

УДК 004.415.2

А. Ю. СЛОБОДЧУК, В. О. ПОЗНЯКОВ, К. Л. НОЗДРАЧОВА, Н. М. ЮДАНОВА, В. О. ЯКІМЕНКО
ЗАСТОСУВАННЯ СИСТЕМ КОНТРОЛЮ ДОСТУПУ ТА РОЗРОБКА МАКЕТУ ПРИБАДУ НА
ОСНОВІ RFID ТЕХНОЛОГІЇ

Розглянуто основні положення систем контролю і управління доступом (СКУД), сфери діяльності та способи застосування. Описана структурна схема систем СКУД. Наведено можливості застосування RFID технології, класифікація RFID міток та подальший їх розвиток, переваги і недоліки радіочастотної ідентифікації та їх багатопільове використання. Виділено основні міжнародні стандарти в області RFID. Сконструйовано, простіший з існуючих, макет основної частини системи контролю доступу на основі RFID. Проведено порівняльний аналіз сучасних аналогів даного пристрою. Виділено різноманітні пристрої схожі за принципом дії, на основі яких запропоновано вдосконалення даного пристрою. Представлені структурна та принципова схеми, а також алгоритм роботи розробленого макету приладу на основі RFID технології.

Ключові слова: система контролю доступу, RFID мітка, зчитувач, ID картка, прилад.

А. Ю. СЛОБОДЧУК, В. О. ПОЗНЯКОВ, Е. Л. НОЗДРАЧОВА, Н. Н. ЮДАНОВА, В. А. ЯКІМЕНКО
ПРИМЕНЕНИЕ СИСТЕМ КОНТРОЛЯ ДОСТУПА И РАЗРАБОТКА МАКЕТА ПРИБОРА
НА ОСНОВЕ RFID ТЕХНОЛОГИИ

Рассмотрены основные положения систем контроля и управления доступом (СКУД), сферы деятельности и способы применения. Описана структурная схема систем СКУД. Приведены возможности применения RFID технологии, классификация RFID меток и дальнейшее их развитие, преимущества и недостатки радиочастотной идентификации, и их многоцелевое использование. Выделены основные международные стандарты в области RFID. Сконструирован, проще из существующих, макет основной части системы контроля доступа на основе RFID. Проведен сравнительный анализ современных аналогов данного устройства. Выделены различные устройства, схожие по принципу действия, на основе которых предложено совершенствование данного устройства. Представлена структурная и принципиальная схемы, а также алгоритм работы разработанного макета прибора на основе RFID технологии.

Ключевые слова: система контроля доступа, RFID метка, считыватель, ID карта, прибор.

A. Yu. SLOBODCHUK, V. O. POZNYAKOV, K. L. NOZDRACHOVA, N.M. YUDANOVA, V.O. YAKIMENKO
APPLICATION OF ACCESS CONTROL SYSTEMS AND DEVELOPMENT OF DEVICE MODEL
BASED ON RFID TECHNOLOGY

The purpose of this work is to understand, to some extent, the performance of RFID based access systems, where they are used and what they are needed for. The basic provisions of access control and management systems, areas of activity and methods of application are considered. The structural diagram of access control systems is described. The possibilities of using RFID technology, the classification of RFID tags and their further development, the advantages and disadvantages of radio frequency identification and their multi-use are given. Highlighted the main international standards in the field of RFID. Designed, simpler from the existing ones, the layout of the main part of the RFID-based access control system. A comparative analysis of modern analogues of this device. Various devices are identified that are similar in principle of operation, on the basis of which the improvement of this device is proposed. The structural and circuit diagrams, as well as the algorithm of the developed device layout based on RFID technology, are presented.

Keywords: access control system, RFID tag, reader, ID card, device.

Вступ. На даний час розвиток технологій має величезне значення у побуті людини, що, в першу чергу, впроваджує технології у сьогоденні для зручності життя. Найпоширеніша технологія на сьогоднішній день зв'язана з зчитувальними пристроями, що застосовуються у різних сферах діяльності. Системи зчитування розділяються на різноманітні види, в залежності від сфери використання. Наприклад, підприємствам, які мають велику кількість кадрів, потрібно вести облік робочого часу, слідкувати за входом та переміщенням по території підприємства, та у певній мірі підтримувати безпеку певних ділянок підприємства. Як правило в таких ситуаціях впроваджують систему контролю доступу. Таким чином система охоплює великий об'єм робіт, на опрацювання яких було потрібно велика кількість часу та персоналу. Це дає змогу не тільки зменшити витрати, а також скоротити час на опрацювання даних та полегшити роботу діючому персоналу. Також система регулює доступ до різних приміщень, за наявності спеціальних карт, тому ризик потрапляння сторонніх осіб значно зменшується.

Основні положення. Система контролю і управління доступом (скорочено СКУД або СКД) – це комплекс технічних та програмних засобів безпеки, що здійснює регулювання входу / виходу та переміщень людей чи транспортних об'єктів на територіях, які знаходяться під охороною, для адміністративного моніторингу та попереджень несанкціонованого проникнення [1].

Основні можливості СКУД – це контроль і управління доступом. Головна функція. Вона дозволяє розділити права доступу співробітників і відмовити в проході небажаним особам. Можлива організація дистанційного керування пристроями для блокування. Можна заборонити прохід співробітникам у вихідні та святкові дні на підприємство, а також після робочої зміни.

Збір і видача статистики. Збір інформації система контролю і управління доступом веде постійно. Хто через яку точку пройшов і скільки разів. По кожному із співробітників можна отримати інформацію: час приходу / відходу, спроби доступу в

© А. Ю. Слободчук, В. О. Позняков, К. Л. Ноздрачова,
 Н. М. Юданова, В. О. Якіменко, 2019

заборонені зони і приміщення, спроби проходу в заборонений час. Можна відстежити, як співробітник переміщається по території, коли проходить СКУД зчитувачі. Всі виявлені дисциплінарні порушення можна занести до особової справи працівника, а керівництво порушника буде проінформовано належним чином.

Доступ співробітників лише з електронними перепустками. Працівник, проходячи через пункт пропуску, ідентифікує себе картою, і на екрані монітора охорони може виводитися інформація про співробітника і фотографія теж. Це виключить можливість проникнення під чужим ідентифікатором. У правилах реакції СКУД можна блокувати повторний вхід через пункт пропуску на підприємство по одній карті доступу протягом короткого проміжку часу.

Облік робочого часу. СКУД дозволяє вести облік робочого часу, базуючись на оцінках приходу і відходу зі свого робочого місця людей. В результаті можна обчислити сумарний робочий час співробітника з урахуванням «перекурів», обідів та ін. А на початку робочого дня вона може формувати звіт про працівників, які не пройшли контрольну точку в зазначений час, що дозволить виявити тих, хто запізнився або які не вийшли на роботу. За аналогією можна створити звіт і в кінці робочої зміни.

Автономність роботи системи. Оснащена безперебійним живленням, СКУД не припинить свою роботу при централізованому відключенні електрики. Крім того, завдяки функціоналу контролера, вона може продовжувати роботу і при зупинці керуючого комп'ютера.

