Министерство образования, науки и молодежной политики Нижегородской области
Государственное бюджетное профессиональное образовательное учреждение
«Арзамасский коммерческо-технический техникум»

РАБОТА

на региональный конкурс творческих работ «Наше будущее»

на тему: **Использование платформы Arduiono для разработки системы безопасности**

Номинация: «Я – программист»

Разработчики:
Буталов Д.В.,
студенты ГБПОУ АКТТ,
гр. 16-05СП,
специальность:
22.02.06 Сварочное производство

Руководители:
Саблукова Н.Г.,
зав. отделением СПО ГБПОУ АКТТ

Арзамас, 2019

Содержание

Введение

«Умный дом» - это единая система управления и контроля комфортом и безопасностью дома и его обитателей. Она контролирует не только целостность инженерных систем, но сохранит дом от визита непрошенных гостей. Одной из составляющих системы «Умный дом» является система контроля и управления доступом. Использование биометрических систем или доступ в жилье по отпечаткам пальцев формирует систему защиты помещений на совершенно новом уровне, абсолютно конфиденциально. Биометрические решения представляют собой обязательную часть всей концепции «умный дом», однако сегодня инженеры и технари не предлагают еще пакетного решения.

Эти системы на порядок выше находятся в сравнении с системами контроля доступа, основанных на использовании пластиковых карточек RFID. Подобные биометрические системы контроля доступа и охраны помещения применяются в системах видеонаблюдения или идентификации по звуку, голосу.

Рассматривая всю совокупность биометрических технологий, можно выделить две основные группы, которые обособляются в зависимости от типа параметров считывания. Одна из групп подобных устройств работает разнообразными статистическими объектами, типа, отпечатков пальцев, геометрии руки, рисунка сетчатки глаза, особенностей геометрии лица.

Другая группа устройств по биометрическому распознаванию хозяина работает с динамическими характеристиками. К такому типу следует отнести динамику подписи или идентификацию по звуку и персональным голосовым особенностям.

Следовательно, биометрические параметры ориентируются на считывание индивидуальных для каждого человека персональных характеристик. Причем самыми популярными для обработки, с целью контроля доступа в помещение,

среди подобных качественных особенностей личности являются своеобразие радужной оболочки глаз, а также отпечатки пальцев и даже результаты ДНК. Так как со временем и под действием других факторов, как настроение или стресс, такие характеристики, как почерк или голос, могут видоизменяться. Поэтому их относят к специальной группе характеристик, которые меняют свои параметры со временем.

Целью проекта является создание устройства, способного идентифицировать личность человека по отпечаткам пальцев.

Объект исследования - автоматизированные системы идентификации.

Предмет исследования – разработка системы безопасности на основе программируемого микроконтроллера Arduino.

Для достижения цели поставлены и решены следующие задачи:

- проанализировать возможности использования биометрических систем для организации системы безопасности на примере Умного дома;
- выявить функциональные требования к устройству;
- разработать модель устройства;
- обосновать выбор платформы;
- реализовать и провести тестирования программы и устройства;
- провести ряд эксплуатационных испытаний.

Arduino – популярная платформа для создания автоматики своими руками. Она подходит для изготовления автоматики в сельском хозяйстве, в рекламной деятельности, в сфере игровых развлечений и других видах деятельности.

Подобное устройство имеет небольшую стоимость (около 2000 рублей) и вес, выполняя функции заводских устройств.

Новизна данной работы состоит в возможности использования Arduino при проектировании систем безопасности.

1 Теоретическая часть

1.1 Системы безопасности в Умном доме

Системы безопасности в Умном Доме — гарантия защиты от непрошеных гостей. Она состоит из следующих компонентов.

1) Пожарная сигнализация и система предотвращения аварий, связанных с поломкой техники, повреждением водопровода, утечкой газа или возникновением открытого огня, защитит ваш дом от несчастных случаев. Система резервного электропитания обезопасит дом от последствий аварийного отключения электропитания, сделав такое отключение незаметным для находящихся в доме.

