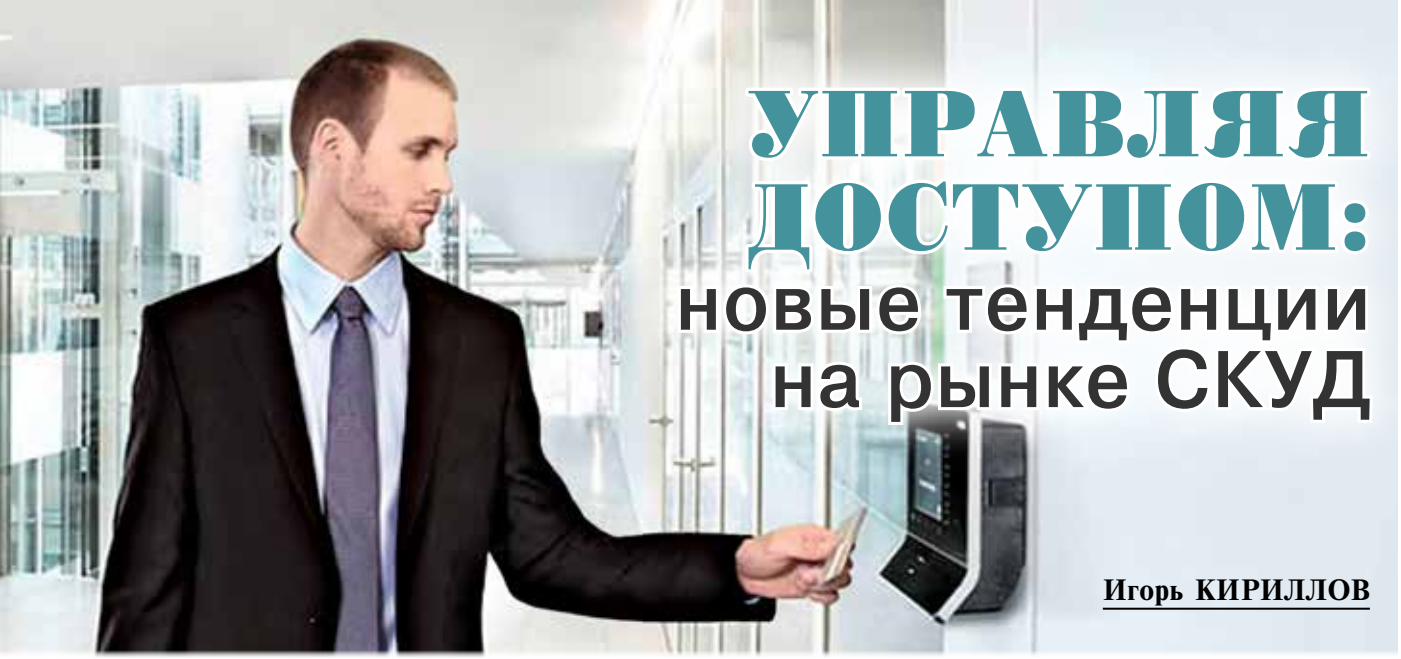

УПРАВЛЯЯ ДОСТУПОМ: новые тенденции на рынке СКУД

Игорь КИРИЛЛОВ

Системы контроля и управления доступом (СКУД) долгое время оставались «отдельным миром», но последние технологические тенденции говорят о том, что и эта подсистема постепенно переходит на IP. Для СКУД открываются новые возможности, однако появляется и много нехарактерных ранее проблем.

Стремление контролировать доступ в те или иные помещения присуще человеческой природе. Всевозможные методы контроля и разграничений прав доступа совершенствовались на протяжении веков, пока, наконец, не обрели форму централизованных автоматизированных электронных систем. Но и они не стоят на месте — в этом направлении прогресс продолжается и рынок растет.

Долгое время системы управления и контроля доступом (СКУД, СКД) развивались как бы отдельно от ИТ-мира. Здесь были свои специфические стандарты, протоколы, технологические подходы. Но в последние несколько лет ситуация кардинально изменилась. Благодаря росту популярности и все большему распространению IP рынок СКУД также не избежал влияния этого протокола. Ну а где IP, там и IT ☺.

В общем, проблема, вполне очевидно, выходит на новый уровень — системы контроля доступа начинают играть на поле глобальных цифровых технологий. При этом консервативные СКУД продержались, похоже, дольше остальных (даже системы охранного видеонаблюдения мощно и однозначно мигрируют в сторону IP). Но говорить о тотальном переходе пока не приходится. Все же здесь сильны технологические традиции, школа специалистов, рынок интеграторов и поставщиков. Поменять все в одночасье не получится. Но вполне ощутимые преимущества новых подходов подталкивают СКУД к тотальной модернизации. Даже с учетом того, что, переходя на сторону IP, любая технология сталкивается с большим (и новым для себя) пакетом проблем, присущим данному стеку протоколов, которые, тем не менее, постепенно решаются.

