

Содержание

Введение	2
1 Техническое задание	3
2 Теоретические основы	4
2.1 История развития СКУД	4
2.1.1 Первое поколение	4
2.1.2 Второе поколение	5
2.1.3 Третье поколение	6
2.2 Основные составляющие СКУД	7
2.2.1 Контроллер	7
2.2.2 Считыватель	8
2.2.3 Программное обеспечение	9
2.3 Виды СКУД	10
3 Обзор и анализ существующих решений	12
4 Выбор и обоснование предложенного решения	13
5 Реализация технического задания	14
6 Экономическая часть	15
7 Охрана труда и экология	16
Заключение	17
Список литературы	18

					Код специальности									
Изм.	Лист	№ докум.	Подп.	Дата	Тема									
Разраб.	Имя автора											Лит.	Лист	Листов
Провер.	Имя проверяющего											1	18	
Реценз.										Группа				
Н. Контр.														
Утверд.														

Введение

Система контроля и управления доступом (далее СКУД) - это совокупность программных и аппаратных средств, предоставляющая возможность управления пропускным режимом, с целью ограничить доступ к определённым территориям или помещениям лицам, не имеющим к ним разрешения. Подобные системы широко используются среди не только крупных организаций и предприятий, но и малого бизнеса, индивидуальных предпринимателей. Причинами такого успеха являются:

- централизованное управление пропускным режимом на объекты;
- сокращение времени на проверку документов;
- упрощение ведения статистики.

Для обеспечения контроля доступа в больших предприятий существует большое количество решений на рынке, однако для малых помещений с соответственно пониженной ценой наблюдается недостаток предложений. Именно поэтому, до сегодняшнего дня, малые организации используют простые замки или, к примеру, домофоны. Такие устройства значительно снижают удобство и быстроту доступа к определенным объектам.

Решением данной проблемы является разработка собственной СКУД, что определяет цель дипломного проекта. Для достижения данной цели должны быть решены следующие задачи:

- изучение теории по системам СКУД;
- анализ существующих решений на рынке, выявление их основных возможностей и недостатков;
- изучение теории по методам идентификации пользователей;
- выбор программных и аппаратных инструментов для разработки системы СКУД.

Структура работы включает в себя ...

					Код специальности	Лист
						2
Изм.	Лист	№ докум.	Подп.	Дата		

1. Техническое задание

Требования к работе разрабатываемой системы контроля доступа

					Код специальности	Лист
						3
Изм.	Лист	№ докум.	Подп.	Дата		

2. Теоретические основы

СКУД - система контроля и управления доступом. В более широком смысле это совокупность программных и аппаратных средств технической защиты, цель которых - ограничение и отслеживание событий входа/выхода на определенной территории.

2.1. История развития СКУД

История СКУД начинается в связи с потребностью введения контроля над доступом людей на ограниченные территории, заменив старые, неактуальные способы контроля на автоматизированные и удобные в управлении системы. Структурная схема первых систем (на сегодняшний день также используются):

- считыватель (программно-аппаратное устройство, которое принимает коды от внешних устройств);
- валидатор (логический блок, предназначенный для проверки кода на его соответствие);
- реле (программный или аппаратный модуль, предназначенный для управления устройствами блокировки прохода).

2.1.1. Первое поколение

СКУД первого поколения выполняли лишь базовые функции: считыватель ключей получал определенный код, передавал его в валидатор, далее валидатор проверял код на соответствие и принимал решение о открытии/закрытии блокирующего устройства.

