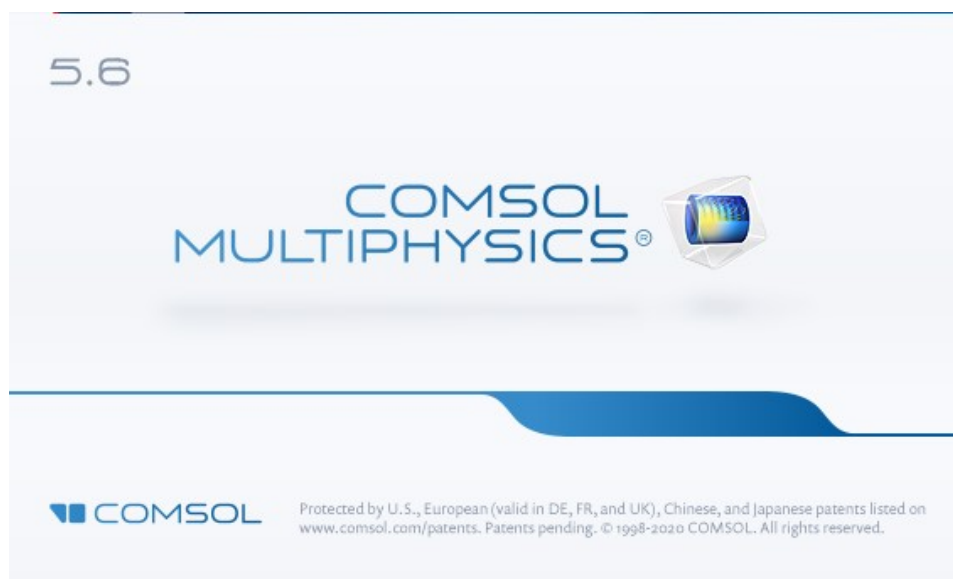


Рисунок 3.6 - Copyright Side Comsol Multiphysics

Обираємо Model Wizard та 3D у вкладці вибору Space Dimension. Далі обираємо фізику «Electromagnetic Waves, Frequency Domain (emw)» (рис. 3.7).

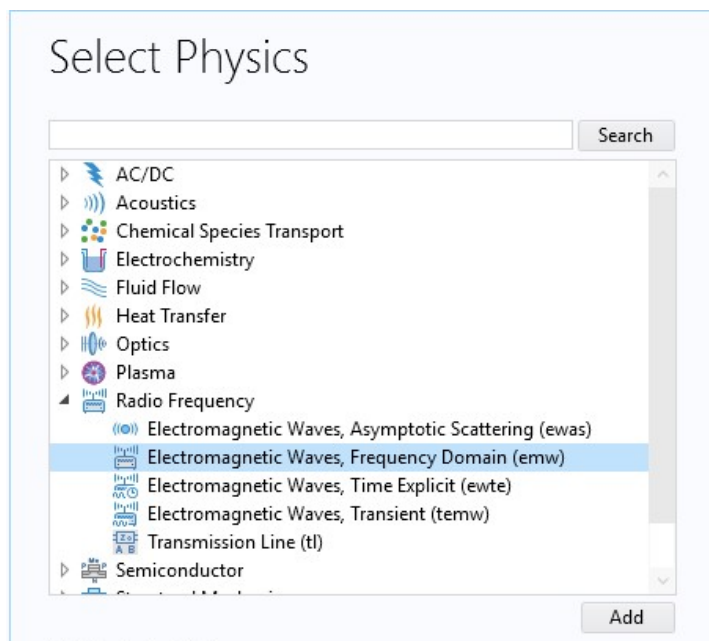


Рисунок 3.7 – Вибір фізики

Далі у розділі «Study» додаємо до фізики «Adaptive Sweep Frequency» і створюємо проект. У вкладці «Params» (рис. 3.8) встановлюємо усі вхідні та розраховані параметри.

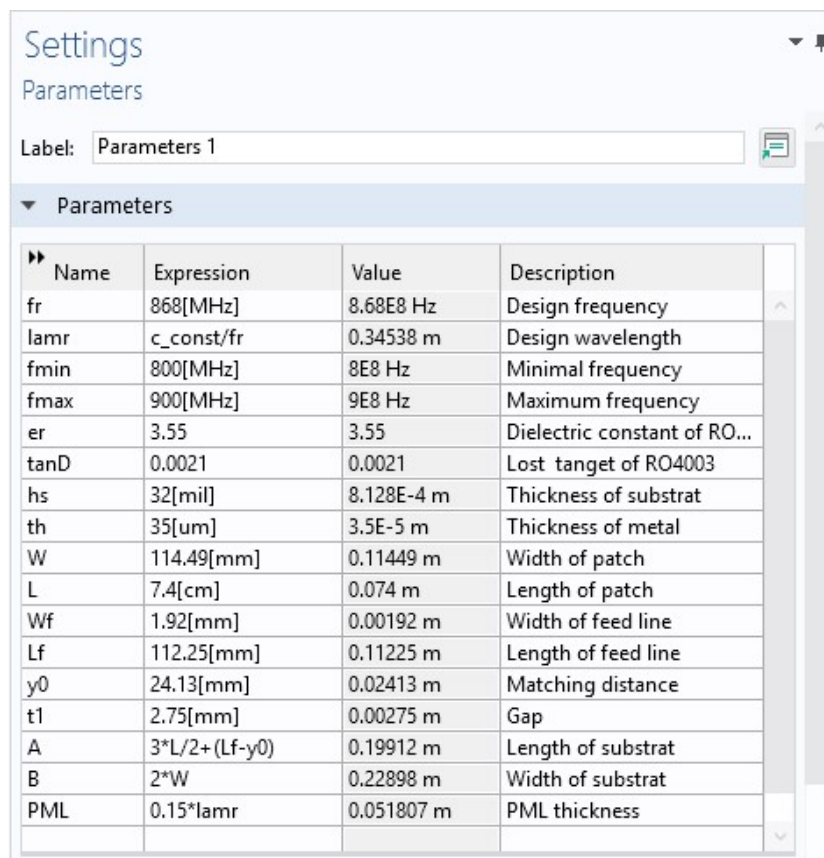


Рисунок 3.8 – Встановлення параметрів моделювання

Переходимо на вкладку «Geometry» і додаємо «Block» (рис. 3.9) для субстрату.

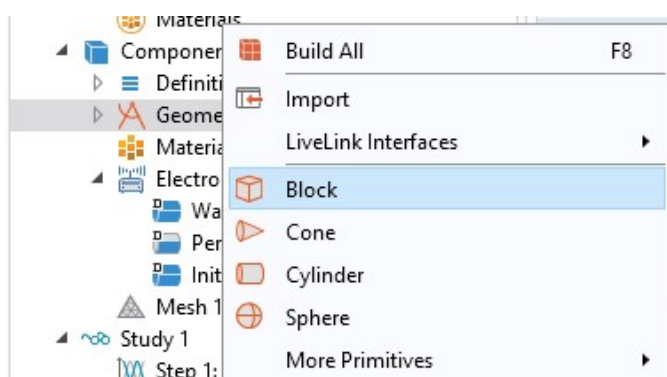
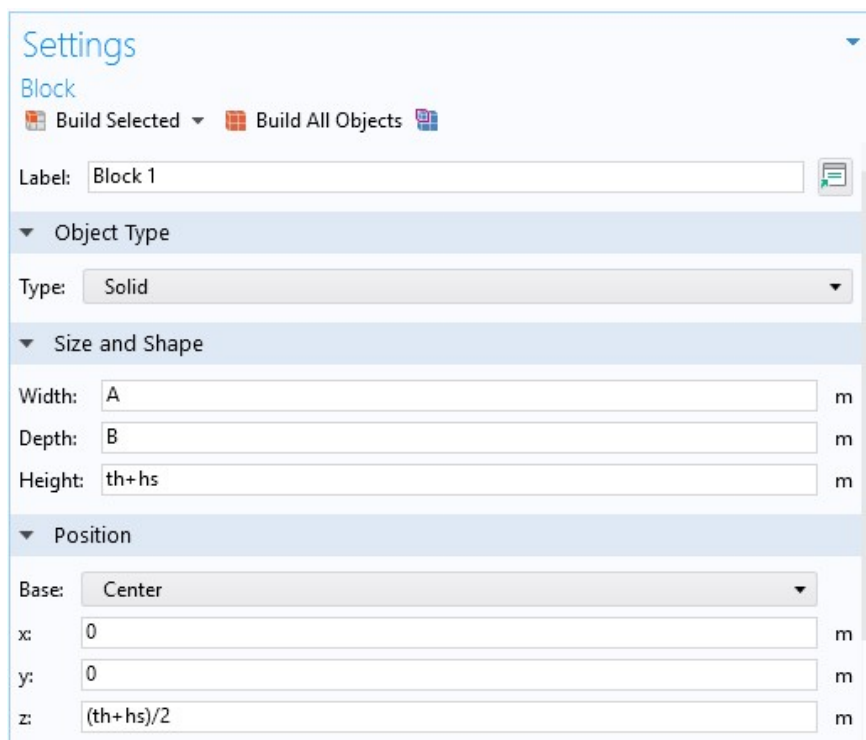


Рисунок 3.9 – Додавання «Block» до геометрії

Додаємо параметри до створеної геометрії (рис. 3.10).



Settings

Block

Build Selected Build All Objects

Label: Block 1

Object Type

Type: Solid

Size and Shape

Width: A m

Depth: B m

Height: $th+hs$ m

Position

Base: Center

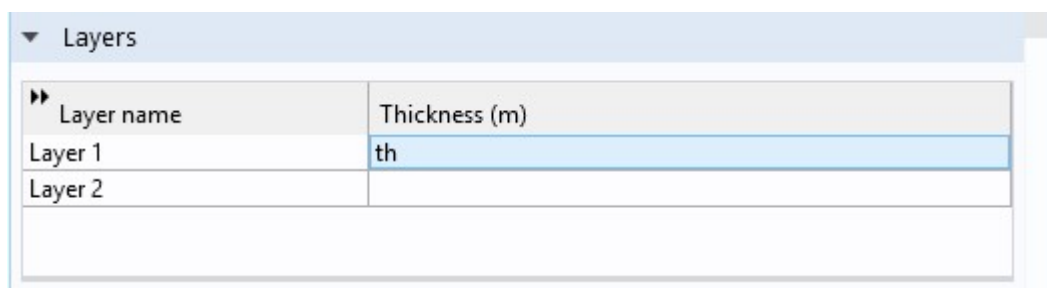
x: 0 m

y: 0 m

z: $(th+hs)/2$ m

Рисунок 3.10 – Встановлення параметрів до «Block»

Тепер додаємо шар і вказуємо його параметром товщину металу (рис. 3.11).



Layers	
Layer name	Thickness (m)
Layer 1	th
Layer 2	

Рисунок 3.11 – Встановлення параметрів до шару

Отримана геометрія зображена на рис. 3.12.

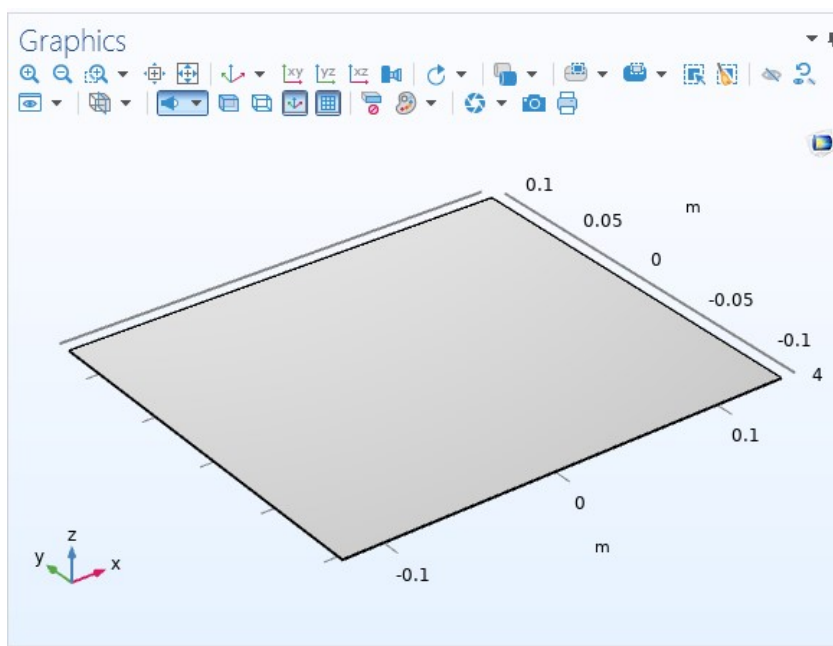


Рисунок 3.12 – Результат моделювання «Block»

Знову переходимо на вкладку «Geometry» і додаємо «Work Plane» (рис. 3.13) для патчу та лінії живлення.

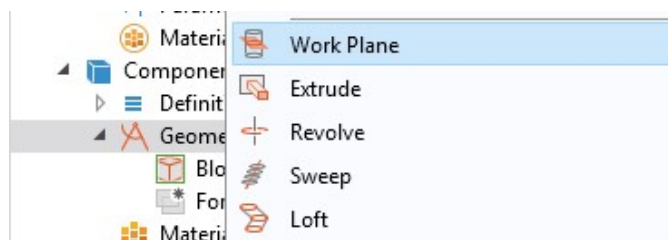


Рисунок 3.13 – Додавання «Work Plane» до геометрії

Встановлюємо координати цієї площини так, щоб вона була розміщена над «Block» (рис. 3.14).

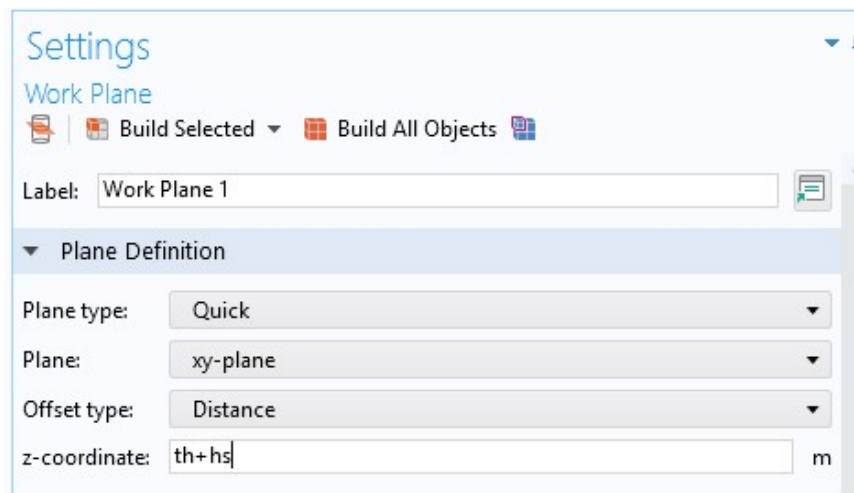


Рисунок 3.14 – Налаштування "Work Plane"

Тепер створюємо у цій площині прямокутник (рис. 3.15).

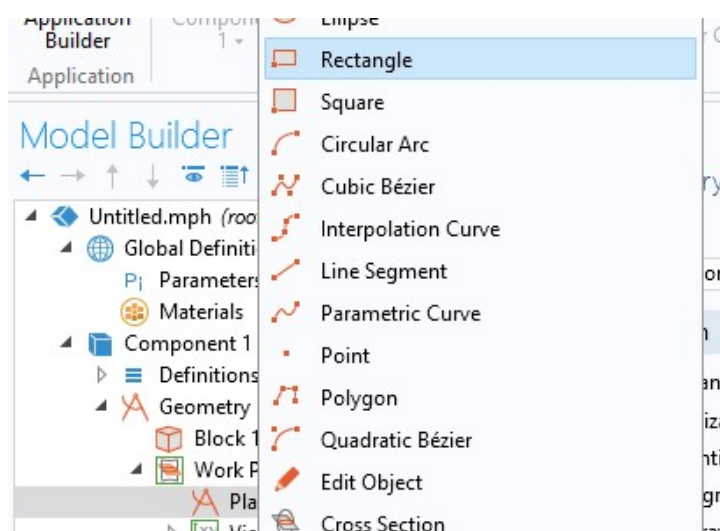


Рисунок 3.15 – Додавання прямокутника на площині

Задаємо параметри прямокутника (рис. 3.16).

