Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за першим (бакалаврським) рівнем вищої освіти
на тему:

Програмне забезпечення системи контролю промислового підприємства на основі технології радіочастотної ідентифікації з використанням плати мікроконтролера Arduino Uno R3

КбПЗ_2026

Виконав здобувач вищої освіти
IV курсу, групи КІ-22-2
ОПП «Комп’ютерна інженерія»
спеціальності 123 «Комп’ютерна інженерія»
_____Федорчук С.І.
«____» _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____Кислун О.А
«____» _____ 2026 р.
Рецензент _____

м. Кропивницький

Центральноукраїнський національний технічний університет

Факультет *Механіко-технологічний*
Кафедра *Кібербезпеки та програмного забезпечення*
Рівень вищої освіти *бакалавр*
Галузь знань ._12 _____*“*Інформаційні технології*”*_____
Спеціальність *123 “*Комп’ютерна інженерія*”*
Освітньо-професійна (освітньо-наукова) програма _*“*Комп’ютерна інженерія*”*_

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., проф.
_____ Олексій СМІРНОВ
“____”_____2026_року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ПЕРШИМ (БАКАЛАВРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Федорчук Софії Ігорівні
(прізвище, ім’я, по батькові)

1. Тема роботи *Програмне забезпечення системи контролю промислового підприємства на основі технології радіочастотної ідентифікації з використанням плати мікроконтролера Arduino Uno R3*
2. Керівник роботи *Кислун Олег Андрійович, канд. техн. наук, доцент*
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від “27” лютого 2026року №136-02
3. Строк подання роботи до захисту *10.06.2026 р.*
4. Мета та завдання випускної кваліфікаційної роботи. *Метою роботи є розробка програмного забезпечення системи управління мікрокліматом приміщень*
5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Призначення та область використання.
2.Перегляд аналогічних існуючих систем.
3. Опис і обґрунтування проектних рішень.
4. Етапи програмування системи.
5. Впровадження системи в промислову експлуатацію
6. Висновки.
6. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

Структурна схема системи	*1 аркуш*
Функціональна схема системи	*1 аркуш*
Діаграма процесів	*1 аркуш*
Блок-схема алгоритму роботи системи керування	*1 аркуш*
Блок-схема алгоритму системи моніторингу	*2 аркуші*

КОПІЯ 2026

7. Дата видачі завдання «27» лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем керування	10.03.2026	
2.	Постановка задачі, оформлення ТЗ	15.03.2026	
3.	Розробка моделі компонента	20.03.2026	
4.	Розробка структур даних	25.03.2026	
5.	Розробка алгоритмів зв’язку та відображення	30.03.2026	
6.	Програмування алгоритмів	10.04.2026	
7.	Оформлення ПЗ	17.05.2026	
8.	Попередній захист роботи	23.05.2026	

КбПЗ_2026

Дата видачі завдання
«__»_____2026р.

Підпис керівника

_____ _____
(прізвище та ініціали)

Завдання прийнято до виконання
«__»_____2026р.

Підпис здобувача

_____ _____
(прізвище та ініціали)

АНОТАЦІЯ

Федорчук С.І. Програмне забезпечення системи контролю промислового підприємства на основі технології радіочастотної ідентифікації з використанням плати мікроконтролера Arduino Uno R3. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

У випускній кваліфікаційній бакалаврській роботі розглянуто розроблення програмного забезпечення системи контролю промислового підприємства із застосуванням технології радіочастотної ідентифікації (RFID) та мікроконтролерної платформи Arduino Uno R3. Актуальність теми обумовлена необхідністю автоматизації процесів контролю доступу, обліку персоналу та моніторингу виробничих процесів на сучасних підприємствах.

У роботі проведено аналіз сучасних RFID-систем, досліджено принципи їх функціонування та визначено основні вимоги до побудови автоматизованої системи контролю. Обґрунтовано вибір апаратної платформи Arduino Uno R3 та засобів програмної реалізації системи.

Розроблено програмне забезпечення, яке забезпечує взаємодію з RFID-зчитувачем, обробку та передачу ідентифікаційних даних, а також збереження інформації у базі даних. Реалізовано функції контролю доступу, реєстрації подій, ведення журналу відвідувань та формування звітної інформації для подальшого аналізу діяльності підприємства.

У роботі також передбачено можливість розширення функціональних можливостей системи та інтеграції з іншими засобами автоматизації. Розроблена система характеризується доступністю, гнучкістю та простотою впровадження у виробниче середовище.

Ключові слова: RFID, Arduino Uno R3, система контролю, автоматизація, мікроконтролер, ідентифікація, програмне забезпечення, промислове підприємство.

КОПЗ–2026

ABSTRACT

Fedorchuk S. Software for industrial enterprise control based on radio frequency identification technology using the Arduino Uno R3 microcontroller board. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

The final qualifying bachelor's thesis considers the development of software for an industrial enterprise control system using radio frequency identification (RFID) technology and the Arduino Uno R3 microcontroller platform. The relevance of the topic is due to the need to automate access control processes, personnel accounting, and monitoring of production processes at modern enterprises.

The paper analyzes modern RFID systems, investigates the principles of their functioning, and identifies the main requirements for building an automated control system. The choice of the Arduino Uno R3 hardware platform and software implementation tools for the system is justified.

Software has been developed that provides interaction with an RFID reader, processing and transmission of identification data, and storing information in a database. The functions of access control, event registration, attendance log, and generation of reporting information for further analysis of the enterprise's activities have been implemented.

The paper also provides for the possibility of expanding the functionality of the system and integrating it with other automation tools. The developed system is characterized by accessibility, flexibility, and ease of implementation in the production environment.

Keywords: RFID, Arduino Uno R3, control system, automation, microcontroller, identification, software, industrial enterprise.

КОПЗ-2026

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ 2
ВСТУП..... 3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ 3
1.1 Призначення системи..... 5
1.2 Область застосування..... 12
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ 13
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським рівнем вищої освіти) 13
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування..... 35
2.3 Розгорнута постановка завдання 37
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ 38
3.1 Опис функціонування системи 38
3.2 Розробка структурної схеми..... 39
3.3 Розробка функціональної схеми 40
3.4 Розробка діаграми процесів..... 45
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ..... 46
4.1 Розробка блок-схем та опис алгоритмів функціонування системи..... 46
4.2 Захист розробленого програмного забезпечення..... 67
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ..... 71
6 ОСНОВНІ ВИСНОВКИ..... 77
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 79

КПЗ – 2026

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

АЦП – аналогово-цифровий перетворювач;

ВЧ – високочастотний;

ІС – інтегральна схема;

НВЧ – надвисокочастотний;

ПВХ – Полівінілхлорид;

ПЗ – програмне забезпечення;

РЧ – радіочастотний;

СКУД – системи контролю та управління доступом;

AM – 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 (дискова операційна система);

EEPROM – Electrically Erasable Programmable Read-Only Memory (Електрично видаляєма 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).

КПІ–2026

ВСТУП

Технології автоматизованого збору даних та ідентифікації набувають дедалі більшого значення у процесах управління ланцюгами постачання, виробничими потоками, відстеженням мобільних активів, контролем складських запасів і логістичними операціями, а також у будь-яких системах, де необхідно визначати точне місцезнаходження об’єктів у режимі реального часу.

Радіочастотна ідентифікація (RFID) є бездротовою технологією ідентифікації об’єктів, що широко застосовується для побудови автоматизованих систем у різних галузях діяльності. Принцип її роботи базується на використанні електромагнітних хвиль для передавання та приймання інформації, яка зберігається у транспондері, між міткою та зчитувальним пристроєм. Порівняно з традиційними методами ідентифікації RFID має низку переваг, серед яких більша дистанція зчитування, висока швидкість обміну даними, відсутність необхідності прямої видимості між зчитувачем і міткою, а також можливість одночасного зчитування великої кількості тегів.

Технологія RFID найбільш повно відповідає вимогам сучасних комп’ютеризованих систем управління, у яких необхідне оперативне розпізнавання об’єктів та реєстрація прав доступу користувачів у реальному масштабі часу. Саме тому система автоматизації складських процесів була розроблена на основі даної технології. Запропонована система передбачає моніторинг об’єктів на складі, реалізацію контролю та керування доступом, а також забезпечення безпеки під час роботи з транспортними засобами.

Технологія RFID широко застосовується у промисловості, логістиці, складському обліку, транспортних системах, медицині та системах контролю доступу. На виробничих підприємствах RFID використовується для ідентифікації продукції, відстеження переміщення матеріалів, контролю роботи персоналу та автоматизації виробничих процесів. У складських комплексах технологія

КПЗ_2026

дозволяє здійснювати автоматичний облік товарів, зменшувати помилки при інвентаризації та підвищувати швидкість обробки вантажів.

У системах моніторингу та управління RFID може застосовуватись для ідентифікації операторів, обладнання або окремих виробничих вузлів. Інтеграція RFID із мікроконтролерними платформами, такими як ESP32, дозволяє створювати інтелектуальні системи контролю доступу, обліку робочого часу та автоматичного запуску технологічних процесів після ідентифікації користувача.

Таким чином, RFID-технологія є ефективним інструментом автоматичної ідентифікації, що забезпечує підвищення рівня автоматизації, безпеки та ефективності управління виробничими процесами. Її використання дозволяє мінімізувати людський фактор, прискорити обробку інформації та забезпечити надійний контроль об’єктів у реальному часі.

КбПЗ_2026

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Радіочастотна ідентифікація (RFID) - це узагальнена назва технологій, що використовують радіочастотний зв'язок для передавання даних. У найпростішому вигляді RFID-система складається з ідентифікаційної мітки, закріпленої на об'єкті, та зчитувального пристрою, який здійснює опитування мітки з метою її розпізнавання й отримання збереженої на ній інформації (рис. 1.1).

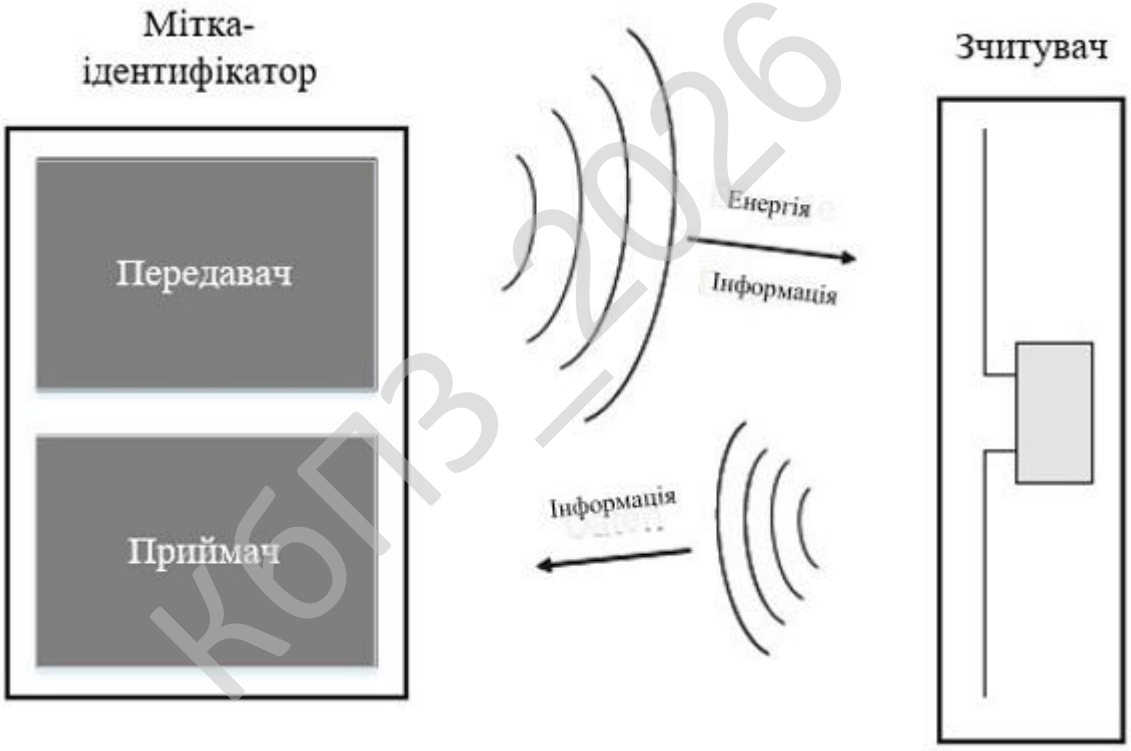


Рисунок 1.1 – Найпростіша RFID-система

Завдяки широким функціональним можливостям технологія RFID активно поширюється у різних сферах застосування - від безконтактних транспортних карток і систем доступу до автоматизації виробничих та логістичних процесів.

RFID-мітка призначена для зберігання інформації, обсяг якої може змінюватися від 32 біт до 32 000 байтів залежно від типу пристрою та сфери його

КОПЗ 2026

застосування. Такі мітки поділяються на пасивні та активні, що відрізняються способом живлення та дальністю зчитування.

RFID-зчитувач виконує роль керуючого пристрою щодо мітки та водночас виступає підлеглим елементом відносно програмного забезпечення або хост-системи. Така взаємодія реалізується за принципом «ведучий–підлеглий» (master–slave), що схематично представлено на рисунку 1.2.

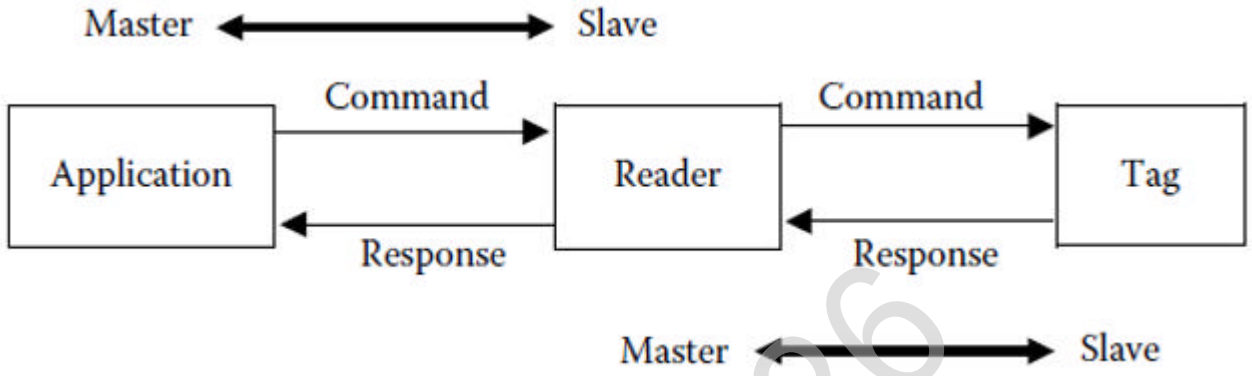


Рисунок 1.2 – Архітектура «ведучий-підлеглий» (master-slave) RFID-системи

Теги розміщуються в межах зони дії зчитувача. Зона зчитування — це фізична область, у якій електромагнітне поле, сформоване зчитувачем, має достатню потужність для живлення міток (у випадку пасивних тегів), приймання переданих ними сигналів та їх коректного декодування. У кожний момент часу зчитувач може коректно опрацювати сигнал лише від одного тегу в межах своєї зони опитування, так само як і тег зазвичай взаємодіє лише з одним зчитувачем.

Найбільш поширеним способом передавання сигналів у радіочастотних системах є амплітудна модуляція. Відповідно до загальноприйнятої моделі радіосигналу (1), на його характеристики впливають амплітуда (A), кутова частота (ω) та фаза (φ). Залежно від того, який із цих параметрів змінюється під час передавання інформації, розрізняють основні види модуляції: амплітудну (AM), частотну (FM) та фазову (PM).

$$ss(tt) = AA(tt) \cdot \cos\left[\omega\omega tt + \varphi\varphi(tt)\right] \qquad (1.1)$$

Амплітудна модуляція є чутливою до втрат у каналі передавання, що може негативно впливати на якість сигналу в умовах змінних характеристик

КОПЗ_2026

середовища. Частотна модуляція, у свою чергу, потребує ширшого частотного діапазону роботи системи, тоді як фазова модуляція обмежується технічними можливостями використовуваного обладнання. Для підвищення ефективності передавання сигналів зазначені методи часто комбінуються, що дозволяє зменшити їхні недоліки та забезпечити більш надійний зв'язок.

Система радіочастотної ідентифікації (RFID) має суттєві переваги порівняно з іншими технологіями ідентифікації, такими як штрихкодові системи, оптичне розпізнавання символів, смарт-картки та біометричні методи (голосова ідентифікація, відбитки пальців, сканування сітківки ока). Основними перевагами RFID є відсутність необхідності прямої видимості між зчитувачем і міткою, можливість роботи у складних фізичних умовах, енергоефективність, стабільність функціонування та здатність одночасно ідентифікувати значну кількість об'єктів.

Разом із перевагами технологія RFID має певні обмеження. Зокрема, у середовищах із великою кількістю металевих конструкцій або за несприятливих умов експлуатації (підвищена температура, вологість тощо) необхідно застосовувати системи з підвищеною завадостійкістю, наприклад низькочастотні RFID-рішення.

Як і будь-які радіочастотні системи, RFID потребує використання протоколів керування доступом до середовища передачі (MAC), що дозволяють уникати колізій сигналів. Колізії призводять до перевитрати мережевих ресурсів і зменшення швидкості зчитування, що особливо критично для RFID-систем через обмежені обчислювальні можливості та обсяг пам'яті тегів.

Стандарти RFID традиційно розробляються Міжнародною організацією зі стандартизації (ISO). Зокрема, стандарти ISO 18000-6A та ISO 18000-6B регламентують роботу систем у надвисокочастотному діапазоні та широко застосовуються у світовій практиці. Кодування даних у RFID-системах охоплює процес обробки інформації від моменту передавання сигналу до мітки й до його повернення зчитувачу.

Для RFID визначено декілька методів кодування даних, вибір яких впливає

КПЗ_2026

на вартість реалізації системи, можливості виправлення помилок та надійність передавання інформації. Основні вимоги до синхронізації та методів кодування регламентуються стандартами ISO 14443, ISO 15693 та ISO 18000-6. До найбільш поширених методів кодування, що застосовуються в індуктивних та ємнісних RFID-системах [1], належать:

1. NRZ (Non-Return-to-Zero) - двійкова «1» подається високим логічним рівнем, а «0» - низьким.

2. Манчестерське кодування - зміна сигналу відбувається в середині тактового інтервалу; «0» відповідає переходу від низького до високого рівня, а «1» - від високого до низького.

3. Кодування Міллера - «1» представлена переходом у середині тактового циклу, тоді як «0» зберігає попередній логічний стан; при послідовності нулів перехід виконується на початку циклу.