Охорона в реальному часі. Система контролю управління доступом СКУД надає можливість знімати і ставити певні приміщення під охорону. І можна отримувати відомості в реальному часі про позаштатних ситуаціях через організовану систему оповіщення через відповідальних осіб. А також тривожні події фіксуються в базі, що дозволить переглянути цю інформацію пізніше.

Співробітник охорони, завдяки засобам СКУД, може, не сходячи з робочого місця, управляти турнікетами і дверима, подавати сигнали тривоги. Досить помістити в його комп'ютер поверхові плани будівлі і схеми розташування контрольних точок.

Управління через Інтернет або з мобільного телефону. При підключенні СКУД до всесвітньої мережі адміністрація може дистанційно керувати системою і контролювати її роботу.

Інтеграція з іншими системами. Пожежна, охоронна сигналізація, відео спостереження прекрасно інтегруються з СКУД. Інтеграція з відео спостереженням забезпечує візуальний контроль над зоною, що охороняється. І дозволяє в найкоротші терміни виявити, по можливості ідентифікувати і заблокувати порушника.

Поєднання з охоронною сигналізацією дозволяє налаштувати спільне реагування на несанкціоноване проникнення. Так можна змусити спрацювати сирену у охорони в кабінеті, запалити тривожну лампу або

просто заблокувати двері в потрібній частині підприємства.

Інтеграція з пожежною сигналізацією життєво необхідна. Це дозволить автоматично розблокувати всі контрольні точки при пожежі. Що істотно спростить евакуацію працівників у критичний період[2].

Впровадження СКУД дозволяє організувати безпеку та контроль об'єктів без залучення великої кількості працівників охорони та стабільну роботу автоматизованих систем у режимі 24/7 (наприклад, банкоматів, які встановлено в окремих приміщеннях відділень)[1].

Обладнання та принцип роботи.

1) Перегороджуючі пристрої.

– встановлюються на двері: електрозащипки; електромагнітні замки; електромеханічні замки;
– встановлюються на проходах / проїздах: шлюзові кабінети; ворота і шлагбауми.

2) Ідентифікатори. Основні типи виконання –

карточка, брелок, мітка. Є базовим елементом системи контролю доступу, оскільки зберігає код, який служить для визначення прав («ідентифікації») власника. Це може бути Touchmemo, безконтактна карта (наприклад, RFID-мітки), або контактний тип карт із магнітною смугою. В якості ідентифікатора може виступати так само код, що вводиться на клавіатурі, а також окремі біометричні ознаки людини – відбиток пальця, малюнок сітківки або райдужної оболонки ока, тривимірне зображення особи, малюнок капілярних ліній долоні.

Надійність (стійкість до злому) системи контролю доступу в значній мірі визначається типом використовуюваного ідентифікатора: наприклад, найбільш поширені безконтактні карти proximity можуть підробляти в майстернях з виготовлення ключів на обладнанні, що є у вільному продажу. Тому для об'єктів, що вимагають більш високого рівня захисту, подібні ідентифікатори не підходять. Принципово вищий рівень захищеності забезпечують RFID-мітки, в яких код карти зберігається в захищеній області та шифрується.

3) Контролери. Це ключовий елемент системи: саме контролер визначає, пропустити чи ні власника ідентифікатора через точку проходу, оскільки зберігає коди ідентифікаторів зі списком прав доступу кожного з них. Коли людина пред'являє (підносить до зчитувального пристрою) ідентифікатор, зчитаний з нього код порівнюється та зберігається в базі, на підставі чого приймається рішення про відкриття точки проходу. Контролер для своєї роботи вимагає електроживлення, тому контролери, як правило, мають власний акумулятор, який підтримує його працездатність від декількох годин до декількох діб на випадок аварії електромережі.

4) Зчитувачі. Це пристрій, який отримує («зчитує») код ідентифікатора і передає його в контролер. Варіанти виконання зчитувача залежать від типу ідентифікатора: для «таблетки» – це два електричних контакти (у вигляді «лузи»), для proximity-карти – це електронна плата з антеною в

корпусі, а для зчитування, наприклад, малюнка райдужної оболонки очка до складу зчитувача повинна входити телевізійна камера [3].

Сфера використання. 1) Мережеві СКУД. У них всі контролери з'єднані з центральним сервером. Мережеві системи зручні для великих об'єктів (офіси, виробничі підприємства), оскільки керувати навіть десятком дверей, на яких встановлені автономні системи, стає надзвичайно важко. Незамінні мережеві системи в наступних випадках:

- якщо необхідна інформація про події, що відбулися раніше або потрібен додатковий контроль в реальному режимі часу. Наприклад, в мережеві системі існує функція фотоверифікації: на прохідній при піднесенні людиною, що увійшла, ідентифікатора до зчитувача, службовець (вахтер, охоронець) може на екрані монітора бачити фотографію людини, якій в базі даних привласнений даний ідентифікатор, і порівняти із зовнішністю минаючого, що підстраховує від передачі карток іншим людям;

- якщо необхідно організувати облік робочого часу і контроль трудової дисципліни;

- якщо необхідно забезпечити взаємодію (інтеграцію) з іншими підсистемами безпеки, наприклад, відеоспостереженням або пожежною сигналізацією.

У системі мереж з одного місця можна не тільки контролювати події на всій території, що охороняється, а й централізовано керувати правами користувачів, вести базу даних. Мережеві системи дозволяють організувати кілька робочих місць, розділивши функції управління між різними співробітниками і службами підприємства.

У мережевих системах контролю доступу можуть застосовуватися бездротові технології (радіоканали). Використання бездротових мереж найчастіше визначається конкретними ситуаціями: складно або неможливо прокласти дротові комунікації між об'єктами, скорочення фінансових витрат на монтаж точки проходу і т.д. Існує велика

кількість варіантів радіоканалів, проте в СКУД використовуються тільки деякі з них.

- Bluetooth. Даний вид бездротового пристрою передачі даних являє собою аналог Ethernet. Його особливість полягає в тому, що відповідає необхідність прокладати паралельні комунікації для об'єднання компонентів при використанні інтерфейсу RS-485.

- Wi-Fi. Основна перевага даного радіоканалу полягає у великій дальності зв'язку, яка здатна досягати декількох сотень метрів. При цьому скорочуються як тимчасові, так і фінансові витрати на прокладку вуличних комунікацій.

- ZigBee. Спочатку сферою застосування даного радіоканалу була система охоронної та пожежної сигналізації. Дана бездротова технологія працює в не ліцензованому діапазоні 2,45 ГГц.

- GSM. Перевага використання даного бездротового каналу зв'язку – практично суцільне покриття. До основних методів передачі інформації в розглянутій мережі відносяться GPRS, SMS і голосовий канал.

2) Автономні СКУД системи дешевше, простіше в експлуатації, не вимагають прокладки сотень метрів кабелю, використання пристроїв сполучення з сервером, самого сервера. При цьому до мінусів таких систем відноситься неможливість створювати звіти, вести облік робочого часу, передавати й узагальнювати інформацію про події, управлятися дистанційно.