Settings

Rectangle

Build Selected Build All

Label: Patch

Object Type

Type: Solid

Size and Shape

Width: L m

Height: W m

Position

Base: Corner

xw: $-A/2 + (Lf - y_0)$ m

yw: $-B/2 + W/2$ m

Рисунок 3.16 – Задавання параметрів прямокутника (Patch)

Отримуємо прямокутник зображений на (рис. 3.17).

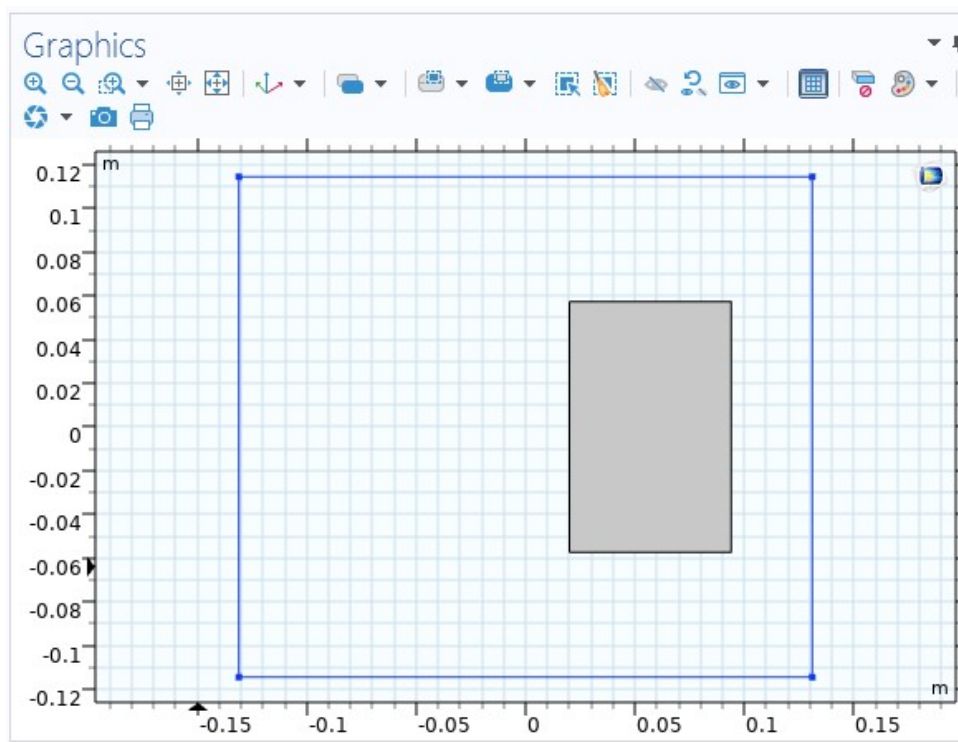


Рисунок 3.17 – Прямокутник «Patch»

Створюємо ще один прямокутник для створення проміжку для лінії живлення. Задаємо його параметри (рис. 3.18).

Settings
Rectangle

Build Selected Build All

Label: Matching

Object Type

Type: Solid

Size and Shape

Width: y_0 m

Height: $2 \cdot t_1 + W_f$ m

Position

Base: Corner

xw: $-A/2 + (L_f - y_0)$ m

yw: $-(2 \cdot t_1 + W_f)/2$ m

Rotation Angle

Rotation: 0 deg

Layers

Рисунок 3.18 – Задавання параметрів прямокутника (Matching)

Отримуємо інший прямокутник на площині створеного раніше (рис. 3.19).

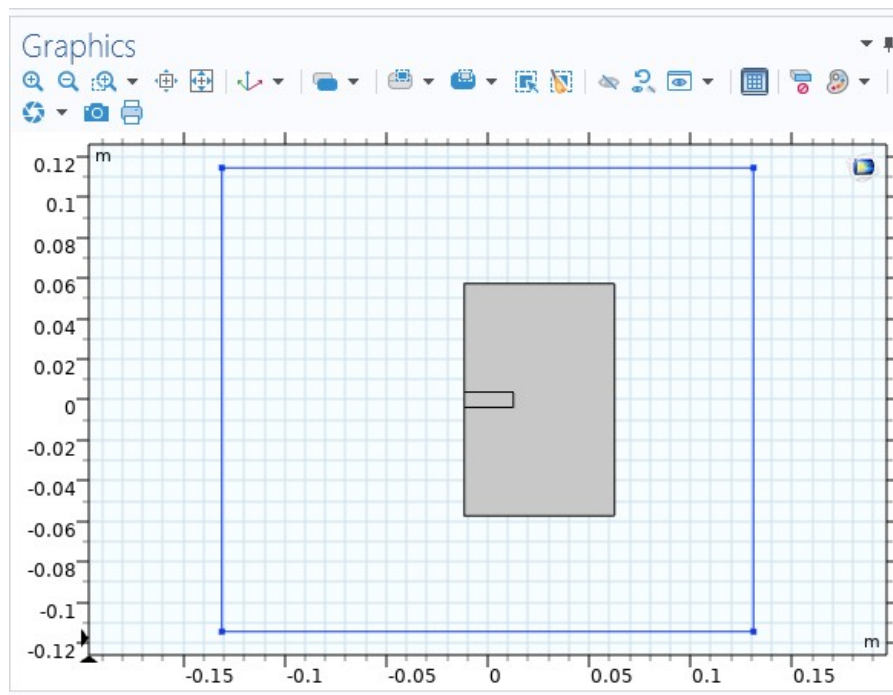


Рисунок 3.19 – Прямокутник «Matching» на прямокутнику «Patch»

Далі за допомогою команди «Difference» (рис. 3.20) видаляємо з площини «Patch» площину «Matching».

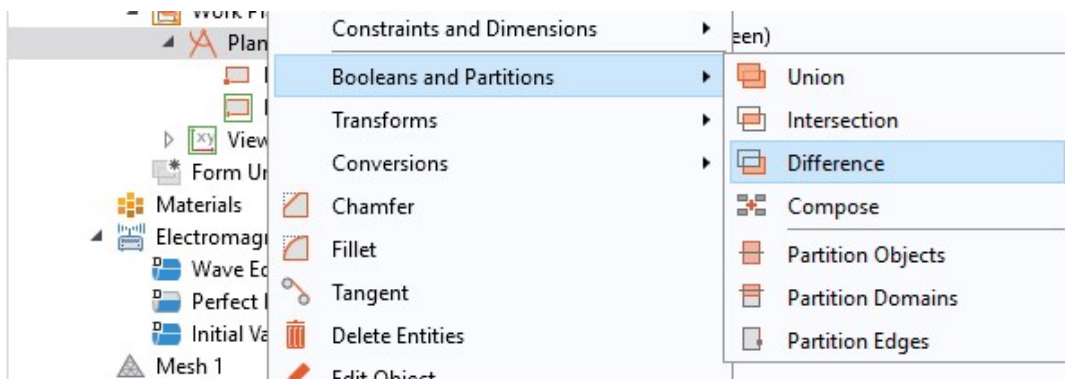


Рисунок 3.20 – Команда «Difference»

Отримуємо результат зображень на (рис. 3.21).

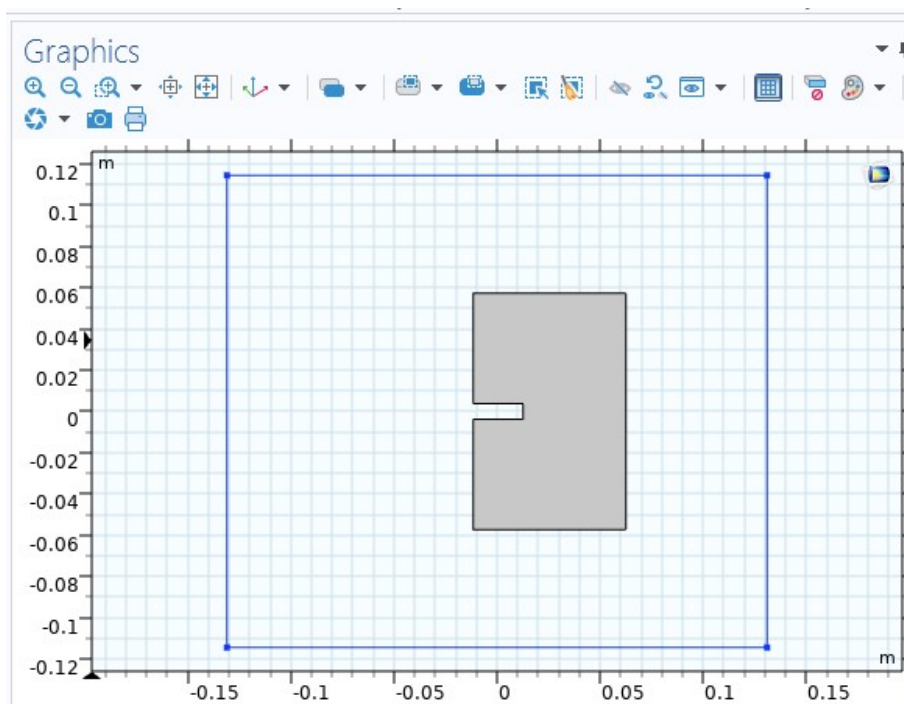


Рисунок 3.21 – Результат команди «Difference»

Далі створюємо ще один прямокутник для лінії живлення (Feed Line).
Задаємо його параметри (рис. 3.22).

Рисунок 3.22 – Задавання параметрів прямокутника (Feed Line)

Отримуємо ще один прямокутник (Feed Line) (рис. 3.23).

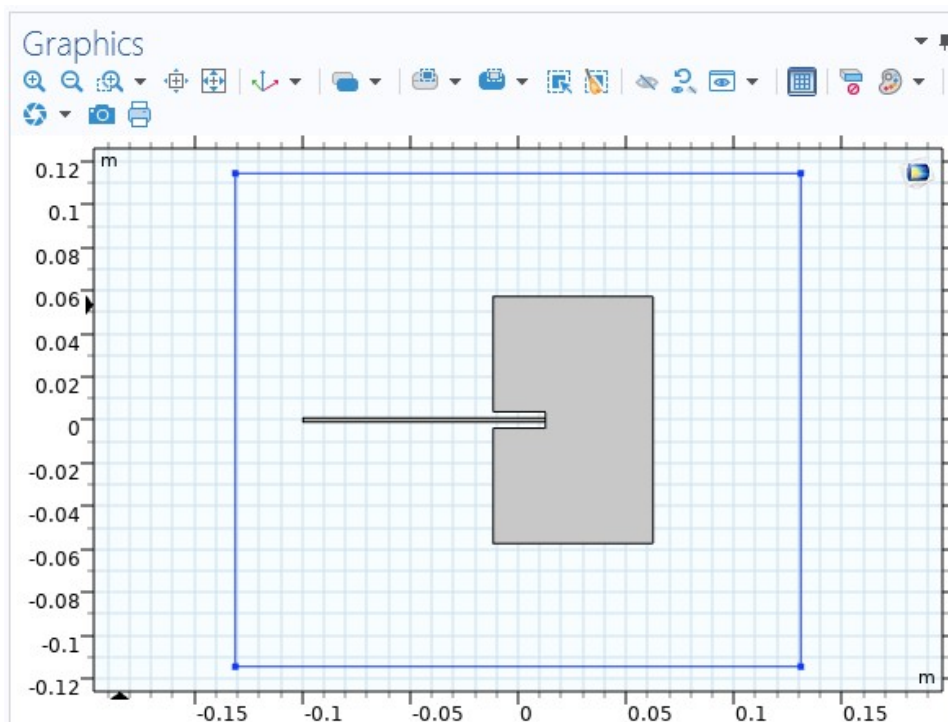


Рисунок 3.23 – Прямокутник «Feed Line» разом з прямокутником «Patch»

Далі застосовуємо команду «Union» (рис. 3.24) для об'єднання прямокутників «Feed Line» та «Patch».

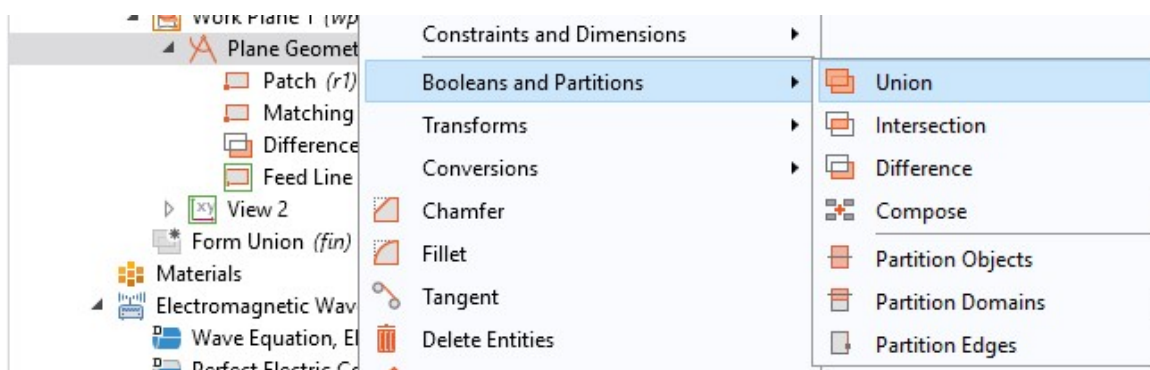


Рисунок 3.24 – Команда «Union»

Результат команди «Union» зображений на рисунку 3.25.

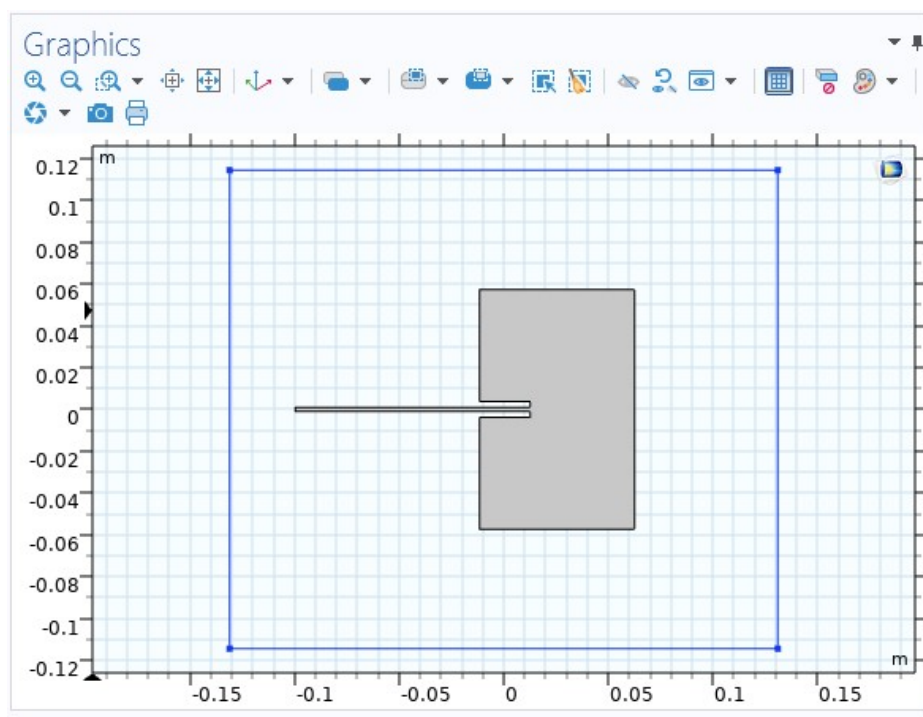


Рисунок 3.25 – Результат команди «Union»

Далі переходимо на вкладку «Work Plane» і натискаємо «Build All Objects». Тепер створений об'єкт відображається на раніше створеній площині (рис. 3.26).

