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

Факультет електроніки

(повна назва інституту/факультету)

Акустичних та мультимедійних електронних систем

(повна назва кафедри)

«На правах рукопису»
УДК 004.738.5.057

«До захисту допущено»

Завідувач кафедри

Сергій НАЙДА

(ініціали, прізвище)

“ 07 ” грудня 2020 р.

Магістерська дисертація

зі спеціальності 171 Електроніка

(код і назва спеціальності)

на тему: Електронна система керування засобами доступу до об'єкта

Виконав: студент II курсу, групи ДВ-91мп

(шифр групи)

Андрій ТОПОРІВСЬКИЙ (підпис)

(прізвище, ім’я, по батькові)

Науковий керівник ст. викл., к.т.н., Наталія ФІЛІПОВА (підпис)

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

Рецензент доцент кафедри ЕПС к.т.н., доц. Катерина КЛЕН (підпис)

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

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

Київ – 2020 року

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

Інститут (факультет) Факультет електроніки
(повна назва)

Кафедра Акустичних та мультимедійних електронних систем
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою Електронні системи мультимедіа та засоби Інтернету речей

Спеціальність 171 Електроніка
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ С. А. Найда
(підпис) (ініціали, прізвище)
«07» грудня 2020 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
ТОПОРІВСЬКОМУ АНДРІЮ
РУСЛАНОВИЧУ
(прізвище, ім'я, по батькові)

1. Тема дисертації Електронна система керування засобами доступу до об'єкта

науковий керівник дисертації ст. викл. к.т.н. ФІЛІПОВА Н. Ю.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

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

2. Строк подання студентом дисертації 1.12.2020 р.

3. Об'єкт дослідження: Електронна система керування засобами доступу до об'єкта

4. Предмет дослідження (Вихідні дані – для магістерської дисертації за освітньо-професійною програмою): методи та технології управління та автоматизації шлагбаума.

5. Перелік завдань, які потрібно розробити: 1) Проаналізувати існуючі методи розпізнавання номерних знаків. 2) Проаналізувати програмні та апаратні засоби створення електронної системи керування засобами доступу до об'єкта, запропонувати рішення, що дозволяють спростити і здешевити вартість реалізації такої системи. 3) Розробити та дослідити електронну систему керування засобами доступу до об'єкта.

6. Перелік графічного (ілюстративного) матеріалу: 1) 97 рис, 21 табл., 1 презентація, 10 слайдів.

7. Орієнтовний перелік публікацій:
8. Дата видачі завдання 10. 09. 2019 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Написання першого розділу: Огляд стану предметної області	15.12.2019	Виконано
2	Дослідження існуючих методів виміру характеристик мережі. Дослідження існуючих платформ.	30.05.2020	Виконано
3	Написання третього розділу: Проектування архітектури системи. Реалізація прототипу та тестування	10.10.2020	Виконано
4	Написання четвертого розділу: Розробка програмного забезпечення для системи.	09.11.2020	Виконано
5	Підготовка матеріалів до друку та оформлення пояснювальної записки	30.11.2020	Виконано
6	Підготовка та оформлення плакатів для доповіді	03.12.2020	Виконано

Студент _____ А. Р. ТОПОРІВСЬКИЙ
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Н. Ю. ФІЛІППОВА
(підпис) (ініціали, прізвище)

УДК 004.738.5.057

РЕФЕРАТ

Топорівський А.Р. Електронна система керування засобами доступу до об'єкта: магістерська дис.: 171 Електроніка . Київ, КПІ ім. Ігоря Сікорського, 2020. 102 с.

Інтернет речі, Автоматизація шлагбауму, розпізнавання номерних знаків, платформа Інтернету речей, хмарна система.

Актуальність теми. В останні роки набувають все більшої популярності системи з розпізнаванням державних номерних знаків транспортних засобів, спроектовані для об’єктів з обмеженим доступом, чим обумовлена необхідність спрощення та здешевлення для популяризації таких систем.

Мета та задачі дослідження. Аналіз підходів до розширення області використання систем контролю доступу з подальшим забезпеченням можливості використання існуючих рішень, які взаємодіють, використовуючи існуючі протоколи передачі даних. Головним завданням є дослідження, що полягає у проектуванні системи керування засобами доступу до об’єкта для забезпечення взаємодії камери встановленої на в’їзді до об’єкту з обмеженим доступом, з функціоналом реалізованим на базі МК та серверного комп’ютера через існуючі протоколи передачі даних.

Вирішення поставлених завдань та досягнуті результати. В результаті виконання роботи була реалізована система, що захоплює стоп-кадри з камери, сканує номерні знаки на фото та керує засобом доступу. Дана реалізація також включає можливість додавання номерних знаків, при скануванні яких відбувається автоматичне керування засобом доступу. Для керування було розроблено скрипт. Система проста у розгортанні та може бути використана як доповнення до існуючої системи.

Об’єкт дослідження - електронна система контролю доступу до об`єкта.

Предмет дослідження - системи, методи та технології управління та автоматизації засобами доступу.

Методи дослідження. Для вирішення проблеми в даній роботі використовуються методи аналізу, синтезу, системного аналізу, порівняння та логічного узагальнення результатів.

Наукова новизна полягає у аналізі та удосконаленні методів, що дозволяють керувати засобами доступу, виконувати аналіз потоку камери, та автоматизовувати засоби доступу.

Практичне значення одержаних результатів. Розроблена система може бути розгорнута на будь-якому об’єкті з обмеженням доступу для транспортних засобів. Вана включає в собі дешеву реалізацію та простоту у встановленні та може бути використана для інтеграції в існуючі системи з підтримкою обраного протоколу.

SUMMARY

Toporivsky A.R. Electronic control system for means of access to the object: master's thesis .: 171 Electronics. Kyiv, KPI named after Igor Sikorsky, 2020. 102 p.

Internet of Things, barrier automation, license plate recognition, Internet of Things platform, cloud system.Master's dissertation: 102 p., 29 pic., 4 tabl., 23 sources, 4 supplement.

Actuality of theme. In recent years, systems with the recognition of state license plates of vehicles designed for objects with limited access have become increasingly popular, which necessitates simplification and reduction in price for the promotion of such systems.

The purpose and objectives of the study. Analysis of approaches to expanding the scope of access control systems with the subsequent provision of the possibility of using existing solutions that interact using existing data transmission protocols. The main task is to study the design of the control system of the means of access to the object to ensure the interaction of the camera installed at the entrance to the object with limited access, with functionality implemented on the basis of MK and server computer through existing data protocols

Solving the set tasks and achieved results. As a result of the work, a system was implemented that captures stills from the camera, scans license plates in the photo and controls the means of access. This implementation also includes the ability to add license plates, when scanning which is automatically controlled by the access means. A script was developed for management. The system is easy to deploy and can be used as a supplement to an existing system.

Object of study - electronic system of access control to object.

Subject of study - systems, methods and technologies of access control and automation.

Research methods. To solve the problem in this work, methods of analysis, synthesis, systems analysis, comparison and logical generalization of results are used.

Scientific novelty of the work is the analysis and improvement of methods that allow you to control the means of access, perform analysis of the flow of the camera, and automate the means of access.

The practical significance of the obtained results. The developed system can be deployed on any object with restricted access for vehicles. The bathtub includes a low-cost implementation and is easy to install and can be used to integrate into existing systems with support for the selected protocol.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

МК	–	мікроконтролер;
HTTP	–	Hypertext transfer protocol (протокол передачі гіпер-текстових документів);
ЖК	–	Житловий Комплекс;
IP	–	Internet Protocol (інтернет протокол);
DDNS	–	Dynamic Domain Name System;
ТЗ	–	Транспортний Засіб;
NAT	–	Network Address Translation;
UDP	–	User Datagram Protocol;
TCP	–	Transmission Control Protocol (протокол керування передачею);
RTSP	–	Real Time Streaming Protocol.

ВСТУП

Останнім часом використання нейронних мереж для реалізацій комп’ютерного зору значно збільшився. Це призводить до того, що рівень комфорту життя стає вищим, багато процесів автоматизуються, нівелюється людський фактор.

У багатьох розвинених країнах вже впроваджено автоматичне розпізнавання обличь, номерних знаків, фіксація порушень правил дорожнього руху, аналізування «гарячих» зон в супермаркетах. Також існують магазини які сканують обличчя і забраний товар з прилавок та автоматично знімають кошти за обрані вами товари.

Таким чином, рівень комфорту і якість життя в країні зростає. У світі вже представлено декілька рішень для розпізнавання номерних знаків транспортних засобів і автоматизації керуванням засобів доступу до об’єкта.

Однак такі розумні системи зазвичай мають високу вартість і потребують великих інвестицій в реалізацію. Отже, у багатьох країнах, що розвиваються, це може бути не ефективним та не доступним рішенням.

1 АНАЛІТИЧНИЙ ОГЛЯД ЕЛЕКТРОННИХ СИСТЕМ КЕРУВАННЯ ЗАСОБАМИ ДОСТУПУ ДО ОБ'ЄКТА

1.1 Система контролю і управління доступом

Система контролю і управління доступом, СКУД (англ. Physical Access Control System, PACS) - сукупність програмно-апаратних технічних засобів контролю і засобів управління, що мають на меті обмеження і реєстрацію входу-виходу об'єктів (людей, транспорту) на заданій території через «точки проходу»: двері, ворота, КПП [1].

Основне завдання - управління доступом на задану територію (кого пускати, в який час і на яку територію), включаючи також:

- обмеження доступу на задану територію;
- ідентифікацію особи, яка має доступ на задану територію.

Додаткові завдання:

- облік робочого часу;
- розрахунок заробітної плати (при інтеграції з системами бухгалтерського обліку);
- ведення бази персоналу / відвідувачів;
- інтеграція з системою безпеки, наприклад:
- з системою відеоспостереження для суміщення архівів подій систем, передачі системі відеоспостереження повідомлень про необхідність стартувати запис, повернути камеру для запису наслідків зафіксованого підозрілого події;
- з системою охоронної сигналізації (СОС), наприклад, для обмеження доступу в приміщення, які стоять на охороні, або для автоматичного зняття і постановки приміщень на охорону.
- з системою пожежної сигналізації (СПС) для отримання інформації про стан пожежних сповіщувачів, автоматичного розблокування

евакуаційних виходів і закривання протипожежних дверей в разі пожежної тривоги.

На особливо відповідальних об'єктах мережу пристроїв СКУД виконується фізично не пов'язаної з іншими інформаційними мережами.

1.2 Перегороджуючі пристрої

Встановлюються на двері:

- Електрозасувки - найменш захищені від злому, тому їх зазвичай встановлюють на внутрішні двері (внутрішньоофісні і т. П.) Електрозасувки, як і інші типи замків, бувають відкриваються напругою (тобто двері відкриваються при подачі напруги живлення на замок), і закриваються напругою (відкриваються, як тільки з них знімається напруга живлення, тому рекомендовані для використання пожежною інспекцією) [2].
- Електромагнітні замки - практично всі замикаються напругою, тобто придатні для установки на шляхах евакуації при пожежі.
- Електромеханічні замки - досить стійкі до злому (якщо замок міцний механічно), багато хто має механічний перевзвод (це означає, що якщо на замок подали відкриває імпульс, він буде розблоковано до тих пір, поки двері не відкриють).

Встановлюються на проходах / проїздах:

- Турнікет-тринод поясний зі зчитувачем системи контролю доступу
- Турнікети - використовуються на прохідних підприємств, суспільно значущих об'єктах (стадіони, вокзали, метро, деякі держустанови) - всюди, де потрібно організувати контрольований прохід великої кількості людей. Турнікети діляться на два основних типи: поясні та повнозростові. Якщо поруч з турнікетом немає швидко відкривається вільного проходу (на випадок пожежі), поясний турнікет повинен бути обладнаний т.зв. планками «антипаніка» -

планками, переламивающимися зусиллям якої нормальної людини (вимога пожежної інспекції).

- Шлюзові кабіни - використовуються в банках, на режимних об'єктах (на підприємствах з підвищеними вимогами до безпеки).
- Ворота і шлагбауми - в основному, встановлюються на в'їздах на територію підприємства, на автомобільних парковках і автостоянках, на в'їздах на прибудинкову територію, у двори житлових будинків. Основна вимога - стійкість до кліматичних умов і можливість автоматизованого управління (за допомогою системи контролю доступу). Коли мова йде про організацію контролю доступу проїзду, до системи пред'являються додаткові вимоги - підвищена дальність зчитування міток, розпізнавання автомобільних номерів (в разі інтеграції з системою відеоспостереження).
- Автоматичні дорожні бар'єри - використовуються для гарантованого запобігання несанкціонованого проїзду автотранспорту на територію, що захищається. Є заходами антитерористичного захисту, оскільки проїзд через піднятий бар'єр призводить до руйнування підвіски автомобіля.

1.3 Ідентифікатор

Основні типи виконання - картка, брелок, мітка. Є базовим елементом системи контролю доступу, оскільки зберігає код, який служить для визначення прав («ідентифікації») власника. Це може бути Touch memory, безконтактна картка (наприклад, RFID -мітки), або застаріваючий тип карт із магнітною смугою. В якості ідентифікатора можуть виступати також коди, що вводиться на клавіатурі, або окремі біометричні ознаки людини - відбиток пальця, малюнок сітківки або райдужної оболонки ока, тривимірне зображення обличчя [3].

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

Крім безпосереднього використання в системах контролю доступу, RFID -мітки широко застосовуються і в інших областях. Наприклад, в локальних розрахункових системах (оплата обідів в їдальні та інших послуг), системах лояльності і так далі.

1.4 Контролер

Автономний контролер - це «мозок» системи: саме контролер визначає, пропустити чи ні власника ідентифікатора в двері, оскільки зберігає коди ідентифікаторів зі списком прав доступу кожного з них у власній незалежній пам'яті. Коли людина пред'являє (підносить до зчитувального пристрою) ідентифікатор, лічений з нього код порівнюється з зберігаються в базі, на підставі чого приймається рішення про відкриття дверей [4].

Мережевий контролер об'єднується в єдину систему з іншими контролерами і комп'ютером для можливості централізованого контролю і управління. У такому випадку рішення про надання доступу може прийматися як контролером, так і програмним забезпеченням головного комп'ютера. Найчастіше об'єднання контролерів в мережу здійснюється за допомогою промислового інтерфейсу RS-485 або локальної мережі Ethernet.

У випадках, коли необхідно забезпечити роботу контролера при аваріях електромережі, блок контролера забезпечується власним акумулятором, або зовнішнім блоком резервного живлення. Час роботи від акумулятора може зайняти від декількох годин до декількох діб.

1.5 Зчитувач

Це пристрій, який отримує («зчитує») код ідентифікатора і передає його в контролер. Варіанти виконання зчитувача залежать від типу ідентифікатора: для «таблетки» - це два електричних контакту (у вигляді «лузи»), для proximity-карти - це електронна плата з антеною в корпусі, а для зчитування, наприклад, малюнка райдужної оболонки ока до складу зчитувача повинна входити камера [5]. Якщо зчитувач встановлюється на вулиці (ворота, вхідні двері будівлі, проїзд на територію автостоянки), то він повинен витримувати кліматичні навантаження - перепади температур, опади - особливо, якщо мова йде про об'єкти в районах з суворими кліматичними умовами. А якщо існує загроза вандалізму, необхідна ще і механічна міцність (сталевий корпус). Окремо можна виділити зчитувачі для дальньої ідентифікації об'єктів (з відстанню ідентифікації до 50 м.). Такі системи зручні на автомобільних проїздах, парковках, на в'їздах на платні дороги і т. П. Ідентифікатори (мітки) для таких зчитувачів, як правило, активні (містять вбудовану батарейку).

1.6 Конвертери середовища

Служать для підключення апаратних модулів СКУД один до одного і до ПК. Наприклад, є популярними конвертори RS-485 ↔ RS-232 і RS-485 ↔ Ethernet [6]. Деякі контролери СКУД вже мають вбудований інтерфейс Ethernet, що дозволяє без використання будь-яких додаткових пристроїв підключатися до ПК і зв'язуватися один з одним.

1.7 Програмне забезпечення

Чи не є обов'язковим елементом системи контролю доступу, використовується в разі, коли потрібна обробка інформації про проходах, побудова звітів, або коли для початкового програмування, управління та збору інформації в процесі роботи системи необхідно мережеве програмне забезпечення, яке встановлюється на один або кілька ПК, з'єднаних в мережа.

Всі СКУД можна віднести до двох великих класів або категорій: мережеві системи і автономні системи.

1.8 Мережеві системи

У мережній системі всі контролери з'єднані з комп'ютером, що дає безліч переваг для великих підприємств, але зовсім не потрібно для «однодверних» СКУД [7]. Мережеві системи зручні для великих об'єктів (офіси, виробничі підприємства), оскільки управляти навіть десятком дверей, на яких встановлені автономні системи, стає надзвичайно важко. Незамінні мережеві системи в наступних випадках:

- якщо необхідно реалізувати складні алгоритми допуску груп співробітників з різними привілеями в різні зони підприємства і мати можливість оперативно їх змінювати;
- якщо необхідно вибірково видаляти або створювати пропуску (мітки) для великої кількості точок проходу або для великої кількості співробітників (велика текучка і втрати пропусків);
- якщо необхідна інформація про що відбулися раніше події (архів подій) або є потреба у додатковому контроль в реальному часі. Наприклад, в мережевий системі існує функція фотоверіфікації: на прохідній при піднесенні входять людиною ідентифікатора до зчитувача, службовець (вахтер, охоронець) може на екрані монітора бачити фотографію людини, якого в базі даних визначено цю

ідентифікатор, і порівняти із зовнішністю проходить, 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 мережній системі 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, так звані радіоканали. Використання бездротових мереж часто визначається конкретними ситуаціями: складно або неможливо прокласти провідні 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 відпадає необхідність прокладати паралельні комунікації для об'єднання компонентів при використанні інтерфейсу RS-485.
- Wi-Fi. Основна перевага даного радіоканалу полягає в великої дальності зв'язку, здатної досягати декількох сотень метрів. Це особливо необхідно для з'єднання між собою об'єктів на великих відстанях. 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. Технології не стоять на місці і активно розвиваються, тому ZigBee може використовуватися і в системах контролю доступу. Дана бездротова технологія працює в неліцензованому діапазоні 2,45 ГГц.
- GSM. Перевага використання даного бездротового каналу зв'язку - практично суцільне покриття. До основних методів передачі інформації в даній мережі відносяться GPRS, SMS і голосової канал.

