Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
Информатики и радиоэлектроники
Кафедра инженерной психологии и эргономики

УДК 62-519

Лавров
Игорь Владимирович

СИСТЕМА УПРАВЛЕНИЯ КОНТРОЛЕМ ДОСТУПА

АВТОРЕФЕРАТ
на соискание академической степени магистра техники и технологий

1-59 81 01 «Управление безопасностью производственных процессов»

Магистрант И.В. Лавров

Научный руководитель
В.В Мазюк, кандидат
технических наук, доцент

Заведующий кафедрой ИПиЭ
К.Д.Яшин, кандидат
технических наук, доцент

Нормоконтролёр
Е.С. Иванова,
ассистент кафедры ИПиЭ

Минск 2016

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Основной целью данной магистерской диссертации является разработка контроллера системы контроля и управлением доступа для тренировки режимного объекта с ограниченным доступом. В работе рассматриваются вопросы проектирования подобного вида устройств.

В первой главе рассматриваются аспекты существующих систем с RFID идентификацией. Разрабатываемый в рамках магистерской диссертации проект представляет собой центральное устройство управления системы управления контролем доступа, возможности и интерфейсы которого определяют доступный функционал; подобное устройство в своем составе имеет каждая СКУД. Для начала проводится анализ существующих СКУД с технологией RFID. Затем рассматриваются существующие высокоинтегрированные решения для обеспечения RFID аутентификации, т.к. зачастую используются именно они в серийных коммерческих изделиях, а также в любительских целях. Далее рассматривается вопрос наличия уязвимостей в топологии микросхем узкого назначения, а также приводятся данные из имеющихся публикаций по данному вопросу, после чего делается вывод, что необходимо реализовывать RFID-цепь на дискретных аналоговых элементах. Выполняется постановка задач и целей проектирования.

Вторая глава рассматривает парадигму безопасности, принятые понятия, организационные и технические меры, которые применяются уже долгое время, вводится понятие зон доступа и многое другое. Рассматривается структура конкретного проектируемого устройства и его место в системе пропуска персонала по определенным атрибутам доступа (метки, пароли). Выполняется проектирование схемы электрической структурной, принципиальной и анализ элементной базы. Также сформированы эргономические требования к рабочему месту оператора АРМ на пункте охраны, который является важным звеном в обеспечении безопасности данной системы.

Третья глава содержит раздел с подробным описанием структуры программного обеспечения устройства и подробное описание всех его частей на функциональном уровне. Также в рамках этой главы проведено испытание устройства, в рамках возможных ситуаций использования, моделирующих поведение злоумышленника и допущенного лица.

ВВЕДЕНИЕ

В последние годы одним из наиболее эффективных и цивилизованных подходов к решению задачи комплексной безопасности объектов различных форм собственности является использование систем контроля и управления доступом (СКУД). Правильное использование СКУД позволяет закрыть несанкционированный доступ на территорию, в здание, отдельные этажи и помещения. В то же время они не создают препятствий для прохода персонала и посетителей в разрешенные для них зоны. Интерес к СКУД неуклонно растет, что уже приводит к их все более широкому распространению.

Следует помнить, что СКУД не устраняет необходимость контроля со стороны человека, но значительно повышает эффективность работы службы безопасности, особенно при наличии многочисленных зон риска. СКУД освобождает охранников от рутинной работы по идентификации, предоставляя им дополнительное время по выполнению основных функций: охране объекта и защите сотрудников и посетителей от преступных посягательств. Оптимальное соотношение людских и технических ресурсов выбирается в соответствии с поставленными задачами и допустимым уровнем возможных угроз. Однако в настоящее время процесс выбора подходящих СКУД носит сложный характер, поскольку реально отсутствует какая-либо аналитическая информация по имеющимся сегодня в мире СКУД.

Одним из направлений обеспечения информационной безопасности на предприятии или в организации является инженерно-техническая защита, в рамках которой используются системы контроля и управления доступом. Перед проектирующим систему информационной защиты организации специалистом нередко ставится задача обеспечения для сотрудников защиты на некоторой территории, внутри которой возможен свободный обмен. Такие требования могут предъявляться к некоторым помещениям режимных объектов, в которых важно контролировать прохождение всех допущенных, и, разумеется, не допущенных лиц.

