Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2021, № 1, с.129-136.

Поступила: 03.02.2021
Окончательный вариант: 25.03.2021

УДК 004.415.2

Решение проблемы смены систем контроля и управления доступом путем создания универсального устройства

Чеверев В. А.*, Фролов Е. А., Котилевец И. Д., Иванова И. А.

*vladimch552@gmail.com
МИРЭА – Российский технологический университет, Москва, Россия

Данная работа рассматривает проблемы перехода с одной системы контроля и управления доступом (СКУД) на другую, такие как: прокладка проводов, смена программного обеспечения (ПО) при смене считывателей и отсутствие масштабируемости. Данные проблемы являются актуальными и трудно решаемыми по сей день, что приводит к большим финансовым затратам и трудностям при смене СКУД. Были рассмотрены основные составляющие системы контроля и управления доступом, а также были проанализированы достоинства и недостатки уже существующих видов СКУД. В качестве решения найденных проблем было предложено следующее:

1. создание специального ПО, которое позволит агрегировать информацию разных протоколов передачи данных;
2. создание универсальной системы, которая включается в себя преимущества автономного и сетевого СКУД.

Таким образом, представленные решения приведут к улучшению технико-экономических и эксплуатационных характеристик, а именно:

1. конвертация данных, которая отбросит необходимость прокладывать провода при переходе на новую систему;
2. использование радиоканала удешевит и ускорит монтаж данной системы;
3. высокая отказоустойчивость благодаря децентрализованной системе;
4. простая масштабируемость системы.
5. облегчение и удешевление перехода на новые системы.

Ключевые слова: *система контроля и управления доступом, программное обеспечение, децентрализованная система, информационная безопасность.*

Введение

На сегодняшний день существует множество различных производителей СКУД [1], что позволяет клиенту выбирать среди существующих наиболее подходящий для решения поставленной задачи. Производители СКУД предлагают свое ПО и контроллеры, которые

имеют разные стандарты передачи данных, что приводит к определенным проблемам, например, смена всех считывателей на новые, если новые считыватели имеют другой стандарт передачи данных, то необходимо заново прокладывать провода через весь объект, что приводит к еще одной проблеме, невозможность ПО работать с новым форматом данных. Решить эти проблемы возможно путем создания специального ПО для информационных процессов в системах контроля и управления доступом.

1. Основная часть

Система контроля и управления доступом (СКУД) – это совокупность технических средств, направленных на контроль входа и выхода в помещение с целью обеспечения безопасности и регулирования посещения определенного объекта. Основными составляющими данной системы являются [2-3]:

1) Контроллер - устройство, управляющее работой всех элементов системы.
2) Считыватель идентификаторов (от пин-кода до биометрии [4]).
3) Программное обеспечение (база данных и тд.).
4) Преграждающее устройство (турникет, электромеханический или электромагнитный замок).
5) Источник питания.
6) Идентификаторы.
7) На сегодняшний день выделяют 3 вида СКУД:
8) Автономный.
9) Централизованный (сетевой).
10) Универсальный [4-8].

Автономный СКУД - система, работающая без постоянной связи с сервером, что обеспечивает отказоустойчивость в случае неполадок на стороне сервера. Данные системы удобны для оборудования небольшие организации. Среди преимуществ таких систем можно выделить следующее:

1) Низкая цена оборудования.
11) Отсутствие необходимости прокладывания кабелей для связи с центральным пультом управления.
12) Простота настройки и программирования для малых систем.
13) Простота и высокая скорость монтажа.
14) Широкий выбор идентификаторов.

Также существуют недостатки, основным из которых является отсутствие мониторинга и прямого управления в режиме реального времени [6]. Кроме того, немаловажными являются проблемы масштабируемости и хранения данных. Проблема масштабируемости обусловлена усложнением администрирования системы при увеличении количества пропускных пунктов. Проблема хранения данных заключается в контроллерах считывания автономной системы, именно на них хранятся уникальные идентификаторы карт [10-12], чтобы в случае отсутствия связи с сервером, была возможность пропустить сотрудника.

Такой метод хранения небезопасен [13], из-за возможности извлечь идентификаторы из считывателей.

В централизованной системе контроля и управления доступом, все контроллеры соединены с компьютером, что создает централизованную систему управления. В случае сетевой системы, компьютер является точкой управления всей системой, откуда выполняются все процессы в реальном времени. Таким образом, получается двухуровневая топология [7].