У складі автономної системи контролю доступу використовуються також електронні замки, передають інформацію по бездротових каналах зв'язку: в двері встановлюється механічний замок з електронним управлінням і вбудованим зчитувачем. Замок по радіоканалу пов'язаний з хабом, який вже по проводах обмінюється інформацією з робочою станцією, на якій встановлено програмне забезпечення [3].

Структурна схема і опис систем контролю і управління доступом. Структурна схема СКУД приведена на рис. 1.



Рис. 1 – Структурна схема СКУД

Як ключі-носії ознаки (повна аналогія з ключами в звичайному розумінні цього слова) можуть використовуватись карти різних типів: магнітні, "проксимити", або ж сама людина (як носій індивідуальних біологічних ознак), людська пам'ять, що запам'ятовує набір цифр, котрим є PIN-код (індивідуальний код користувача) і ін.

Для знімання інформації з ключів призначені пристрої ідентифікації. Залежно від типу носія,

природно, змінюються і пристрої ідентифікації. Знімання інформації з будь якого вигляду карт здійснюють спеціальні зчитувачі, які використовують ті або інші фізичні принципи. Для знімання інформації про біологічні ознаки людини використовують спеціальні біометричні зчитувачі (термінали), а PIN-код вводиться з клавіатур різних типів.

Інформація, що знімається з ключів, поступає в процесорний блок – контролер, який її обробляє, аналізує, приймає рішення про можливість проходу. Будь-яка система обов'язково має плату, на якій розміщуються мікропроцесор і інші напівпровідникові елементи. Ця плата розташована в окремому блоці-контролері, або вона вставлена прямо в корпус зчитувача. В кожній з цієї архітектури є свої плюси і мінуси. Архітектура контролера, поєднаного зі зчитувачем, стійкіша до обривів мережі, але і менш захищена від зломів, оскільки блок, що приймає рішення, розташований зовні охоронного приміщення.

СКД може взаємодіяти з персональним комп'ютером. У системах досить великої ємкості комп'ютер, використовуючи спеціалізоване програмне забезпечення, повністю управляє контролерами, збирає, обробляє і архівує інформацію, що поступає з об'єкту, здійснює взаємодію з сигналізацією і охоронним телебаченням.

Найважливішим елементом СКД є периферійне обладнання, оскільки саме воно вступає в безпосередній "фізичний контакт" з користувачем в процесі ідентифікації і аутентифікації його особи.

Для введення ідентифікаторів користувача в СКД застосовуються наступні основні види периферійного устаткування:

- кодонаборні термінали;
- зчитуючі пристрої;
- біометричні термінали; [4].

RFID можливості і застосування. RFID (англ. Radio frequency identification) – радіочастотна ідентифікація.

Радіочастотне розпізнавання здійснюється за допомогою закріплених за об'єктом спеціальних міток, що несуть ідентифікаційну інформацію. Цей метод вже став основою побудови сучасних безконтактних інформаційних систем, і має стійку назву RFID-технології [5].

Особливості технології:

– RFID-міткам не потрібен контакт або пряма видимість, дані з мітки можуть бути отримані на відстані.

– RFID-мітки читаються швидко і точно, що дозволяє виконувати велику кількість сканувань.

– RFID-мітки можна використовувати навіть в агресивних середовищах, через бруд, фарбу, пар, воду, пластмасу, деревину, а також використовувати імплантацію в тіло.

– Пасивні RFID-мітки мають фактично необмежений термін експлуатації, мають низьку собівартість.

– RFID-мітки можуть нести велику кількість інформації.

– RFID-мітки легко відстежити на порівняно невеликій відстані: метро, офіси, банки, магазини, зупинки.

– RFID-мітки можуть бути використані як для читання, так і для запису великого обсягу інформації [5].

Класифікація RFID-міток. Існує декілька способів систематизації RFID-міток і систем:

- за робочою частотою;
- за джерелом живлення;
- за типом пам'яті.

а) За джерелом живлення

За типом джерела живлення RFID-мітки діляться на: пасивні; активні; напівпасивні.

Пасивні RFID-мітки не мають вбудованого джерела енергії. Електричний струм, що індукується в антені електромагнітним сигналом від зчитувача, забезпечує достатню потужність для функціонування кремнієвого CMOS-чипа, розміщеного в мітці, і передачі у відповідь сигналу.

Комерційні реалізації низькочастотних RFID-міток можуть бути вбудовані в стикер (наклейку) або імплантовані під шкіру.

У 2006 Hitachi виготовила пасивний пристрій, названий μ -Chip (мю-чип), розмірами $0,15 \times 0,15$ мм (не включаючи антену) і тонше за паперовий лист (7.5 мкм). Такого рівня інтеграції дозволяє досягти технологія «кремній-на-ізоляторі» (SOI). μ -Chip може передавати 128-бітовий унікальний ідентифікаційний номер, записаний в мікросхемі на етапі виробництва. Цей номер не може бути змінений надалі, що гарантує високий рівень достовірності і означає, що цей номер буде жорстко прив'язаний (асоційований) з тим об'єктом, до якого приєднується або в який вбудовується цей чип. μ -Chip від Hitachi має типовий радіус зчитування 30 см (1 фут). У лютому 2007 року Hitachi представила RFID-пристрій, що має розміри $0,05 \times 0,05$ мм, і завтовшки, достатньою для вбудовування в лист паперу.

У наш час основна проблема RFID-пристроїв полягає в тому, що для них потрібна зовнішня антена, яка за розмірами перевершує чип у найкращому разі в 80 разів. Найменша вартість RFID-міток, які стали стандартом для таких компаній, як Wal-Mart, DOD, Target, Tesco у Великій Британії і Metro AG в Німеччині, становить приблизно 5 центів за мітку фірми Smart Code. До того ж, через розкид розмірів антен, і мітки мають різні розміри – від поштової марки до листівки. На практиці максимальна дистанція зчитування пасивних міток варіюється від 10 см (4 дюймів) (згідно зі стандартом ISO 14443) до декількох метрів (стандарті EPC і ISO 18000-6), залежно від вибраної частоти і розмірів антени. В деяких випадках антена може бути виготовлена друкарським способом.

Виробничі процеси від Alien Technology під назвою Fluidic Self Assembly, від Smart Code – Flexible Area Synchronized Transfer (FAST) і від Symbol Technologies PICA направлені на подальше зменшення вартості міток за рахунок застосування масового паралельного виробництва. Alien Technology в наш час використовує процеси FSA і HiSam для виготовлення міток, тоді як PICA процес від Symbol Technologies знаходиться ще на стадії розробки. Процес FSA дозволяє проводити понад 2 мільйони IC пластин в годину, а PICA процес – понад 70 мільярдів міток в рік (якщо його

допрацюють). У цих технічних процесах ІС приєднуються до пластин міток, які у свою чергу приєднуються до антен, утворюючи готовий чип. Приєднання ІС до пластин і надалі пластин до антен – просторово найчутливіші елементи процесу виробництва. Це означає, що при зменшенні розмірів ІС монтаж (англ. Pickandplace) стане найдорожчою операцією. Альтернативні методи виробництва, такі як FSA і HiSam, можуть значно зменшити собівартість міток. Стандартизація виробництва (англ. Industrybenchmarks) приведе до подальшого падіння цін на мітки при їхньому широкомасштабному впровадженні.

