

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ: КУДА ИДЕМ?

И. Раков

к.т.н., генеральный директор,

П. Шмелев

директор по развитию,

Ю. Сукощиков

начальник отдела,

О. Батманов

главный конструктор,

научно-исследовательский центр «ФОРС»

Системы контроля и управления доступом (СКУД) переживают период расцвета. Написаны обзорные статьи и книги, многоопытными стали производители, просвещенными – заказчики. Нам представляется делом неблагодарным пытаться в компактной статье сколь-нибудь полно и последовательно отразить все современное многообразие СКУД, их элементов и решаемых ими задач. Это стезя для авторов учебников и монографий. Поэтому мы ограничимся рассмотрением лишь нескольких относительно новых (последние 2-3 года) аспектов современного развития СКУД.

РОССИЙСКИЙ РЫНОК СКУД В ЦЕЛОМ

В настоящее время большинство специалистов в областях разработки, производства, продажи и установки систем контроля и управления доступом (СКУД) отмечают хотя и незначительный, но уверенный рост объемов потребления. Даже в период кризиса спад в этом сегменте рынка не был катастрофическим и выражался в основном в некотором замедлении реализации крупных проектов, динамика компактных установок при этом практически не изменялась. По-видимому, заказчики все более осознают, что СКУД относится к тем немногим средствам безопасности, которые не только повышают уровень

противостояния объекта реализации потенциальных угроз, но и приносят прямой и значимый экономический эффект.

Положительные тенденции развития экономики страны в 2011 году позволяют прогнозировать дальнейшее увеличение спроса на СКУД. К основным традиционным потребителям – государственным режимным организациям, крупным промышленным предприятиям, банкам, бизнес-центрам – добавляются относительно новые: учреждения образования, культуры, медицины.

Общее увеличение потребления СКУД также будет, вероятно, обусловлено расширением функционала самих систем, тенденцией к возрастанию требований к оснащенности

объектов техническими средствами обеспечения безопасности ввиду активизации противоправных действий, а также необходимостью модернизации систем, установленных более 5 лет назад.

ФУНКЦИОНАЛ

В последние годы сформировался устойчивый набор основных функций СКУД как средства регулирования доступа и автоматизации учета рабочего времени. Сейчас практически невозможно найти сетевую систему без встроенного или поставляемого отдельно модуля формирования и печати различных отчетов по учету рабочего времени и контролю трудовой дисциплины. Дальнейшим развитием этого направления является интеграция с системами управления предприятием (ERP, HR-системами) и бухгалтерского учета на уровне обмена информацией о кадровых изменениях, персональных данных, полномочиях и правилах прохода через точки доступа. Многие СКУД, особенно предназначенные для оснащения малых и средних объектов, интегрированы с популярным семейством управляющих программ 1С. Большинство современных сетевых СКУД оснащены открытыми интерфейсами для интеграции в систему управления предприятием. Реализуются проекты, предполагающие интеграцию СКУД с системами SAP, Boss и др. В ближайшее время открытость СКУД (как и любых систем АСУ) к интеграции станет, по-видимому, стандартом, будет расти номенклатура поддерживаемых ими систем управления, уровень автоматизации и глубина взаимодействия. Это же относится и к интеграции СКУД с другими подсистемами обеспечения безопасности.

Конкуренция количественных характеристик СКУД сместилась в сторону более «тонких» показателей. Если раньше в качестве основных показателей рассматривалось число пользователей в системе и автономно хранимых событий в ней, то современный заказчик требует значительного количества (сотни и тысячи) уровней доступа, временных расписаний и составляющих их интервалов, высоких скоростей обмена в информационной магистрали, скорости принятия решений, числа и гибкости программирования основных и дополнительных входов и выходов, наличия и числа типовых конфигураций для управления точками прохода различных типов (двери, турникеты, шлюзы, шлагбаумы и пр.).

