УДК 004.056.53

А.Н. Патрин[1], А.И. Петров[1], Д.Н. Титов[1]*

Разработка интеллектуальной системы оповещения несанкционированного доступа

[1]Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
*e-mail: ya@apatrin.ru

Аннотация. В современном информационном обществе обеспечение безопасности данных – задача первостепенной важности. Телекоммуникационная инфраструктура, хранящая и передающая огромные массивы данных, становится привлекательной мишенью для злоумышленников. Важно понимать, что угрозы могут быть не только виртуальными, но и вполне реальными, физическими. Доступ к ценной информации можно получить, проникнув в телекоммуникационный шкаф, где находятся серверы и сетевое оборудование. Для защиты от подобных угроз необходимо создать надежную систему безопасности. Одним из ключевых элементов такой системы станет средство сигнализации, способное моментально реагировать на попытки несанкционированного доступа к телекоммуникационному шкафу и оповещать ответственных лиц о потенциальной угрозе.

Ключевые слова. Arduino, геркон, телекоммуникационный шкаф, сигнализация

A.N. Patrin[1], A.I. Petrov[1], D.N. Titov[1]*

Development of an intelligent unauthorized access notification system

[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: ya@apatrin.ru

Annotation. In the modern information society, ensuring data security is of paramount importance. Telecommunications infrastructure, which stores and transmits huge amounts of data, is becoming an attractive target for intruders. It is important to understand that threats can be not only virtual, but also quite real, physical. Access to valuable information can be obtained by entering the telecommunications cabinet, where servers and network equipment are located. To protect against such threats, it is necessary to create a reliable security system. One of the key elements of such a system will be an alarm system capable of instantly responding to attempts of unauthorized access to a telecommunications cabinet and notifying responsible persons of a potential threat.

Keywords. Arduino, reed switch, telecommunication cabinet, alarm system

Введение

Целью проекта по разработке интеллектуальной системы предупреждения о несанкционированном доступе является повышение уровня безопасности и надежности функционирования телекоммуникационных сетей путем создания системы, способной обнаруживать и оповещать о попытках несанкционированного доступа к телекоммуникационному шкафу.

Проект по разработке интеллектуальной системы предупреждения о несанкционированном доступе направлен на решение этой задачи путем создания комплексной системы, способной не только обнаруживать попытки несанкциониро-

ванного проникновения в телекоммуникационный шкаф, но и оперативно оповещать ответственных лиц о подобных инцидентах [1–7].

Разработка подобной интеллектуальной системы станет важным шагом на пути к обеспечению комплексной безопасности телекоммуникационных сетей. Она позволит не только защитить ценное оборудование и конфиденциальные данные от несанкционированного доступа, но и обеспечить стабильную и бесперебойную работу всей телекоммуникационной инфраструктуры.

Методы и материалы

Разрабатываемая система сигнализации представляет собой программно-аппаратный комплекс, состоящий из следующих компонентов:

Микроконтроллер Arduino: является управляющим компонентом системы, отвечает за обработку данных, поступающих от сенсора, принятие решений об отправке уведомлений и ведение журнала событий [8–11].

Сенсор открытия дверцы: устанавливается внутри телекоммуникационного шкафа и реагирует на изменение положения дверцы. В качестве сенсора может использоваться датчик Холла (Датчик Холла – полупроводниковый прибор, который преобразует информацию о магнитном поле в электрический сигнал. Он работает на основе эффекта Холла, открытого в 1879 году американским физиком Эдвином Холлом), геркон (герметизированный контакт – это электромеханическое устройство, которое используется для замыкания или размыкания электрической цепи под действием магнитного поля) или другой подходящий тип сенсора. Помимо самого датчика необходим магнит, который необходим для срабатывания вышеуказанного элемента [12–16].

Модуль подключения к общей сети: обеспечивает передачу сигнала тревоги на устройства ответственных сотрудников. В зависимости от требований к системе и доступных возможностей, модуль может использовать различные технологии – GSM, Wi-Fi, Ethernet, для отправки уведомлений в виде SMS-сообщений, email-писем, push-уведомлений или других типов сообщений. На рисунке 1 указана схема сборки данной системы [17, 18].

Модуль реального времени: необходим для того, чтобы система записывала в свою собственную базу данных информацию о точной дате и времени каждого открытия и закрытия дверцы шкафа [19, 20].

