

Федеральное государственное бюджетное образовательное учреждение высшего образования  
«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»  
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)

ДОПУСКАЕТСЯ К ЗАЩИТЕ:

Факультет И  
индекс факультета  
Выпускающая кафедра И4  
индекс кафедры  
Группа И4М31  
индекс группы

Заведующий кафедрой И4  
индекс кафедры  
Страхов С. Ю.  
Фамилия ИО  
«    »      2018 г.  
подпись

## ОТЧЕТ

о прохождении производственной практики  
наименование практики

Густова Владимира Владимировича

Фамилия, имя, отчество обучающегося

Обучающегося по  
направлению/специальности 11.04.01  
нужное подчеркнуть код полное наименование направления/специальности  
Радиотехника

Руководитель практики от  
профильной организации: Гордиенко А. Н.,  
Фамилия ИО, ученая степень, ученое звание, должность  
Руководитель направления IT-технологий и развития

Срок прохождения практики: с 02.07.2018 г. по 22.07.2018 г.

Должность обучающегося на практике: инженер

Руководитель практики  
от профильной  
организации:

Гор Гордиенко А. Н.  
Подпись Фамилия ИО  
«20» 07 2018 г.

САНКТ-ПЕТЕРБУРГ  
2018 г.

## Содержание

Введение.....	3
1. Сведения о компании.....	4
2. Выбор элементной базы.....	5
3. Реализация системы.....	9
Заключение.....	11
Список использованных источников.....	12

## **Введение**

**Цель работы:** разработать систему экстренного уничтожения информации на съемных накопителях.

**Задача работы:** реализовать систему экстренного уничтожения информации для пользователя, имеющую наиболее удобные способы активации.

### **Характеристика актуальности темы:**

Уничтожение важных данных на съемных накопителях, представляющих особую важность, актуально во время пика развития информационных технологий, чтобы вся конфиденциальная информация, документация и данные любого типа, были надежно защищены от несанкционированного доступа.

Необходимо заранее обезопасить себя, чтобы в случае экстренных обстоятельств не произошло утечки информации.

### **Обоснование цели и задач работы:**

При коммерческом шпионаже хищение данных может оказывать высокое влияние на дальнейшую судьбу компании на том или ином рынке. Вследствие чего, необходимо иметь способ предотвращения утери информации. Соответственно задачей будущей системы является получение максимальной защищенности от злоумышленников. Для этого в дальнейшем будут рассмотрены три способа активации системы, чтобы выявить все достоинства и недостатки уничтожения данных каждым из рассмотренных методов.

### **Определения объекта и предмета исследования:**

Первостепенной задачей является определение необходимых факторов для гарантированного выведения из строя накопителей. В дальнейшем будем исследовать предельно допустимое значение напряжения на примере USB Flash – памяти.



## 1 Сведения о компании

В качестве места прохождения практики была выбрана компания ООО «БЭТМЭН» (Общество с ограниченной ответственностью «БЭТМЭН»).

Компания была основана в 1994 году. С этого же года «БЭТМЭН» осуществляет свою деятельность в сфере безопасности.

Время, политические перемены и экономические реформы в государстве сказались на направлениях деятельности компании. Сначала главным направлением деятельности организации была выбрана сфера информационной и физической безопасности. Компания принимала участие в нескольких международных выставках, позиционируясь, как поставщик технических средств съема и защиты информации для правоохранительных органов, охранных предприятий, детективных агентств и служб безопасности различных организаций. Однако, в 1996 году было принято постановление правительства РФ от 1 июля 1996 г. N 770 "Об утверждении положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в российскую федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности". В связи со вступлением в законную силу данного Постановления Правительства РФ, организация сначала приостановила работу в данном направлении, а в дальнейшем и полностью отказалась от работы со специальными техническими средствами, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации.

С 2000 года организация специализируется на следующих направлениях деятельности: Комплексные системы безопасности, антитеррористическое и досмотровое оборудование, аудио- и видеозапись. IP-видеонаблюдение. Деятельность по технической защите конфиденциальной информации (являемся лицензиатами Гостехкомиссии при Президенте РФ с 2000 года, лицензиатами ФСТЭК России с 2005 года).

С 2002 года по 2008 год организация являлась постоянным участником международных выставок: «Охрана и Безопасность» (Sfitex), «MILIPOL PARIS».

