

А. И. Петров¹✉, Д. Н. Титов¹

Разработка и изготовление системы сигнализирования несанкционированного физического доступа

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: malfas131@gmail.com

Аннотация. Объем информации постоянно растет, а с ним и оборудования для ее хранения и обработки. В том числе и телекоммуникационные шкафы. Угрозы могут быть не только виртуальные, но и физические. Для защиты от угроз с физическим проникновением в телекоммуникационный шкаф была создана система безопасности. В данной системе используются платы с микроконтроллером и Ethernet, что позволяет моментально реагировать на попытки несанкционированного доступа к телекоммуникационному шкафу и выводить информацию на ответственным лицам [1, 2].

Ключевые слова. микроконтроллер Arduino, механический концевой выключатель, Ethernet, телекоммуникационный шкаф, охранная сигнализация

A. I. Petrov¹✉, D. N. Titov¹

Development and manufacturing of an unauthorized physical access alarm system

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: malfas131@gmail.com

Annotation. The volume of information is constantly growing, and with it the equipment for its storage and processing. Including telecommunication cabinets. Threats can be not only virtual, but also physical. A security system has been created to protect against threats with physical penetration into the telecommunication cabinet. This system uses microcontroller and Ethernet cards, which allows you to instantly respond to attempts of unauthorized access to the telecommunication cabinet and output information to responsible persons [1,2].

Keywords. Arduino microcontroller, mechanical limit switch, Ethernet, telecommunication cabinet, security alarm system

Введение

Обеспечение сохранности данных требует контроля не только на программном, но и на физическом уровне [3]. Телекоммуникационные шкафы с серверным и сетевым оборудованием часто становятся объектом несанкционированного доступа [4]. Проникновение в такой шкаф может привести к утечке конфиденциальной информации, хищению оборудования и нарушению работы сетей [5].

Микроконтроллерные платформы, в частности Arduino, представляют собой удобную основу для разработки подобных устройств [6]. В качестве канала передачи сообщений целесообразно использовать проводную сеть Ethernet,

которая присутствует в большинстве офисных и производственных зданий [7]. Такой подход исключает абонентскую плату и обеспечивает высокую надежность доставки [8]. Целью настоящей работы является создание системы оповещения о несанкционированном доступе к телекоммуникационному шкафу на базе Arduino, механического датчика и Ethernet-модуля [9].

Методы и материалы

При разработке системы были учтены требования: детектирование открытия дверцы, передача тревожных сообщений через Ethernet, ведение журнала событий с временной привязкой, автономность и низкая стоимость [10]. В качестве управляющего элемента выбран микроконтроллер Arduino Uno (ATmega328P), который обладает достаточным количеством цифровых выводов и поддерживает подключение модулей по интерфейсу SPI [11].

Для фиксации положения дверцы применен механический концевой выключатель с нормально замкнутыми контактами [12]. При закрытой дверце выключатель находится в нажатом состоянии, при открытии контакты возвращаются в исходное положение, вызывая изменение напряжения на входе микроконтроллера [13]. Механический датчик выбран вместо геркона, поскольку он не требует магнита, устойчив к вибрациям и не может быть обойден внешним магнитным полем [14].

Передача сигнала тревоги реализована через Ethernet-модуль W5100, подключаемый к Arduino по шине SPI [15]. Модуль обеспечивает отправку UDP-пакетов или HTTP-запросов на заданный IP-адрес [16]. Для ведения журнала событий используется модуль реального времени DS3231 (интерфейс I2C), который сохраняет точные дату и время каждого открытия и закрытия дверцы [17]. Питание системы осуществляется от адаптера 5 В с возможностью резервирования через аккумулятор [18].

На рис. 1 приведена электрическая схема подключения механического датчика, модуля Ethernet и модуля RTC к плате Arduino.

Результаты

Разработанный прототип был собран на макетной плате и испытан в лабораторных условиях [19]. Алгоритм работы включает непрерывный опрос цифрового пина, соединенного с механическим датчиком. При закрытой дверце на входе контроллера поддерживается стабильный логический уровень. В момент открытия дверцы возникает перепад напряжения [20].