Существует трехуровневая топология [7], которая представлена на рис. 1. Такая топология используется не часто, ее отличие в том, что между ПК и контроллером прохода, располагается более мощный контроллер, имеющий большие вычислительные ресурсы и управляющий несколькими простыми контроллерами прохода.

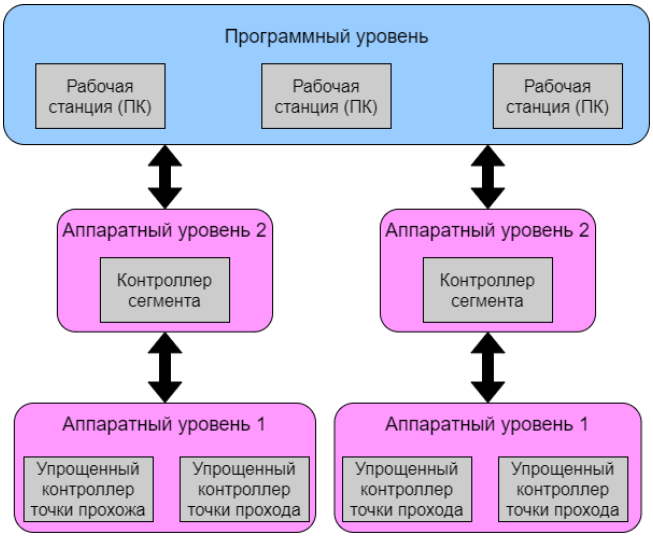

Рис. 1. Трехуровневая сетевая топология

Преимуществом такой системы является:

Централизованное управление любым компонентом системы в любое время, а при наличии *Web*-сервера, делать это можно через мобильные устройства.

2) Возможен учет рабочего времени [14-15], так как вся информация собирается на одном сервере и ее можно анализировать.
3) Возможность добавить уровни доступа.

Универсальный СКУД совмещает в себе автономные и сетевые контроллеры. Если есть связь между контроллером и управляющим компьютером, система работает как сетевая, в ином случае, если связи нет, работает как автономная.

Универсальная система в данный момент более популярна на западе, где представлены множество аналогов, но все они работают только со своей продукцией, что опять же приводит к отсутствию стандарта и проблемам при смене СКУД. Существует три варианта построения универсального СКУД:

1) Проводной онлайн.
2) Автономная точка доступа.

3) Беспроводной онлайн.

Проводной онлайн, является самым распространенным. Были рассмотрены два самых популярных производителя СКУД, а именно Perco и Parsec. В случае с Perco, в каталоге товаров отсутствует наличие беспроводных решений СКУД. Parsec в свою очередь предоставляет два варианта беспроводных СКУД, но от других производителей. Первым вариантом являются замки-личинки со встроенными считывателями карт от Aperio, вторым вариантом является беспроводной считыватель компании «Аргус-Спектр» СК-Р, который на данный момент снят с производства.

Состоит из контроллера СКУД, считывателей карт, заграждающего устройства и блока питания. Контроллер является сетевым и общение с БД [16] как правило происходит по стандарту *EtherNet/IP* [17], а не *RS-485*[18-19], который используется в большинстве автономных и сетевых СКУД.

Автономная точка доступа используется реже. Несмотря на наличие слова «автономный», как таковой эта система не является, ведь для работы в реальном времени, все еще требуется прямое подключение к серверу.

Беспроводной онлайн включается в себя точки доступа с радиомодулем [20]. Также данным модулем оснащены турникеты и электронные замки, что позволяет полностью отказаться от проводного подключения, за исключением питания.

2. Решение проблемы

Во-первых, создание универсальной системы, которая включается в себя преимущества автономного и сетевого СКУД. Такое решение будет являться универсальным, что увеличит его спрос на рынке. Топология данной СКУД будет напоминать сетевую и иметь беспроводную связь с сервером и считывателями, как показано на рис. 2. Благодаря устройствам между сервером и считывателями, в результате будет получена децентрализованная система.