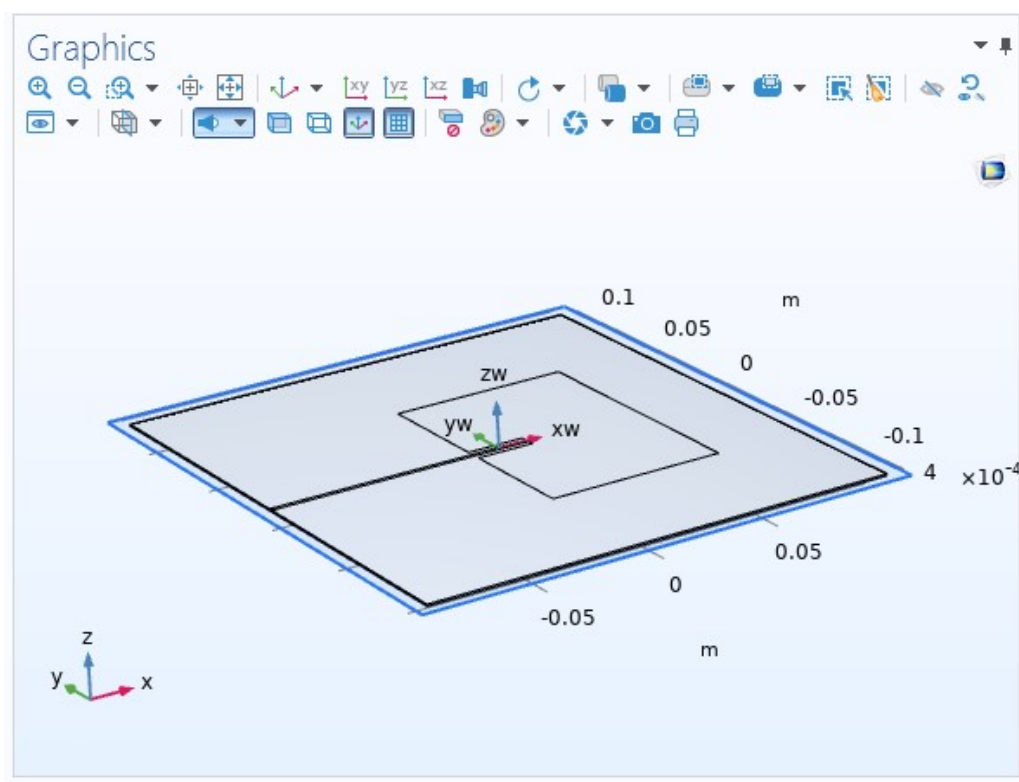


Рисунок 3.26 – Побудований об'єкт на площині

Застосовуємо команду «Extrude» до створеного об'єкту і екструдуємо його на відстань th (товщина металу). Результат зображений на рисунку 3.27.

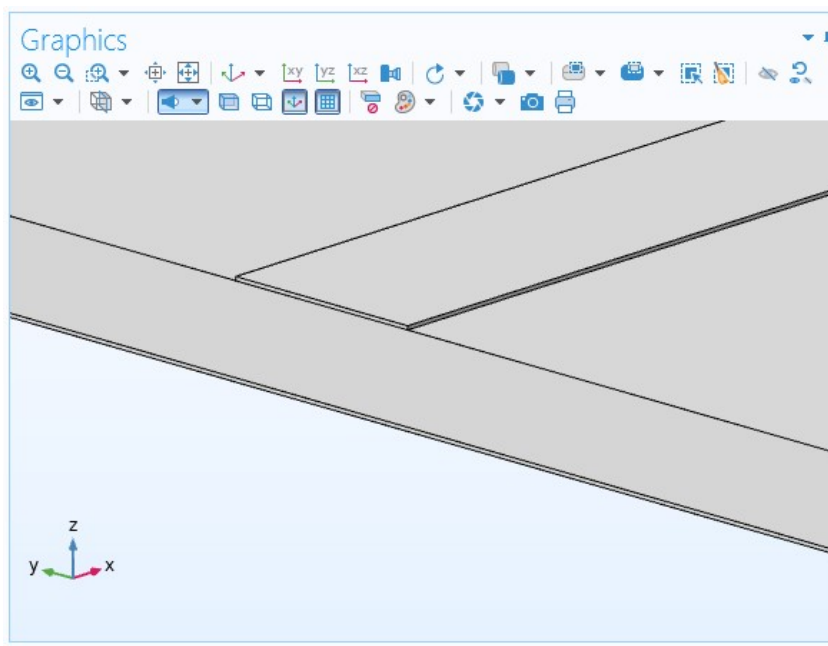


Рисунок 3.27 – Результат команди «Extrude»

Створюємо ще одну площину перпендикулярно до об'єкту для створення порту для лінії живлення, додаємо прямокутник і задаємо параметри (рис. 3.28).

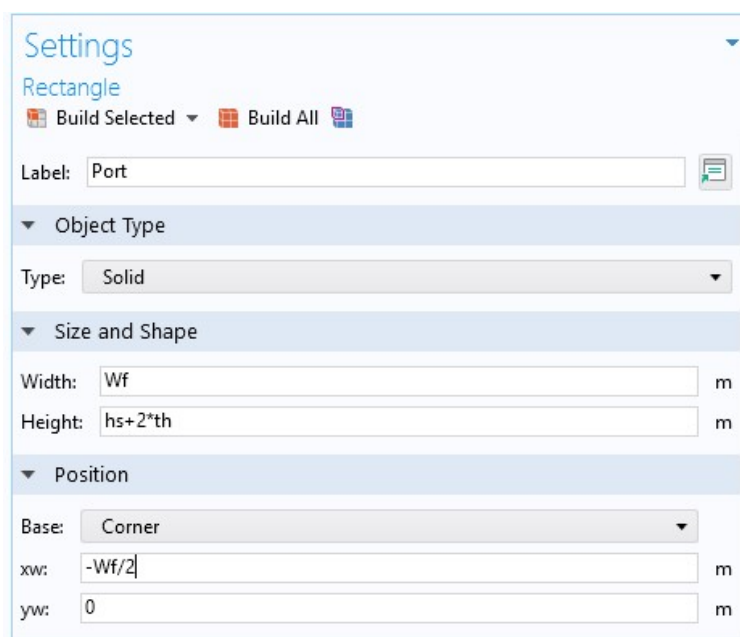


Рисунок 3.28 – Налаштування параметрів об'єкту «Port»

Створений об'єкт зображений на рисунку 3.29.

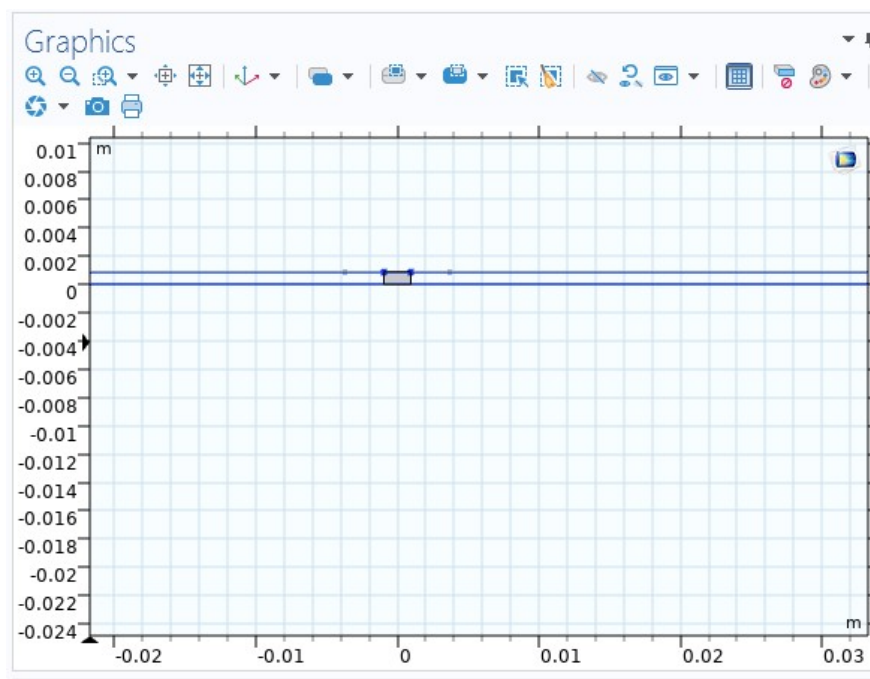


Рисунок 3.29 – Створений об'єкт «Port»

Створюємо сферу товщиною PML для зображення дії антени дальнього поля (Far Field) (рис. 3.30).

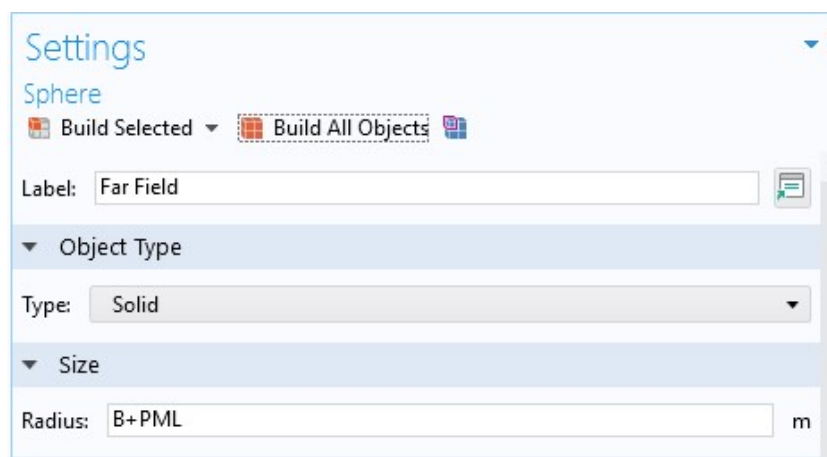


Рисунок 3.30 – Налаштування об'єкту Sphere

Створений об'єкт зображений на рисунку 3.31.

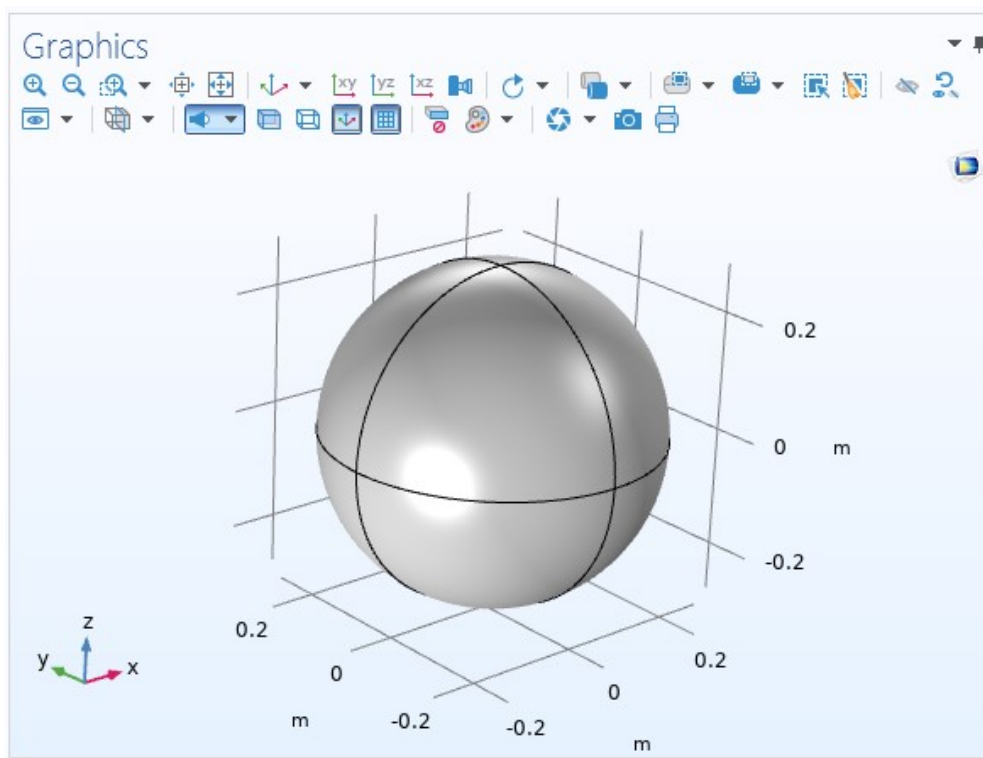


Рисунок 3.31 – Створена сфера «Far Field»

І за допомогою команди «Union» об'єднуємо усі створені об'єкти. Далі у вкладці «Definitions» створюємо сам PML (Perfectly Matched Layer) (рис. 3.32).

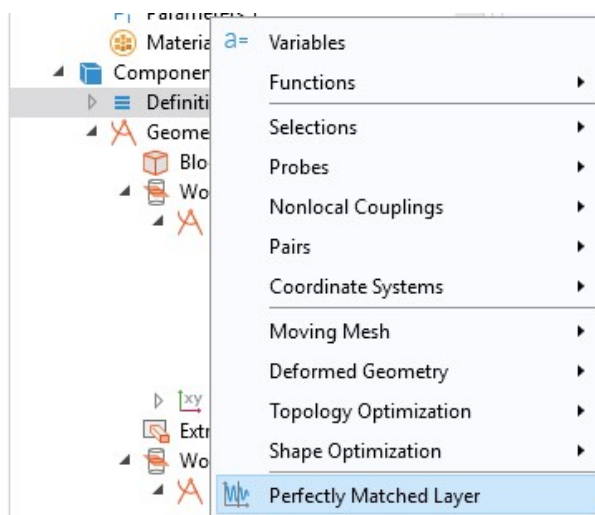


Рисунок 3.32 – Додавання «Perfectly Mathed Layer»

Обираємо сферичний тип і виділяємо усі сектори сфери, щоб додати шар до всіх них. Потім додаємо матеріали до створених об'єктів «Air» для сфери, та «Copper» для самої антени (рис. 3.33).

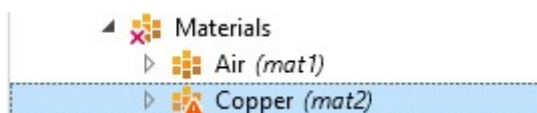


Рисунок 3.33 – Додавання матеріалів до створених об'єктів

Також створюємо матеріал субстрату RO4003C для самого патчу та задаємо його параметри (рис. 3.34).

Material Contents					
Property	Variable	Value	Unit	Property group	
☒ Relative permittivity	epsilon_r_is...	$\epsilon_r(1-i\tan\delta)$	1	Basic	
☒ Relative permeability	mu_r_iso ;...	1	1	Basic	
☒ Electrical conductivity	sigma_iso...	0	S/m	Basic	

Рисунок 3.34 – Параметри матеріалу субстрату RO4003C

Переходимо у вкладку «Electromagnetic Waves, Frequency Domain (emw)» і додаємо характеристику Far-Field Domain. Ця характеристика застосовується до схованої площини усередині сфери (рис. 3.35).