2) Видеонаблюдение состоит из видеокамер, которые могут быть расположены как вокруг дома так и внутри него, и записывающего устройства (видеорегистратора), подключенного к монитору или всей телевизионной сети дома. Также возможно осуществлять видеонаблюдение через интернет.

3) Система резервного питания защитит дом от проблем, связанных с отключением электроэнергии, таким образом, что находящиеся в доме даже не заметят отключения. Она обеспечит бесперебойное питание дома независимо от внешних источников. Еще об источниках резервного электроснабжения.

4) Система предупреждения аварий защитит от любых проблем, связанных с перебоями в сети электропитания, утечки воды или газа, оставленным включенным электроприбором. Она автоматически предотвратит все возможные негативные последствия аварий и предупредит хозяев дома или обслуживающую организацию.

5) В систему контроля и управления доступом входят электромагнитные замки на двери или калитку (с доступом по ключам-«таблеткам» или электронным картам), домофония (возможность видеть звонящего человека, разговаривать с ним, удаленно открывать дверь), автоматика шлагбаумов, откатных или распашных ворот (открытие с помощью радиоканального брелка).

6) Охранная сигнализация предотвратит проникновение в дом или на территорию вокруг дома. GSM сигнализация известит хозяина дома через телефонных звонок или СМС. Возможна постановка на учет в охранную фирму.

1.2 Использование биометрических систем для Умного дома

Революционным решением в области развития технологий умных домов становится применение биометрических систем контроля. Такой подход позволяет повысить безопасность жильцов умного дома во много раз и вместе с тем увеличить степень конфиденциальности имеющихся сведений.

Возможности биометрических систем

Новые биометрические системы аутентификации в умном доме в технологическом плане на порядок выше распространенных пластиковых карточек. Например, биометрическая технология обнаружения позволяет идентифицировать человека по таким параметрам как:

- отпечатки пальцев
- геометрия руки
- рисунок сетчатки глаза
- особенности геометрии лица

Не менее оригинальным решением идентификации жильцов умного дома становится их распознавание, основанное на динамике подписи и их голосовых особенностях. Подделать голос, в принципе, при соответствующем умении возможно, также как попытка подделки подписи, но здесь стоит отметить, что преступник при всем желании не сумеет полностью отобразить динамические особенности оригинальной подписи, что делает незаконное проникновение в умный дом невозможным. Главное здесь, время от времени обновлять идентификационный стандарт подписи, поскольку со временем почерк человека может меняться.

Приоритетные направления биометрических систем

Главной функцией работы биометрических систем является формирование в своей информационной базе персональных характеристик каждого из жильцов умного дома. Здесь важно подчеркнуть, что наиболее устойчивыми показателями, на основании которых дом сможет произвести объективную идентификацию человека, становятся отпечатки пальцев, уникальность структуры ДНК и своеобразие глазной оболочки

2 Требования к разработке

2.1 Общие сведения о разработке

- Устройство будет идентифицировать личность человека по отпечатку пальцев.
- Контроллер системы безопасности может использоваться как система управления контролем доступа в домашних условиях и на предприятиях.
- Контролер системы безопасности имеет большое применение в разных областях, это могут быть квартиры, частные дома, банки, предприятия, а также компьютерной и другое оборудование

2.2. Технические требования

- Масса устройства должна быть не более 0,5 кг.
- Габариты должны быть не более 150x200x100mm
- Конструкция устройства должна обеспечивать допуск для быстрой и удобной сборки и разработки, для проведения ремонта и профилактических работ.
- Устройство будет регистрировать отпечаток пальца человека.
- Устройство должно обеспечивать непрерывный режим работы с учетом требований.
- Напряжение питания 5 Вольт.

2.3. Требования к надежности

Срок службы устройства не менее 5 лет. Конструкция должна обеспечивать возможность ремонта и модернизации в течение срока службы. Срок сохранности до ввода его в эксплуатацию не менее 12 месяцев с момента выпуска. Среднее время наработки на отказ не менее 50000 часов. Среднее время восстановления работоспособности при аппаратных повреждениях около 1 часа.

3 Разработка устройства

3.1. Принципиальная схемы технического устройства

Принципиальная схема разработанной системы безопасности представлена на рис. 1.