4. Модифіковане кодування Міллера - переходи сигналу замінюються короткими негативними імпульсами.

5. FM0 (двофазне кодування) - перехід відбувається на початку кожного тактового циклу; «0» має додатковий перехід у середині циклу, а «1» - ні.

6. Уніполярне кодування - «1» відповідає високому рівню в першій половині тактового інтервалу, «0» - низькому рівню протягом усього циклу.

7. Диференційне кодування - логічна «1» викликає зміну рівня сигналу, тоді як «0» залишає його незмінним.

8. Диференційне двофазне кодування - зміна рівня відбувається у середині тактового циклу; «1» додатково спричиняє зміну на початку циклу.

9. Імпульсно-інтервальне кодування (PIE) - «1» представлена паузою тривалістю 2T перед імпульсом, а «0» - паузою тривалістю T.

Застосування відповідного методу кодування дозволяє забезпечити надійну передачу даних та ефективну роботу RFID-систем у різних умовах експлуатації.

КОПЗ – 2026

1.2 Область застосування

В даній випускні кваліфікаційній бакалаврській роботі буде розроблятись програмне забезпечення системи контролю промислового підприємства на основі технології радіочастотної ідентифікації.

Сучасний розвиток промислових підприємств характеризується активним впровадженням автоматизованих інформаційних систем, спрямованих на підвищення ефективності виробництва, оптимізацію управління ресурсами та забезпечення контролю технологічних процесів. Одним із перспективних напрямів автоматизації є використання технології радіочастотної ідентифікації (RFID), яка дозволяє здійснювати швидку та надійну ідентифікацію об’єктів без фізичного контакту.

Розроблюване програмне забезпечення системи контролю промислового підприємства на основі RFID-технології призначене для автоматизованого збору, обробки та аналізу інформації щодо переміщення матеріальних ресурсів, стану обладнання та доступу персоналу до виробничих зон. Основною областю застосування системи є підприємства різних галузей промисловості, де необхідний постійний контроль виробничих процесів та облік об’єктів у режимі реального часу.

Система може застосовуватись на машинобудівних підприємствах для контролю переміщення деталей між виробничими дільницями, відстеження етапів обробки продукції та автоматичного формування виробничої статистики. Використання RFID-міток дозволяє ідентифікувати кожну одиницю продукції або заготовку, що значно зменшує ймовірність помилок під час виробництва та обліку.

У складських та логістичних підрозділах підприємства система забезпечує автоматичний облік матеріалів, комплектуючих та готової продукції. RFID-технологія дозволяє здійснювати швидке зчитування інформації під час приймання, зберігання або відвантаження товарів без необхідності ручного

КПЗ_2026

введення даних. Це суттєво скорочує час обробки вантажів та підвищує точність інвентаризації.

Важливою сферою застосування системи є контроль доступу персоналу до виробничих зон та технологічного обладнання. Кожен працівник може бути оснащений персональною RFID-карткою або міткою, що дозволяє автоматично ідентифікувати його при вході до приміщення або запуску обладнання. Такий підхід забезпечує підвищення рівня промислової безпеки та дозволяє обмежувати доступ до небезпечних або відповідальних виробничих ділянок.

Система також може використовуватись для контролю робочого часу працівників та аналізу виробничої активності персоналу. Автоматична реєстрація присутності працівників на робочих місцях дозволяє отримувати достовірні дані щодо використання трудових ресурсів підприємства та оптимізувати організацію виробничого процесу.

У сфері технічного обслуговування обладнання RFID-система забезпечує ідентифікацію машин, агрегатів та інструментів. Кожен об’єкт може бути оснащений RFID-міткою, що містить інформацію про технічні характеристики, дату останнього обслуговування або ремонтні роботи. Це дозволяє автоматизувати процес планово-попереджувального ремонту та зменшити ризик виходу обладнання з ладу.

Розроблюване програмне забезпечення може інтегруватися з існуючими автоматизованими системами управління підприємством, такими як ERP, MES або SCADA-системи. Завдяки цьому забезпечується централізоване управління виробничими даними та формування аналітичної інформації для прийняття управлінських рішень.

Особливо актуальним є застосування системи на підприємствах із великою територією або розподіленою структурою виробництва. RFID-технологія дозволяє здійснювати дистанційний контроль об’єктів без необхідності прокладання значної кількості кабельних мереж. Це зменшує витрати на впровадження та підвищує гнучкість системи.

КБПЗ–2026

У харчовій та переробній промисловості система може застосовуватись для відстеження партій продукції на всіх етапах виробництва - від надходження сировини до відвантаження готового продукту. Такий підхід забезпечує простежуваність виробничого процесу та відповідність вимогам контролю якості.

Крім промислових підприємств, система може використовуватись у транспортних вузлах, складських комплексах, енергетичних об’єктах та сервісних центрах, де необхідна автоматизована ідентифікація об’єктів і контроль їх переміщення.

Застосування RFID-технології у поєднанні з сучасним програмним забезпеченням дозволяє реалізувати концепцію цифрового підприємства, у межах якої всі виробничі процеси контролюються автоматично, а інформація доступна в режимі реального часу. Це сприяє підвищенню продуктивності праці, зменшенню втрат ресурсів та покращенню управління виробництвом.

Таким чином, область застосування розроблюваної системи контролю промислового підприємства охоплює широкий спектр задач, пов’язаних з ідентифікацією, обліком, моніторингом та управлінням виробничими процесами.

Використання RFID-технології забезпечує підвищення рівня автоматизації підприємства, зниження впливу людського фактора та створення ефективної системи контролю виробничої діяльності.

КбПЗ–2026

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти

Аналіз компонентів RFID-системи. Апаратні компоненти

RFID-система складається з трьох основних компонентів: зчитувача, ідентифікаційної мітки та програмного забезпечення. Зчитувач включає радіочастотний модуль приймання та передавання сигналів, процесор обробки сигналу, блок керування, антену як елемент зв’язку, а також інтерфейс передавання даних (наприклад, RS232 або RS485) для взаємодії з головною інформаційною системою.

RFID-мітка виконує роль програмованого пристрою для збереження та передавання інформації. Вона складається з елемента зв’язку у вигляді резонансного кола та малопотужної CMOS-мікросхеми. До складу мікросхеми входять аналоговий радіочастотний інтерфейс, конденсатор налаштування антени, випрямляч живлення, модуль цифрового керування, енергонезалежна пам’ять типу EEPROM, а також схеми модуляції даних.

Технологія RFID забезпечує безконтактне зчитування та запис інформації в енергонезалежну пам’ять мітки за допомогою радіосигналу. RFID-мітки можуть мати різні габарити та конструктивне виконання залежно від умов експлуатації та сфери застосування, що представлено на рисунку 2.1.

КПЗ_2026



Рисунок 2.1 – Різні типи RFID-міток

Зчитувач формує радіочастотне електромагнітне поле та здійснює обмін даними з міткою в момент її потрапляння у зону дії сигналу. Залежно від способу живлення RFID-мітки поділяються на такі типи:

– активні мітки - оснащені власним джерелом живлення (акумулятором), яке забезпечує роботу всіх функціональних елементів;

– напівактивні мітки - мають акумулятор, що використовується лише для живлення мікросхеми, тоді як передавання сигналу здійснюється за рахунок енергії зчитувача;

– пасивні мітки - не містять власного джерела живлення, що робить їх дешевшими, компактнішими та більш надійними порівняно з активними аналогами.

Основним елементом RFID-мітки є інтегральна схема - кремнієвий чіп, розміри якого зазвичай не перевищують 1×1 мм (рис. 2.2). Мікросхема функціонує подібно до мікропроцесора та виконує головне завдання - передавання унікального ідентифікаційного коду мітки. Цей ідентифікатор зберігається у внутрішній пам’яті пристрою. Після отримання енергії від антени логічна схема мікросхеми зчитує ідентифікаційний номер і передає його шляхом

КОПІЯ 2026

модуляції сигналу зворотного розсіювання. Залежно від типу мітки вона може містити додаткову пам’ять для запису користувацьких даних за допомогою RFID-зчитувача [2].

RFID-мітки переважно працюють у високочастотному (HF) або надвисокочастотному (UHF) діапазонах. Високочастотні мітки зазвичай мають невелику дальність зчитування, що вимірюється кількома сантиметрами або дюймами. Це робить їх зручними для задач інвентаризації, коли об’єкти розташовані близько один до одного та безпосередньо до зчитувача.

– За типом використовуваної пам’яті RFID-мітки поділяються на:

– RO (Read Only) - пам’ять тільки для зчитування;

– WORM (Write Once Read Many) - одноразовий запис із можливістю багаторазового зчитування;

– RW (Read/Write) - багаторазовий запис і зчитування;

– енергозалежну пам’ять - використовується для виконання обчислювальних операцій після подачі живлення.

Функціонування інтегральних схем RFID базується на використанні транзисторів, Зчитувач формує радіочастотне електромагнітне поле та здійснює обмін даними з міткою в момент її потрапляння у зону дії сигналу. Залежно від способу живлення RFID-мітки поділяються на такі типи:

– активні мітки - оснащені власним джерелом живлення (акумулятором), яке забезпечує роботу всіх функціональних елементів;

– напівактивні мітки - мають акумулятор, що використовується лише для живлення мікросхеми, тоді як передавання сигналу здійснюється за рахунок енергії зчитувача;

– пасивні мітки - не містять власного джерела живлення, що робить їх дешевшими, компактнішими та більш надійними порівняно з активними аналогами.

КБПЗ_2026

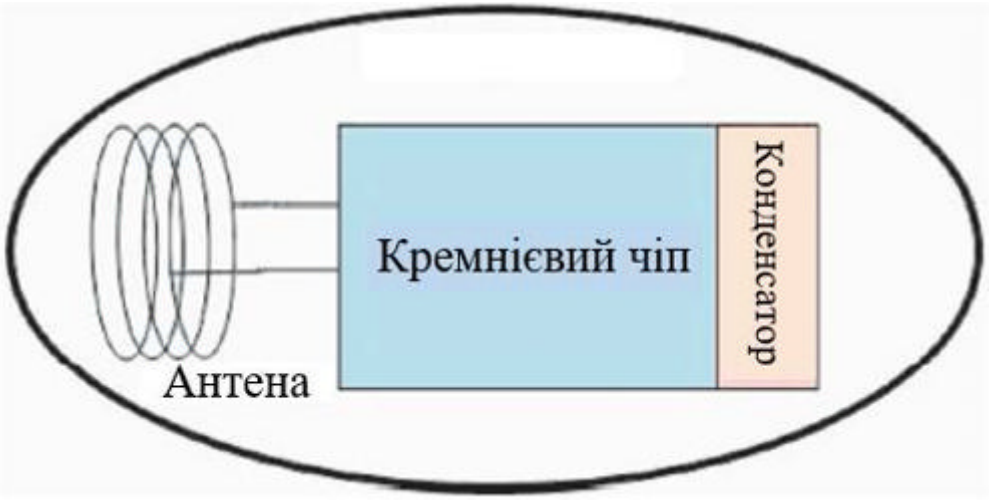


Рисунок 2.2 – Будова RFID-мітки

Розмір антени значною мірою визначає габарити RFID-мітки, оскільки саме антена є її найбільшим конструктивним елементом. Вона забезпечує передавання та приймання радіохвиль, виконуючи функцію зв’язку між міткою та зчитувачем. У пасивних RFID-мітках антена додатково виконує роль перетворювача енергії, забезпечуючи живлення мікросхеми за рахунок електромагнітного випромінювання, створеного антеною зчитувача. Отримана енергія надходить на контакти антени, після чого передається до випрямляча всередині мікросхеми, де перетворюється у постійну напругу живлення. Конструкція антени може відрізнятися залежно від умов застосування та призначення RFID-системи [2].

На відміну від більшості радіочастотних систем, у яких антени розраховані на стандартні навантаження 50 або 75 Ом, антена RFID-мітки повинна бути безпосередньо узгоджена з мікросхемою, що зазвичай характеризується високим вхідним опором. Таке узгодження є необхідною умовою для забезпечення максимальної передачі потужності від антени до мікросхеми та ефективної роботи транспондера. Саме тому процедура узгодження імпедансів є одним із ключових етапів під час проєктування RFID-міток.

Еквівалентна схема підключення антени наведена на рисунку 2.3. Напруга VsV_sVs формується прийнятим сигналом. Антена характеризується

КОПЗ_2026

комплексним вхідним опором ZANTZ_{ANT}ZANT, тоді як мікросхема має опір навантаження ZLOADZ_{LOAD}ZLOAD, значення якого залежить від робочої частоти та конструкції чіпа і може бути визначене експериментально.

Для забезпечення максимальної передачі енергії необхідно, щоб вхідний опір антени був узгоджений з імпедансом мікросхеми на робочій частоті. Це означає, що дійсна частина опору антени повинна дорівнювати дійсній частині опору навантаження, а уявна складова вхідного опору антени має бути рівною за величиною та протилежною за знаком уявній складовій імпедансу навантаження. Такий підхід забезпечує оптимальну ефективність роботи RFID-мітки.

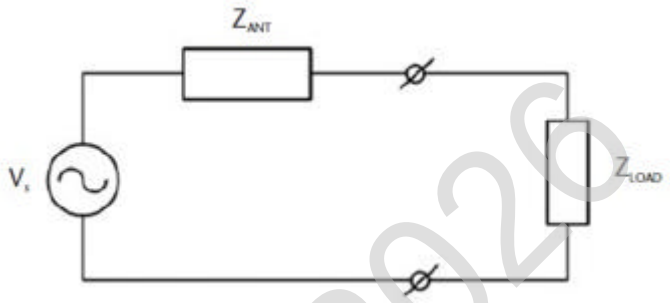


Рисунок 2.3 – Еквівалентна схема RFID-мітки

Субстрат є матеріальною основою RFID-мітки, яка забезпечує механічне з'єднання всіх її компонентів. Підкладка може бути як жорсткою, так і гнучкою залежно від умов експлуатації та сфери застосування, а також виготовлятися з різних матеріалів. Наприклад, RFID-мітки, що використовуються для контролю стану автомобільних шин, працюють у складних умовах підвищеної температури та високого тиску. У таких випадках мітка розміщується у спеціальній захисній капсулі, що запобігає пошкодженню антени та мікросхеми. Натомість RFID-мітки для відстеження документів повинні мати гнучку підкладку, яка дозволяє їм згинатися разом із паперовим носієм. У складних умовах експлуатації, де важливими є компактність і надійність, застосовуються спеціальні матеріали, наприклад гнучкі магнітні композитні підкладки, що дозволяють зменшити розміри антени та знизити вартість мітки.

У розвитку RFID-технологій сформувалися два основні підходи до

КПІ – 2026

передавання енергії від зчитувача до мітки: магнітна індукція та захоплення електромагнітних хвиль. Ці методи базуються на використанні властивостей ближнього та дальнього електромагнітного поля антени. Під час проходження змінного струму через котушку формується змінне магнітне поле — так зване ближнє поле. Одночасно відбувається поширення електромагнітних хвиль у просторі, що відповідає дальньому полю та лежить в основі радіозв'язку. Обидва підходи можуть забезпечувати передачу енергії, необхідної для роботи RFID-мітки, потужність якої зазвичай становить від 10 мкВт до 1 мВт залежно від типу пристрою, а також використовуються для передавання даних шляхом модуляції сигналу [3].

Зв'язок у ближньому полі реалізується відповідно до закону електромагнітної індукції Фарадея. Зчитувач пропускає змінний струм через власну котушку, створюючи змінне магнітне поле. Якщо у цьому полі розташувати RFID-мітку з меншою котушкою, у ній індукується змінна напруга. При підключенні котушки до конденсатора накопичена енергія може використовуватися для живлення мікросхеми мітки. Передавання даних від мітки до зчитувача здійснюється методом модуляції навантаження.

Струм, що виникає у котушці мітки, створює власне магнітне поле, яке частково впливає на поле зчитувача. Це проявляється у вигляді незначної зміни струму в котушці зчитувача, пропорційної навантаженню мітки. Аналогічний принцип використовується у силових трансформаторах, хоча у RFID-системах зв'язок між котушками значно слабший. Змінюючи навантаження своєї антени, мітка формує сигнал, що кодує її ідентифікатор, який зчитувач відновлює шляхом аналізу змін струму. Тип модуляції визначається необхідною швидкістю передавання даних, довжиною ідентифікатора та використанням додаткових бітів корекції помилок.

RFID-зчитувач виступає керуючим пристроєм (master), який забезпечує живлення мітки та ініціює процес обміну даними, надсилаючи відповідні запити. Керування зчитувачем може здійснюватися через комп'ютерний термінал або

КПЗ-2026

автоматизовані програмні сценарії. Стаціонарні зчитувачі підключаються до мереж електроживлення та передачі даних, тоді як мобільні або ручні пристрої працюють автономно (рис. 2.4). Для подальшої обробки інформації зчитувач може бути підключений до центрального комп'ютера або бази даних.



Рисунок 2.4 – Стаціонарний та мобільний зчитувач

RFID-зчитувач складається з двох основних функціональних частин: блоку керування та радіочастотного модуля, який включає передавальний і приймальний тракт. Блок керування містить апаратні та програмні засоби, що забезпечують керування роботою зчитувача, організацію взаємодії з головною комп'ютерною системою та RFID-мітками, а також виконання обробки отриманих даних.

Передавальний модуль формує радіочастотний сигнал із заданими параметрами частоти та рівня потужності й передає його через резонансну антенну систему. Приймальна частина зчитувача приймає радіосигнал, сформований RFID-міткою, після чого виконує його демодуляцію та декодування. Отримані двійкові дані передаються до блоку керування для подальшої обробки та передачі у вищий рівень інформаційної системи [4].

Програмні компоненти

Будь-яка RFID-система функціонує під керуванням спеціалізованого

КПІ_2026

програмного забезпечення, яке може бути реалізоване як у вигляді вбудованого ПЗ контролера, так і у формі складних інформаційних систем, що працюють на серверному обладнанні або у глобальних територіально розподілених мережах [5].

Порівняно з апаратними компонентами RFID, програмне забезпечення потребує більш глибокого врахування умов експлуатації системи. Сам зчитувач зазвичай є відносно простим пристроєм і може бути швидко впроваджений із мінімальними витратами. Натомість програмна частина повинна інтегруватися з бізнес-процесами підприємства, тому її необхідно адаптувати відповідно до конкретних задач застосування. Навіть однакові типи зчитувачів у межах одного приміщення можуть використовуватися для різних функцій, що потребує ретельного проєктування, налаштування та планування RFID-інфраструктури.