Нерідкі ситуації, коли установка повноцінної системи безпеки може виявитися невиправдано дорогою для вирішення поставленого завдання. У таких ситуаціях оптимальним рішенням буде установка автономного контролера на кожну з точок проходу, які необхідно обладнати доступом.

1.9 Автономні системи

Автономні системи дешевше, простіше в експлуатації, не вимагають прокладки сотень метрів кабелю, використання пристроїв сполучення з комп'ютером, самого комп'ютера [8]. При цьому до мінусів таких систем відноситься неможливість створювати звіти, вести облік робочого часу, передавати і узагальнювати інформацію про події, управлятися дистанційно. При виборі автономної системи з високими вимогами щодо безпеки рекомендується звернути увагу на наступне:

- Зчитувач повинен бути відділений від контролера, щоб дроти, по яких можливо відкривання замка, були недоступні зовні.
- Контролер повинен мати резервне джерело живлення на випадок відключення електроживлення.
- Переважно використовувати зчитувач в вандалозахисному корпусі.

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 дротах обмінюється інформацією з робочою станцією, на якій встановлено програмне забезпечення.

Для автономної системи можливо використовувати «зворотний метод», коли на контрольних точках встановлюються ідентифікатори, а співробітники відзначаються зчитувачем-контролером, згодом дані передаються при першій нагоді - поява зв'язку у зчитувача. Цей метод зручно використовувати, наприклад, в місцях де відсутній зв'язок, можливість прокладки електроживлення або інших комунікацій. Також "зворотний метод" може використовуватися для контролю патрулювання великих периметрів: після обходу території або після закінчення зміни охоронець здає на перевірку контролер, в якому записані всі пройдені контрольні точки із зазначенням послідовності проходу і часу проходу кожної точки.

1.10 Додаткові можливості

- GSM модуль, який дозволяє посилати SMS з інформацією про проході (використовується, наприклад, в школах).
- для мережевої СКУД (також деякі автономні системи) - можливість віддаленого управління по мережі Інтернет (наприклад, для управління системою контролю доступу з центрального офісу, якщо підприємство має безліч філій).
- комплекс для персоналізації пластикових карт (принтер для друку на пластиковій картці даних власника, в тому числі, фотографії).
- режим «антіпассбек» - якщо людина вже пройшов на територію, що охороняється, то повторне пред'явлення його ідентифікатора на вхід

буде заборонено (поки картка не буде пред'явлена на вихід), що виключить можливість проходу по одній карті двох і більше осіб. При цьому мережева СКУД дозволяє організувати такий режим на всіх точках проходу, об'єднаних в мережу, що забезпечує повнофункціональну захист по всьому периметру контрольованої території.

1.11 Застосування СКУД

Сфери застосування СКУД різноманітні:

- офіси компаній, бізнес-центри;
- банки;
- установи освіти (школи, технікуми, вузи);
- промислові підприємства;
- охоронювані території;
- автостоянки, парковки;
- місця проїзду автотранспорту;
- приватні будинки, житлові комплекси, котеджі;
- готелі;
- громадські установи (спорткомплекси, музеї, метрополітен та ін.)

1.12 Основні типи компаній на ринку

- Виробники
- Дистриб'ютори
- проектувальники
- інтегратори

- торгові доми
- монтажні організації
- кінцеві замовники
- Великі кінцеві замовники (мають власну службу безпеки)

Висновки до розділу

У даному розділі описано поняття СКУД.

Зназначено, що основна задача системи контролю і управління доступом є обмеження доступу на задану територію та ідентифікацію особи, яка має доступ на задану територію.

Виходячи з основної задачі СКУД можна зрозуміти що система обов’язково має містити в собі перегороджуючі пристрої.

Перегороджуваючі пристрої можуть бути різні. Наприклад для встановлення на двері може бути - електромеханічна клямка, електромагнітні замки, електромеханічні замки тощо. А для встановлення на проходах/проїздах – турнікети, шлюзові кабіни, автоматичні дорожні бар'єри, ворота і шлагбауми. В даному проекті як раз використовується останній – шлагбаум.

Основні типи виконання ідентифікатора який служить для визначення прав («ідентифікації») власника - картка, брелок, мітка. В даній роботі буде використовуватись не зовсім класичний ідентифікатор – державний номерний знак транспортного засобу.

Головними перевагами автоматизації відкривання воріт є висока швидкість операцій, безпека, можливість повноцінного контролю даних, універсальність, можливість ведення обліку, простота, зручність і доступність. Головні недоліки: необхідність придбання додаткових контролерів.

2 ТЕХНІЧНІ АСПЕКТИ СТВОРЕННЯ ТА РЕАЛІЗАЦІЇ ЕЛЕКТРОННОЇ СИСТЕМИ КЕРУВАННЯ ЗАСОБАМИ ДОСТУПУ ДО ОБ'ЄКТА

2.1 Компоненти системи контролю доступу

Компоненти системи контролю доступу включають:

- Панель управління доступом (також відома як контролер);
- Вхід з контролем доступу, такий як двері, турнікет, паркінг, ліфт або інший фізичний бар’єр;
- Зчитувач встановлений біля входу. (У випадках, коли вихід також контролюється, другий зчитувач використовується на протилежному боці входу.);
- Апаратні засоби блокування, такі як електричні замки дверей та електромагнітні замки;
- Магнітний перемикач дверей для контролю положення дверей;
- Пристрої із запитом на вихід (RTE) для виходу. Коли натискається кнопка RTE або детектор руху виявляє рух у дверях, сигналізація дверей тимчасово ігнорується під час відкривання дверей. Вихід із дверей без електричного розблокування дверей називається механічним вільним виходом. Це важлива функція безпеки. У випадках, коли замок повинен бути електрично розблокований при виході, пристрій із запитом на вихід також відмикає двері [9].

2.2 Топологія контролю доступу

Рішення щодо контролю доступу приймаються шляхом порівняння облікових даних зі списком контролю доступу. Цей пошук можна виконати хостом або сервером, панеллю керування доступом або зчитувачем. Розвиток систем контролю доступу спостерігав постійний поштовх пошуку від

центрального вузла до краю системи або зчитувача. Домінуючою топологією близько 2009 року є концентратор, на якому в якості концентратора виступала панель управління, а зчитувачі - спиці. Функції пошуку та управління здійснює панель управління. Спиці спілкуються через послідовний зв’язок; зазвичай RS-485. Деякі виробники висувають рішення до краю, розміщуючи контролер біля дверей. Контролери мають IP-адресу , і вони підключаються до хоста та бази даних за допомогою стандартних мереж.

2.3 Типи читачів

Зчитувачі контролю доступу можна класифікувати за функціями, які вони можуть виконувати:

- Основні (неінтелектуальні) пристрої зчитування: просто прочитайте номер картки або PIN-код і перешліть їх на панель управління. У разі біометричної ідентифікації такі зчитувачі виводять ідентифікаційний номер користувача. Як правило, протокол Wiegand використовується для передачі даних на панель управління, але інші варіанти, такі як RS-232, RS-485 та Clock / Data, не є рідкістю. Це найпопулярніший тип зчитувачів контролю доступу. Прикладами таких зчитувачів є RF Tiny від RFLOGICS, ProxPoint від HID та P300 від Farpointe Data [10];
- Напівінтелектуальні зчитувачі: мають усі входи та виходи, необхідні для управління дверним обладнанням (замок, контакт дверей, кнопка виходу), але не приймають жодних рішень щодо доступу. Коли користувач представляє картку або вводить PIN-код, зчитувач надсилає інформацію на головний контролер і чекає на її відповідь. Якщо з'єднання з основним контролером перервано, такі пристрої зчитування перестають працювати або функціонують у погіршеному режимі. Зазвичай напівінтелектуальні зчитувачі підключаються до панелі управління через шину RS-485 .

Прикладами таких зчитувачів є InfoProx Lite IPL200 від CEM Systems та AP-510 від Apollo;

- Інтелектуальні зчитувачі: мають усі входи та виходи, необхідні для управління дверним обладнанням; вони також мають пам'ять і обробну потужність, необхідну для самостійного прийняття рішень щодо доступу. Як і напівінтелектуальні зчитувачі, вони підключені до панелі управління через шину RS-485. Панель управління надсилає оновлення конфігурації та отримує події з пристроїв зчитування. Прикладами таких зчитувачів можуть бути InfoProx IPO200 від CEM Systems та AP-500 від Apollo. Існує також нове покоління інтелектуальних зчитувачів, яких називають " зчитувачами IP ". Системи з пристроями для зчитування IP зазвичай не мають традиційних панелей управління, і вони зв’язуються безпосередньо з ПК, який виконує роль хоста.

Деякі зчитувачі можуть мати додаткові функції, такі як РК-дисплей та функціональні кнопки для збору даних (наприклад, події годин / виходу для звітів про відвідуваність), камера / динамік / мікрофон для домофона та підтримка читання / запису смарт-карт.

2.4 Топології системи контролю доступу

1. **Серійні контролери**. Контролери підключені до головного ПК через послідовну лінію зв'язку RS-485 (або через струм струму 20 мА в деяких старих системах). Потрібно встановити зовнішні перетворювачі RS-232/485 або внутрішні карти RS-485, оскільки стандартні ПК не мають портів зв'язку RS-485.

Переваги:

- Стандарт RS-485 дозволяє проводити довгі прокладки кабелю до 1200 м (4000 футів);

- Відносно короткий час відгуку. Максимальна кількість пристроїв на лінії RS-485 обмежена до 32, що означає, що хост може часто запитувати оновлення стану від кожного пристрою та відображати події майже в реальному часі;
- Висока надійність та безпека, оскільки лінія зв'язку не використовується спільно з іншими системами.

Недоліки:

- RS-485 не допускає проводки типу «зірка», якщо не використовуються сплітери;
- RS-485 не дуже підходить для передачі великих обсягів даних (тобто конфігурації та користувачів). Максимально можлива пропускна здатність становить 115,2 кбіт / с, але в більшості систем вона знижена до 56,2 кбіт / с або менше, щоб підвищити надійність;
- RS-485 не дозволяє хост-ПК взаємодіяти з декількома контролерами, підключеними до одного порту одночасно. Тому у великих системах передача конфігурації та користувачів контролерам може тривати дуже довго, заважаючи нормальній роботі;
- Контролери не можуть ініціювати зв’язок у випадку тривоги. Хост-ПК діє як ведучий на лінії зв'язку RS-485, і контролерам доводиться чекати, поки вони опитуються;
- Спеціальні послідовні комутатори потрібні для того, щоб створити надлишкову настройку хост-ПК;
- Потрібно встановити окремі лінії RS-485 замість того, щоб використовувати вже існуючу мережеву інфраструктуру;
- Кабель, що відповідає стандартам RS-485, значно дорожчий за звичайний мережевий кабель UTP категорії 5;
- Робота системи сильно залежить від головного ПК. У разі виходу з ладу головного ПК події з контролерів не отримуються, і функції,

що вимагають взаємодії між контролерами (тобто анти-зворотний зв'язок), перестають працювати;

Система контролю доступу з використанням послідовного головного та субконтролерів.

2. Серійний головний та підконтролер. Вся дверна фурнітура підключена до субконтролерів (вони ж дверні контролери або дверні інтерфейси). Субконтролери зазвичай не приймають рішення про доступ, а натомість пересилають всі запити основним контролерам. Основні контролери зазвичай підтримують від 16 до 32 субконтролерів.

Переваги:

- Робоче навантаження на хост-ПК значно зменшується, оскільки йому потрібно лише спілкуватися з кількома основними контролерами;
- Загальна вартість системи нижча, оскільки субконтролери - це, як правило, прості та недорогі пристрої;
- Усі інші переваги, перелічені в першому абзаці, застосовуються.

Недоліки:

- Робота системи сильно залежить від основних контролерів. У разі виходу з ладу одного з основних контролерів події з його субконтролерів не отримуються, і функції, що вимагають взаємодії між субконтролерами (тобто антипропускна здатність), перестають працювати;
- Деякі моделі субконтролерів (як правило, з меншою вартістю) не мають пам’яті та обробної потужності для самостійного прийняття рішень щодо доступу. Якщо основний контролер виходить з ладу,

субконтролери переходять у деградований режим, в якому двері або повністю заблоковані, або розблоковані, і жодних подій не реєструється. Таких субконтролерів слід уникати або використовувати їх лише в районах, які не потребують високої безпеки;

- Основні контролери, як правило, дорогі, тому така топологія не дуже підходить для систем з декількома віддаленими місцями, які мають лише кілька дверей;
- Усі інші недоліки, пов'язані з RS-485, перелічені в першому абзаці, застосовуються.

Система контролю доступу за допомогою послідовного головного контролера та інтелектуальних зчитувачів

3. Серійні основні контролери та інтелектуальні зчитувачі. Вся дверна фурнітура підключається безпосередньо до інтелектуальних або напівінтелектуальних зчитувачів. Читачі, як правило, не приймають рішення про доступ, а пересилають всі запити на головний контролер. Тільки якщо підключення до головного контролера буде недоступним, читачі використовуватимуть свою внутрішню базу даних для прийняття рішень щодо доступу та запису подій. Напівінтелектуальний зчитувач, який не має бази даних і не може функціонувати без головного контролера, слід використовувати лише в районах, які не потребують високого рівня безпеки. Основні контролери зазвичай підтримують від 16 до 64 зчитувачів [11]. Усі переваги та недоліки такі ж, як і перелічені у другому пункті.

Системи контролю доступу за допомогою послідовних контролерів та серверів терміналів

4. Послідовні контролери з термінальними серверами. Незважаючи на стрімкий розвиток і все більше використання комп'ютерних мереж, виробники контролю доступу залишалися консервативними і не поспішали представляти

продукти з підтримкою мережі. Коли натискали на рішення з мережевим підключенням, багато хто обрав варіант, що вимагає менших зусиль: додавання термінального сервера , пристрою, який перетворює послідовні дані для передачі через LAN або WAN.

Переваги:

- Дозволяє використовувати існуючу мережеву інфраструктуру для підключення окремих сегментів системи;
- Забезпечує зручне рішення у випадках, коли встановлення лінії RS-485 було б складним або неможливим.

Недоліки:

- Збільшує складність системи;
- Створює додаткову роботу для установників: зазвичай сервери терміналів повинні бути налаштовані самостійно, а не через інтерфейс програмного забезпечення контролю доступу;
- Послідовний зв’язок між контролером та сервером терміналів виступає як вузьке місце: навіть якщо дані між головним ПК та сервером терміналів рухаються зі швидкістю мережі 10/100/1000 Мбіт / сек, він повинен сповільнитися до послідовної швидкості 112,5 кбіт / сек або менше. Також виникають додаткові затримки в процесі перетворення між послідовними та мережевими даними.

Усі переваги та недоліки, пов'язані з RS-485, також застосовуються.

Система контролю доступу за допомогою основних контролерів з підтримкою мережі

5. Мережеві основні контролери. Топологія майже така сама, як описано у другому та третьому абзацах. Застосовуються ті самі переваги та недоліки, але

вбудований мережевий інтерфейс пропонує кілька цінних удосконалень. Передача конфігурації та даних користувача до основних контролерів відбувається швидше, і може здійснюватися паралельно. Це робить систему більш чутливою і не перешкоджає нормальній роботі. Для досягнення надмірного налаштування хост-ПК не потрібне спеціальне обладнання: у випадку відмови основного хост-ПК вторинний хост-ПК може почати опитування мережевих контролерів. Також усуваються недоліки, введені серверами терміналів (перелічені в четвертому абзаці).

Система контролю доступу за допомогою IP-контролерів

6. IP-контролери . Контролери підключені до головного ПК через Ethernet LAN або WAN.

Переваги:

- Існуюча мережева інфраструктура повністю використана, і немає необхідності встановлювати нові лінії зв'язку;
- Немає обмежень щодо кількості контролерів (як 32 на рядок у випадках RS-485);
- Спеціальні знання щодо встановлення, припинення, заземлення та усунення несправностей RS-485 не потрібні;
- Зв'язок з контролерами може здійснюватися на повній швидкості мережі, що важливо при передачі великої кількості даних (баз даних з тисячами користувачів, можливо, включаючи біометричні записи);
- У разі тривоги контролери можуть ініціювати підключення до головного ПК. Ця здатність важлива у великих системах, оскільки вона служить для зменшення мережевого трафіку, спричиненого непотрібним опитуванням;
- Спрощує установку систем, що складаються з декількох ділянок,

які розділені на великі відстані. Базового посилання на Інтернет достатньо для встановлення зв’язку з віддаленими місцями;

- Доступний широкий вибір стандартного мережевого обладнання для забезпечення зв’язку в різних ситуаціях (волоконно-оптична, бездротова, VPN, подвійна мережа, PoE)

Недоліки:

- Система стає сприйнятливою до проблем, пов’язаних з мережею, таких як затримки у випадку великого трафіку та несправності мережевого обладнання;
- Контролери доступу та робочі станції можуть стати доступними хакерам, якщо мережа організації недостатньо захищена. Цю загрозу можна усунути фізичним відокремленням мережі контролю доступу від мережі організації. Більшість IP-контролерів використовують платформу Linux або власні операційні системи, що ускладнює їх злом. Також використовується галузеве стандартне шифрування даних;
- Максимальна відстань від концентратора або перемикача до контролера (якщо використовується мідний кабель) становить 100 метрів (330 футів);
- Робота системи залежить від головного ПК. У разі виходу з ладу головного ПК події з контролерів не отримуються, і функції, що вимагають взаємодії між контролерами (тобто проти зворотної передачі), перестають працювати. Однак деякі контролери мають параметр однорангового зв'язку для того, щоб зменшити залежність від головного ПК.

Система контролю доступу за допомогою IP-зчитувачів

7. Зчитувачі IP . Зчитувачі підключені до головного ПК через Ethernet LAN або WAN.

Переваги та недоліки контролерів IP стосуються і пристроїв зчитування IP:

Переваги:

- Більшість зчитувачів IP підтримують PoE. Ця функція дозволяє дуже легко забезпечувати живлення від батареї всією системою, включаючи замки та різні типи детекторів (якщо вони використовуються);
- Зчитувачі IP усувають необхідність у корпусах контролерів;
- При використанні зчитувачів IP не витрачається витрачена потужність (наприклад, 4-дверний контролер мав би 25% невикористаної потужності, якби керував лише 3-ма дверима);
- Системи зчитування IP-адрес легко масштабуються: немає необхідності встановлювати нові основні або субконтролери;
- Помилка одного зчитувача IP не впливає на інші зчитувачі в системі.