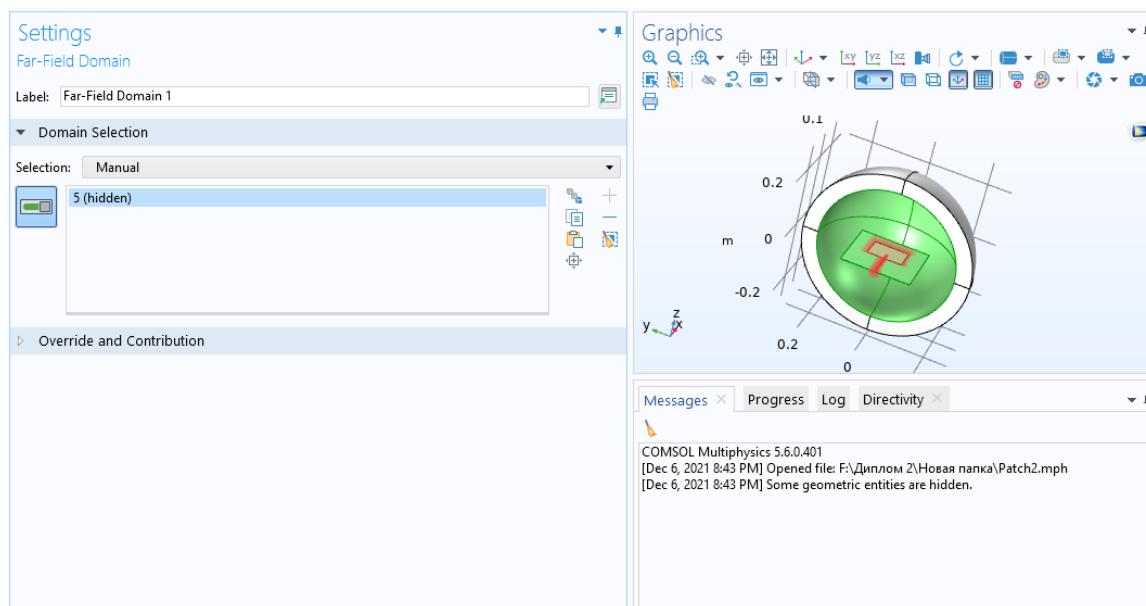


Рисунок 3.35 – Результат додавання Far-Field Domain

Додаємо характеристику Lumped Port і встановлюємо її значення (рис. 3.36).

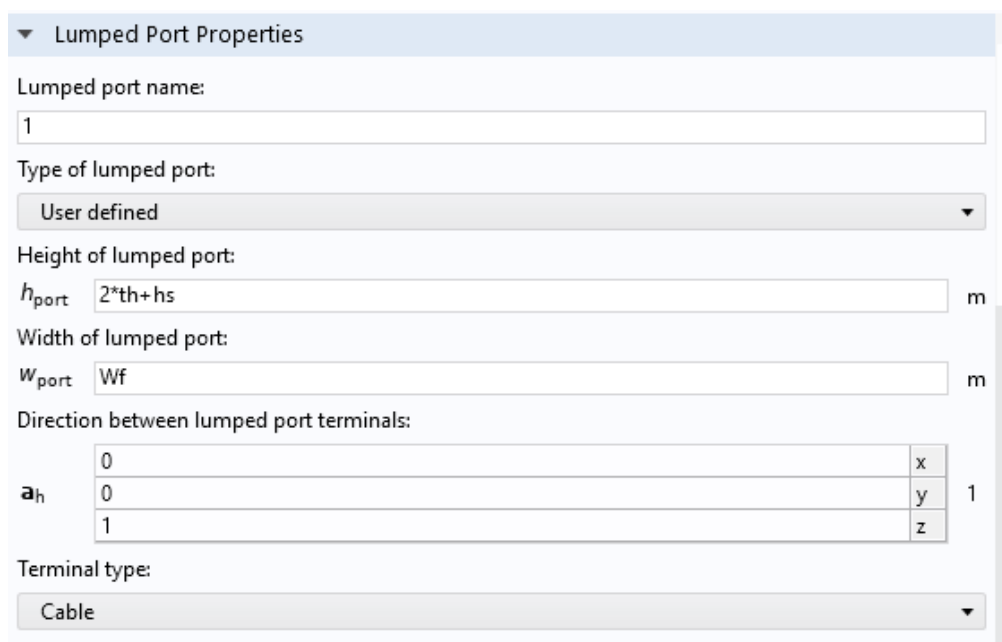


Рисунок 3.36 – Характеристики Lumped Port

Застосовуємо її до об'єкту «Port» (рис. 3.37).

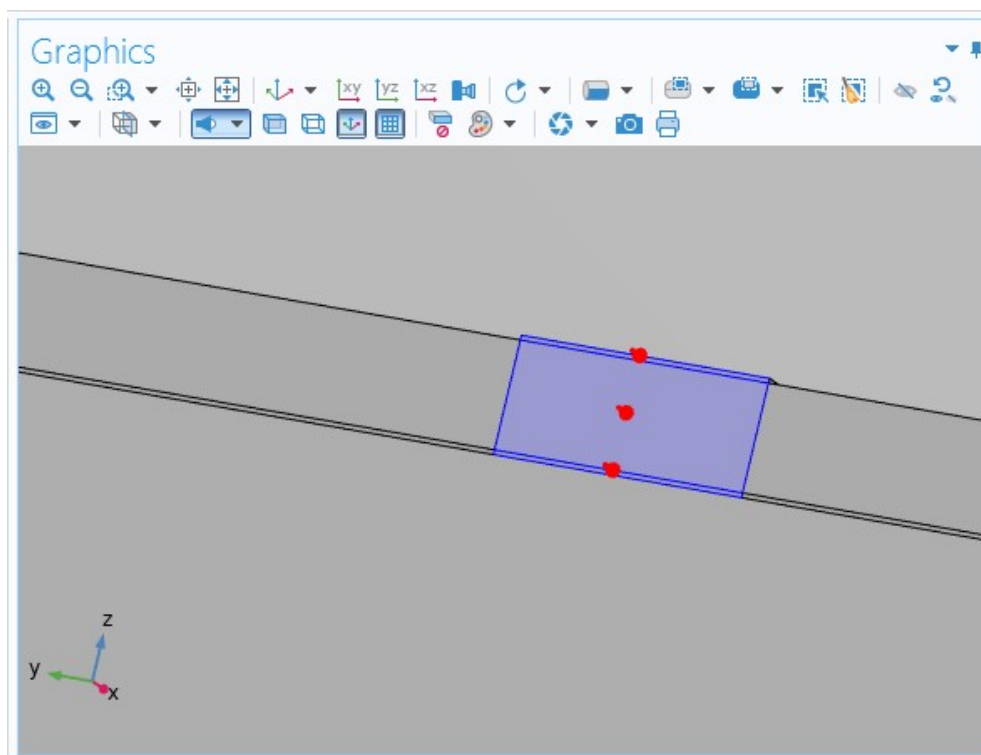


Рисунок 3.37 – Результат додавання Lumped Port

Переходимо у вкладку Mesh та натискаємо «Build All». Результат операції зображений на рисунку (рис. 3.38).

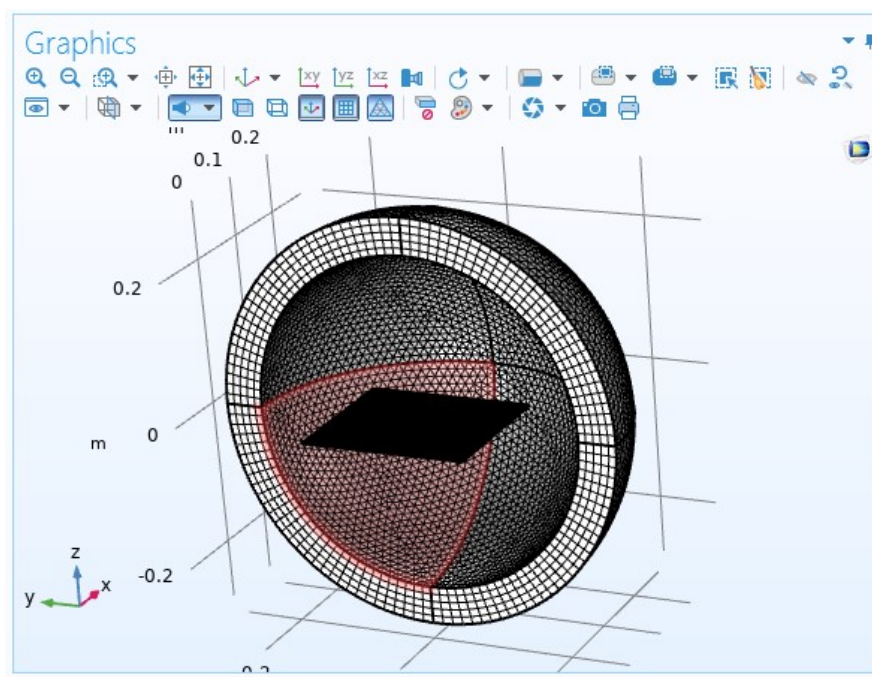


Рисунок 3.38 – Результат побудови Mesh

Для подальших розрахунків було зменшено точність моделювання (кількість полігонів) деяких площин. Результат зменшення точності зображений на рис. 3.39.

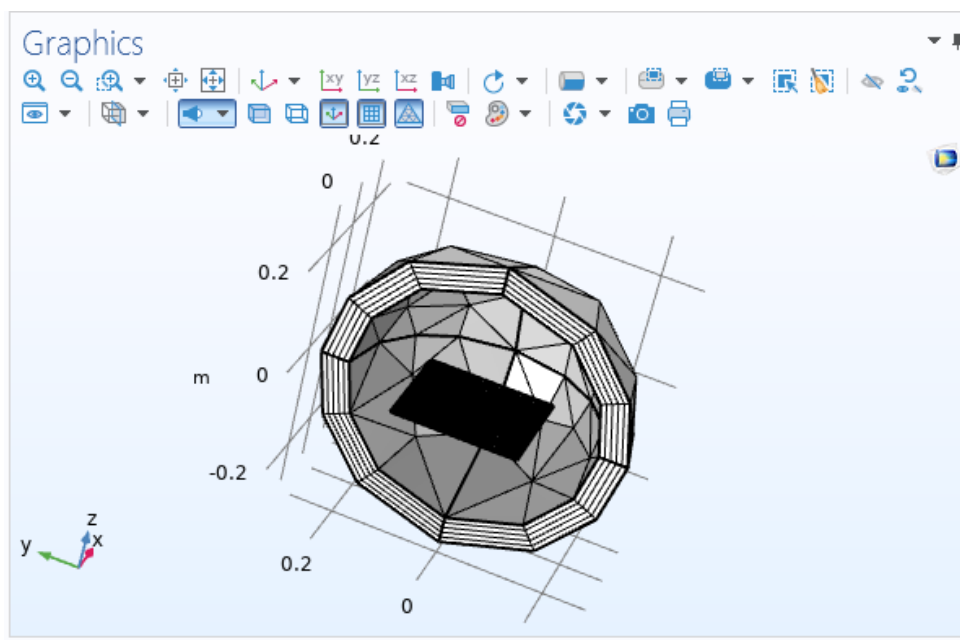


Рисунок 3.39 – Результат зменшення точності моделювання

Переходимо у вкладку «Step 1: Adaptive Frequency Sweep» і встановлюємо межі частотного діапазону та крок для дослідження (рис. 3.40).

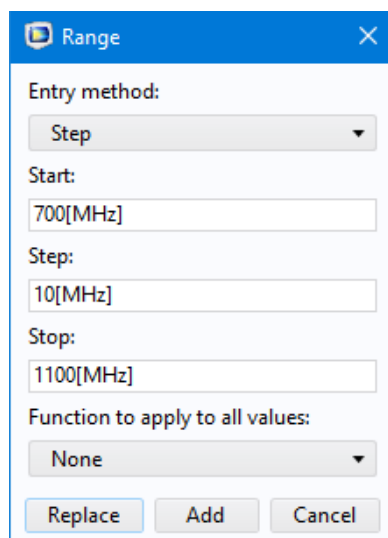


Рисунок 3.40 – Параметри частотного діапазону для дослідження

Для цієї антени за замовчуванням розрахунок відбувається ітераційним методом (Iterative), який потребує багато ресурсів, тому краще застосувати прямий (Direct) метод. Результат симуляції на частоті 870 МГц зображений на рисунку 3.41.

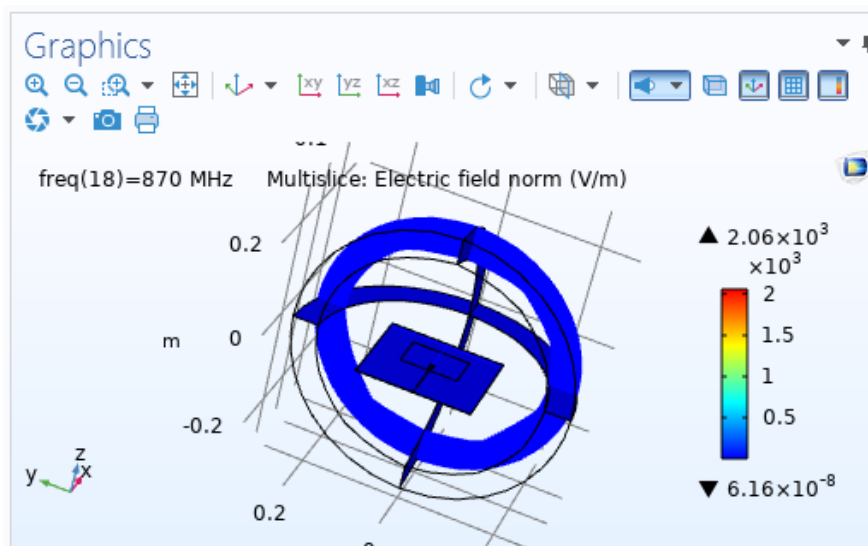


Рисунок 3.41 – Результат симуляції на частоті 900 МГц

Далі переходимо у вкладку 3D Far Field і бачимо результат симуляції на частоті 870 МГц (рис. 3.42).

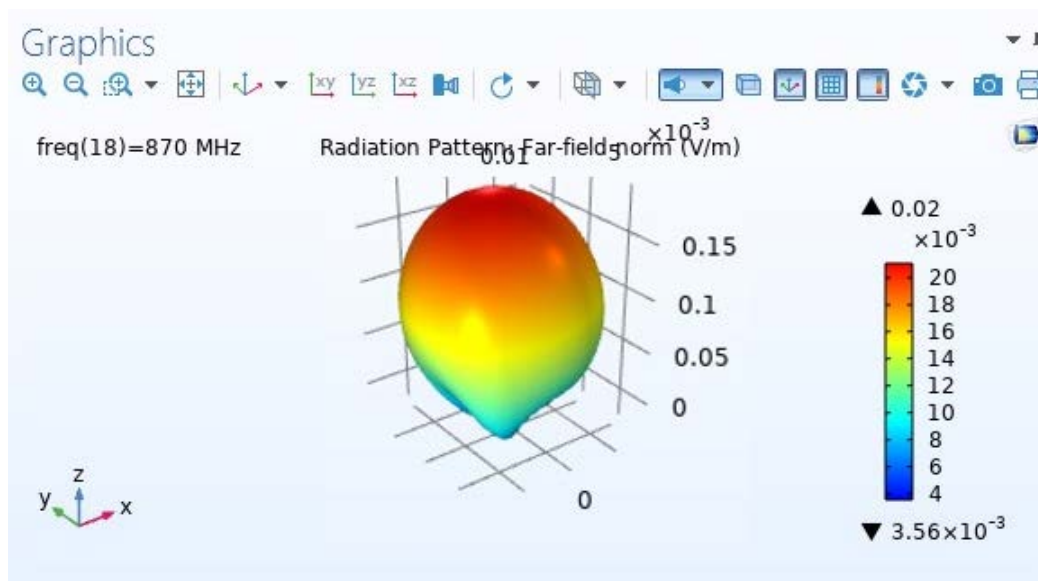


Рисунок 3.42 – Результат симуляції 3D Far Field на частоті 870 МГц

Як видно з рисунку на частоті 870 МГц антена має гарні показники випромінювання у режимі дальнього поля, а отже підходить для використання у цьому діапазоні частот.

Для портальних зчитувачей краще використовувати патч-антени з круговою, а не лінійною поляризацією, тому було використано 4 антени UHF Advantenna-p33 та UHF-зчитувач ID ISC.LRU (рис. 3.43).