Передавання RFID-даних до програмного забезпечення передбачає їх централізоване зберігання. Надалі ці дані разом із супровідними атрибутами можуть використовуватися для аналізу та прийняття рішень у режимі реального часу. Інформація про місцезнаходження об’єктів, їх властивості або належність до певного контейнера дозволяє відстежувати виробничі процеси та відновлювати повний маршрут переміщення об’єкта. Наприклад, у виробництві медичного обладнання RFID-маркування дає змогу зберігати історію проходження виробу через усі етапи технологічного процесу. У разі виявлення дефекту можна швидко ідентифікувати інші вироби, що проходили аналогічні операції, для подальшої перевірки.

Ефективність програмного забезпечення особливо зростає у випадках виникнення аномальних ситуацій, таких як помилки зчитування або запису, несанкціоноване переміщення об’єкта чи інші нестандартні події, які автоматично визначаються системою.

Серед найбільш поширених програмних рішень для RFID-систем можна виділити такі:

– Radio Frequency Maestro - система автоматизації процесів приймання

КБПЗ-2026

та відвантаження продукції, що забезпечує керування даними складу в режимі реального часу та може адаптуватися до потреб дистриб'юторських підприємств [6].

– STP Source Tagging Platform - високопродуктивна платформа для кодування та перевірки RFID-міток із пропускною здатністю до 9500 тегів за хвилину та швидкістю перевірки до 15000 тегів за хвилину.

– BSI RFID Inventory - програмне рішення для автоматизованого управління запасами, яке підтримує планування інвентаризації, контроль змін кількості та вартості товарів, а також інтеграцію з ERP-системами підприємства [5].

– rTooltrack - система керування інструментами та виробничим обладнанням, що використовує пасивні RFID-мітки для скорочення часу інвентаризації та пошуку відсутніх об'єктів. Підтримує корпоративну синхронізацію даних із захищеним обміном інформацією.

– eTurns TrackStock - хмарне програмне забезпечення для автоматизованого управління запасами, яке забезпечує контроль інвентарю в реальному часі та автоматичне поповнення матеріалів із використанням RFID, штрих-кодів, IoT-датчиків і мобільних пристроїв [5].

– Virtual Asset Tracker - система керування активами, розроблена компанією Radiant RFID, що забезпечує відстеження місцезнаходження об'єктів, аналітику, звітність і інтеграцію з ERP-системами. Підтримує роботу з активними й пасивними RFID-мітками та мобільними пристроями.

– RedBeam RFID Asset Tracking - програмне забезпечення для обліку та відстеження обладнання, транспорту й інших матеріальних активів. Система підтримує кодування міток, налаштування зон зчитування, ведення історії обслуговування, формування звітності та роботу з базами даних SQL [5].

Таким чином, програмне забезпечення є ключовим елементом RFID-системи, оскільки саме воно забезпечує інтеграцію апаратних компонентів із інформаційними процесами підприємства, автоматизацію обліку та підвищення

КПЗ_2026

ефективності управління ресурсами.

Безпека та конфіденційність у системах RFID

Порушення конфіденційності в RFID-системах може проявлятися у двох основних формах: витік інформації та відстеження місцезнаходження користувача. Перший тип пов'язаний із безпосереднім отриманням даних із RFID-мітки, що можуть розкривати особисті характеристики власника. Наприклад, інформація про лікарські препарати може свідчити про стан здоров'я людини, а дані про придбані товари - про спосіб життя або споживчі вподобання. Особливе занепокоєння викликає можливість пов'язування позначених товарів із конкретними покупцями у централізованих базах даних, що дозволяє створювати персоналізовані маркетингові профілі.

Другий тип загроз стосується можливості відстеження переміщення людини. Навіть за відсутності прямого зв'язку між міткою та особою, статичні ідентифікатори можуть бути використані для аналізу даних, отриманих від різних зчитувачів, розташованих у фіксованих точках. У результаті формується маршрут пересування користувача за RFID-мітками, які він носить із собою.

Будь-який протокол RFID повинен відповідати базовим вимогам безпеки:

1. Захист конфіденційності - RFID-мітка не повинна передавати інформацію, що дозволяє ідентифікувати її вміст або власника. Більшість недорогих міток використовують постійні ідентифікатори, що потенційно можуть розкривати конфіденційні дані, пов'язані з грошовими засобами, медичними препаратами чи особистими речами [4].

2. Захист від відстеження - оскільки мітки можуть зчитуватися навіть із сумок або одягу, а зчитувачі можуть бути прихованими, необхідно уникати використання незмінних ідентифікаторів, які дозволяють ідентифікувати людину або групу об'єктів [4].

Під час оцінювання безпеки RFID важливо враховувати, що інколи більшу цінність мають фізичні активи, ніж самі дані. Навіть без втрати інформації організація може зазнати значних матеріальних збитків. Для ефективного захисту

КПЗ 2026

необхідно визначити можливі цілі атак і характер потенційних загроз.

З точки зору радіочастотної безпеки, RFID-мітки та зчитувачі розглядаються як єдина система, яка може піддаватися таким типам атак:

– підробка (spoofing);

– вставка шкідливих даних;

– повторна передача сигналу (replay-атака);

– відмова в обслуговуванні (DoS).

Атаки можуть бути комбінованими. Наприклад, зловмисник може використати модифіковану RFID-мітку для впровадження шкідливих даних через проміжне програмне забезпечення до серверної частини системи.

Для запобігання таким загрозам необхідно насамперед визначити вимоги безпеки системи. Наприклад, у складській системі, де RFID-зчитувач розміщений над конвеєрною стрічкою, потенційний зловмисник може перехоплювати радіосигнали. У цьому випадку доцільно:

- зменшити потужність передавання зчитувача до мінімально необхідного рівня;

- змінити розташування або орієнтацію антен;

- застосувати екранування, наприклад клітку Фарадея.

Надійне керування проміжним програмним забезпеченням забезпечує коректність передавання даних усередині системи. Аномальні значення (наприклад, текст замість числового ідентифікатора) можуть свідчити про спробу атаки. Для перевірки цілісності інформації часто застосовуються контрольні суми та механізми шифрування.

Захист інфраструктури також передбачає:

- використання криптографічного захисту каналів зв’язку;

- фізичне обмеження доступу до мережевого обладнання;

- контроль підключення нових пристроїв до мережі;

- аудит програмного коду та запобігання переповненню буфера;

- застосування політик доступу користувачів.

КБПЗ – 2026

Окрім базових, RFID-системи повинні задовольняти й додаткові вимоги:

1. Ефективність ідентифікації - система повинна підтримувати масштабованість, оскільки база даних може містити мільйони або навіть мільярди ідентифікаторів, а зчитувачі здатні одночасно обробляти багато міток [4].

2. Захист від клонування міток - копіювання RFID-тегів може призвести до підміни товарів або несанкціонованого доступу. Одним із методів протидії є використання технологій обмеження відстані (distance-bounding), які контролюють час затримки сигналу та унеможливлюють підробку відповіді мітки [4].

Таким чином, забезпечення безпеки RFID-систем потребує комплексного підходу, що поєднує криптографічний захист, правильне проєктування радіочастотної інфраструктури, контроль програмного забезпечення та фізичну безпеку обладнання.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Особливості застосування технології радіочастотної ідентифікації на підприємстві

З урахуванням усіх складових RFID-рішення, зокрема апаратного забезпечення, програмного забезпечення, інженерії бізнес-процесів та управління інформаційними потоками, можна зробити висновок, що впровадження таких систем потребує значних фінансових ресурсів, кваліфікованого персоналу та тривалого часу реалізації. Основною відмінністю RFID-проєктів від інших інформаційних систем є значний обсяг робіт саме на початковому етапі аналізу. Цей етап передбачає детальне дослідження наявних даних, а також глибоке розуміння поточних процесів підприємства і перспектив їх подальшого розвитку.

Впровадження RFID фактично являє собою процес інтеграції фізичних операцій із цифровими інформаційними системами підприємства. Така інтеграція

КПЗ_2026

дозволяє поєднати реальні виробничі або логістичні дії з існуючим програмним середовищем, формуючи керовану інформаційно-фізичну інфраструктуру бізнесу.

У результаті дані автоматично збираються та стають доступними для оперативного аналізу і прийняття управлінських рішень.

Інформація, отримана в електронному вигляді в режимі реального часу, має значно більшу цінність порівняно з даними, що збираються вручну та обробляються із затримкою (рис. 2.5). Можливість впливу на виробничі процеси на рівні окремих компонентів забезпечує підвищення швидкості виконання повторюваних операцій і зменшення кількості помилок. Крім того, інтеграція автоматизованих сценаріїв обробки реальних подій створює додаткові можливості для оптимізації процесів і зниження витрат за рахунок підвищення ефективності управління.



Рисунок 2.5 – Стек програмних компонентів RFID

Особливості застосування технології RFID у промисловості визначаються низкою специфічних факторів, зокрема необхідністю роботи в умовах широкого

діапазону температур і вологості, наявністю значної кількості металевих конструкцій у робочому середовищі, а також складною геометрією виробів, що підлягають ідентифікації [5].

Однією з основних проблем під час впровадження RFID у промислових умовах стало зниження ефективності ідентифікації металевих об’єктів або роботи систем у середовищах із високим вмістом металу. Наприклад, в автомобільній промисловості більшість деталей виготовляється саме з металу, що ускладнює стабільне зчитування RFID-міток. Для розв’язання цієї проблеми були розроблені спеціалізовані RFID-мітки типу on-metal tag, призначені для роботи безпосередньо на металевих поверхнях.

До найбільш поширених конструкцій RFID-міток, адаптованих для металевих середовищ, належать:

- мітки з простою прямокутною антеною;
- мітки з компактною петльовою антеною;
- мітки з плоскою інвертованою антеною F-типу (PIFA);
- мітки з патч-антеною з електромагнітним зазором.

Попри різноманітність конструкцій, усі подібні мітки мають спільний недолік - більшу товщину порівняно зі стандартними плоскими RFID-етикетками. Наприклад, у патч-антен товщина визначається діелектричною підкладкою, тоді як у петльових антен вона залежить від геометричних розмірів самої петлі. У зв’язку з цим універсального рішення для маркування металевих об’єктів не існує. Вибір типу RFID-мітки залежить від характеристик об’єкта, доступного місця для встановлення, вартості реалізації та необхідної дальності зчитування.

Вплив рідин на роботу RFID також відрізняється залежно від типу системи. Вода та інші рідини мають відносно незначний вплив на RFID-системи ближнього поля, оскільки більша довжина хвилі менш схильна до поглинання середовищем. Натомість системи дальнього поля, що працюють на коротших хвилях, значно сильніше зазнають впливу рідин, унаслідок чого ефективна відстань зчитування може істотно зменшуватися [7].

КПІ – 2026

На практиці RFID-мітки ближнього поля є більш придатними для маркування контейнерів із рідинами, таких як пляшки з напоями, молоком або мастильними матеріалами. Залежність індуктивності антени від частоти поблизу водного середовища наведено на рисунку 2.6. Навіть при розміщенні котушкової антени безпосередньо у воді спостерігається лише незначне зменшення її індуктивності, що підтверджує ефективність використання RFID-систем ближнього поля для подібних застосувань.

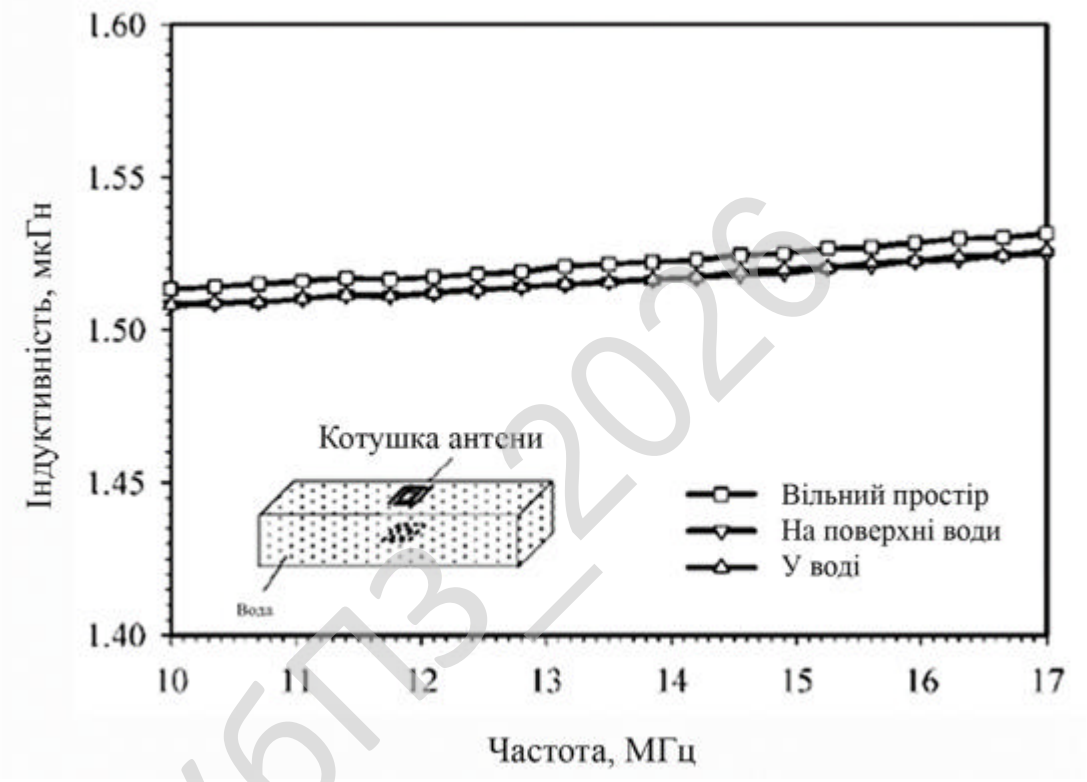


Рисунок 2.6 – Розрахована індуктивність котушкової антени з водою

У процесі розвитку промислового масового виробництва виробничі процеси постійно вдосконалювалися та раціоналізувалися. Це призвело до появи конвеєрного виробництва, у межах якого окремі технологічні операції виконуються послідовно на визначених ділянках виробничої лінії. Такий підхід забезпечує високу продуктивність, однак здебільшого орієнтований на виготовлення однотипної продукції з однаковими функціональними характеристиками та зовнішнім виглядом.

Сучасні виробники зацікавлені у глибшому аналізі процесів, що

КБТЗ_2026

відбуваються на кожному етапі виробництва. Збір і аналіз даних про виробничу діяльність, а також контроль параметрів навколишнього середовища дозволяють виявляти причини дефектів продукції та визначати напрями оптимізації процесів. Використання реальних виробничих даних забезпечує оперативне реагування на відхилення та підвищує загальну ефективність виробництва. Чим більший обсяг доступної інформації, тим точніше можна оцінити стан технологічного процесу.

Важливим аспектом є забезпечення простежуваності продукції — отримання точної інформації про те, який виріб був виготовлений, із яких матеріалів і комплектуючих він складається. Це дозволяє швидко визначати партії продукції, що можуть містити дефектні елементи. Крім того, достовірні виробничі записи мають юридичне значення, оскільки у випадку відмови продукції вони можуть підтвердити відповідність виробництва чинним технічним стандартам. Дані, отримані від сенсорів, допомагають встановити причини несправностей і звузити перелік потенційно проблемних виробів, а також оцінити показники ефективності, наприклад тривалість виробничого циклу [8].

Практичним прикладом застосування RFID у промисловості є рішення, представлене 3 листопада 2020 року компанією CribMaster, підрозділом Stanley Black & Decker. Було розроблено вдосконалену систему керування інструментами з підтримкою RFID, яка забезпечує виробничим підприємствам повний контроль над використанням обладнання. Лінійка Accu використовує RFID-зчитувач із чотирма антенами, RFID-мітки, закріплені на кожному інструменті, та програмне забезпечення управління запасами для обробки отриманих даних. Така система забезпечує відображення стану активів у режимі реального часу - від дрібних комплектуючих до великогабаритних інструментів [9].

Подібні рішення є особливо важливими для аерокосмічної галузі, де навіть один загублений інструмент може призвести до зупинки виробництва або серйозних аварій. Найбільш критичним ризиком є явище FOD (Foreign Object Damage) - пошкодження, спричинене сторонніми предметами. За оцінками компанії Boeing, інциденти, пов’язані з FOD, щорічно завдають авіаційній

КБПЗ_2026

промисловості збитків на суму близько 4 мільярдів доларів.

Автоматизація контролю інструментів за допомогою RFID дозволяє визначати, які інструменти знаходяться у сховищі, а які ще залишаються у виробничій зоні. Це значно знижує ризик виникнення FOD та сприяє впровадженню профілактичних програм безпеки, особливо у критично важливих виробничих середовищах. Аналогічні проблеми характерні не лише для авіабудування, а й для сфер технічного обслуговування, експлуатації та будівництва, де контроль матеріальних ресурсів має вирішальне значення.

Системи контролю та управління доступом

Електронні системи контролю доступу з використанням носіїв даних застосовуються для автоматизованої перевірки прав доступу користувачів до будівель, приміщень або окремих зон. Під час проєктування таких систем необхідно враховувати існування двох принципово різних типів організації - онлайн та офлайн систем контролю доступу, які мають різні функціональні можливості та сфери застосування.

Онлайн-системи зазвичай використовуються у випадках, коли необхідно здійснювати перевірку доступу великої кількості користувачів через обмежену кількість точок входу, наприклад у адміністративних або комерційних будівлях. У таких системах усі термінали підключені до центрального комп’ютера через мережу. Центральний сервер керує базою даних користувачів, у якій визначаються носії даних, що мають право доступу до конкретних точок проходу. Дані авторизації передаються до терміналів або проміжних контролерів дверей і зберігаються у вигляді локальних таблиць доступу. У подібних системах можуть використовуватися транспондери лише для зчитування [10].

Офлайн-системи найчастіше застосовуються у випадках, коли велика кількість окремих приміщень має обмежене коло користувачів. У цьому випадку кожен термінал автономно зберігає перелік дозволених ідентифікаторів доступу та не має постійного з’єднання з центральним сервером або іншими терміналами.

Безконтактні системи контролю доступу забезпечують значно більшу

КПЗ-2026

зручність використання, оскільки для ідентифікації достатньо піднести транспондер на невелику відстань до антени зчитувача. Носії доступу можуть реалізовуватися у вигляді безконтактних смарт-карт, брелоків або навіть наручних пристроїв.

Суттєвою перевагою таких систем є їх висока надійність і низькі вимоги до обслуговування. Зчитувачі не піддаються значному впливу пилу, вологи чи забруднень, а антени можуть встановлюватися під поверхнею стін, залишаючись непомітними та захищеними від механічних пошкоджень або вандалізму. Крім того, зчитувальні пристрої можуть інтегруватися у турнікети та інші елементи пропускної інфраструктури.

