Практики о практике

За этим круглом столом, который прошел в Санкт-Петербурге, встретились люди, в отрасли известные и уважаемые. А если говорить о таком сегменте рынка, как СКУД российского производства, то они среди тех, кто считается законодателями мод. Но, как и положено практикам, речь участники повели о сугубо практических вопросах.

В этом номере с вами:
Александр НИКИТЕНКОВ: , генеральный директор ООО «Мегабит»
Вячеслав ТЕСАКОВ: , генеральный директор ООО «Равелин Лтд»
Леонид СТАСЕНКО: , президент ООО «НПО Релвест»

Вопрос для обсуждения:
Где находится (должен находиться) «мозг» в СКУД (в контроллере, в компьютере, в карточках)?

Александр НИКИТЕНКОВ:
– На сегодняшний день наиболее широко применяется классическая схема СКУД: размещение механизма принятия решения по управлению им в контроллере СКУД, а все операции, требующие значительных вычислительных мощностей (учет рабочего времени, отчеты по времени пребывания на объекте, хранение списков данных о пользователях СКУД в системной БД), производятся на системных серверах или АРМ. С ростом возможностей электронных компонентов, применяемых в контроллерах СКУД, эти функции совместятся. Наиболее характерный пример – контроллеры СКУД отечественных производителей систем доступа со встроенным web-сервером, которые могут одновременно управлять, хранить системные события и производить формирование отчетов по рабочему времени через Internet-браузеры. Стоимость решений СКУД на контроллерах со встроенным web-сервером неуклонно снижается и прогнозируемо скоро сравнится с классическими решениями СКУД.

Вячеслав ТЕСАКОВ:
– На этот вопрос нет однозначного ответа. Дело в том, что его решение зависит от варианта применения системы. Как известно, система должна быть максимально надежной, защищенной и одновременно удобной в использовании. Поэтому развитие СКУД шло по разным направлениям. Поскольку СКУД относится к системам с распределенной структурой, следовательно, необходимая для принятия решений информация может находиться в разных местах: контроллере, сервере, карточке. При этом степень надежности работы такой системы не изменяется, так как она решает свою определенную задачу. Например, для СКУД офисного применения наиболее приемлемым решением считается вариант, когда «мозг» находится в контроллере. Это обеспечивает

устойчивость и надежность работы в подобной системе. Системы, применяемые на объектах категории повышенной опасности, используют в своей работе различные варианты подтверждения прохода, при этом необходимые данные могут частично храниться на сервере. В гостиничных системах оптимальным решением является вариант, когда информация, необходимая для принятия решений, находится на карте клиента, соответственно, в этом случае интеллектуальная деятельность распределяется между картой и контроллером. И не надо забывать, что важной частью СКУД является инструмент дальнейшей обработки полученной информации. В отличие от других систем, СКУД не только принимают решение о проходе/проезде, но и дают возможность оперативной обработки результатов.

Леонид СТАСЕНКО:
– Смотря какой аспект интеллекта рассматривать. Если говорить о доступном функционале (управление точкой прохода), то однозначно эти «мозги» должны быть максимально близко к объекту управления. Этим обеспечивается максимальная живучесть системы за счет того, что контроллер имеет всю информацию и логику обработки, необходимую для принятия решения о допуске или недопуске пользователя в конкретную дверь. В частности, мы как разработчики СКУД всегда придерживались только такого подхода.
Другое дело, такой сопутствующий СКУД функционал, как учет рабочего времени. Здесь, напротив, «мозги» должны работать с централизованной информацией, собранной, возможно, со многих точек прохода, т. е. где-то на сервере, рядом с базой данных системы. Ну и, конечно же, есть функции, которые реализуются совместной работой контроллеров и ПО на компьютере, возможно, даже с участием оператора. Здесь в качестве примера можно привести функцию видеоверификации, т. е. когда оператор должен сравнивать живого человека с его фотографией из базы данных. Другой пример – глобальный антипассбэк, когда контроллерам необходима информация о проходе человека через точки, обслуживаемые другими контроллерами. Функцию, конечно же, можно реализовать с применением перезаписываемых карт, когда положение пользователя прописывается в карту при каждом проходе, но такая реализация антипассбэка пока что скорее экзотика, чем правило.