С 2011 года компания стала постоянным участником госзаказов на основе электронных аукционов (<http://zakupki.gov.ru>).



## 2 Выбор элементной базы

### Платформа Arduino

Первоначальной задачей являлся выбор платформы для разработки и прототипирования. Проанализировав рынок программных и аппаратных средств, для создания подобного рода проектов было принято решение работать с платформой Arduino, т. к. она соответствовала следующим критериям:

- удобный язык программирования, схожий с языком «Си»;
- кроссплатформенность;
- возможность визуального программирования;
- большой ассортимент дополнительных периферийных устройств;
- отладочная плата не требует программатора и подсоединяется напрямую к компьютеру;
- наличие широкой технической документации, как с описанием примеров кода, так и с аппаратной частью.

Далее была выбрана модель отладочной платы - Arduino MEGA 2560 (рисунок 1), поскольку ранее был некоторый опыт работы с данным микроконтроллером.

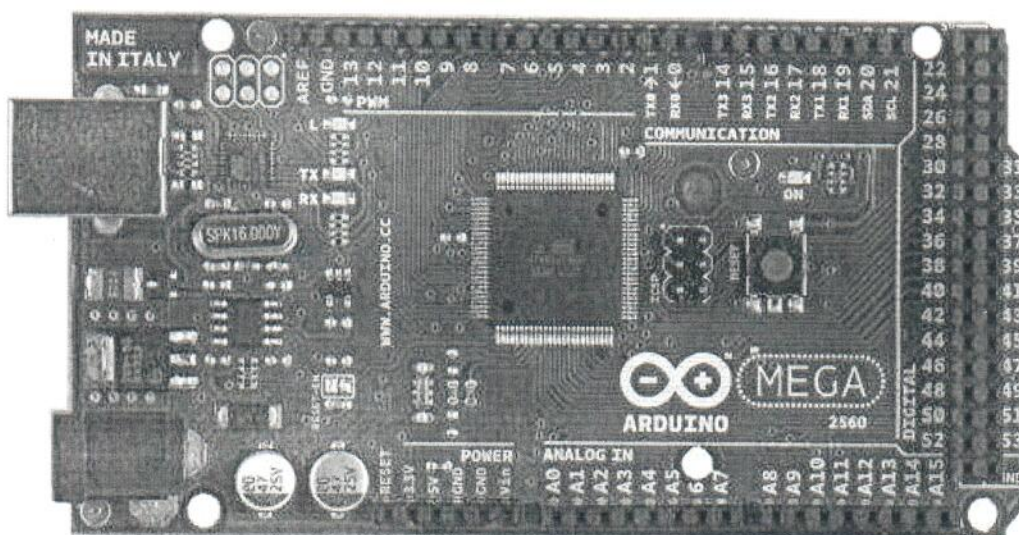


Рисунок 1 – Микроконтроллер Arduino MEGA 2560.

### Ethernet модуль

Основным каналом для экстренного уничтожения информации выступает Ethernet модуль. Он позволяет подключаться, как и к локальной сети, так и к всемирной паутине. Помогает наладить обмен данными в локальных сетях автоматике без применения ПК. В нашем случае была использована модель

ENC28J60 (рисунок 2, 3). Ethernet модуль ENC28J60 преобразует данные Ethernet в протокол SPI.

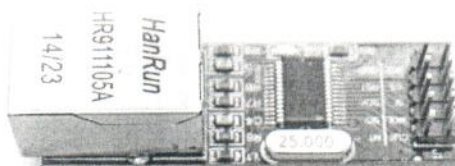


Рисунок 2 – Ethernet модуль.