Рисунок 3.43 – UHF-зчитувач ID ISC.LRU (а) і антена UHF Advantenna-p33 (б)

Антени розміщено безпосередньо у проході по обидва боки. На кожній стороні по дві RFID антени одна над іншою – це важливо для збільшення ймовірності успішного сканування всіх міток, що потрапили в зону дії антен, оскільки RFID мітки не впорядковано, а хаотично. Схема розміщення представлена малюнку знизу. Антени закріплено безпосередньо на стіні. Для перекриття всієї зони сканування антени можна повертати по відношенню одне до одного по вертикалі або горизонталі.

Оскільки товар у фурі може знаходитись на висоті до трьох метрів від землі, то на рис. 3.44 (розміщення антен) X становить 40 см, $Y = 300$ см, $Y_1 = Y/4 = 75$ см, $Y_2 = Y/2 = 150$ см. Ширина воріт становить 400 см, а ширина зони сканування – 320 см.

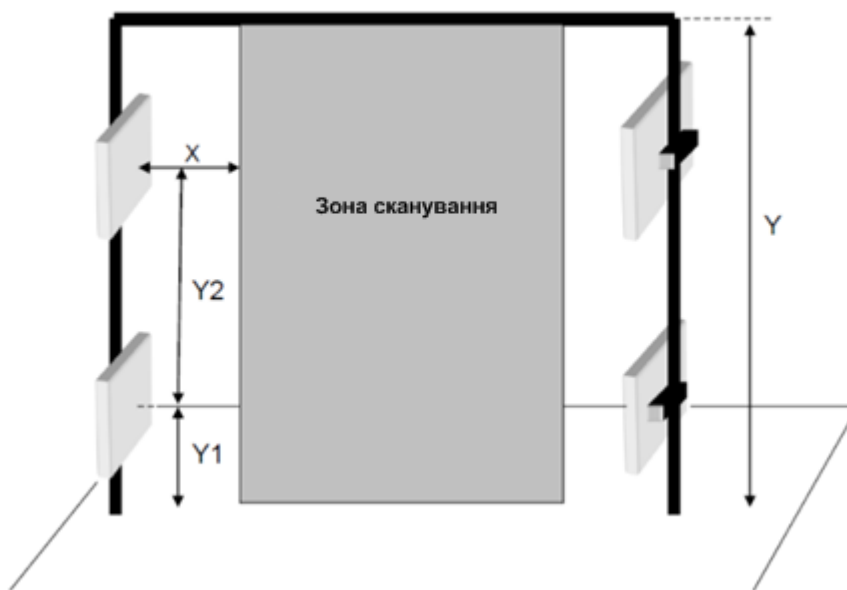


Рисунок 3.44 – Розміщення антен у портальному зчитувачеві

3.3 Вибір транспондерів

RFID мітки складаються з двох основних компонентів – антени та мікросіпа. Габаритні розміри антен міток, що працюють у дальній зоні (far field), визначаються розміром антени. Антена є резонатором та має реальний вхідний імпеданс. Це забезпечує підвищення ефективності випромінювання та прийому, полегшує узгодження та передачу потужності від/до електронної схеми, яка під'єднана до антени. Таким чином, компактність RFID-міток залежить від розмірів антени, які перевершують розміри чіпа у багато разів і, як правило, визначають габарити міток.

Сучасні транспондери RFID варіюються за ціною від декількох центів (лише для читання, пасивні мітки) до кількох сотень доларів США (активні мітки з власним джерелом живлення та можливістю розпізнавання). На собівартість транспондера впливає якість кремнієвого чіпа, антени та субстрату. Вони можуть важити до граму (складаються з невеликого кремнієвого чіпа і тонкої антени на лавсановій підкладці). Діапазони варіюються від 0,02 метра до 1 метра для міток

ближнього поля, до 15 метрів для дальнього поля і до 300 метрів для високоякісних активних тегів. Більшість антен виготовляються з гнучкого матеріалу [12].

Друкована плата (PCB) є матеріалом, який утримує етикетку разом. Підкладка може бути жорсткою або гнучкою і складатися з багатьох різних типів матеріалів, залежно від типу та призначення мітки. Наприклад, мітки, які використовуються для відстеження компонентів на конвеєрі, де можуть зустрічатися надзвичайно високі температури, мають тенденцію бути набагато більш жорсткими і зазвичай розміщуються всередині захисного корпусу. Гнучкі мітки повинні бути достатньо міцними, щоб витримувати а також захистити внутрішню IC. RFID-мітки, що використовуються в рішеннях для відстеження документів, можуть бути дуже гнучкими, для того, щоб згинатись разом з папером. Гнучкі мітки використовують тонкі пластикові плівки, в які вбудовані компоненти та схеми мітки. Мітки, які можуть бути застосовані до деталей у процесі виробництва, можуть бути негнучкими, та використовувати епоксидну смолу.

Для створеного RFID-рішення для WMS існує необхідність друкування RFID-міток прямо при прийомі товарів, тому варто зупинитись на виборі RFID-етикеток ZBR2000 (рис. 3.45). Ці транспондери мають високу чутливість у діапазоні зчитування до 17 метрів у вільному просторі, що забезпечує стабільну, надійну роботу та допомагає досягти кращої рентабельності інвестицій.



Рисунок 3.45 – RFID-етикетка ZBR2000

Що стосується міток для використання співробітниками при реалізації СКУД, то було обрано транспондери у вигляді пластикових карток-пропусків. Було обрано безконтактні картки EM-MARINE 0,8 мм (ЧІП ORIGINAL EM4200) – товщиною 0,8 мм, які працює на частоті 125 кГц (рис. 3.46).



Рисунок 3.46 – Безконтактна картка EM-MARINE 0,8 мм
(ЧІП ORIGINAL EM4200)

Безконтактна картка з оригінальним чіпом EM4200 у розмірі 40 біт. Використовується лише для читання. Виготовляється з покращеною (квадратною) антеною, що збільшує відстань спрацьовування карти до 10 см. Картка виглядає як ПВХ-пластина білого кольору, товщиною 0,8 мм. Завдяки гладкій ламінованій поверхні з двох сторін, на таку карту можна наносити високоякісну графіку та тексти для персоналізації та брендування. Розміри картки – 86x54x0.8 мм. Стандарт – ISO18000-2. Діапазон робочих температур від -30 до +70 °С.

У якості транспондерів призначених для уникнення травм співробітників при використанні транспортних засобів обрано мітки-браслети SafeTags (рис. 3.47) від компанії Kinexon.



Рисунок 3.47 – SafeTag у вигляді браслету

Транспондер підтримує візуальну та звукову сигналізацію у тому випадку, коли працівник знаходиться на небезпечній відстані від транспортного засобу. Також пристрій можна вимикати за допомогою кнопки для водіїв, щоб почати керувати транспортним засобом. Задану безпечну відстань можна встановити з точністю до 10 сантиметрів. Пристрій працює автономно, до 24 годин не потребує зарядки.

3.4 Вибір програмного забезпечення

Для системи управління складом необхідне програмне забезпечення, яке повинне мати можливість бут інтегрованим до існуючої архітектури системи. А також працювати із базою даних та підтримувати інвентаризацію. Тому було обрано Zebra MotionWorks Enterprise – це інноваційна платформа, яка дозволяє підприємствам перетворювати дані про місцезнаходження своїх активів на аналітичну бізнес-інформацію. Дана платформа виконує збір, обробку та аналіз даних з міток, якими позначені об'єкти, а потім передає цю інформацію на єдину

інтегровану консоль управління для надання точної оперативної інформації про місцезнаходження та стан кожного об'єкта.

MotionWorks Enterprise є локальним корпоративним програмним забезпеченням для серверів, яке надає всі базові інструменти для розгортання та управління мережними датчиками, збору та збагачення даних, а також оповіщення про події, пов'язані з детекцією руху та самим рухом, за допомогою звітів, потоків даних та API. Система займається картами, моніторингом та складанням звітів про датчики та етикетки, а також відстежуваними корпоративними ресурсами.

Для системи СКУД було обрано програмне забезпечення ZKTeco Access 3.5 (рис. 3.48), яке також підтримує облік часу. Додаток спеціально розроблений для управління контролерами та терміналами ZKTeco. ПЗ може формувати звіти.



Рисунок 3.48 – Головне вікно ПЗ ZKTeco Access 3.5

Характеристики програмного забезпечення ZKTeco Access 3.5:

- потужний технічний ресурс, що дозволяє керувати даними контролю доступу 30000 осіб, з можливістю підключення 100 пристроїв стандартної конфігурації;
- висока продуктивність та підвищена функціональність;
- автоматичне керування списком користувачів;

- багаторівневе керування системою, заснованою на ролях, що забезпечує необхідну безпеку даних користувача.

Системні вимоги:

- CPU: Частота 2.0 ГГц або вище;
- пам'ять: 1 Гб або більше;
- обладнання: 10 Гб вільного місця на жорсткому диску або більше.

Для безпеки працівників при роботі з транспортними засобами використано програмне забезпечення KINEXON SafeZone (рис. 3.49)

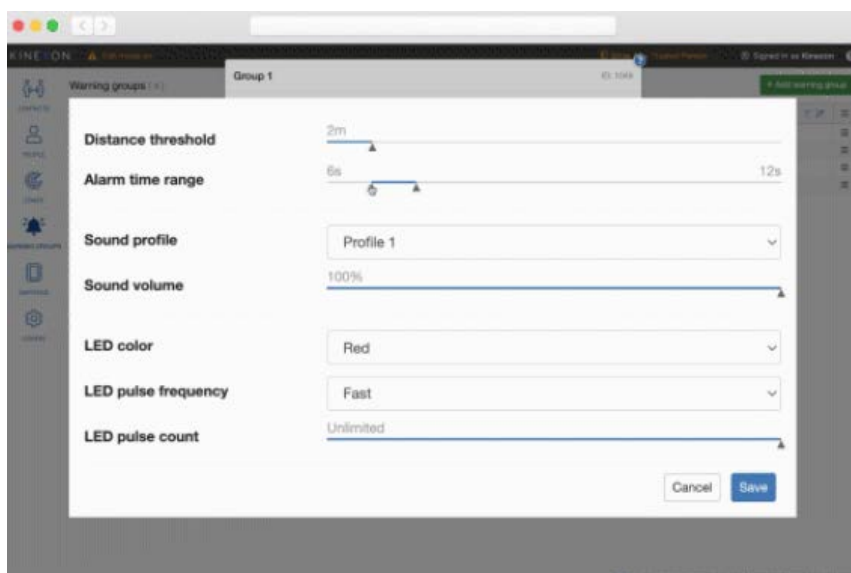


Рисунок 3.49 – Вікно налаштувань транспондера у ПЗ KINEXON SafeZone

Є можливість інтегрувати KINEXON SafeZone безпосередньо в існуючу IT-інфраструктуру (локально або в Amazon-хмарі) і отримати легкий прямий доступ до програми. Додаткова інфраструктура не потрібна. Це гарантує швидке впровадження та гнучке масштабування рішення в інших областях.

3.5 Вибір додаткових компонентів

Для реалізації системи управління складом необхідні також такі компоненти як RFID-принтер, та комутатор. У якості RFID-принтера було обрано ZT610 (рис. 3.50) компанії Zebra.

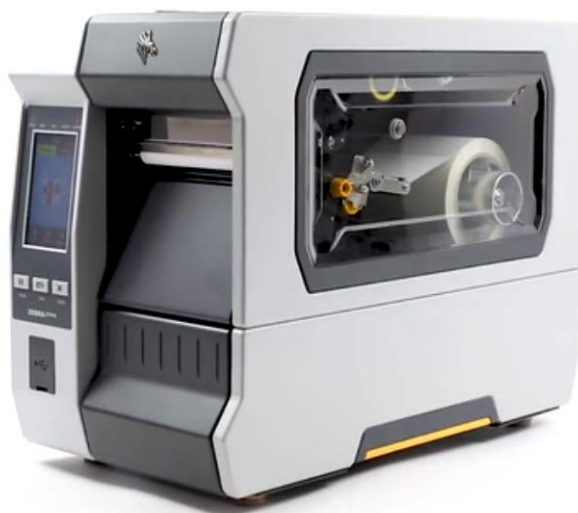


Рисунок 3.50 – RFID-принтер ZT610

Інтеграція RFID-модуля у принтер ZT610 для виконання кодування на місці експлуатації займе лише п'ять хвилин. Після встановлення RFID-модуля можна використовувати ці принтери не тільки для точного та ефективного друку, але і для кодування етикеток для найпередовіших програм відстеження на рівні об'єктів. Технологія кодування, що налаштовується, дозволяє використовувати різні матеріали для друку і спрощує калібрування RFID, позбавляючи від складних інструкцій з розміщення. Інтуїтивне меню додатково скорочує час на налаштування.

Унікальна програмна платформа забезпечує неперевершений рівень доступності оперативних даних та управління системами друку як на місці експлуатації, так і у віддаленому режимі. А хмарні програми спрощують всі процеси: від налаштування до управління та безпеки.

Принтер забезпечує неперевершену якість друку у найважчих умовах роботи та практично повністю виключає простої внаслідок несправності принтера.

Надійна суцільнометалева конструкція принтерів підходить для роботи в умовах екстремальних температур, пилу, сміття, вологи тощо.

У якості комутатора використано комутатор TP-LINK TL-SG1024D (TL-SG1024D) (рис. 3.51). 24-портовий гігабітний настільний / монтуємий в стійку комутатор TL-SG1024D є просте рішення для переходу на гігабітний Ethernet. Застосування інноваційної енергозберігаючої технології дозволить зберегти до 20% споживаної електроенергії, тому TL-SG1024D є екологічно безпечне пристрій для вашої офісної мережі.

Модель TL-SG1024D оснащена 24 портами 10/100/1000 Мбіт / с, що значним чином збільшує пропускну здатність вашої мережі, дозволяючи передавати файли великого розміру в найкоротший час. Тому користувачі будинку, в офісі, в робочій групі або дизайн-студії тепер можуть швидше передавати великі, чутливі до пропускну здатності каналу файли.

24-портовий гігабітний комутатор TL-SG1024D підтримує останні енергозберігаючі технології, за допомогою яких ви зможете збільшити пропускну здатність вашої мережі зі значно меншими енерговитратами. Пристрій автоматично вибирає режим живлення в залежності від статусу з'єднання і довжини кабелю для того, щоб зберегти електроенергію і тим самим обмежити кількість викидів вуглецю, що здійснюються при її виробленні.

При виключенні комп'ютера або мережевого устаткування, відповідний порт звичайного комутатора продовжує споживати значну кількість електрики. Комутатор TL-SG1024D може автоматично визначати статус з'єднання на кожному порту і скорочувати споживання електроенергії на непрацюючих портах.

Короткий кабель споживає менше електрики через менших втрат при передачі; але на більшості комутаторів це не береться до уваги – вони подають однакове живлення незалежно від довжини кабелю – 10 або 50 метрів. На відміну від звичайних комутаторів з подачею однакового живлення на всі порти, комутатор TL-SG1024D визначає довжину підключеного кабелю Ethernet і вибирає відповідний режим живлення.

Функції авто-узгодження гігабітного комутатора полегшують установку пристрою. Не потрібно додаткового налаштування. Функція авто-узгодження на кожному порту визначає швидкість з'єднання мережевого пристрою (10, 100 або 1000 Мбіт / с) і робить налаштування сумісності та оптимального режиму роботи.



Рисунок 3.51 – Комутатор TP-LINK TL-SG1024D (TL-SG1024D)

Що стосується системи СКУД, то є необхідність використання контролерів. Тому було обрано мережевий контролер ZKTeco C5S120 для 2 дверей (рис. 3.52).