В передовых СКУД появились такие необходимые для крупных объектов функции, как автоматизация ввода персональных данных пользователей и оформления пропусков, реализуемых на основе автоматического распознавания содержимого документов, удостоверяющих личность, – паспортов, водительских удостоверений. Во избежание необходимости установки слишком большого числа специализированных программ в СКУД встраиваются web-сервисы для оформления и согласования заявок на пропуск, позволяющие пользоваться для этого обычными браузерами. Развиваются пользовательские интерфейсы СКУД, в частности, появляются возможности назначения групповых прав доступа сотрудникам подразделений, работы с многоуровневыми древовидными структурами предприятий. Функция запрета повторного прохода (antipassback) реализуется в передовых СКУД аппаратно и обеспечивает создание нескольких десятков уровней вложенности зон контроля. Весьма востребованы в последнее время такие функции мощных СКУД, как подсчет числа пользователей в контролируемой зоне и на предприятии в целом (что особенно важно при чрезвычайных ситуациях), поиск сотрудников по месту последнего предъявления карты, контроль перемещения пользователей по территории предпри-

ятия, контроль несения службы персоналом охраны при патрулировании объекта и пр.

Современные СКУД обеспечивают эффективный контроль и управление не только доступом персонала, но и позволяют контролировать перемещение транспортных средств по территории предприятий, создавая логистические подсистемы систем управления предприятием. Это особенно важно в ситуациях, когда на общей охраняемой территории расположено несколько предприятий, на территорию допускается транспорт подрядчиков и заказчиков, и позволяет избежать существенных отклонений от заданного маршрута и графика движения и тем самым снизить риски противоправных действий.

НЕСПЕЦИФИЧЕСКИЕ НОВЫЕ ТЕХНОЛОГИИ

Будучи электронными информационными системами, СКУД постоянно совершенствуются, вбирая в себя достижения электроники и информатики. Растущая вычислительная мощность микропроцессоров, увеличение объема и надежности элементов памяти является основой для обеспечения соответствия возможностей СКУД растущим требованиям заказчиков. Появление мощных микропроцессоров со встроенной репрограммируемой памятью обеспечило возможность дистанционного обновления и развития аппаратной части СКУД без демонтажа ее элементов, что позволяет поддерживать актуальность системы на протяжении всего срока эксплуатации без дополнительных финансовых затрат. С точки зрения производителя такой подход обеспечивает дополнительные конкурентные преимущества и позволяет развивать систему за счет вывода на рынок нового оборудования и сохранения совместимости со старыми аппаратными версиями.

Среди тенденций развития СКУД следует особо отметить всеобщий интерес к внедрению IP-технологий. Возможность использования локальных вычислительных сетей (ЛВС) для передачи информации в некоторых системах присутствует уже более 10 лет. Их структура предусматривает использование последовательных интерфейсов RS-485 или аналогичных для объединения линейных контроллеров и специальные шлюзы или центральные контроллеры для объединения оборудования в единую информационную сеть по каналам Ethernet. Основным отличием оборудования нового поколения является полный отказ от использования последовательных интерфейсов. Практически все ведущие производители вывели на рынок или анонсировали контроллеры доступа с возможностью прямого подключения к сети Ethernet. Новые технологии приносят дополнительные возможности, к которым можно отнести удобство использования оборудования и более низкую стоимость внедрения СКУД на объектах с развитой IT-инфраструктурой. Производители получают возможность организации прямого обмена информацией между контроллерами и питания устройств от сети Ethernet с применением технологии PoE (Power over Ethernet).

Следует, однако, отметить, что далеко не везде имеется необходимая оснащенность каналами Ethernet, а приобретение дополнительного оборудования и прокладка соответствующих коммуникаций может оказаться невыгодной, если в местах организации точек доступа не планируется размещение других IP-устройств или компьютеров. Ограниченная нагрузочная способность не позволяет использовать технологию PoE для питания контроллеров и исполнительных устройств суммарной мощностью более 13 Вт, а ее структура усложняет реализацию длительного резервирования электропитания системы и повышает общую стоимость оборудования ЛВС. Вопросы защиты сети от несанк-



Рис. 1. Бесконтактные считыватели папиллярных узоров поверхности пальца

ционированного доступа, обеспечения достаточной пропускной способности и правильная организация маршрутизации пакетов данных также требуют внимательного рассмотрения. Учитывая эти моменты, можно предположить, что наиболее востребованными будут универсальные системы, обеспечивающие возможность использования оборудования с классическими и Ethernet интерфейсами как по отдельности, так и в необходимых сочетаниях. Некоторые производители уже имеют в своем арсенале подобные решения, причем в ряде случаев для выбора того или иного типа интерфейса достаточно приобрести соответствующие модули расширения контроллеров СКУД.