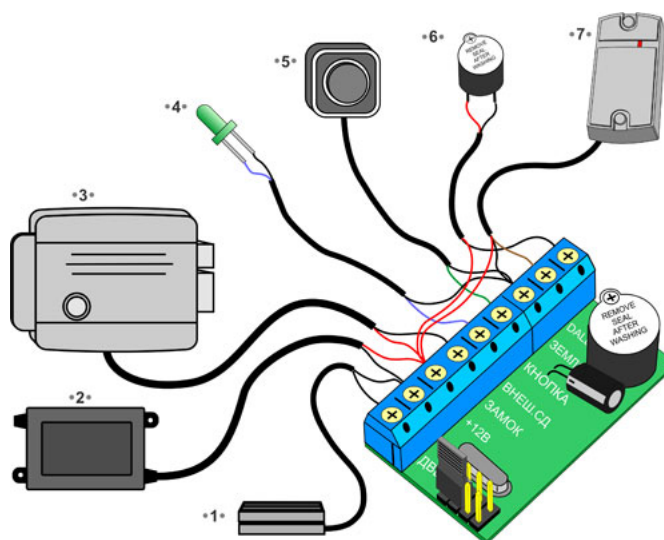


Рисунок 1 – пример простого СКУД – Z-5R

В качестве устройств содержащих в себе ключ доступа широко использовалась TouchMemory – устройства, имеющие однопроводный протокол обмена информацией и флеш-память для её хранения.



Рисунок 2 – элеткронный ключ Button.com, реализующий систему TouchMemory

Подобные устройства хоть и не отличались большой функциональностью, внесли в развитие СКУД несколько нововведений:

- отказ от линий связи, что привело к использованию паллиативных механизмов программирования;
- внедрение протокола MicroLan, на основе которого позже будет создано множество охранных и пожарных систем.

Несмотря на все достоинства, СКУД первого поколения не отвечали еще нескольким основным требованиям – ведению журнала событий и простоте программирования контроллеров.

2.1.2. Второе поколение

Опыт использования первых СКУД показал, что они востребованы, однако пользователи нуждаются в увеличении функциональности и безопасности.

В связи с увеличением мощности микроконтроллеров, а также появлением доступа к технологиям Ethernet. Из этого исходят следующие нововведения:

- появились журналы событий. Они не работали в реальном времени, но значительно повышали безопасность охраняемых объектов;
- контроллеры стали способны сами получать и передавать данные для обработки, без необходимости в управляющих командах;
- на платах СКУД предусматривался канал связи Ethernet. Отныне локальные сети стали ключевыми линиями связи.

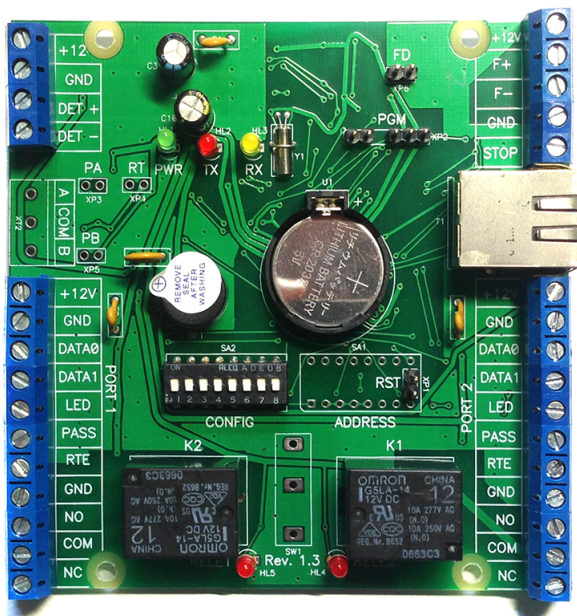


Рисунок 3 – Сетевая СКУД Sigur – поддерживает работу по сети за счет встроенного Ethernet порта

В процессе использования СКУД нового поколения, были выявлены следующие недостатки:

- журналы событий не работали в реальном времени. Такая функция позволила бы незамедлительно реагировать на определенные события;
- не было поддержки более сложных алгоритмов валидации ключей, соответственно безопасность нельзя было повысить;
- не поддерживались разные виды идентификаторов, такие как штрих-коды, отпечатки пальцев и т.п.

2.1.3. Третье поколение

Применение локальных сетей ускорило развитие СКУД. Ранее совмещенные элементы систем контроля и управления доступом стали разделяться, образуя распределенные системы. Это означало, что стало возможным располагать на разные объекты считыватели, подключённые к одному контроллеру СКУД.

Также, чаще роль контроллера СКУД стал выполнять персональный компьютер, с установленным управляющим программным обеспечением. Такая структура позволила:

- наделить системы СКУД гибкостью, возможностью использования различного ПО, выбираемого по требуемым характеристикам;

- использовать любые поддерживаемые методы идентификации – от простых TouchMemory до биометрии.