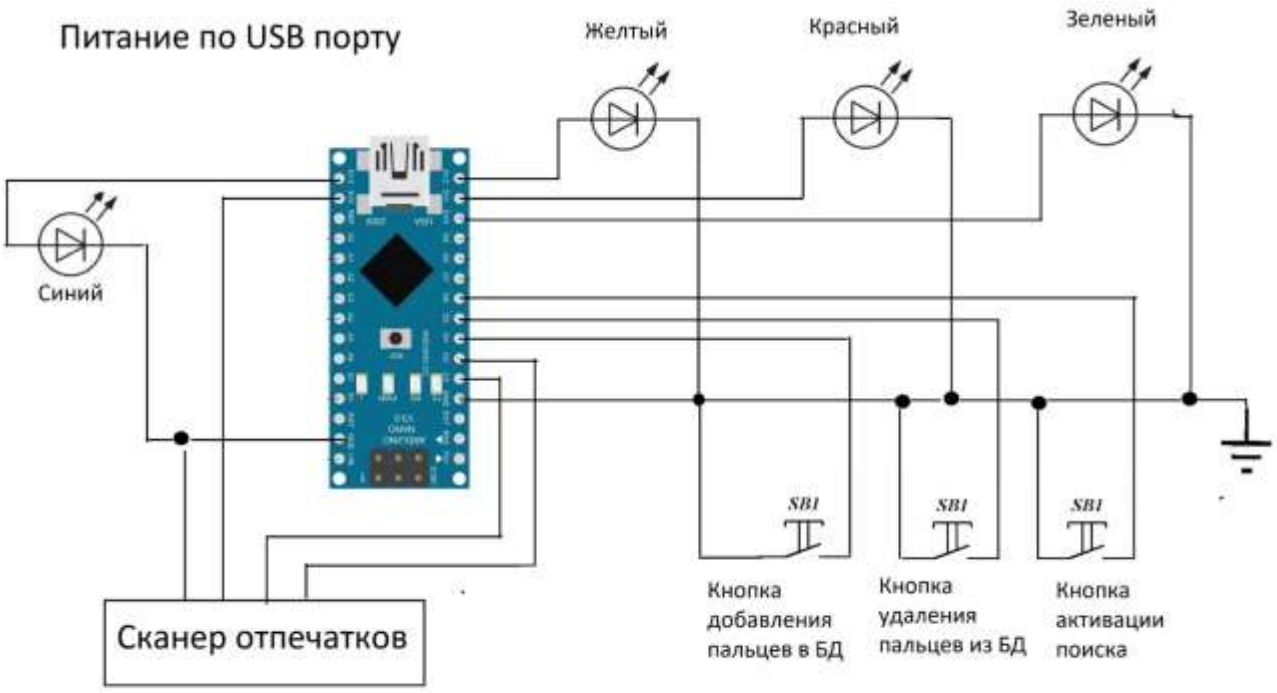

Рис. 1 Принципиальная схема

3.2 Блок-схема программы

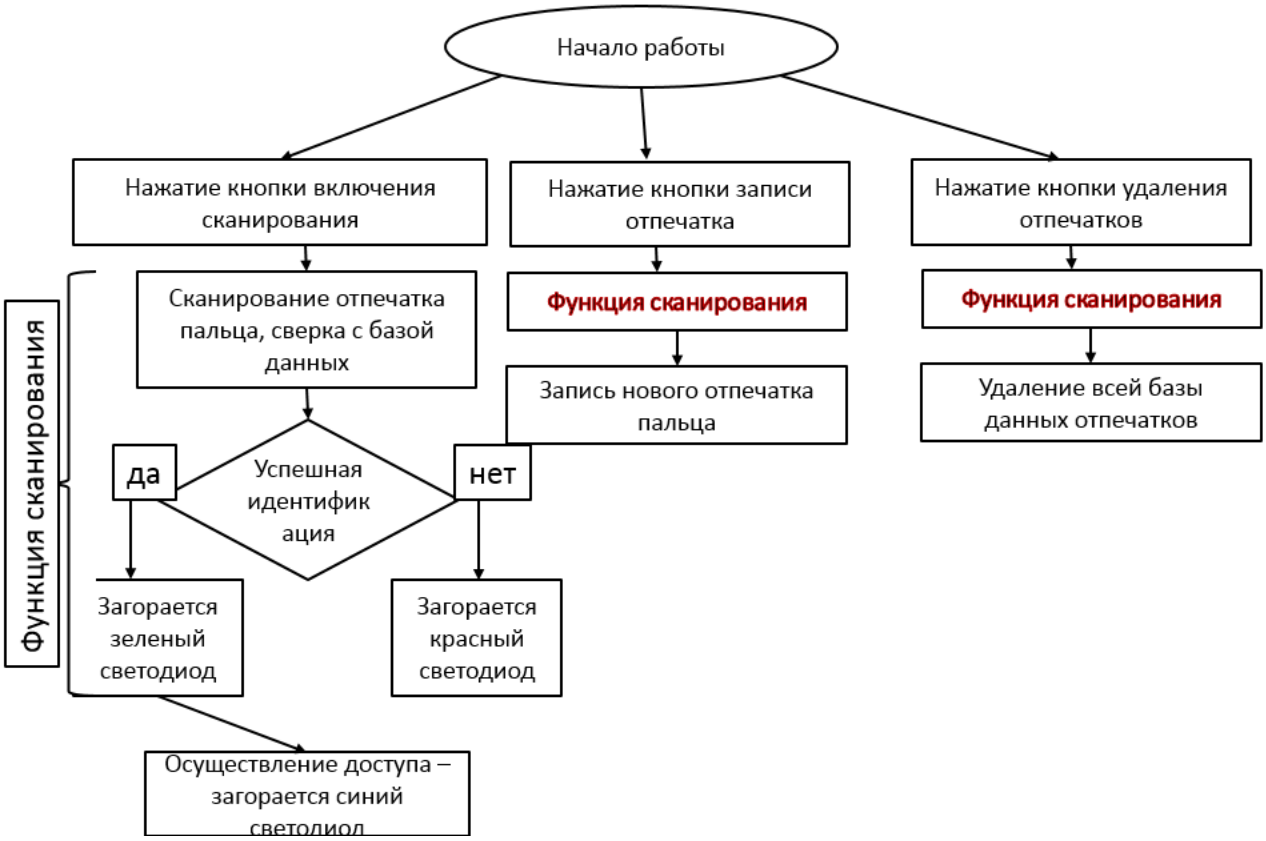

Рис 2. Блок схема работы программы

3.3. Описание элементной базы

Состав элементов для макета на Arduino

1) Arduino NANO

Рис. 3

Arduino — это открытая платформа, которая позволяет собирать всевозможные электронные устройства. Arduino будет интересен креативщикам, дизайнерам, программистам и всем пытливым умам, желающим собрать собственный гэджет. Устройства могут работать как автономно, так и в связке с компьютером. Всё зависит от идеи.

Платформа состоит из аппаратной и программной частей; обе чрезвычайно гибки и просты в использовании. Для программирования используется упрощённая версия C++, известная так же как Wiring. Разработку можно вести как с использованием бесплатной среды Arduino IDE, так и с помощью произвольного C/C++ инструментария. Поддерживаются операционные системы Windows, MacOS X и Linux.

Монтаж схемы не требует пайки и выполняется на беспаечных макетных платах. Конструирование ещё не было таким быстрым и простым.

Таблица 1. Основные характеристики Arduino Nano

Микроконтроллер	ATmega328p
Рабочее напряжение	5В
Входное напряжение (рекомендуемое)	7-12В
Входное напряжение (предельное)	6-20В
Цифровые Входы/Выходы	14 (3 из которых могут работает также как выходы ШИМ)
Аналоговые входы	7
Постоянный ток через вход/выход	40 mA
Постоянный ток для вывода 3.3 В	50 mA
Флеш-память	32 KB (из которых 2 KB используются для загрузчика)
ОЗУ	2 KB
Энергонезависимая память	1 KB
Тактовая частота	16 MHz
Рабочая температура	-40 – 125 C°

2) Оптический сканер отпечатков пальцев

Рис. 4

- Светодиоды в качестве индикаторов (Рис. 3)

Рис. 5

- Тактовые кнопки.

