

УДК 681.518:004.056

СИСТЕМА ЭЛЕКТРОННОГО УЧЕТА КЛЮЧЕЙ ПРЕДПРИЯТИЯ

Бычков Владислав Ярославич¹, кандидат технических наук., доцент кафедры радиоэлектроники

e-mail: dragruz@yandex.ru

Грошков Даниил Андреевич¹, студент

e-mail: groshkov.daniil@yandex.ru

¹ Волжский государственный университет водного транспорта, Нижний Новгород, Россия

Аннотация. В статье рассматривается концепция создания автоматизированной системы учета ключей для повышения безопасности внутренних помещений предприятия. Основная идея проекта – замена «журнального» учета ключей предприятия на электронную систему с возможностью фиксации времени выдачи и возвращения, идентификацией сотрудника и ограничение доступа к помещению при нарушении регламента сотрудником.

Ключевые слова: учет ключей, контроль доступа, автоматизация, безопасность предприятия, электронный журнал, RFID, NFC.

ELECTRONIC SYSTEM FOR ACCOUNTING OF ENTERPRISE KEYS

Vladislav Y. Bychkov¹, Candidate of Technical Sciences, Associate Professor

e-mail: dragruz@yandex.ru

Daniil A. Groshkov¹, Student

e-mail: groshkov.daniil@yandex.ru

¹ Volga State University of Water Transport, Nizhny Novgorod, Russia

Abstract. The article discusses the concept of creating an automated key management system to improve the security of an enterprise's internal premises. The main idea of the project is to replace the traditional "logbook" key management system with an electronic system that can record the time of key issuance and return, identify the employee, and restrict access to the premises if an employee violates the regulations.

Keywords: key accounting, access control, automation, enterprise security, electronic journal, RFID, NFC.

В настоящее время остро стоит вопрос с обеспечением безопасности предприятий. Однако, некоторые предприятия продолжают обеспечивать контроль выдачи ключей в письменной форме, в журнале учета ключей. Связи с развитием технологий позволяющих отслеживать перемещение сотрудников предприятия такой метод ведения учета ключей

является устаревшим и для устранения ошибок, связанных с человеческим фактором, необходимо провести модернизацию, чтобы уменьшить время на поиск «носителя» ключа и обеспечить удобный доступ к помещениям.

Главным отличием разрабатываемого устройства является модульность и как следствие универсальность позволяющую использовать систему на предприятиях любых масштабов и в том числе на пассажирских судах.

Первый модуль (рис. 1) отвечает за хранение и выдачу ключей, состоит из блоков индикации, контроля, управления и блоков выдачи ключей. Данные модули могут собираться в последовательную цепь и управляться совместно, единственная необходимость — это программная настройка и размещение обозначений на слотах для визуальной идентификации позиций ключей. Модуль, объединяющий ряд блоков с линиями связи, подсоединяется к общей шине при помощи шлейфа.