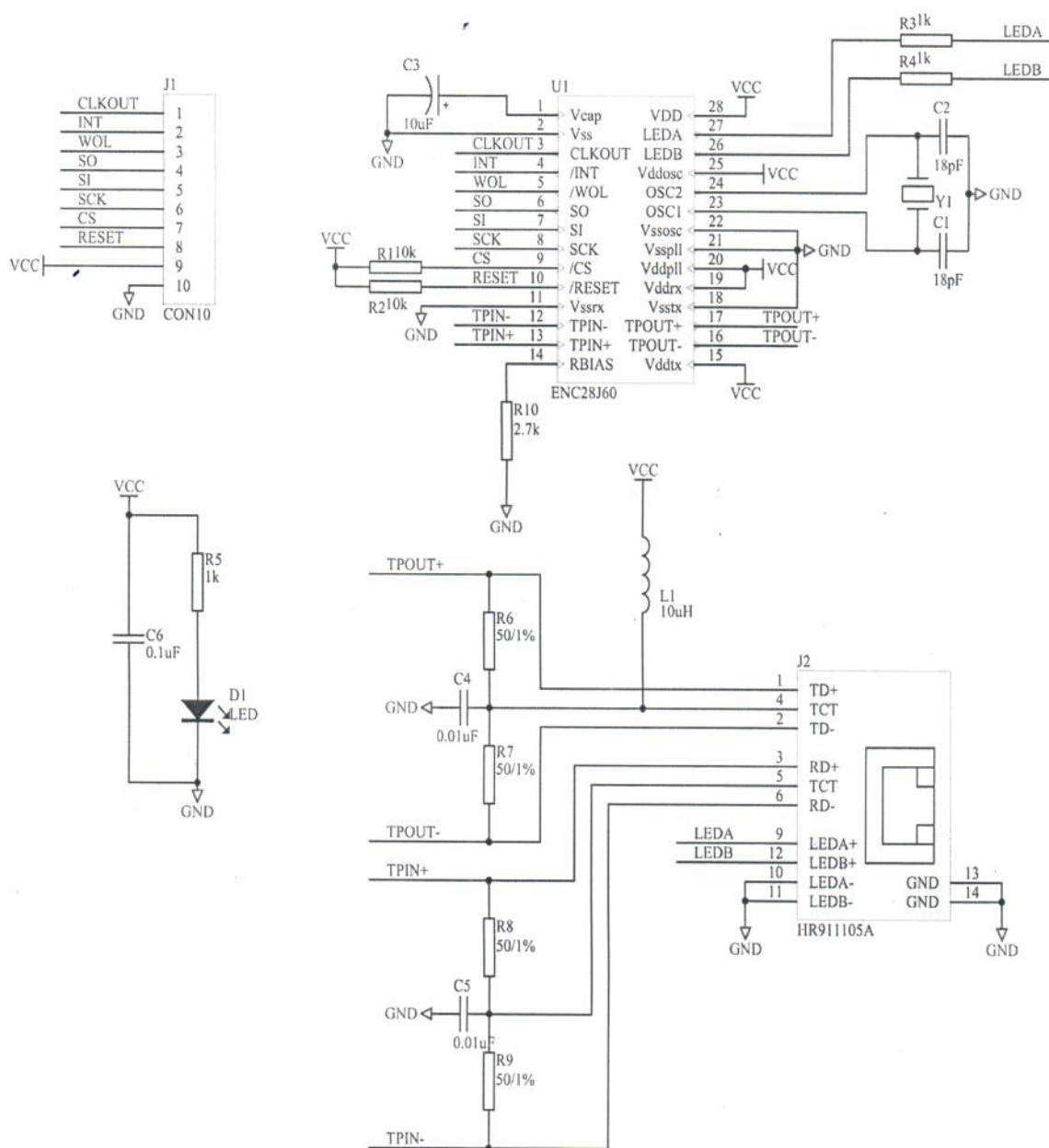


Рисунок 3 – Принципиальная схема Ethernet.

## Модуль беспроводного управления с пультом на 4 канала

Выступает в качестве второстепенного канала экстренного уничтожения информации.

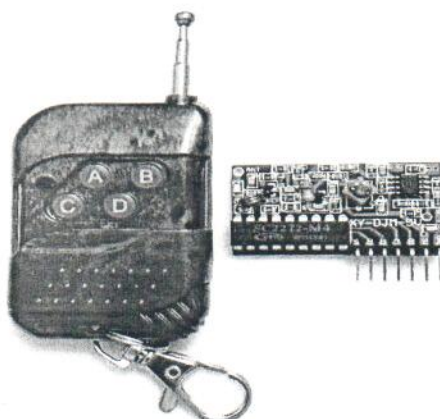


Рисунок 4 – Модуль беспроводного управления с пультом на четыре канала.

## Модуль реле

Модуль позволит создать сопряжение электронного устройства с силовой электроникой. Он необходим для того, чтобы обезопасить наше устройство от высокого напряжения.



Рисунок 5 – Модуль реле.