Несколько слов о мировом рынке

Прежде чем перейти к обзору технологических тенденций, скажем несколько слов о мировом рынке систем контроля и управления доступом. В 2015 году он оценивался международными аналитическими компаниями примерно в $5,9–6 млрд. В 2016-м, как ожидается, его рост составит 7–7,5%. В абсолютных цифрах это означает, что в текущем году объем рынка составит примерно $6,3–6,4 млрд. Основной рынок потребления уже многие годы находится в США, на втором месте — экономически развитые государства Азии (Южная Корея, Япония, КНР и другие) на третьем — страны ЕС.

Наиболее активный рост в последнее время отмечен в сегменте пользовательских решений, причем значительная часть продаж приходится на самые простые устройства, в частности, электронные замки. Таким образом, мировой рынок СКУД в корпоративном сегменте можно оценить всего в несколько миллиардов долларов, что в целом достаточно немного. По украинскому сегменту достоверных данных нет, но опрос специалистов и сотрудников отраслевых компаний, проведенный «СиБ» в процессе подготовки статьи, позволяет сделать вывод о том, что общий объем данного сегмента в нашей стране вряд ли превышает $2–3 млн.

При этом мировой рынок поделен между большим количеством специализированных компаний. Некоторые из них, например ***Schneider Electric***, ***Bosch Security Systems***, ***Tyco Security***, ***CDVI***, ***Siemens Building Technologies***, ***Honeywell***, представлены в том числе и у нас в стране. С 2015 года на рынке аппаратных и программных решений для СКУД начала активно работать ***Axis Communications***, которая раньше занималась исключительно системами IP-видеонаблюдения. Также известными игроками на международном рынке СКУД являются такие компании, как ***3M***, ***Aiphone***, ***Assa Abloy***, ***AuthenTec/UPEK***, ***BIO-key***, ***Digital-Persona***, ***Linear***, ***Imprivata***, ***Safran***, ***SecuGen***, ***GE Security*** и другие — всего несколько десятков. Кроме того, имеется огромное количество производителей, выпускающих решения бытового уровня — домофоны, электронные замки и т.д., которые, строго говоря, тоже можно отнести к разряду систем контроля доступа.

Как работает СКУД

Современная СКУД представляет собой целостный программно-аппаратный комплекс, настраиваемый

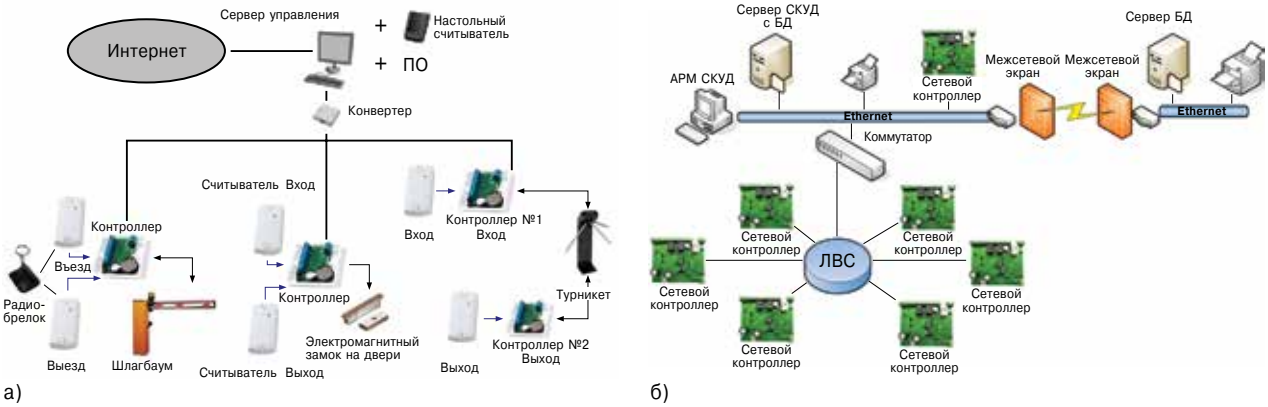

Рис. 1. Общая логическая схема PC-based (а) и веб-ориентированной (б) СКУД

и управляемый с помощью специального ПО. Система состоит из нескольких основных элементов. Во-первых, это разнообразные преграждающие устройства — электронные замки, турникеты, шлагбаумы, ворота и т.д., с чем приходится иметь дело непосредственно посетителю. Эти устройства, в свою очередь, подключаются к управляющим модулям — контроллерам, которые оснащены процессорами, памятью и различными интерфейсами взаимодействия. В общем, это как раз те устройства, которые отвечают за аутентификацию объекта, соблюдение политики прав доступа и т.д. Они могут быть как локальными (автономными), так и объединенными в общую систему.