Рис. 2. 3D считыватель геометрии лица



ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Способы идентификации пользователей СКУД можно разделить на две группы. Первую из них образуют способы, основанные на применении внешних по отношению к пользователю идентификаторов – электронных ключей, содержащих уникальный код, который распознается СКУД и которому в ее базе данных поставлены в соответствие персональные данные пользователя. Вторую группу образуют способы идентификации, основанные на использовании биометрических характеристик самого пользователя.

Биометрическая идентификация весьма привлекательна, поскольку идентификационный признак неотъемлем от пользователя, его нельзя потерять, забыть, передать, весьма сложно или невозможно подделать, его не нужно изготавливать, выдавать, обновлять и пр. Именно поэтому биометрическая идентификация в настоящее время – самое быстроразвивающееся направление на рынке систем безопасности. Даже исторически первые биометрические технологии идентификации – по контурам ладони и отпечаткам пальцев – постоянно совершенствуются. Так, с помощью телевизионных устройств созданы бесконтактные считыватели этих признаков (рис. 1). В отличие от традиционных, они более гигиеничны, так как не предполагают контакта пальца с какой-либо поверхностью, а потому значительно проще в обслуживании.

Телевизионные устройства лежат в основе 2D и 3D (рис. 2) технологий распознавания и идентификации лиц, а также известных идентификаторов по рисунку радужной оболочки глаз и относительно новых – по внутренней структуре сосудов пальца (рис. 3).

Рис. 3. Считыватель сосудистой структуры пальца



Однако, несмотря на высокую привлекательность, бурное развитие и, по-видимому, хорошие перспективы биометрической идентификации, совокупные показатели скорости и надежности распознавания в таких устройствах пока существенно уступают устройствам с внешними ключами, подавляющее число которых имеет в своей основе RFID (Radio Frequency Identification) технологии.

По-прежнему наиболее востребованными остаются считыватели и идентификаторы форматов EM-Marine и HID Proxcard II. Несмотря на отсутствие защиты от копирования, их доля в общем объеме средств идентификации не уменьшается. Это обусловлено не только низкой стоимостью отлаженных решений и поддержкой большинством производителей, но и наличием большого количества уже установленных систем. При расширении и даже замене системы на более совершенную, потребитель стремится сохранить имеющиеся в обращении карты для исключения процессов сбора имеющихся и выдачи новых идентификаторов. Для крупных предприятий с количеством персонала в несколько тысяч человек это может привести к значительным материальным и временным затратам, особенно при использовании печати на картах информации о владельце и предприятии. Для снижения вероятности несанкционированного доступа по копии идентификатора обычно используют совокупность дополнительных средств защиты – фото- и видеоверификацию, доступ с подтверждением, доступ по карте и PIN-коду, доступ по двум картам и т.п.

Тем не менее, практически все участники рынка СКУД понимают необходимость применения более защищенных от копирования технологий идентификации. Такие механизмы реализованы в бесконтактных smart-картах форматов Mifare, iCLASS и др. За последние несколько лет их сто-

Рис. 4. Antitailgating система на основе видеокамеры



Рис. 5. Antitailgating система на основе инфракрасных датчиков

имость снизилась в несколько раз и вплотную приблизилась к стоимости карт форматов EM-Marine и HID. Карты формата Mifare различных исполнений массово применяются в транспортных приложениях и в качестве социальных карт во многих городах России.

Использование встроенной памяти smart-карт и ее возрастающая емкость позволяют хранить на ней не только идентификационный признак, но и данные о владельце, в том числе биометрические, месте работы, должности, табельном номере и пр., а также его права доступа. За счет увеличения суммарного объема идентификационной информации полностью исключается ситуация ее совпадения в разных картах. При этом существенно меняется функционал и снижается стоимость стационарного оборудования СКУД. Возможность хранения на карте биометрических данных облегчает реализацию высокодостоверных и быстродействующих точек доступа, сводя задачу распознавания (выбор одного из всех) к задаче идентификации (сравнение с единственным образцом).