Не кремнієві мітки виготовляються з полімерних напівпровідників. В наш час їхньою розробкою займаються декілька компаній в усьому світі. Мітки, що виготовляються в лабораторних умовах і працюють на частотах 13.56 МГц були продемонстровані в 2005 році компаніями POLYIC (Німеччина) і Philips (Голландія). У промислових умовах полімерні мітки виготовлятимуться методом прокатного друку (технологія нагадує друк журналів і газет), внаслідок чого вони будуть дешевші, ніж мітки на основі ІС. Це може закінчитися тим, що для більшості сфер застосування мітки почнуть друкувати так само просто, як і штрих-коди, і вони стануть такими ж дешевими.

Пасивні мітки УВЧ (ультрависокочастотні дециметрові хвилі) і НВЧ (надвисокочастотні сантиметрові і міліметрові хвилі) діапазонів (860–960 МГц і 2,4-2,5 ГГц) передають сигнал методом модуляції відбитого сигналу частоти, що несе (англ. Backscattering Modulation модуляція зворотного розсіяння). Антена зчитувача випромінює сигнал несучої частоти і приймає відбитий від мітки модульований сигнал. Пасивні мітки ВЧ діапазону передають сигнал методом модуляції навантаження сигналу частоти, що несе (англ. Load Modulation модуляція навантаження). Кожна мітка має ідентифікаційний номер. Пасивні мітки можуть містити перезаписувану незалежну пам'ять EEPROM-типу. Дальність дії міток становить 1–200 см (ВЧ-МІТКИ) і 1-10 метрів (УВЧ і НВЧ-мітки).

Активні RFID-мітки володіють власним джерелом живлення і не залежать від енергії зчитувача, унаслідок чого вони читаються на дальній відстані, мають великі розміри і можуть бути оснащені додатковою електронікою. Проте, такі мітки найдорожчі, а у батарей обмежений час роботи. Активні мітки в більшості випадків надійніші (наприклад, здійснюють меншу кількість помилок), ніж пасивні, завдяки особливій сесії зв'язку між міткою і пристроєм зчитування. Активні мітки, маючи власне джерелом живлення, також можуть генерувати вихідний сигнал більшого рівня, ніж пасивні, дозволяючи застосовувати їх в агресивніших для радіочастотного сигналу середовищах: воді (включаючи людей і тварин, які в основному складаються з води), металах (корабельні контейнери, автомобілі), для великих відстаней на повітрі. Більшість активних міток дозволяють передати

сигнал на відстані в сотні метрів при тривалості життя батареї живлення до 10 років. Деякі RFID-мітки мають вбудовані сенсори, наприклад, для моніторингу температури товарів, які швидко псуються. Інші типи сенсорів в сукупності з активними мітками можуть застосовуватися для вимірювання вологості, реєстрації поштовхів/вібрації, світла, радіації, температури і газів в атмосфері (наприклад, етилену).

Активні мітки зазвичай мають набагато більший радіус зчитування (до 300 м) і обсяг пам'яті, ніж пасивні, і здатні зберігати більший обсяг інформації для відправки приймачем. В даний час, активні мітки роблять розмірами не більше звичайної пілюлі і продають за ціною в декілька доларів.

Напівпасивні RFID-мітки, також їх називають напівактивними, дуже схожі на пасивні мітки, але оснащені батареєю, яка забезпечує чип енергоживленням. При цьому дальність дії цих міток залежить тільки від чутливості приймача зчитувача і вони можуть функціонувати на більшій відстані і з кращими характеристиками.

б) За типом використовуваної пам'яті

За типом використовуваної пам'яті RFID-мітки діляться на:

- RO (англ. Read Only) дані записуються тільки один раз, відразу при виготовленні. Такі мітки придатні тільки для ідентифікації. Ніяку нову інформацію в них записати не можна, і їх практично неможливо підробляти.

- WORM (англ. Write Once Read Many) окрім унікального ідентифікатора такі мітки містять блок одноразово записуваної пам'яті, яку надалі можна багато разів читати.

- RW (англ. Read and Write) такі мітки містять ідентифікатор і блок пам'яті для читання/запису інформації. Дані в них можуть бути перезаписані багаторазово[5].

в) За робочою частотою.

Мітки діапазону LF (125–134 кГц).

Пасивні системи даного діапазону мають низькі ціни і в зв'язку з фізичними характеристиками використовуються для підшкірних міток при чіпування тварин і людей. Однак, у зв'язку з довжиною хвилі, існують проблеми зі зчитуванням на великі відстані, а також проблеми, пов'язані з появою колізій при зчитуванні.

Мітки діапазону HF (13,56 МГц).

Системи 13 МГц дешеві, не мають екологічних та ліцензійних проблем, добре стандартизовані, мають широку лінійку рішень. Застосовуються в платіжних системах, логістиці, ідентифікації особистості. Для частоти 13,56 МГц розроблений стандарт ISO 14443 (види А / В). На відміну від Mifare 1K, в даному стандарті забезпечена система диверсифікації ключів, що дозволяє створювати відкриті системи. Використовуються стандартизовані алгоритми шифрування.

Для існуючих в даному діапазоні частот стандартів були знайдені серйозні проблеми в безпеці: була відсутня криптографія у дешевих чипів

карти Mifare Ultralight, введена в експлуатацію в Нідерландах для системи оплати проїзду в міському громадському транспорті OV-chipkaart, пізніше була зламана більш надійна картка Mifare Classic.

Як і для діапазону LF, в системах, побудованих в HF-діапазоні, існують проблеми зі зчитуванням з великих відстаней, зчитування в умовах високої вологості, наявності металу, а також проблеми, пов'язані з появою колізій при зчитуванні.

Мітки діапазону UHF (860-960 МГц)

Мітки даного діапазону мають найбільшу дальність реєстрації, в багатьох стандартах даного діапазону присутні антиколізійні механізми. Орієнтовані спочатку для потреб складської та виробничої логістики, мітки діапазону UHF не мали унікального ідентифікатора. Передбачалося, що ідентифікатором для мітки буде служити EPC-номер (Electronic Product Code) товару, який кожен виробник буде заносити в мітку самостійно при виробництві. Однак скоро стало ясно, що крім функції носія EPC-номера товару добре б покласти на мітку ще й функцію контролю справжності. Тобто виникла вимога, яка суперечить самому собі: одночасно забезпечити унікальність мітки і дозволити виробнику записувати довільний EPC-номер.

Довгий час не існувало чіпів, які б задовольняли цим вимогам повністю. Випущений компанією Philips чіп Gen 1.19 володів незмінним ідентифікатором, але не мав ніяких вбудованих функцій по паролюванню банків пам'яті мітки, і дані з мітки міг вивантажити хто завгодно, що має відповідне обладнання. Розроблені згодом чіпи стандарту Gen 2.0 мали функції паролювання банків пам'яті (пароль на читання, на запис), але не мали унікального ідентифікатора мітки, що дозволяло при бажанні створювати ідентичні клони міток.