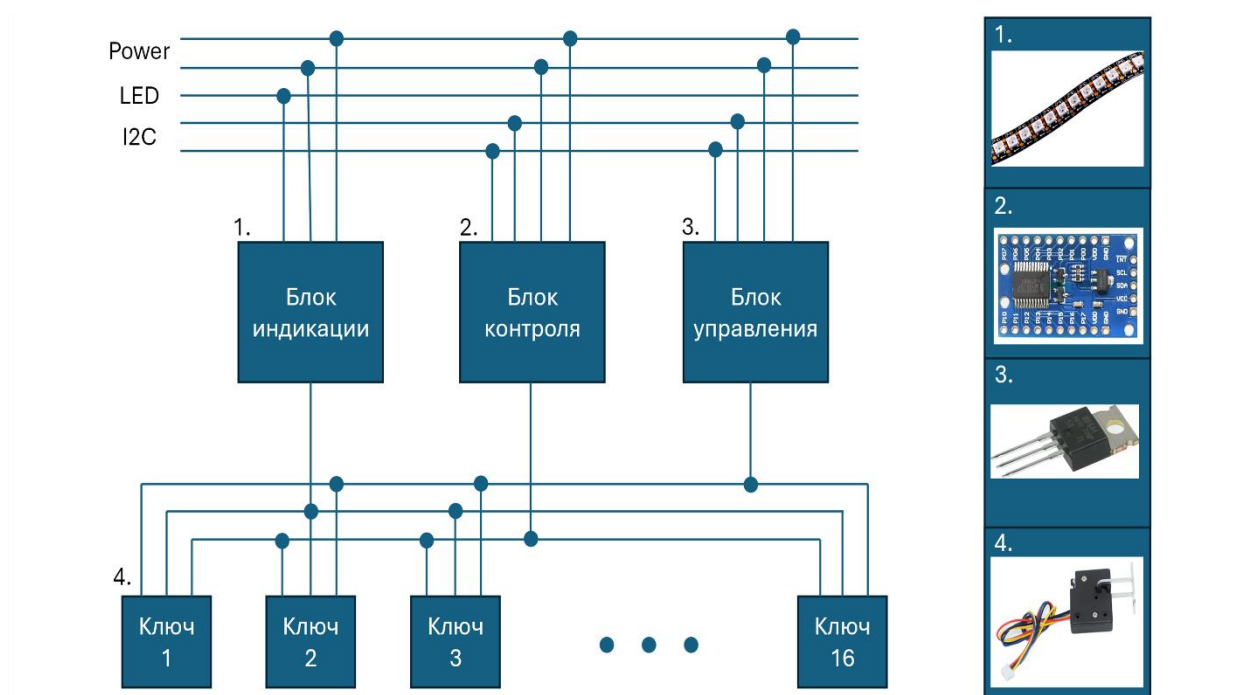


Рисунок 1 – Схематичное изображение первого модуля

1. Блок индикации предполагает световую индикацию выдаваемого ключа, недостающих ключей, а также уведомляет о неправильно ключах, размещенных в несоответствующих им слотах. Для этого используются адресные светодиоды, что позволяет использовать только одну дискретную ножку контроллера для управления всеми светодиодами вне зависимости от количества модулей в системе.

2. Блок контроля, служит для считывания состояний всех замков в реальном времени, т.е. определяет наличие ключей и регистрирует их возврат. Для этой задачи используется плата расширения GPIO PCF8575 [1], которая за счет шины «I2C» [2] позволяет расширить количество контактов контроллера, что дает возможность реализовать систему с как минимум 128 ключами.

3. Блок управления, необходим для обеспечения питания системы выдачи ключей. Используются n-канальные MOSFET транзисторы, что позволяет управлять открытием замков при помощи сигналов микроконтроллера, не нагружая контакты управления высоким током. Для управления транзисторами используется та же плата расширения PCF8575, что и в блоке контроля, за счет использования набора цифровых ключей.

4. Блок замка, оснащен силовыми управляющими контактами, при подаче питания на которые, с транзистора и происходит открытие замка. Также есть сухой контакт, показывающий текущее состояние при открытии или закрытии замка (за счет конструкции замка также определяется и наличие ключа в слоте).

Второй модуль (рис. 2) является главным управляющим элементом устройства. Он берет на себя задачу согласования и управления модулями, а также реализует графический интерфейс пользователя и функцию идентификации пользователя. Состоит из контроллера, дисплея, блока идентификации и источника аварийного питания.