Рисунок 3.52 – Мережевий контролер ZKTeco C5S120

Характеристики мережевого контролера:

- пам'ять 100000 RFID карт, 200000 записів журналу подій;
- можливість підключення 4 зчитувачів;
- входи: 2 кнопки, 2 геркони, 1 AUX вхід;

- виходи: 2 реле для замків, 1 дод. реле для виходу AUX;
- інтерфейси - Wiegand, RS485, Wi-Fi, Ethernet;
- розміри 191 x 171 x 31.6 мм;
- високошвидкісний 32-розрядний процесор 1.2 ГГц, 128 МБ ОЗУ та 256 МБ Flash;
- вбудована операційна система LINUX;
- підтримка декількох форматів карт Wiegand та клавіатурного пароля;
- вбудований в панель управління апаратний сторожовий таймер запобігає збоям;
- захист від перевантаження по струму, перенапруги та зворотної напруги для адаптера живлення, що підключається;
- захист від перевантаження струму для живлення зовнішніх зчитувачів;
- захист від перенапруги для всіх портів введення/виводу;
- захист від перенапруги для портів зв'язку.

Для турнікету у СКУД передбачена можливість роботи через сигнал кнопки. Кнопку виходу було обрано YLI ISK-841A (рис. 3.53). ISK-841A - безконтактна кнопка зі світловою індикацією, використовується в системах контролю доступу. Тип монтажу – врізний. Відчинення дверей відбувається при піднесенні руки або будь-якого предмета до кнопки, без торкання. Кнопка ISK-841A має стильний дизайн, а яскраве підсвічування сповістить про стан дверей ("зелений" - зачинено, "червоний" - відчинено).



Рисунок 3.53– Кнопка виходу СКУД YLI ISK-841A

У якості замку для дверей СКУД було обрано замок електромагнітний CoVi Security CS-280G (рис. 3.54). CoVi Security GS-280G – накладний електромагнітний замок з силою утримання до 280 кг на розрив. Призначений для внутрішньої установки на металеві, пластикові, металопластикові, дерев'яні або скляні двері (з використанням монтажного куточка CS-280).



Рисунок 3.54 – Замок електромагнітний CoVi Security CS-280G

Магнітний або електромагнітний замок – пристрій для замикання дверей, принцип роботи якого заснований на магнітній взаємодії. Складається з корпусу з електромагнітом і планки з металу з високою магнітною проникністю.

Принцип роботи електромагнітного замка CoVi Security CS-280G. Електромагнітний замок встановлюється на дверну коробку, відповідна планка - на двері. При подачі живлення (DC12V/DC24V) замок примагнічується до відповідної планки, надійно замикаючи двері. При відсутності живлення – замок відкривається, що відповідає вимогам протипожежної безпеки.

Для таких компонентів СКУД як контролери, зчитувачі, замки, кнопка та турнікет необхідне джерело живлення 12В постійного струму. Тому було обрано трансформатор понижуючий ОСМ 1-0,1 220/220/12 УПП УТОС (рис. 3.55).

Трансформатори серії ОСМ (ОСМ1), однофазні сухі трансформатори напруги, використовуються як понижуючі багатоцільові (для потреб місцевого

освітлення), а так само призначені для живлення ланцюгів верстатного обладнання, для використання у лабораторних стендах промислового призначення, для живлення ланцюгів автоматики, в приводах.



Рисунок 3.55 – Трансформатор понижуючий ОСМ 1-0,1 220/220/12 УПП
УТОС

Для таких компонентів WMS як зчитувачі необхідне джерело живлення 24В постійного струму. Тому було обрано трансформатор Hager ST315, 230В/24В (рис. 3.56).



Рисунок 3.56 – Трансформатор понижуючий Hager ST315, 230В/24В

Простий та швидкий монтаж – можна встановлювати у будь-якому розподільчому щитку на монтажній планці. Напруга первинної обмотки становить 230В~. Напруга вторинної обмотки – 24В~. Номінальний струм становить 5,25 А (12В), 2,63 А (24В). Чотири модулі на din-рейці.

3.6 Розрахунок вартості системи контролю та управління складом

Таблиця 3.1 – Розрахунок вартості системи контролю та управління складом

Назва обладнання	Кількість	Ціна за одиницю (грн.)	Загальна вартість (грн.)
Мобільний зчитувач MC3330xR	8	31999	255992
RFID-зчитувач HIKVISION DS-K1802E	7	689	4823
Турнікет трипод EXPERT	1	29795	29795
RFID-зчитувач Zebra UWB Wand	4	5687	22748
UHF-зчитувач ID ISC.LRU	6	65 953	395 718
Антенa UHF Advantenna-p33	24	11 365	272760
RFID-принтер ZT610	1	65499	65499
Видаткові матеріали для друку міток	1	30000	30000
Безконтактна картка EM-MARINE 0,8 MM	100	7,12	712
SafeTag	30	100	3000
Програмне забезпечення Zebra MotionWorks Enterprise	1	19546	19546
Програмне забезпечення ZKTeco Access 3.5	1	9999	9999
Програмне забезпечення KINEXON SafeZone	1	27856	27856
Комутатор TP-LINK TL-SG1024D (TL-SG1024D)	2	2298	4596
Мережевий контролер ZKTeco C5S120	4	5236	20944
Кнопка виходу СКУД YLI ISK-841A	1	510	510
Замок електромагнітний CoVi Security CS-280G	7	560	3920
Трансформатор понижуючий ОСМ 1-0,1 220/220/12 УПП УТОС	1	389	389
Трансформатор понижуючий Hager ST315, 230В/24В	2	1992	3984
Сумарна вартість (грн.)	1 172 791		

Висновки до розділу

Для реалізації системи контролю та управління складом було підібрано якісні компоненти, сумарна вартість яких 1 172 791 грн.

Система управління складом починається з портальних воріт, які побудовані за допомогою UHF-зчитувача ID ISC.LRU та 4 антен UHF Advantenna-p33. Було обґрунтовано доцільність використання патч-антен у результаті розрахунку та моделювання антени за допомогою програмного забезпечення Comsol Multiphysics.

Усі ящики на складі обладнані RFID-етикетками ZBR2000. У випадку постачання товару від сторонніх компаній потрібне втручання людини. Оскільки, до кожної коробки потрібно нанести RFID-тег. Для цього у зоні відвантаження передбачений RFID-принтер ZT610 для міток, підключений до WMS-системи.

Працівники з базою даних за допомогою програмного забезпечення Zebra MotionWorks Enterprise віддалено заносять інформацію у теги про те, де саме має зберігатись товар. Оператори, використовуючи мобільний зчитувач MC3330xR, розвозять та збирають їх по потрібним стелажам.

Що стосується системи контролю доступом до приміщення, то у кожного співробітника є безконтактна картка EM-MARINE 0,8 ММ. Біля головного входу розташований турнікет трипод EXPERT із вбудованим зчитувачем. При зчитуванні коректної картки співробітник зможе пройти далі.

До інших приміщень складу можна потрапити через двері з RFID-зчитувачем HIKVISION DS-K1802E та електромагнітним замком CoVi Security CS-280G. При зчитуванні коректної картки (у базі даних міститься інформація про цей ідентифікатор і дозволені зони доступу) подається струм на електромагнітний замок і двері можна відчинити. Зчитувачі підключені до мережевого контролера ZKTeco C5S120 і уся система СКУД використовує програмне забезпечення ZKTeco Access 3.5.

Безпека працівників при роботі з автомобільною технікою реалізована за допомогою системи сигналізації при зближенні з транспортним засобом. Усі працівники другої зони – зони зберігання матимуть браслет з SafeTag. Програмне

забезпечення KINEXON SafeZone використовується для роботи з цими транспондерами. Транспорт у свою чергу обладнаний зчитувачем RFID-зчитувач Zebra UWB Wand. При зближенні працівника і транспорту більше, ніж на визначену відстань, браслет потрапляє у зону зчитувача та починає сигналізувати про це пішохода. Щодо водіїв, то вони також мають носити браслети у зоні зберігання. Тому передбачена можливість вимкнення сигналізації за допомогою кнопки для безпосереднього керування транспортним засобом.

Зв'язок головних компонентів із серверами забезпечує комутатор TP-LINK TL-SG1024D (TL-SG1024D). А специфічне живлення трансформатор понижуючий ОСМ 1-0,1 220/220/12 УПП УТОС та трансформатор понижуючий Hager ST315, 230В/24В.

4 РОЗРОБКА СТАРТАП ПРОЕКТУ

4.1 Опис ідеї проекту

Швидкий доступ до знань – це одна з найбільших переваг, якими може скористатись сьогодні людина. З кожним днем стає все більше цифрової інформації, але основою цих усіх нулів та одиниць є друковані видання, які поступово мігрують у цифровий світ. Але варто визначити, що ще досить довгий час друковані книжки будуть користуватись великим попитом.

Тому у цей перехідний період існує необхідність автоматизувати роботу бібліотек. Ця необхідність виникла вже давно й наразі одним із найпопулярніших рішень є система заснована на штрих-кодах. Ця система має багато недоліків: недовговічність штрих-коду, поштучне сканування тощо. Система радіочастотної ідентифікації може нівелювати усі ці недоліки та надати більше переваг.

Сутність стартапу полягає в автоматизації роботи бібліотеки. Впровадження пасивної надвисокочастотної (НВЧ) системи радіочастотної ідентифікації. Ця технологія регулюється стандартом ISO 18000-6-с і працює у діапазоні 860-960 МГц.

Переваги цього рішення:

- теги RFID, наклеєні на книгу, надають книзі індивідуальну ідентичність та безпеку під час процедури видачі та повернення;
- антикрадіжна система;
- читацькі картки RFID зіставляються з тегами книги під час видачі та поверненні;
- можливість автоматичної видачі та повернення дає змогу самостійно зареєструватися та виписати книги без будь-якого ручного втручання співробітників бібліотеки;
- RFID-бокс для скидання книг дозволяє бібліотеці функціонувати для повернення книги, навіть коли бібліотека закрита;

- станція пошуку книг дозволяє користувачеві шукати певну книгу за частки секунд;
- ручний зчитувач RFID дозволяє швидко проводити інвентаризацію на відстані та допомагає шукати втрачену книгу;
- уся система RFID інтегрована з центральною базою даних.

Розглянемо доцільність імплементації рішення за допомогою бізнес-моделі «Канвас» (рис. 4.1).

Бізнес-модель «Канвас»

8. Ключові партнери - Освітні заклади; - підприємства, які виробляють апаратні компоненти для RFID-рішень	7. Ключові дії - Розробка системи автоматизації; - розробка програмного забезпечення; - розробка сайту для реклами послуги; 6. Ключові ресурси - Стартовий капітал; - апаратні компоненти; - програмні компоненти;	2. Ключові цінності - Зменшення годин людської праці; - виключення людського фактору; - швидка інвентаризація; - можливість отримання та повернення книги у неробочий час.	4. Взаємовідносини з клієнтами Залучення бібліотек м. Києва за допомогою презентації технології. Створення сайту, де кожен зможе ознайомитись з перевагами та технічними характеристиками рішення 3. Канали збуту - Презентація продукту у бібліотеках;	1. Сегменти споживачів Насамперед бібліотеки учбових закладів, а також звичайні бібліотеки
9. Структура витрат - Обладнання; - програмне забезпечення - реклама.		5. Потіки доходів - оплата за інтеграцію рішення; - оплата за супроводжуючу технічну підтримку.		

Рисунок 4.1 – Бізнес-модель «Канвас»

4.2 Технологічний аудит ідеї проекту

Основною ідеєю є впровадження пасивної надвисокочастотної (НВЧ) системи радіочастотної ідентифікації. Ця технологія регулюється стандартом ISO 18000-6-с і працює у діапазоні 860-960 МГц. Система передбачає те, що усі книжки обладнані RFID-транспондером у вигляді етикетки.

Транспондер містить інформацію про книжку, а також її точне місцезнаходження на складі. Усі користувачі бібліотеки мають свої картки-транспондери класу Mifare 13.56 МГц, у якості читацьких квитків. Тому, якщо книжку забрав користувач, то у базі відображається номер-ідентифікатор користувача, у якого зараз перебуває книга, а також кількість днів через яку, книга має повернутись до бібліотеки.

Усі читачі зареєстровані у системі, вони мають доступ до загальнодоступної частини, і також мають інформацію про те, які книжки у них на руках, і коли їх потрібно повернути. На сайті доступні нагадування про завершення строку тримання книжки, для того, щоб користувач вчасно повертав книгу.

Що стосується процесу отримання книжки користувачем, то він може починатись онлайн або офлайн. У разі передзамовлення на сайті, читач може прийти до бібліотеки, самостійно сканувати свій квиток і отримати замовлену літературу.

Коли бібліотека отримує онлайн чи офлайн запит, працівники отримують витяг з бази даних про те, які книжки потрібно зібрати і де вони знаходяться. Після збору замовлення бібліотекар може однією дією сканувати усі книжки за допомогою мобільного RFID-зчитувача і зв'язати ці книжки з номером-ідентифікатором картки користувача. Процес інвентаризації також займає набагато менше часу. Оскільки, для цього необхідно лише пройти з мобільним зчитувачем серед книжкових рядів.

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Спочатку проведемо аналіз за допомогою моделі 5-ти сил Портера (рис. 4.2).



Рисунок 4.2 – Модель 5-ти сил Портера

Далі проведемо SWOT аналіз сильних/слабких сторін та можливостей/загроз (табл. 4.1).

У результаті аналізу було визначено ризики та наслідки впровадження створеного стартапу. Отже, для створення великої клієнтської бази необхідна вдала піар-стратегія та індивідуальний підхід до клієнта. У боротьбі з конкурентами необхідно вказувати на надійність обладнання та можливість постійної технічної підтримки.

Таблиця 4.1 – SWOT-аналіз сильних/слабких сторін та можливостей/загроз

	Можливості	Загрози
	1) Нарощування клієнтської бази, за рахунок презентацій у бібліотеках, на наукових та технічних виставках. 2) Мала кількість конкурентів. 3) Постійна технічна підтримка 4) Можливість впровадити рішення у декількох бібліотеках одразу.	1) Цінова конкуренція. 2) Ріст кількості конкурентів. 3) Невдала піар-стратегія.
Сильні сторони 1) Висока якість обладнання. 2) Налаштування рішення під потреби конкретного клієнта. 3) Можливість інтеграції в існуючі системи.	Сильні сторони – Можливості	Сильні сторони – Загрози
	1с-2м Висока якість обладнання створює переваги перед іншими конкурентами. 1с -3м Висока якість обладнання зменшує необхідність постійної технічної підтримки. 2с-1м Презентація можливостей змін рішення під потреби клієнтів під час пошуку компаніями рішення автоматизації. 2с-4м Налаштування рішення під потреби кожного клієнта дозволить одночасно впроваджувати рішення на різних об'єктах. 3с – 1м Можливість інтеграції в існуючі системи сприяє для впровадження на об'єктах з застарілими рішеннями.	1с – 1з Висока якість обладнання є поясненням цінової політики. 2с-2з Клієнти будуть обирати унікальне рішення, яке може розробити компанія. 3с -2з Можливість інтеграції в існуючі системи збільшить переваги перед іншими клієнтами.
Слабкі сторони 1) Високі ціни. 2) Мала клієнтська база. 3) Малий стартовий бюджет.	Слабкі сторони – Можливості	Слабкі сторони – Загрози
	1сл-2м Через малу кількість конкурентів до цінової політики буде менше запитань. 1сл -3м Рішення включає постійну технічну підтримку, тому має високу ціну. 2сл -1м Програми лояльності та реклама у соцмережах і школах збільшать клієнтську базу. 2сл - 3м Оскільки мала кількість конкурентів, то клієнтської бази перший час буде достатньо. 3сл – 4м Впровадження рішення у декількох об'єктах вже окупить стартовий бюджет.	1сл – 1з Через високі ціни, клієнт може обрати більш дешевий продукт. 1сл – 2з Конкуренти можуть поставити низькі ціни за рахунок менш якісного обладнання. 2сл – 3з Мала клієнтська база може бути наслідком невдалої піар-стратегії. 3сл – 3з Малий стартовий бюджет не дозволить дороговартісну піар-стратегію.

