КОНТРОЛЬ ДОСТУПА И ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Александр Крахмалев

Рассматриваются вопросы построения систем контроля доступа, а также даны основные термины и определения

В целях повышения уровня безопасности в практику все более внедряются так называемые интегрированные системы обеспечения безопасности. В состав этих систем входят охранная и пожарная сигнализации (ОПС), телевизионные системы наблюдения (ТСН), а также система контроля доступа (СКД), которая широко применяется наряду с существующими системами защиты и охраны. Многие фирмы представляют СКД на российский рынок в большом ассортименте. Ряд отечественных организаций работает над созданием систем контроля доступа, применяя при этом определенные компоненты и устройства ведущих зарубежных фирм.

Вместе с тем выбор технических средств носит (в определенной степени) случайный характер, так как потребитель имеет представление о СКД часто только по рекламным проспектам, что в результате приводит к неоправданному расходу средств или к неэффективному использованию систем. Кроме того, отечественные разработчики СКД нередко производят и поставляют на рынок изделия, которые не прошли важные этапы разработки, предусмотренные государственными стандартами на разработку новой продукции (согласование с заказчиком технических заданий и технических условий, проведение приемочных, эксплуатационных и квалификационных испытаний). Это приводит к появлению изделий низкого качества. Для обоснования применения и качественной разработки СКД необходимо иметь нормативные документы, а также справочную, методическую литературу по вопросам выбора и применения СКД, представляющие базу для сертификации как отдельных устройств, так и систем в целом.

В НИЦ "Охрана" совместно с ведущими организациями в данной сфере (в рамках работ по стандартизации в области интегрированных систем безопасности) проводится разработка ГОСТ Р "Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний". С основными положениями проекта стандарта можно будет ознакомиться в очередных номерах журнала "Техника охраны". Однако стандарт не может дать полное представление о СКД, необходимое для пользователей, работников проектных и монтажных организаций, а также других специалистов в этой области. В данной статье сделана попытка привести основные сведения и обозначить некоторые проблемы, связанные с СКД.

Системы контроля доступа — относительно новое направление технических средств обеспечения безопасности, которое широко развивается. Это связано с целым рядом факторов.

Система охранной сигнализации функционирует, как правило, в нерабочее время. При этом двери, окна и заграждения находятся в закрытом состоянии. В рабочее время указанная система отключена, большинство входов открыто, что способствует свободному перемещению служащих, посетителей, а также возможных нарушителей. Поэтому для повышения безопасности в рабочее время необходима эффективная система контроля за помещениями, сотрудниками и посетителями. В то же время сотрудники, обладающие необходимыми полномочиями, должны чувствовать себя свободно и перемещаться по зданию или территории объекта без каких-либо помех. Это может быть достигнуто благодаря СКД.

СКД может гарантировать полную автоматизацию контроля и управления доступом, что в общем случае приведет к экономии средств на обеспечение безопасности.

СКД может решать дополнительно и другие задачи (учет рабочего времени, быстрый поиск местонахождения сотрудника, управление лифтами, освещением, вентиляцией и т. д.).

Прежде чем приступить к описанию технических возможностей СКД, необходимо остановиться на терминоло-

гии в данной области, так как это во многом определяет осмысление практических задач, а также взаимопонимание специалистов. Уточним понятия **безопасность** и **охрана.**

Понятие **безопасность** имеет достаточно широкий смысл. Поэтому для четкого понимания задач обеспечения безопасности в каждом конкретном случае необходимо исходить из анализа угроз. При этом следует рассматривать как источники угроз, так и объект защиты от них. В общем виде здесь могут выступать три компонента: человек, природа и техногенная среда (то, что создано человеком, включая информацию).

Говоря о понятиях: **охрана, охранная сигнализация, система телевизионного (охранного) наблюдения, система контроля доступа,** в качестве объекта защиты выступают все три компонента (человек, природа и техногенная среда), а в качестве источника угроз – человек. Исходя из этого задачу обеспечения безопасности можно рассматривать как организацию мер по защите жизни и здоровья людей, сохранности их имущества, собственности и экологической обстановки от источника угроз, в качестве которого выступает человек.