Недоліки:

- Для використання в зонах підвищеного захисту IP-зчитувачам потрібні спеціальні модулі введення / виведення, щоб виключити можливість проникнення через доступ до проводки блокування та / або виходу. Не всі виробники IP-зчитувачів мають такі модулі;
- Будучи більш витонченими, ніж базові зчитувачі, зчитувачі IP також є більш дорогими та чутливими, тому їх не слід встановлювати на відкритому повітрі в районах із суворими погодними умовами або високою ймовірністю вандалізму, якщо це спеціально не призначено для зовнішньої установки. Кілька виробників роблять такі моделі.

.

Висновки до розділу:

У даному розділі визначено та досліджено технічні аспекти створення та реалізації електронної системи керування засобами доступу до об'єкта, компоненти системи контролю доступу, топологія контролю доступу та типи читачів.

Визначені існуючі підходи застосування системи контролю і управління доступу:

- Ідентифікація відвідувачів;
- Автоматизація відкривання воріт;
- Облік відвідувачів;
- Контроль об’єкту;
- Аналітика доступу до об’єкта.

Проведено аналіз переваг та недоліків різних типів контроллерів систем управління доступом.

3 ТЕХНІЧНІ АСПЕКТИ ЕЛЕКТРОННОЇ СИСТЕМИ КЕРУВАННЯ ЗАСОБАМИ ДОСТУПУ ДО ОБ'ЄКТА

3.1 Завдання проекту

Ідея проекту полягає в тому щоб створити універсальну бюджетну електронну систему керування засобами доступу до об'єкта.

Основне завдання – автоматизація управління доступом на територію житлового комплексу. Система включає в себе:

- Ідентифікація транспортного засобу шляхом розпізнавання державного номерного знаку;
- Звірка ідентифікованого номерного знаку з базою даних мешканців житлового комплексу;
- Автоматичне відкриття шлагбауму, якщо номерний знак є в базі даних.

Додаткові завдання:

- Ведення бази відвідувачів.

3.2 Розробка структурної схеми

Структурна схема електронної системи складається з:

- Камера з відеореєстратором у якого є можливість транслювати відеопотік (або IP камера);
- Комп’ютер (ПК, сервер, Raspberry PI тощо) з підключеним Arduino через інтерфейс USB;
- Передавач 433 МГц з амплітудною модуляцією.

Якщо використовується raspberry pi, то Arduino не потрібний, так як можна використовувати GPIO Raspberry PI.

Безпровідний передавач 433 МГц має бути з амплітудною модуляцією.

Компьютер виступає в ролі основного контроллеру системи. Він потрібен для прийому, обробки та передаванню інформації:

- Прийом відеопотоку камери;
- Розпінавання номерних знаків транспортних засобів які хочуть заїхати на терирторію житлового комплексу;
- Звірка розпізнаних знаків з базою данних;
- Логування часу та номерного знаку ТЗ який в'їжджає на територію ЖК;
- Відправлення сигналу на контроллер шлагбауму через GPIO (Arduino) та передавач 433 МГц.

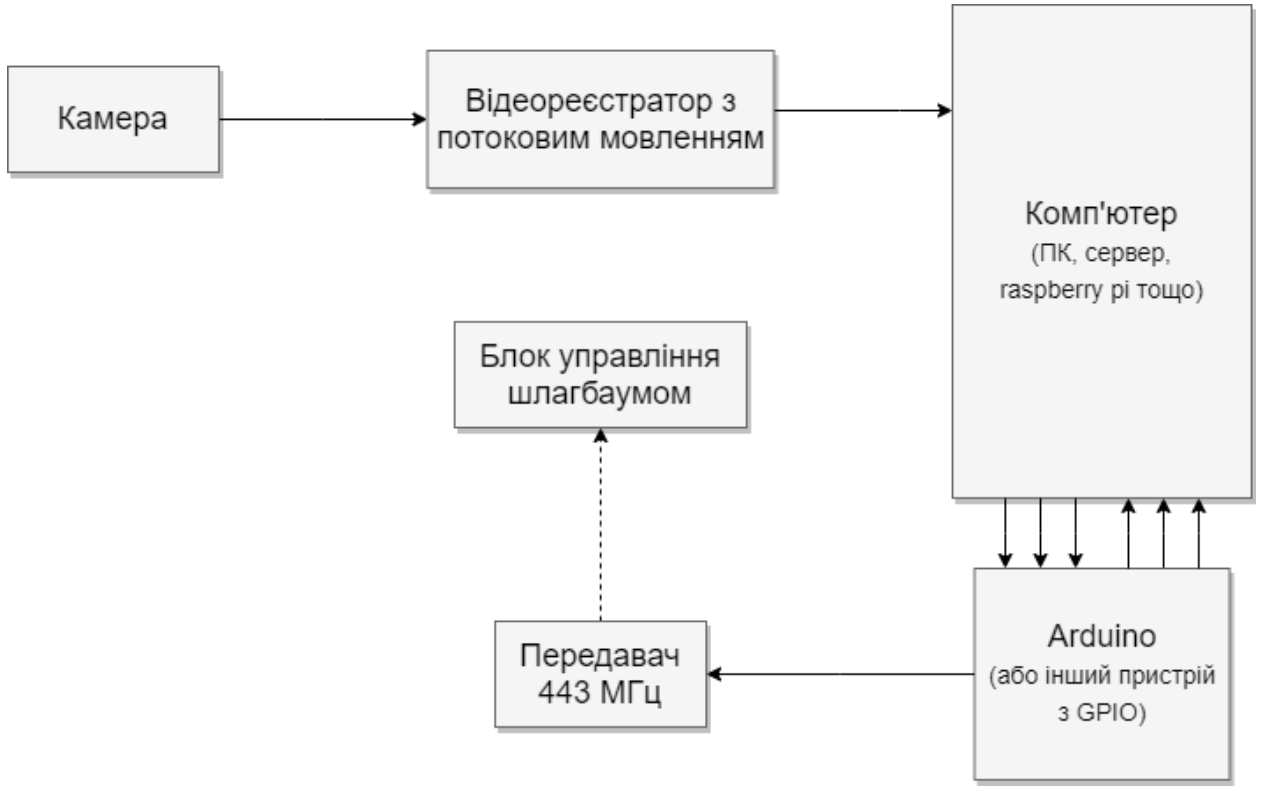


Рисунок 3.1 – Структурна схема електронної системи

3.3 Алгоритми кодування радіоканалу

Сигнали радіоканал по якому передаються дані між сигналізацією і ключем поширюються на всі боки і з цього обмін інформацією, можна "прослухати". В межах міста знаходяться багато інших сигналізацій які не повинні реагувати на чужий пульт. Щоб захистити канал обміну від випадкового або навмисного впливу, сигнал обміну між ключом і блоком сигналізацій кодується.

Дані по радіоканалу передають у вигляді послідовностей - пакетів. Кожен пакет сигналів можна уявити як команду (наприклад, "Поставити на охорону і Закрити замки" або "Зняти з охорони і відкрити замки").

Підсумуємо, на які типи поділяються подібні системи. На сьогодні у день алгоритми шифрування радіо обміну діляться на наступні основні категорії:

- статичний код
- динамічний код
- діалоговий код

Статичний код

Найперші сигналізації з радіоканалом мали статичний код - кожній команді відповідав свій командний пакет. Формат пакета вибирався користувачем або монтажником за допомогою перемикачів всередині ключа, або Запевняю перемичок. Варіантів коду було не багато і своїм ключем можна було відкрити чужу машину якщо збігалися коди команд. Статичний код брелка сигналізації встановлюється перемичками [12].

Таке кодування не забезпечувало належного захисту, досить було записати команду "зняти з охорони", а потім відтворити її і машина знімається з охорони як з рідного брелка. Тоді і з'явилися перші кодграббери призначені для

перехоплення, декодування і повтору коду, щоб зняти автомобіль з охорони з метою викрадення.

Види чіпів мають статичний код і приємним в пультах управління сигналізацій

Види чіпів:

- [6010] HT-6010, HT6014, SH-312E - 3-х статусний код
- [H600] HT-600, HT-680, HT6187, HT6270, TT-13, ПК-10Т - 3-х статусний код
- [5026] AX5026, CT5026 - 3-х статусний код
- [5326] AX5326, AX5326S - 3-х статусний код
- [2262] PT-2262, M3E, CT5062 - 3-х статусний код
- [8092] TT8092 - 3-х статусний код
- [4134] MC41342, MC145026, SC41342 - 3-х статусний код

На прикладі чіпів HT6010, HT6012, HT6014 розглянемо принцип кодування 3 12 (3-х статусний код) і обміну між пультом і сигналізацією.

До складу сімейства входить 3 мікросхеми кодерів (HT6010, HT6012, HT6014) і три мікросхеми декодерів (HT6030, HT6032, HT6034) [13].

До складу кодової послідовності, що генерується кодерами цього сімейства, входить преамбула, що синхронізує біт і 12-розрядне поле адреси / даних, довжина періоду одного біта дорівнює 6-ти імпульсам тактової частоти (рис. 3.2).

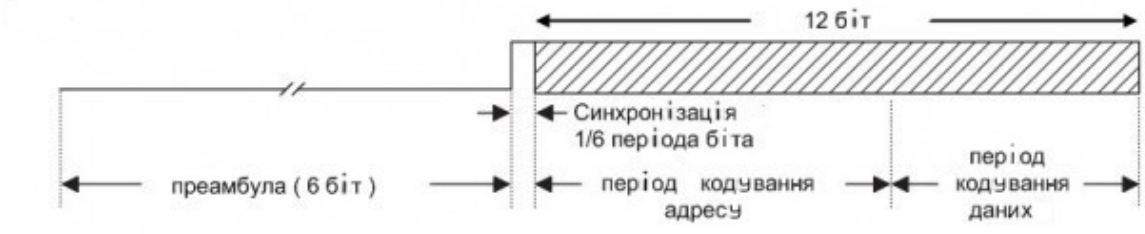


Рисунок 3.2 – склад кодової послідовності генерується кодерами ht6010, ht6012, ht6014

Значення адреси і даних на цих чіпах встановлюється за допомогою перемикачів, зовнішньої схемою або програмно. Кожен висновок адреси / даних кодера кодується трьома станами: підключений до мінуса електроживлення (логічний нуль), підключений до плюса електроживлення (логічна одиниця), не підключений (не має з'єднання) - (рис. 3.3).

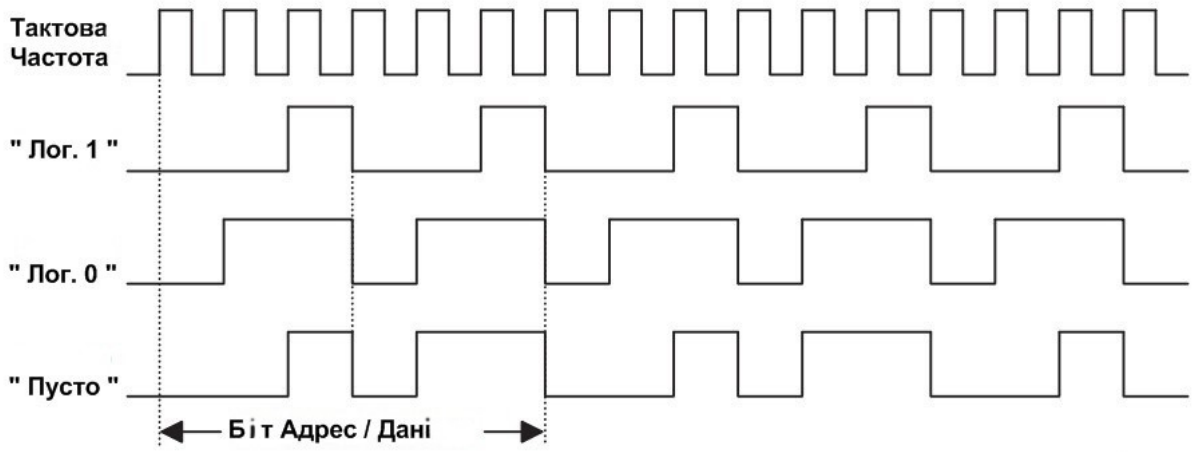


Рисунок 3.3 – -х статусний код, що генерується кодерами ht6010, ht6012, ht6014

Типова схема підключення кодера HT6012 представлена на рис. 3.4, (A0-A9) - Кодує адресну посилку з 10-ти біт (пароль дотупа) (D10-D11) - 2-а біта даних, резистор (Rosc) - задає тактовою частоту роботи чипа. Дані з виходу (DOUT) передаються на вхід передавача з амплітудною модуляцією який може працювати на частоті 433 МГц або 310 МГц [14].

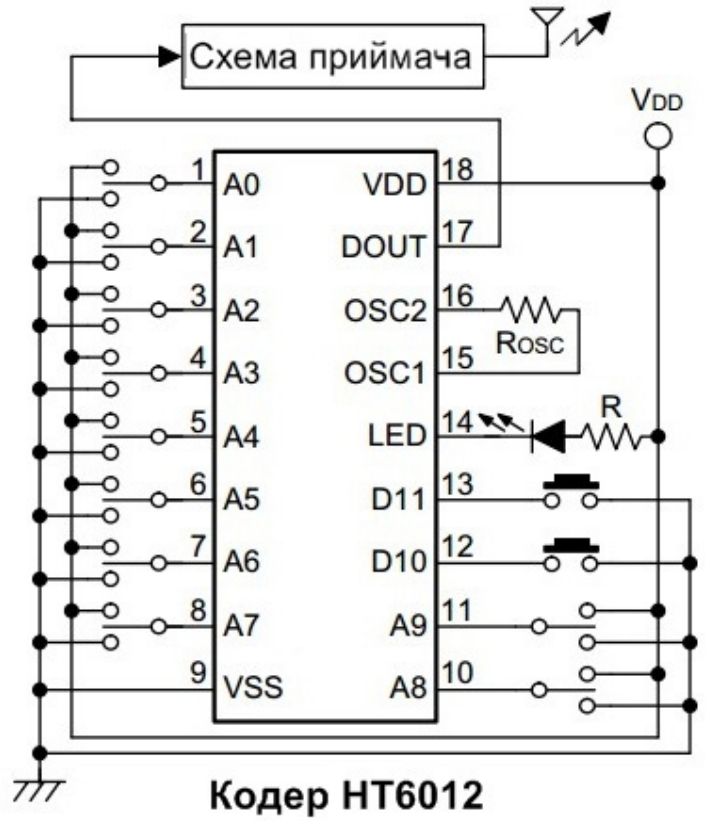


Рисунок 3.4 – Типова схема підключення кодера HT6012

Декодери перевіряють прийняту кодову послідовність, інформаційна частина якої складається з 12 біт (N біт адреси і N біт даних). Прийняті дані передаються до відповідних вихідні засувки тільки якщо команда була два рази поспіль правильно розшифрувати і прийнятий адреса (пароль) збігся з встановленим в декодере. При правильно прийнятої команді на виході VT з'являється високий рівень сигналу. Декодери цього сімейства можуть мати 0, 2 і 4 вихідних засувок даних (відповідно, 12, 10 і 8 входів адреси). На малюнку 4 показана типова схема включення декодера HT6032 інформаційна частина якої складається з 12 біт (10 біт адреси і 2 біти даних) [15].

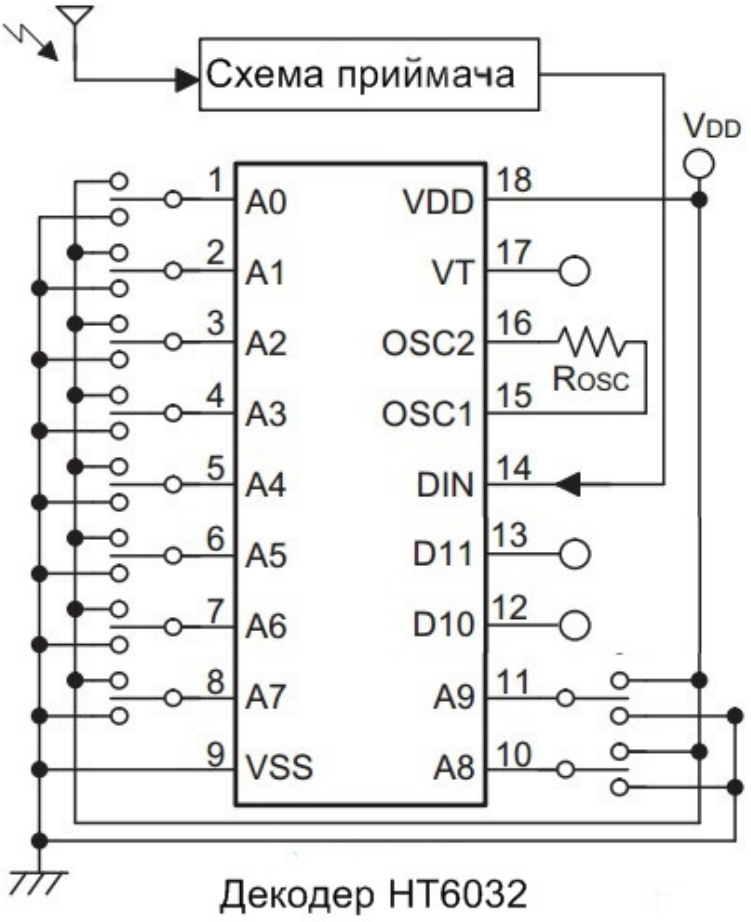


Рисунок 3.5 – Типова схема підключення декодера HT6032

Динамічний код

Із зростанням попиту на охоронні системи автомобілів і впорядкування частоти радіоканалу на 433.92 Мгц, виробники сигналізацій перейшли на новий вид кодування, ось тоді і з'явилося поняття динамічний код. Даний варіант має на увазі те, що при кожному натисканні на кнопку брелка в ефір надсилається унікальний код команди, ймовірність повторення якого дуже мала. Тепер записану в пам'яті граббера посилку можна було просто викинути, адже блок сигналізації вже з нею відпрацював і викинув зі списку правильних пакетів. У разі якщо коди були не великими за кількістю бітів в команді, ще можна було користуватися методом підбору кодів за допомогою сканера, але ці випадки були одиничними, і тривало це не довго, з'явився революційний метод кодування під назвою KEELOQ.

KEELOQ

У 80-х роках в африканській компанії NANOTEQ, що займається питаннями інформаційної безпеки, була розроблена система алгоритмів захисту під назвою KEELOQ (часто це кодування виробники вказують як CODE HOPPING). У 1995 році фірма MICROCHIP придбала відділення Keeloq у фірми Nanoteq разом з ліцензійними правами [16].