Нарешті, в 2008 році компанія NXP випустила два нових чіпа, які на сьогоднішній день відповідають всім вище перерахованим вимогам. Чіпи SL3S1202 і SL3FCS1002 виконані в стандарті EPC Gen 2.0, але відрізняються від всіх своїх попередників тим, що поле пам'яті TID (Tag ID), в яке при виробництві зазвичай пишеться код типу мітки (і він в рамках одного артикулу не відрізняється від мітки до мітки), розбите на дві частини. Перші 32 біта відведені під код виробника мітки і її марку, а другі 32 біта – під унікальний номер самого чіпа. Поле TID – незмінне, і, таким чином, кожна мітка є унікальною. Нові чіпи мають всі переваги міток стандарту Gen 2.0. Кожен банк пам'яті може бути захищений від читання або запису паролем, EPC-номер може бути записаний виробником товару в момент маркування.

У UHF RFID-системах в порівнянні з LF і HF нижче вартість міток, при цьому вище вартість іншого обладнання.

Радіочастотні UHF-мітки ближнього поля

Мітки ближнього поля (англ. UHF Near-Field), яка є безпосередньо радіомітками, а використовуючи магнітне поле антени, дозволяють вирішити проблему зчитування в умовах високої вологості, присутності води і металу. За допомогою даної технології

очікується початок масового застосування RFID-міток в роздрібній торгівлі фармацевтичними товарами (такими, що потребують контролю достовірності, обліку, але при цьому часто містять воду і металеві деталі в упаковці)[6].

Зчитувачі – прилади, які читають інформацію з міток і записують в них дані. Ці пристрої можуть бути постійно підключеними до облікової системи, або працювати автономно. Залежно від частотного діапазону мітки, дистанція стійкого зчитування і запису даних може бути різною. Розрізняють стаціонарні та мобільні.

Стаціонарні зчитувачі кріпляться нерухомо на стінах, дверях, рухомих складських пристроях (штабеляторах, навантажувачах). Вони можуть бути виконані у вигляді замку, вмонтовані в стіл або закріплені поряд з конвеєром на шляху проходження виробів.

В порівнянні з мобільними, зчитувачі такого типу зазвичай мають більшу зону читання та потужність, і здатні одночасно обробляти значний потік інформації. Стаціонарні зчитувачі на виробництві інтегруються в інформаційну систему що дозволяє поетапно фіксувати переміщення маркованих об'єктів в реальному часі, або ідентифікувати положення мічених предметів в просторі.

Мобільні зчитувачі володіють порівняно меншою дальністю дії і часто не мають постійного зв'язку з програмою контролю і обліку. Мобільні зчитувачі мають внутрішню пам'ять, в яку записуються дані з прочитаних міток (потім цю інформацію можна синхронізувати з системою обліку) і, як і стаціонарні зчитувачі, здатні записувати дані в мітку (наприклад, інформацію про проведений контроль) [5].

Зробивши підсумки аналізованої літератури можна виділити переваги радіочастотної ідентифікації:

- можливість перезапису. Дані RFID-мітки можуть записуватись і доповнюватись багато разів, тоді як дані на штрих-коді не можуть бути змінені – вони записуються відразу при друку.

- Відсутність необхідності прямої видимості. RFID-зчитувачу не потрібно пряма видимість мітки, щоб вивантажити її дані. Взаємна орієнтація мітки і зчитувача часто не грає ролі. Мітки можуть читатися через упаковку, що робить можливим їх приховане розміщення. Для читання даних мітки досить хоча б ненадовго потрапити в зону реєстрації, переміщуючись, в тому числі, і на досить великій швидкості. Навпаки, зчитувачу штрих-коду завжди необхідна пряма видимість штрих-коду для його читання.

- Більша відстань читання. RFID-мітка може зчитуватися на значно більшій відстані, ніж штрих-код. Залежно від моделі мітки і зчитувача радіус зчитування може становити до декількох сотень метрів. У той же час подібні відстані потрібні не завжди.

– Більший обсяг зберігання даних. RFID-мітка може зберігати значно більше інформації, ніж штрих-код.

– Підтримка читання декількох міток. Промислові зчитувачі можуть одночасно зчитувати безліч (більше тисячі) RFID-міток в секунду, використовуючи так звану антиколізійну функцію. Пристрій зчитування штрих-коду може одноразово сканувати тільки один штрих-код.

– Зчитування даних мітки при будь-якому її розташуванні. З метою забезпечення автоматичного зчитування штрихового коду комітети по стандартам (в тому числі EAN International) розробили правила розміщення штрих-міток на товарній і транспортній упаковці. До радіочастотних міток ці вимоги не відносяться. Єдина умова – перебування мітки в зоні дії зчитувача.

– Стійкість до впливу навколишнього середовища. Існують RFID-мітки, що мають підвищену міцність і опірність жорстким умовам робочого середовища, а штрих-код легко пошкоджується (наприклад, вологою або забрудненням). У тих сферах застосування, де один і той же об'єкт може використовуватися необмежену кількість разів (наприклад, при ідентифікації контейнерів або зворотної тари), радіочастотна мітка виявляється більш прийнятним засобом ідентифікації, так як її не потрібно розміщувати на зовнішній стороні упаковки. Пасивні RFID-мітки мають практично необмежений термін експлуатації.

– Багатоцільове використання. RFID-мітка може використовуватися для виконання інших завдань, крім функції носія даних. Штрих-код не програмується і є лише засобом зберігання даних.

– Високий ступінь безпеки. Унікальне незмінне число-ідентифікатор, що привласнюється мітці при виробництві, гарантує високий ступінь захисту міток від підробки. Також дані на мітці можуть бути зашифровані. Радіочастотна мітка має можливість закрити паролем операції запису і зчитування даних, а також зашифрувати їх передачу. В одній мітці можна одночасно зберігати відкриті і закриті дані [6].

Недоліки радіочастотної ідентифікації:

– Працездатність мітки втрачається при частковому механічному пошкодженні.

– Вартість системи перевищує номінальну вартість системи обліку, заснованої на штрих-кодах.

– Простота самостійного виготовлення. Штрих-код можна надрукувати на будь-якому принтері.

– Схильність до завад у вигляді електромагнітних полів.

– Недовіра користувачів, можливості використання її для збору інформації про людей.

– Встановлена технічна база для зчитування штрих-кодів істотно перевершує за обсягом рішення на основі RFID.

– Недостатня відкритість вироблених стандартів[6].

Порівняльні характеристики RFID з аналогом представлені в таблиці 1 [6].