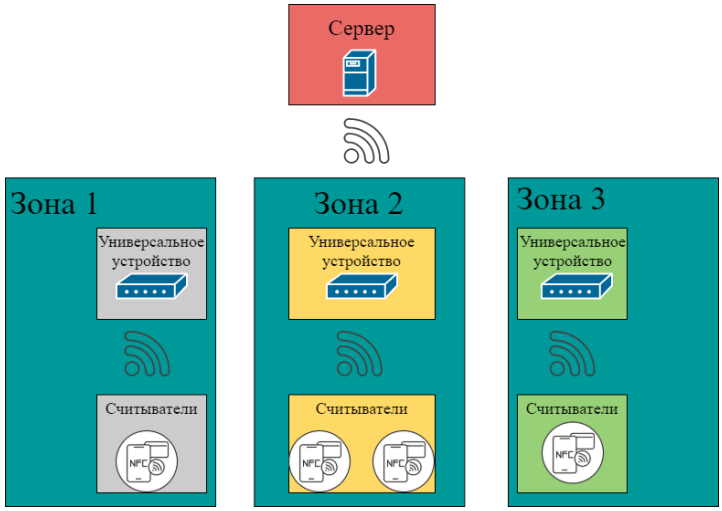

Рис. 2. Топология универсального децентрализованного СКУД

Во-вторых, создание своего контроллера управления и считывателя, позволит полностью отказаться от проводов и перейти на радиоканал, в котором одно универсальное устройство сможет управлять, более десятка считывателей. В качестве считывателя, будет использоваться RFID модуль на базе микросхемы MFRC-522. Сравнение технических характеристик промышленного считывателя и разрабатываемого, указаны в таблице 1. В качестве контроллера была разведена плата на базе модуля ESP-8266, техническое сравнение указано в таблице 2.

Таблица 1. Сравнение считывателей

	MFRC-522	промышленный считыватель
Напряжение питания	3.3V	12V
Потребление тока	13-26mA	35-40mA
Дальность считывания	6 см	3-6 см
Рабочая частота	13.56MHz	125 Hz
Интерфейс передачи данных	SPI	Wiegand-26/34/42/50, Dallas TM
Скорость передачи данных	10 Мбит/с	400бит-4Кбит/с
Рабочая температура	-20°C…+80°C	-30°C…+40°C
Рабочая влажность	Не более 95%	Не более 98%
Габариты	40x60 мм	115x45x22 мм

Таблица 2. Сравнение контроллеров

	ESP-8266	промышленный контроллер
Напряжение питания	3.3… 5V	9.9…17.8V
Потребление тока	220mA	160mA
Сетевой интерфейс	Wi-Fi 802.11 b/g/n 2,4 ГГц	Ethernet RJ45 10/100M
Тип контроллера	Сетевой	Сетевой
Поддерживаемы форматы	Em-Marine, HID	Em-Marine, HID
Кол-во подключаемых считывателей	2	4
Количество подключаемых замков	2	4
Управление устройствами	электронный замок, турникет, шлагбаум, ворота	электронный замок, турникет, шлагбаум, ворота
Рабочая температура	-40°C…+125°C	0°C…+40°C

Рабочая влажность	Не более 95%	Не более 85%
Габариты	47x25 мм	240x260x57 мм

В-третьих, возможно использование считывателей других производителей, в таком случае подключение к контроллеру будет проводное и лимит подключенных считывателей не будет превышать десяти штук. Для работы с такими считывателями используется программные конвертеры, что позволит принимать данные по одному стандарту, а передавать уже по-другому. Сам контроллер всегда общается с сервером по беспроводной связи, в случае потери соединения с сервером, у контроллера имеется модуль памяти меток.

В-четвертых, разработка специального ПО позволит агрегировать данные с разных интерфейсов, что приведет к хранению данных одного формата на сервере.

В-пятых, не мало важным фактором разрабатываемой системы является безопасность. Рассмотрим способы передачи данных в СКУД:

- wiegand;
- rs-485;
- ethernet;
- Wi-Fi.

С помощью разных программных обеспечений и аппаратных решений можно получить данные до того, как они дойду до точки назначения. Например, последовательно подключив к wiegand BLEKey, можно сэмулировать раннее приложенную карту. Rs-485 можно прослушать с помощью обычного конвертера rs-485 в rs-232. Схема подключения будет последовательной. Ethernet можно перехватить, использовав атаку «человек посередине» (MITM) и анализатор трафика по типу SpyNet. Также ни один из интерфейсов не имеет шифрования. Единственным фактором защиты данных интерфейсов является физическая, т.е. защищенность стеной. Что касается беспроводной технологии, то данные передаются на сервер по HTTPS, используя POST запросы. На сервере, полученный идентификатор кэшируется и записывается в базу данных (БД), если злоумышленник получит доступ к БД, то не сможет воспользоваться полученной информацией.

Достоинства данного решения:

Конвертация данных, которая отбросит необходимость прокладывать провода при переходе на новую систему;

1) Использование радиоканала удешевит и ускорит монтаж данной системы;
2) Высокая отказоустойчивость благодаря децентрализованной системе;
3) Простая масштабируемость системы;
4) Облегчение и удешевление перехода на новые системы;
5) Высокая степень защищенности.