Существует, однако, и ряд аргументов в пользу традиционного построения СКУД. В таких системах персональные данные и права доступа хранятся в базах данных системы, они могут централизованно и оперативно контролироваться и корректироваться при утере или краже карты, изменении персональных данных, графика работы и т.п. Использование карт сторонних организаций (например, вышестоящих) для экономии средств на приобретение идентификаторов затруднено, так как связано с необходимостью раскрытия информации о структуре хранения данных на картах, согласования размещения дополнительной информации.

Для чтения защищенной информации необходимо обеспечить хранение уникального ключа доступа к данным в считывателе. Для этого используется двухсторонний обмен информацией контроллера со считывателем или запись ключей доступа к данным специально подготовленной мастер-картой при ее предъявлении к считывателям. Первое решение более удобно, но требует применения специальных считывателей и контроллеров. Второе решение позволяет использовать стандартные контроллеры с интерфейсом Wiegand, но усложняет настройку и модификацию параметров системы.

Внедрение защищенных технологий считывания кодов – вопрос времени и сдерживается только общетехнической инерционностью систем. Что касается разделения информационного функционала между картой и стационарным оборудованием, то наиболее перспективными пред-

ставляются системы с хранением на карте идентификационных признаков и централизованным хранением прав доступа (включая расписание) и персональных данных пользователей.

Промежуточным вариантом использования smart-карт, позволяющим постепенно переходить на современные идентификаторы без замены стационарного оборудования СКУД, является использование для идентификации их серийных номеров. Некоторые производители поставляют на рынок соответствующие считыватели с интерфейсом Wiegand. Такой механизм не использует защищенные режимы и подвержен риску копирования, как и традиционные EM-Marine и ProxCard идентификаторы.

Системы RFID идентификации дальнего действия с расстояниями считывания несколько метров находят все более широкое применение при создании СКУД транспортных средств. Основной задачей, решаемой в таких системах, является обработка коллизий, когда в зоне действия считывателя оказывается одновременно несколько идентификаторов.

Кроме собственно идентификации пользователей, определения и реализации прав доступа пользователей, современные СКУД включают и такой дополнительный функционал, как идентификацию условий доступа. К давно используемым ограничениям числа одновременно находящихся в зоне доступа пользователей, ограничению их биологических характеристик (вес, рост) добавляются ограничения входа для лиц с багажом, а также antitailgating-системы, препятствующие одновременному проходу двух и более лиц по одному идентификатору. Принцип работы таких систем основан на анализе при помощи телевизионных (рис. 4) или инфракрасных (рис. 5) детекторов зоны перед входом в точку доступа и блокировании возможно-

сти входа при выявлении в зоне, обеспечивающей проход за время открытого состояния исполнительного устройства более одного человека. В наиболее ответственных зонах доступа, а также при ограниченных размерах зон перед точкой доступа такой анализ совмещается с организацией входа по логике шлюза.

ИСПОЛНИТЕЛЬНЫЕ УСТРОЙСТВА

Рынок предоставляет современному проектировщику огромное многообразие исполнительных устройств, которые автоматически реализуют решение СКУД об осуществлении или запрете доступа. Электромеханические, электромоторные и магнитные замки, защелки, приводы предполагают установку на всевозможные типы дверей, ворот и калиток – от стеклянных до засыпных дверей денежных хранилищ. Стоечные и тумбовые турникеты-триподы, роторные полу- и полноростовые турникеты, шлюзовые кабины, вращающиеся и сдвижные двери обеспечивают широкие возможности по организации различных проходных. Отметим оригинальные решения для стадионов, позволяющие в перерывах между мероприятиями наглухо закрывать доступ на объект (рис. 6, 7), а также турникет с дополнительной калиткой для велосипеда, открываемой при разрешении доступа пользователю и наличия значительной массы металла в зоне чувствительности соответствующего датчика (рис. 8).