Таблиця 1 – Порівняльні характеристики RFID з аналогом

Характеристики технології	RFID	Штрих-код	QR-код
Необхідність в прямої видимості мітки	Читання навіть прихованих міток	Читання без прямої видимості неможливо	Читання без прямої видимості неможливо
Об'єм пам'яті	Від 10 до 512 000 байт	До 100 байт	До 3 072 байт
Можливість перезапису даних і багаторазового використання мітки	Має	Відсутня	Відсутня
Дальність реєстрації	До 100 м	До 4 м	До 1 м
Одночасна ідентифікація декількох об'єктів	До 200 міток в секунду	Неможлива	Залежить від зчитувача
Стійкість до впливів навколишнього середовища: механічному, температурному, хімічному, вологому	Підвищена міцність і стійкість	Залежить від матеріалу, на який наноситься	Залежить від матеріалу, на який наноситься
Термін життя мітки	Більше 10 років	Залежить від способу друку та матеріалу, з якого складається відзначається об'єкт	Залежить від способу друку та матеріалу, з якого складається відзначається об'єкт
Безпека і захист від підробки	Підробити можливо	Підробити легко	Підробити легко

Закінчення таблиці 1

Робота при пошкодженні мітки	Неможлива	Важко	Важко
Ідентифікація об'єктів, що рухаються	Так	Важко	Важко
Схильність перешкод у вигляді електромагнітних полів	Має	Немає	Немає
Ідентифікація металевих об'єктів	Можлива	Можлива	Можлива
Використання як стаціонарних, так і ручних терміналів для ідентифікації	Так	Так	Так
Можливість введення в тіло людини або тварини	Можлива	Важко	Важко
Габаритні характеристики	Середні і малі	Малі	Малі
Вартість	Середня	Низька	Низька

Міжнародні стандарти RFID, як складової частини технології автоматичної ідентифікації, розробляються і приймаються міжнародною організацією ISO спільно з IEC. Підготовка проектів (розробка) стандартів проводиться в тісній взаємодії з ініціативними зацікавленими організаціями і компаніями.

1) Організації-розробники стандартів

EPCglobal (спільне підприємство GS1 і GS1 US) працює за міжнародними стандартами в галузі використання RFID і EPC, з метою створити можливість ідентифікації будь-якого об'єкта в ланцюзі постачань товарів компаній у всьому світі.

Одна з місій EPCglobal полягає в упорядкуванні великої кількості RFID-протоколів, що з'явилися в світі починаючи з 1990-х років і створенні єдиного протоколу для реалізації прориву в сприйнятті RFID комерційними організаціями.

AIM global – міжнародна торгова асоціація, що представляє постачальників автоматичної ідентифікації та мобільних технологій. Асоціація активно підтримує розвиток AIM стандартів за рахунок власного Technical Symbolology Committee, Global Standards Advisory Groups і групи експертів RFID, а також через участь в промислових, національних (ANSI) і міжнародних (ISO) групах розробок.

GRIFS – дворічний проект зі створення Форуму сумісності стандартів RFID координується GS1 спільно з ETSI і CENI. Проект фінансується Європейським співтовариством. Почав свою діяльність в січні 2008 року. В рамках даного проекту проведено три конференції в Токіо, Гонконгу і Брюсселі в 2008-2009 роках.

EPC Gen2 – скорочення від «EPCglobal Generation 2».

Розподіл міток на класи було прийнято задовго до появи ініціативи EPCglobal, проте не існувало загальноприйнятого протоколу обміну між зчитувачами і мітками. Це призводило до несумісності зчитувачів і міток різних виробників. У

2004 р. ISO / IEC прийняла єдиний міжнародний стандарт ISO 18000, що описує протоколи обміну (радіоінтерфейси, англ. Airinterface) у всіх частотних діапазонах RFID від 135 кГц до 2,45 ГГц. Діапазону УВЧ (860-960) МГц відповідає стандарт ISO 18000-6A / B. З урахуванням технічних проблем, які проявлялися при зчитуванні міток класів 0 і 1 першого покоління, в 2004 р. фахівці Hardware Action Group EPCglobal створили новий протокол обміну між зчитувачем і міткою УВЧ діапазону – Class 1 Generation 2. У 2006 р. пропозиція EPC Gen2 з незначними змінами було прийнято ISO / IEC як доповнення 3 до існуючих варіантів А і в стандарту ISO 18000-6, і на даний момент стандарт ISO / IEC 18000-6С є найбільш поширеним стандартом технології RFID в УВЧ діапазоні. Цей стандарт був затверджений всупереч претензіям компанії Intermec про те, що його прийняття може порушити ряд їх патентів, пов'язаних з RFID. Було вирішено, що стандарт сам по собі не порушує патентів, однак при певних обставинах у виробників може виникнути необхідність платити мита Intermec.

Сучасні мітки стандарту Gen2 використовують ефективний антиколізійний механізм, заснований на розвинутій технології «слотів» – багатосесійність управління станом міток під час «інвентаризації», – тобто, зчитуванні міток в зоні реєстрації. Даний механізм дозволяє збільшити швидкість зчитування-інвентаризації міток до 1500 міток/с. (запис – до 16 міток / с.) при використанні промислових портальних зчитувачів, наприклад, компанії Impinj. Зчитувач і мітки на початку запиту генерують число q в діапазоні від 0 до 2 певною мірою n . Якщо число q зчитувача і однією з міток співпало, то вони проводять обмін інформацією. Якщо ж кількість відгукнулися міток не дорівнює одиниці, то зчитувач виробляє новий запит, при якому число q генерується заново. У разі, якщо часто виникає ситуація, в якій не стався обмін інформацією з міткою (тобто якщо міток занадто багато або занадто мало в порівнянні з діапазоном, в якому лежить число q), зчитувач коригує ступінь двійки n , змінюючи межі діапазону.

Даний алгоритм працює набагато швидше алгоритму, який використовується в Gen1, так як в першому випадку зчитувач побітно перебирає до 64 біт, а в другому працює теорія ймовірності і є механізм регулювання.

Крім того, Gen2 мітки дозволяють ефективно використовувати в перекриваючих і близьких зонах кілька зчитувачів одночасно (технологія англ. Multiple Reader Mode) за рахунок рознесення один від одного частотних каналів зчитувачів[6].

Станом на 2008 рік в якості міжнародного стандарту в області RFID виступає різне безліч стандартів описують різні області RFID:

- ISO 11784 – «Радіочастотна ідентифікація тварин – Структура кодів»
- ISO 11785 – «Радіочастотна ідентифікація тварин – Технічна концепція»
- ISO 14223 – «Радіочастотна ідентифікація тварин – Транспондери з розширеними функціями»
- ISO 10536 – «Карти ідентифікаційні. Безконтактні чіпові карти»
- ISO 14443 – «Карти ідентифікаційні. Безконтактні чіпові карти. Карти з малою відстанню зчитування»
- ISO 15693 – «Карти ідентифікаційні. Безконтактні чіпові карти. Карти середньої дальності зчитування»

- DIN / ISO 69873 – «Носії даних для інструменту і затискних пристроїв»
- ISO / IEC 10374 – «Ідентифікація контейнерів»
- VDI 4470 – «Системи охорони товарів»
- ISO 15961 – «RFID для управління товарами: керуючий комп'ютер, функціональні команди міток і інші синтаксичні можливості»
- ISO 15962 – «RFID для управління товарами: синтаксис даних»
- ISO 15963 – «Унікальна ідентифікація радіочастотних міток і реєстрація власника для управління унікальністю»
- ISO 18000 – «RFID для управління товарами: бездротовий інтерфейс»
- ISO 18001 – «Інформаційні технології – RFID для управління товарами – Рекомендовані профілі додатків»[6].