Задача обеспечения **пожарной безопасности** предполагает учет взаимодействия всех трех компонентов как в качестве объектов защиты, так и источников угроз.

Понятие **контроль и управление доступом** можно определить как комплекс мероприятий, направленных на ограничение и санкционирование передвижения людей и транспортных средств, перемещения предметов в помещениях, зданиях, сооружениях и на территориях объектов. Технические средства СКД включают в себя: механические, электромеханические, электрические, электронные конструкции, устройства и программные средства, обеспечивающие реализацию контроля и управления доступом.

В основу функционирования СКД положен принцип сравнения тех или иных идентификационных признаков, принадлежащих конкретному физическому лицу или объекту и заложенных в памяти системы. Каждый из пользователей (сотрудников) получает индивидуальный идентификатор (карту, брелок или другой подобный предмет), в/на который с помощью специальной технологии занесена кодовая информация. Идентификатор может быть закреплен также на определенном предмете и транспортном средстве. В качестве идентификационных признаков могут быть использованы также биометрические показатели человека (отпечатки пальцев, геометрия кисти руки, голос и т. д.). У входа в контролируемое помещение устанавливают специальные устройства, считывающие информацию с идентификатора или биометрические показатели. Затем информация поступает в СКД, которая на основании анализа данных о пользователе персонального идентификатора реагирует соответствующим образом: открывает или блокирует дверь, включает сигнал тревоги, регистрирует присутствие человека на рабочем месте и т. д.

Кроме того, СКД может обеспечить выполнение других задач, например:

– сбор и обработку информации о перемещении лиц и предметов по объекту;

– организацию и учет рабочего времени;

– управление освещением, лифтами, вентиляцией и сервисной автоматикой на объекте;

– управление режимами работы и автоматикой автостоянок;

– осуществление функций ОПС;

– управление приборами ТСН.

При решении задач управления доступом СКД должна выполнять следующие функции:

– **санкционирование** – присвоение каждому пользователю персонального идентификатора, регистрацию его в СКД (или регистрацию его биометрических показателей) и задание временных интервалов и уровня доступа для пользователя (в какие помещения и когда он имеет право заходить);

– **идентификацию** – опознавание пользователя по предъявленному идентификатору или биометрическому показателю;

– **аутентификацию** – установление подлинности пользователя по предъявленному идентификатору;

– **авторизацию** – проверку полномочий, заключающуюся в контроле соответствия времени и уровня доступа, установленным в процессе санкционирования;

– **разрешение доступа или отказ в доступе** – анализ результатов предыдущих процедур;

– **регистрацию** – протоколирование всех действий в СКД;

– **реагирование** – реакцию СКД на несанкционированные действия (подача предупреждающих и тревожных сигналов, отказ в доступе и т. д.).

Санкционирование осуществляется оператором или администратором СКД и заключается в вводе необходимых данных в компьютер системы контроля доступа или в контроллер. Все остальные функции могут выполняться СКД автоматически. При этом аутентификация может быть выполнена в полной мере только с использованием биометрических показателей.

Рассмотрим основные понятия, используемые в СКД, и составные элементы СКД, из которых построена система контроля доступа.

Точка доступа – место, где непосредственно осуществляется контроль доступа (например: дверь, турникет, проходная, ворота, оборудованные считывателем, исполнительным механизмом, электромеханическим замком и другими необходимыми средствами).

Зона доступа – совокупность точек доступа, связанных между собой определенным общим признаком (например: "Второй этаж", "Склад готовой продукции" и т. д.).

Временной интервал доступа (окно времени) – интервал, в течение которого разрешается доступ в данную точку доступа.

Уровень доступа – совокупность временных интервалов доступа ("окон времени") и точек доступа, назначаемых определенному лицу или группе лиц, которым разрешен доступ в определенные точки доступа в заданные временные интервалы.

Устройство заграждающее – устройство, препятствующее свободному проходу людей или перемещению (передвижению) транспортных средств в помещения, здания, зоны доступа и на территории (дверь, турникет, кабина или шлюз прохода, ворота, шлагбаум и т. д.).

Устройство исполнительное – устройство, обеспечивающее приведение в открытое или закрытое состояние заграждающего устройства (электромагнитный или электромеханический замки и исполнительные механизмы, управляющие заграждающим устройством).

