Содержание

Введение

1. Автономные контроллеры

2. Сетевые контроллеры

3. Распределенные СКУД

4. Контроллеры СКУД iSecure Pro

Выводы

Литература

Введение

Тема реферата "Контроллеры систем контроля управления доступом".

Контроллеры - интеллектуальный элемент системы контроля управления доступом (СКУД), подразделяют на автономные, сетевые и интегрированные. Контроллеров в системе может быть несколько, а в больших системах они еще и многоуровневые. Контроллеры низкого уровня устанавливаются обычно вблизи считывателя и с задачей справляются сами, если же встречают незнакомую карту, запрашивают контроллер более высокого уровня, который их координирует. В более сложных случаях запрос идет на центральный компьютер, хранящий всю базу данных. В минимальном варианте контроллер может быть встроен в корпус считывателя. Иногда все проблемы ложатся на стандартный компьютер. Хорошие контроллеры обязательно поддерживают режим связи с удаленным компьютером по телефонной линии. Это позволяет централизованно координировать базу данных во всех филиалах одной организации, и, кроме того, иметь оперативные рапорты обо всех нештатных ситуациях.

Цель написания реферата – ознакомится с автономными, сетевыми и интегрированными СКУД, рассмотреть достоинства и недостатки различных систем.

1. Автономные контроллеры

Автономные (локальные) СКУД, управляемые микрокомпьютером, как правило, обслуживают один КПП (возможно, с несколькими линейками прохода и соответственно контрольными терминалами). Идентификационная информация о пользователях и их полномочиях хранится в локальной базе данных. СКУД такого типа наиболее просты по конфигурации, но и наименее надежны с точки зрения возможности вывода их из строя. Они могут применяться в основном на тех объектах, где не требуется высокий уровень безопасности. Часто в литературе такие системы носят название однодверных. На рис. 1 приведена типовая схема построения такой системы.

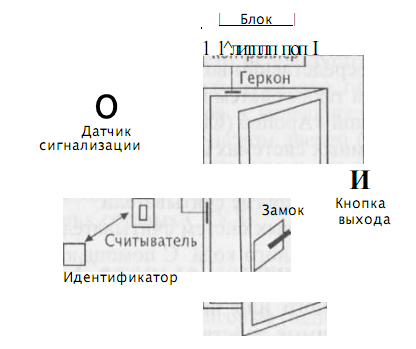


Рис. 1. Схема системы с разделенным контроллером и считывателями

Чаще всего к контроллеру можно подключить до двух считывателей, которые устанавливаются на две двери или на одну для контроля входа и выхода. Один из считывателей можно заменить на клавиатуру для набора кода.

Кроме этого, система позволяет подключать электрозамки, кнопки выхода, герконы, ИК-датчики, сирену и др.

Существуют однодверные системы, аналогичные описанной выше, но в них считыватель и контроллер объединены в один корпус (рис. 2), т. е. блок, принимающий решение об открытии замка, находится в считывающем модуле. Это, с одной стороны, удешевляет систему, но с другой - уменьшает функциональные возможности, а главное - увеличивает вероятность взлома корпуса считывателя и замыкание контактов, к которым подключен замок.