Вопрос для обсуждения:
Каковы основные тенденции применения proximity-карточек?

Александр НИКИТЕНКОВ:
– Применение низкочастотных (125 кГц) proximity-карт будет еще востребовано довольно длительное время. Отзывы потребителей СКУД свидетельствуют, что развитие уже установленных систем на их объектах планируется с применением имеющихся идентификаторов. На современном рынке присутствует значительное количество считывателей для таких карт по весьма доступным ценам, что немаловажно для принятия решений заинтересованными лицами. В последующем будет наблюдаться переход на перезаписываемые карты, обладающие более высокой степенью защиты от клонирования и взлома.

Вячеслав ТЕСАКОВ:
– Основная тенденция развития карт, используемых в СКУД, – это повышение надежности идентификации. Как известно, в каждой карте есть микросхема, информацию с которой и считывает считыватель. С развитием технологий появились две новые возможности. Во-первых, возможность копирования карт, во-вторых, возможность хранения дополнительных данных на самой карте. Копировать карты стало выгодно с момента, когда информационный протокол считывания карты стал открытым и когда это стало

интересно пользователям. В нашей стране на этот рынок существенное влияние оказал домофонный рынок как самый массовый. Сегодня массово применяемые карты стандарта EM-marine, могут быть скопированы у любой станции метро. О какой тогда защищенности системы контроля доступа может идти речь? К сожалению, наши клиенты очень мало обращают внимания на такие мелочи, так как гонятся за низкой ценой. Однако стоит признать, что в последнее время этому вопросу стало уделяться больше внимания. Рынок созрел. Одновременно появился целый ряд карт и считывателей, которые позволяют надежно решить данную задачу. Теперь пользователь имеет возможность выбрать, какую систему построить – защищенную или незащищенную. Компании – производители считывателей и карт разработали специализированные защитные алгоритмы, которые используют внутреннюю защищенную область памяти карт. Это, с одной стороны, безусловно, снижает возможности выбора у заказчиков, с другой – повышает надежность и защищенность внедряемых СКУД. Но, на мой взгляд, с развитием информационных технологий здесь появляется и другая крайность – это подмена такого элемента СКУД, как идентификатор, другим, на первый взгляд удобными устройствами, такими, например, как телефон. Идентификатор – это специализированное защищенное электронное устройство, которое является серьезным элементом, определяющим защищенность СКУД. Использование же устройства свободного доступа рано или поздно приведет к тому, что информация будет вскрыта или уничтожена. Здесь, мне кажется, надо опять идти от решаемой задачи. Для каких-то решений использование таких устройств, безусловно, будет оправданно, например, доступ в метро. Однако для доступа, например, в банке использовать данное решение, на мой взгляд, нецелесообразно.

Леонид СТАСЕНКО:
-–Да, тенденция использования памяти карт сейчас есть, в особенности в простых системах, в том числе в гостиничных СКУД номерного фонда. Перезаписываемые карты с объемами памяти, измеряемыми килобайтами, уже не редкость, цены на них вполне приемлемые. Если еще учесть, что многие из них имеют механизмы криптозащиты хранимых на карте данных, становится понятным, что не использовать память карт просто грех. Однако в профессиональных СКУД данная тенденция пока не наблюдается. Тут и консерватизм отрасли безопасности как таковой, и невозможность принципиально реализовать специальный функционал на контроллерах, разработанных чаще всего много лет назад. Из реализованного в жизни можно упомянуть запись на карту свертки отпечатка пальца для того, чтобы проще и быстрее произвести верификацию пользователя при использовании биометрических считывателей.

Еще следует учесть, что разных карт много и обеспечить поддержку технологии использования памяти карты в СКУД можно только для конкретного типа карты и, как следствие, со считывателями только определенного типа. А ведь контроллер СКУД для коммерческого рынка не должен быть жестко привязан к считывателям и картам только одного типа – ценность такого контроллера для широких масс сразу теряется.