Устройство управления доступом – устройство и программные средства, обеспечивающие прием и обработку информации от устройств идентификации, управление исполнительными устройствами, отображение и протоколирование информации.

Идентификатор (носитель идентификационного признака) – предмет, в/на который с помощью специальной технологии занесена кодовая информация. Носителем идентификационного признака может быть человек. В этом случае идентификация проводится по биометрическим показателям человека.

Считыватель – электронное устройство, предназначенное для считывания кодовой информации с идентификатора.

Кроме того, определим понятие СКД, как совокупности средств контроля и управления, обладающих технической, информационной, программной и эксплуатационной совместимостью.

Рассмотрим два определения термина **система контроля доступа,** который может иметь следующие значения.

Во-первых, СКД может представлять собой продукт (изделие или совокупность изделий), который поставляется каким-либо изготовителем. При этом изготовитель гарантирует соответствие параметров и характеристик продукта требованиям технических условий и/или стандартов. Такой продукт, как правило, проходит обязательно сертификацию, проводимую независимым (от изготовителя и продавца) экспертом, по подтверждению соответствия установленным требованиям стандартов или других нормативных документов.

Во-вторых, СКД – это то, что монтируется на объекте, при этом элементы системы могут быть поставлены различными изготовителями и вопрос совместного использования указанных элементов на каждом конкретном объекте решается проектировщиком. Ответственность за работоспособность всей системы несет, как правило, проектировщик.

Понятия **идентификатор и идентификация** являются основными понятиями для СКД. Идентификация может проводиться по следующим основным методам:

– **биометрическая идентификация** – основана на определении индивидуальных физических признаков личности;

– **идентификация по вещественному коду,** записанному на физическом носителе (идентификаторе), в качестве которого применяются различные ключи, карты, брелоки и т. д.;

– **идентификация по запоминаемому коду,** вводимому вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств.

Биометрическая идентификация

При идентификации по индивидуальным биометрическим показателям определяется прежде всего человек (носитель этих показателей), а не выданный ему документ – карта, код, ключ и т. п. Это является основным отличием данных СКД от любых других идентифицирующих устройств. Самыми распространенными показателями человека при биометрической идентификации являются:

- отпечатки пальцев;
- узор кровеносных сосудов сетчатки глаза;
- геометрия кисти;
- изображение лица;
- динамика подписи;
- голосовые характеристики.

Для лучших устройств биометрической идентификации характерны высокая степень принятия "своего" пользователя с возможной ошибкой не более 0,1 % и отклонения "чужого" – с ошибкой до 0,0001 %. Данные характеристики позволяют использовать эти устройства в СКД на особо важных объектах: правительственных учреждениях, хранилищах банков, военных базах, компьютерных центрах, где самым важным требованием является секретность. Другие требования, например, по пропускной способности, стоимости, удобству пользования, имеют второстепенное значение.

Идентификация по запоминаемому коду

В качестве считывателей в этом случае чаще всего используется цифровая или алфавитно-цифровая клавиатура. Клавиатурные считыватели, хотя и считаются недостаточно защищенными от манипуляций (подбор кода, наблюдение), имеют определенные достоинства. Например: разрядность кода может быть выбрана произвольно; код может быть установлен пользователем и произвольно им изменяться, быть неизвестным оператору СКД; имеется возможность ввода дополнительных кодов (кода тревоги при нападении, кодов управления).

Идентификация по вещественному коду

Наибольшее распространение получили СКД, которые используют идентификацию по вещественному коду. В качестве идентификаторов применяются: карты, брелоки, браслеты, ключи и т. п. устройства.