3.4 Программный код устройства

```
#include <Adafruit_Fingerprint.h>                    // подключаем библиотеку для работы с модулем отпечатков пальцев

#include <SoftwareSerial.h>                          // подключаем библиотеку для работы с программным UART

uint8_t id;                                          // идентификационный номер, под которым будет сохранён шаблон отпечатка пальца

SoftwareSerial mySerial(2, 3);                       // объявляем объект mySerial для работы с библиотекой SoftwareSerial
```

```
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);  // объявляем объект finger   для работы с библиотекой Adafruit_Fingerprint

int led_green = 10;

int led_red = 11;

int led_yellow = 12;

int lock = 13;

boolean result = false;

void setup(){

pinMode(4, INPUT_PULLUP); //кнопка записи отпечатков

pinMode(5, INPUT_PULLUP); //кнопка удаления отпечатков

pinMode(6, INPUT_PULLUP); //кнопка распознавания отпечатков

pinMode(10, OUTPUT); //светодиод подтверждения

pinMode(11, OUTPUT); //светодиод отклонения

pinMode(12, OUTPUT); //светодиод ошибки

pinMode(13, OUTPUT); //светодиод вместо эл. замка



finger.begin(57600);   // Инициализация программного UART на скорости 57600 (скорость модуля по умолчанию)

  if(finger.verifyPassword()){digitalWrite(10, HIGH);}

  else{digitalWrite(12, HIGH);    }

  delay(500);
```

```
  digitalWrite(10, LOW);
}
byte skan(){  //функция сканирования отпечатка пальца
  int n = 0;
  while(n == 0){

   if(finger.getImage()        == FINGERPRINT_OK){             // Захватываем
```
изображение, если результат выполнения равен константе FINGERPRINT_OK (корректная загрузка изображения), то проходим дальше
```
  if(finger.image2Tz()        == FINGERPRINT_OK){             // Конвертируем
```
полученное изображение, если результат выполнения равен константе FINGERPRINT_OK (изображение сконвертировано), то проходим дальше
```
  if(finger.fingerFastSearch() == FINGERPRINT_OK){             // Находим
```
соответствие в базе данных отпечатков пальцев, если результат выполнения равен константе FINGERPRINT_OK (найдено соответствие), то проходим дальше
```
    return true;
  }
  else{
    return false;
  }
  }}
  delay(100);                                    // Задержка перед следующим
```
сканированием 0,5 сек

```
  }
}
byte check(){  //функция проверки наличия отпечатков
  for(uint8_t id = 0; id<162; id++){
  if(finger.loadModel(id) != FINGERPRINT_OK){   //Если id пуст, возвращаем его номер
    return id;
  }}
}
void record(byte id){   //функция записи нового пальца
  digitalWrite(12, HIGH);   // режим записи

  int p = -1;
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();        //получение первого снимка
    switch (p) {
    case FINGERPRINT_OK:
      break;
    default:
      break;
    }
```

```
}
p = finger.image2Tz(1);   //конвертирование первого снимка
switch (p) {
  case FINGERPRINT_OK:
    digitalWrite(10, HIGH);
    delay(1000);
    digitalWrite(10, LOW);
    break;
  default:  //ошибка
    return p;
}
delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
  p = finger.getImage();
}
p = -1;
while (p != FINGERPRINT_OK) {   //повторное считывание пальца
  p = finger.getImage();
  switch (p) {
  case FINGERPRINT_OK:
```

```
    break;
  default:
    break;
  } }
p = finger.image2Tz(2);    //конвертирование второго снимка
switch (p) {
  case FINGERPRINT_OK:
       break;
  default:
    return p;
}
p = finger.createModel();        //сохранение отпечатка
if (p == FINGERPRINT_OK) {


}  else {  //ошибка
  return p;
}
p = finger.storeModel(id);
if (p == FINGERPRINT_OK) {
  digitalWrite(10, HIGH);
  digitalWrite(12, HIGH);
```

```
    delay(1000);
    digitalWrite(12, LOW);
    delay(1000);
    digitalWrite(10, LOW);
  } else {    //ошибка
    return p;
  }
}
void loop(){
  //Поиск отпечатков если не активны кнопки
  if(digitalRead(6) == LOW) {    //если нажата кнопка считывания
 boolean result = skan();
 if(result == true){
  digitalWrite(lock, HIGH);
  digitalWrite(led_green, HIGH);
    delay(1000);
    digitalWrite(lock, LOW);
    digitalWrite(led_green, LOW);
 }
 else{
  digitalWrite(led_red, HIGH);
```

```
  delay(1000);
  digitalWrite(led_red, LOW);
}
 }
 //добавление отпечатка при кнопке 4
 if(digitalRead(4) == LOW){

  int id = check();  //получаем номер пустого сектора
  if (id != 0){  //если в базе есть отпечаток то проверяем зарегистрированный палец

  result = skan();
   }
   else{    //если в базе нет отпечатков
    result = true;  //проходим дальше
   }
  if(result == true){    //если палец распознан или сохраненных отпечатков нет

  digitalWrite(led_yellow, HIGH);   // режим отладки
   record(id);   //запись отпечатка в пустой сектор
delay(100);
 }  }
```

```
//Удаление отпечатков при нажатии кнопки 5
if(digitalRead(5) == LOW){
digitalWrite(led_yellow, HIGH);   // режим отладки
 //проверяем зарегистрированный палец
  boolean result = skan();
  if(result == true){    //если палец распознан
    digitalWrite(led_green, HIGH);  //зажигаем зеленый светодиод
    int id = check();  //получаем номер пустого сектора
    delay(1000);
finger.emptyDatabase();   //удаление всех отпечатков
digitalWrite(led_red, HIGH);
delay(1000);
 digitalWrite(led_red, LOW);
  digitalWrite(led_green, LOW);
   digitalWrite(led_yellow, LOW);
}}  }
```