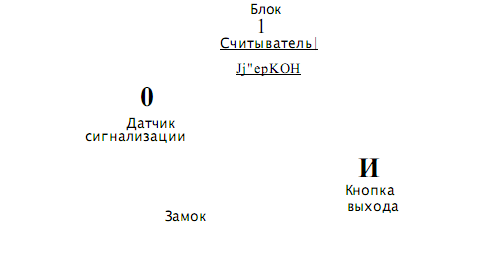


Рис. 2. Схема системы с совмещенным контроллером и считывателем

В еще более дешевых системах совмещаются в одном корпусе принимающий решение блок, клавиатура для набора кода, считыватель и замок. Наибольшее распространение такие системы получили в гостиницах. На объектах с требованиями повышенной безопасности применяются контроллеры с цифровым управлением реле замка. Выносной модуль реле замка монтируется непосредственно возле замка и управляется особым цифровым кодом. Примером таких систем являются СКУД на основе контроллеров, предлагаемых фирмой "Apollo" (США). Чаще всего в автономных системах используются считыватели магнитных карт "тач-мемори" и проксимити, гораздо реже - биометрические средства, индентифкаторы Виганда или другие считыватели. Но в большинстве автономных систем считыватели совмещены с клавиатурой для набора индивидуального кода. С помощью клавиатуры осуществляется программирование систем. Системы на основе одного или нескольких автономных контроллеров осуществляют все необходимые действия, присущие СКУД, автономно (без использования управляющего компьютера). Контроллеры в таких системах обязаны иметь собственный буфер памяти номеров карт (идентификаторов) и происходящих в системе событий. Обычно они имеют выход на локальный принтер для распечатки протокола событий. Программируются указанные контроллеры, как правило, с каких-либо кнопочных панелей или с помощью мастер-карт, позволяющих заносить в память контроллера новые карты и удалять старые. Один контроллер в таких системах обычно управляет доступом в одну (максимум - две) двери. В качестве идентификаторов (электронных пропусков) в таких системах могут применяться: магнитные карты, электронные "таблетки" - "i Button", радиочастотные PROX-карты и др. Все устройства управления дверями и охранными шлейфами (реле управления замком, входы для подключения датчика двери, кнопки выхода и охранных датчиков) располагаются в автономных системах обычно на плате самого контроллера. Часто сам контроллер конструктивно объединяется в одном корпусе со считывателем. Наиболее простые автономные системы (часто называемые - "гостиничными") вообще объединяют в одном корпусе контроллер принятия решений, считыватель/клавиатуру и электрозамок. Следует, однако, отметить, что данная мера, позволяющая снизить себестоимость системы, может привести к снижению безопасности, увеличивая вероятность взлома системы. В целях повышения безопасности в наиболее совершенных автономных системах применяется вынесенное цифровое реле управления замком. Данная мера позволяет предотвратить попытки проникновения в помещение путем прямого подключения электрозамка к проводам питания.

В некоторых системах предусмотрена возможность расширения. Достигается это различными способами:

- за счет объединения отдельных контроллеров в сеть (использование добавочного сетевого модуля в дополнение к контроллеру);

- путем увеличения мощности и усложнения самого контроллера, что позволяет подключать к нему более двух считывателей.

В обоих случаях для связи контроллеров между собой или с периферийными исполнительными модулями часто используется какой-либо стандартный интерфейс, например RS-485. Следует, однако, помнить, что программировать приходится каждый контроллер в отдельности (несмотря на обмен данными между ними). Для систем с числом дверей более трех данный процесс может оказаться весьма утомительным и трудоемким (особенно при большом числе пользователей). В этом случае более предпочтительным является установка простейших сетевых СКУД.

2. Сетевые контроллеры

Сети контроллеров бывают одноранговые (одноуровневые) и многоранговые (многоуровневые), где число уровней редко превышает два.

В одноранговой сети имеется единственная шина (она может удлиняться за счет повторителей или разветвителей). В одноранговой сети все ее узлы (контроллеры доступа) имеют равные права (рис. 3). Среди представителей этого семейства - системы Northern Computers, Kantech, Parsec и большинство других систем, в том числе и российского производства.



Рис. 3. Одноранговая сеть

Недостатки одноранговой сети:

- необходимость иметь в каждом контроллере полную базу данных (список пользователей, их прав и т. д.);

- невозможность реализации некоторых глобальных функций, требующих взаимосвязанной работы нескольких контроллеров (например, глобальный "антипассбэк" - запрет повторного прохода). Этот недостаток имеет место только в сетях, где компьютер является ведущим, т. е. обмен информацией происходит только по его инициативе. Если сеть контроллеров работает на принципе произвольного доступа, недостаток отсутствует.

Достоинства, максимальная "живучесть" сети, поскольку каждый контроллер имеет все необходимое для автономной работы при выключенном компьютере или повреждении сети. Для систем безопасности это является существенным фактором. В многоранговой сети контроллеров имеется ведущий, или мастер-контроллер, который координирует работу "ведомых" контроллеров, реально управляющих одной или несколькими точками прохода. Самый известный в России представитель - система Apollo. Такие системы имеют как достоинства, так и недостатки.