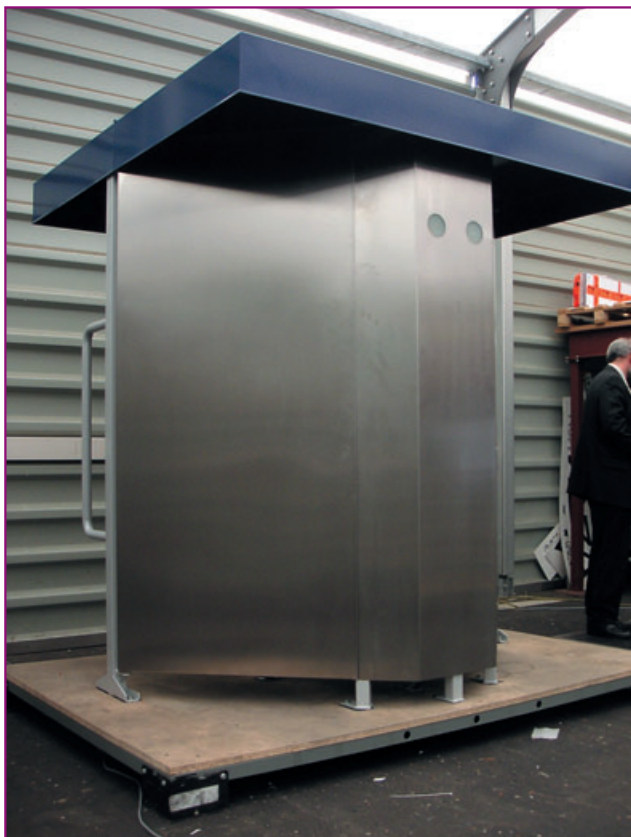
В последнее время в качестве исполнительных устройств выступают различные противотаранные устройства, особенно эффективные при парном использовании и включении по логике шлюза.

Сравнительно молодым классом исполнительных уст-

Рис. 6. Турникет для стадионов в открытом состоянии



Рис. 7. Турникет для стадионов в закрытом состоянии



ройств являются автоматизированные хранилища с ограниченным доступом к содержимому ячеек. Кроме различных конструкций «ключниц», предметами хранения выступают персональные радиостанции (рис. 9), ноутбуки (рис. 10), оружие и др.

**ИЗМЕНЕНИЯ
В НОРМАТИВНОЙ БАЗЕ**

За прошедшее пятилетие произошел ряд изменений в нормативно-законодательных актах, так или иначе касающихся рынка СКУД. Особо хотелось бы отметить два новых документа, тем более что реакция рынка на появление этих документов различна.

Введение в действие государственного стандарта – ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний», в котором наконец-то узаконен переход к терминам и определениям, реально применяемым на рынке СКУД, – в целом оценено рынком положительно. Собственно, замена понятийного аппарата в новом стандарте – главное его отличие от действовавшего ранее ГОСТ Р 51241-98.

А вот принятие ФЗ №152 «О персональных данных» рынком СКУД было практически проигнорировано, а напрасно.

В качестве уникальных данных, присущих субъекту доступа, СКУД оперирует сведениями о фамилии, имени, отчестве субъекта, его должности, служебном телефоне, адресе регистрации, времени входа/выхода и т.п. Согласно определению закона (№152-ФЗ «О персональных данных») СКУД – это информационная система персональных данных (Пдн), а сами Пдн, обрабатываемые СКУД, подлежат защи-