Третьим важным элементом являются считыватели, представляющие собой различные картридеры, сканеры, радиодатчики и т.д. Они тоже подключаются к контроллерам. Запрограммировать и обслуживать несколько контроллеров можно и вручную, но в случае крупных распределенных систем уже не обойтись без специального ПО — и это четвертый важнейший элемент современной СКУД. Кроме того, поскольку различные устройства часто используют разные интерфейсы, то для их сопряжения и построения целостной системы могут понадобиться также разнообразные конверторы.

На сегодняшний день существуют три основные схемы объединения элементов СКД. Первая — классическая — подразумевает, что считыватели и запирающие устройства подсоединяются к локальному контроллеру, а тот, в свою очередь, к т.н. «мастер-контроллеру», с которого осуществляется управление всей сетью безопасности. Такие системы активно развивались еще в 80-е — 90-е годы.

Более совершенной считается технология т.н. PC-based (**рис. 1**), когда в качестве главного управляющего контроллера используется обычный ПК или сервер с установленным на него ПО, к которому по ЛВС подключаются остальные устройства контроля доступа. Но в этом случае для сопряжения компьютера и сети СКД требуются специальные конвертеры.

Третья, наиболее современная схема, подразумевает подключение всех основных устройств к общей IP-сети — это т.н. веб-ориентированные (или IP) СКУД, которые получили достаточно широкое распространение в последние пять лет. В этом случае управление средой может осуществляться не только с локального компьютера, но и с любого терминала (например, смартфона), подключенного к IP-сети, в т.ч. глобальной.

Общий алгоритм работы СКУД примерно таков: к считывателю прикладывается «ключ (это может быть, например, бесконтактная магнитная карта, жетон или просто палец), с которого считывается код-идентификатор. Данная информация передается на контроллер, который на основе запрограммированных политик определяет уровень прав доступа владельца «ключа» и в разрешенном случае дает команду преграждающим устройствам, скажем, магнитному замку, на открытие. Если система централизованная, данные о событии могут передаваться в узел управления, где они обрабатываются и хранятся (в этом случае решение о допуске на объект может принимать сервер).

В описанные схемы работы укладываются все современные СКУД — от простейших систем, вроде бытовых домофонов, до сложных решений для крупных промышленных объектов. Зачастую СКД интегрируются и с другими подсистемами, в том числе — камерами видеонаблюдения, охранной сигнализацией и даже программными средствами учета рабочего времени и т.д.

Кто ты? Подскажет смартфон!

Поскольку основная задача систем контроля доступа заключается в том, чтобы пропускать на объект только определенных людей, важным фактором становится правильная идентификация человека и определение его прав доступа. В простейшем случае, чтобы открыть замок, достаточно ввести цифровой код на клавиатуре. Но это не всегда удобно — цифровой пароль легко подсмотреть и относительно сложно запомнить (особенно если их много — для различных помещений). Поэтому самым распространенным видом ключей сегодня остаются пластиковые карты — бесконтактные (proximity) или на основе встроенного перезаписываемого чипа (т.н. smart card). Такой метод аутентификации более надежен, чем цифровой пароль. При этом имеется стойкая тенденция перехода от бесконтактных к смарт-картам, поскольку они более надежны, ведь благодаря сложным криптографическим алгоритмам, используемым в картах с чипом, такой ключ фактически невозможно подделать. В то же время любую личную карту достаточно легко украсть или потерять, что также не дает гарантии правильной идентификации объекта.

Вопреки распространенному мнению, биометрические датчики (как правило, под ними подразумевают сканеры отпечатков пальцев) не являются самым надежным

Рис. 2. Комплексный считыватель СКД, оснащенный сканером отпечатка пальца

Рис. 3. В качестве ключа в современных СКД может использоваться обычный смартфон

вариантом. Как показывает практика, у недорогих устройств такого типа достаточно высокий показатель ложных срабатываний. В одном случае они могут не пропустить человека с правильными отпечатками, а в другом — открыть дверь постороннему. Да и на практике сам отпечаток, если очень нужно, достаточно легко скопировать и воссоздать.