Розробка макету основного елемента системи на основі RFID. Розроблений макет приладу складається з RFID зчитувача «RC522», стабілізатора 3,3 В, мікроконтролера ATmega 328P (модуль Arduino), стабілізатора 5 В, реле відкриття замка, реле світлової та звукової сигналізації, блоку живлення.

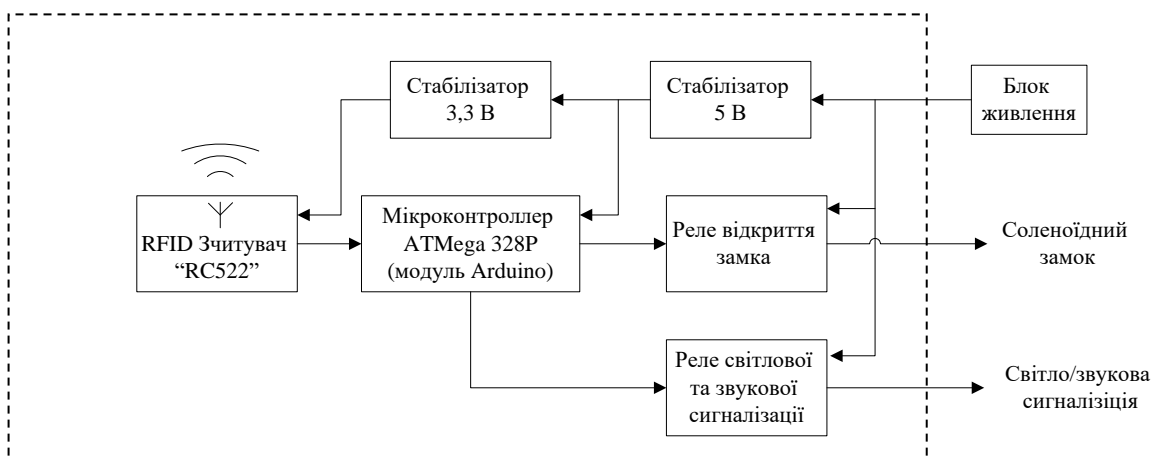


Рис. 2 – Структурна схема макету.

Розроблений макет постійно шукає RFID карту. Якщо карта знайдена, зчитується її ID. Якщо ID карта є в базі даних, пристрій включає реле, що відкриває замок, включає звукове оповіщення і через заданий час вимикає реле і звукове сповіщення. Якщо ID карти в базі даних немає, звучить довгий звуковий сигнал і знову триває пошук RFID карти.

Алгоритм роботи (рис. 3). При включенні живлення мікроконтролер в пристрої читає і виконує програму, яка закладена в даній пам'яті. Насамперед він налаштовує пристрої введення / виведення, настроює і запускає сторожовий таймер після чого входить в нескінченний цикл. У нескінченному циклі мікроконтролер опитує службову кнопку. Якщо вона натиснута, то мікроконтролер опитує RFID зчитувач на предмет наявності в полі зчитувача RFID карт. Якщо RFID карти в полі зчитувача немає і службова

кнопка натиснута, то мікроконтролер за допомогою RFID зчитувача продовжує шукати карту. Коли карта знайдена, зчитується її ID номер. Якщо ID номер карти є в базі даних і службова кнопка натиснута то триває пошук інших ID карт. Якщо ж номер ID карти немає в базі даних, то даний номер ID додається в базу даних і звучить короткий звуковий сигнал.

У той момент, коли службова кнопка не була натиснута, мікроконтролер за допомогою зчитувача шукає RFID карту. Якщо карта знайдена, зчитується її ID номер. Якщо ID номер карти є в базі даних, пристрій включає реле, що відкриває замок, включає звукове оповіщення і через заданий час вимикає реле і звукове сповіщення. Якщо ID номеру карти в базі даних немає, звучить довгий звуковий сигнал і знову триває пошук RFID карти.

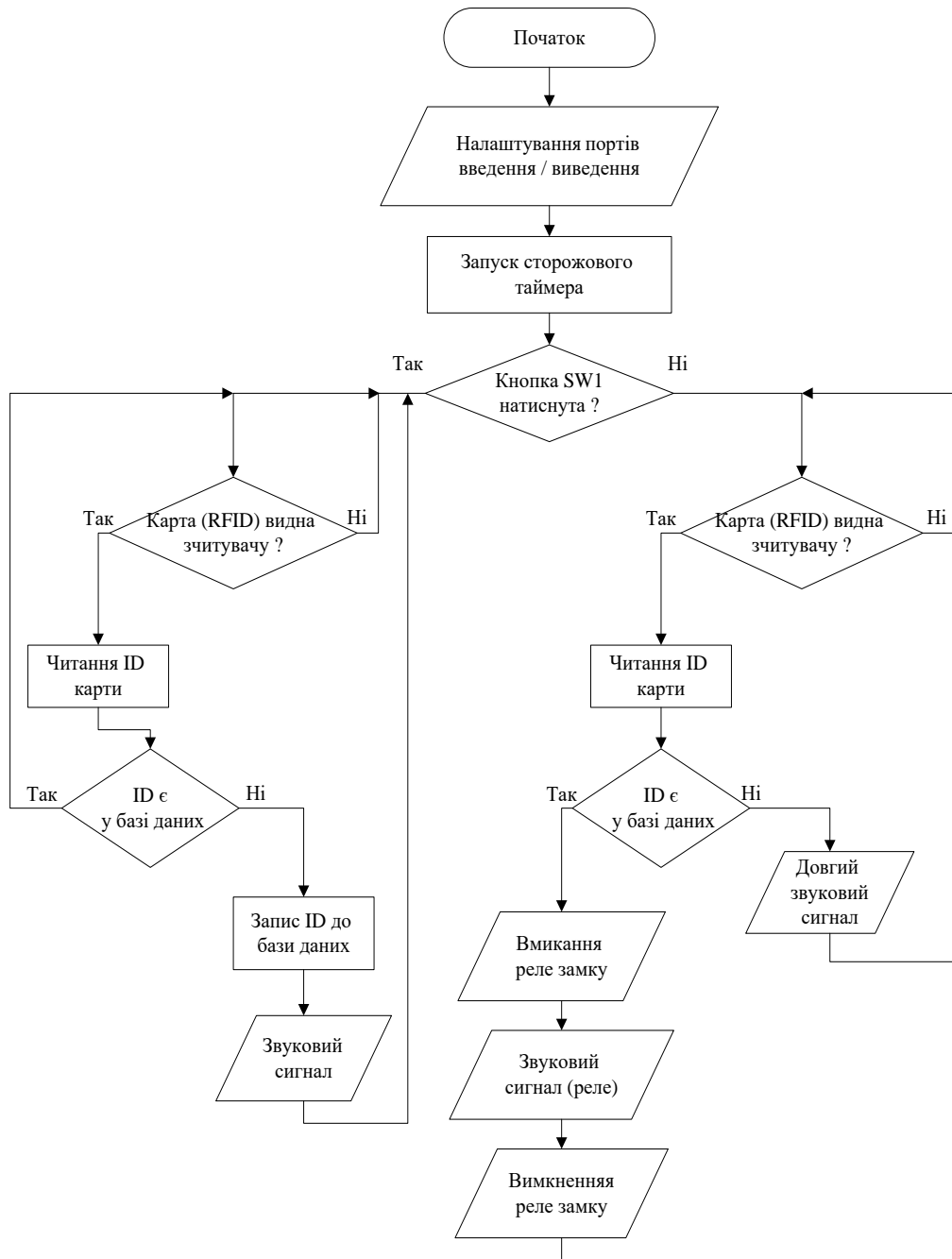


Рис. 3 – Алгоритм роботи пристрою.