Рис. 4. Многоранговая сеть

Недостатки многоранговой сети:

- нарушение работы системы при повреждении связи между мастер-котроллером и ведомыми контроллерами, поскольку значительная часть информации и алгоритмов являются, прерогативой мастер-контроллера;

- удорожание небольших систем за счет высокой стоимости мастер-контроллера (из-за его явной избыточности).

Достоинства многоранговой сети:

- централизованная память для баз данных, что сегодня не очень существенно;

- реализация всех функций даже при выключении компьютера;

- выигрыш в стоимости одной точки прохода при средних и больших размерах системы.

Оценивая общую топологию, необходимо отметить, что сегменты сети могут существовать в рамках системы в единственном экземпляре (см. рис. 3, 4), либо таких сегментов может быть много (рис. 5), т. е. оборудование СКУД может подключаться не к единственному ПК, а к любому из ПК, объединенных, в свою очередь, в компьютерную сеть. Вариант, показанный на рис. 5, позволяет строить сети любого масштаба (при наличии компьютерной сети между рабочими станциями). Далеко не все системы обеспечивают подключение оборудования к любому из ПК в сети.

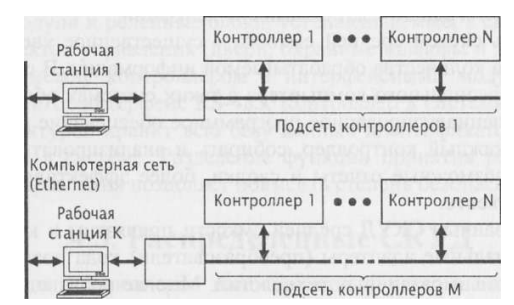


Рис. 5. Полная схема сети СКУД

Сетевые (централизованные) СКУД находятся под непосредственным и постоянным управлением центрального компьютера системы охраны объекта, обслуживающего все периферийные звенья КПП (рис. 6). База данных централизована. Применение таких систем экономически оправдано, лишь когда к центральному компьютеру подключено достаточно большое число терминалов - от нескольких десятков и более. Преимущество таких систем в том, что они в отличие от автономных позволяют вести централизованную регистрацию времени прохода служащих и осуществлять статистическую машинную обработку этих сведений, а также оперативно вводить все необходимые изменения в режимы доступа тех или иных лиц или в целом на объект.

Сетевые СКУД способны обеспечить высокий уровень безопасности объекта. Для повышения надежности функционирования системы может быть применена параллельная обработка данных на двух ПЭВМ.

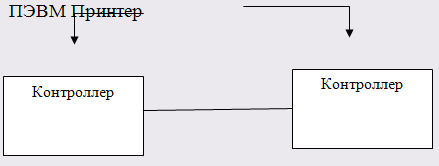


Рис. 6. Схема централизованной СКУД

Число контроллеров зависит от емкости системы и максимального числа считывателей, обслуживаемых одним контроллером. Обычно для увеличения эффективности работы и уменьшения стоимости всей системы безопасности объекта централизованные СКУД позволяют осуществлять интеграцию с датчиками сигнализации. Особенность систем средней емкости - существенное увеличение числа пользователей и количества обрабатываемой информации. В связи с этим использование персонального компьютера в таких системах обязательно. Компьютер и его специализированное программное обеспечение позволяют программировать каждый контроллер, собирать и анализировать информацию, составлять всевозможные отчеты и сводки, более эффективно отслеживать ситуацию на объекте. Централизованные СКУД средней емкости привязаны к конкретной технологии. Специальные адаптеры (преобразователи) кода позволяют подсоединить считыватели различных технологий. Многие производители даже заявляют о том, что их система интегрируется с любым считывателем. Но, как правило, либо это утверждение недостаточно обосновано, либо требует серьезных дополнительных затрат на установку новых модулей.