Ниже приведены основные типы идентификаторов:

– *карта с перфорацией* – карта с нанесенным рядом отверстий, расположение и количество которых определяет код. Считывание кода осуществляется с помощью оптических элементов;

– *карта со штрих-кодом*, который считывается в оптическом диапазоне. Код может быть закрыт непрозрачным покрытием и считываться в инфракрасном свете;

– *карта с магнитной полосой*, на которой записан код. Считывание кода осуществляется с помощью магнитной головки по типу магнитофонной;

– *карта Виганда (Wiegand)* – карта с запрессованными внутри проволочками из специального сплава, расположение которых образует определенный код. При движении карты в магнитном поле происходит считывание кода;

– *бесконтактная карта (Proximity)* – внутри карты расположена специализированная микросхема с зашитым кодом и антенной в виде запрессованной катушки. Считывание кода с микросхемы осуществляется путем обмена радиосигналами с приемным устройством;

– *электронный ключ "touch-memory"* – представляет собой электронную микросхему в герметичном корпусе из нержавеющей стали диаметром 16 мм и толщиной 3,3 или 5,8 мм. Микросхема содержит 48-разрядный уникальный серийный номер, считываемый прикасанием ключа к считывателю.

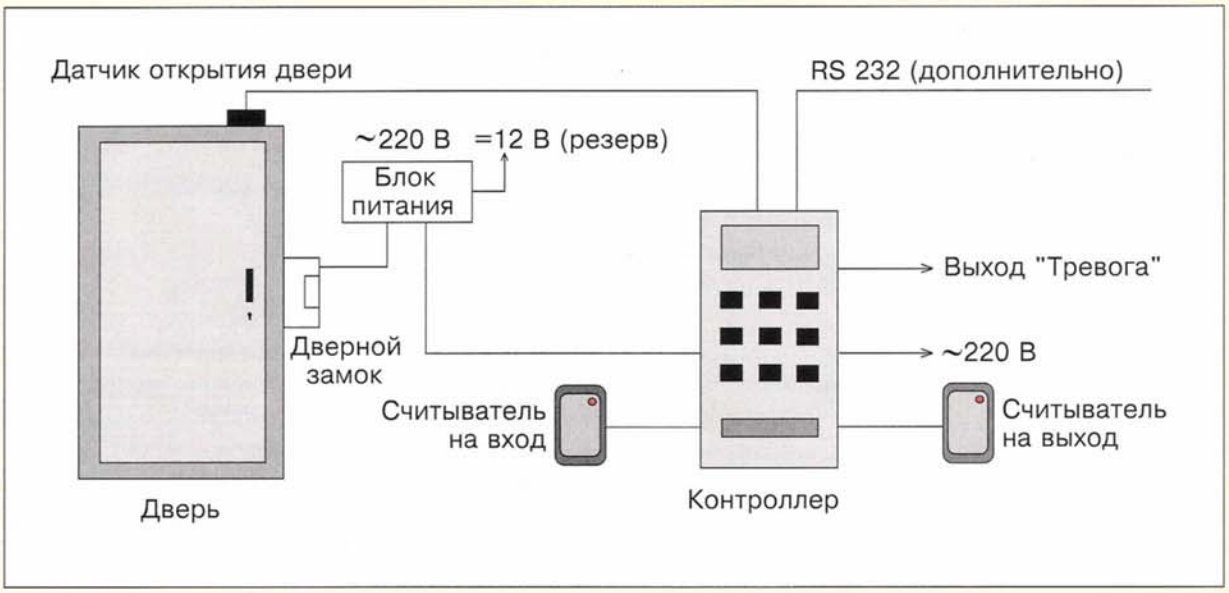


Рисунок 1 – Примерная структура автономной системы контроля доступа

Кроме того, постоянно появляются новые виды идентификаторов, которые используют различные физические принципы записи информационных кодов. Основная цель – создать идентификатор, который невозможно подделать или скопировать. СКД, использующая идентификацию по вещественному коду, не защищена от несанкционированного проникновения при использовании идентификатора посторонним лицом, например, при краже, утере или умышленной передаче его другому лицу. Для защиты от несанкционированного проникновения необходимо применять двухуровневую идентификацию, например карту и кодовую клавиатуру, однако этот вариант также может быть обойден при сговоре. Более высокий уровень защиты от несанкционированного проникновения имеет только биометрическая идентификация.

Одной из важных характеристик СКД является ее структура. По структуре СКД можно разделить на два основных вида:

– **автономная** – для управления одним или несколькими заграждающими устройствами без передачи информации на центральный пункт охраны и без контроля со стороны дежурного оператора. Примерная структура автономной СКД приведена на рисунке 1;

– **сетевая** – для управления большим количеством заграждающих устройств с обменом информацией с центральным пунктом охраны и возможностью контроля и управления СКД со стороны дежурного оператора. Примерная структура сетевой СКД приведена на рисунке 2.