Результаты

На данный момент разработана электрическая схема системы и проверена на виртуальном стенде (рис. 1). Она полностью выполняет все функции, которые требуются. Алгоритм данной системы максимально прост и последователен. Магнит, закрепленный на дверце, замыкает контакты геркона, вследствие чего система понимает, что на данный момент шкаф закрыт. В случае размыкания геркона с магнитом на микроконтроллер поступает сигнал и микроконтроллер понимает, что дверцу открыли. Он же, в свою очередь, обрабатывая сигнал с геркона отправляет уведомление на привязанное к нему устройство, а после запи-

сывает точную дату и время открытия/закрытия, благодаря модулю реального времени. Электрическая схема данной системы представлена на рисунке 1.

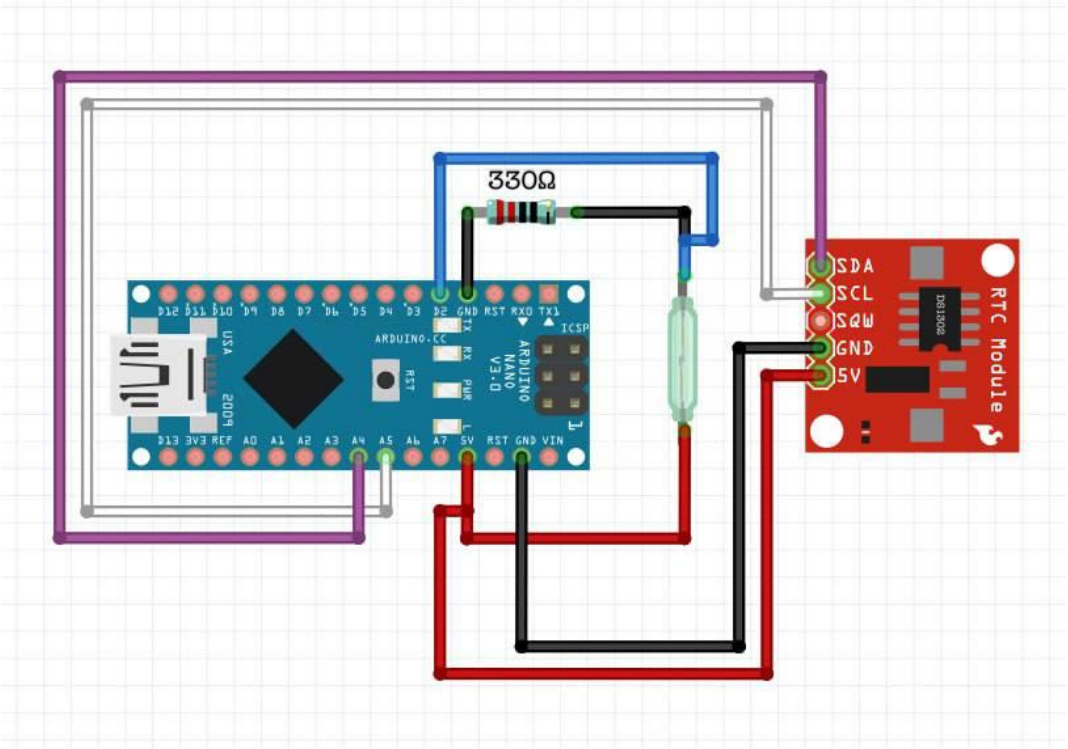

Рис. 1. Схема сборки системы сигнализации

Данная система предназначена для использования в промышленных организациях, в которых возможна утечка конфиденциальной информации, что может повлечь за собой как, финансовые, так и репутационные потери. Также сигнализация может быть использована в личных целях, поскольку принцип ее работы и установки может быть реализован с минимальными затратами. Принцип работы указан ниже.

1. Сенсор, установленный внутри шкафа, постоянно контролирует положение дверцы.

2. При открытии дверцы, сенсор генерирует сигнал, который поступает на микроконтроллер Arduino.

3. Arduino обрабатывает полученный сигнал и, в случае подтверждения факта открытия дверцы, инициирует отправку уведомления через выбранный модуль связи.

4. Уведомление содержит информацию о времени открытия дверцы и другую необходимую информацию, позволяющую идентифицировать шкаф и оценить серьезность ситуации.

5. Параллельно с отправкой уведомления, Arduino сохраняет информацию о событии в журнале, фиксируя дату и время открытия и каждого закрытия дверцы.

Заключение

Разработка данной системы является очень важным проектом, поскольку он затрагивает следующие аспекты защиты информации.

Повышение уровня безопасности: система обеспечивает контроль доступа к телекоммуникационному шкафу и позволяет оперативно реагировать на попытки несанкционированного проникновения.

Предотвращение утечек информации: своевременное оповещение о несанкционированном доступе позволяет предотвратить хищение или повреждение оборудования, а также утечку конфиденциальной информации.