В качестве центрального элемента такой системы можно предложить устройства, разрабатываемые на базе микроконтроллеров, которое управляет исполнительными устройствами, опрашивает устройства авторизации и взаимодействует с удаленным АРМ оператора, который разрешает или запрещает доступ на основе базы данных о пользователях. В данной работе в качестве способа авторизации будет использоваться получившая широкое распространение технология радиочастотной идентификации (RFID).

RFID или радиочастотная идентификация – технология, использующая радиочастотное электромагнитное излучение для чтения/записи информации на небольшое устройство, называемое тэг (tag), метка (label), или транспондер (transponder). Задачей RFID системы является хранение информации об объекте с возможностью её удобного считывания. Метка может содержать данные о типе объекта, стоимости, весе, температуре, данные логистики, вообще любой информации, которая может храниться в цифровой форме.

Любая RFID система состоит из трёх базовых компонентов:

1. Считывающего устройство, называемое ридером (от англ. reader) (передатчик/приемник).
2. Антенны.
3. Радиочастотных меток (смарт-меток) с встроенной антенной, приемником и передатчиком.

Существует большое число разновидностей этих компонентов. Они различаются по устройству, размерам и форме. Применительно к СКУД, чаще всего используются метки в виде карточки, выполненные по технологии Mifare (13,56 МГц) либо EM-Marin (125 кГц)[1].

В простоте технологии RFID и кроется одно из её самых слабых мест: стоит потерять метку или её похитит злоумышленник (также часто применяется термин «скомпрометировать»), и система получает уязвимость. В данной работе описан один из способов повышения надежности подобных RFID-систем, на опыте разработки прототипа устройства управления.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Как правило, для реализации RFID-идентификации используется следующая связка: микроконтроллер общего назначения и специализированная интегральная схема, зачастую программируемая (полностью или частично), которые взаимодействуют между собой посредством одного из стандартных интерфейсов: I^2C, UART, SPI. Почти все основные производители, так или иначе связанные с embedded-разработкой имеют свои варианты подобных решений. Данные микросхемы обладают важными преимуществами: малые габариты, малое энергопотребление, малое количество вспомогательных элементов. Именно благодаря этому, зачастую используются именно они в серийных коммерческих изделиях, а также и в любительских целях. Далее рассматриваются некоторые из подобных микросхем.

При всех достоинствах, использование подобных решений влечет за собой возможность активизации аппаратного бэкдора, который может быть использован злоумышленником, имеющим отношение к производителю. Особенно важно исключить подобные возможности взлома в сфере госбезопасности и защиты национальных интересов. Реальность такова, что большинство современных крупных производителей микросхем являются fabeless-компаниями (т.е. не обладают непосредственными производственными мощностями, исключение – Intel, Samsung, IBM и еще некоторые немногие) и сами занимаются непосредственно только проектированием топологии микросхемы, а непосредственно полупроводниковое производство доверяют контрактным производителям, крупнейшим из которых является, например, тайваньская TSMC. Таким образом, увеличение числа посредников в производственной цепочке увеличивает возможность аппаратной закладки. Причем данные закладки могут быть топологически исполнены так, что даже визуальный контроль не позволит выявить уязвимости.

Несколько лет назад группа исследователей компьютерной безопасности опубликовала доклад, описывающий технику внедрения бэкдоров на уровне микросхем, реализуемых в форме внесения в эталонный шаблон микросхемы модификаций через изменение полярности штатно присутствующих в схеме транзисторов, что позволяет вносить дополнительную логику без изменения дизайна транзисторных блоков и делает невозможным обнаружение троянских вставок большинством существующих методов проверки, таких как оптический анализ и сравнение с эталоном.

Указанная техника может быть использована для внедрения бэкдоров без ведома заказчика, путём скрытых модификаций на этапе производства,

которые, например, могут быть внесены подкупленным сотрудником предприятия. В качестве демонстрации работы метода, в докладе приведён пример внедрения гипотетического бэкдора в аппаратный генератор случайных чисел процессоров Intel и в iMDPL-реализацию AES SBox-преобразований.

Все вышеописанные случаи и проведенные исследования лишний раз подтверждают, что интегральные микросхемы, в особенности узкопрофильного назначения – в нашем случае микросхемы RFID – вполне могут иметь аппаратный вектор уязвимости, который сложно распознать и обезвредить.

Объектом исследования в диссертации являются СКУД, использующие RFID технологию. Предмет исследования – методы и способы повышения надежности систем авторизации подобного типа.

Задачи исследования были поставлены следующие:

1. Изучить аналоги и сопутствующую литературу по подобным RFID системам, научные статьи по исследованиям защищенности интегральных схем.