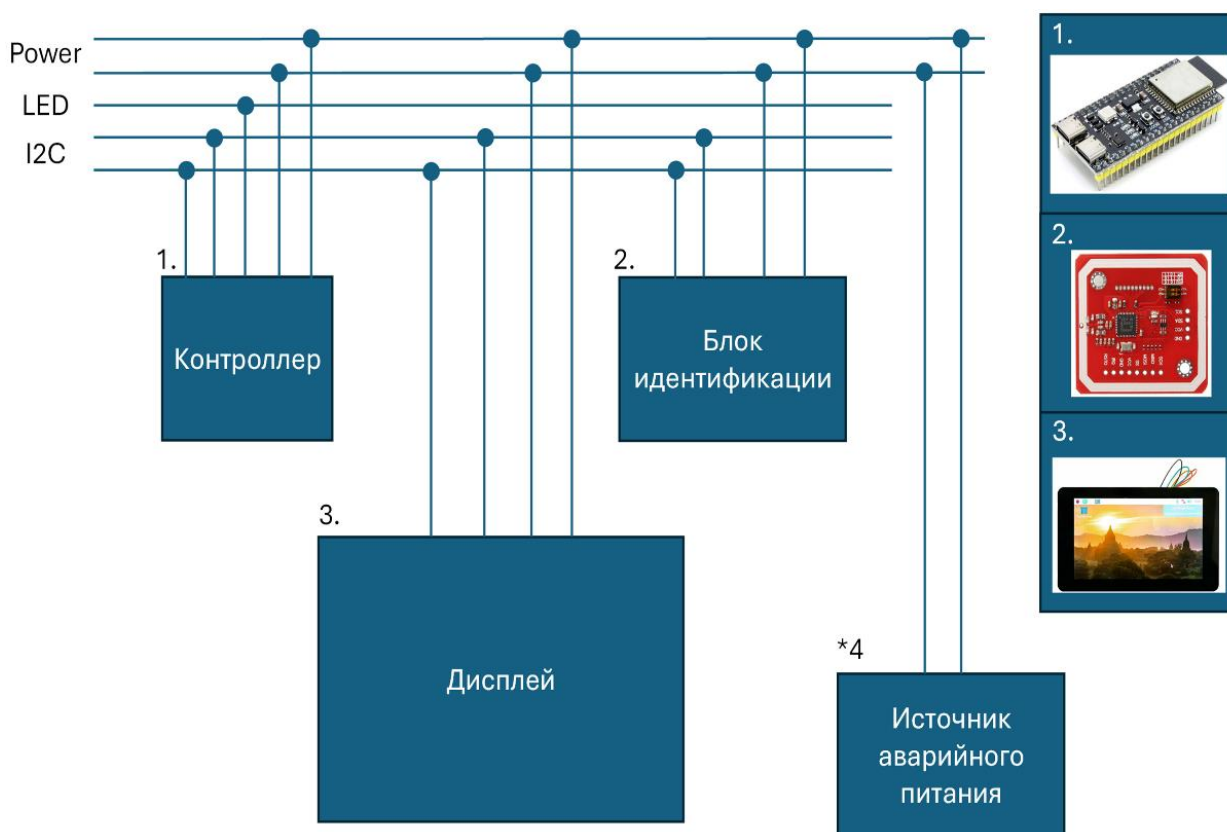


Рисунок 2 – Схематичное изображение второго модуля

1. Контроллер выполняется на базе ESP32 [3] (оптимален по доступности, цене и функционалу) и берет на себя управление системой считывания, выдачи и отвечает за выдачу кода на адресные светодиоды индикации.

2. Блок идентификации, для определения пользователя в системе. Самым распространенным вариантом идентификации на предприятиях является RFID метки, либо их разновидность NFC, которую также поддерживают современные телефоны. Чаще всего личные пропуска подобного типа уже существуют и используются для пропускной системы и логично использовать именно их для управления доступом к системе выдачи ключей. Поэтому блок идентификации включает в себя как классических RFID модуль на 125 кГц, так и NFC модуль на 13,56 МГц. Кроме идентификации пользователя блок также позволяет создавать систему уровней доступа, т.к. зачастую некоторые помещения должны быть с ограниченным доступом.

3. Сенсорный дисплей, на котором пользователи будут вводить номер аудитории, к которой они хотят получить доступ. Также планируется выводить на экран подсказки к системе: ключ находится не в своей ячейке, ключ уже выдан другому пользователю, дополнительная информация для службы безопасности и т.п.

4. Источник аварийного питания для работы устройства при отключении основного питания, в том числе для реализации функции полной разблокировки всех ключей (например, в случае пожара).

Основная сложность реализации системы учета ключей заключается в разнообразии форм и размеров ключей, ведь они могут быть не только от разных типов замка, но и вообще картой RFID, поэтому самым простым решением будет ввести специализированный брелок (рис. 3) на ключ, ведь на нем все равно должна присутствовать отметка от какого он помещения.

Брелок является многозадачным и решает как базовые задачи, так и реализует дополнительные функции, связанные с безопасностью и удобством. К примеру, одной из важнейших задач брелка является правильное позиционирование в нужном слоте системы для чего он оснащается микросхемой с интерфейсом «1-wire» позволяющей контролировать, что в слот возвращен конкретный ключ. Положение ключа внутри слота контролируется его конструкцией, за счет формы брелка он фиксируется в своем слоте и может быть вставлен только в одном положении. Конструкция позволяет разместить на верхней плоскости гравировку или надпись с текстовым обозначением помещения для которого предназначается ключ. В качестве дополнительной функции брелок может быть оснащен микросхемой RFID/NFC (если помещение оснащено электронным замком, что позволяет отказаться от самой карточки). При этом подделать брелок достаточно сложно, а заменить при утере можно только через службу безопасности.