Заключение

Система контроля и управления доступом развивается и по сей день, появляются множество различных решений, которые позволяют обеспечить более надежную защиту.

Недостатки в таких системах существуют, но их стараются устранять обновлением ПО и использованием новых многофункциональных устройств. Представленные в данной статье решения, являются одними из вариаций универсальной системы, которые должны помочь исправить проблемы СКУД.

Список литературы

1. Ширяев Н.А. Водолажская Ю.В. Российский рынок систем контроля и управления доступом // *Охрана, безопасность, связь.* 2017. №1-2, с. 126-131.
2. Сивухин В.М. Исаков И.М. О современных системах защиты от несанкционированного доступа и перспективах их развития // *Научный журнал.* 2020, №8, с. 4-6.
3. Иванов П.Д. Суверина И.Д. Анализ состояния и перспективы развития систем контроля и управления доступом в России // *Инженерный журнал: наука и инновации.* 2014. №10, с. 1-11.
4. ГОСТ Р 51241-2008. *Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний*. Введ. 2009-09-01. М.: Стандартинформ, 2008.
5. Зелевич Е.П. Технологии современных систем контроля и управления доступом // *T-Comm: Телекоммуникации и транспорт.* 2009, №1, с. 26-29.
6. Болдырев А.Г.. Автономные системы контроля доступа: вчера, сегодня, завтра [Электронный ресурс] URL:http://secuteck.ru/articles2/sys_ogr_dost/avtonomnye-sistemy-kontrolya-dostupavcherasegodnya-zavtra (Дата обращения: 28.11.2020).
7. Стасенко Л. Сетевые СКУД Преимущества и перспективы [Электронный ресурс] URL: http://lib.secuteck.ru/articles2/sys_ogr_dost/setevye-skud-preimuschestva-i-perspektivy (Дата обращения: 28.11.2020).
8. Катренко А. Комбинированные СКУД [Электронный ресурс] URL: http://secuteck.ru/articles2/sys_ogr_dost/kombinirovannye-skud-pervyy-yubiley (Дата обращения: 28.11.2020).
9. Ворона В. А. Тихонов В. А. *Системы контроля и управления доступом*. М: Горячая линия - Телеком, 2010.
10. Багдасарян А.С., Бутенко В.В., Кащенко Г.А., Семенов Р.В. Применение радиочастотной идентификации в системах контроля и управления доступом к критически важным объектам // *Труды научно-исследовательского института радио.* 2010, №3, с. 53-59.
11. Грибова В.В. Использование смарт-карт в системе контроля и управления доступом (СКУД) // *Евразийский научный журнал.*2017, №4, с. 225-226.
12. Фаткулин А.Н. Окладникова Е.Н. Сухарев Е.Н. Анализ современных систем контроля и управления доступом // *Актуальные проблемы авиации и космонавтики.* 2011, №7, с. 263-264.

13. Оладько В.С. Риски систем управления и контроля доступа // *Молодой ученый*. 2016, №28, с. 133-136.
14. Романов Е.Л. Архитектура системы учета рабочего времени, совмещенной со СКУД // *Динамика систем, механизмов и машин.* 2016, №2, с. 291-293.
15. Козлов А.Е. Система контроля и управления доступом на предприятие: понятие, характеристика и основные требования // *Вестник Воронежского государственного технического университета.* 2019, №15, с. 42-47.
16. Когельман Л.Г., Артозей Е.А. Модель системы защиты информации. Система контроля управления доступом // *Современные информационные технологии*. 2016, № 23, с. 94-98.
17. EtherNet/IP [Электронный ресурс] URL: https://www.eskovostok.ru/catalog/communication/ethernet_ip (Дата обращения: 29.11.2020).
18. Топология СКУД [Электронный ресурс] URL: https://www.parsec.ru/products/parsecnetoffice-topology/ (Дата обращения: 30.11.2020).
19. Максимов Р.Л., Рафиков А.Г. Разработка автоматической скуд повышенной безопасности на базе типового решения скуд BioSmart с использованием автоматного подхода // *Вопросы кибербезопасности.* 2015, № 5, с. 73-80.
20. Пасиков Е.Г. Мурыгин А.В. Анализ возможностей применения беспроводных технологий в профессиональных системах контроля и управления доступом // *Актуальные проблемы авиации и космонавтики.* 2011. №7, с. 402-403.