Главная особенность таких СКУД в том, что они имеют возможность конфигурирования аппаратуры и управления процессом доступа с компьютерных терминалов (терминала). Различные СКУД имеют свои индивидуальные особенности и различаются по архитектуре, возможностям, масштабу (предельному числу считывателей/дверей), числу управляющих компьютеров, типу применяемых считывателей, степени устойчивости к взлому, степени устойчивости к электромагнитным воздействиям.

В соответствии с указанными параметрами производится разделение сетевых СКУД на 3 основных класса по ГОСТ Р 51241-98. Большинство сетевых СКУД сохраняют многие достоинства автономных систем, основное из которых - работа без использования управляющего компьютера. Это означает, что при выключении управляющего компьютера система фактически превращается в автономную. Контроллеры данных систем так же, как и автономные контроллеры, имеют собственный буфер памяти номеров карт пользователей и событий, происходящих в системе. Наличие в системе компьютера позволяет службе безопасности оперативно вмешиваться в процесс доступа и осуществлять управление системой в режиме реального времени. Важнейшим элементом сетевых СКУД является программное обеспечение (ПО). Оно отличается большим разнообразием как по возможностям - от относительно простых программ для одного управляющего терминала, позволяющих добавлять в базу данных новых пользователей и убирать выбывших, до сложнейших программ с архитектурой клиент-сервер. В системах данного класса используются мощные центральные контроллеры, осуществляющие процесс управления большим числом периферийных исполнительных устройств. Например, один контроллер AAN-100 компании Apollo может управлять процессом доступа в 96 дверей. Как правило, контроллеры в таких системах являются чисто электронными устройствами и не содержат релейных выходов. В таких системах функции управления внешними устройствами и охранными шлейфами обычно выполняют внешние интерфейсные модули и релейные блоки, устанавливаемые, в свою очередь, недалеко от объектов управления (двери, охранные шлейфы и др.). Для обмена информацией между контроллером и интерфейсными модулями наиболее часто используется интерфейс RS-485. Контроллер в системах с централизованной архитектурой хранит всю базу данных идентификаторов и событий, произошедших в системе. Разделение функции принятия решений и непосредственно управления позволяет повысить степень безопасности СКУД.

3. Распределенные СКУД

Возможности контроллеров наиболее полно раскрываются в распределенных СКУД. Распределенные СКУД наиболее совершенны с точки зрения организации процесса обработки информации в системе, так как наилучшим образом противостоят сбойным и аварийным ситуациям, в частности, при сбоях в работе центрального ПК, нарушении целостности проводной линии, связывающей его с периферией и т. п. Периферийные пункты оснащены локальными сетями на базе микрокомпьютеров (контроллеров), которые выполняют процедуру проверки самостоятельно, а центральный компьютер включается в работу лишь для актуализации локальных баз данных и статистической и логической обработки информации. На рис. 7 показана схема разветвленной сети СКУД. Отличительная особенность СКУД с распределенной архитектурой состоит в том, что база данных идентификаторов (и событий в системе) содержится не в одном, а в нескольких контроллерах, которые, как правило, сами выполняют функции управления внешними устройствами и охранными шлейфами через реле и входы охранной сигнализации, расположенные непосредственно на плате самого контроллера. Еще одна отличительная особенность системы такого класса - возможность связи входных и выходных устройств разных контроллеров системы. Например, можно запрограммировать систему так, чтобы срабатывание датчика сигнализации у входа в офис, вызывало блокирование электрозамков, подключенных к нескольким контроллерам, контролирующим близлежащие помещения.