У загальному випадку система контролю та управління доступом (СКУД) включає такі основні компоненти (рис. 2.7):

1. Контролери СКУД - електронні мікропроцесорні пристрої, що забезпечують автентифікацію користувачів за допомогою ідентифікаційних пристроїв, реалізацію логіки авторизації доступу та керування виконавчими механізмами [5].

2. Пристрої введення ідентифікаційних даних та виконавчі пристрої - зчитувачі RFID, турнікети, двері з електромагнітними або електромеханічними замками, ворота, шлагбауми та шлюзові системи.

3. Програмне забезпечення - додатковий компонент, що забезпечує централізоване керування системою з персонального комп’ютера, ведення журналів подій, формування звітності та реалізацію розширених функцій адміністрування доступу.

КПЗ – 2026

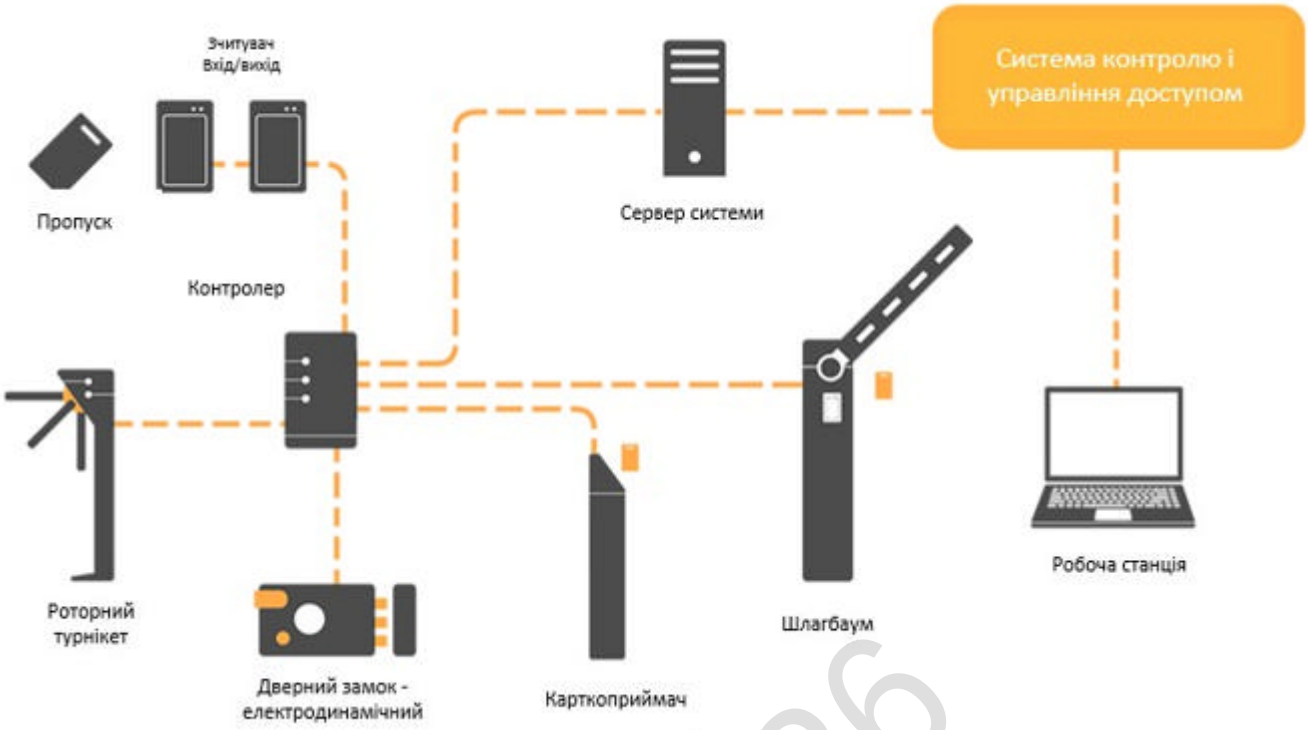


Рисунок 2.7 – Основні елементи системи контролю та управління доступом

КПІВ_2026

2.3 Розгорнута постановка завдання

У промисловому виробництві широко застосовуються верстати з високими швидкостями обертання та переміщення робочих елементів, що значно підвищує ризик виникнення аварійних ситуацій під час обслуговування або заміни інструменту. Однією з причин небезпеки може бути неправильне встановлення інструменту або помилки під час монтажу елементів, наприклад ланцюгового магазину верстата.

Зменшити ймовірність виникнення подібних ситуацій можна шляхом використання RFID-технології. Для цього RFID-мітка встановлюється безпосередньо у вал або кріпильні елементи тримача інструменту. Виробник інструменту попередньо записує у мітку всі необхідні технічні та геометричні параметри. Після встановлення інструментів оператором система автоматично виконує їх зчитування, визначає правильне розташування у магазині інструментів та передає відповідні дані до системи керування верстатом. Такий підхід усуває

необхідність ручного введення інформації, що значно знижує ризик людської помилки та запобігає аваріям, пов’язаним із неправильною швидкістю обертання, напрямком руху або некоректним позиціонуванням інструменту відносно заготовки.

RFID-технологія також ефективно застосовується для підвищення безпеки працівників, які працюють зі спеціалізованим транспортом на складах, виробничих підприємствах або будівельних майданчиках. Значна частина виробничих травм пов’язана зі зіткненнями між транспортними засобами та пішоходами. Використання RFID-систем попередження дозволяє істотно зменшити такі ризики.

Принцип роботи подібної системи є досить простим: працівники носять RFID-мітки, закріплені на одязі, рукаві або захисній касці, тоді як транспортні засоби оснащуються RFID-зчитувачами. У разі небезпечного наближення працівника до техніки система автоматично подає сигнал попередження як водію, так і пішоходу.

Особливо важливою перевагою RFID є її ефективність у складних умовах експлуатації. На відміну від камер відеоспостереження або стандартних засобів індивідуального захисту, система здатна працювати навіть за умов поганої видимості, запиленості, задимлення або недостатнього освітлення. RFID-зчитувач може ідентифікувати мітки навіть за перешкодами чи поворотами, забезпечуючи додатковий рівень контролю та підвищуючи загальну безпеку персоналу на підприємстві.

Управління ланцюгами постачання (Supply Chain Management, SCM) охоплює процес переміщення продукції між різними учасниками - від постачання сировини до доставки готового товару кінцевому споживачу. Кожен ланцюг постачання має власну структуру, що формується відповідно до особливостей продукції та виробничих потреб підприємства. Водночас усі логістичні системи мають спільну мету - забезпечення простоти, стандартизації та високої швидкості виконання операцій.

КБПЗ-2026

Важливу роль у ланцюгах постачання відіграють складські комплекси, оскільки практично всі матеріальні ресурси хоча б один раз проходять етап зберігання перед реалізацією. Операції складування, обробки та транспортування товарів включають значну кількість процесів, які безпосередньо впливають як на собівартість продукції, так і на рівень логістичного сервісу.

Традиційно працівники складів виконують звірку відправлень із накладними, пакувальними листами та замовленнями шляхом ручного підрахунку і введення даних. Такий підхід часто призводить до помилок і збільшує час обробки вантажів. Особливо актуальною стає потреба в отриманні достовірної інформації про переміщення продукції в режимі реального часу, що є критично важливим для галузі споживчих товарів, де обробляються великі обсяги різноманітної продукції та складні логістичні маршрути.

Попри широке використання штрих-кодів, сучасна промисловість потребує більш детальної інформації, ніж можуть забезпечити традиційні методи ідентифікації. RFID-технологія дозволяє зберігати та передавати розширені дані, зокрема:

-повну інформацію про продукцію, прив’язану до кожного контейнера або піддона;

-відомості про виробництво, номер партії, підприємство-виробника та показники якості;

-технічні характеристики виробу та правила його експлуатації.

Практичним прикладом застосування RFID є встановлення зчитувачів на вантажних доках або зонах завантаження транспортних засобів. Під час переміщення вантажів навантажувачами система автоматично ідентифікує продукцію та фіксує фактичну кількість завантажених одиниць. Це дозволяє миттєво перевіряти відповідність замовлення та запобігати помилкам ще на етапі відвантаження.

Завдяки RFID-технології помилки, пов’язані з відправленням неправильного товару або невірної кількості продукції, виявляються

КбПЗ_2026

безпосередньо під час виконання операцій, а не після завершення доставки. Поетапне підтвердження руху товарів забезпечує своєчасне виявлення відхилень, що значно знижує витрати на їх усунення та підвищує ефективність управління логістичними процесами.

Радіочастотна ідентифікація (RFID) є бездротовою технологією автоматизованого збору даних. У найпростішому вигляді RFID-система складається з ідентифікаційної мітки, закріпленої на об’єкті, та зчитувача, який здійснює опитування мітки з метою її розпізнавання і отримання збереженої інформації.

RFID-мітка виконує роль програмованого пристрою передавання даних і включає елемент зв’язку у вигляді резонансного контуру та малопотужну CMOS-мікросхему. Зчитувач формує радіочастотне поле та забезпечує обмін інформацією з міткою під час її потрапляння в зону зчитування. Програмне забезпечення, своєю чергою, забезпечує інтеграцію апаратних компонентів у єдину інформаційну систему, виконуючи функції обробки, зберігання та керування даними.

Для забезпечення надійної роботи RFID-систем особливу увагу необхідно приділяти вимогам безпеки та конфіденційності, серед яких:

- захист конфіденційної інформації;
- запобігання відстеженню користувачів або об’єктів;
- забезпечення ефективної та достовірної ідентифікації;
- захист від підробки або клонування RFID-міток.

Під час впровадження RFID-технології у промислових умовах необхідно враховувати низку обмежувальних факторів, зокрема:

- температурні умови та рівень вологості середовища;
- наявність великої кількості металевих об’єктів;
- складну геометрію виробів, що підлягають ідентифікації;
- вплив води та інших рідин на роботу системи.

Завдяки своїм можливостям технологія RFID отримала широке

КБПЗ_2026

застосування в автоматизації виробничих процесів, зокрема для моніторингу виробництва, реалізації систем контролю та управління доступом (СКУД), підвищення рівня охорони праці, а також оптимізації логістики та управління ланцюгами постачання.

Згідно з технічним завданням на кваліфікаційну роботу, реалізації розробка програмного забезпечення системи радіочастотної ідентифікації для контролю промислового підприємства.

В процесі розробки кваліфікаційної роботи необхідно виконати наступний обсяг проекту:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику розробки відповідної системи та програмного забезпечення. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран результатів аналізу та тестування;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) сформувати висновки про виконаний обсяг робіт та одержані результати.

КБПЗ_2026

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

Розробка плану об’єкту контролю та автоматизації

Оскільки RFID-система планується до впровадження в уже функціонуючу інфраструктуру, що містить інші технічні системи та обладнання, необхідно визначити спосіб її інтеграції з наявним середовищем об’єкта. Тому перед завершенням проєктування та безпосереднім встановленням RFID-системи обов’язковим етапом є проведення комплексного аналізу об’єкта.

Такий аналіз передбачає дослідження фізичної інфраструктури приміщення та радіочастотного середовища з метою визначення оптимальних місць розташування зон зчитування або планування нових точок ідентифікації. Це дозволяє забезпечити стабільну роботу системи, мінімізувати перешкоди та досягти максимальної ефективності зчитування RFID-міток.

Об’єктом автоматизації виступає склад споживчих товарів (рис. 3.1), який умовно поділяється на декілька функціональних зон:

1. Зона приймання та відвантаження товарів - призначена для завантаження і розвантаження продукції. Вона обладнана шістьма воротами для в’їзду та виїзду великогабаритного транспорту.

2. Основна складська зона - використовується для зберігання товарів і включає дев’ять стелажів, два конвеєри для транспортування продукції між складом і зоною відвантаження, робочі місця пакувальників та допоміжне обладнання для переміщення вантажів.

3. Фойє та зона очікування - призначена для перебування гостей і водіїв транспортних засобів. У цій зоні також передбачено окремі санітарні приміщення для чоловіків і жінок.

4. Адміністративна зона - включає офісні приміщення операторів, робочі місця персоналу, що працює з базами даних, а також кабінет керівника складу.

КПЗ_2026

5. Зона відпочинку працівників - містить їдальню та окремі санітарні приміщення для персоналу.

Такий поділ об’єкта на функціональні зони дозволяє коректно спроєктувати розміщення RFID-обладнання, визначити критичні точки контролю руху товарів і персоналу та забезпечити ефективну інтеграцію системи автоматичної ідентифікації у складську логістичну інфраструктуру.

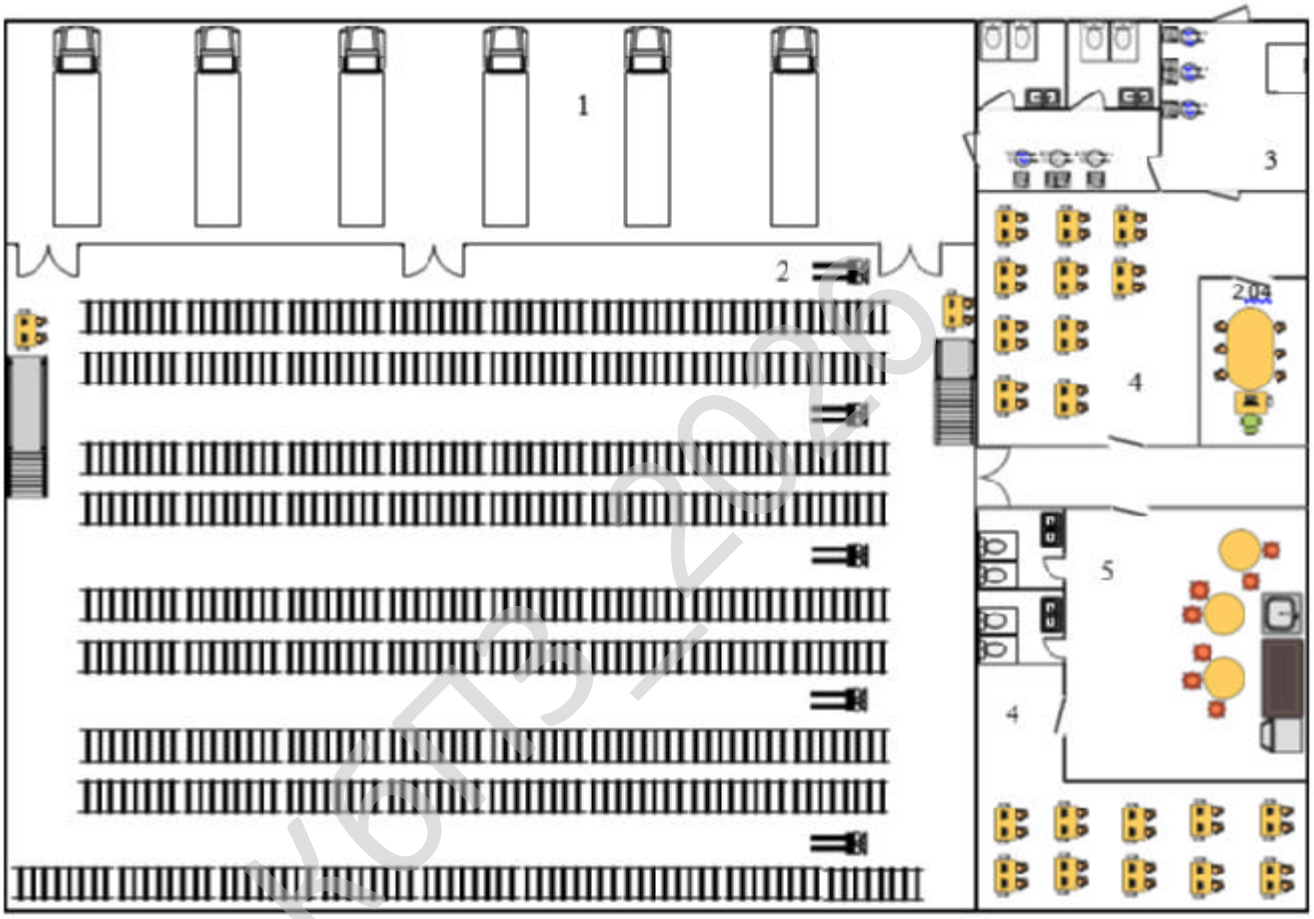


Рисунок 3.1 – План об’єкту контролю та автоматизації

3.1 Розробка структурної схеми

Функціонування традиційного складського комплексу здійснюється за визначеним послідовним алгоритмом обробки товарів. Робочий процес розпочинається у зоні приймання, де кожна одиниця продукції, ящик або палета проходить ручне сканування та первинну реєстрацію. Після цього вантаж

направляється до зони сортування, звідки за допомогою складської техніки транспортується до місця зберігання.

Формування замовлень також виконується вручну оператором, який здійснює відбір необхідних товарів зі складських позицій. Зібрані замовлення подаються конвеєрною системою до пакувальної зони, де розташовані різні типи тари, призначені для підготовки продукції до транспортування.

Після завершення пакування продукція переміщується до зони відвантаження, звідки здійснюється її подальше транспортування споживачам або торговим партнерам.

Опис системи радіочастотної ідентифікації

Впровадження RFID-системи у логістичні процеси складу дозволяє здійснювати контроль руху товарів у режимі реального часу на всіх етапах обробки продукції, що забезпечує своєчасне виявлення помилок, порушень або невідповідностей. Проведення інвентаризації при цьому значно спрощується — працівнику достатньо пройти складське приміщення з ручним RFID-зчитувачем, перебуваючи на відстані приблизно 1–2 метри від товарів [5].

Система контролю переміщення та обліку продукції розробляється з метою модернізації існуючого складського комплексу. Для автоматизації роботи застосовується пасивна надвисокочастотна (НВЧ) RFID-система, що відповідає стандарту ISO 18000-6C та функціонує у частотному діапазоні 860–960 МГц. Основними перевагами даної технології є відносно низька вартість RFID-міток, висока швидкість зчитування інформації та ефективні механізми запобігання колізіям сигналів.

Запропоновану систему умовно поділено на три функціональні підсистеми:

1. Система управління складом (WMS - Warehouse Management System).
2. Система контролю та управління доступом (СКУД).
3. Система забезпечення безпеки працівників.

КОПЗ_2026

Система управління складом (WMS)

Робота системи починається з портальних воріт, оснащених RFID-зчитувачами. У разі прибуття транспорту з основного підприємства всі ящики вже мають RFID-мітки, тому інформація про отриманий товар автоматично передається до бази даних. Якщо ж продукція надходить від сторонніх постачальників, у зоні приймання використовується RFID-принтер, підключений до WMS, за допомогою якого на упаковку наноситься відповідна мітка.