При обнаружении перепада микроконтроллер считывает текущее время с модуля RTC, формирует строку-уведомление, содержащую идентификатор шкафа и временную метку. Затем через Ethernet-модуль отправляется UDP-пакет на сервер или рабочую станцию ответственного сотрудника. После подтверждения отправки информация о событии сохраняется в энергонезависимую память EEPROM Arduino. Аналогичным образом фиксируется момент закрытия дверцы, что позволяет вести полный журнал доступа.

Тестирование показало, что задержка между размыканием контакта датчика и отправкой сетевого пакета составляет не более 50 миллисекунд. Ложные срабатывания при вибрациях отсутствовали. Модуль RTC обеспечил точность временных меток ± 2 минуты в месяц. Передача через Ethernet не создает дополнительных расходов на связь и гарантирует доставку сообщения в пределах локальной сети. Схема сборки показана на рис. 1.

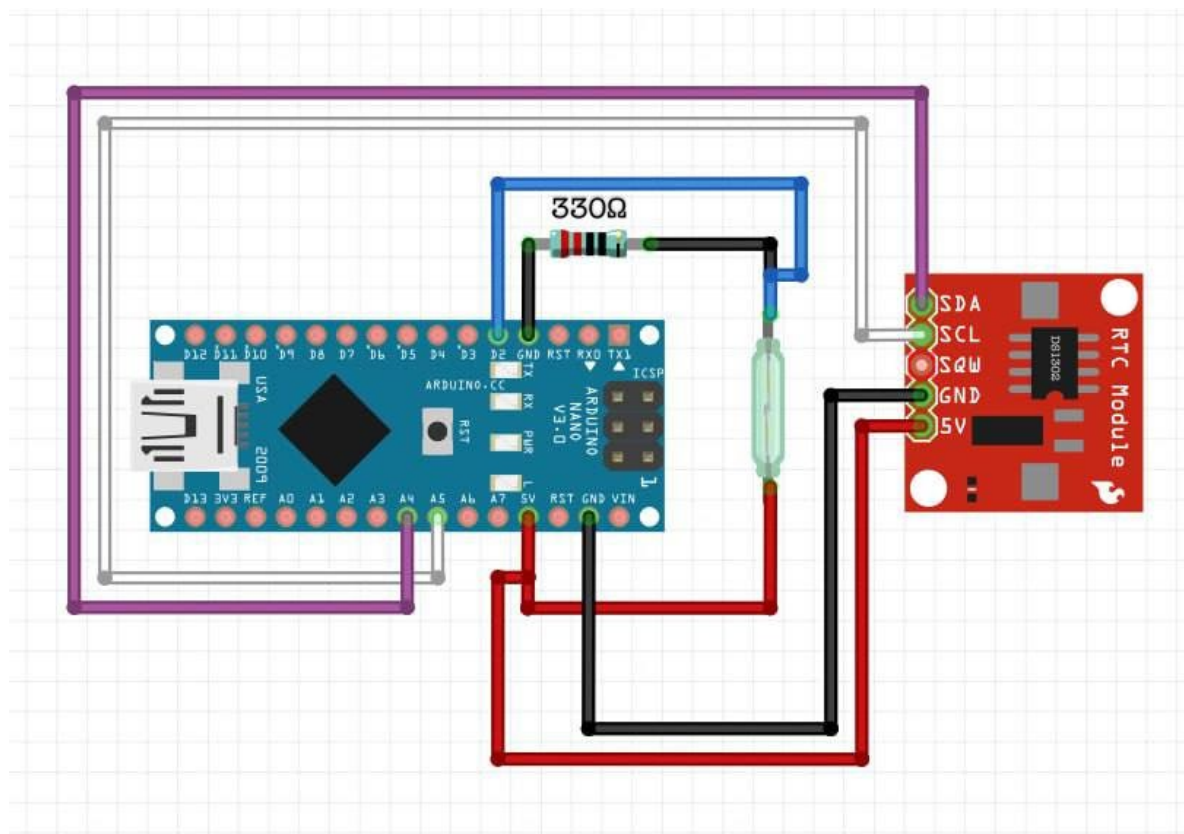


Рис. 1. Электрическая схема подключения микроконтроллера Arduino к механическому датчику, модулю RTC и Ethernet-модулю W5100

Основным преимуществом использования проводного Ethernet-канала является высокая надежность и устойчивость к помехам, а также отсутствие абонентской платы. Система легко интегрируется в существующую корпоративную сеть. Микроконтроллерная платформа Arduino позволяет добавлять дополнительные функции, такие как периодическая отправка тестовых сообщений о работоспособности.