Вопрос для обсуждения:
Облачные СКУД

Вячеслав ТЕСАКОВ:
– Очень модное на сегодня направление развития. Безусловно, и в СКУД уже появляются зачатки облачных технологий. Например, удаленное хранение данных. Но рынок еще не сформировался, и поэтому цена такой услуги еще довольно высока. С другой стороны, пользователи еще не привыкли к такой возможности и опасаются утечки информации. За рубежом такие технологии уже используются – и клиенты довольны. Я думаю, что и у нас скоро это появится.

Леонид СТАСЕНКО:
– Вопрос несколько надуманный, все рассуждения об облачных СКУД скорее дань моде. Практического выигрыша такие решения не дают, да и солидные организации не станут размещать свои базы данных о персонале в чужих облаках. Они скорее будут содержать свой штат системных администраторов и хорошие собственные серверы, чем выносить что-то за пределы предприятия.
Далее: для обеспечения функционирования той же СКУД облака должны гарантированно быть доступными 24 часа в сутки 365 дней в году, а сегодня еще мало кто может обеспечить такой сервис. Поэтому, как говорится, смотри пункт первый.
С другой стороны, на режимных предприятиях и интернета (а иногда и мобильной связи) вообще по определению нет для соблюдения соответствующего режима, установленного нормативными актами.
Можно, конечно, вынести в облака тот же учет рабочего времени, хотя, что на этом можно будет выиграть, мне пока не вполне понятно. Без огромного количества клиентов подобный сервис будет либо слишком дорог, либо нерентабелен для тех, кто его пытается содержать.

Вопрос для обсуждения:
Тенденции развития замков («мозг» внутри)

Вячеслав ТЕСАКОВ:
– Электронные замки, безусловно, удобное решение. Но их тоже разумно использовать для решения определенного круга задач. Здесь существуют две проблемы: скорость связи и энергопотребление. Данного вида устройства не имеют оперативного канала связи с сервером, и обмен информацией происходит либо через карту пользователя, либо посредством беспроводных средств связи. Поэтому получается довольно большая задержка между произошедшим событием и поступлением информации на сервер. Однако для гостиничных систем это приемлемо. Также приемлемо для мест, куда проход осуществляется достаточно редко, а произвести прокладку кабеля затруднительно. Например, это стеклянные либо эксклюзивные двери.
С энергопотреблением проблема более сложная. Ведь чем больше проходов осуществляется через подобную точку, тем меньше будет служить встроенный элемент электропитания. На сегодня с учетом вышеперечисленных условий этот срок достигает одного года, потом требуется замена. А теперь представьте, если таких дверей сто. Но я думаю, что с развитием систем электропитания это направление будет активно развиваться.

Леонид СТАСЕНКО:
– Есть такая тенденция, но опять же пока в простых, сравнительно бюджетных системах, в основном для гостиниц. Да, электроника шагнула очень далеко вперед, и сегодня встроить небольшую базу данных о картах и логику управления замком даже в объем замкового цилиндра не является принципиальной проблемой. Получается достаточно надежное

решение, простое в монтаже и ремонте. Но как только мы соберемся сделать online-систему, да еще и с хорошими временными параметрами (время принятия решения, время доставки информации о событиях в центральную базу данных), ситуация меняется. На батарейках такое решение не построишь (иначе батарейки менять придется слишком часто).
Да, ниша для подобных систем есть, и даже немаленькая, но заменить серьезную СКУД масштаба предприятия такие замки не смогут, по крайней мере в обозримом будущем.

Вопрос для обсуждения:
Интеграция СКУД с другими системами. Использование IP-технологий в СКУД.

Александр НИКИТЕНКОВ:
– Интеграция СКУД, систем видеонаблюдения и охранных систем позволяет обеспечивать качественный рост потребительских характеристик каждой из систем. Оптимальной будет интеграция систем безопасности отдельных производителей, представляющих наиболее современные и продуманные решения. Препятствием для этого является многообразие протоколов работы оборудования ведущих производителей, что каждый раз требует проведения отдельных работ по включению перспективного оборудования в единый комплекс.