## Вторичные комплектующие

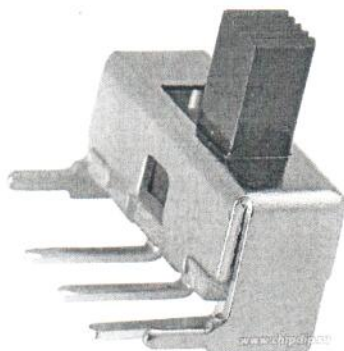


Рисунок 6 – Переключатель движковый.

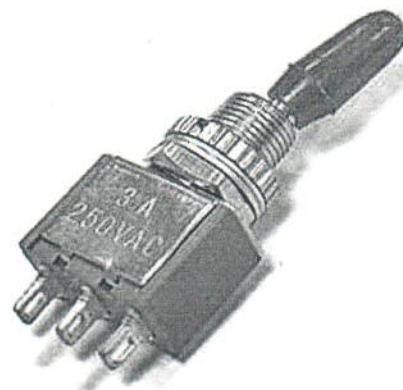


Рисунок 7 – Кнопка вкл./выкл.



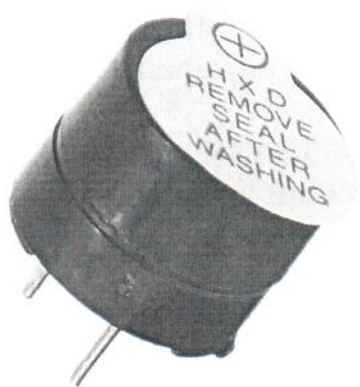


Рисунок 8 – Зуммер.

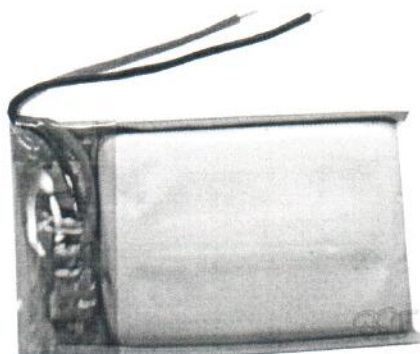


Рисунок 9 – Аккумулятор.



### 3 Реализация системы

При разработке данной системы необходимо было реализовать работу следующих элементов:

- 1) Звуковая индикация.
- 2) Световая индикация.
- 3) Подключить высоковольтный модуль к цепи с низким напряжением.
- 4) Реализовать включение высоковольтного модуля с помощью реле.
- 5) Осуществить возможность управления устройством с помощью интерфейса Ethernet.
- 6) Добавить возможность активации по радиоканалу.
- 7) Физическая активация.
- 8) Подобрать источники питания всех узлов проекта.
- 9) Разработать WEB – интерфейс.
- 10) Присвоить MAC – адрес и статический IP – адрес.
- 11) Произвести коммутацию всех узлов, а так же пуско - отладочные работы.

Для срабатывания зуммера, в необходимое для нас время, с определенной продолжительностью и тональностью, было выполнено следующие: плюсовой контакт зуммера подключили к одному из входов микроконтроллера, а минусовой к разъему GND.

Световая индикация необходима для отслеживания стабильности работы микроконтроллера. Она присутствует практически на всех элементах устройства экстренного уничтожения информации, что позволяет отследить работоспособность каждого элемента по отдельности для возможности вычисления ошибки. Поскольку разработанное устройство может позиционироваться скрытно, наличие звуковой индикации становится значительным демаскирующим признаком в отличие от световой.

Было необходимо обеспечить питание 3,7 В для модуля повышения напряжения, а так же проработать схему коммутации для включения и отключения, в определенный момент времени, для предотвращения случайной потери информации (рисунок 10). На выходе модуля повышения напряжения с  $U=7000$  В предполагается набор разъемов для подключения цифровых накопителей. Для уничтожения информации на съемном USB – накопителе достаточно 9 В, поданных на контакты Rx и Tx, но поскольку подразумевается подключать наиболее большое количество накопителей разных типов необходимо было сделать «запас» напряжения.

Основным элементом устройства экстренного уничтожения информации является высоковольтный модуль. Его первостепенная задача заключается в уничтожении элементов накопления данных, что должно происходить

своевременно и без ложных срабатываний. Поскольку сам модуль реле управляется с помощью 5 В, его нужно подключить к микроконтроллеру. Для начала обеспечим питание модуля реле, подавая питание 5 В, а ввод для управления замыкания реле подключим восьмой pin микроконтроллера. Состояние работы реле будем отслеживать по двум светодиодам, встроенным в данный модуль.