MICROCHIP розробив новий ряд компактних мікросхем кодеров і декодерів на основі алгоритму Keeloq з динамічним (стрибаючим) кодом. Низька вартість і високий ступінь захисту, а також мініатюрні розміри зробили революцію в індустрії автомобільних сигналізацій. Дуже багато систем і зараз використовують в пультах сигналізацій готові кодери, такі як HCS200, HCS300, HCS301, HCS320 [17].

Таблиця 3.1 – алгоритм Keeloq

Кодери Microchip	Кодова посилка біт	«Стрибаючий код» біт	Кодове зерно біт	Функцій	Напруга живлення, В
HCS101	66	-	-	7	3,5 – 13,3
HCS200	66	32	32	7	3,5 – 13,0
HCS201	66	32	32	7	3,5 – 13,0
HCS300	66	32	32	15	2,0 – 6,3
HCS301	66	32	32	15	3,5 – 13,0
HCS320	66	32	32	15	3,5 – 13,0

В основу алгоритму покладено псевдовипадковий "стрибучий" код, так що ніхто, крім "свого" приймача, не може передбачити, який код повинен бути переданий в наступний раз. "Стрибки" код генерується кодером за ліцензованим алгоритму на основі 64-бітного коду "ключа шифрування", 28-бітного серійного номера і 16-бітного лічильника синхронізації.

Розглянемо детальніше реалізацію алгоритму Keeloq на основі кодеров сімейства HCS компанії MICROCHIP.

Перш ніж використовувати мікрочіп в пультах сигналізацій він повинен бути запрограмований виробником сигналізації в процесі виробництва. Вся запрограмована інформації зберігається у вмонтованому EEPROM (незалежна пам'ять), і це:

- 16-бітове значення слова конфігурації (визначає режим роботи кодера);
- 28-бітний серійний номер, який повинен бути унікальним для кожного кодера;
- 64-х бітний унікальний ключ шифрування, який згенерований під час виготовлення (ключ шифрування генерується по нелінійному закону з 28-бітного серійного номера і 64-х бітного ключа виробника);
- 16-бітове значення лічильника синхронізації

При натисканні будь-якої кнопки пульта, кодер читає кнопку і модифікує лічильник синхронізацій. Потім значення лічильника синхронізації об'єднується з ключем шифрування в алгоритмі шифрування, і в результаті виходить 32-біт зашифрованої інформації. Ці дані змінюються кожного разу після натискання кнопки, тому ця частина кодової комбінації називається динамічним кодом. Приймачі і передавачі Keeloq працюють в послідовному коді з посилкою довжиною 66 біт (рис.3.6), що складається з кодованої "стрибає" частини в 32 біта, 28 біт серійного номера, 4 біт користувача (стан кнопок), 1 біта індикації розряду батареї і 1 фіксованого біта (біт повтору) [18].

Рисунок 3.6 – Keeloq в послідовному коді з посилкою довжиною 66 біт

В ефірі пакет Keeloq розділений на умовну складову ТЕ (Базова тактова тривалість) і складається з Преамбули (Тр), Хедера (Th), Даних (Thop + Tfix) і Паузи (Tg) (рис.3.7) У різних брелках з різним рівнем заряду батарейки тривалість ТЕ може відрізнятися і за специфікацією складати від 260 мкс до 660 мкс, але в межах одного пакета тривалість ТЕ відносно стабільна.

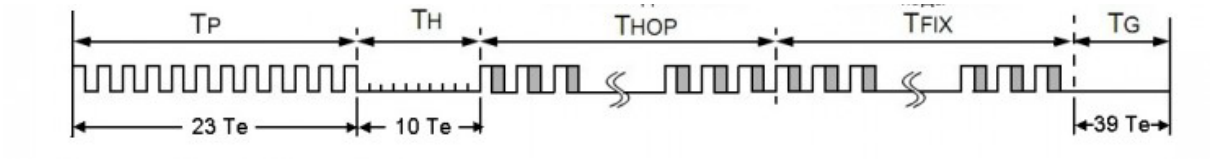


Рисунок 3.7 – Пакет Keeloq в ефірі

Передача пакета Keeloq кодером HCS ... в ефір починається з преамбули і вона складається з 23-х ТЕ які чергуються високим і низьким рівнем. Преамбула потрібна для "розгойдування" приймача і настройки ТЕ для декодера. Далі йде Хедер тривалістю 10 ТЕ низького рівня. За хедер йде передача даних. Дані складаються з 66 інформаційних біт, кожен біт має період тривалістю 3-и ТЕ (Рис.3.8)

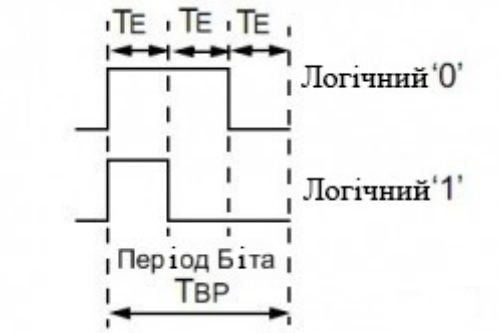


Рисунок 3.8 – Передача біта даних Keeloq

На рис.3.8 видно, що логічна одиниця складається з одного ТЕ високого рівня і двох ТЕ низького рівня, логічний нуль складається з двох ТЕ високого рівня і одного ТЕ низького рівня. Треба зауважити, що дані передаються в ефір від молодшого байта (LSb) до старшого (MSb) (рис.3.6). Після передачі даних йде пауза довгої 39 TI і якщо кнопка утримується після паузи сного піде чергова преамбула.

Типова схема підключення кодера HCS2XX - HCS3XX представлена на рис. 3.9 фактично це схема чотирьох кнопкового пульта сигналізації.

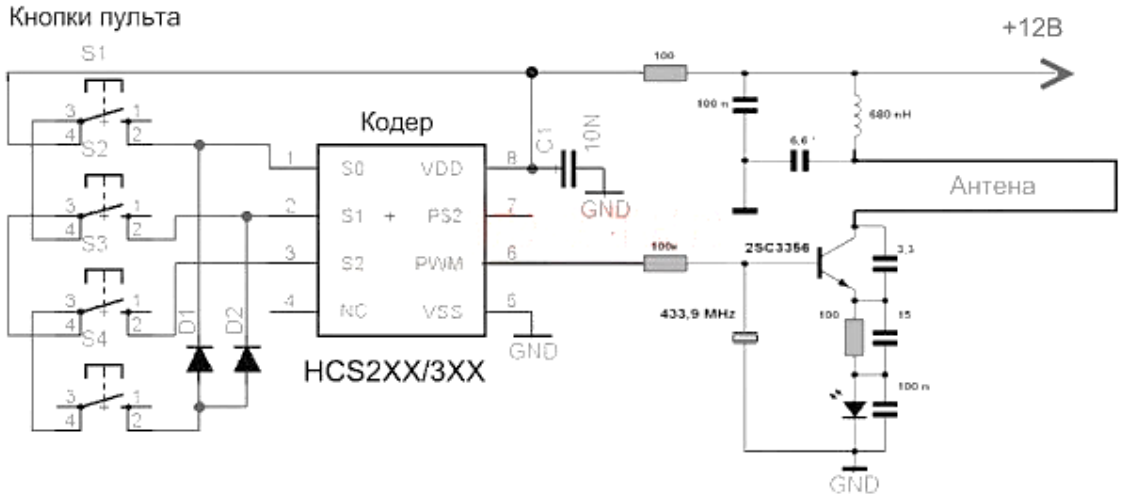


Рисунок 3.9 – Схема підключення HCS200 HCS300 Microchip

Декодери Microchip за технологією Keeloq

Декодери Keeloq призначені для дешефрації команд надходять від кодера по каналу зв'язку. Після перевірки прийнятого в кодової послідовності серійного номера і "стрибаючого коду", декодер на підставі функціонального коду активізує виходи відповідні входів кнопок в кодере. Виходи будуть утримуватися в активному стані до тих пір, поки натиснута кнопка на кодере. У таблиці представлені короткі характеристики кодереров HCS500, HCS512, HCS515 і з якими кодерами вони працюють [19].

Таблиця 3.2 – Декодери Microchip за технологією Keeloq

Пристрій	Кодова посилка біт	Кількість підтримуваних передавачів	Інтерфейс зв'язку	Функцій	Напруга живлення, В	Типи підтримуваних кодерів HCSXXX
HCS500	67	7	SPI	15	4,5 – 5,5	200, 300, 301, 360, 410
HCS512	67	4	-	15	3,0 – 6,0	200, 300, 301, 360, 361
HCS515	67	7	SPI	15	4,5 – 5,5	200, 201, 300, 301, 320, 360, 361, 362, 365, 370, 410, 412, 473

Для виконання команд декодоров, йому необхідно вказати 28/32-бітний серійний номер і 64-бітний секретний ключ кодера, а також однією з умов є синхронізація з кодером. У декодерах Keeloq використовується незалежна ключова система: для кожного пульта (передавача) в декодере зберігатися свій серійний номер, секретний ключ і поточна синхронізація.

3.4 Вибір компонентів

Так як ідея проекту полягає в тому щоб створити доволі універсальну і недорогу систему підбираємо доступні і недорогі компоненти.

3.4.1 Комп'ютер

Комп'ютер має бути з операційною системою Windows або Linux (краще друга). CUDA (Від англ. Compute Unified Device Architecture) - програмно-апаратна архітектура паралельних обчислень, яка дозволяє істотно збільшити обчислювальну продуктивність завдяки використанню графічних процесорів

фірми Nvidia. Наявність CUDA в комп'ютері істотно збільшить швидкість розпізнавання номерних знаків на стоп-кадрі з камери.

Raspberry Pi - це серія невеликих одноплатних комп'ютерів, розроблених у Великобританії Фондом Raspberry Pi спільно з Broadcom. На початку проект Raspberry Pi схилявся до пропаганди викладання базової інформатики в школах та країнах, що розвиваються. Пізніше оригінальна модель стала набагато популярнішою, ніж передбачалося, продаючи за межами цільового ринку для таких видів використання, як робототехніка. Зараз він широко використовується у багатьох областях, наприклад, для моніторингу погоди, через низьку вартість, модульність та відкриту конструкцію.

Після випуску другого типу плат, Фонд Raspberry Pi створив нову організацію, яку назвали Raspberry Pi Trading, і встановив Ебена Аптона як генерального директора, відповідаючи за розробку технологій. Фонд був переосвітлений як освітня благодійна організація для сприяння викладанню базових інформатик у школах та країнах, що розвиваються.

Raspberry Pi - один із найбільш продаваних британських комп'ютерів. Станом на грудень 2019 року було продано понад тридцять мільйонів плат. Більшість піс виготовляються на фабриці Sony у місті Пенкоед, Уельс, тоді як інші виготовляються в Китаї та Японії.

Якщо обрати Raspberry PI, то не знадобиться Arduino, так як останній використовується тільки для того щоб з комп'ютеру передати сигнал на передавач 443 мГц через GPIO виходи.

Для даного проекту було обрано звичайний персональний комп'ютер на операційній системі Windows, так як це самий доступний варіант, який є майже у кожного.

3.4.2 Arduino

Arduino - це апаратно-програмна компанія з відкритим кодом, спільнота проектів та користувачів, яка розробляє та виготовляє одноплатні мікроконтролери та набори мікроконтролерів для побудови цифрових пристроїв. Її апаратні продукти ліцензовані за ліцензією CC-BY-SA, тоді як програмне забезпечення ліцензовано за GNU Lesser General Public License (LGPL) або GNU General Public License (GPL), дозволяючи виготовлення плат Arduino та розповсюдження програмного забезпечення будь-ким. Плати Arduino можна придбати на офіційному веб-сайті або через уповноважених дистриб’юторів.

Для реалізації даної електронної системи підійде будь-який Arduino з хоча б одним GPIO виходом, живленням 5 В та можливістю підключитись до комп’ютера через інтерфейс USB.

Було обрано Arduino Uno Rev3, так як даний пристрій відповідає всім вимогам описаним вище, має велику популярність і як наслідок – велику кількість магазинів які продають дану плату, та має невелику вартість. Також Arduino Uno Rev3 має запас функціоналу відносно даного проекту, для можливості подальшого розвитку електронної системи.

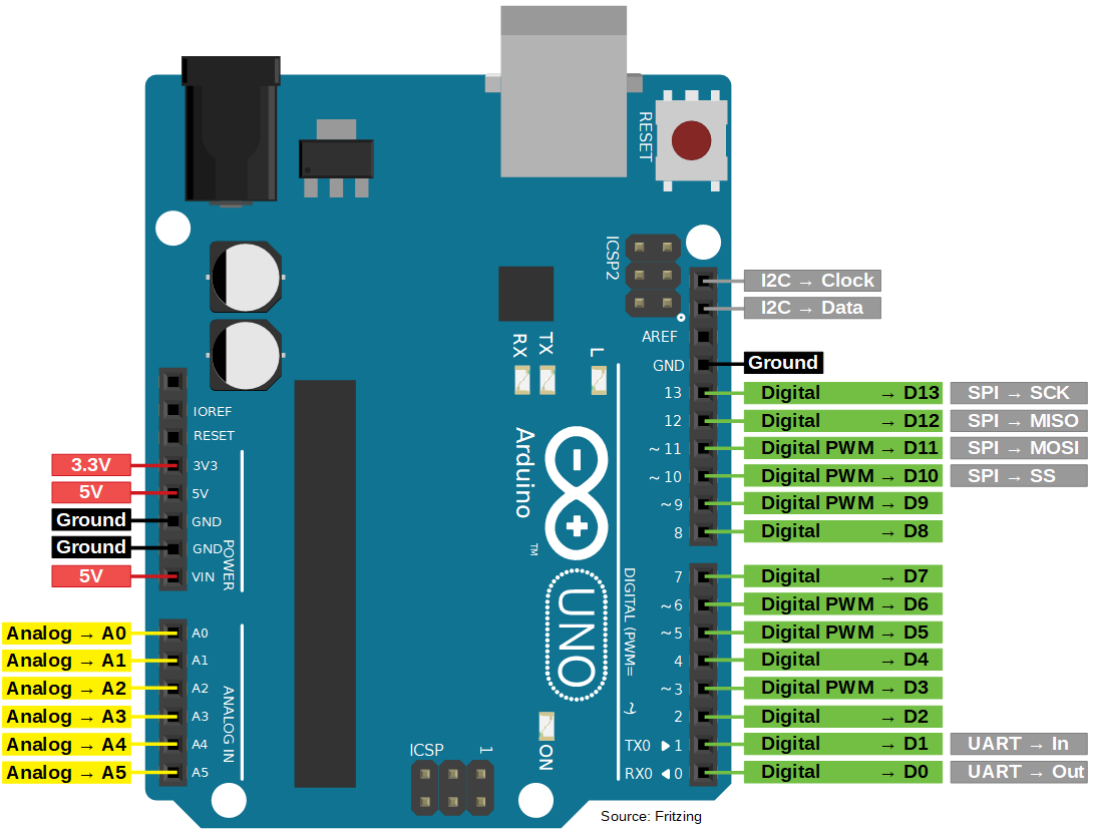


Рисунок 3.10 – входи/виходи Arduino Uno

3.4.3 Відеореєстратор

Відеореєстратор потрібно підбирати такий, який має моживість потокового мовлення камер. Це дає можливість встановити комп'ютер віддалено від відеореєстратора. Наприклад, якщо відеореєстратор транслює потік в мережу інтернет то комп'ютер можна віддаляти на велику відстань від реєстратора. Головне щоб відстань була не більше ніж радіус дії передавача 433 МГц. Якщо передавач буде встановлений біля шлагбауму і приймати сигнал також через мережу інтернет то комп'ютер можна віддаляти на будь-яку відстань, але в даному проекті розглядаємо тільки пряме підключення передавача через Arduino, який підключений до комп'ютера по інтерфейсу USB.

В житловому комплексу вже встановлений IP відеореєстратор Hikvision, котрий і буде використовуватись в даній електронній системі керування

засобами доступу до об'єкта. Раєстратор для потокової трансляції відео використовує протокол Hikvision (8000 порт).

Розглянемо хід налаштування відеореєстратора Hikvision для можливості видаленого підключення до нього через мережу інтернет.

Трансляція порт-адреси (англ. Port address translation, PAT) - технологія трансляції мережевої адреси в залежності від TCP / UDP- порту одержувача. Є окремим випадком NAT [20]. Також може використовуватися термін DNAT (Destination NAT). Це говорить Вікіпедія, а простими словами кидок портів - відкриття зовнішнього доступу до вашої внутрішньої мережі з Інтернету за допомогою позначення на роутері або маршрутизаторі точок їх "зіткнення".

Кидок портів дає можливість отримати настроюється доступ до вашої локальної мережі з мережі Інтернет, що дозволяє, наприклад, перебуваючи далеко від об'єкта спостереження знімати дані з камер за допомогою звичайного веб-браузера, додатки спостереження IVMS-4200 або мобільного додатка IVMS-4500.