Заключение

Разработанную систему можно использовать для обеспечения контроля доступа в помещение, если подключить электрический замок через реле.

Также можно на основе данной системы осуществить систему авторизации пользователя на компьютере или другом оборудовании.

В процессе выполнения работы путем решения поставленных задач была достигнута цель: разработано устройство, способное идентифицировать личность человека по отпечаткам пальцев.

Система безопасности отвечает всем необходимым условиям, позволяет надежно обеспечить контроль доступа в помещении.

Данная система является макетной моделью и может быть усовершенствована.

Список литературы и Интернет ресурсов

Книжные издания:

1. Бобровников Л.З. Радиотехника и электротехника
2. Потопов Ю. В. Российский рынок САПР печатных плат // Электронные компоненты. 2001. № 5. С. 58—60.
3. Пирогова Е.В. Проектирование и технология печатных плат
4. Угрюмов Е.П. Цифровая схемотехника.-СПб.:БХВ-Санкт-Петербург,2000.-528 с.: ил.

Интернет ресурсы:

5. [Электронный ресурс] Википедия. Форма доступа: https://ru.wikipedia.org/wiki
6. [Электронный ресурс] Амперка. Форма доступа: http://amperka.ru
7. [Электронный ресурс]dvrobot.ru. Форма доступа: http://dvrobot.ru
8. [Электронный ресурс]Arduino.ru. Форма доступа: http://arduino.ru/
9. [Электронный ресурс] Амперка. Форма доступа: http://amperka.ru/product/arduino-uno
10. [Электронный ресурс]dvrobot.ru. Форма доступа: http://dvrobot.ru/238/374.html
11. [Электронный ресурс] Амперка. Форма доступа: http://amperka.ru/product/flame-sensor
12. [Электронный ресурс]dvrobot.ru. Форма доступа: http://dvrobot.ru/238/437.html
13. [Электронный ресурс]dvrobot.ru. Форма доступа: http://dvrobot.ru/238/394.html
14. [Электронный ресурс]dvrobot.ru. Форма доступа: http://dvrobot.ru/240/122.html
15. [Электронный ресурс] Амперка. Форма доступа: http://amperka.ru/product/piezo-buzzer
16. [Электронный ресурс] Амперка. Форма доступа: http://amperka.ru/product/led-5mm