Рис. 8. Турникет с калиткой для велосипеда

Рис. 9. Автоматическое хранилище для радиостанций

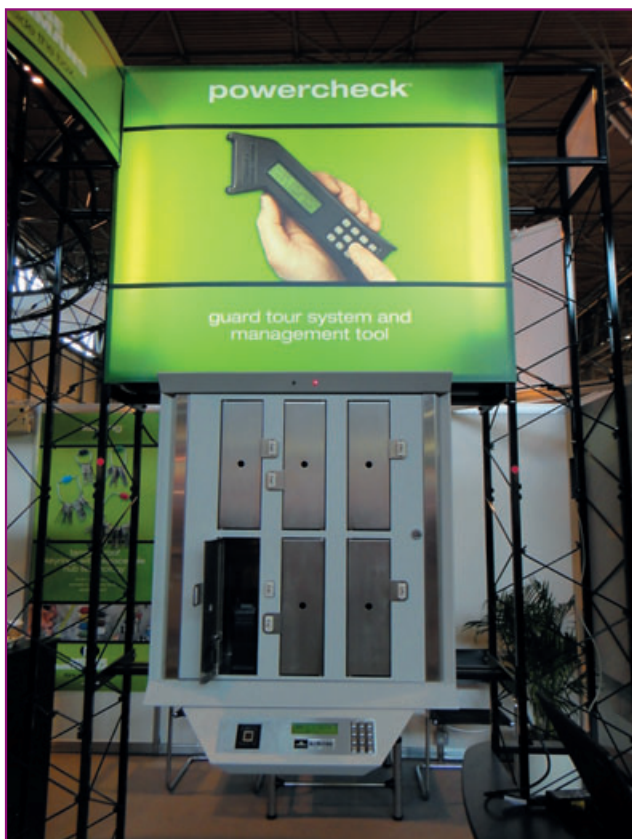


Рис. 10. Автоматическое хранилище для ноутбуков



те методами и способами, определенными регуляторами в этой сфере (ФСБ, ФСТЭК и Роскомнадзор РФ).

Обязанность защиты ПДн возлагается на оператора ПДн (юридическое лицо, осуществляющее обработку ПДн). Помимо организационных мероприятий по защите ПДн (политика безопасности, положения, регламенты, приказы, должностные инструкции) законом предусмотрены и технические мероприятия по защите ПДн. Они воплощаются во внедрении сертифицированных средств защиты ПДн.

К сожалению, большинство производителей, инсталляторов и пользователей СКУД далеки от тематики защиты информации и, в частности, ПДн. Поэтому в процессе создания СКУД заказчик, потенциальный оператор ПДн, зачастую оказывается не информирован о необходимости создания системы защиты ПДн, а функционал большинства СКУД – недостаточным для реализации требований закона.

Серьезность ситуации будет, вероятно, оценена рынком после окончания времени, отведенного на приведение систем обработки ПДн требованиям закона, определенным правительством, и вступления в действие санкций за его нарушение.

Проектирование системы защиты ПДн необходимо осуществлять одновременно с проектированием СКУД, что позволяет оптимизировать конфигурацию СКУД с точки зрения стоимости соответствующей СЗИ и обеспечить существенную экономию средств. Более того, одновре-

менное проектирование СКУД и системы защиты СКУД является требованием нормативно-правовых актов в сфере ЗИ. Ввод в строй и эксплуатация СКУД, обрабатывающей персональные данные, но не оснащенной системой защиты ПДн, является нарушением оператором (владельцем СКУД) действующего законодательства.

Средства защиты информации (СЗИ) реализуют функции управления доступом к ПДн, регистрации и учета, обеспечения целостности, обеспечения безопасного межсетевого взаимодействия, антивирусной защиты, обнаружения вторжений, анализа защищенности.

Кроме СЗИ, «надстраиваемых» над СКУД, сама СКУД должна реализовывать определенный нормативными документами набор функций по контролю и управлению манипуляциями с базой данных пользователей.

Подтверждением соответствия СКУД требованиям законодательства в области защиты ПДн является аттестация СКУД на соответствие требованиям по безопасности информации. Выполнение работ по технической защите ПДн (внедрение средств защиты), а также аттестацию системы защиты полномочны проводить только организации, имеющие соответствующую лицензию ФСТЭК России.

Не претендуя на полноту и истину в последней инстанции, надеемся, что отмеченные в статье моменты и тенденции послужат пищей для полезных размышлений и выводов всех участников рынка СКУД.

**ЛУЧШИЙ КАБЕЛЬ
ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ**



ПАРИТЕТ
ТОРГОВО-ПРОМЫШЛЕННЫЙ ДОМ

ПРОИЗВОДСТВО КАБЕЛЯ

Кабели с повышенными требованиями безопасности

КСРЭВ нг(А)-FRLS
КСРП нг(А)-FRHF

**огнестойкие кабели
не горят в огне!***

PK 75-3-313 нг(С)-HF
PK 75-3,7-318 нг(С)-HF
КСВВ нг(А)-LS
ParLan cat 5e нг-HF
кабель для RS-485

**не распространяют горения
при групповой прокладке**

www.paritet-podolsk.ru
paritet@podolsk.ru
т/ф. (495) 926-22-69 (многокан.)
(4967) 65-05-25, 67-48-58.

* - 180 мин работы в открытом пламени