Современная сетевая СКД отличается большим разнообразием структур и обладает развитыми функциями. С точки зрения усиления режима обеспечения безопасности объекта интерес представляет интеграция с системами ОПС и ТСН. Говоря об интеграции этих систем, следует выделить два наиболее общих уровня – интеграцию с системами ОПС и ТСН на **релейном** уровне и интеграцию на **системном** уровне.

Релейный уровень предполагает наличие дополнительного модуля (или дополнительных входов/выходов)

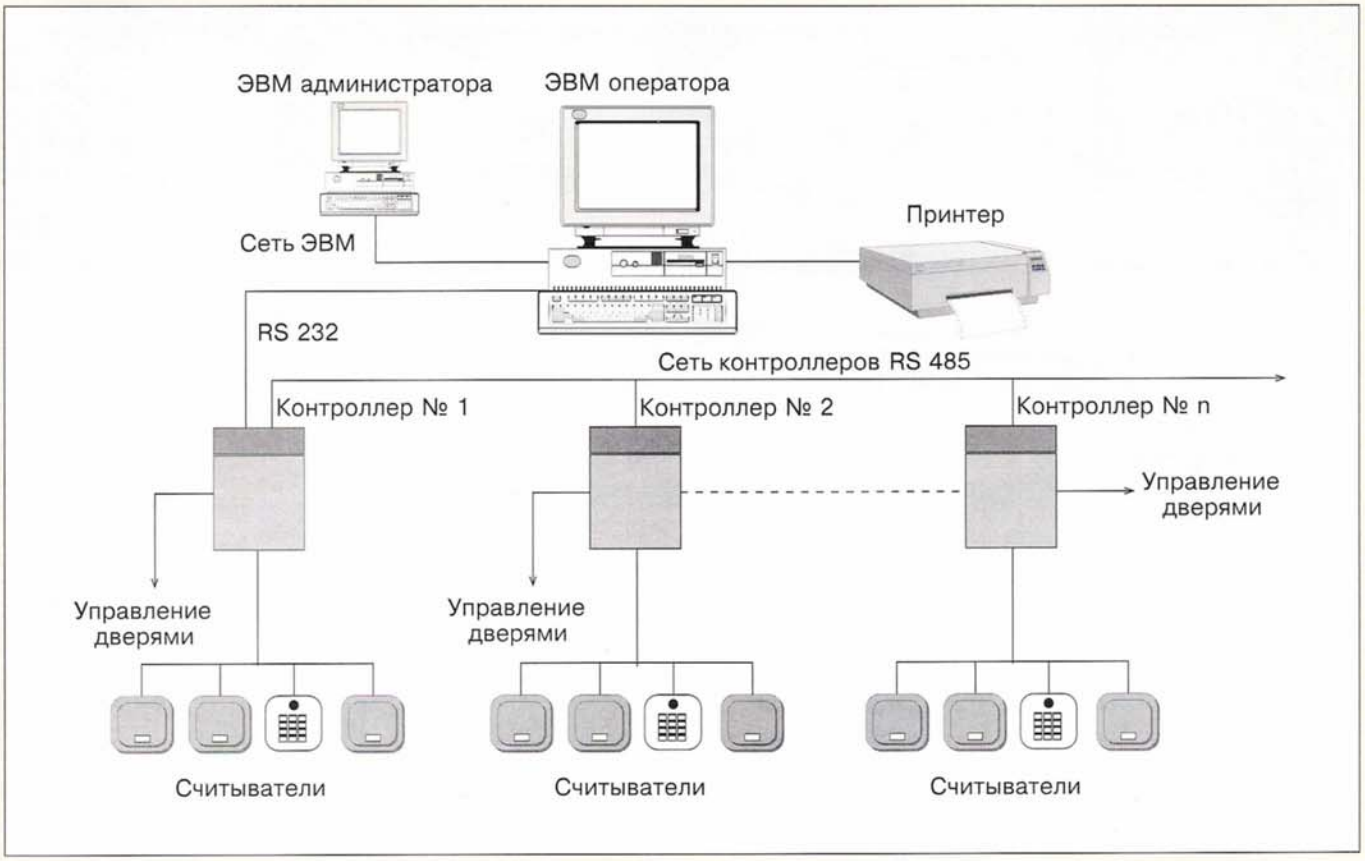


Рисунок 2 — Примерная структура сетевой системы контроля

в контроллере, к которому подключаются охранные или пожарные извещатели и релейные выходы для управления телекамерами и другими устройствами.