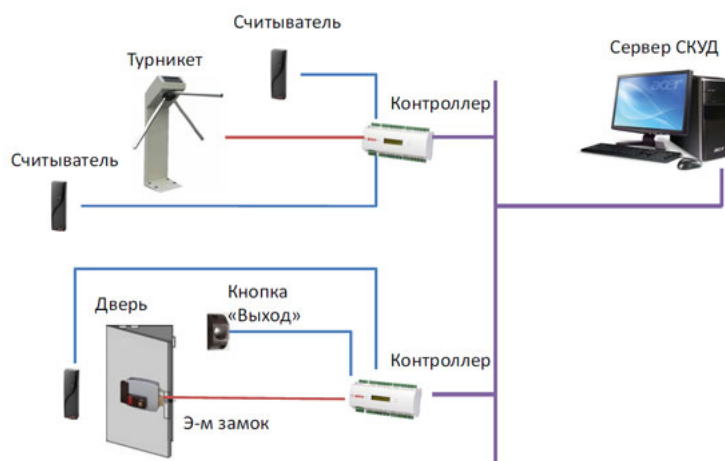


Рисунок 4 – структурная схема СКУД третьего поколения

Третье поколение СКУД вследствие больших нововведений получила и ряд нерешённых проблем:

- все элементы системы теперь зависели от одного-двух серверов, на которых выполнялось управляющее программное обеспечение;
- за счёт большого числа новых методов идентификации появилось множество проблем с безопасностью. Такая ситуация подтолкнула производителей к использованию и разработке новых протоколов обмена информацией между устройствами.

2.2. Основные составляющие СКУД

2.2.1. Контроллер

В современных системах контроля и управления доступом контроллер - одна из самых функциональных модулей. Он выполняет роль центрального модуля управления – в его памяти хранятся коды идентификаторов, а значит контроллер принимает решение о допуске определённого человека на охраняемый объект.

В случае необходимости автономного контроллера, он совмещается со считывателем в одном устройстве, что позволяет сократить затраты, снизить стоимость и упростить монтаж.

При использовании СКУД на несколько точек доступа, ощутимо возрастает значимость характеристик.



Рисунок 5 – пример контролеров – автономный Z-5R (слева), Anviz SAC844 (слева)

2.2.2. Считыватель

Считыватель - устройство, которое получает код идентификатора и передаёт его в контроллер для обработки. Считыватели, в зависимости от модели, позволяют принимать в качестве идентификатора следующие идентификаторы:

- proximity-карты;
- TouchMemory;
- код доступа;
- биометрия (отпечатки пальцев, радужная оболочка глаз, лица).



Рисунок 6 – считыватели Smartec

2.2.3. Программное обеспечение

В случае использования компьютера в качестве контроллера, существует специальное программное обеспечение, роль которого – управление подключёнными модулями и хранение идентификаторов.

Программное обеспечение используется при необходимости более широкого функционала, чем может предоставить обычный контроллер, например:

- ведение отчётности, быстрый доступ к отчётам;
- подключение баз данных сотрудников, например в 1С;
- удалённое управление, изменение баз данных, конфигураций.