Но здесь на помощь приходят современные технологии. К примеру, есть специальные сканеры, позволяющие определить пульсацию в кровеносных капиллярах пальцев, что исключает возможность подлога отпечатка на искусственном носителе. Однако такие системы, несмотря на то что разработаны достаточно давно, используются нечасто. То же можно сказать и про сканер радужной оболочки глаза и другие высокотехнологичные решения — далеко не всем они по карману.

Тем не менее биометрические технологии являются сегодня очень перспективными, и многие компании в мире активно их развивают. Новые модели считывателей (**рис. 2**) используют дактилоскопические сканеры с высоким разрешением, а также усовершенствованные алгоритмы распознавания отпечатков, что позволяет свести возможность ложных срабатываний к минимуму.

Кроме того, на рынок постепенно проникает более надежная технология биоидентификации — по рисунку кровеносных капилляров на пальцах. К тому же сами сканеры становятся дистанционными, что, как минимум, более гигиенично, чем традиционные устройства, где имеется непосредственный контакт кожи пользователя со считывателем.

Последнее технологическое слово в данном направлении пока что сказано в области нанотехнологий. На различных тематических выставках уже демонстрируются новые электронные пропуска, создаваемые на базе микроскопических схем, которые рисуются на коже пальца человека (что-то вроде временной татуировки). Также есть сведения о разработке «радиотаблеток» — специальных излучающих радиочастотных капсул. Такую «пилюлю» необходимо проглотить, после чего она действует как автоматический пропуск.

В качестве ключа может использоваться также обычный смартфон (**рис. 3**). Еще в 2013 году Google разработала технологию Host-based Card Emulation (HCE), которая позволяет имитировать бесконтактную карту на телефоне. При этом связь со считывателем осуществляется посредством NFC (Near Field Communication). Есть подобные решения для смартфонов и на базе Bluetooth, например Bluetooth Smart.

В данном случае принцип использования пользовательского устройства аналогичен бесконтактной карте (приложил — открыл). При этом благодаря современному ПО и технологиям связи кодовые ключи можно оперативно и централизованно обновлять или задавать динамический алгоритм их смены для тех или иных пользователей (кому-то можно открыть только однократный проход или заблокировать доступ в те или иные помещения в нерабочее время).

Но приблизить ключ к считывателю на расстояние нескольких сантиметров, как в случае с пластиковыми картами, не всегда возможно или удобно, например — в случае проезда автотранспорта. Здесь неплохо было бы увеличить дистанцию до нескольких метров, чтобы открывать ворота или шлагбаум еще на подъезде. Такую возможность дают новые варианты реализации Bluetooth Smart. Более того, благодаря увеличенной дистанции считыватели можно размещать с внутренней стороны ворот (или вообще в каком-то секретном месте), что исключает несанкционированное физическое воздействие на них со стороны злоумышленников.

Также для идентификации автомобилей используются различные варианты технологий RFID, в частности Long Range Readers — считыватели дальней дистанции, позволяющие опознать автомобиль на расстоянии до шестнадцати метров по установленным на нем пассивным радиометкам. Более современным и надежным методом считается идентификация с помощью криптозащищенных полупассивных радиометок, работающих в СВЧ-диапазоне (т.н. SHF-метки). В этом случае сама метка не просто обрабатывается сканером считывателя, но передает собственный сигнал по каналу, зашифрованному с помощью AES. Таким образом происходит не только аутентификация автомобиля и водителя, но и самой метки, что должно защищать ее от подделки. Современные SHF-сканеры позволяют дистанционно считывать информацию с автомобиля, движущегося на скорости до 200 км/ч.

В то же время каждый отдельный метод аутентификации имеет свои недостатки, поэтому на ответственных объектах, как правило, применяется комбинация различных технологий доступа. Кроме того, в последние несколько лет в сферу СКУД активно проникают ИТ, а значит, появляются новые методы определения прав

пользователей. Так, благодаря активному развитию видеосистем распознавания образов все чаще применяются решения, использующие визуальную идентификацию. В этом случае СКУД объединяется с камерами видеонаблюдения и специальным ПО (которое устанавливается на сервере). Эффективность таких решений, уже и так вполне достаточная для коммерческого использования, постоянно растет.