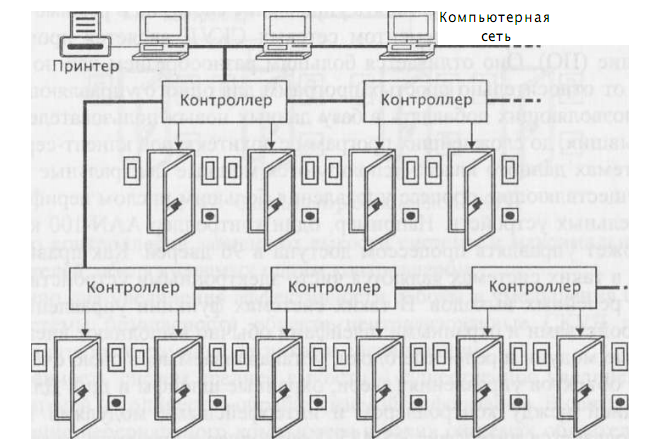


Рис. 7. Схема разветвленной сети СКУД

Кроме того, программное обеспечение больших систем позволяет использовать для управления сразу несколько компьютеров и осуществлять распределение исполнительных функций между ними. Например, можно на компьютер администратора возложить обязанности отслеживать местонахождение сотрудников и использование ими рабочего времени; оператору компьютера отдела кадров вменить в обязанность пополнять базу данных, печатать пропуска; на проходную установить компьютер с программами, помогающими идентифицировать личность, а на пост охраны - выводить тревожную графику и т. д. Большие системы, как правило, работают в самом тесном взаимодействии с другими инженерными системами объекта: охранной сигнализацией, с системами телевизионного наблюдения и контроля, с системами жизнеобеспечения, оперативной связи и др. Из-за невозможности удаленной установки от объекта управления данные контроллеры устанавливаются непосредственно внутри защищаемых ими помещений. Это не способствует снижению вероятности несанкционированного манипулирования контроллером, но имеет свои плюсы - при обрыве линии связи между контроллерами и компьютером система продолжает выполнять основные функции по управлению процессом доступа в автономном режиме. Наиболее часто в системах с распределенной архитектурой контроллер может управлять проходом в 1-2 двери. Типичный пример таких систем:

- контроллер компании NORTHERN COMPUTERS (контроллер N-1000 II) - на 2 двери;

- контроллер компании KANTECH (КТ-200) - на 2 двери.

Распределенные системы обладают также тем преимуществом, что благодаря своей модульной конструкции позволяют наращивать мощность СКУД постепенно, переходя от локальных пунктов к распределенной сети; проще выполняется модернизация оборудования; авария на отдельном КПП не влияет на работу всей сети; для обработки проверяемых лиц требуется меньше времени. Из систем с централизованной архитектурой обычно получаются системы со смешанной логикой путем добавления специализированных считывателей или интерфейсных модулей с собственным буфером памяти идентификаторов и событий. Благодаря использованию такого технического решения достигается избыточное резервирование функций, резко повышающее степень безопасности системы. Поскольку контроллер в СКУД с централизованной архитектурой управляет большим числом дверей, повреждение линии связи между ним и интерфейсными модулями управления оконечными устройствами может привести к блокированию значительной части или всей системы. Локальный считыватель с собственной базой данных в этом случае переходит в автономный режим управления доступом на своем участке. Пример такого решения - считыватель АР-500 компании Apollo или интерфейсный блок управления четырьмя дверями AIM-4SL. Системы, построенные с использованием данных модулей, обладают наивысшей степенью безопасности. Приведем наиболее известные сетевые СКУД разной архитектуры с указанием числа считывателей, поддерживаемого одним контроллером. Большинство контроллеров, на основе которых строятся системы с компьютерным управлением, поддерживают четное число считывателей: 2, 4, 8,16, 24, 32, 50, 64, 96 (на 1 контроллер). Наиболее известные на российском рынке компании: Apollo, ADVANTOR, CARDAX, COTAG, eff-eff HIRSCH, lei, KANTECH, Keri Systems, NORTHERN COMPUTERS, РАС, TSS-201, Westinghous и др.

4. Контроллеры СКУД iSecure Pro

Реализацию контроллера рассмотрим на примере контроллеров iSecure Simplex СКУД iSecure Pro компании SimplexGrinnell, которые представляют собой самостоятельные микропроцессорные системы с распределенной обработкой данных. Они предназначены для управления устройствами контроля доступа и охранной сигнализации, такими, как считыватели, клавиатуры, дверные магнитоконтактные датчики, кнопки выхода, дверные замки, сирены и другие, а также для обеспечения взаимосвязи системы контроля доступа с системами и базами данных различных подразделений компании. При потере связи с управляющим компьютером встроенная в контроллер программа позволяет ему функционировать самостоятельно до восстановления связи.