2. Провести теоретическое проектирование опытного макета системы контроля управления доступа, с учетом компенсации слабых мест существующих систем. Подготовить графический материал, документацию к нему.

3. Разработать программное обеспечение для спроектированного аппаратного решения, собрать рабочий макет, провести его испытание, сделать выводы по результатам испытаний макетного образца.

Целью работы является проектирование контроллера СКУД с двухфакторной аутентификацией: на базе RFID технологии и цифровой клавиатуры. Антенная цепь RFID должна быть выполнена на дискретной элементной базе, без применения готовых интегрированных решений. Предполагается использовать карты стандарта EM-Marin, т.к. они производятся предприятиями Республики Беларусь.

В проектируемой системе будет принято следующее расположение устройств аутентификации: первичное устройство аутентификации будет расположено за пределами зоны доступа, снаружи, а вторичное, подтверждающее устройство аутентификации – цифровая клавиатура – будет находиться на следующем уровне доступа. Логично было бы предположить, что пройдя внутрь, лицо, использовавшее карту, должно введением кода за определённый ограниченный короткий, но достаточный временной промежуток, подтвердить этим принадлежность карты владельцу. Схематичное изображение подобной системы приведено на рисунке 1:

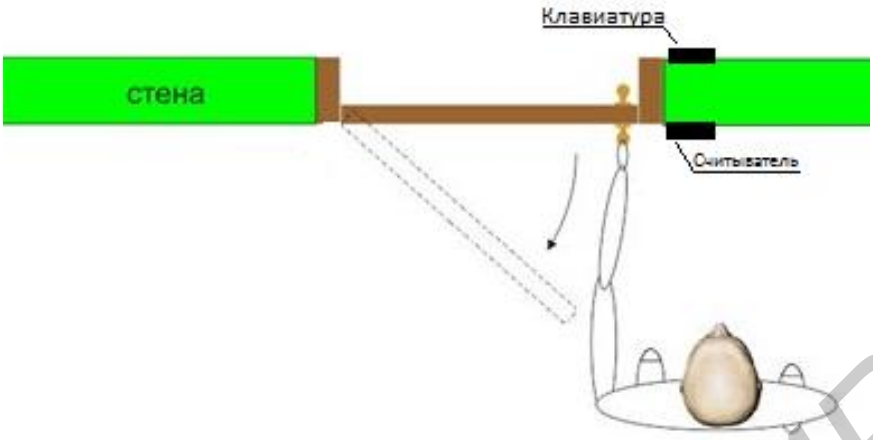

Рисунок 1 – Схематичное изображение расположения устройств ввода

Данный механизм позволил бы закрыть фундаментальную уязвимость, существующую в системах в использованием RFID. Однако подобный шаг создавал бы еще большую уязвимость: в том случае, если картой воспользовалось недоверенное лицо и не ввело пароль находясь на следующем уровне доступа, то такой злоумышленник получает на некоторое время несанкционированный доступ в помещение, что недопустимо исходя из парадигмы безопасности. Поэтому для использования подобной комбинации устройств ввода (аутентификации) предлагается использовать тамбур-шлюз.

Шлюз или шлюзовая кабина - это устройство или набор устройств, позволяющих реализовать при проходе режим шлюзования, т.е. разделить поток, последовательно строго по одному пропуская пользователей через несколько преграждающих устройств (как правило, дверей, отвечающих тем или иным требованиям по защите от взлома). Шлюзы могут быть предназначены как для прохода персонала, так и для провоза грузов и материалов (транспортные шлюзы). Существуют, например, так называемые, медицинские шлюзы, позволяющие производить дезинфекцию и полностью исключающие проникновение воздуха через створки, специальные шлюзы радиационные с дозиметрической аппаратурой и т.д. На рисунке 2 показан стандартный алгоритм прохода через шлюз, который может быть реализован при автоматической работе шлюза:

Рисунок 2 – Стандартный алгоритм прохода через шлюз

С целью получения дополнительных данных алгоритм работы может быть изменен, внутри шлюза от пользователя могут потребовать предъявления дополнительных данных, его могут подвергнуть дополнительному исследованию с использованием биометрии, металлодетектора, гамма-детектора, весовой системы и т.п. В любом случае, это будет прерывание стандартного алгоритма прохода с введением дополнительных условных схем.