Системный уровень предполагает подключение к общей магистрали (каналу связи, сети) отдельных контроллеров (охранные панели, контроллеры управления ТСН).

Интеграция с системами ТСН на релейном уровне предполагает управление телекамерами с выводом изображения на телевизионный монитор.

Интеграция с системами ТСН на системном уровне предполагает управление телекамерами с выводом изображения в реальном времени на экран компьютера в окне. Соответственно должно быть программное обеспечение, которое поддерживает интеграцию.

Анализируя современные сетевые СКД, можно определить, что они строятся на основе компьютерных сетей, а также локальных сетей различного уровня сложности специальных вычислительных устройств — контроллеров. Для построения наиболее совершенных сетевых СКД можно предложить концепцию четырех уровней сетевого взаимодействия. Примерная структура такой СКД приведена на рисунке 3.

Первый (высший) уровень представляет собой компьютерную сеть типа клиент/сервер на основе сети Ethernet, с протоколом обмена tcp/ip и с использованием сетевых операционных систем WindowsNT или Unix. Этот уровень обеспечивает связь между сервером и рабочими станциями операторов.

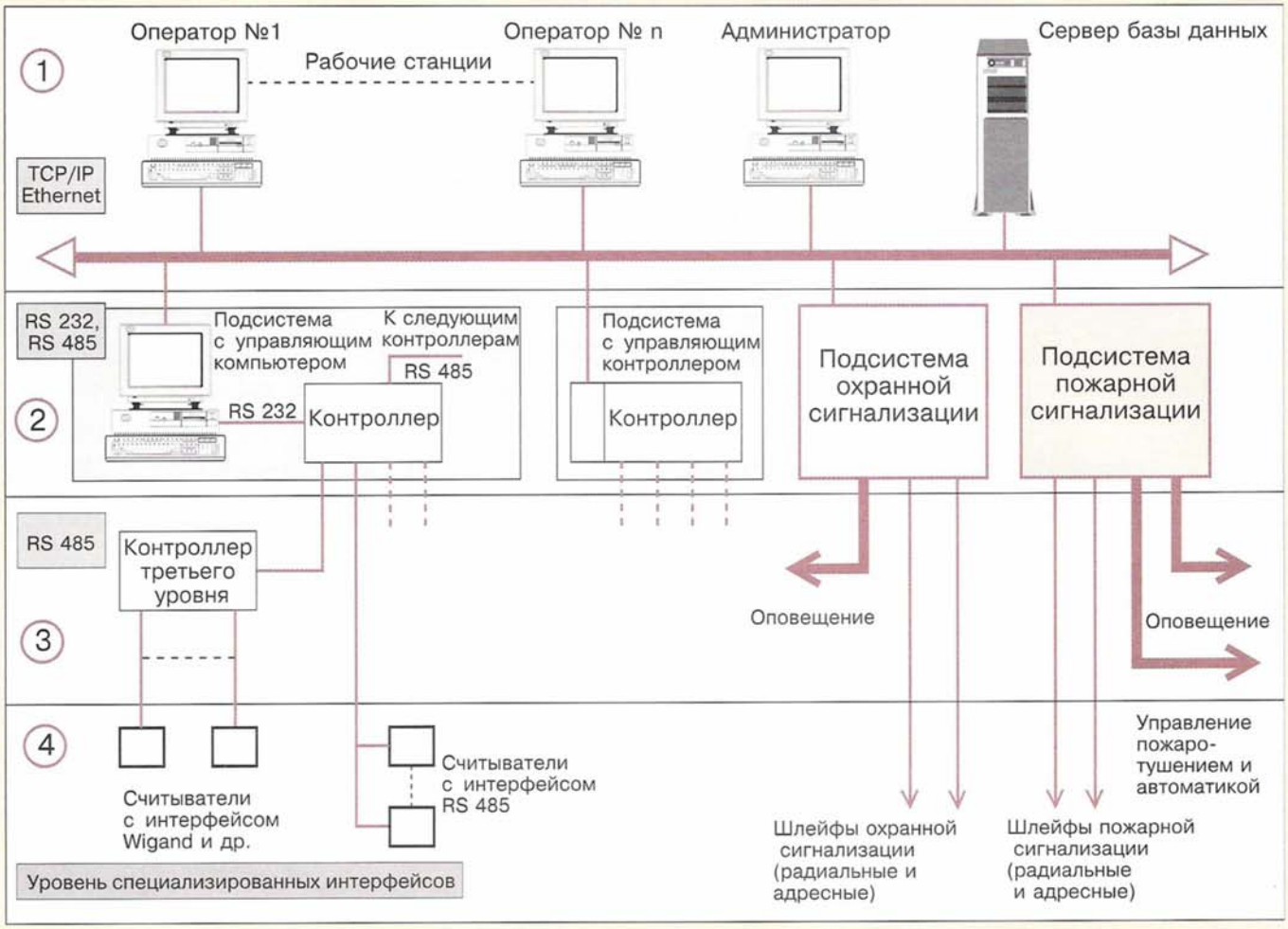
Второй уровень обеспечивает связь между контроллерами и компьютерами подсистем. На этом уровне наиболее часто используется интерфейс RS 232.