Вячеслав ТЕСАКОВ:
– На сегодня вопрос, нужна ли интеграция с другими системами или не нужна, уже не стоит. Да, нужна. Во-первых, есть обязательное требование по взаимодействию с системой пожарной сигнализации. Во-вторых, практически все современные СКУД интегрированы с системами видеонаблюдения. Так как только таким способом можно получить подтверждение факта прохода конкретного человека. Но и в этой задаче появились подводные камни. Использование сложных интеграционных оболочек зачастую неудобно пользователям и существенно удорожает проект. Поэтому появился ряд простых интеграций. Когда системы СКУД взаимодействуют с другими системами без использования специального ПО, это облегчает их применение. С другой стороны, использование СКУД на больших распределенных объектах без использования интеграционных оболочек, на мой взгляд, невозможно. И еще, нельзя забывать о том, что СКУД является источником данных для систем управления предприятием. Поэтому большинство СКУД интегрированы еще и с такими программами, как, например, 1С.
Вопрос с внедрением IP-технологий аналогичен вопросу об интеграции. На сегодня существует большое число объектов, где требуется внедрение СКУД, и уже существует локальная сеть. Безусловно, ее использование будет оправданным решением. Но надо не забывать, что это канал открытого доступа. Следовательно, нужно позаботиться о том, чтобы защитить информационный канал СКУД специальными средствами. Одновременно нужно помнить о том, что использование только IP-решений не всегда оправданно с экономической точки зрения. Поэтому, на мой взгляд, будущее за универсальными СКУД, которые смогут работать по различным каналам связи – проводным, IP и беспроводным.

Леонид СТАСЕНКО:
– Разговоры об интеграции СКУД с другими подсистемами безопасности, да и не только безопасности, начались почти одновременно с рождением СКУД в современном ее понимании. При этом каждый решает эту задачу своим, как правило, уникальным способом. Это связано в первую очередь с отсутствием до настоящего времени хоть каких-нибудь стандартов обмена информацией между подсистемами (охрана, пожарная безопасность, видеонаблюдение, СКУД, кадровые системы предприятий и т. д.).
Безусловно, интеграция подсистем во многих случаях не просто полезна – она необходима. Здесь главное – не перегнуть палку, поскольку интеграция есть не самоцель,

она должна привносить синергетический эффект в комплексную систему и быть направленной на решение вполне конкретных задач. В то же время СКУД не должна подменять собой, например, систему видеонаблюдения. Видео в СКУД требуется для видеоверификации, для распознавания автомобильных номеров, но создавать в СКУД круглосуточные видеоархивы – это полный нонсенс. В то же время иметь возможность по событиям СКУД, охранной и пожарной синхронизации оперативно находить соответствующие фрагменты в видеоархивах подсистемы видеонаблюдения – очень востребованная функция.

Здесь мы плавно переходим ко второй части вопроса: IP в СКУД. Во-первых, использование IP-инфраструктуры часто упрощает вопросы интеграции подсистем. Во-вторых, использование готовой информационной инфраструктуры предприятия значительно снижает стоимость монтажа, поскольку отпадает необходимость в прокладке трасс того же RS-485, зачастую достаточно протяженных. Заметим попутно, что подсистема доступа в современных сетях занимает настолько мизерную часть общего трафика, что об этом даже говорить не стоит (чего не скажешь об IP-видеонаблюдении). Надо только не забывать, что использование сетевой инфраструктуры (если это общая сеть Ethernet предприятия) повышает риск атак на подсистемы безопасности, поскольку они становятся доступными практически с любого рабочего места, где есть ПК. Но этот риск можно свести к минимуму при грамотной настройке сетевых коммутаторов и маршрутизаторов, которые имеют сейчас достаточный набор функций для защиты от взлома, имитации и т. д., позволяют прокидывать через общедоступную часть сети защищенные VPN-каналы, короче, все в ваших руках, было бы только желание.

И еще одно преимущество мы получаем для точек доступа с большим количеством персонала: контроллер с IP-интерфейсом «перезаливается» при необходимости на пару-тройку порядков быстрее, чем контроллер с таким же объемом базы данных и с интерфейсом RS-485.

Наша статистика показывает, что в последние несколько лет соотношение контроллеров с IP-интерфейсом и с RS-485 заметно меняется и скоро это соотношение станет уже один к одному.

Источник: http://www.tzmagazine.ru