У результаті аналізу було визначено ризики та наслідки впровадження створеного стартапу. Отже, для створення великої клієнтської бази необхідна вдала піар-стратегія та індивідуальний підхід до клієнта. У боротьбі з конкурентами необхідно вказувати на надійність обладнання та можливість постійної технічної підтримки.

4.4 Розроблення ринкової стратегії проекту

Розглянемо ринкову стратегію проекту з точки зору розгорнутої матриці можливостей (рис. 4.3) та загроз компанії (рис. 4.4).

Ймовірність використання можливостей	Вплив можливостей на компанію		
	Сильний	Середній	Незначний
Висока		Нарощування клієнтської бази, за рахунок презентацій у бібліотеках, на наукових та технічних виставках	Постійна технічна підтримка
Середня	Мала кількість конкурентів		
Низька		Можливість впровадити рішення у декількох бібліотеках одразу	

Рисунок 4.3 – Розгорнута матриця можливостей компанії

Ймовірність реалізації загроз	Вплив загроз на компанію			
	Руйнування	Крипичний стан	Важкий стан	«Легкі пошкодження»
Висока				Цінова конкуренція
Середня			Ріст кількості конкурентів Невдала піар-стратегія	
Низька				

Рисунок 4.4 – Розгорнута матриця можливостей компанії

За результатами аналізу можливостей та загроз компанії можна зробити висновок, що запуск стартапу залежить від вдалого впровадження на перших об'єктах і гарних відгуків користувачів. Мала кількість конкурентів дозволить зайняти гарне місце на ринку і цінова політика буде обґрунтована.

4.5 Розроблення маркетингової програми стартап-проекту

Першим кроком для запуску стартапу буде знаходження перших клієнтів шляхом презентацій у бібліотеках, наукових та технічних виставках. Оскільки, на ринку існує декілька конкурентів, то лояльність споживачів буде формуватися у першу чергу гарними відгуками перших клієнтів. Великий вплив у розвиток лояльності до стартапу буде відігравати фідбек від користувачів, на сайті.

Наступним кроком буде розвиток сайту та створення сторінок у соцмережах. Далі буде залучатись таргетована реклама послуг у соцмережах. Одним з головних факторів конкурентоспроможності стартапу є використання якісних компонентів. Тому необхідно просувати цей фактор у рекламі.

4.6 Фінансово-економічний аналіз

Для реалізації впровадження пасивної надвисокочастотної (НВЧ) системи радіочастотної ідентифікації було обране надійне обладнання. Перелік необхідних матеріалів і розрахунок вартості впровадження системи на табл. 4.2.

Розраховано орієнтовну суму матеріальної частини проекту, що складає 258 424 грн.

Таблиця 4.2 – Перелік необхідних матеріалів і розрахунок вартості

Назва обладнання	Кількість	Ціна за одиницю (грн.)	Загальна вартість (грн.)
Мобільний зчитувач MC3330xR	4	31999	127996
Настільний RFID зчитувач Mifare 13.56МГц	8	1602	12816
RFID-принтер ZT610	1	65499	65499
Видаткові матеріали для друку міток	1	15063	15063
Смарт-карта FUDAN 1K (ЧІП FM11RF08, ISO14443A)	1000	7,05	7050
Ліцензійне програмне забезпечення	1	30000	30000
Сумарна вартість (грн.)	258 424		

Витрати на реалізацію стартапу:

- заробітна плата для співробітників (на першому етапі 4 інженери, 3 програмісти, 1 адміністратор, 1 юрист) – 270 тис. грн. на місяць.

- оренда приміщення – 30 тис. грн. на місяць.

Отже, витрати за перший місяць – 300 тис. грн.

Обладнання для реалізації одного типового рішення – 258,424 тис. грн. Націнка за впровадження рішення та технічну підтримку становить 50 тис. грн. Щоб забезпечити окупність початкових інвестицій потрібно мати, як мінімум 6 клієнтів. У разі постійної співпраці з виробниками апаратних компонентів можна зменшити ціну комплектуючих.

Висновки до розділу

Сутність стартапу полягає в автоматизації роботи бібліотеки. Впровадження пасивної надвисокочастотної (НВЧ) системи радіочастотної ідентифікації. Ця

технологія регулюється стандартом ISO 18000-6-с і працює у діапазоні 860-960 МГц.

У результаті аналізу було визначено ризики та наслідки впровадження створеного стартапу. Для створення великої клієнтської бази необхідна вдала піар-стратегія та індивідуальний підхід до клієнта. У боротьбі з конкурентами необхідно вказувати на надійність обладнання та можливість постійної технічної підтримки. За результатами аналізу можливостей та загроз компанії можна зробити висновок, що запуск стартапу залежить від вдалого впровадження на перших об'єктах і гарних відгуків користувачів. Мала кількість конкурентів дозволить зайняти гарне місце на ринку і цінова політика буде обґрунтована

Для реалізації впровадження пасивної надвисокочастотної (НВЧ) системи радіочастотної ідентифікації було обране надійне обладнання. Перелік необхідних матеріалів і розрахунок вартості впровадження системи на табл. 4.2. Розраховано орієнтовну суму матеріальної частини проекту, що складає 258 424 грн.

Обладнання для реалізації одного типового рішення – 258,424 тис. грн. Націнка за впровадження рішення та технічну підтримку становить 50 тис. грн. Щоб забезпечити окупність початкових інвестицій потрібно мати, як мінімум 6 клієнтів. У разі постійної співпраці з виробниками апаратних компонентів можна зменшити ціну комплектуючих.

ВИСНОВКИ

Технологія радіочастотної ідентифікації набула широкого поширення в автоматизації таких виробничих процесів як моніторинг виробничих процесів, системи контролю доступу до приміщення (СКУД), охорона праці, забезпечення ланцюжка поставок.

Об'єктом автоматизації обрано склад споживчих товарів. Для автоматизації роботи складу розроблено пасивну надвисокочастотну (НВЧ) систему радіочастотної ідентифікації. Ця технологія регулюється стандартом ISO 18000-6-с і працює у діапазоні 860-960 МГц.

Систему умовно можна розділити на три частини. Перша частина – це система управління складом або ж (WMS – Warehouse Management System). Друга частина – це система контролю доступу до приміщення (СКУД). Третя частина пов'язана з охороною праці і спрямована на безпеку працівників під час роботи з автомобільною технікою (візками тощо).

Для спроектованої системи контролю та управління складом було підібрано якісні компоненти, сумарна вартість яких 1 172 791 грн. Було обґрунтовано доцільність використання патч-антен у результаті розрахунку та моделювання антени за допомогою програмного забезпечення Comsol Multiphysics.

Спроектowana система відповідає вимогам безпеки та конфіденційності, а також може бути інтегрована в існуючу мережеву інфраструктуру

Сутність стартапу полягає в автоматизації роботи бібліотеки. Впровадження пасивної надвисокочастотної (НВЧ) системи радіочастотної ідентифікації. Ця технологія регулюється стандартом ISO 18000-6-с і працює у діапазоні 860-960 МГц.

Обладнання для реалізації одного типового рішення – 258,424 тис. грн. Націнка за впровадження рішення та технічну підтримку становить 50 тис. грн. Щоб забезпечити окупність початкових інвестицій потрібно мати, як мінімум 6 клієнтів. У разі постійної співпраці з виробниками апаратних компонентів можна зменшити ціну комплектуючих.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. RFID Applied / J.Banks, M. Pachano, L. Thompson, D. Hanny. – Hoboken, New Jersey: John Wiley & Sons, Inc., 2007. – 509 p.
2. Rida A. RFID-Enabled Sensor Design and Applications / A. Rida, L. Yang, M. Tentzeris. – Norwood: ARTECH HOUSE, 2010. – 209 p.
3. Want R. RFID Explained: A Primer on Radio Frequency Identification Technologies / Roy Want., 2006. – 83 p.
4. Kitsos P. RFID Security Techniques, Protocols and System-on-Chip Design / P. Kitsos, Y. Zhang. – New York: Springer Science+Business Media, 2008. – 443 p.
5. Байдюк А. В. Технологія радіочастотної ідентифікації для автоматизації процесів промисловості: Бакалаврська робота/ УДК 621.396.9:0 / Байдюк Анастасія Владиславівна – Київ, 2020. – 73 с.
6. RFID Software [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: <https://softwareconnect.com/rfid/> (дата звернення: 1.10.2021).
7. Chen Z. Antennas for portable devices / Zhi Ning Chen. – Chichester: John Wiley & Sons Ltd, 2007. – 290 p.
8. Günther O. RFID in Manufacturing / O. Günther, W. Kletti, U. Kubach. – Berlin: Springer, 2008. – 163 p.
9. Swedberg C. CribMaster Updates Its RFID Units' Real-Time Tool Management [Електронний ресурс] / Claire Swedberg. – 2020. – Режим доступу до ресурсу: <https://www.rfidjournal.com/cribmaster-updates-its-rfid-units-real-time-tool-management> (дата звернення: 7.10.2021).
10. Finkenzeller K. RFID Handbook fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication, third edition. – Munich: John Wiley & Sons Ltd, 2003. – 462 p.
11. Расчет патч антенны [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: <https://3g-aerial.biz/onlajn-raschety/raschety-antenn/raschet-patch-antennyy> (дата звернення: 1.12.2021).

12. Radio Frequency Identification Technologies (RFID): A Workshop Summary of Committee on Radio Frequency Identification Technologies/ The National Academy of Engineering Washington: The National Academies Press, 2004. – 52 p.

ДОДАТОК А
ABSTRACT

ABSTRACT

Radio frequency identification is a wireless technology for data collection. The simplest RFID system consists of an identifier tag that is attached to an object and a reader that can poll the tag to identify the tag and retrieve the information written on the tag.

The label performs the function of a programmable device for data transmission and consists of a communication element (resonant tuned circuit) and a low-power CMOS chip. The reader emits a radio frequency signal, and exchanges data when the tag approaches the reader signal. System software is a tool for integrating hardware components into a single computer system with its own functions and databases.

For the security and confidentiality of RFID systems, it is important to follow the general security rules:

- protection of confidentiality;
- protection against tracking;
- identification efficiency;
- protection against tag forgery or cloning.

The following limiting factors should be considered when choosing RFID technology for industrial use:

- temperature and humidity of the environment;
- the presence of a large number of metal objects in the environment;
- complex forms of products;
- the presence of water and other liquids.

The technology of radio frequency identification has become widespread in the automation of such production processes as monitoring of production processes, access control systems (ACS), labor protection, supply chain.

In supply chains, warehousing plays an important role in the storage of finished products. All physical items are stored in warehouses at least once before sale. Storage, handling and transportation of goods involve many manual processes that affect the cost

and ability to provide services. Therefore, it is advisable to automate these processes to avoid errors.

The object of automation is the composition of consumer goods. A passive ultra-high frequency (UHF) radio frequency identification system has been developed to automate the operation of the warehouse. This technology is regulated by the ISO 18000-6-c standard and operates in the 860-960 MHz band.

The system can be divided into three parts. The first part is a warehouse management system or (WMS - Warehouse Management System). The second part is the premises access control system (ACS). The third part is related to labor protection and is aimed at the safety of workers when working with vehicles (trolleys, etc.).

The warehouse management system takes into account each point of movement of goods and orders for the warehouse. The components are portal readers at the entrance and exit gates, RFID printer for unlabeled goods (from third parties), mobile readers for operators and packers, as well as database software that combines all these elements.

The premises access control system (ACS) used to access the premises and individual storage areas. Each employee has a tag in the form of a plastic card. At the main entrance is a turnstile with a built-in reader. As for access to certain areas, there are doors with readers. When reading the correct card (the database contains information about this ID and allowed access zones), the current is not electromagnetic lock and the door can be opened.

The safety of workers when working with automotive equipment will be implemented through an alarm system when approaching the vehicle based on radio frequency identification technology. In poor visibility, standard personal protective equipment and even cameras are ineffective when it comes to preventing collisions between pedestrians and vehicles. The RFID system provides all employees with an additional level of control and protection. After all, the reader identifies the tags and because of the turns, and the system is not affected by environmental conditions such as dust and smoke, and poor lighting.

To implement the system of control and management of the warehouse, high-quality components were selected, the total cost of which is 1 172 791 UAH.

The warehouse management system starts with the portal gate, which is built using the UHF reader ID ISC.LRU and 4 UHF antennas Advantenna-p33. The expediency of using patch antennas as a result of calculation and modeling of the antenna using Comsol Multiphysics software was substantiated.

All boxes in the warehouse are equipped with RFID-labels ZBR2000. In the case of supply of goods from third parties requires human intervention. Because, you need to put an RFID tag on each box. To do this, a RFID ZT610 printer for labels connected to the WMS system will be provided in the shipment area.

Database workers use Zebra MotionWorks Enterprise software to remotely tag information about where the product should be stored. Operators, using the mobile reader MC3330xR, deliver and collect them on the necessary racks.

As for the access control system, each employee will have a contactless EM-MARINE 0.8 MM card. Near the main entrance there will be a tripod turnstile EXPERT with a built-in reader. When reading the correct card, the employee will be able to go further.

Other storage rooms can be accessed through a door with an HIKVISION DS-K1802E RFID reader and a CoVi Security CS-280G electromagnetic lock. When reading the correct card (the database contains information about this ID and allowed access zones), the current is not electromagnetic lock and the door can be opened. Readers are connected to the ZKTeco C5S120 network controller and the entire ACS system uses ZKTeco Access 3.5 software.

The safety of workers when working with automotive equipment is implemented through an alarm system when approaching the vehicle. All employees in the second storage area will have a SafeTag bracelet. KINEXON SafeZone software is used to work with these transponders. The vehicle, in turn, will be equipped with a Zebra UWB Wand RFID reader. When the worker and the vehicle get closer than the specified distance, the bracelet falls into the area of the reader and begins to signal the pedestrian. As for drivers, they must also wear bracelets in the storage area. Therefore, it is possible to turn off the alarm with a button for direct control of the vehicle.

The TP-LINK TL-SG1024D (TL-SG1024D) connects the main components to the servers. A specific power supply transformer lowering OSM 1-0,1 220/220/12 UPP UTOS and transformer lowering Hager ST315, 230V / 24V.

The essence of the startup is to automate the work of the library. Introduction of passive ultra-high frequency (UHF) radio frequency identification system. This technology is regulated by the ISO 18000-6-c standard and operates in the 860-960 MHz band.

The analysis identified the risks and consequences of implementing a startup. To create a large client base requires a successful PR strategy and individual approach to the client. In the fight against competitors, it is necessary to point out the reliability of equipment and the possibility of constant technical support. Based on the analysis of the company's opportunities and threats, it can be concluded that the launch of the startup depends on the successful implementation of the first objects and good user feedback. A small number of competitors will allow you to take a good place in the market and the pricing policy will be justified

Reliable equipment was selected for the implementation of passive ultra-high frequency (UHF) radio frequency identification system. The list of required materials and calculation of the cost of implementing the system in table. 4.2. The estimated amount of the material part of the project, which is UAH 258,424, has been calculated.

Equipment for the implementation of one standard solution - 258,424 thousand UAH. Margin for the implementation of the solution and technical support is 50 thousand UAH. To ensure a return on initial investment you need to have at least 6 clients. In the case of constant cooperation with manufacturers of hardware components, you can reduce the price of components.

Додаток Б
ТЕХНІЧНЕ ЗАВДАННЯ
на магістерську дисертацію
"Система контролю промислового підприємства на основі технології
радіочастотної ідентифікації"

1 Назва роботи

Система контролю промислового підприємства на основі технології радіочастотної ідентифікації

2 Підстави для виконання

Робота проводиться на підставі завдання на магістерську дисертацію відповідно до наказу № 3666-с від 06.11.2021 р.