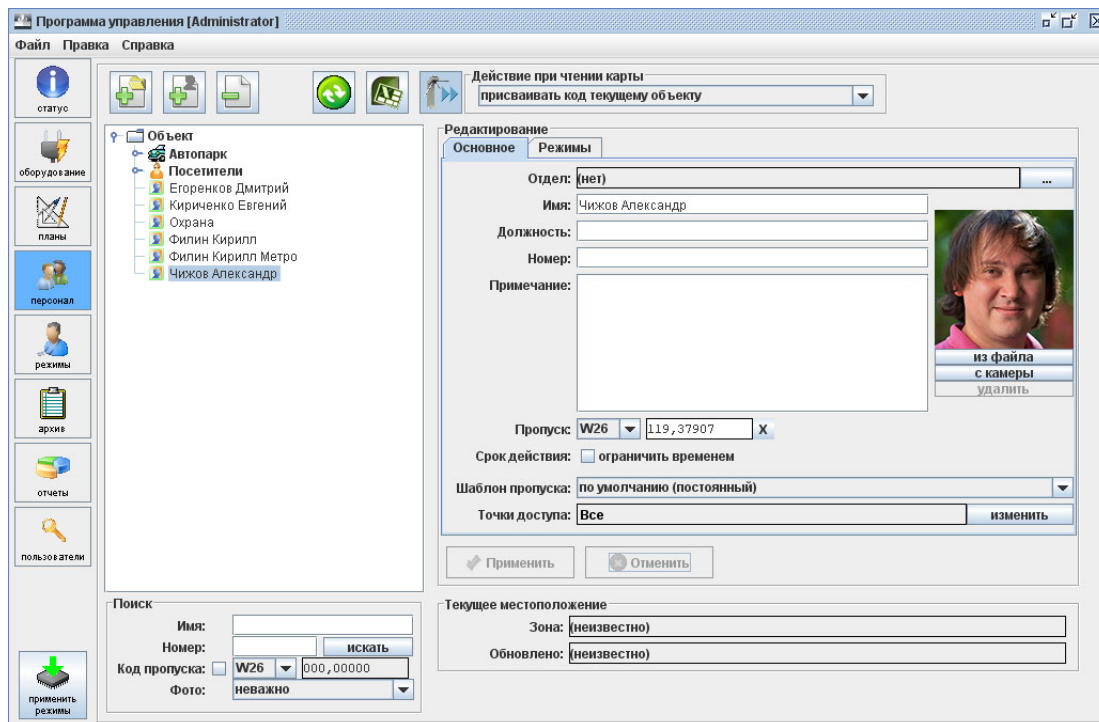


Рисунок 7 – программное обеспечение Castle

2.3. Виды СКУД

Все системы контроля и управления доступом можно разделить на две категории: сетевые и автономные системы.

В сетевой системе все контроллеры соединены с компьютером, что позволяет управлять десятками дверей, проходных пунктов, турникетов. Подобные системы удобны для больших объектов (офисов, производственных предприятий).

Сетевые системы используются для:

- использования сложных алгоритмов допуска сотрудников с разными привилегиями в разные зоны объекта;
- организации учёта рабочего времени;
- при взаимодействии с другими системами безопасности, например с пожарной сигнализацией.

В сетевой СКУД могут применяться как проводные, так и беспроводные методы передачи данных, например:

- Bluetooth;
- Wi-Fi;
- GSM.

Автономные системы менее функциональны, дешевле, проще в эксплуатации. Они не требуют прокладки сотен метров кабеля, а также сопряжения и управления с компьютера. При этом, автономные системы могут иметь некоторый функционал сетевых СКУД, например, ведение отчётов, удалённое управление, но должны обеспечивать безопасность хранения информации, т.к. все идентификаторы располагаются непосредственно в автономной системе.

					Код специальности	Лист
						11
Изм.	Лист	№ докум.	Подп.	Дата		

3. Обзор и анализ существующих решений

Тут существующие решения в:

- 3.1 системах СКУД
- 3.2 ПО для распознавания лиц

					Код специальности	Лист
						12
Изм.	Лист	№ докум.	Подп.	Дата		

4. Выбор и обоснование предложенного решения

Тут выбор и обоснование:

- 4.1 аппаратной платформы
- 4.2 языка программирования
- ...

					Код специальности	Лист
						13
Изм.	Лист	№ докум.	Подп.	Дата		

5. Реализация технического задания

Тут описание проведённой работы:

– ...

					Код специальности	Лист
						14
Изм.	Лист	№ докум.	Подп.	Дата		

6. Экономическая часть

- 6.1 расчет себестоимости
- 6.2 оценка эффективности внедрения

					Код специальности	Лист
Изм.	Лист	№ докум.	Подп.	Дата		15

7. Охрана труда и экология

Нужно ли это делать?

- 7.1 вредные факторы
- 7.2 правила техники безопасности
- 7.3 противопожарная безопасность

					Код специальности	Лист
						16
Изм.	Лист	№ докум.	Подп.	Дата		

Заключение

					Код специальности	Лист
Изм.	Лист	№ докум.	Подп.	Дата		17

Список литературы