Після ідентифікації товари транспортуються конвеєром до складської зони. Оператори, використовуючи програмне забезпечення, записують у мітки інформацію про місце подальшого зберігання. Надалі працівники за допомогою мобільних зчитувачів розміщують продукцію на відповідних стелажах.

Процес відвантаження починається з формування замовлення, що містить перелік необхідних товарів із зазначенням їх ідентифікаторів і місця розташування. Це дозволяє операторам швидко здійснювати відбір продукції та доставляти її до зони завантаження. Під час пакування кожен ящик повторно зчитується мобільним терміналом, що забезпечує контроль правильності комплектації.

Фінальна перевірка виконується портальним RFID-зчитувачем на виїзних воротах, який фіксує факт залишення товаром складу. Таким чином, контроль здійснюється на кожному етапі логістичного процесу, що дозволяє оперативно виявляти помилки комплектування.

Система контролю доступу (СКУД)

СКУД забезпечує контроль доступу до складського приміщення та окремих його зон. Кожен працівник отримує RFID-картку доступу. Біля головного входу встановлено турнікет із вбудованим зчитувачем, який дозволяє прохід лише після успішної ідентифікації.

Доступ до складських зон реалізується через двері з електромагнітними замками та RFID-зчитувачами. Після перевірки ідентифікатора система подає живлення на замок, що дозволяє відкрити двері відповідно до визначених прав

КПЗ_2026

доступу. Портальні ворота з електроприводом у зоні завантаження можуть відкриватися лише керівником складу або службою охорони.

Система безпеки працівників

Безпека персоналу під час роботи зі складською технікою реалізується за допомогою RFID-системи попередження зіткнень. Працівники зони зберігання використовують браслети з вбудованими RFID-мітками, оснащені світловою та вібраційною сигналізацією. Транспортні засоби обладнані RFID-зчитувачами.

У разі небезпечного наближення працівника до техніки браслет потрапляє в зону зчитування та активує попереджувальний сигнал. Водії також використовують подібні браслети, при цьому передбачена можливість тимчасового вимкнення сигналізації під час безпосереднього керування транспортним засобом.

Таким чином, запропонована RFID-система забезпечує комплексну автоматизацію складських процесів, підвищує точність обліку товарів, контроль доступу та рівень безпеки працівників.

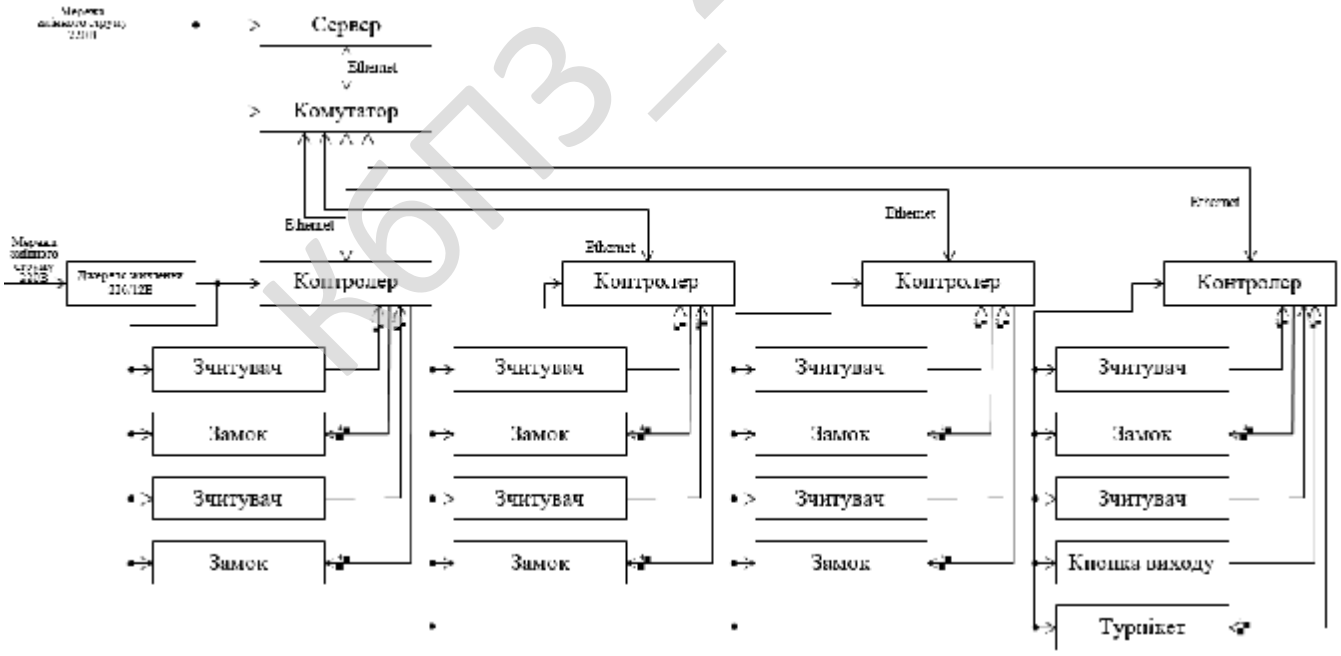


Рисунок 3.2 - Структурна схема системи

КБПЗ_2026

3.2 Розробка функціональної схеми

Система контролю та управління доступом передбачає використання семи дверей і одного турнікета, робота яких забезпечується чотирма контролерами доступу. До трьох контролерів підключено по два RFID-зчитувачі та два електромагнітні замки, тоді як четвертий контролер обслуговує один RFID-зчитувач, один електромагнітний замок, турнікет і кнопку виходу. Усі контролери з'єднані із сервером через мережевий концентратор за допомогою двостороннього Ethernet-з'єднання.

Живлення елементів системи організовано від джерела постійного струму напругою 12 В, необхідного для роботи контролерів доступу, зчитувачів, електромагнітних замків і турнікета. Для цього застосовано трансформаторний перетворювач. Сервер і мережевий комутатор живляться безпосередньо від мережі змінного струму. Загальна структурна схема системи контролю доступу наведена на рисунку 3.2.

Інфраструктура системи управління складом (WMS) базується на серверному комплексі зі спеціалізованим програмним забезпеченням, яке забезпечує взаємодію зі стаціонарними RFID-зчитувачами, RFID-принтерами та проміжним програмним забезпеченням обладнання. RFID-принтери підключаються до концентратора через Ethernet-мережу, після чого концентратор забезпечує обмін даними із сервером.

Мобільні RFID-зчитувачі працюють під керуванням проміжного програмного забезпечення, яке завантажується через USB-інтерфейс. Як RFID-принтери, так і мобільні зчитувачі оснащені власними вбудованими джерелами живлення.

Портальні RFID-зчитувачі складаються з центрального зчитувального модуля та чотирьох антен, підключених за допомогою SMA-кабелів. Для їх роботи необхідне живлення постійним струмом напругою 24 В, яке забезпечується трансформаторним перетворювачем. Серверне обладнання та

КПІ – 2026

мережевий комутатор, аналогічно системі СКУД, отримують живлення від мережі змінного струму. Структурна схема системи управління складом представлена на рисунку 3.3.

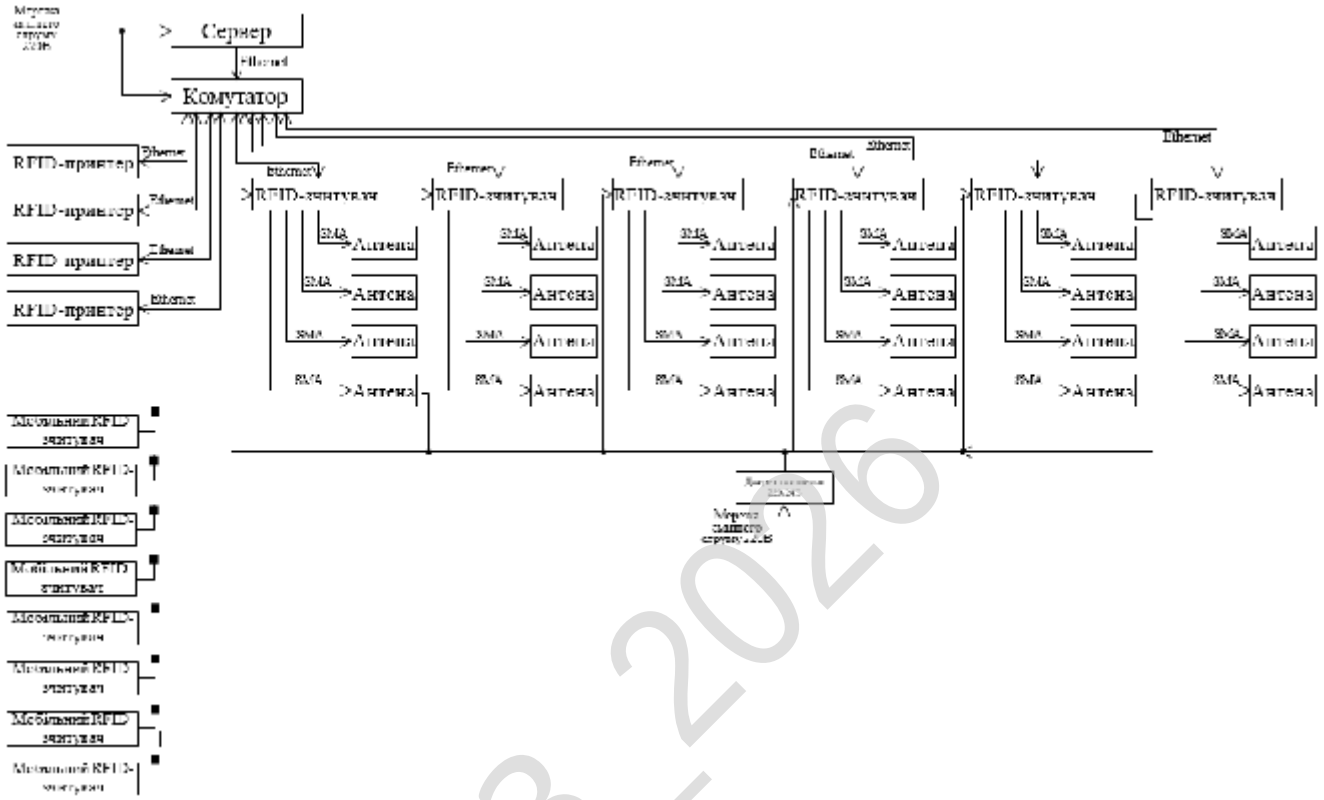


Рисунок 3.3 – Функціональна схема системи

Система сигналізації небезпечного зближення з транспортними засобами має відносно просту структуру та складається з RFID-зчитувачів із власними джерелами живлення, встановлених на транспортній техніці, транспондерів, які використовуються працівниками, а також програмного забезпечення, що забезпечує обробку сигналів і керування системою.

Працівники складу носять RFID-транспондери у вигляді браслетів або персональних пристроїв, тоді як складська техніка обладнується RFID-зчитувачами. У разі наближення працівника до транспортного засобу на небезпечну відстань система автоматично фіксує появу транспондера в зоні зчитування та формує попереджувальний сигнал.

КПІЗ_2026

Схема розташування всіх елементів системи контролю на плані складського приміщення представлена на рисунку 3.4.

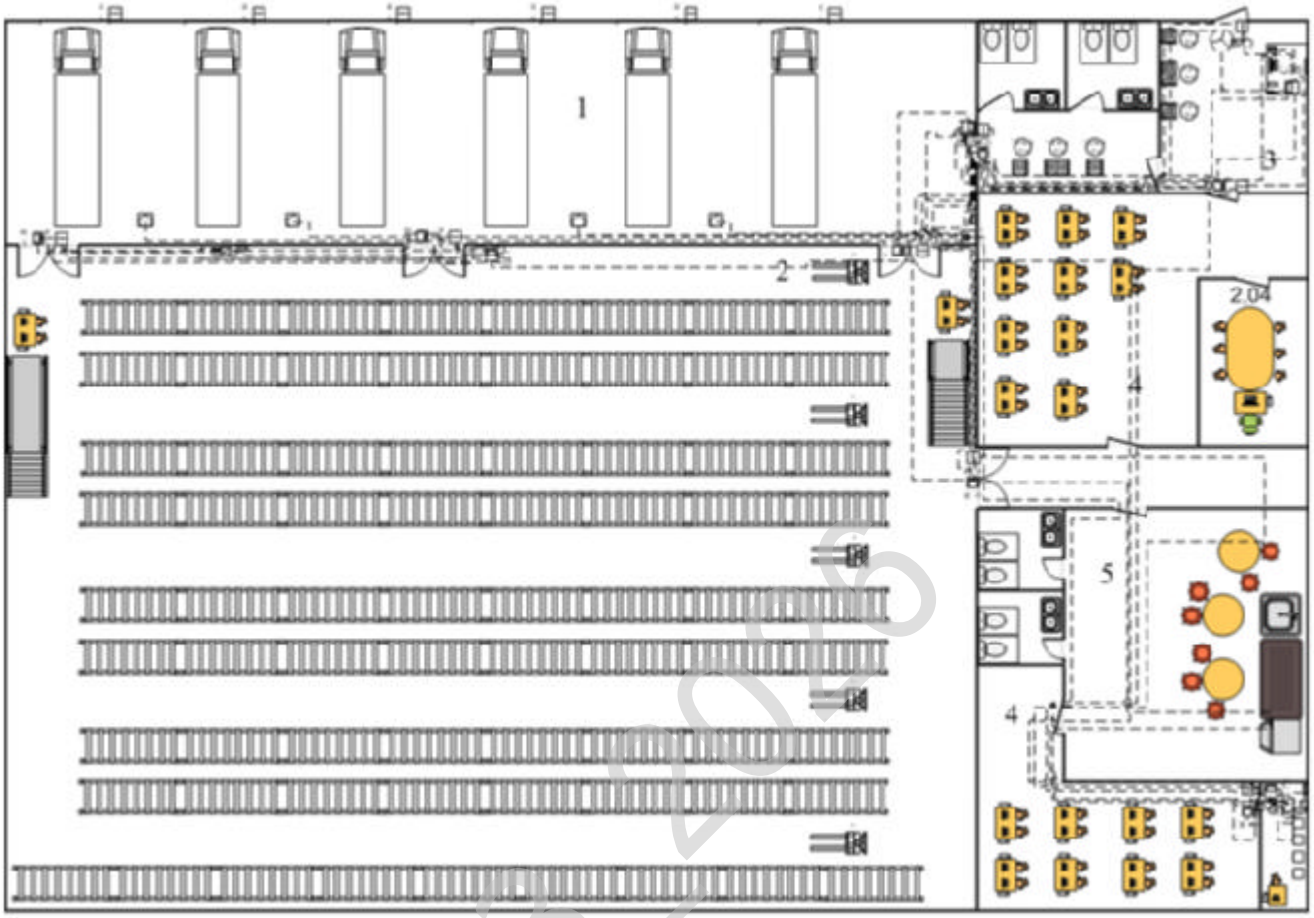


Рисунок 3.4 – Розміщення пристроїв системи контролю на плані складу

3.3 Розробка діаграми процесів

Діаграма взаємодії процесів описує логіку функціонування системи контролю та управління доступом на промисловому підприємстві, що базується на використанні технології радіочастотної ідентифікації (RFID). Система забезпечує ідентифікацію користувачів, обробку запитів доступу, взаємодію з сервером та керування виконавчими пристроями, такими як турнікет, шлагбаум та електромагнітний замок. Робота системи починається з моменту піднесення RFID-картки або пропуску до зчитувача. Зчитувач виконує процес ідентифікації, зчитуючи унікальний код користувача та передаючи його до контролера.

КПЗ_2026

Контролер виступає центральним елементом локальної системи, який приймає рішення або передає дані до серверної частини для подальшої обробки. Після отримання ідентифікатора користувача контролер передає запит до сервера системи. Сервер виконує обробку запиту, що включає перевірку прав доступу користувача, аналіз часу доступу, зони доступу та інших параметрів. На основі цих даних сервер формує відповідь, яка містить рішення щодо дозволу або заборони доступу. Отримавши відповідь від сервера, контролер переходить до етапу керування виконавчими пристроями. У випадку дозволу доступу активуються механізми відкриття, такі як турнікет, шлагбаум або дверний замок. Якщо доступ заборонено, система може сформувати сигнал тривоги або повідомлення.

Паралельно з цим система фіксує подію у базі даних, що дозволяє вести журнал відвідувань та контролювати переміщення персоналу. Інформація передається до робочої станції, де оператор може переглядати дані, аналізувати події та здійснювати управління системою.

Таким чином, діаграма відображає повний цикл взаємодії процесів - від зчитування RFID-мітки до прийняття рішення та керування виконавчими механізмами, що забезпечує ефективний контроль доступу на підприємстві.

КОПЗ_2026



Рисунок 3.5 – Діаграма взаємодії процесів

Висновки до розділу

У ланцюгах постачання складські комплекси виконують ключову функцію зберігання готової продукції, оскільки практично всі матеріальні об’єкти проходять етап складування щонайменше один раз перед реалізацією. Процеси зберігання, обробки та транспортування товарів значною мірою залежать від ручних операцій, що впливають на витрати підприємства та якість надання

логістичних послуг. Саме тому автоматизація складських процесів є доцільним рішенням для зменшення кількості помилок і підвищення ефективності роботи.

Об’єктом автоматизації обрано склад споживчих товарів. Для модернізації його роботи розроблено пасивну надвисокочастотну (НВЧ) RFID-систему, що функціонує відповідно до стандарту ISO 18000-6C у частотному діапазоні 860–960 МГц.

Запропоновану систему умовно поділено на три основні підсистеми:

- систему управління складом (WMS - Warehouse Management System);
- систему контролю та управління доступом (СКУД);
- систему забезпечення безпеки працівників.

Система управління складом (WMS) забезпечує контроль усіх етапів переміщення товарів і виконання замовлень у межах складу. До її складу входять портальні RFID-зчитувачі, встановлені на в’їзних та виїзних воротах, RFID-принтер для маркування продукції, що надходить без ідентифікаційних міток, мобільні зчитувачі для операторів і пакувальників, а також програмне забезпечення з централізованою базою даних, яке об’єднує всі компоненти системи в єдине інформаційне середовище.

Система контролю та управління доступом (СКУД) призначена для обмеження доступу до складського приміщення та його окремих функціональних зон. Кожен працівник використовує персональний RFID-ідентифікатор у вигляді пластикової картки. На головному вході встановлено турнікет із вбудованим зчитувачем, а доступ до внутрішніх зон реалізовано через двері з RFID-зчитувачами та електромагнітними замками. Після перевірки ідентифікатора система подає живлення на замок, що дозволяє відкрити двері відповідно до встановлених прав доступу.