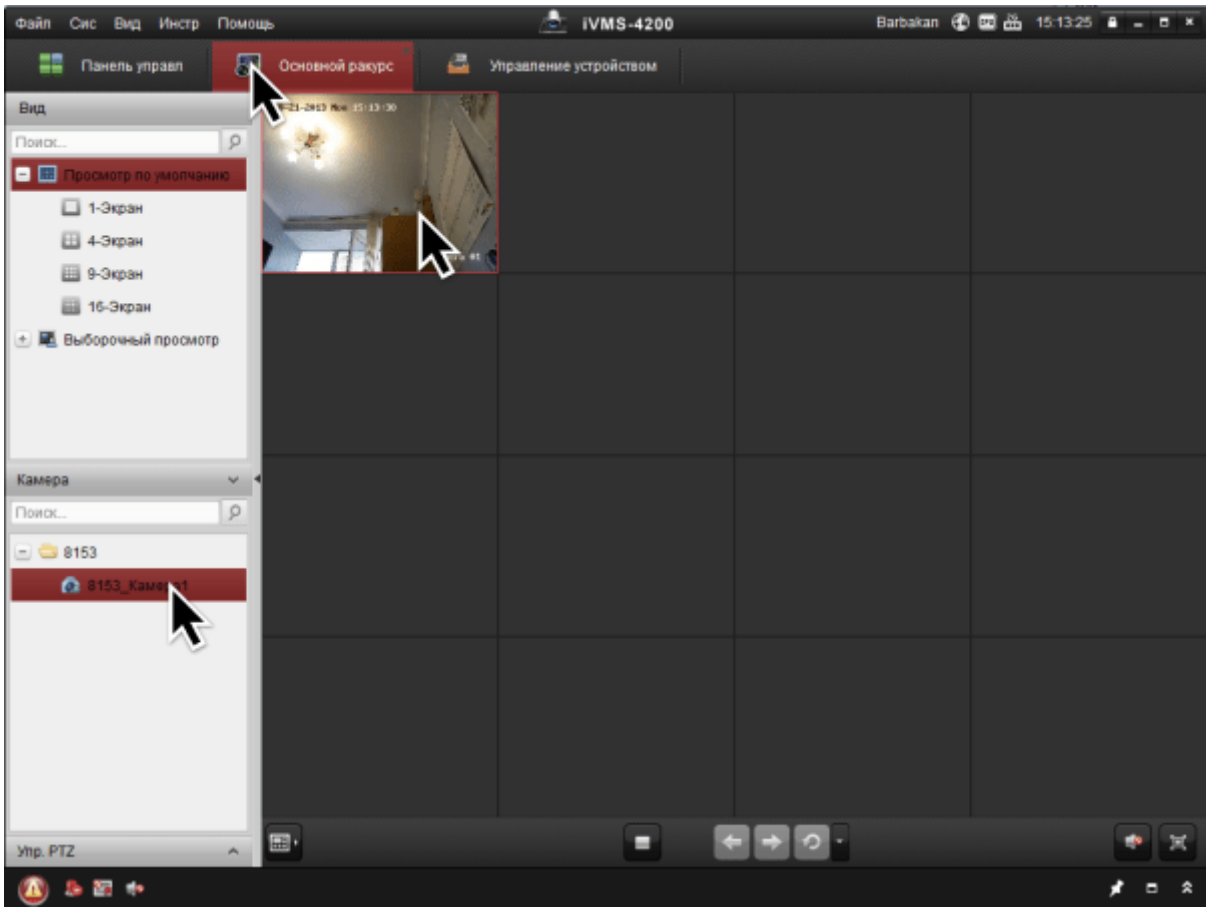


Рисунок 3.11 – Віддалене підключення до IP-камері через IVMS-4200

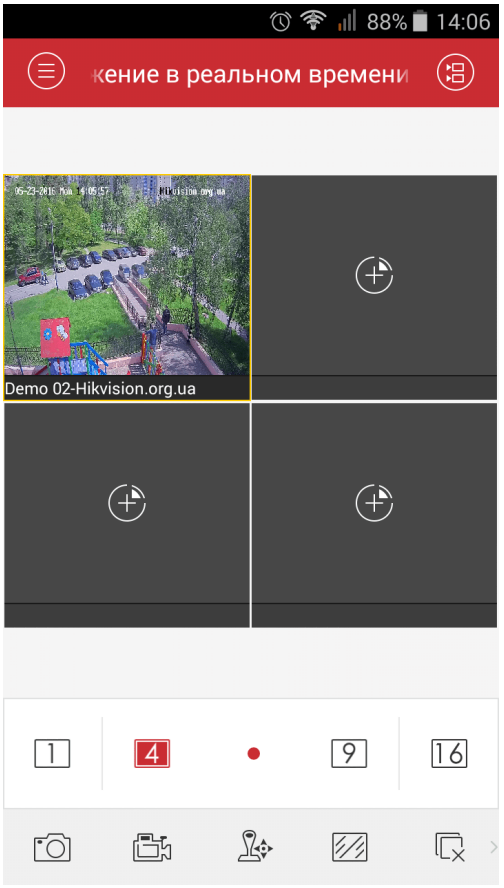


Рисунок 3.12 – Віддалене підключення до IP-камері через IVMS-4500

По-перше, для зовнішнього доступу до локальної мережі без використання хмари або додаткових проміжних сервісів, ваш IP-адреса має бути білим, статичним, тобто не змінюється від сесії до сесії. З'єднання в такому випадку надійне і захищене. Деякі провайдери надають білий IP безкоштовно, а у інших за нього доводиться платити.

Щоб дізнатися свій IP-адресу, можна написати в пошуковику, наприклад, "мій IP", "дізнатися IP" і т.д., або отримати свій IP в налаштуваннях роутера. Після порівняйте його зі списками " сірих" (динамічних) IP-адрес, але найпростіше, щоб уникнути непорозумінь, зв'язатися з провайдером і обумовити окремо, що вам потрібен постійний зовнішній IP.

Сірі IP-адреси:

- 10.0.0.0 - 10.255.255.255

- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Налаштування роутера / маршрутизатора

Якщо IP адреса не статична але «біла», то потрібно додатково налаштувати на роутера DDNS. DDNS – це динамічна ієрархічна розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу.

Для отримання прямого доступу до камери потрібно налаштувати роутер способом "проброса" на ньому портів або "маршрутизації". Налаштування роутера (NAT) виконується за інструкцією від виробника маршрутизатора. Для простоти припустимо, що ми маємо справу з роутером (для маршрутизатора все йде так само). Щоб зайти в налаштування роутера найпростіше знайти відеоінструкцію за запитом «проброска портів на "назву і модель роутера"».

У загальних рисах це виглядає наступним чином:

Потрыбно перейти на внутрішній IP роутера ("192.168.0.1", або "10.0.0.1", або будь-який інший, він вказаний в інструкції до роутера), ввести логін і пароль (стандартний логін і пароль вказаний на нижній частині роутера). Знайти пункт "Налаштування NAT / DNAT" / "Port forwarding" / "Віртуальний сервер".

Рисунок 3.13 – Приклади сторінок настройки портів в веб-інтерфейси роутерів

Потрібно налаштувати маршрутизацію таким чином, щоб перенаправити передачу даних з зовнішньої мережі на внутрішню по необхідних портів. Простіше кажучи, прописати кілька рядків із зазначенням IP-адреси камери і відповідні номери, що позначають самі порти в своїх рядках. Зверніть увагу, що маршрутизація повинна бути "дзеркальної" (тобто, з порту 8000 зовнішньої мережі на порт 8000 внутрішньої), інакше підключення може працювати некоректно.

Порти для доступу до камери:

1. 80 - веб-інтерфейс;
2. 554 - RTSP-порт для прямого отримання потоку з камери [21];
3. 8000 - SDK-порт, необхідний для підключення до ПО IVMS і реєстраторам;
4. 8200 - порт даних, сервісний порт. Визначається автоматично (порт №4 = порт №3 +200).

В налаштуваннях камери порти можна змінити на інші. Це може бути необхідно, якщо в одній локальній мережі знаходиться декілька пристроїв, що вимагають для себе окремі порти. Наприклад, якщо на першій камері порти 80, 554, 8000 і 8200, то на другій камері необхідно проставити порти 81, 555, 8001 і 8201. Після проброса портів по своєму зовнішньому IP-адресою можна зайти на пристрій з Інтернету в вікні браузера. При зміні 8000 порту на інший, порт 8200 зміниться автоматично (порт №4 = порт №3 +200).

Приклад: при зміні 8000 порту в камері на 8004, порт 8200 автоматично зміниться на 8204.

Якщо з якоїсь причини вам знадобилося звернутися до конкретного порту з браузера (наприклад, зайти на веб-інтерфейс камери), це можна зробити, ввівши в адресний рядок адресу веб-інтерфейсу камери в формі:

"IP адреса": "номер порту", наприклад, 111.111.111.111:80.

Рисунок 3.14 – Сторінка входу веб-інтерфейсу камери при віддаленому доступі

3.4.4 Передавач

Передавач має працювати від живлення 3.3 В або 5 В. Та має один вхід для даних.

Було обрано пару «приймач – передавач» STX882 + SRX882.

SRX887 - це супергетеродинний модуль приймача, що має потужну рушійну силу. Він має високу стабільність, захист від перешкод та економічну ефективність, але також має потужну рушійну силу, сертифіковану ROHS, FCC, CE, Модуль може бути підключений безпосередньо до мікроконтролера. Так це зручніше для користувачів, які розробляють бездротові продукти. Його також можна використовувати на Arduino та Raspberry Pi.

Переваги STX882: низька вартість, малий розмір, ультра-висока потужність.

Має вищу стабільність і високу рентабельність, на 3.6В потужність може досягати 50 МВт.

Порти модуля можуть бути безпосередньо підключені до мікроконтролеру.

Характеристики:

- робоча напруга: 3.3 В
- довжина х ширина х висота: 12 х 15.3 х 6.2 мм
- вага в грамах: 1.26
- дальність передачі: <100м
- частота: 433 МГц
- швидкість передачі даних: до 10 Кб / сек
- потужність передавача: 50 мВт

Таблиця 3.3– Електронні характеристики передавача STX882-443

Parameter	Min	Typ.	Max.	Unit	Condition
Operation condition					
Working voltage	1.2	3.0	6	V	
Temperature range	-20	25	70	℃	
Current consumption					
TX current		34		mA	@3.3V,15dBm
Sleep Current		⩽0.01		uA	@DATA As Low level
RF parameters					
Frequency Range	433.82	433.92	434.02	MHZ	@433MHZ
	314.9	315	315.1	MHZ	@315MHZ
RF power	12	13	13.5	dBm	@2.4V
	14	15	15.5	dBm	@3V
	19	20	20.5	dBm	@5V
Air rate	0.1		9.6	Kbps	

STX882 - це недорогий, невеликий розмір, надпотужний модуль передавача ASK з низькою гармонікою. Він має високу стабільність і високу вартість, при потужності 3,6 В для досягнення 50 мВт, в даний час він знаходиться на ринку під тим самим напругою, який передає модуль передачі потужності ASK. Модуль можна підключити безпосередньо до мікроконтролера. Так це зручніше для користувачів, які розробляють бездротові продукти.

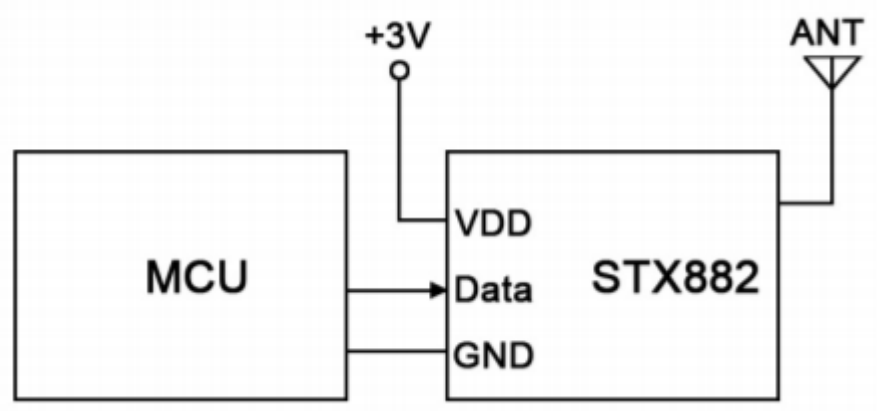


Рисунок 3.15 – Схема підключення передавача до Arduino/Raspberry Pi

Також передавач має досить малі розмірі що додає системі компактності.

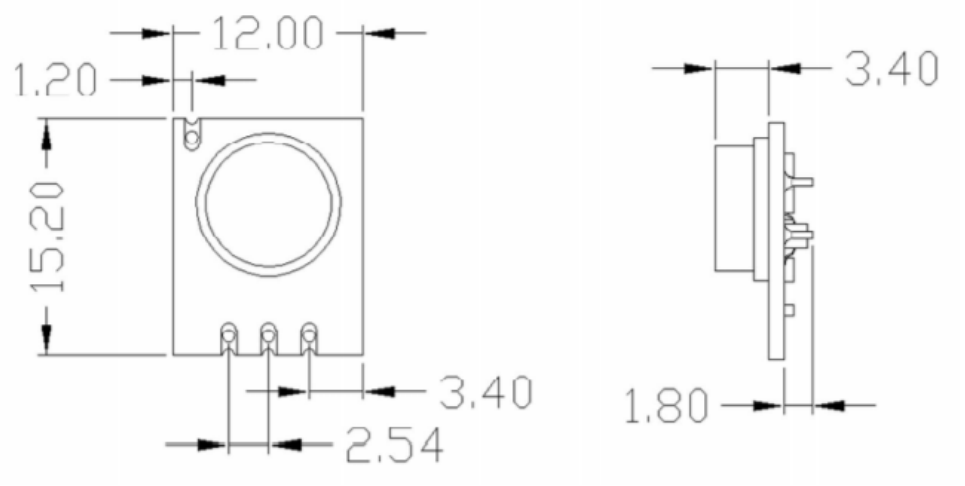


Рисунок 3.16 – Фізичні розміри передавача STX882-443. Розміри вказані в міліметрах

Висновки до розділу

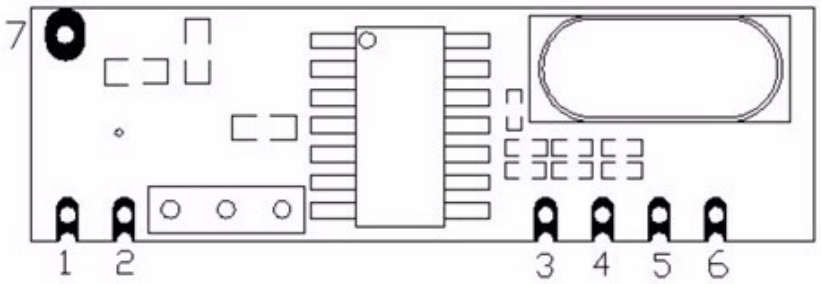
В ході виконання даного розділу, оттримані наступні висновки:

1. Структурна схема включає: камера, відеореєстратор, комп’ютер, Arduino та передавач даних який працює на частоті 433 МГц.
2. Обираючи приймач та передавач який працює на частоті 433 МГц потрібно звернути увагу, що модуляція має бути обов’язково амплітудна.
3. Якщо комп’ютер встановлюватиметься на віддалені то відеореєстратор має тами «білу» статичну IP адресу. Комп’ютер бажано щоб мав CUDA, так як його наявність істотно збільшить швидкість розпізнавання номерних знаків на стоп-кадрі з камери.
4. Антену 433МГц передавача можна живити як 3.3 В так і 5 В. Проте при нижчій напрузі він матиме нижчу потужність безпровідної передачі. При 3.3 В потужність буде приблизно 16 dBm, а при 5 В – 20.5 dBm.
5. Проаналізувавши наявну компонентну базу, обрано ключові компоненти схеми.

4 РОЗРОБКА ПРОГРАМНОГО ЗАБЕПЕЧЕННЯ

4.1 Сканування коду відкриття

Для того щоб Arduino передавав на передавач код відкриття шлагбауму потрібно сканувати код який посилає пульт керування шлагбаумом. Для цього використаємо Arduino з приймачем 433 МГц сигналу SRX882-433.



Pin Number	Pin Definitions	Description
1	ANT	Connect with 50 ohm coaxial antenna
2	GND	Connected to power ground
3	VCC	Positive power supply
4	CS	1: Normal working 0: Sleep mode
5	DATA	Data output
6	GND	Connected to power ground
7	ANT	Connect with 50 ohm coaxial antenna

Рисунок 4.1 – Входи/виходи приймача 433 МГц сигналу SRX882-433

Таблиця 4.1 – Електронні характеристики передавача STX882-443

Входи/виходи	
SRX882-433	**Arduino**
6 (GND)	GND
3 (VCC)	5V
5 (DATA)	DIGITAL 2

Антену підключати не потрібно, щоб випадково не сканувати сигнал шуму чи сигнал іншого ключа. Свій ключ потрібно буде піднести до приймача перед натисканням на кнопку відкривання шлагбауму. Для впевненості в роботі

приймача можна його 4 вихід підключити на Arduino вихід 5V, але це не обов’язково.

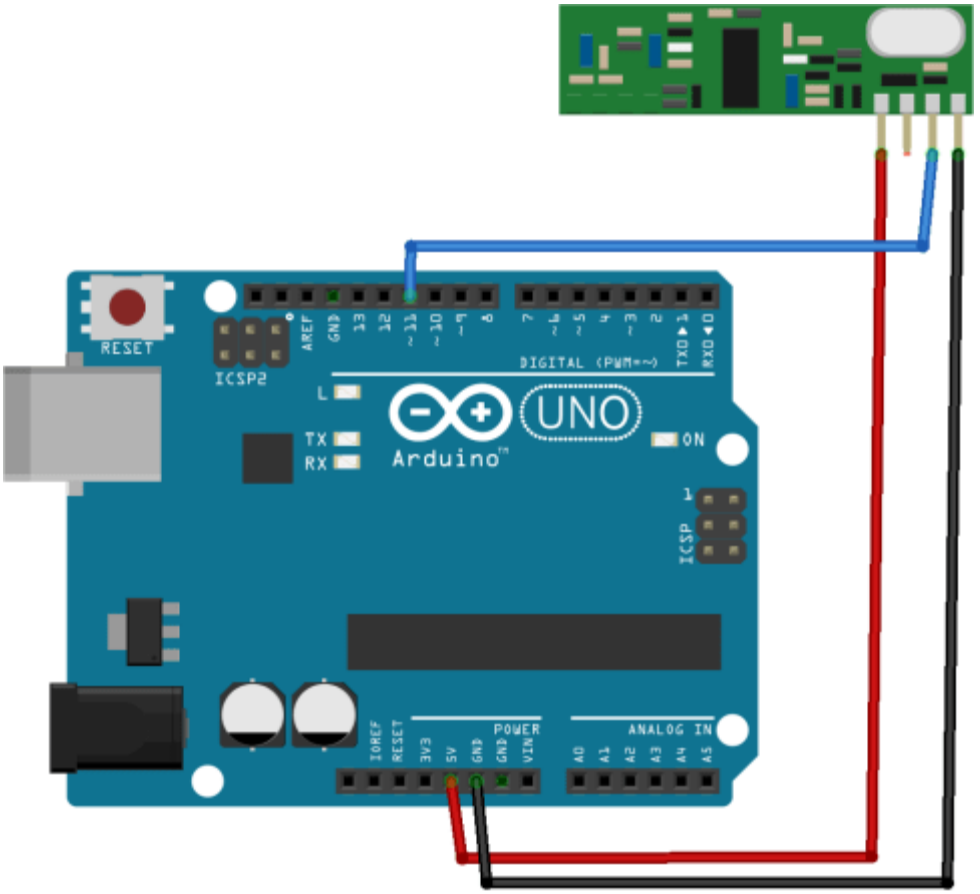


Рисунок 4.2 – Схема підключення приймача до Arduino

Далі відкриваємо Arduino IDE. Потрібно встановити бібліотеку для роботи з 315/433 МГц AM- приймачами/передавачами. Переходимо в вкладку «Інструменти», далі натискаємо «Управління бібліотеками…» (Ctrl+Shift+I). Справа зверху в полі вводимо «rcswitch». Встановлюємо знайдену бібліотеку.