Все контроллеры системы контроля доступа iSecure интегрируются с аппаратно-программной платформой комплексной системы безопасности iSecure PRO Simplex и обеспечивают стандартную организацию сетей Ethernet, TCP/IP, LAN/WAN и интеграцию с действующими в компании информационными системами. Для эффективного управления ресурсами контроллеры iSecure имеют распределенный уровень интеллекта, а для снижения эксплуатационных расходов - встроенную самодиагностику.

Основные характеристики контроллеров iSecure Simplex:

- iSecure имеет модульную, конфигурируемую и легко расширяемую схему;

- распределенная интеллектуальная архитектура контроллера позволяет выполнять непрерывную самодиагностику и регистрацию сбоев, обеспечивая его надежное функционирование и освобождая головной узел от рутинных операций;

- специальный пакет средств графической диагностики представляет оператору информацию на трех уровнях: общий вид всей сети, внутренняя

конфигурация и статус каждого контроллера системы контроля доступа, а также статус всех устройств доступа и модулей контроллера;

- каждый контроллер iSecure Simplex может иметь индивидуальную конфигурацию в сети, которая позволяет объединять сотни контроллеров, поддерживающих тысячи считывателей магнитных карт, охранных датчиков, дверей доступа и других устройств;

- съемные модули конфигурации контроллера заменяются непосредственно на объекте, что ускоряет процесс их обслуживания и сокращает эксплуатационные расходы;

- через интерфейсные платы контроллеры поддерживают различные виды связи.

Используя Ethernet TCP/IP, можно значительно сократить расходы на монтаж и обслуживание системы, соединив контроллеры через уже существующие локальные или глобальные сети. В контроллерах удаленных объектов используется плата модемной связи:

- контроллеры совместимы с широким спектром оборудования систем безопасности компании Simplex, включая систему нового поколения iSecure Pro Simplex, а также с оборудованием других производителей;

- при применении отказоустойчивой архитектуры сети iSecure Path с автоматической реконфигурацией потоков данных контроллеры обеспечивают максимальную живучесть всей системы безопасности в случае повреждения линий связи.

Все контроллеры iSecure Simplex имеют российские сертификаты. Схема подключения контроллера в систему контроля доступа iSecure PRO Simplex показана на рис. 8.



Рис. 8. Схема подключения контроллера в систему контроля доступа iSecure PRO Simplex

Конструктивные и технические характеристики контроллеров iSecure системы контроля доступа Simplex рассмотрены ниже.

1. Внутренняя архитектура. На материнской плате контроллера распо-лагаются: слот ЦПУ для карты ЦПУ с 32-разрядным встроенным процессо-ром Intel, слот карты связи для проводной сетевой карты 4120, либо модуль-ной сетевой карты 4120, шесть) слотов расширения для модулей вхо-дов/выходов и модулей подключения считывателей, а также источник питания с узлом зарядки батарей.

Контроллер имеет компактные размеры, позволяющие устанавливать его в небольших помещениях. Датчик вскрытия крышки корпуса обеспечивает защиту от несанкционированного доступа к узлам контроллера.

2. Технические характеристики контроллера:

- встроенный 32-разрядный процессор компании Intel;

- внутренняя самодиагностика и встроенный индикатор состояния;

- поддерживает клавиатуры и считыватели проксимити-карт, магнитных карт, Виганда-карт, биометрических данных, радиочастотных приемников и карт со штрих-кодом;

- возможность программирования формата карты.

Рабочие возможности по поддержке:

- до 8 форматов карточек на контроллер;

- до 96 контролируемых входов;

- до 48 релейных выходов;

- до 5000 владельцев карточек и 3000 сообщений (стандартная конфи-гурация);

до 50000 владельцев карточек и 25000 сообщений (расширяемая кон-фигурация) ;

- до 12 считывателей.

Модули-компоненты (рис. 9).

Карты линии связи (одна на контроллер): карта линии связи 4120 для проводного подключения, модульная карта линии связи 4120 или модем.