Система забезпечення безпеки працівників реалізована у вигляді RFID-системи попередження зіткнень між персоналом і складською технікою. В умовах обмеженої видимості традиційні засоби безпеки або відеоспостереження не завжди є ефективними. RFID-технологія забезпечує додатковий рівень захисту,

КПЗ_2026

оскільки зчитувачі здатні виявляти транспондери навіть за перешкодами або поворотами, а їх робота практично не залежить від пилу, диму чи недостатнього освітлення. Це дозволяє своєчасно попереджати працівників і водіїв про небезпечне зближення та знижувати ризик виробничого травматизму.

КБПЗ_2026

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

Зростання використання технології RFID у різних галузях, а також поширення мобільних RFID-зчитувачів призводить до ситуацій, коли декілька зчитувачів працюють на малій відстані один від одного. У таких випадках можуть виникати колізії сигналів, що негативно впливає на швидкість та точність обробки інформації.

RFID-зчитувач виконує ряд функцій, серед яких живлення транспондера, його ідентифікація, зчитування та запис даних, а також взаємодія з програмним забезпеченням для подальшої обробки отриманої інформації. Конструктивно зчитувач складається з трьох основних компонентів:

- приймально-передавального модуля, який забезпечує двосторонній зв’язок;
- мікроконтролера, що відповідає за шифрування та дешифрування переданих і прийнятих даних;
- однієї або кількох антен.

Крім того, зчитувач виступає джерелом енергії для пасивних RFID-міток. Він здатний одночасно обробляти інформацію від великої кількості міток, що знаходяться в зоні дії. Для запобігання помилкам під час одночасного зчитування даних застосовується механізм антиколізії [5].

У процесі роботи зчитувача радіочастотний сигнал перетворюється на сигнал нижчої частоти за допомогою змішувача та гетеродина. На кожному етапі обробки використовуються аналогові фільтри для відокремлення сигналів поза робочою смугою частот. Перед оцифруванням сигнал поділяється на синфазну та квадратурну складові, після чого вони надходять до аналого-цифрового перетворювача (АЦП). У НВЧ-діапазоні пропускна здатність каналу становить

КПЗ – 2026

приблизно 25 МГц, тоді як ширина спектра сигналу мітки дорівнює близько 500 кГц. Завдяки цьому один зчитувач може одночасно обробляти сигнали приблизно від 50 міток, що працюють у межах даного частотного каналу.

RFID-зчитувачі можуть оснащуватися різними апаратними інтерфейсами підключення. Вони варіюються від послідовного інтерфейсу RS-232 до бездротових стандартів зв’язку, таких як 802.11b/g. Найбільш поширеними є інтерфейс RS-232 для підключення на невеликій відстані, RS-485 для використання в промислових системах середньої дальності, а також TCP/IP через Ethernet або 802.11b/g для мереж підприємства.

Розглянемо вибір мобільних зчитувачів для роботи операторів. Серія Zebra MC3300 RFID являє собою лінійку інтегрованих RFID-зчитувачів НВЧ-діапазону, створених на основі технології радіочастотної ідентифікації та мобільної платформи Android. Модель MC3330xR (рис. 4.1) призначена для зчитування RFID-міток і штрих-кодів у стандартних робочих діапазонах. Вона широко застосовується на складах, у магазинах, готелях, медичних закладах та у великих логістичних компаніях.

КбПЗ 2026



Рисунок 4.1 – Мобільний зчитувач MC3330xR

Середовище кросплатформної розробки Xamarin дозволяє програмістам застосовувати наявні знання та інструменти мови C# для створення швидких і

зручних додатків для пристроїв на базі Android. Використання комплекту EMDK for Xamarin від компанії Zebra дає можливість легко інтегрувати всі розширені функції пристрою MC3330xR у додатки, створені на платформі Xamarin. Комплект розробника корпоративних мобільних додатків (EMDK) спрощує створення програм для підприємств, що сприяє скороченню часу розробки та підвищенню економічної ефективності цього процесу.

Однією з основних переваг даного мобільного зчитувача є наявність вбудованої кільцевої антени, яка забезпечує стабільне зчитування незалежно від положення транспондера. Пристрій оснащений акумулятором ємністю 7000 мА·год, що дозволяє працювати протягом тривалого часу без підзарядки. Крім того, зчитувач підтримує роботу зі штрих-кодами, що значно полегшує інтеграцію системи на підприємствах, де вже використовується штрихкодовий облік.

Для системи контролю доступу було обрано зчитувачі HIKVISION DS-K1802E (рис. 4.2). Дані пристрої оснащені 8-бітним процесором, мають ступінь захисту IP65 та використовують інтерфейс підключення Wiegand (W26, W34). Вони призначені для роботи з картами стандарту Em-Marine на частоті 125 кГц із максимальною відстанню зчитування до 50 мм. Для роботи зчитувач потребує живлення 12 В і може функціонувати в температурному діапазоні від –20 °C до +65 °C.

КбПЗ_2026



Рисунок 4.2 – RFID-зчитувач HIKVISION DS-K1802E

Важливим компонентом системи контролю та управління доступом є турнікет, встановлений на вході до будівлі. У даній системі використано готове рішення - турнікет-трипод EXPERT (рис. 4.3).

Цей турнікет забезпечує пропускну здатність не менше 20 осіб за хвилину у режимі одиничного проходу. Контроль доступу може здійснюватися кількома способами: за допомогою пристроїв зчитування безконтактних карт стандарту RFID 125 кГц або Mifare 13,56 МГц, через дистанційне керування за допомогою пульта чи контролера системи контролю доступу, а також у ручному режимі.



Рисунок 4.3 – Турнікет трипод EXPERT

КПЗ_2026

До основних переваг даного турнікета належать компактні габарити та невелике енергоспоживання, що зумовлено простотою його конструкції. Крім того, передбачена можливість встановлення внутрішнього лічильника проходів. Пристрій може живитися як від мережі змінного струму 100–240 В, 50/60 Гц, так і від джерела постійного струму 12 В, при цьому споживана потужність становить близько 30 Вт.

Щодо зчитувачів, які встановлюються на транспортних засобах складу, було обрано RFID-зчитувач Zebra UWB Wand (рис. 4.4). Даний пристрій призначений для застосувань, де необхідна висока точність визначення місцезнаходження об’єктів та швидке оновлення даних у режимі реального часу.

Технологія UWB (Ultra-Wideband) використовує запатентовані рішення, що дозволяють реалізувати функції RTLS (системи визначення місцезнаходження в реальному часі) за допомогою транспондерів із дуже тривалим терміном роботи акумулятора.

Крім того, система Zebra UWB відповідає сучасному міжнародному стандарту IEEE 802.15.4f, а також проекту стандарту ISO-24730-61 Draft. Це забезпечує сумісність інфраструктури не лише з UWB-мітками виробництва Zebra, а й з іншими пристроями, що відповідають зазначеним стандартам, що дозволяє зберегти інвестиції в інфраструктуру та забезпечує можливість подальшого розширення системи.



Рисунок 4.4 – RFID-зчитувач Zebra UWB Wand

КОПІЯ 2026

Перевагами даного зчитувача є висока продуктивність завдяки роботі в багатопроменевому режимі, що забезпечує стабільний та швидкий обмін даними. Пристрій характеризується високою точністю визначення місцезнаходження об’єктів у режимі реального часу.

Ще однією важливою перевагою є тривалий термін роботи акумулятора транспондерів - до 7 років при частоті передавання сигналу 1 Гц. Система також забезпечує значну дальність роботи RTLS, яка може досягати 200 метрів у межах прямої видимості. Крім того, зчитувач відзначається високою пропускною

здатністю та здатний одночасно обробляти дані до 3500 транспондерів.

Вибір антен

Виконаємо проєктування прямокутної патч-антени із використанням субстрату RO4003C для портального RFID-зчитувача. На початковому етапі необхідно визначити вихідні параметри та розрахувати інші характеристики, потрібні для подальшого моделювання антени (рис. 3.5).

До основних вхідних параметрів належать:

- резонансна частота: fr=868f_r = 868fr=868 МГц;

- товщина субстрату (діелектричного шару): h=32h = 32h=32 мм;

- товщина металевого патча: t1=35t_1 = 35t1=35 мкм;

- діелектрична проникність субстрату RO4003C: εr=3,55\varepsilon_r = 3{,}55εr=3,55;

- швидкість поширення електромагнітних хвиль: c=3·108c = 3 \cdot 10^8c=3·108 м/с;

- тангенс кута діелектричних втрат субстрату RO4003C: tan δ=0,0021\tan \delta = 0{,}0021tanδ=0,0021.

На основі зазначених параметрів виконуються подальші розрахунки геометричних розмірів антени та її електромагнітних характеристик для моделювання роботи зчитувача.

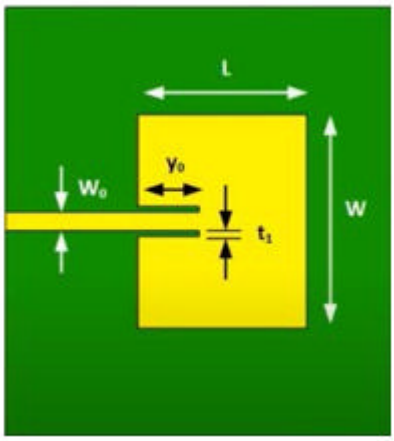


Рисунок 4.5 – Модель патч-антени

Для створення моделі в середовищі Comsol Multiphysics спочатку

КБПЗ_2026

необхідно відкрити Model Wizard та у вкладці вибору Space Dimension обрати режим 3D. Після цього на етапі вибору фізичних інтерфейсів потрібно додати модуль Electromagnetic Waves, Frequency Domain (emw), який використовується для моделювання поширення електромагнітних хвиль у частотній області (рис. 4.6).

Цей інтерфейс дозволяє досліджувати характеристики антени, зокрема розподіл електромагнітного поля, резонансні властивості та параметри випромінювання.

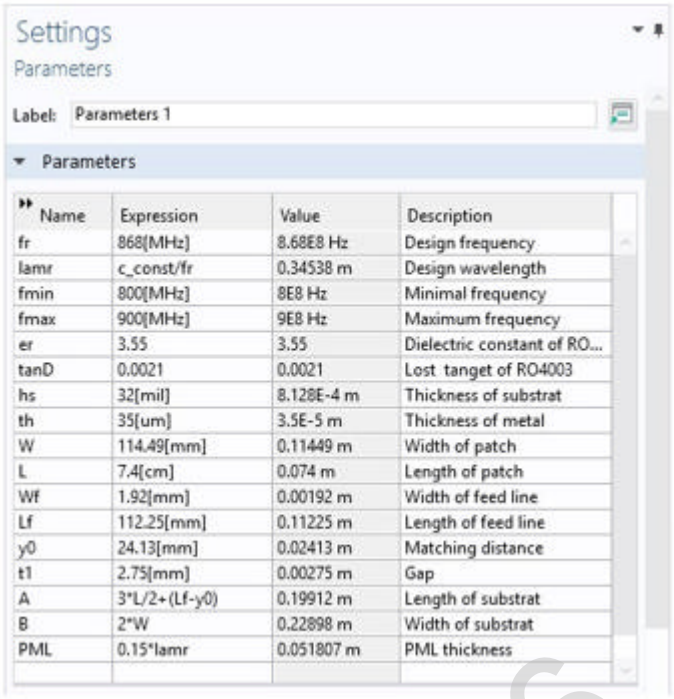


Рисунок 4.6 – Copyright Side Comsol Multiphysics

Далі в розділі Study до обраної фізичної моделі додаємо режим Adaptive Sweep Frequency, після чого створюємо новий проєкт. У вкладці Parameters (рис. 3.8) задаємо всі необхідні вхідні та попередньо розраховані параметри, які будуть використовуватися під час моделювання антени.

Введення цих параметрів дозволяє коректно задати геометричні розміри та електромагнітні характеристики моделі, що забезпечує точність подальших розрахунків і аналізу роботи антени.

КОПЗ – 2026



Name	Expression	Value	Description
fr	868[MHz]	8.68E8 Hz	Design frequency
lamr	c_const/fr	0.34538 m	Design wavelength
fmin	800[MHz]	8E8 Hz	Minimal frequency
fmax	900[MHz]	9E8 Hz	Maximum frequency
er	3.55	3.55	Dielectric constant of RO...
tanD	0.0021	0.0021	Lost tanget of RO4003
hs	32[mil]	8.128E-4 m	Thickness of substrat
th	35[um]	3.5E-5 m	Thickness of metal
W	114.49[mm]	0.11449 m	Width of patch
L	7.4[cm]	0.074 m	Length of patch
Wf	1.92[mm]	0.00192 m	Width of feed line
Lf	112.25[mm]	0.11225 m	Length of feed line
y0	24.13[mm]	0.02413 m	Matching distance
t1	2.75[mm]	0.00275 m	Gap
A	3*L/2+(Lf-y0)	0.19912 m	Length of substrat
B	2*W	0.22898 m	Width of substrat
PML	0.15*lamr	0.051807 m	PML thickness

Рисунок 4.7 – Встановлення параметрів моделювання

Після цього переходимо до вкладки Geometry та додаємо елемент Block (рис.4.8), який буде використовуватися для створення моделі субстрату. Цей геометричний елемент задає об’єм діелектричного шару антени та визначає його основні розміри відповідно до попередньо встановлених параметрів.

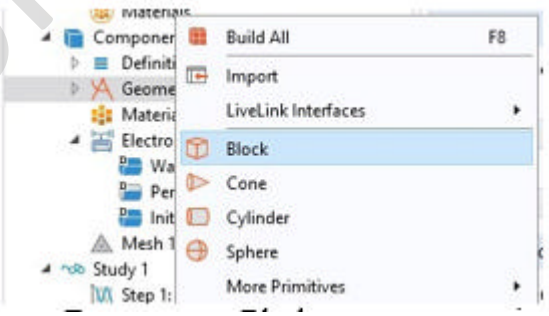


Рисунок 4.8 – Додавання «Block» до геометрії

Після створення геометричного елемента необхідно задати для нього відповідні параметри. Для цього до створеного об’єкта Block додаються значення розмірів, що відповідають параметрам субстрату, визначеним раніше.

Встановлення цих параметрів дозволяє точно задати геометричні

КбПЗ_2026

характеристики моделі та забезпечує відповідність створеної структури розрахованим розмірам антени (рис. 4.9).

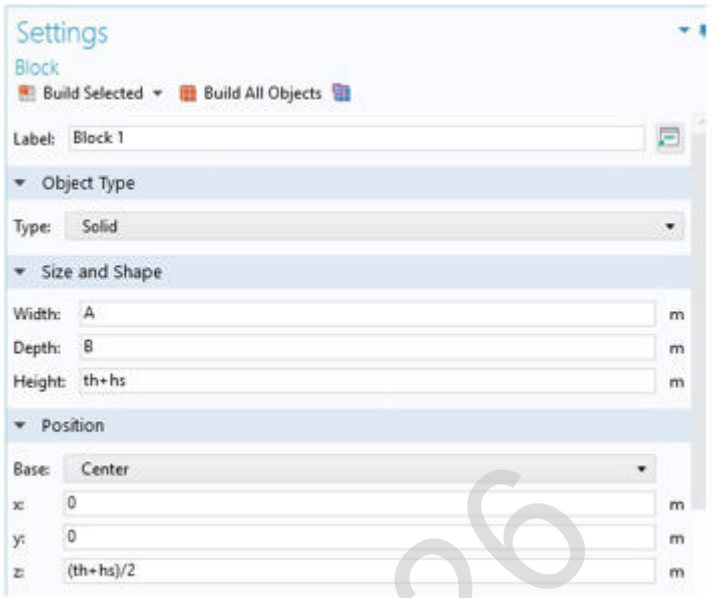


Рисунок 4.9 – Встановлення параметрів до «Block»

Далі додаємо новий шар, який буде відповідати металевому покриттю антени, та задаємо для нього параметр товщини металу (рис. 4.10). Це дозволяє коректно змоделювати провідний шар патча, враховуючи його реальну фізичну товщину, що впливає на електромагнітні характеристики антени.

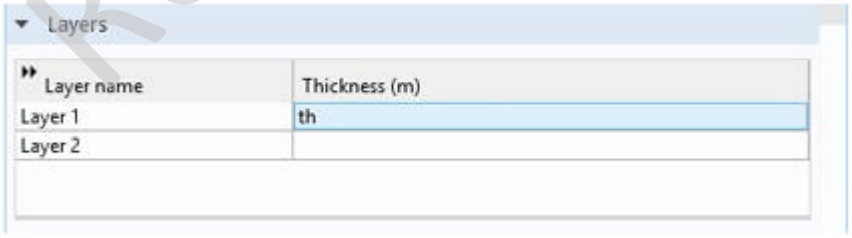


Рисунок 4.10 – Встановлення параметрів до шару

Сформована у результаті виконаних дій геометрична модель антени представлена на рис. 4.11. Вона відображає основні конструктивні елементи антени, включаючи субстрат, металевий патч та інші складові, що були створені на попередніх етапах моделювання.

КОПЗ_2026

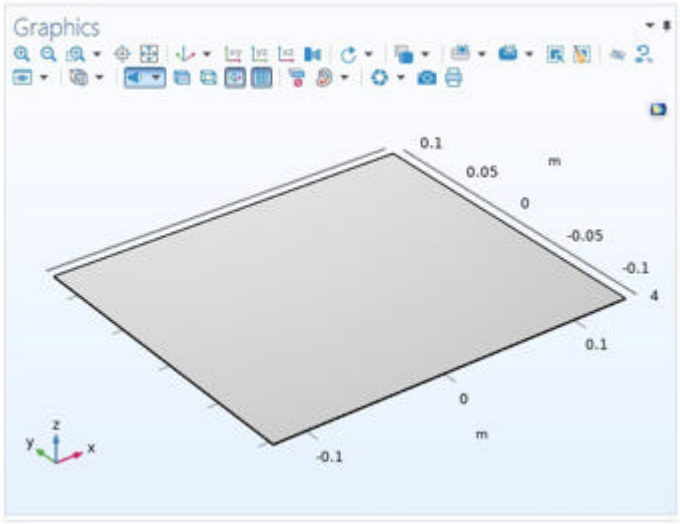


Рисунок 4.11 – Результат моделювання «Block»

Після цього знову переходимо до вкладки Geometry та додаємо елемент Work Plane (рис. 4.12), який буде використовуватися для побудови геометрії патча та лінії живлення антени.

Робоча площина дозволяє створювати двовимірні елементи, на основі яких формуються основні провідні частини антени, зокрема сам патч та мікросмужкова лінія живлення.