Третий уровень обеспечивает связь между контроллерами и считывателями. Здесь, как правило, применяются интерфейс RS 485 или интерфейсы считывателей Wigand (ставшие уже стандартом) или магнитные карты.

Четвертый уровень извещателей ОПС и цепей управления — сбалансированные и несбалансированные радиальные шлейфы, релейные выходные цепи, адресные шлейфы. Как правило, здесь применяются нестандартные специализированные интерфейсы и протоколы (например обмен информацией по адресным двухпроводным шлейфам).

Однако интеграция систем безопасности имеет следующие отрицательные стороны.

Во-первых, при решении вопроса об интеграции указанных систем следует исходить из того, что интегрированная система безопасности должна обеспечить более высокую надежность. Этого можно добиться только при работе подсистем в автономном режиме, чтобы выход из строя или неисправность одной из подсистем не приводили к выходу из строя (неисправности) всей системы.



(1)(2)(3)(4) – уровни сетевого взаимодействия.

Рисунок 3 – Примерная структура интегрированной системы безопасности

Во-вторых, учитывая, что управление системой безопасности осуществляется с использованием компьютеров, полностью передавать управление этой системой компьютерам нецелесообразно, так как компьютер является наименее надежным звеном системы. Для обеспечения высокой надежности системы безопасности следует применять специализированные компьютеры, а также использовать различные методы резервирования системных ресурсов, баз данных и режима питания. Кроме того, элементы указанной системы должны иметь распределенный интеллект, чтобы обеспечивать выполнение своих основных функций автономно.

В-третьих, сеть высшего уровня должна быть локальной (физически отделенной от остальных информационных сетей объекта). Для передачи данных в сети надо (при необходимости) использовать криптографические методы защиты информации, а также имитостойкие протоколы обмена информацией.

Рассматривая совместное применение СКД и средств ОПС, можно отметить, что в отечественной практике СКД применяется (в большинстве случаев) как самостоятельная система и часто рассматривается как средство усиления режима обеспечения безопасности объекта. В то же время контроль доступа является фундаментальным понятием процесса обеспечения безопасности. В любой системе охранной сигнализации присутствуют элементы контроля доступа, которые используются для обеспечения взятия и снятия объекта под охрану. Переход систем охранной сигнализации на автоматический режим работы (постановка объекта под охрану и снятие объекта с охраны осуществляются пользователем) потребует введения в указанную систему полноценных элементов контроля доступа. При этом развитая СКД имеет в своем составе модули, позволяющие обеспечить подключение охранных и пожарных датчиков. Отсюда следует сделать вывод, что СКД может рассматриваться как основа для создания интегрированных систем обеспечения безопасности.

Об авторе:
Крахмалев Александр Кузьмич,
зам. начальника отдела, кандидат технических наук
НИЦ "Охрана"