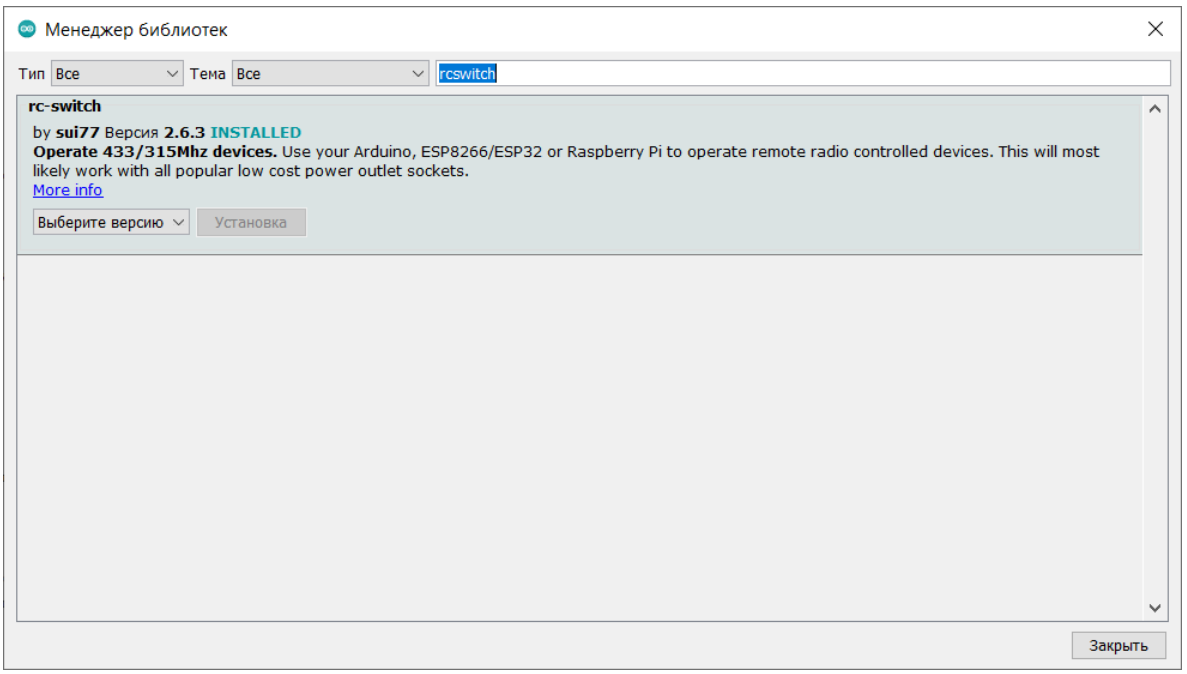


Рисунок 4.2 – Управління бібліотеками Arduino IDE

Після того як схема зібрана, можна прошивати скетч (Див. Додаток Б програмний код) на Arduino.

ReceiveDemo_Simple

```
/*
  Simple example for receiving

  https://github.com/sui77/rc-switch/
*/

#include <RCSwitch.h>

RCSwitch mySwitch = RCSwitch();

void setup() {
  Serial.begin(9600);
  mySwitch.enableReceive(0);  // Receiver on interrupt 0 => that is pin #2
}

void loop() {
  if (mySwitch.available()) {

    Serial.print("Received ");
    Serial.print( mySwitch.getReceivedValue() );
    Serial.print(" / ");
    Serial.print( mySwitch.getReceivedBitlength() );
    Serial.print("bit ");
    Serial.print("Protocol: ");
    Serial.println( mySwitch.getReceivedProtocol() );

    mySwitch.resetAvailable();
  }
}
```

Рисунок 4.2 – Лістинг скетчу в Arduino IDE, який сканує коди на частоті 433 МГц

Після того як скетч завантажиться на Arduino відкриваємо монітор порту. Підносимо ключ до приймача і натискаємо кнопку відкриття шлагбауму який буде автоматизовуватись. Отримуємо відповідь від Arduino в форматі:

Received 9286993 / 24bit Protocol: 1,

де 9286993 – код, 24bit – його бітність, 1 – протокол передачі даних, який використовується.

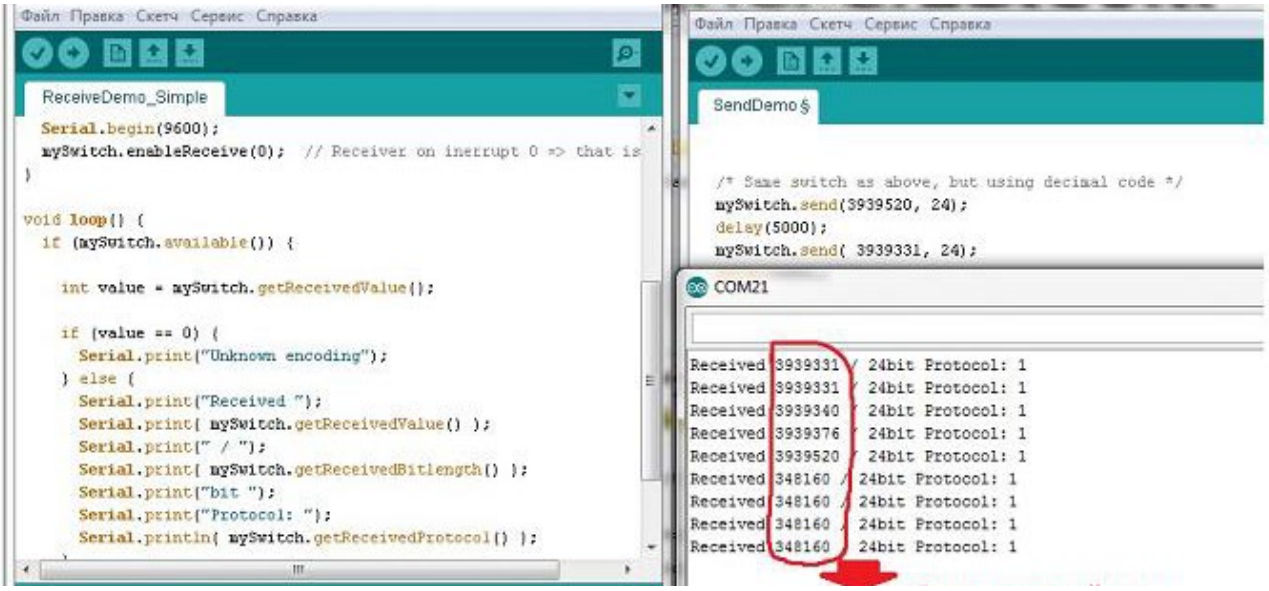


Рисунок 4.3 – Прийнятий код (обведено червоним)

4.2 Розробка основного скрипту

Основний скрипт бере стоп-кадр з відеопотоку відеореєстратора. Сканує кадр на наявність автомобільних номерів в зоні заїзду. Якщо в кадрі в зоні заїзду розпізнається номерний знак транспортного засобу, то номер звіряється з базою даних номерних знаків мешканців ЖК. Якщо номер є в базі то основний скрипт відправляє через COM порт сигнал на Arduino щоб той відкрив шлагбаум. (Див. Додаток В основний програмний код)

Також скрипт при запуску додає в базу даних відсутні данні про марку модель і колір машини, по номеру ТЗ, з відкритої української бази автомобільних номерів України «Avto-Nomer.com.ua» [22].

Функція отримання стоп-кадру з камери

Це функція яка отримує стоп-кадр з камери яка підключена до відеорєстратора Hikvision, котрий транслює потік в мережу (локальну або глобальну).

Для реалізації даної функції використана бібліотека «hikvisionapi».

Вхідні дані функції:

- **Host** – IP адреса відеореєстратора. Вона може бути як локальною так і глобальною в мережі інтернет. Якщо реєстратор транслює потік в мережу інтернет то провайдер має надавати «білу» IP адресу, тобто не за NAT провайдером;
- **Port** – зовнішній порт в який транслюється потік;
- **User** – ім’я користувача для доступу до відеореєстратора;
- **Password** – пароль для доступу до відеореєстратора;
- **Channel** – канал камери.

Вихідні дані функції:

- **Рядок** в якому вказаний шлях куди зберігся стоп-кадр

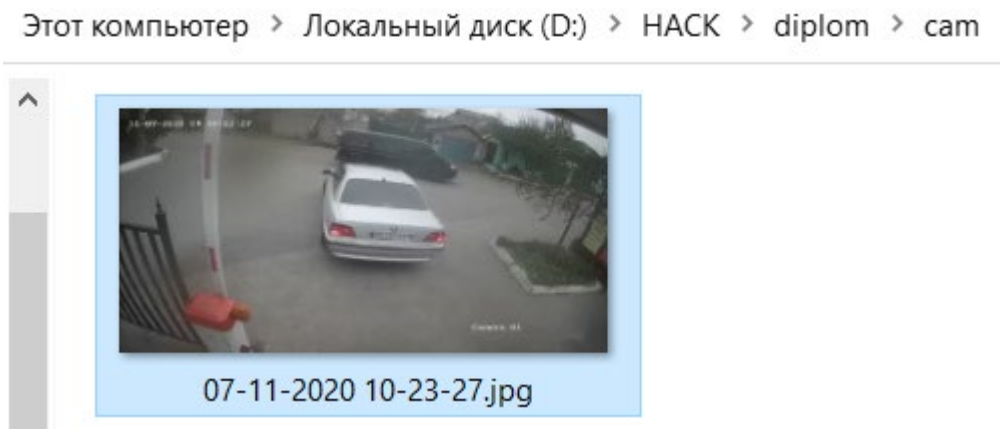


Рисунок 4.3 – Результат виклику функції отримання стоп-кадру

Рисунок 4.4 – Стоп-кадр з камери на в’їзді в територію з обмеженим доступом

Функція розпізнавання номерних знаків

Для розпізнавання номерних знаків транспортних засобів було обрано бібліотеку «NomeroffNet».

Nomeroff Net - це розпізнавальна система розпізнавання номерних знаків для мови програмування python 3-ї версії, заснована на застосуванні нейронної мережі сегментації та адаптованому OCR-модулі, що працює на основі архітектури GRU.

Нижче представлений список компаній які надають послуги розпізнавання номерних знаків:

Automatic License Plate Recognition

Є opensource і комерційна версія. Opensource-версія показала дуже низький відсоток розпізнавання, крім того, вона вимагала специфічні залежності для своєї збірки і роботи (особливо нам не сподобалася). Комерційна версія, вірніше комерційний сервіс працює добре. Вміє працювати з російськими та українськими номерами. Ціни помірні - 49 $ / 50K розпізнавань в місяць.

Recognitor

Хороша якість. Зону з номером знаходить дуже добре. Сервіс не вміє працювати з українськими та європейськими номерами. Варто відзначити хорошу роботу з неякісними знімками (в снігу, фото невеликого формату, ...). Ціна на сервіс теж прийнятна, але за малі обсяги беруться неохоче.

Є безліч комерційних систем із закритим ПЗ, але гарною opensource реалізації немає, хоча й інструменти з відкритим кодом, які лежать в основі вирішення цього завдання давно вже існують.

Які інструменти потрібні для розпізнавання номерів

Знаходження об'єктів на зображенні або в відео-потоці це завдання з області комп'ютерного зору, яка вирішується різними підходами, але найчастіше за допомогою, так-званих, згортальних нейронних мереж. Потрібно знайти не просто область на фото в якій зустрічається шуканий об'єкт, але і відокремити всі його точки від інших об'єктів або фону. Цей різновид завдань називається «Instance Segmentation». На ілюстрації нижче візуалізовані різні типи завдань комп'ютерного зору.

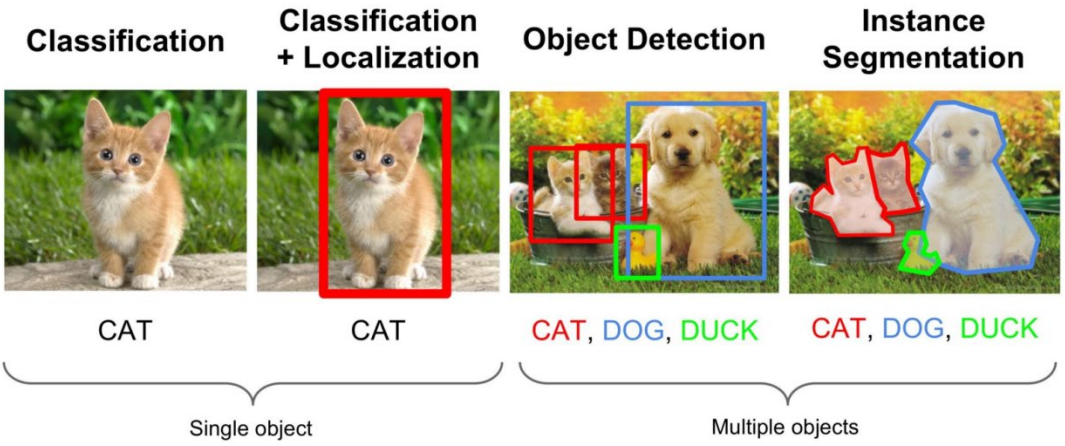


Рисунок 4.5 – Класифікація об’єктів комп’ютерним зором

Із сучасних архітектур згортальних мереж для задач сегментації часто використовують: U-Net або Mask R-CNN . Було обрано Mask R-CNN.

Другий інструмент, яка знадобиться - це бібліотека з розпізнавання текстів, яка б могла працювати з різними мовами і яку можна легко налаштовувати під специфіку текстів, які будемо розпізнавати. Тут вибір не такий вже й великий, найрозумнішою є tesseract від Google.

Так само є ряд менш «глобальних» інструментів, за допомогою яких потрібно буде нормалізувати область з номерним знаком (привести його в такий вид, при якому розпізнавання тексту буде можливим). Зазвичай для таких перетворень використовують opencv.

Так само, можна буде спробувати визначити країну і тип, до якої відноситься знайдений номерний знак, щоб в пост обробці застосувати уточнююче шаблон, характерний для цієї країни і цього типу номера. Наприклад, український номерний знак, починаючи з 2015 року оформлений в синьо-жовтому оформленні складається з шаблону «дві букви чотири цифри дві літери».

Рисунок 4.6 – Державний номер знак України нового зразку (після 2015 року)

Крім того, маючи статистику частоти «зустрічей» в номерних знаках того чи іншого поєднання букв або цифр можна поліпшити якість обробки поста в «спірних» ситуаціях.

Знадобляться наступні програмні компоненти:

- Python3;
- opencv-python не нижче версії 3.4;
- Mask RCNN, tesseract;
- через менеджер пакетів pip3 потрібно буде встановити кілька модулів на python3.

Модулі для python3:

- cython
- numpy>=1.16.*
- tensorflow>=2.3.*
- opencv_python
- tqdm
- setuptools
- scikit_image
- jupyter
- imgaug

- detectron2
- asyncio
- pycocotools
- matplotlib
- GitPython
- torch==1.6.*
- torchvision==0.7.0
- PyYAML==5.3

Для встановлення бібліотеки NomeroffNet потрібно склонувати git написавши в терміналі наступний код:

git clone https://github.com/ria-com/nomeroff-net.git -b 0.1.0

cd nomeroff-net

git clone https://github.com/youngwanLEE/centermask2.git [23]

Для Centos, Fedora і інших RedHat OS:

yum install python3-devel

yum install gcc

yum install libSM [23]

Для Ubuntu і інших Debian OS:

apt-get install gcc

apt-get install -y libsm6

apt-get install -y libglib2.0

apt-get install python3.6-dev

apt-get install -y libfontconfig1 libxrender1 [23]

Встановлення python залежностей:

pip3 install torch==1.6

pip3 install PyYAML==5.3

pip3 install 'git+https://github.com/facebookresearch/detectron2.git'

pip3 install torchvision==0.7.0

pip3 install Cython

pip3 install numpy

pip3 install -r requirements.txt [23]

Вхідні дані функції:

- **Рядок** в якому вказаний шлях куди зберігся стоп-кадр

Вихідні дані функції:

- **Список** рядків розпізнаних номерних знаків.

Рисунок 4.7 – Результат виклику функції розпізнавання номеру

Метод відправки в Arduino команди відкриття шлагбауму

Коли розпізнаний номер збігається з номером який є в базі даних мешканців ЖК python скрипт через COM порт відправляє сигнал (байт «1») на Arduino методом:

serial.Serial(com_port, 9600).write(b'1'),

де *com_port* – послідовний порт Arduino (наприклад "COM7”)

Інші функції

Також є додаткові функції створені для зручності і функціоналу скрипту.

Функція *get_vehicle(plate_number)*

Її задача парсити з бази «avto-nomer.com.ua» дані про ТЗ.

Функція *update_vehicle_in_database(csv_path)*

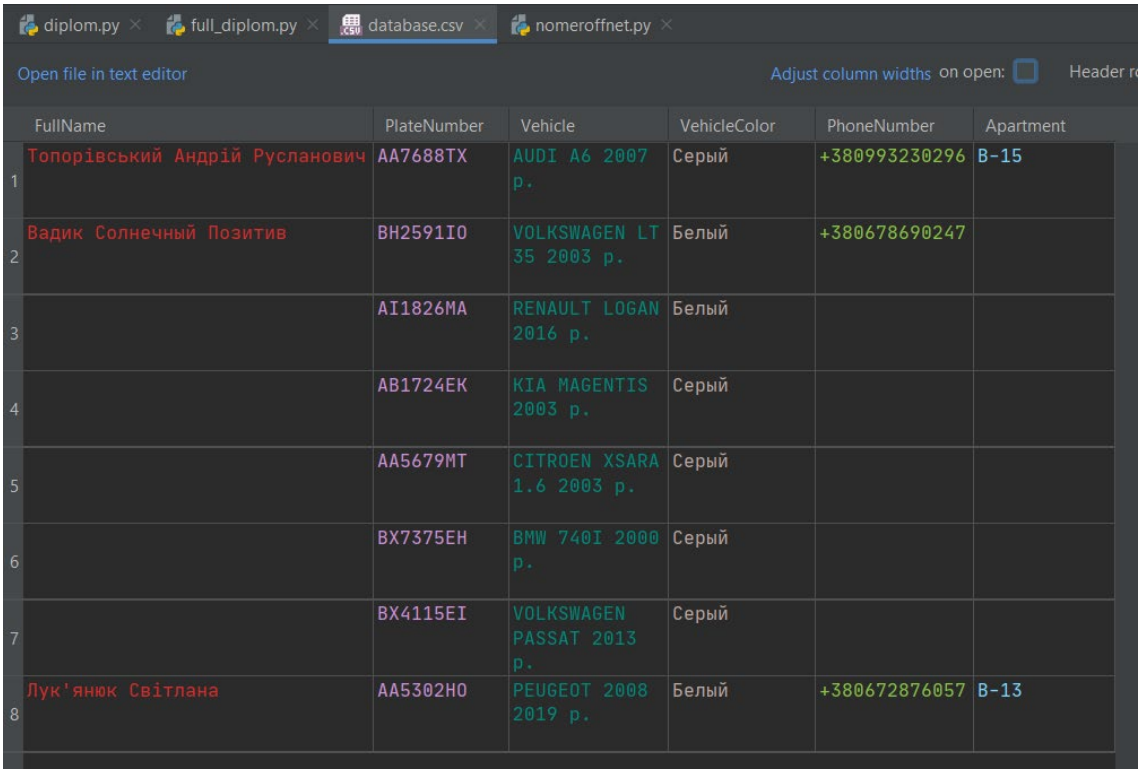
Оновлює отриману інформацію про ТЗ в базу.