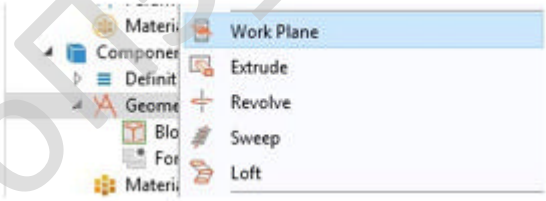


Рисунок 4.12 – Додавання «Work Plane» до геометрії

Далі необхідно задати координати створеної робочої площини таким чином, щоб вона була розташована над об’єктом «Block», який представляє субстрат.

Таке розміщення площини дозволяє коректно побудувати геометрію патча та лінії живлення безпосередньо на поверхні субстрату, що відповідає реальній конструкції мікросмужкової антени.

Для даної антени за замовчуванням розрахунок виконується ітераційним

КОПЗ_2026

методом (Iterative), який потребує значних обчислювальних ресурсів. Тому доцільно використати прямий метод (Direct), що дозволяє підвищити стабільність обчислень та отримати результат швидше для даної моделі.

Результат проведеної симуляції на частоті 870 МГц представлений на рис. 4.13.

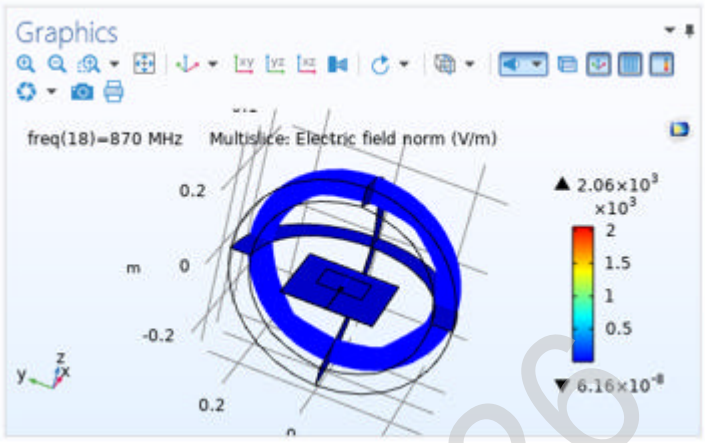


Рисунок 4.13 – Результат симуляції на частоті 900 МГц

Після цього переходимо до вкладки 3D Far Field, де відображається результат моделювання випромінювання антени у дальньому полі. У цьому режимі можна проаналізувати просторову діаграму спрямованості антени та оцінити її характеристики випромінювання.

Результат симуляції на частоті 870 МГц представлено на рис. 4.14.

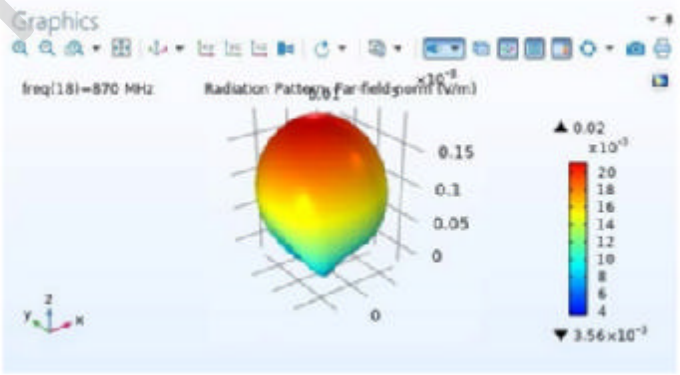


Рисунок 4.14 – Результат симуляції 3D Far Field на частоті 870 МГц

Як видно з рисунка, на частоті 870 МГц антена демонструє хороші

КПІ_2026

характеристики випромінювання у режимі дальнього поля, що свідчить про її придатність для роботи в цьому частотному діапазоні.

Для портальних зчитувачів доцільніше використовувати патч-антени з круговою поляризацією, оскільки вони забезпечують більш стабільне зчитування RFID-міток незалежно від їх орієнтації, на відміну від антен з лінійною поляризацією. З цієї причини у системі було застосовано чотири антени UHF Advantenna-p33 разом із UHF-зчитувачем ID ISC.LRU (рис. 4.15).



Рисунок 4.15 – UHF-зчитувач ID ISC.LRU (а) і антена UHF Advantenna-p33

Антени встановлюються безпосередньо у проході по обидва боки воріт. На кожній стороні розміщується по дві RFID-антени, одна над іншою. Таке розташування дозволяє підвищити ймовірність успішного зчитування всіх RFID-міток, що потрапляють у зону дії системи, оскільки мітки на товарах розміщені не впорядковано, а хаотично. Схему розміщення антен наведено на рисунку нижче.

Антени закріплюються безпосередньо на стінах проходу. Для забезпечення повного перекриття зони сканування передбачена можливість регулювання кута їхнього нахилу відносно одна одної як по вертикалі, так і по горизонталі. Це дозволяє оптимально налаштувати область зчитування.

Оскільки товар у фурі може розміщуватися на висоті до 3 метрів від рівня землі, у розрахунках (рис. 4.16 – схема розміщення антен) прийнято такі значення параметрів:

- X = 40 см;
- Y = 300 см;

КПІЗ_2026

- $Y_1 = Y / 4 = 75$ см;
- $Y_2 = Y / 2 = 150$ см.

При цьому ширина воріт становить 400 см, а ширина зони сканування - 320 см, що забезпечує ефективне зчитування RFID-міток під час проходження транспорту або переміщення вантажу через портал.

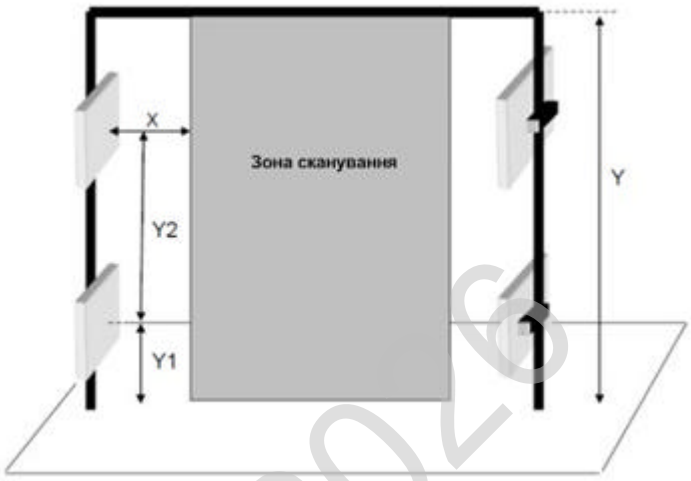


Рисунок 4.16 – Розміщення антен у портальному зчитувачеві

4.1 Розробка блок-схем та опис алгоритмів функціонування системи

Алгоритм роботи автоматизованої системи контролю доступу на основі технології радіочастотної ідентифікації описує послідовність дій, які виконуються для ідентифікації користувача, перевірки прав доступу, прийняття рішення та керування виконавчими пристроями. Система працює у безперервному режимі, забезпечуючи контроль доступу персоналу до об’єктів підприємства.

Робота системи починається з подачі живлення та запуску програмного забезпечення мікроконтролера і серверної частини. На етапі ініціалізації здійснюється налаштування всіх компонентів системи, включаючи RFID-зчитувач, контролер, інтерфейси зв’язку, виконавчі механізми та підключення до серверу. Також перевіряється працездатність обладнання та готовність системи до роботи.

КБПЗ 2026

Після успішної ініціалізації система переходить у режим очікування. У цьому режимі RFID-зчитувач постійно контролює наявність RFID-картки у зоні дії. При піднесенні картки зчитувач виконує її ідентифікацію та зчитує унікальний код, який передається до контролера.

Контролер отримує ідентифікаційні дані та формує запит до серверної частини системи. Сервер виконує обробку отриманого запиту, що включає перевірку наявності користувача в базі даних, аналіз прав доступу, перевірку часових обмежень та відповідності доступу до конкретної зони. На основі цих параметрів формується рішення щодо дозволу або заборони доступу.

У випадку позитивного рішення сервер передає сигнал дозволу контролеру. Контролер, у свою чергу, активує виконавчі пристрої, такі як турнікет, шлагбаум або електромагнітний замок, забезпечуючи фізичний доступ користувача до об’єкта. Додатково система може подавати світловий або звуковий сигнал про успішну авторизацію.

Якщо доступ заборонено, система формує відповідне повідомлення, а також може активувати сигнал тривоги або зафіксувати підозрілу подію. У цьому випадку виконавчі пристрої залишаються у закритому стані.

Паралельно з процесом прийняття рішення система виконує реєстрацію події. У базі даних фіксується інформація про користувача, час доступу, місце проходу та результат перевірки. Це дозволяє вести журнал подій і здійснювати подальший аналіз.

Після завершення обробки запиту система повертається у режим очікування та готова до обробки наступного запиту. Такий циклічний принцип роботи забезпечує безперервний контроль доступу та високу швидкість реагування системи.

Додатково система підтримує функції адміністрування, що включають реєстрацію нових RFID-карток, зміну прав доступу, перегляд журналів подій та налаштування параметрів роботи. Ці операції виконуються через робочу станцію адміністратора та взаємодіють із серверною частиною системи.

КБПЗ_2026

Таким чином, алгоритм роботи системи забезпечує повний цикл функціонування - від зчитування RFID-картки до прийняття рішення та керування доступом, що дозволяє ефективно організувати контроль на підприємстві, підвищити рівень безпеки та автоматизувати процеси управління доступом.

Алгоритм функціонування системи наведено на рисунку 4.17.

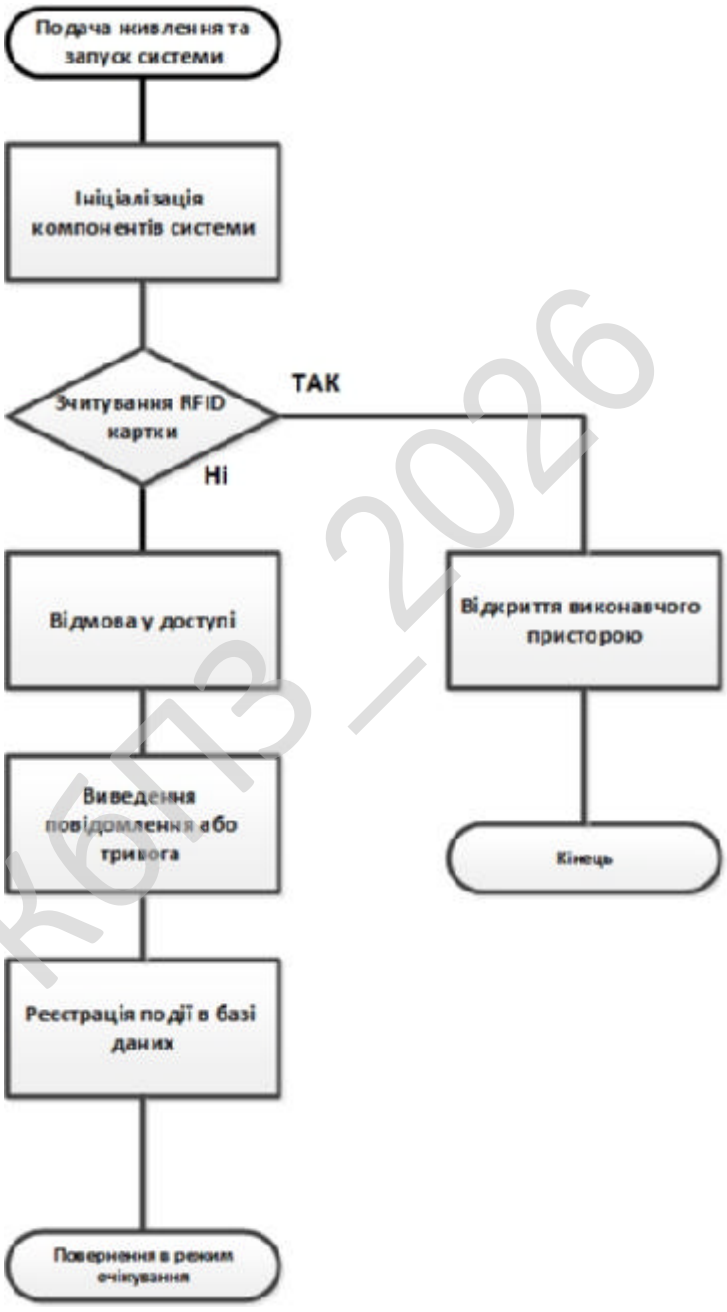


Рисунок 4.17 – Загальний алгоритм функціонуваня системи

КПЗ_2026

Алгоритм роботи контролера програмного забезпечення в системі контролю доступу на основі технології RFID визначає послідовність дій, які виконує контролер для обробки запитів доступу, взаємодії з сервером та керування виконавчими пристроями. Контролер є ключовим елементом системи, який забезпечує оперативне прийняття рішень та стабільну роботу всієї інфраструктури доступу. Робота алгоритму починається з моменту отримання запиту на перевірку доступу. Такий запит формується RFID-зчитувачем після зчитування унікального ідентифікатора RFID-картки користувача. Контролер приймає цей ідентифікатор та ініціює процес обробки. На етапі обробки запиту контролер виконує попередній аналіз даних, перевіряє коректність отриманого коду та визначає подальший сценарій обробки. У разі необхідності контролер може звернутися до серверної частини системи для отримання актуальної інформації про користувача.

Далі виконується перевірка наявності користувача у базі даних. Якщо користувач не знайдений, система формує відмову у доступі. У цьому випадку контролер може активувати сигналізацію, зафіксувати подію у журналі та повернутися у режим очікування. Якщо користувача знайдено, контролер переходить до перевірки прав доступу. На цьому етапі аналізуються такі параметри, як рівень доступу, дозволені зони, часові обмеження та інші політики безпеки. Це дозволяє визначити, чи має користувач право на доступ до конкретного об’єкта. У разі дозволу доступу формується відповідний керуючий сигнал. Контролер активує виконавчі пристрої, такі як турнікет, шлагбаум або електромагнітний замок.

Додатково може здійснюватися індикація (світлова або звукова) для підтвердження успішного проходу. Якщо доступ заборонено, контролер формує сигнал відмови. У цьому випадку система може відобразити повідомлення про відмову, активувати звуковий сигнал або передати інформацію до системи безпеки.

КПЗ–2026

Після прийняття рішення формується відповідь на запит, яка може передаватися до інших компонентів системи або відображатися користувачу. Одночасно відбувається реєстрація події у базі даних, що дозволяє вести облік доступу та аналізувати історію подій.

Завершальним етапом алгоритму є повернення контролера у режим очікування. У цьому режимі система готова до обробки наступного запиту, що забезпечує безперервність роботи та оперативне реагування на дії користувачів.

Таким чином, алгоритм роботи контролера охоплює повний цикл обробки запиту доступу - від отримання ідентифікаційних даних до прийняття рішення та керування виконавчими механізмами, забезпечуючи надійність, безпеку та ефективність функціонування системи контролю доступу на підприємстві.

КБПЗ_2026

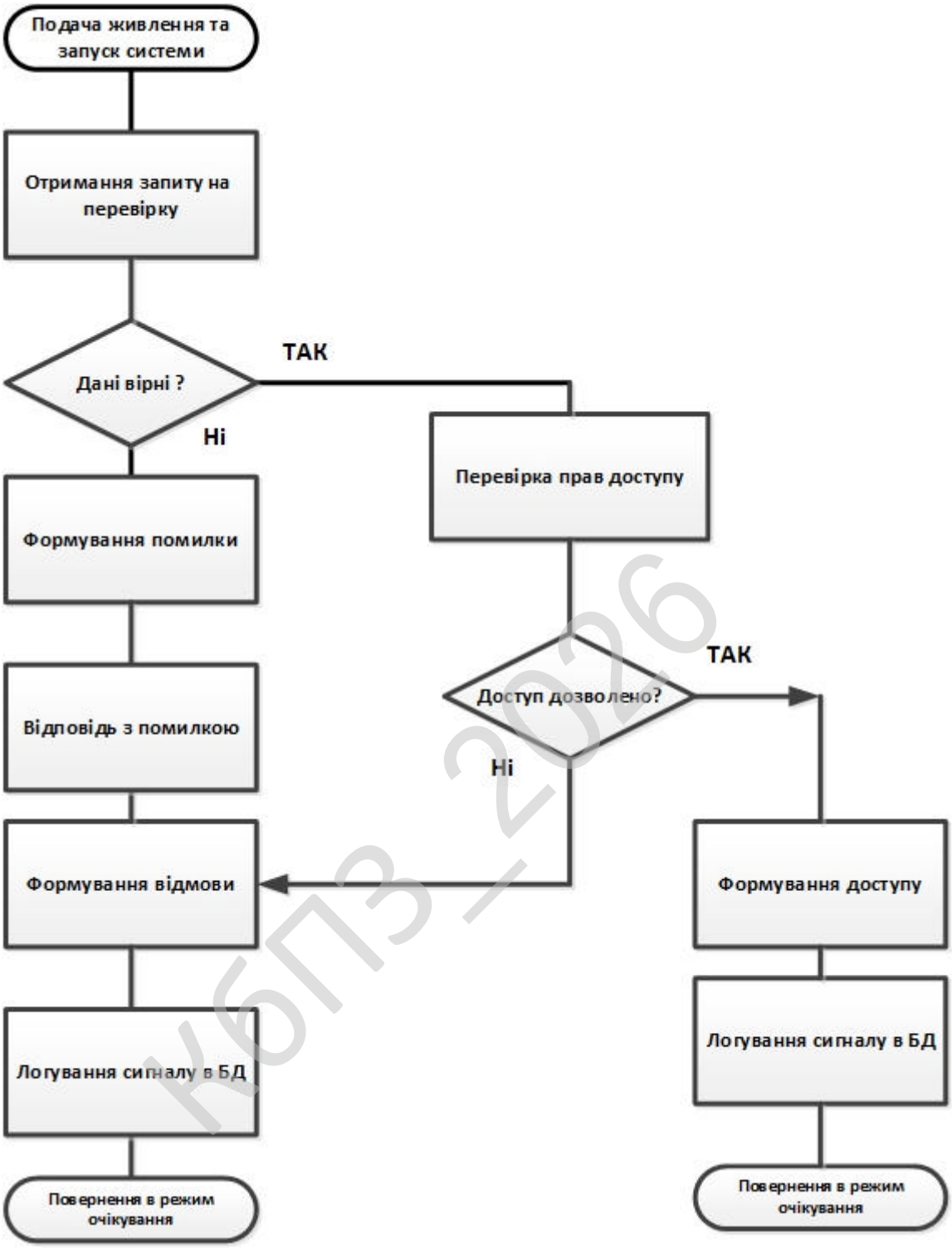


Рисунок 4.18 - Алгоритм роботи програмного забезпечення мікроконтролера

КбПЗ_2026

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Вибір транспондерів

RFID-мітки складаються з двох основних елементів - антени та мікрочіпа. Розміри антен міток, що працюють у зоні дальнього поля (far field), визначаються насамперед розмірами самої антени. Антена виконує роль резонатора та має певний вхідний імпеданс, що забезпечує ефективніше випромінювання і приймання сигналу, а також полегшує узгодження та передачу потужності між антеною і електронною схемою, підключеною до неї. У зв'язку з цим компактність RFID-міток значною мірою залежить саме від розмірів антени, які зазвичай у багато разів перевищують розміри мікрочіпа і фактично визначають габарити мітки.