Классический шлюз для систем безопасности - набор двух дверей, контролируемых логикой и оснащенных средствами СКУД. По функционалу существует деление шлюзовых кабин на автоматические, полуавтоматические и ручные. По конструктивному исполнению существует три основные разновидности шлюзовых кабин:

1. Шлюзовые кабины с распашными дверьми, оснащенным различными типами устройств - от доводчиков, электромагнитных или электромеханических замков до сложных электроприводов.

2. Шлюзовые кабины с раздвижными дверьми.

3. Шлюзовые кабины с вращающимися створками.

Многие производители предлагают шлюзовую кабину как законченное, готовое к эксплуатации изделие с возможностью дополнить рядом ограниченных опций. При упоминании слова «шлюзовая кабина» миллионы людей во всем мире вспоминают автоматические шлюзовые кабины с раздвижными дверьми, устанавливаемые, как правило, в банках и представляющие собой законченное устройство с двумя дверьми и различными дополнительными опциями, интегрированными в единый усиленный корпус.

Плюсы подобного подхода - простота монтажа и настройки. Все уже собрано и настроено, необходимо просто доставить изделие на место и подключить к питанию и системе контроля доступа. Минусы - громоздкую конструкцию тяжело, а иногда и невозможно смонтировать в удаленном от входа проеме, ее вес иногда зашкаливает за тонну, что не всегда приемлемо для несущих перекрытий здания, кроме того, стандартные типоразмеры требуют дополнительных трудозатрат на отделку оставшихся щелей.

После включения в состав системы шлюзовой кабины с двумя дверями, схематическое изображение системы будет выглядеть так, как показано на рисунке 3 Причем алгоритм прохода будет такой: сначала используется RFID-метка для открытия первой двери, затем используется цифровой код для открытия второй двери. При этом, если лицо израсходовало все попытки ввода кода, то об этом сообщается на автоматизированное рабочее место (АРМ) пункта охраны. Предполагается, что в этом случае при помощи визуального контроля или с использованием видеокамеры, установленной внутри или снаружи тамбур-шлюза, принимается решение о ручном допуске – в том случае если это допущенное лицо и оно просто забыло цифровой код; или о недопуске – в случае если это лицо злоумышленник. Использование тамбур шлюза в данной ситуации так же имеет еще одну положительную сторону: в случае если злоумышленник попадет внутрь кабины посредством RFID-метки, но не введет верный код, то он останется заблокированным внутри тамбур шлюза, что автоматически обезвреживает его. Усовершенствованный вариант прохода схематично изображен на рисунке 3:

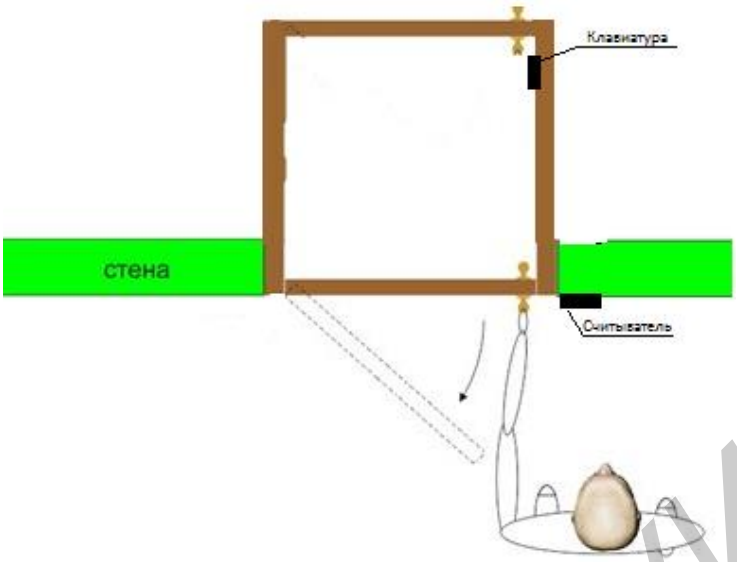

Рисунок 3 – Схематичный вид после добавления тамбур шлюза

В качестве запирающего устройства предполагается электромагнитный замок. Выбор сделан в пользу именно подобного запирающего устройства, т.к. он более устойчив ко взлому, чем механические аналоги, а также имеет одну важную особенность: если возникнет пожар, то, согласно требованиям ТНПА, помещение должно быть обесточено. Это в свою очередь будет обеспечивать беспрепятственный проход людей в случае экстренной ситуации автоматически.