Функція *get_plate_numbers_from_database(csv_path)*

Повертає з бази даних список номерних знаків в ній.

База даних

В якості бази даних було обрано простий CSV файл. Так як він займає малий об’єм пам’яті, швидкий та зручний в доступі.



	FullName	PlateNumber	Vehicle	VehicleColor	PhoneNumber	Apartment
1	Топорівський Андрій Русланович	AA7688TX	AUDI A6 2007 р.	Серый	+380993230296	B-15
2	Вадик Солнечный Позитив	BH2591IO	VOLKSWAGEN LT 35 2003 р.	Белый	+380678690247	
3		AI1826MA	RENAULT LOGAN 2016 р.	Белый		
4		AB1724EK	KIA MAGENTIS 2003 р.	Серый		
5		AA5679MT	CITROEN XSARA 1.6 2003 р.	Серый		
6		BX7375EH	BMW 740I 2000 р.	Серый		
7		BX4115EI	VOLKSWAGEN PASSAT 2013 р.	Серый		
8	Лук'янюк Світлана	AA5302HO	PEUGEOT 2008 2019 р.	Белый	+380672876057	B-13

Рисунок 4.8 – Скріншот бази даних

Блок-схема

Виходячи з створених функцій і ідеї проекту розроблено блок схему скрипту.

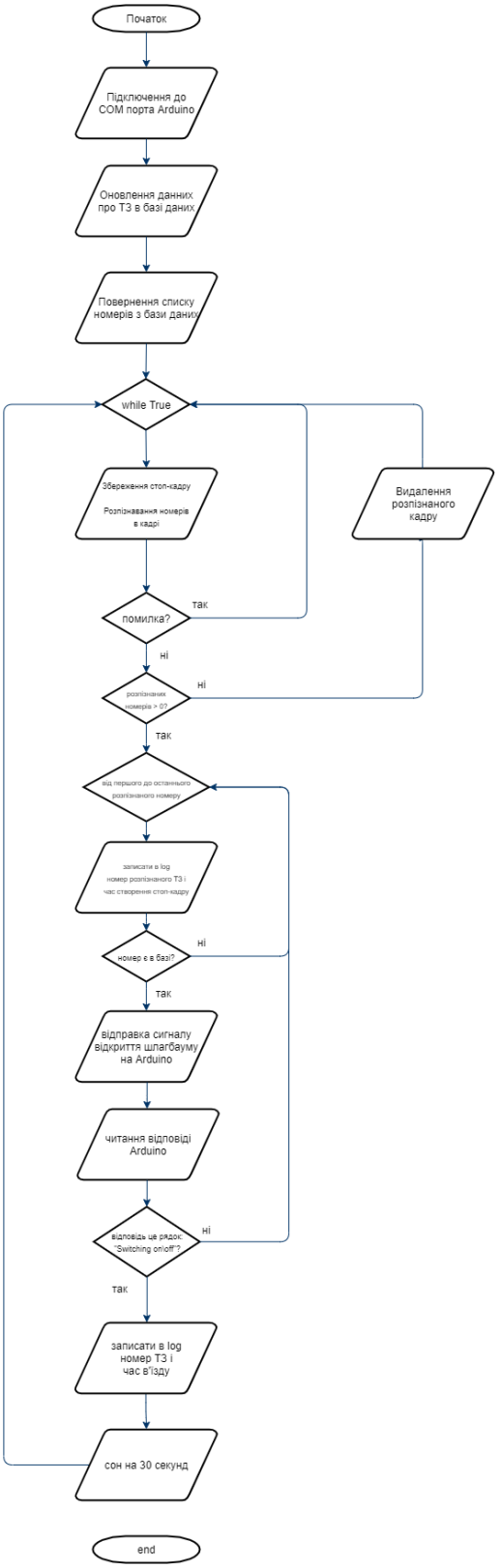


Рисунок 4.9 – Блок-схема роботи скрипту

4.3 Скетч для Arduino

Основна задача Arduino – це по сигналу від основного скрипту, відправити код відкриття шлагбауму (Див. Додаток Г скетч).

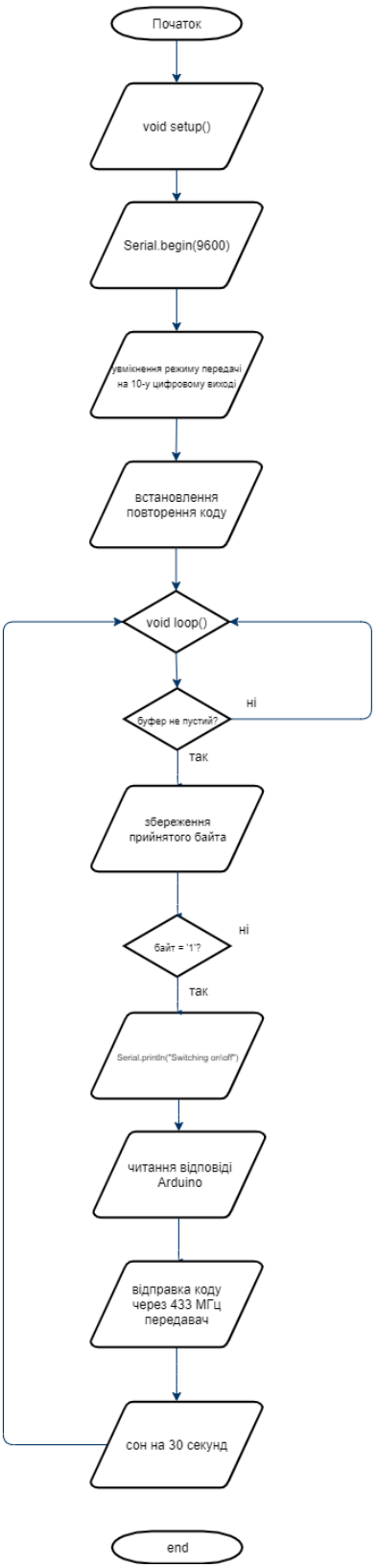


Рисунок 4.10 – Блок-схема роботи скетчу

Висновки до розділу

1. На базі існуючих бібліотек та найкращих практик при роботі з комп’ютерним зором, розроблено програмне забезпечення автоматизації шлагбауму.
2. Nomeroff Net дозволяє розпізнавати номерні знаки навіть якщо вони повернуті майже перпендикулярно відносно матриці камери, що дозволяє обмежитись встановленням в коді правильної зони розпізнавання, і не оформлювати в’їзд на об’єкт з обмеженим доступом так щоб машина стояла прямо перед камерою.
3. Весь код написаний в процедурному стилі (не об’єктно орієнтованому).
4. Программа включає перевірку номерних знаків з базою даних
5. Також програмне забезпечення виконує ведення записів відвідувань ЖК.

ВИСНОВКИ

У магістерській дисертації запропоновано варіант реалізації електронної системи керування засобами доступу до об’єкта.

Проведено дослідження методів та технологій розпізнавання номерних знаків. Проаналізовано програмні та апаратні засоби створення електронної системи керуванням засобами доступу до об’єкта, та запропоновані рішення, що дозволяють спростити і здешевити ввартість реалізації такої системи.

На основі проведених досліджень отримано наступні результати:

1. Основний скрипт, який аналізує стоп-кадр з IP камери на наявність в ньому номерних знаків, порівнює розпізнані номера з номерами в базі даних та при співпадінні відправляє сигнал на Arduino для подальшого відкриття шлагбауму.
2. На підставі недоліків та переваг використання основних технологій для розпізнавання номерних знаків, обрано бібліотеку для мови програмування python 3, яка виконувала функцію розпізнавання номерних знаків ТЗ.
3. Розроблена структурна схема включає МК, передавач 433 МГц.
4. Розроблено скетч для Arduino, який приймає сигнал від основного скрипту і спрацьовує на відкривання засобу доступу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЯ

1. Юджин Шульц. Ризики через зближення систем фізичної безпеки та середовищ інформаційних технологій. 2007. С. 80–84.
2. Niemelä Harri. Вивчення ділових можливостей та доданої вартості програм NFC в галузі безпеки. 2011. URL: https://www.theseus.fi/handle/10024/37824 (дата звернення: 22.09.2020).
3. Ньюмен Роберт. Безпека та контроль доступу за допомогою біометричних технологій. 2010. URL: https://www.worldcat.org/oclc/535966830 (дата звернення: 01.10.2020)
4. Федеральна експертна рада фінансових установ. Аутентифікація в банківському середовищі Інтернету. 2008. URL: https://www.ffiec.gov/pdf/authentication_guidance.pdf (дата звернення: 01.10.2020).
5. Офіс майбутнього MicroStrategy включає мобільну ідентифікацію та кібербезпеку. 2014. URL: https://www.washingtonpost.com/business/capitalbusiness/microstrategys-office-of-the-future-includes-mobile-identity-and-cybersecurity/2013/04/13/eb82e074-a1e3-11e2-be47-b44febada3a8_story.html (дата звернення: 04.10.2020).
6. iPhone 5S: переломний момент у біометрії? 2013. URL: https://www.bankinfosecurity.com/iphone-5s-biometrics-turning-point-a-6065/op-1 (дата звернення: 05.10.2020).
7. Контроль доступу NFC: прохолодно і швидко, але не близько. 2013. URL: https://www.securitysystemsnews.com/article/nfc-access-control-cool-and-coming-not-close (дата звернення: 07.10.2020).
8. Покиньте ці липкі брелки: легкий доступ за допомогою ключа EC. 2012. URL: https://web.archive.org/web/20140407101653/http://www.wirelessdesignmag.co

m/blogs/2012/06/ditch-those-tacky-key-chains-easy-access-ec-key (дата звернення: 07.10.2020).

9. Kisi And KeyMe, два додатки для смартфонів, можуть зробити застарілі клавіші від будинку. 2013. URL: https://www.huffpost.com/entry/house-keys-extinct_n_4339682, (дата звернення: 20.10.2020).
10. Родос Брайан. Розробка посібника з контролю доступу. 2019. URL: https://ipvm.com/reports/designing-an-access-control-system (дата звернення: 20.10.2020).
11. Відкриття нових дверей з контролем доступу до IP - Secure Insights. 2018. URL: https://www.axis.com/blog/secure-insights/opening-new-doors-with-ip-access-control/ (дата звернення: 20.06.2018).
12. Еволюція контролю доступу. 2019. URL: https://www.isonas.com/news-education/the-evolution-of-access-control/ (дата звернення: 25.10.2020).
13. Система управління інцидентами :: NIMS Online :: Обслуговування спільноти Національної системи управління інцидентами (NIMS). 2007. URL: https://web.archive.org/web/20070318154341/http://www.nimsonline.com/nims_3_04/incident_command_system.htm (дата звернення: 29.10.2020).
14. Інтелектуальна політика контролю доступу для житлових та комерційних будівель. 2019. URL: https://clonemykey.com/all/smart-access-control-policies-for-residential-commercial-buildings/ (дата звернення: 02.11.2020).
15. Грем Пулфорд. Механічні замки з високим рівнем безпеки: Енциклопедичний довідник . 2007. С. 76
16. Кібербезпека: контроль доступу. 2014. URL: https://evolllution.com/opinions/cybersecurity-access-control/ (дата звернення: 05.11.2020).
17. SP 800-162, Посібник із визначення атрибутів та контролю доступу (ABAC). 2014. URL: https://web.archive.org/web/20160305222004/http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf (дата звернення: 05.11.2020).

18. Шапранов Матьє-П. Розширення безпеки в реальному часі для мереж EPCglobal . 2014.
19. Перейра Енріке Г. Г., Фонг Філіп В. Л.. SEPD: Модель контролю доступу для спільного використання ресурсів в середовищі IoT. 2019. С. 195–216.
20. Сонване Абхілаш Віджай, Махадевія Джиміт Харешкумау, Малек Сарфараз Мохаммедханіф, Пандя Суміт, Шах Нішіт Шантібхай, Modhwadiya Rajesh Hardasbhai. Система та метод управління мережевою безпекою та управлінням, що базується на політиці та ідентичності. 2015. URL: https://archive.is/3R3yJ#selection-153.1-153.19 (дата звернення: 15.11.2020).
21. OrBAC: Організаційний контроль доступу - офіційний веб-сайт моделі OrBAC. 2013. URL: https://web.archive.org/web/20170610205017/http://orbac.org/ (дата звернення: 11.12.2020).
22. База автомобільних номерів України. URL: https://avto-nomer.com.ua/ (дата звернення: 30.11.2020).
23. Github Nomeroff Net. URL: https://github.com/ria-com/nomeroff-net (дата звернення: 30.11.2020).

ДОДАТОК А

ABSTRACT

The idea of the project is to create a universal budget electronic control system for access to the facility.

The main task - automation of access control to the residential complex. The system includes:

• Vehicle identification by state license plate recognition;

• Reconciliation of the identified license plate with the database of residents of the residential complex;

• Automatic barrier opening if the license plate is in the database.

Additional tasks:

• Maintaining a visitor base.

Access control, security systems (Engl. Physical Access Control System, PACS) - set of software and hardware engineering control means and control means, aimed at limiting and recording input-output objects (people, vehicles) in a given area through the "pass point ": Doors , gates , checkpoint .

The main task is to control access to a given territory (who to let in, at what time and to what territory), including also:

- restricting access to a given territory;
- identification of a person who has access to a given territory.

Additional tasks:

- accounting of working hours;
- payroll calculation (when integrated with accounting systems);
- maintaining a base of personnel / visitors;
- integration with a security system, for example:
- with a video surveillance system for combining system event archives, transmitting notifications to the video surveillance system about the

need to start recording, turn the camera to record the consequences of a recorded suspicious event;

- with a security alarm system (SOS), for example, to restrict access to armed rooms, or to automatically disarm and arm rooms.
- with a fire alarm system (SPS) for obtaining information about the state of fire detectors , automatic unblocking of evacuation exits and closing fire doors in the event of a fire alarm.

At especially critical facilities, the network of ACS devices is physically not connected to other information networks.

Barriers

Installed on the door:

- Electric strikes are the least protected from burglary, therefore they are usually installed on internal doors (intra-office, etc.) Electric strikes , like other types of locks , can be opened by voltage (that is, the door opens when the power is applied to the lock), and closed by voltage (open as soon as the supply voltage is removed from them, therefore they are recommended for use by the fire inspectorate).
- Electromagnetic locks - almost all are voltage-locked, that is, they are suitable for installation on escape routes in case of fire.
- Electromechanical locks are quite resistant to burglary (if the lock is mechanically strong), many have a mechanical reset (this means that if an opening impulse is given to the lock, it will be unlocked until the door is opened).

Installed on aisles / driveways:

- Turnstiles are used at checkpoints, socially significant objects (stadiums, train stations, metro, some government agencies) - wherever it is required to organize a controlled passage of a large number of people. There are two main types of turnstiles: waist and full-height. If

there is no quick-opening free passage near the turnstile (in case of fire), the waist turnstile must be equipped with a so-called. anti-panic bars - bars that are broken by the effort of a normal person (a requirement of the fire inspection).

- Airlock cabins - used in banks, at secure facilities (at enterprises with increased security requirements).
- Gates and barriers are mainly installed at the entrances to the territory of the enterprise, in car parks and parking lots, at the entrances to the adjacent territory, in the courtyards of residential buildings. The main requirement is resistance to climatic conditions and the possibility of automated control (using an access control system). When it comes to organizing travel access control, additional requirements are imposed on the system - increased reading range of tags, license plate recognition (in the case of integration with a video surveillance system).
- Automatic road barriers are used to guarantee the prevention of unauthorized vehicles entering the protected area. They are anti-terrorist measures, since driving through a raised barrier destroys the vehicle's suspension.

Identifier

The main types of performance are card, keychain, tag. It is a basic element of an access control system, since it stores a code that serves to determine the rights ("identification") of the owner. This can be a Touch memory , a contactless card (such as an RFID tag), or an obsolete type of magnetic stripe card. The identifier can also be codes entered on the keyboard, or individual biometric signs of a person - a fingerprint, a drawing of the retina or iris of the eye, a three-dimensional image of a face.

The security (resistance to burglary) of an access control system is largely determined by the type of identifier used: for example, the most common proximity

cards can be counterfeited in key workshops using commercially available equipment. Therefore, such identifiers are not suitable for objects requiring a higher level of protection. A fundamentally higher level of security is provided by RFID tags, in which the card code is stored in a protected area and encrypted.

In addition to direct use in access control systems, RFID tags are widely used in other areas. For example, in local settlement systems (payment for meals in the canteen and other services), loyalty systems, and so on.

Controller

An autonomous controller is the "brain" of the system: it is the controller that determines whether or not the owner of the identifier is allowed to enter the door, since it stores identifier codes with a list of access rights for each of them in its own non-volatile memory. When a person presents (brings to the reader) an identifier, the code read from it is compared with that stored in the database, on the basis of which a decision is made to open the door.

The network controller integrates into a single system with other controllers and a computer for centralized control and management. In this case, the decision to grant access can be made by both the controller and the software of the host computer. Most often, the controllers are networked using an industrial RS-485 interface or an Ethernet local network.

In cases where it is necessary to ensure the operation of the controller in case of power outages, the controller unit is provided with its own battery, or an external backup power unit. Battery life can range from several hours to several days.

Reader

This is a device that receives ("reads") the identifier code and transmits it to the controller. Reader options depend on the type of identifier: for a "tablet" - these are two electrical contacts (in the form of a "pocket"), for a proximity card, it is an

electronic board with an antenna in the housing, and for reading, for example, a pattern of the iris the reader must enter the camera. If the reader is installed on the street (gate, outer door of the building, passage to the parking lot), then it must withstand climatic loads - temperature drops, precipitation - especially when it comes to objects in areas with harsh climatic conditions. And if there is a threat of vandalism, mechanical strength is also required (steel case). Readers for distant identification can be singled out separately .objects (with identification distance up to 50 m). Such systems are convenient for motorways, parking lots, toll road entrances, etc. Identifiers (tags) for such readers are usually active (they contain a built-in battery).