Сучасні RFID-транспондери мають широкий діапазон вартості: від кількох центів для простих пасивних міток лише для зчитування до кількох сотень доларів США для активних міток із власним джерелом живлення та можливістю ідентифікації на великій відстані. На собівартість транспондера впливають характеристики кремнієвого чіпа, антени та матеріалу підкладки. Вага таких міток може становити приблизно до одного грама, оскільки вони складаються з невеликого кремнієвого чіпа та тонкої антени, розміщеної на лавсановій підкладці. Дальність зчитування RFID-міток залежить від їхнього типу: для міток ближнього поля вона становить від 0,02 до 1 метра, для міток дальнього поля - до 15 метрів, а для активних міток високого класу може досягати 300 метрів. Більшість антен таких міток виготовляються з гнучких матеріалів [12].



Рисунок 5.1 – RFID-етикетка ZBR2000

КПЗ_2026

Щодо міток, які використовуються співробітниками у системі контролю та управління доступом (СКУД), було обрано транспондери у вигляді пластикових карток-пропусків. Для реалізації системи застосовано безконтактні картки стандарту EM-MARINE товщиною 0,8 мм, оснащені чіпом ORIGINAL EM4200, що працюють на частоті 125 кГц (рис. 5.2).

Дані картки мають компактні розміри, зручні у використанні та забезпечують надійну ідентифікацію користувачів при проходженні через систему контролю доступу. Товщина 0,8 мм відповідає стандартним параметрам пластикових карт, що дозволяє легко носити їх у гаманцях або спеціальних тримачах. Використання стандарту EM-MARINE забезпечує сумісність карток із більшістю поширених RFID-зчитувачів, які працюють у діапазоні 125 кГц.



Рисунок 5.2 – Безконтактна картка EM-MARINE 0,8 мм (ЧІП ORIGINAL EM4200)

Безконтактна картка з оригінальним чіпом EM4200 має ідентифікатор обсягом 40 біт та призначена виключно для зчитування інформації (read-only). У картці використовується вдосконалена квадратна антена, що дозволяє збільшити відстань зчитування до 10 см.

Картка виготовлена у вигляді білої ПВХ-пластини товщиною 0,8 мм. Завдяки гладкій ламінованій поверхні з обох боків на неї можна наносити якісні графічні зображення та текст, що дає можливість виконувати персоналізацію карток або наносити елементи брендування.

Основні характеристики картки:

- розміри: 86 × 54 × 0,8 мм;

КбПЗ-2026

- стандарт: ISO 18000-2;
- робоча частота: 125 кГц;
- діапазон робочих температур: від –30 °С до +70 °С.

Як транспондери, призначені для підвищення безпеки співробітників під час роботи з транспортними засобами на території підприємства, було обрано мітки-браслети SafeTags (рис. 5.3), розроблені компанією Kinexon. Такі браслети дозволяють відстежувати місцезнаходження працівників у режимі реального часу та допомагають зменшити ризик травмування при взаємодії з технікою.



Рисунок 5.3 – SafeTag у вигляді браслету

КбПЗ_2026

Даний транспондер оснащений системою візуальної та звукової сигналізації, яка спрацьовує у випадку, коли працівник наближається до транспортного засобу на небезпечну відстань. Це дозволяє своєчасно попередити можливі небезпечні ситуації та зменшити ризик травмування персоналу.

Крім того, пристрій має кнопку вимкнення, яка використовується водіями для деактивації сигналізації під час початку керування транспортним засобом. Безпечну відстань між працівником і технікою можна налаштовувати з точністю до 10 см, що забезпечує гнучке налаштування системи відповідно до умов роботи.

Транспондер працює автономно та не потребує підзарядки протягом

Вибір програмного забезпечення

Для системи управління складом (WMS) необхідне програмне забезпечення, яке може інтегруватися з уже існуючою архітектурою системи, працювати з базою даних та підтримувати функції інвентаризації. З огляду на ці вимоги було обрано платформу Zebra MotionWorks Enterprise. Це інноваційне рішення дозволяє підприємствам перетворювати дані про місцезнаходження активів у корисну аналітичну бізнес-інформацію.

Платформа здійснює збір, обробку та аналіз даних, що надходять від RFID-міток, прикріплених до об’єктів. Після обробки ця інформація передається до єдиної інтегрованої консолі управління, яка забезпечує оперативне отримання точних даних про місцезнаходження та стан кожного об’єкта.

MotionWorks Enterprise є локальним корпоративним програмним забезпеченням для серверів і надає базові інструменти для розгортання та управління мережею датчиків, збору та обробки даних, а також формування повідомлень про події, пов’язані з виявленням і переміщенням об’єктів. Система також підтримує формування звітів, передачу потоків даних і використання API для інтеграції з іншими системами. Крім того, вона забезпечує роботу з картами, моніторингом датчиків і міток, а також ведення обліку та відстеження корпоративних ресурсів підприємства.

Для реалізації системи контролю та управління доступом (СКУД) було обрано програмне забезпечення ZKTeco Access 3.5 (рис. 5.4), яке також підтримує функції обліку робочого часу персоналу. Даний програмний продукт спеціально розроблений для управління контролерами та терміналами ZKTeco і дозволяє виконувати адміністрування системи доступу, а також формувати різноманітні звітні документи.

КБПЗ–2026



Рисунок 5.4 – Головне вікно ПЗ ZKTeco Access 3.5

Основні характеристики програмного забезпечення ZKTeco Access 3.5:

- значний технічний ресурс, що дозволяє керувати системою контролю доступу для до 30 000 користувачів з можливістю підключення до 100 пристроїв стандартної конфігурації;

- висока продуктивність та розширений функціонал;

- автоматичне керування списками користувачів;

- багаторівнева система управління, заснована на ролях, що забезпечує належний рівень захисту даних користувачів.

Системні вимоги програмного забезпечення:

- процесор (CPU): частота 2.0 ГГц або вище;

- оперативна пам’ять: 1 ГБ або більше;

- накопичувач: не менше 10 ГБ вільного місця на жорсткому диску.

Для забезпечення безпеки працівників під час роботи з транспортними засобами використано програмне забезпечення KINEXON SafeZone (рис. 5.5). Це рішення дозволяє контролювати відстань між працівниками та технікою, попереджати небезпечні ситуації та підвищувати рівень безпеки на території підприємства.

КОПЗ_2026

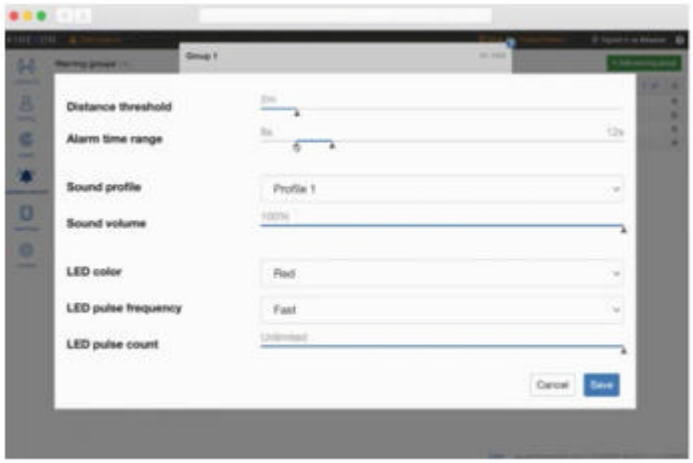


Рисунок 5.5 – Вікно налаштувань транспондера у ПЗ KINEXON SafeZone

Існує можливість інтеграції KINEXON SafeZone безпосередньо в наявну IT-інфраструктуру підприємства. Система може розгортатися як локально, так і в хмарному середовищі Amazon, що забезпечує простий і швидкий доступ до програмного забезпечення.

При цьому використання рішення не потребує додаткової інфраструктури, що значно спрощує процес впровадження. Такий підхід дозволяє швидко інтегрувати систему у вже існуючі IT-процеси підприємства та забезпечує гнучке масштабування рішення для подальшого застосування в інших підрозділах або сферах діяльності.

КбПЗ_2026

6 ОСНОВНІ ВИСНОВКИ

Технологія радіочастотної ідентифікації (RFID) набула широкого застосування для автоматизації різних виробничих процесів, зокрема моніторингу виробництва, систем контролю та управління доступом до приміщень (СКУД), забезпечення охорони праці, а також управління ланцюгами постачання.

Об’єктом автоматизації обрано склад споживчих товарів. Для підвищення ефективності його роботи було розроблено пасивну надвисокочастотну (НВЧ) RFID-систему, яка працює відповідно до стандарту ISO 18000-6C у частотному діапазоні 860–960 МГц.

Запропоновану систему умовно поділено на три основні складові:

1. Система управління складом (WMS – Warehouse Management System).
2. Система контролю та управління доступом (СКУД).
3. Система забезпечення безпеки праці, спрямована на попередження травмування працівників під час роботи з транспортними засобами (навантажувачами, візками тощо).

Для реалізації спроєктованої системи було підібрано необхідні апаратні компоненти, загальна вартість яких становить 1 172 791 грн. Доцільність використання патч-антен була підтверджена шляхом розрахунку та моделювання антени у програмному середовищі Comsol Multiphysics.

Розроблена система відповідає вимогам безпеки та конфіденційності даних, а також може бути інтегрована в існуючу мережеву інфраструктуру підприємства.

Сутність запропонованого проєкту полягає у впровадженні RFID-технології для автоматизації роботи бібліотеки. Для цього також пропонується використання пасивної НВЧ RFID-системи, що працює за стандартом ISO 18000-6C у діапазоні 860–960 МГц.

Вартість обладнання для реалізації одного типового рішення становить

КОПЗ_2026

258,424 тис. грн, а націнка за впровадження та технічну підтримку - 50 тис. грн. Для забезпечення окупності початкових інвестицій необхідно залучити щонайменше 6 клієнтів. У разі налагодження довгострокової співпраці з виробниками апаратних компонентів можливе зниження вартості комплектуючих, що дозволить зменшити загальну вартість рішення та підвищити його конкурентоспроможність.

КБПЗ_2026

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Koval V., Adamiv O., Proc. of the Third IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2005). – Sofia (Bulgaria). – 2005. – P. 120- 124.

2. Yasin, J.N., Mohamed, S.A.S., Haghbayan, MH. et al. Low-cost ultrasonic based object detection and collision avoidance method for autonomous robots. Int. j. inf. tecnol. 13, 97–107 (2021). https://doi.org/10.1007/s41870-020-00513-w.

3. Sabry F. Self Driving Car: Solving Full Self-driving Need Solving Real-world artificial Intelligence. One Billion Knowledgeable. 2022 . 293 p.

4. Shapiro D. G. Three Anecdotes from the DARPA Autonomous Land Vehicle Project. AI Magazine, 2008. 29(2), 40. https://doi.org/10.1609/aimag.v29i2.2108.

5. Young R. Critical Analysis of Prototype Autonomous Vehicle Crash Rates Six Scientific Studies from 2015-2018 SAE International. 2021. 252 p.

6. Рудик А. В. Наукові основи та принципи побудови приладової системи вимірювання прискорення мобільного робота : дис. ... д-ра техн. наук : 05.11.01– Прилади та методи вимірювання механічних величин. Київ, 2018. – 460 с.

7. Поліщук М. М., Ткач М.М. Робототехнічні системи: проектування і моделювання: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2021. 112 с.

8. Мигаль В. Д. Інтелектуальні системи в технічній експлуатації автомобілів: монографія. Х.: Майдан, 2018. 262 с.

9. Staron M. Automotive Software Architectures: An Introduction. Second Edition Springer International Publishing A&G. 2022. 274 p.

10. Vargas J. et al. An Overview of Autonomous Vehicles Sensors and Their Vulnerability to Weather Conditions. Sensors. 2021; 21(16):5397.

11. Wevolver 2020 Autonomous Vehicle Technology Report. URL:https://www.coursehero.com/file/62601304/Wevolver2020AutonomousVehicechnologyReportpdf/

КПІ – 2026

12. React.js [Електронний ресурс] – Режим доступу до ресурсу: https://https://uk.reactjs.org/

13. AngularJS MVC [Електронний ресурс] – Режим доступу до ресурсу: https://www.tutorialspoint.com/angularjs/angularjs_mvc_architecture.htm.

14. Vue.js [Електронний ресурс] – Режим доступу до ресурсу: https://vuejs.org/

15. A Look Inside ADAS Modules. URL: https://amkor.com/semiconductor-story/alook.

16. AV and ADAS Sensors. URL https://community.sw.siemens.com/s/article/AVand- ADAS-Sensors.

17. Гуржій А. М. Основи автоматики та робототехніки: Навчальний посібник/ А.М. Гуржій, А. Т. Нельга, В. М. Співак, О. С. Ітякін:–Дніпро:«Гарант СВ», 2021.- 243с.

18. Lim, B.S. et al. Autonomous Vehicle Ultrasonic Sensor Vulnerability and Impact Assessment. In Proceedings of the IEEE World Forum on Internet of Things (WFIoT), Singapore, 5–8 February 2018; pp. 231–236.

19. Саліхов М. М. Arduino – перспективний інструмент протитопування у робототехніці // Концептуальні шляхи розвитку науки та освіти: матеріали VIII Міжнародної науково-практичної конференції м. Львів, 9-10 червня 2023 року.– Львів: Львівський науковий форум, 2023. – с. 73-79.

20. Bräunl T. Embedded Robotics: From Mobile Robots to Autonomous Vehicles with RaspberryPi and Arduino Springer Nature, 2022. 519 p.

21. Навігаційні системи [Електронний ресурс] : навч. посіб. для студ. Спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» / С.Л. Лакоза; КПІ ім. Ігоря Сікорського, 2021. — 80 с.

22. Imad M. et al. Navigation system for autonomous vehicle: A survey. JCSTS., vol. 2, no. 2, pp. 20–35, 2020.

КБПЗ–2026

23. Ковалець І. В. та ін. Технологія планування траєкторій руху мобільних об’єктів з урахуванням перешкод на складній місцевості. Енергетика і автоматика. - 2017. - № 1. - С. 110-122.

24. HTML [Електронний ресурс] – Режим доступу до ресурсу: https://developer.mozilla.org/uk/docs/Web/HTML.

25. Aguilo I. et al. Artificial Intelligence Research and Development Hardcover by IOS Press. 2003. 500 p.

26. Гребенюк Б. А. Розробка підсистеми управлення інтелектуальним роботом / Б. А. Гребенюк // «Automation and Development of Electronic Devices» ADED-2023: Collection of Students' Scientific Paper. – Kharkiv : Kind of Kharkiv National Universitety of Radio Elektronics [electronic edition], 2023. – Part 1. –336p. P. 263-269.

27. MongoDB [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/MongoDB.

28. Becker M. et al Obstacle avoidance procedure for mobile robots. ABCM Symposium series in Mechatronics. Vol. 2, 2006. P. 250-257.

29. CORS, XSS [Електронний ресурс] – Режим доступу до ресурсу: https://dev.to/maleta/cors-xss-and-csrf-with-examples-in-10-minutes-35k3.

30. AJAX [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/AJAX.

31. Fetch API [Електронний ресурс] – Режим доступу до ресурсу: https://developer.mozilla.org/ru/docs/Web/API/Fetch_API

32. Звенігородський О.С. Інтелектуальна система планування тактики руху автономного робота в квазістаціонарному середовищі: Дис... канд. техн. наук: 05.13.23. — Д., 2002. — 127с.

33. Адамів, О.П. Моделі та інтелектуальні засоби адаптивного керування автономним мобільним роботом. Дис. канд.техн. наук. Одеса, 2007. 124 с.

КБПЗ–2026

34. Koval V., Adamiv O., Proc. of the Third IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2005). – Sofia (Bulgaria). – 2005. – P. 120- 124.

35. npm [Електронний ресурс] – Режим доступу до ресурсу: https://www.npmjs.com/

36. Install MongoDB [Електронний ресурс] – Режим доступу до ресурсу: https://docs.mongodb.com/manual/administration/install-on-linux/

37. Node.js [Електронний ресурс] – Режим доступу до ресурсу: https://www.digitalocean.com/community/tutorials/node-js-ubuntu-18-04-ua.

38. Linux [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Linux.

39. npm-audit [Електронний ресурс] – Режим доступу до ресурсу: https://docs.npmjs.com/cli/audit.

40. Kojima T. et al. Intelligent Technology for More Advanced Autonomous Driving. 2018. Hitachi Review Vol. 67, No. 1. p. 58–63.

41. SQL [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/SQL.

42. MongoDB Compass [Електронний ресурс] – Режим доступу до ресурсу: https://www.mongodb.com/products/compass.

43. Postman [Електронний ресурс] – Режим доступу до ресурсу: https://www.postman.com/

44. Саліхов М. М. Від автоматизованих до автономних транспортних засобів // Наукові досягнення та інновації: шлях до успіху. X Всеукраїнська мультидисциплінарна науково-практична Інтернет-конференція, 31 травня 2023, Україна, Київ : зб. матеріалів — Електрон. дан. — Київ : Ярочéнко Я. В., 2023. — с. 136-142.

45. SPA (Single-page application) [Електронний ресурс] – Режим доступу до ресурсу: https://developer.mozilla.org/en-US/docs/Glossary/SPA.

КПІ_2026

46. Саліхов М.М. Самокеровані автомобілі та системи їх навігації// Практичні та теоретичні питання розвитку науки та освіти: матеріали VIII Міжнародної науково-практичної конференції: м. Львів, 19-20 червня 2023 року. – Львів: Львівський науковий форум, 2023. – С.53-59.

47. SPA (Single-page application) [Електронний ресурс] – Режим доступу до ресурсу: https://developer.mozilla.org/en-US/docs/Glossary/SPA

48. Vargas J. et al. An Overview of Autonomous Vehicles Sensors and Their.

49. Vulnerability to Weather Conditions. Sensors. 2021; 21(16):5397.

50.https://www.coursehero.com/file/62601304/Wevolver2020AutonomousVehicec hnologyReportpdf/

КбПЗ_2026