В качестве устройства обработки сигналов был выбран микроконтроллер фирмы Atmel ATmega8L, обладающий 8 килобайтами флэш памяти (ROM), 1 килобайтом оперативной памяти (RAM) и 512 байтами энергонезависимой памяти (EEPROM). Данный микроконтроллер построен на основе фирменной 8-разрядной архитектуры AVR, имеющей производительность 1 млн операций (MIPS) в секунду при частоте 1 МГц. Подобная производительность достигается за счет гибкого набора из 130 инструкций, большинство которых выполняется за один тактовый цикл.

К данному микроконтроллеру подключены следующие функциональные цепи: цепь считывания RFID-меток, цепь обмена данными с АРМ пункта охраны по интерфейсу RS-485, цепь коммутации токовой нагрузки исполнительных устройств, 12-клавишная цифровая клавиатура, цепь питания, устройство звуковой сигнализации.

Цепь питания представлена линейным регулятором LM78L05, который обеспечивает стабилизированное напряжение питания 5 Вольт. Подключение данного преобразователя выполнено согласно документации на него, с использованием фильтрующих конденсаторов для подавления ВЧ-помех. В

целом же предполагается питание всего модуля и исполнительных устройств (электромагнитных замков) от напряжения 12 Вольт.

Эргономическое проектирование для данного устройства, в первую очередь, будет заключаться в установке требований к АРМ пункта охраны, представленного ЭВМ.

Разработка программного обеспечения для используемого в проекте микроконтроллера ATmega8L велась в среде разработки CodeVision AVR, с использованием языка Си. Далее в таблицу 1 сведены все основные функции, используемые в данной программе:

Таблица 1 – Перечень использованных функций

Название функции	**Описание**
main()	Основная функция, с которой начинается выполнение всего.
hex2Ascii()	Функция преобразования полученных бинарных данных о серийном номере метки в строковую переменную.
init_PWM()	Функция инициализации ШИМ-модулятора, который необходим для генерации синусоиды 125 кГц.
readTagSerialNumber()	Функция чтения 32-битного номера EM-Marin метки.
uart_init()	Функция инициализации UART, предназначенного для связи с АРМ пункта охраны через физический уровень интерфейса RS-485.
uart_putc()	Функция отправки символа по UART
uart_puts()	Функция отправки строки по UART
delay_ms()	Функция временной задержки в милисекундах.
delay_us()	Функция временной задержки в микросекундах.
sei()	Функция разрешения глобальных прерываний.
cli()	Функция запрета глобальных прерываний.
ultoa()	Стандартная библиотечная функция перевода битовой последовательности в ASCII символы
detect_keyboard()	Функция, осуществляющая контроль ввода пароля

ЗАКЛЮЧЕНИЕ

В рамках диссертации были рассмотрены СКУД в составе которых используется RFID технология, было успешно спроектирован и разработан макет программно-аппаратного средства для управления контролем доступа на режимный объект. Результатом работы явились: чертеж схемы электрической принципиальной с перечнем элементов, чертеж схемы электрической структурной, чертеж программного алгоритма. Программный алгоритм был реализован с использованием синтаксиса языка программирования Си в среде CodeVisionAVR, также был собран рабочий прототип считывателя RFID меток, произведенных по технологии EM-Marin. Цель диссертации достигнута, программно-аппаратное средство реализовывает поставленные задачи. Спроектированное устройство обладает повышенными характеристиками безопасности авторизации и внутреннего схемотехнического устройства.

Доклад по теме магистерской диссертации был изложен на 52-ой научной конференции аспирантов, магистрантов и студентов БГУИР.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1-А] Лавров И.В. Особенности проектирования электронного модуля обеспечения безопасности дорожного движения на наземном пешеходном переходе / И.В. Лавров, О.Ч. Ролич // 51-я научная конференция аспирантов, магистрантов и студентов БГУИР, Сб. докладов. – Мн.:БГУИР, – 2015 – С. 122.

[2-А] Лавров И.В. Особенности проектирования графических интерфейсов / И.В. Лавров, К.Д. Яшин // 51-я научная конференция аспирантов, магистрантов и студентов БГУИР, Сб. докладов. – Мн.:БГУИР, – 2015 – С. 123.

[3-А] Лавров И.В. Система управления контролем доступа / И.В. Лавров, В.В. Мазюк // 52-я научная конференция аспирантов, магистрантов и студентов БГУИР, Сб. докладов. – Мн.:БГУИР, – 2016 – С. 160.