WEB – интерфейс необходим для систематизации и автоматизации работы через сетевые интерфейсы. Он позволяет заложить визуальную, текстовую информацию, которая будет отвечать за ряд запрограммированных функций. Так, например, отправка команды на микроконтроллер, подразумевающая под собой включение реле в положение активации модуля повышения напряжения, включения зуммера (звуковой индикации) с определенной задержкой и тональностью, включения световой индикации, а так же отключение всех этих элементов в обратном порядке, будет выглядеть в виде короткой гиперссылки.

**MAC-адрес** (от англ. Media Access Control — управление доступом к среде, также **Hardware Address**) — уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.

**IP-адрес** (сокращения от англ. Internet Protocol Address, где буквосочетание IP (произн. [ай-пи]) является буквенной аббревиатурой слов Internet Protocol «интернет-протокол») — уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. В сети интернет требуется глобальная уникальность адреса; в случае работы в локальной сети требуется уникальность адреса в пределах сети. В версии протокола IPv4 IP-адрес имеет длину 4 байта, а в версии протокола IPv6 IP-адрес имеет длину 16 байт.

Устройству необходимо получить идентификационные данные для авторизации в локальной сети. Так же MAC, IP – адреса необходимы для подключения сетей интернет. Несмотря на это, чтобы подключение осуществилось, основной шлюз должен иметь внешний статический IP – адрес, а так же в маршрутизаторе должно быть создано правило с указанием порта на наше устройство с переадресацией IP – адресов.



## **Заключение**

В ходе прохождения производственной практики была разработана система экстренного уничтожения информации на съемных накопителях. Ее особенностью стало наличие трех каналов активации и возможность подключения большого количества устройств накопления данных, тем самым, позволив системе претендовать на определенную нишу в сфере защиты информации.

Если говорить об актуальности темы, то следует отметить, что уничтожение важных данных на съемных накопителях, представляющих особую важность, актуально во время пика развития информационных технологий, чтобы вся конфиденциальная информация, документация и данные любого типа, были надежно защищены от несанкционированного доступа.

Следует отметить, что были выполнены все поставленные цели, условия и задачи, а так же была выполнена проверка работоспособности устройства экстренного уничтожения информации, в ходе которой были протестированы все каналы активации.



### **Список использованных источников**

1. Правила оформления конструкторской документации при проектировании радиоэлектронных систем: справ. Пос. / В.В Смирнов [и др.]; Под ред. В.В Смирнова; Балт. Гос. Техн. Ун-т. – СПб., 2008. - 70 с.
2. Сапаров В. Е., Максимов Н. А. С19 Системы стандартов в электросвязи и радиоэлектронике: Учеб. Пособие для вузов. – М.: Радио и связь, 1985. - 248 с., ил.
3. Информационно – измерительная техника и электроника: И74 учебник для студ. Высш. Учеб. Заведений/ [Г. Г. Раннев, В. А. Сурогина, В.И. Калашников и др. ]; под ред. Г. Г. Раннева. – М. : Издательский центр «Академия», 2006 – 512 с.
4. Измерительные информационные системы: учебник для студ. высш. Учеб. заведений/ Г. Г. Раннев. – М. : Издательский центр «Академия», 2010. – 336 с.
5. М54 Метрология, стандартизация, сертификация и электроизмерительная техника: Учебное пособие/ К.К. Ким, Г. Н. Анисимов, В. Ю. Барбарович, Б. Я. Литвинов. – СПб.: Питер, 2008. – 368 с.: ил.
6. Раннев Г. Г. Измерительные информационные системы: База необходимых знаний для бакалавров, дипломированных специалистов: учеб. пособие для вузов / Г. Г. Раннев. – М. : Изд-во МГОУ, 2003.
7. Гаскаров Д. В. Интеллектуальные информационные системы: учебник/ Д. В. Гаскаров. – М. : Высш. шк., 2003.
8. Раннев Г. Г. Измерительные информационные системы: Лекции/ Г. Г. Раннев. – М. : Изд-во МГОУ, 1993.
9. Ильин В. А. Информационно – измерительные системы: учеб. пособие / В. А. Ильин. – М. : Изд-во ВЗПИ, 1981.