Брелок выполнен на единой печатной плате, которая служит, как несущий каркас для замка. На нижней стороне для обеспечения контакта с линией «1-wire» располагаются две дорожки (они покрываются иммерсионным золочением для защиты от окисления и истирания) и при необходимости там же может быть нанесен логотип. Верхняя часть залита слоем из эпоксидной смолы или литьевого пластика, для защиты компонентов на поверхности платы и дальнейшего нанесения поверх номера или названия помещения. Заготовки брелков универсальны, что позволяет иметь складской запас. Для добавления ключа достаточно программной регистрации, назначения слота и нанесения идентификатора гравировкой или краской. Крепление брелков к ключам осуществляется стальным тросом с неразъемной опрессовкой либо резьбовым фиксатором – это предотвращает демонтаж без специнструмента.

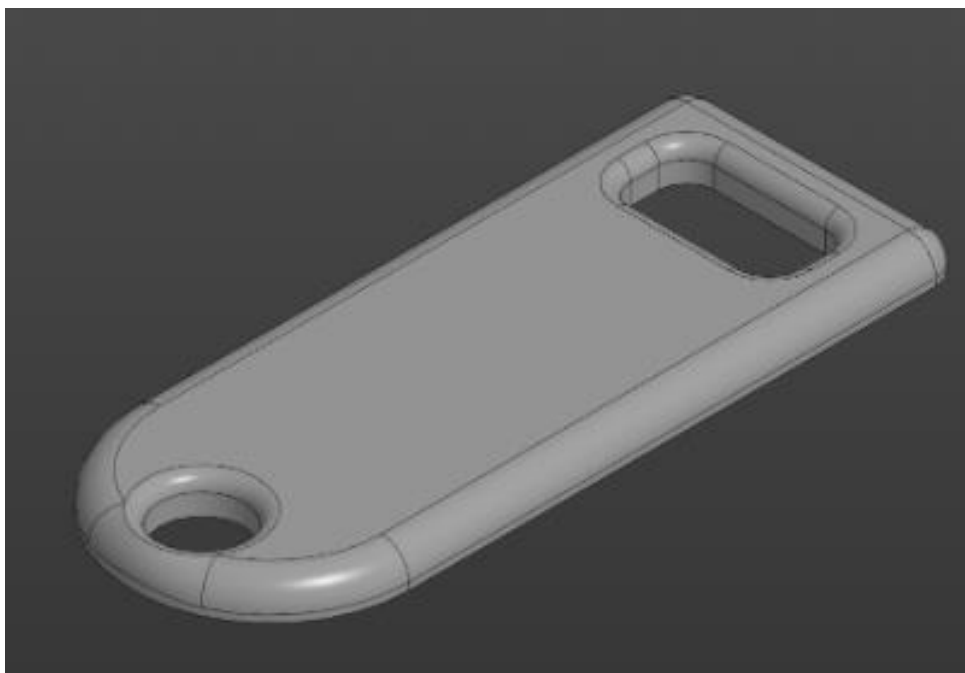


Рисунок 3 – Эскиз формы брелка для ключа

Предлагаемая система универсальна, её можно внедрить не только в новых корпусах предприятий, но и в уже имеющихся, а при оснащении системы центральным сервером, для хранения базы данных и поддержания сетевых подключений, система может, например, применяться на пассажирских судах, где получение ключа от кают может быть реализовано при помощи приложения в телефоне и NFC модуля этого же телефона или на предприятиях где требуется наличие не только общего места хранения ключей, но и дублирующих локальных постов.

Список литературы:

1. PCF8575 Remote 16-bit I/O expander for I²C-bus — Текст: электронный // chipdip.ru : [сайт]. — URL: <https://static.chipdip.ru/lib/496/DOC011496854.pdf> (дата обращения: 13.02.2026).
2. AlexGyver Интерфейс I2C (Wire) для Arduino / AlexGyver. — Текст: электронный // AlexGyver: [сайт]. — URL: <https://alexgyver.ru/lessons/wire-i2c/> (дата обращения: 21.01.2026).
3. esp32-s3_datasheet_en.pdf . — Текст: электронный // espressif.com : [сайт]. — URL: https://documentation.espressif.com/esp32-s3_datasheet_en.pdf (дата обращения: 23.05.2026).