Используются следующие модули расширения: модуль для подключения 2 считывателей, модуль с 16 контролируемыми входами, модуль с 8 релейными выходами, модуль с 8 контролируемыми входами/8 релейными выходами, модуль с 8 контролируемыми входами. Все входы могут быть сконфигурированы для мониторинга как двух, так и четырех состояний.

3. Модули для подключения к контроллеру считывателей. Каждый модуль имеет два порта, каждый из которых поддерживает считыватель карточек, клавиатуру или считыватель, совмещенный с клавиатурой. Каждый порт обеспечивает полный контроль и управление точкой доступа, используя следующие элементы: релейный выход ИЗ или HP (задается перемычкой) для управления дверными замками, контролируемый вход (2 или 4 состояния) дверного магнитоконтактного датчика, контролируемый или неконтролируемый вход кнопки выхода. Кроме этого модуль, содержит 4 многоцелевых контролируемых входа и 2 многоцелевых релейных выхода.

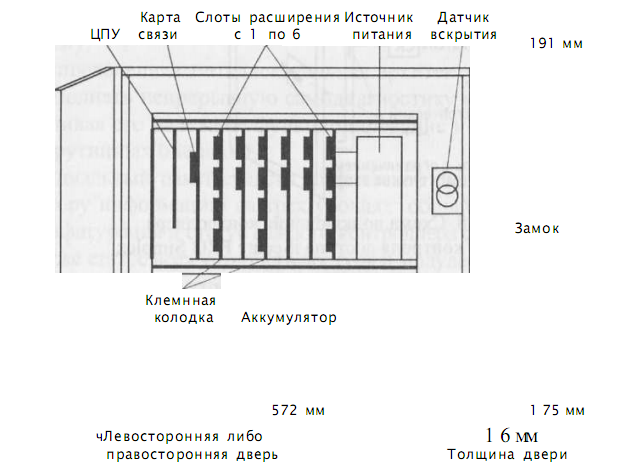


Рис. 9. Внешний вид, размеры контроллера СКУД iSecure Simplex и расположение модулей в стойке

4. Бесперебойное питание. Встроенный источник питания имеет схему заряда аккумуляторов. При использовании аккумулятора емкостью 18 А. ч время стабильной работы контроллера составит около 4 ч. Тестирование аккумуляторов осуществляется контроллером каждые 5 мин. Время заряда батарей составляет менее 24 ч.

Выводы

В процессе написания реферата мы ознакомились с автономными, сетевыми и интегрированными СКУД, рассмотрели достоинства и недостатки перечисленных выше систем, рассмотрели технические характеристики контроллеров СКУД iSecure Pro.

Литература

1. Абалмазов Э. И. Энциклопедия безопасности. Справочник каталог, 1997.
2. Татарченко И. В., Соловьев Д. С. Концепция интеграции унифицированных систем безопасности // Системы безопасности. № 1 (73). С. 86-89.
3. Мащенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: учебное пособие. М.: Горячая линия - Телеком, 2004
4. Горлицин И. Контроль и управление доступом - просто и надежно КТЦ "Охранные системы", 2002.
5. Барсуков В. С. Интегральная защита информации // Системы безопасности, 2002. №5, 6.
6. Стасенко Л. СКУД - система контроля и управления доступом // Все о вашей безопасности. Группа компаний "Релвест" (Sleo@relvest.ru).
7. Абрамов А. М., Никулин О. Ю, Петрушин А. И. Системы управления доступом. М.: "Оберег-РБ", 1998.
8. Гинце А. Новые технологии в СКУД // Системы безопасности, 2005.
9. Флорен М. В. Организация управления доступом // Защита информации "Конфидент", 1995. № 5. С. 87-93.
10. Крахмалев А. К. Средства и системы контроля и управления доступом. Учебное пособие. М.: НИЦ "Охрана" ГУВО МВД России. 2003.
11. Мальцев И. В. Системы контроля доступом // Системы безопасности,1996. № 1. С. 43-45.
12. Комплексные системы безопасности. Каталог. М.: Научно-производственный центр "Нелк", 2001.