3 Мета та актуальність роботи

Метою роботи є створення системи контролю виробничих процесів на основі технології радіочастотної ідентифікації

Актуальність роботи: автоматизація – це один із головних напрямів розвитку виробництва, оскільки цей процес збільшує точність та швидкість роботи з обладнанням та виключає людський фактор. Технологія радіочастотної ідентифікації може забезпечити автоматизацію багатьох виробничих процесів, зокрема моніторинг, інвентаризація, контроль доступу до приміщень, охорона праці та забезпечення ланцюжка поставок.

4 Основні технічні вимоги до виконання роботи

Особливість використання технології RFID у промисловості зумовлюють декілька факторів: робота в широкому діапазоні температур та вологості, наявність в оточуючому середовищі великої кількості металевих предметів, складні форми виробів, що підлягають ідентифікації.

При виборі технології RFID для реалізації у промисловості потрібно враховувати такі обмежуючі фактори:

- температура та вологість середовища;

- наявність в оточуючому середовищі великої кількості металевих предметів;
- складні форми виробів;
- наявність води та інших рідин.

5 Вимоги до технологічності

Система RFID буде встановлена у вже існуючій інфраструктурі, яка містить інші системи та пристрої. Тому потрібно визначити, як ця система RFID впишеться в існуючу інфраструктуру об'єкта. З цієї причини перед фіналізацією проекту системи RFID і перед установкою системи RFID потрібно провести аналіз об'єкту. Саме для цього необхідно проаналізувати фізичну інфраструктуру об'єкту та радіочастотне середовище, щоб знайти відповідні місця для зон зчитування або позначити заплановані зони зчитування.

6 Вимоги до рівня уніфікації

В конструкції необхідно намагатись максимально використовувати стандартні компоненти та уніфіковані вироби, а також запозичені складальні одиниці та деталі.

7 Вимоги до безпеки

По відношенню до безпеки пристрій, що працює повинен відповідати вимогам ДСТУ 4113-2001 і забезпечувати електробезпеку, пожежну безпеку, механічну надійність та інші вимоги при монтажі, експлуатації, обслуговуванні і ремонті.

8 Економічні показники

Розроблювальний пристрій повинен бути ефективним по відношенню до його виробництва з економічної точки зору. Схемні рішення повинні мати мінімальну вартість реалізації.

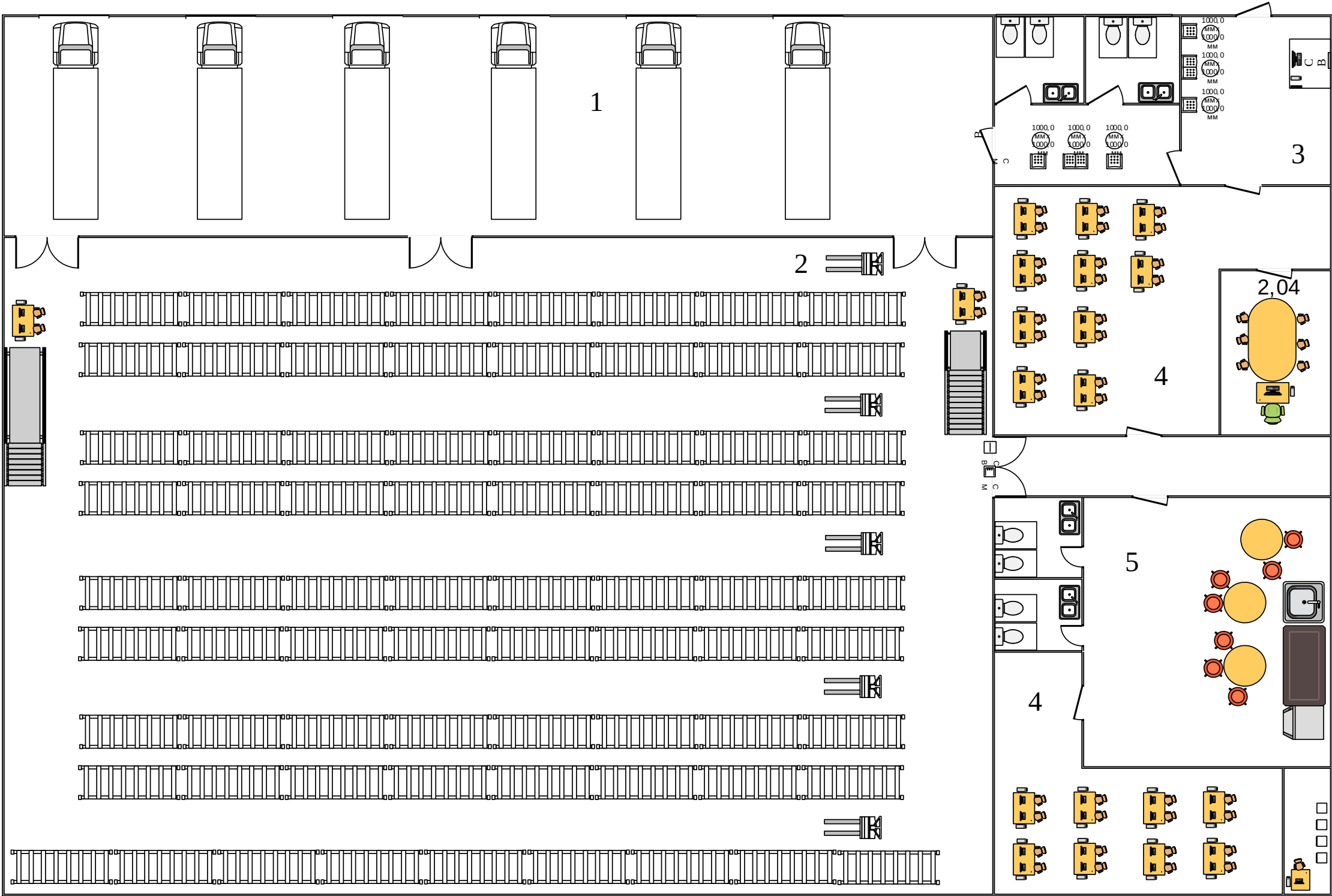
9 Стадії та етапи розробки

1. Аналіз компонентів RFID-систем
2. Розробка плану об'єкту контролю та автоматизації
3. Створення концепту системи радіочастотної ідентифікації
4. Розробка структурної схеми системи радіочастотної ідентифікації
5. Вибір пристроїв для реалізації системи.

10 Порядок приймання роботи

Робота приймається Державною екзаменаційною комісією.

Додаток В
План об'єкту



Зм.	Лист	№ докум.	Підпис	Дата	План об'єкту			Літера		Маса	Масштаб
Розроб.	Байдок А.В.										
Перевірів	Макаренко В.В.										
Т. контр.											
								Аркуш 1		Аркушів 1	
Н. контр.	Дрозденко К.С.										
Затверд.	Макаренко В.В.										
					НТУУ "КПІ" ім. Ігоря Сікорського, ФЕЛ, ДВ-01-мп						

Додаток Г
Функціональна схема
системи контролю та
управління доступом

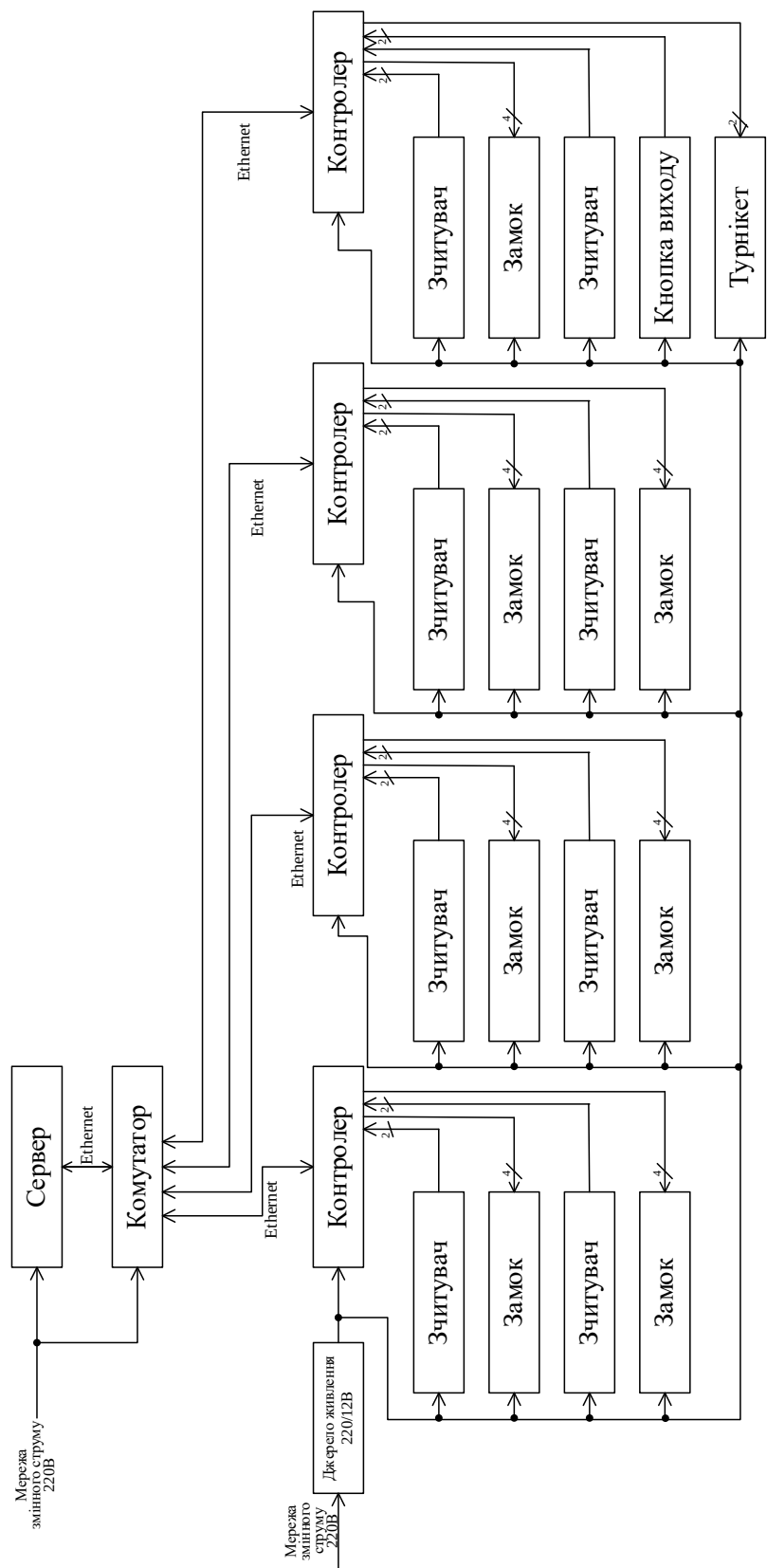
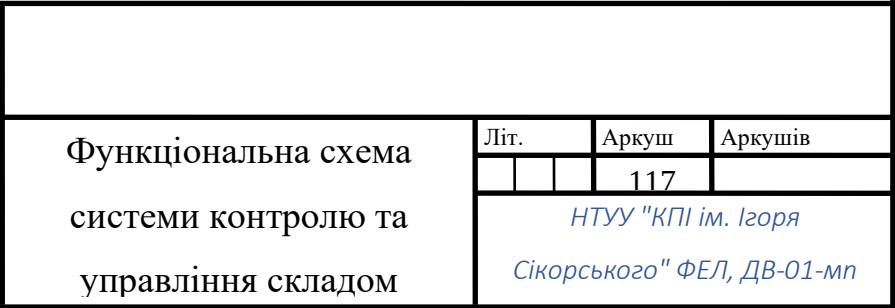


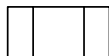
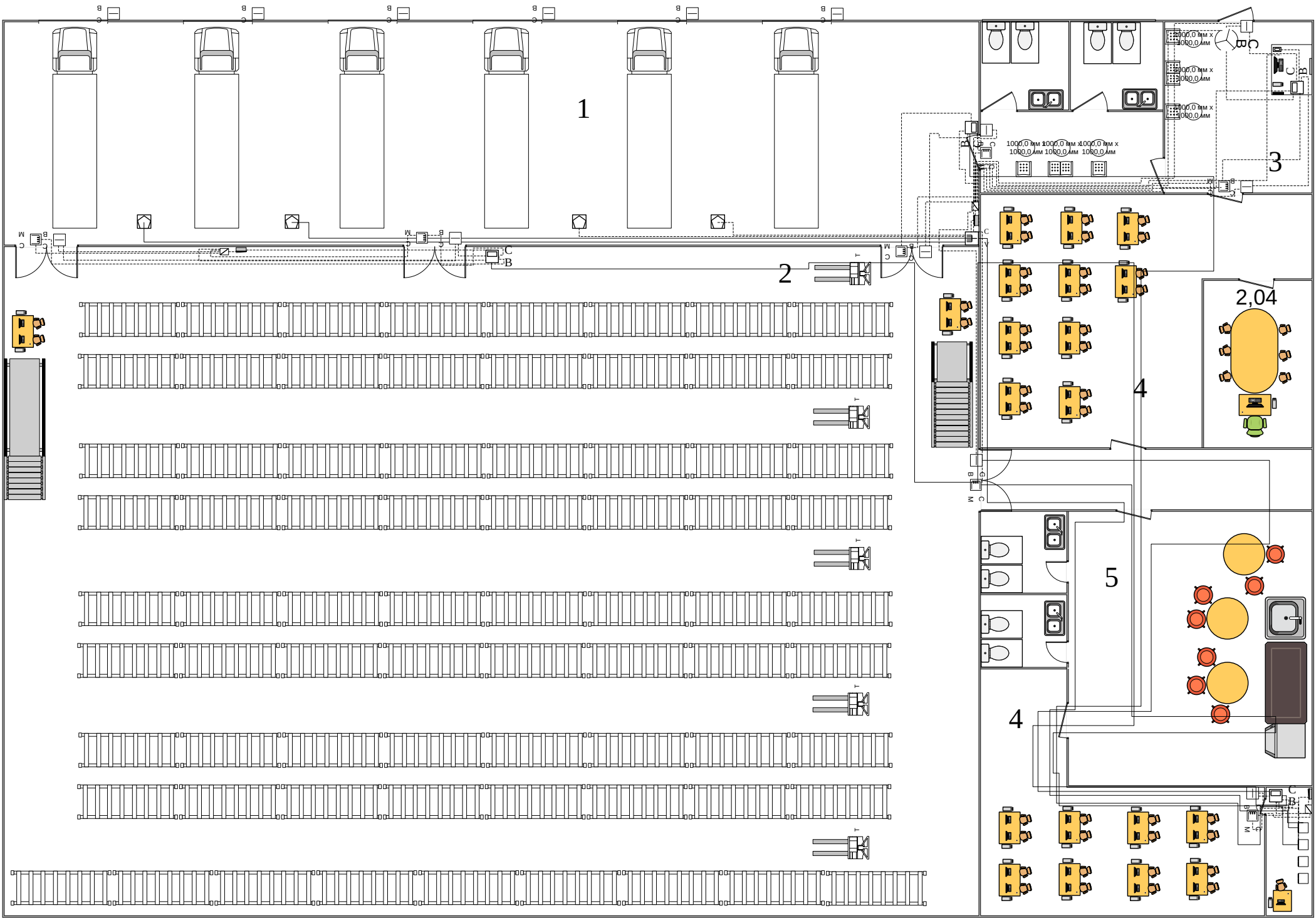
Рисунок 2.3 – Структурна схема системи контролю та управління доступом

Змін.	Арк.	№ докум.	Підпис	Дата					
Розроб.		Байдюк А.В.			Функціональна схема системи контролю та управління доступом	Літ.	Аркуш	Аркушів	
Перев.		Макаренко В.В.						115	
Реценз.						НТУУ "КПІ ім. Ігоря Сікорського" ФЕЛ, ДВ-01-мп			
Н. Контр.		Дрозденко К.С.							
Затв.		Макаренко В.В.							

Додаток Д
Функціональна схема
системи управління
складом



Додаток Е
Розміщення
обладнання на плані
об'єкту



--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--