Заключение

Разработанная система на базе микроконтроллера Arduino, механического концевого выключателя и Ethernet-модуля представляет собой эффективное и экономичное решение для контроля физического доступа к телекоммуникационному шкафу. Механический датчик положения обеспечивает надежное детектирование открытия дверцы, не требует магнита и устойчив к обходу внешними

полями. Ethernet-канал связи гарантирует быструю (менее 50 мс) и бесплатную передачу тревожных сообщений. Прототип успешно прошел испытания, ложные срабатывания отсутствуют, а журнал событий ведется с точной временной привязкой.

Дальнейшее совершенствование системы может включать интеграцию с существующими системами мониторинга (Nagios, Zabbix), использование шифрования передаваемых пакетов, а также переход на питание по PoE. Предложенное решение может быть рекомендовано для использования в офисных и промышленных сетях, где имеется проводная инфраструктура.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Джереми Блум, изучаем ARDUINO: инструменты и методы технического волшебства: Пер. С англ. – СПб.: БХВ–Петербург, 2017. – 336 с.
2. Карабанов С. М., Майзельс Р. М., Шоффа В. Н., Магнитоуправляемые контакты (герконы) и изделия на их основе: монография.: Интеллект, 2011. – 408 с.
3. Блохин А. В., Электротехника: учебное пособие: Изд-во Урал. Ун-та, 2014. – 184 с.
4. Сизова О. В., Информационная безопасность: учеб. пособие: Иваново, 2015. – 120 с.
5. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И., Защита информации: учебное пособие: Изд-во РИОР, 2013. – с.
6. Ищейнов В.Я., Мецатунян М.В., Защита конфиденциальной информации: учебное пособие: Изд-во Форум, 2009. – с.
7. Петин В.А., Arduino и Raspberry Pi в проектах Internet of Things. 2–е. изд., Изд-во БХВ, 2015, – 432 с.
8. Ананьев Л.И., Семенихин С.В., Модель и характеристики программного обеспечения реального времени, 2017, – 18 с.
9. Портной Г., Современные магниточувствительные датчики и приборы на их основе, 2013, – 6 с.
10. Древис Ю.Г., Системы реального времени: технические и программные средства: учебное пособие / Ю. Г. Древис ; М-во образования и науки РФ, Нац. исслед. ядерный ун-т "МИФИ". – Москва : МИФИ, 2010. – 319 с.
11. Галас В.П., Вычислительные системы, сети и телекоммуникации: учебное пособие, Изд-во ВлГУ, 2017, – 284 с.
12. Нидилько М.В., Назначение и область применения, архитектура микроконтроллера, Изд-во РГСУ, 2017, – 3 с.
13. Ефимова Ю.В., Использование Arduino Uno для реализации распределенной системы мониторинга рабочих станций водоснабжения, КНИТУ им. А.Н. Туплева-КАИ, 2018, – 13 с.
14. Безопасность объектов критической информационной инфраструктуры организации, Ассоциация руководителей служб информационной безопасности (АРСИБ), 2019, – 111 с.
15. Джексон Р.Г., Мир электроники. Новейшие датчики, Изд-во Техносфера, 2007, – 375 с.
16. 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.
17. Силантьев И.О., Аникин И.В., Выявление утечек конфиденциальной информации в информационных системах, Научная статья, КНИТУ им. А.Н. Туплева-КАИ, – 2013, – 6 с.
18. Прыгунов А.Г., Русанов Р.И., Шокова Ю.А., Ал-Али Хайдер Тахсин Али, Аль-Фархан Гхассан Хассан Али, Бурнашев И.Я., Звездина М.Ю., Назарова О.Ю., Современное

развитие телекоммуникационных систем компьютерных систем: Монография: Изд-во СкиПро, 2018, – 91 с.

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

20. Емельяненко А.Ю., Иванников А.П., Проблемы и перспективы систем оповещения и информирования населения, Изд-во Аспект, 2023, – 3 с.

© А. И. Петров, Д. Н. Титов, 2026