Обеспечение стабильной работы: система способствует стабильной работе телекоммуникационных сетей, предотвращая сбои и простои, связанные с несанкционированным доступом к оборудованию.

Простота установки и обслуживания: использование доступных компонентов и интуитивно понятного программного обеспечения делает систему простой в установке и обслуживании.

Разработка интеллектуальной системы предупреждения о несанкционированном доступе к телекоммуникационному шкафу является актуальной задачей, решение которой позволит повысить уровень информационной безопасности компаний и организаций. Система, построенная на базе микроконтроллера Arduino, сенсора открытия дверцы и модуля отправки уведомлений, обеспечит надежный контроль доступа к критическому оборудованию, своевременное оповещение о потенциальных угрозах и предотвращение утечек конфиденциальной информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ищейнов, В. Я. Защита конфиденциальной информации: учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. – М.: Форум, 2009.

2. Безопасность объектов критической информационной инфраструктуры организации /Ассоциация руководителей служб информационной безопасности (АРСИБ). – М., 2019. – 111 с.

3. Сизова, О. В. Информационная безопасность: учеб. пособие / О. В. Сизова. – Иваново, 2015. – 120 с.

4. Жук, А. П. Защита информации: учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. – М.: РИОР, 201

5. Силантьев, И. О. Выявление утечек конфиденциальной информации в информационных системах / И. О. Силантьев, И. В. Аникин. – Курск: КНИТУ им. А.Н. Туплева-КАИ, 2013. – 6 с.

6. Прыгунов, А. Г. Современное развитие телекоммуникационных систем компьютерных систем: Монография / А. Г. Прыгунов, Р. И. Русанов, Ю. А. Шокова [и др.]. – М.: СкиПро, 2018. – 91 с.

7. Емельяненко, А. Ю. Проблемы и перспективы систем оповещения и информирования населения / А. Ю. Емельяненко, А. П. Иванников. – М.: Аспект Пресс, 2023. – 3 с.

8. Блум, Джереми. Изучаем ARDUINO: инструменты и методы технического волшебства / Джереми Блум; пер. с англ. – СПб.: БХВ-Петербург, 2017. – 336 с.

9. Ефимова, Ю. В. Использование Arduino Uno для реализации распределенной системы мониторинга рабочих станций водоснабжения / Ю. В. Ефимова. – Курск: КНИТУ им. А.Н. Туплева-КАИ, 2018. – 13 с.

10. Петин, В. А. Arduino и Raspberry Pi в проектах Internet of Things / В. А. Петин. – 2-е изд. – СПб.: БХВ, 2015. – 432 с.

11. Нидилько, М. В. Назначение и область применения, архитектура микроконтроллера / М. В. Нидилько. – М.: РГСУ, 2017. – 3 с.

12. Карабанов, С. М. Магнитоуправляемые контакты (герконы) и изделия на их основе: монография / С. М. Карабанов, Р. М. Майзельс, В. Н. Шоффа. – М.: Интеллект, 2011. – 408 с.

13. Блохин, А. В. Электротехника: учебное пособие / А. В. Блохин. – Екатеринбург: Урал. ун-та, 2014. – 184 с.

14. Портной, Г. Современные магниточувствительные датчики и приборы на их основе / Г. Портной. – 2013. – 6 с.

15. Джексон, Р. Г. Мир электроники. Новейшие датчики / Р. Г. Джексон. – М.: Техносфера, 2007. – 375 с.

16. Алейников, А. Ф. Датчики. Перспективные направления развития / А. Ф. Алейников, В. А. Гридчин, М. П. Цапенко. – 2001. – 107 с.

17. Мовсесян, В. А. Разработка программного модуля для обнаружения несанкционированного доступа в сетях Wi-Fi с открытым и закрытым сегментом: выпускная квалификационная работа: направление подготовки 10.05.01 Компьютерная безопасность; профиль подготовки Разработка защищенного программного обеспечения; очной формы обучения / В. А. Мовсесян; науч. рук. Л. Л. Гусева. – Ставрополь, 2019. – 88 с.

18. Галас, В. П. Вычислительные системы, сети и телекоммуникации: учебное пособие / В. П. Галас. – Владимир: ВлГУ, 2017. – 284 с.

19. Ананьев, Л. И. Модель и характеристики программного обеспечения реального времени / Л. И. Ананьев, С. В. Семенихин. – 2017. – 18 с.

20. Древс, Ю. Г. Системы реального времени: технические и программные средства: учебное пособие / Ю. Г. Древс; М-во образования и науки РФ, Нац. исслед. ядерный ун-т "МИФИ". – Москва: МИФИ, 2010. – 319 с.