СКУД по IP — преимущества и недостатки

Если попытаться описать одним словом тенденции, происходящие сегодня на рынке СКУД, то это слово будет — «унификация». Все основные производители так или иначе стремятся уйти от закрытых стандартов и проповедуют активное использование открытых платформ. Создаются и развиваются мировые технологические альянсы (например, OSDP, в рамках которого разрабатываются общие нормы для индустрии СКУД). Также большую работу проводит PSIA (Physical Security Interoperability Alliance Ассоциация по совместимости систем физической безопасности), которая сегодня занята также разработкой протоколов совместимости устройств СКД на физическом и логическом уровнях. Программа получила рабочее название PLAI (Physical-Logical Access Interoperability). Хорошие новости приходят также из других областей. Например, организация ONVIF, которая известна разработкой стандартизованных протоколов для взаимодействия различных систем безопасности, в частности — для охранного видеонаблюдения, выпустила недавно новый профиль своего стандарта, в котором обозначены принципы взаимодействия СКУД и CCTV.

Вместе с тем отмечается постепенное удешевление аппаратных и программных систем для организации контроля доступа, а также тенденция к упрощению монтажа и обслуживания устройств, что также положительно влияет на общую стоимость как внедрения, так и владения решением безопасности.

Однако наиболее важным трендом является, очевидно, все более активный переход на Ethernet и IP. Причин тому множество. Во-первых, использование этих технологий более удобно. С точки зрения физического подключения Ethernet, как минимум, требует меньше кабелей и соединений, чем в случае традиционных для СКУД сетей связи, например RS-485 или RS-235, ведь, скажем, электропитание можно осуществлять посредством технологии PoE. К тому же Ethernet сейчас распространен повсеместно, и на предприятии проще создать еще один сегмент такой ЛВС, вместо того чтобы строить отдельную независимую сеть со специфическими интерфейсами и кабелями для обычной СКУД. К тому же, благодаря постоянному развитию микроэлектроники, современные контроллеры радикально отличаются от своих предшественников. Теперь это фактически миниатюрные компьютеры с процессорами, памятью, сетевыми интерфейсами, встроенным ПО и другими характерными атрибутами.

Таким образом, СКУД постепенно превращается из группы специализированных устройств с очень ограниченными функциональными возможностями в сеть микрокомпьютеров, связанных по IP. Еще одним следствием этого процесса является возможность реализации разнообразных схем резервирования контроллеров, что может стать существенной проблемой в случае традиционных систем контроля доступа. К положительным моментам относится и то, что переход на IP позволит унифицировать системы СКУД, а также интегрировать их с другими ИТ-системами предприятия. Это даст возможность удешевить как процесс установки, так и процедуру централизованного обслуживания. Более того, теперь снимается ограничение на дальность взаимодействия устройств, ведь они могут быть подключены к Интернету. В этом контексте современная (или, скорее, будущая) СКУД хорошо вписывается в такие передовые концепции, как «облачные» технологии или даже «Интернет вещей» (IoT). Также достаточно перспективным трендом, постепенно набирающим популярность, является объединение элементов СКД с помощью радиосвязи, в частности Wi-Fi.

Использование ИТ в сфере СКУД открывает для таких систем совершенно новые возможности, находящиеся за пределами их традиционного применения. Например, современные решения позволяют подключать к «интеллектуальному» контроллеру химический анализатор, определяющий наличие алкогольного или наркотического опьянения у входящего человека. Первичный анализ производится на основе проб дыхания или слюны в течение минут или даже секунд. Подобные технологии сейчас очень востребованы на опасных и ответственных производствах, поскольку позволяют с высокой точностью определять нарушителей трудовой дисциплины и ограничить их допуск в производственные помещения. Не отстают и «облачные» технологии. Поскольку СКУД теперь можно вывести в Интернет, на рынке начали появляться компании, предлагающие услуги по модели ACaaS (Access Control as a Service), но пока этот сегмент более чем скромен по своим объемам, хотя потенциально и обладает значительными перспективами.

Однако наряду с большими преимуществами, которые открывают новые технологии для сегмента СКУД, они же несут и возможную опасность. В случае использования IP одним из главных моментов становится вопрос обеспечения информационной безопасности, ведь такие сети передачи данных — потенциальный объект атаки киберпреступников. Взломав СУБД или управляющий сервер, можно получить доступ к инструментам управления всей системой, а также к личным данным пользователей, а ведь обеспечение сохранности данных в IP-сетях требует, в свою очередь, дополнительных затрат и соответствующей квалификации персонала.

Тем не менее, несмотря ни на что, потенциально возможные трудности вполне преодолимы. Это показал опыт других систем (например, охранного видеонаблюдения), которые начали свой переход в «цифровую эру» несколько раньше. Так что, очевидно, в ближайшие годы мы станем свидетелями не только постепенной миграции СКУД в сторону все более широкого применения IP, но и созидательного объединения различных систем обеспечения физической безопасности на базе интернет-технологий.

Игорь КИРИЛЛОВ, СиБ