Networked systems

In a networked system, all controllers are connected to a computer, which provides many advantages for large enterprises, but is not required at all for a "one-door" ACS. Networked systems are convenient for large objects (offices, manufacturing plants), since it becomes extremely difficult to manage even a dozen doors on which autonomous systems are installed. Network systems are indispensable in the following cases:

- if it is necessary to implement complex algorithms for admitting groups of employees with different privileges to different zones of the enterprise and be able to quickly change them;
- if it is necessary to selectively delete or create gaps (marks) for a large number of access points or for a large number of employees (high turnover and loss of passes);
- if you need information about previous events (event archive) or you need additional monitoring in real time. For example, in the network system, there is a photo verification function: at the checkpoint, when an incoming person brings an identifier to the reader, an employee (watchman, security guard) can see on the monitor a photo of a person

who is assigned this identifier in the database and compare it with the appearance of the person passing by, which insures against passing cards to other people;

- if it is necessary to organize the recording of working time and control of labor discipline;
- if it is necessary to ensure interaction (integration) with other security subsystems, for example, video surveillance or fire alarms).

In a networked system, from one place, you can not only monitor events throughout the protected area, but also centrally manage user rights, maintain a database. Networked systems allow organizing several workplaces by dividing management functions between different employees and enterprise services.

In networked access control systems, wireless technologies, the so-called radio channels, can be used. The use of wireless networks is often determined by specific situations: it is difficult or impossible to lay wired communications between objects, reduction of financial costs for installation of an access point, etc. There are a large number of radio channel options, but only some of them are used in ACS.

- Bluetooth . This type of wireless data transmission device is analogous to Ethernet. Its peculiarity lies in the fact that there is no need to lay parallel communications for combining components when using the RS-485 interface.
- Wi-Fi . The main advantage of this radio channel is its long communication range, capable of reaching several hundred meters. This is especially necessary for connecting objects at large distances (?). At the same time, both time and financial costs for laying street communications are reduced.
- ZigBee . Initially, the scope of this radio channel was a security and fire alarm system. Technologies do not stand still and are actively

developing, therefore ZigBee can be used in access control systems. This wireless technology operates in the unlicensed 2.45 GHz band.

- GSM . The advantage of using this wireless communication channel is almost complete coverage. The main methods of information transfer in the considered network are GPRS, SMS and voice channel.

It is not uncommon for the installation of a full-fledged security system to be unjustifiably expensive for solving the task. In such situations, the best solution would be to install an autonomous controller at each of the access points that need to be equipped with access.

Autonomous systems

Autonomous systems are cheaper, easier to operate, do not require laying hundreds of meters of cable, using computer interface devices or the computer itself. At the same time, the disadvantages of such systems include the inability to create reports, keep track of working hours, transmit and summarize information about events, and be controlled remotely. When choosing an autonomous system with high safety requirements, it is recommended to pay attention to the following:

- The reader must be separated from the controller so that the wires through which the lock can be opened are not accessible from the outside.
- The controller must have a backup power supply in case of a power outage.
- It is preferable to use the reader in a vandal-resistant housing.

As part of the autonomous access control system, electronic locks are also used that transmit information via wireless communication channels: a mechanical lock with electronic control and a built-in reader is installed in the door. The lock is connected via a radio channel to the hub, which already communicates via wires with the workstation on which the software is installed.

For an autonomous system, it is possible to use the "reverse method", when identifiers are set at checkpoints, and employees are marked by the reader-controller, subsequently the data is transmitted as soon as possible - the appearance of communication at the reader. This method is convenient to use, for example, in places where there is no communication, the possibility of laying power supply or other communications. Also, the "reverse method" can be used to control patrolling of large perimeters: after bypassing the territory or at the end of the shift, the guard submits for verification the controller, in which all passed control points are recorded, indicating the sequence of passage and the time of passage of each point.

Additional features

- GSM module that allows you to send SMS with information about the passage (used, for example, in schools).
- for network access control systems (also some autonomous systems) - the ability to remotely control over the Internet (for example, to manage the access control system from the central office, if the company has many branches).
- complex for personalization of plastic cards (printer for printing the owner's data on a plastic card, including photographs).
- “antipassback” mode - if a person has already entered the protected area, then re-presenting his identifier at the entrance will be prohibited (until the card is presented at the exit), which will exclude the possibility of two or more people passing through one card. At the same time, the network access control system allows organizing such a mode at all points of passage connected to the network, which provides full-featured protection along the entire perimeter of the controlled area.

Application of ACS

The areas of application of ACS are various:

- company offices, business centers;
- banks;
- educational institutions (schools, technical schools, universities);
- industrial enterprises;
- protected areas;
- parking lots, parking lots;
- places of passage of vehicles;
- private houses, residential complexes, cottages;
- hotels;
- public institutions (sports complexes, museums, metro, etc.)

The main types of companies in the market

- Manufacturers
- Distributors
- Designers
- Integrators
- Trading houses
- Installation organizations
- End customers
- Large end customers (have their own security service)

Development of the structural scheme

The block diagram of the electronic system consists of:

• Camera with a video recorder that has the ability to broadcast a video stream (or IP camera);

• Computer (PC, server, Raspberry PI, etc.) with Arduino connected via USB;

• 433 MHz transmitter with amplitude modulation.

If you use a raspberry pi, then you do not need an Arduino, as you can use a GPIO Raspberry PI.

The 433 MHz wireless transmitter must be amplitude modulated.

The computer acts as the main controller of the system. It is needed to receive, process and transmit information:

• Reception of a video stream of the camera;

• Crucifixion of license plates of vehicles that want to enter the territory of the residential complex;

• Reconciliation of recognized characters with the database;

• Logging the time and license plate of the vehicle entering the territory of the LCD;

• Sending a signal to the barrier controller via GPIO (Arduino) and 433 MHz transmitter.

Selection of element base

Since the idea of the project is to create a fairly universal and inexpensive system, we select available and inexpensive components.

Computer

Your computer must be running Windows or Linux (preferably a friend). CUDA (Compute Unified Device Architecture) is a software and hardware architecture for parallel computing that can significantly increase computing performance through the use of Nvidia GPUs. Having a CUDA on your computer will significantly increase the speed at which license plates are recognized in the still image from the camera.

The Raspberry Pi is a series of small single-board computers developed in the UK by the Raspberry Pi Foundation in collaboration with Broadcom. Initially, the Raspberry Pi project tended to promote the teaching of basic computer science in schools and developing countries. Later, the original model became much more popular than expected, selling outside the target market for uses such as robotics. It is now widely used in many areas, such as weather monitoring, due to its low cost, modularity and open design.

Following the release of the second type of board, the Raspberry Pi Foundation created a new organization called Raspberry Pi Trading and appointed

Eben Upton as CEO, responsible for technology development. The Foundation has been re-educated as an educational charity to promote the teaching of basic computer science in schools and developing countries.

The Raspberry Pi is one of the best-selling British computers. As of December 2019, more than thirty million boards were sold. Most dogs are made at Sony's factory in Pencoed, Wales, while others are made in China and Japan.

If you choose Raspberry PI, you will not need an Arduino, as the latter is used only to transmit a signal from a computer to a 443 MHz transmitter via GPIO outputs.

For this project, a regular personal computer running Windows was chosen, as it is the most affordable option that almost everyone has.

Arduino

Arduino is an open source hardware and software company, a community of projects and users that develops and manufactures single-board microcontrollers and sets of microcontrollers for building digital devices. Its hardware products are licensed under the CC-BY-SA license, while the software is licensed under the GNU Lesser General Public License (LGPL) or the GNU General Public License (GPL), allowing Arduino boards to be manufactured and distributed by anyone. Arduino boards can be purchased on the official website or through authorized distributors.

Any Arduino with at least one GPIO output, 5 V power supply and the ability to connect to a computer via USB is suitable for the implementation of this electronic system.

Arduino Uno Rev3 was chosen because this device meets all the requirements described above, is very popular and as a result - a large number of stores that sell this board, and has a low cost. Also, the Arduino Uno Rev3 has a margin of functionality for this project, to allow further development of the electronic system.

Video recorder

You need to choose a DVR that has the ability to stream cameras. This allows you to set up your computer remotely from the DVR. For example, if the DVR

broadcasts a stream to the Internet, the computer can be removed a long distance from registrar. The main thing is that the distance was not more than the range of the transmitter 433 MHz. If the transmitter is installed near a barrier and receives the signal also via the Internet, the computer can be removed at any distance, but in this project we consider only the direct connection of the transmitter via Arduino, which is connected to the computer via USB.

I have already installed an IP video recorder Hikvision in the residential complex, which will be used in this electronic control system for access to the object. The DVR uses the Hikvision protocol (port 8000) to stream video.

Transmitter

The transmitter must be powered by 3.3 V or 5 V. And has one input for data.

The pair "receiver - transmitter" STX882 + SRX882 was selected.

SRX887 is a superheterodyne module of the receiver, which has a powerful driving force. It has high stability, interference protection and cost-effectiveness, but also has a powerful driving force, certified ROHS, FCC, CE, the module can be connected directly to the microcontroller. So it is more convenient for users who develop wireless products. It can also be used on Arduino and Raspberry Pi.

The STX882 is an inexpensive, small, high-power, low-harmonic ASK transmitter module. It has high stability and high cost, with a power of 3.6 V to reach 50 mW, it is currently on the market under the same voltage that transmits the ASK power transmission module. The module can be connected directly to the microcontroller. So it is more convenient for users who develop wireless products

ДОДАТОК Б

Лістинг програми

```
/*
  Simple example for receiving

  https://github.com/sui77/rc-switch/
*/

#include <RCSwitch.h>

RCSwitch mySwitch = RCSwitch();

void setup() {
  Serial.begin(9600);
  mySwitch.enableReceive(0);  // Receiver on interrupt 0 => that is pin #2
}

void loop() {
  if (mySwitch.available()) {

    Serial.print("Received ");
    Serial.print( mySwitch.getReceivedValue() );
    Serial.print(" / ");
    Serial.print( mySwitch.getReceivedBitlength() );
    Serial.print("bit ");
    Serial.print("Protocol: ");
    Serial.println( mySwitch.getReceivedProtocol() );

    mySwitch.resetAvailable();
  }
}
```

ДОДАТОК В

Лістинг основного скрипту

```
from datetime import datetime
import time
import csv
import serial
import os
import glob

if not os.path.exists('cam'):
    os.makedirs('cam')
cam_host = '192.168.0.2'
cam_port = 8000
cam_user = 'admin'
cam_password = 'admin'
cam_channel = 102
csv_path = 'database.csv'
timeout = 30  # На сколько секунд засыпает скрипт после успешного
рапознавания номера который есть в базе
com_port = 'COM7'  # Последовательный порт arduino управляющий
шлагбаумом


def get_vehicle(plate_number: str):
    import requests
    from lxml import html
    brand, model, year, color = '', '', '', ''
    response = requests.get('https://avto-
nomer.com.ua/nomer/{}'.format(plate_number))
    if response.status_code == 200:
        tree = html.fromstring(response.content)
        try:
            brand = tree.xpath('//*[@id="view-mode-list"]/article[@class="car-
item"]/div[@class="car-title"]/a[1]/text()')[0]
            model = tree.xpath('//*[@id="view-mode-list"]/article[@class="car-
item"]/div[@class="car-title"]/a[2]/text()')[0]
            year = tree.xpath('//*[@id="view-mode-list"]/article[@class="car-
item"]/div[@class="car-title"]/text()')[2].replace(',', '').replace('\n', '').replace('\t',
'').replace('г.', 'р.')
            color = tree.xpath('//*[@id="view-mode-list"]/article[@class="car-
item"]/div[@class="car-info"]/div/ul/li[1]/text()')[0].strip()
        except IndexError:
            print('Номер машины {} не найден в базе
ДАИ'.format(plate_number))
    return '{} {} {}'.format(brand, model, year), color
```

```
def update_vehicle_in_database(csv_path: str):
    r = csv.reader(open(csv_path), delimiter=';', lineterminator='\n')  # Here your
csv file
    lines = list(r)
    for i, line in enumerate(lines):
        if line[2] == '':
            lines[i][2], lines[i][3] = get_vehicle(line[1])
    writer = csv.writer(open(csv_path, 'w'), delimiter=';', lineterminator='\n')
    writer.writerows(lines)


def get_plate_numbers_from_database(csv_path: str):
    plate_numbers_list = []
    with open(csv_path, newline='') as f:
        database = csv.reader(f)
        database.__next__()  # Пропускаем шапку
        for row in database:
            # print(row[0])
            if row[0].split(';')[1] != '':
                plate_numbers_list.append(row[0].split(';')[1])
    # print(plate_numbers_list)
    return plate_numbers_list


def get_cam_pic(host: str, port: int, user: str, password: str, channel: int):
    from hikvisionapi import Client
    import cv2

    cam = Client('http://{}:{}'.format(host, port), user, password)
    cam.count_events = 1  # The number of events we want to retrieve (default =
1)
    get_cam_pic_datetime = datetime.now()  # Регистрируем время забора
стопкадра с потока камеры
    response = cam.Streaming.channels[channel].picture(method='get',
type='opaque_data')
    img_path = './cam/{}.jpg'.format(get_cam_pic_datetime.strftime("%d-%m-
%Y %H-%M-%S"))
    with open(img_path, 'wb') as f:
        for chunk in response.iter_content(chunk_size=1024):
            if chunk:
                f.write(chunk)

    # time.sleep(1)
```

```
    # img = cv2.imread('screen.jpg')
    # cv2.imshow("show", img)
    # cv2.waitKey(0)
    return img_path


######################################################################
def number_plate_recognition(img_path: str):
    # Specify device
    import os

    os.environ["CUDA_VISIBLE_DEVICES"] = "0"
    os.environ["TF_FORCE_GPU_ALLOW_GROWTH"] = "true"

    # Import all necessary libraries.
    import numpy as np
    import sys
    import matplotlib.image as mpimg

    # NomeroffNet path
    NOMEROFF_NET_DIR = os.path.abspath('c:/Users/Toporivskyi/nomeroff-
net')
    sys.path.append(NOMEROFF_NET_DIR)

    # Import license plate recognition tools.
    from NomeroffNet import Detector
    from NomeroffNet import filters
    from NomeroffNet import RectDetector
    from NomeroffNet import OptionsDetector
    from NomeroffNet import TextDetector
    from NomeroffNet import textPostprocessing

    # load models
    rectDetector = RectDetector()

    optionsDetector = OptionsDetector()
    optionsDetector.load("latest")

    textDetector = TextDetector.get_static_module("eu")()
    textDetector.load("latest")

    nnet = Detector()
    nnet.loadModel(NOMEROFF_NET_DIR)
```

```
    # Detect numberplate
    # img_path = 'examples/images/example2.jpeg'
    img = mpimg.imread(img_path)

    # Generate image mask.
    cv_imgs_masks = nnet.detect_mask([img])

    for cv_img_masks in cv_imgs_masks:
        # Detect points.
        arrPoints = rectDetector.detect(cv_img_masks)

        # cut zones
        zones = rectDetector.get_cv_zonesBGR(img, arrPoints, 64, 295)

        # find standart
        regionIds, stateIds, countLines = optionsDetector.predict(zones)
        regionNames = optionsDetector.getRegionLabels(regionIds)

        # find text with postprocessing by standart
        textArr = textDetector.predict(zones)
        textArr = textPostprocessing(textArr, regionNames)
        print(textArr)
        # ['JJF509', 'RP70012']
        return textArr


if __name__ == "__main__":
    com = serial.Serial(com_port, 9600)  # Подключаемся к Arduino
    time.sleep(2)  # wait for the serial connection to initialize

    update_vehicle_in_database(csv_path)  # Добавляем в базу марку и модель машины, где не указаны
    database_plate_numbers = get_plate_numbers_from_database(csv_path)  # Извлекаем список номеров записанных в базе данных

    # plate_number_leases_cache = {}
    while True:
        cam_pics = glob.glob('./cam/*')
        for file in cam_pics:
            os.remove(file)
        try:
            cam_pic = get_cam_pic(cam_host, cam_port, cam_user, cam_password, cam_channel)  # Сохраняем стопкадр из потока камеры
```

```
            cam_plate_numbers = number_plate_recognition(cam_pic)  # Распознаём номера на стопкадре
        except:
            continue
        else:  # Если ошибок при получении стоп-кадра и распознавания номера небыло:
            if len(cam_plate_numbers) != 0:  # Если в кадре есть хотя бы один распознанный номер
                for plate_number in cam_plate_numbers:
                    with open("log.txt", "a") as log:
                        log.write("\nТЗ з номером {} розпізнаний в {}".format(plate_number, cam_pic.replace('./cam/', '').replace('.jpg', '')))
                    if plate_number in database_plate_numbers:
                        print('Найден номер который есть в базе данных')
                        com.write(b'1')  # Посылаем сигнал на ардуино для открытия шлагбаума
                        response = com.readline().decode().replace('\r', '').replace('\n', '')  # Читаем ответ ардуино
                        if response == 'Switching on/off':
                            print('Arduino отправил сигнал открытия шлагбаума')
                            with open("log.txt", "a") as log:
                                log.write("\nТЗ з номером {} заїхав на територію в {}".format(plate_number, datetime.now()))
                            time.sleep(timeout)
                            break
            if os.path.exists(cam_pic):
                os.remove(cam_pic)  # Удаляяем распознанный стопкадр
            else:
                print("The file does not exist")
```

ДОДАТОК Г

Лістинг скетча

```
#include <RCSwitch.h>

RCSwitch mySwitch = RCSwitch();
char data;

void setup() {
Serial.begin(9600);
// Transmitter is connected to Arduino Pin #10
mySwitch.enableTransmit(10);
// Optional set pulse length.
// mySwitch.setPulseLength(320);
// Optional set protocol (default is 1, will work for most outlets)
mySwitch.setProtocol(1);
// Optional set number of transmission repetitions.
mySwitch.setRepeatTransmit(5);
// mySwitch.send(9286993, 24); //код открытия шлагбаума
}

void loop() {
  // Вывод только при получении данных
  if (Serial.available() > 0)
  {
    data = Serial.read();
    // Serial.println(data);          // выводим байт в последовательный порт
    if (data == '1')
    {
      Serial.println("Switching on/off");
      /* using decimal code */
      mySwitch.send(9286993, 24); //код открытия шлагбаума
    }
  }
}
```