Принципова схема макету приладу зображена на рис. 4.

Пристрій живиться постійною напругою 12 В. Конденсатор С4 виконує роль фільтра напруги живлення 12 В. Стабілізатор DA2 знижує вхідну напругу 12 В до рівня 5 В. Даними 5 В живиться DD2. Конденсатор С3 служить фільтром напруги 5 В. Стабілізатор напруги DA1 знижує вхідну в нього напругу 5В до рівня 3,3 В. Конденсатор С2 служить фільтром напруги 3,3 В. Дана напруга 3,3 В живить

DD1. Конденсатор С1 необхідний для послаблення брязкоту контактів SV1. Резистори R1-R3 є струмообмежуючими для баз транзисторів VT1 – VT3, які працюють в ключовому режимі. VT1 включає бузер BZ1. VT2 управляє К1. VT3 управляє К2. Для послаблення викидів ЕРС котушок електромагнітних реле К1, К2 служать діоди VD1, VD2.

Фото діючого макету приладу представлено на рис. 5.



Рис. 5 – Діючий макет пристрою

Висновки

Розглянуті технології, що дозволяють зчитувати, зберігати та обробляти дані, стежити за переміщенням об'єктів, на яких є мітка. Серед них було виділено RFID технологію, яка вважається найбільш поширеною, розвинутою, з більшим потенціалом у розвитку і застосуванні у повсякденному житті. RFID технології набули популярності в охоронній промисловості, на багатьох промислових та комерційних підприємствах, як система яка контролює час перебування та переміщення по робочій території, а також у торговельній сфері, як контроль за переміщенням товару.

Також було розроблено діючий макет приладу на основі RFID технології, особливості якого полягають в більшій доступності в порівнянні з існуючими завдяки підбору більш дешевих та не менш практичних радіоелементів і прошитою для більш вузьких та конкретних задач.

Список літератури

1. Система контролю і управління доступу [Електронний ресурс] / Вікіпедія – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8E_%D1%96_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC_ – Назва з екрану.
2. Система контролю і управління доступом [Електронний ресурс] / Lovevaquero – Режим доступу до ресурсу: <https://uk.ilovevaquero.com/tehnologii/108991-skud-eto-sistema-kontrolya-i-upravleniya-dostupom.html>. – Назва з екрану.
3. Системи контролю та управління доступом. Огляд. [Електронний ресурс] / Валтек – Режим доступу до ресурсу: <https://valtek.com.ua/ua/system-integration/security-control-system/access-control/access-control-review>. – Назва з екрану.
4. Системи контролю та управління [Електронний ресурс] / Studfile – Режим доступу до ресурсу: <https://studfile.net/preview/5157574/page:5/>. Останній доступ : 2016. – Назва з екрану.

5. Радіочастотна ідентифікація [Електронний ресурс] / Вікіпедія – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D1%96%D0%BE%D1%87%D0%B0%D1%81%D1%82%D0%BE%D1%82%D0%BD%D0%B0_%D1%96%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F. – Назва з екрану.
6. RFID [Електронний ресурс] / Вікіпедія – Режим доступу до ресурсу: <https://ru.wikipedia.org/wiki/RFID>. – Назва з екрану.

References (transliterated)

1. Sistema kontrolyu i upravlinnya dostupu [Elektronnij resurs] / Vikipediya – Rezhim dostupu do resursu: https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8E_%D1%96_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC_. – Nazva z ekranu.
2. Sistema kontrolyu i upravlinnya dostupom [Elektronnij resurs] /lovevaquero – Rezhim dostupu do resursu: <https://uk.ilovevaquero.com/tehnologii/108991-skud-eto-sistema-kontrolya-i-upravleniya-dostupom.html>. – Nazva z ekranu.
3. Sistemi kontrolyu ta upravlinnya dostupom. Oglyad. [Elektronnij resurs] / Valtek – Rezhim dostupu do resursu: <https://valtek.com.ua/ua/system-integration/security-control-system/access-control/access-control-review>. – Nazva z ekranu.
4. Sistemi kontrolyu ta upravlinnya [Elektronnij resurs] / Studfile – Rezhim dostupu do resursu: <https://studfile.net/preview/5157574/page:5/>. Ostanij dostup : 2016. – Nazva z ekranu.
5. Radiochastotna identifikaciya [Elektronnij resurs] / Vikipediya – Rezhim dostupu do resursu: https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D1%96%D0%BE%D1%87%D0%B0%D1%81%D1%82%D0%BE%D1%82%D0%BD%D0%B0_%D1%96%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F. – Nazva z ekranu.
6. RFID [Elektronnij resurs] / Vikipediya – Rezhim dostupu do resursu: <https://ru.wikipedia.org/wiki/RFID>. – Nazva z ekranu.

Надійшла (received) 12.10.19

Відомості про авторів / Сведения об авторах / About the Authors

Слободчук Антон Юрійович (Слободчук Антон Юрьевич, Slobodchuk Anton Yuryvich) – аспірант кафедри комп'ютерних та радіоелектронних систем контролю та діагностики, НТУ «ХПІ», м. Харків, Україна, email: antonslobodchuk@gmail.com

Позняков Владислав Олександрович (Позняков Владислав Александрович, Poznyakov Vladislav Alexandrovich) – магістрант кафедри комп'ютерних та радіоелектронних систем контролю та діагностики, НТУ «ХПІ», м. Харків, Україна, email: pozniakov199730@gmail.com

Ноздрачова Катерина Леонідівна (Ноздрачева Екатерина Леонидовна, Nozdrachova Katerina Leonidivna) – кандидат технічних наук, доцент, доцент кафедри комп'ютерних та радіоелектронних систем контролю та діагностики, НТУ «ХПІ», м. Харків, Україна, ORCID ID: 0000-0002-1996-2301, e-mail: nozdrachova@gmail.com

Юданова Ніна Миколаївна (Юданова Ніна Николаевна, Udanova Nina Mikolayivna) – старший викладач кафедри комп'ютерних та радіоелектронних систем контролю та діагностики, НТУ «ХПІ», м. Харків, Україна

Якіменко Вячеслав Олександрович (Якіменко Вячеслав Александрович, Yakimenko Viacheslav Aleksandrovich) – бакалаврант кафедри комп'ютерних та радіоелектронних систем контролю та діагностики, НТУ «ХПІ», м. Харків, Україна