СКУД. Как решать новые задачи заказчикам из промышленного сектора

Мнения экспертов

Большинство экспертов придерживаются мнения, что рынок систем контроля и управления доступом (СКУД) в России достаточно развит и способен успешно преодолевать новые задачи. Мы пригласили экспертов из компаний "ААМ Системз", "АРМО-Системы", "Семь печатей", НВП "Болид", "АВИКС ДЦ", "дормакаба Евразия", Sigur и "ТерраЛинк" обсудить, что делать заказчику крупного распределенного объекта, если с рынка ушел поставщик оборудования или ПО, на какие технологии идентификации стоит обратить внимание, как относиться к биометрии и др.

Алексей Гинце
Директор по связям с общественностью компании "ААМ Системз"

Олег Тихонов
Директор департамента интегрированных систем безопасности компании "АРМО-Системы"

Аркадий Гамбург
Генеральный директор компании "Семь печатей"

Что делать заказчику, если с рынка ушел поставщик оборудования и (или) ПО для СКУД? (Варианты: ушел поставщик контроллеров/считывателей/программного обеспечения)

Алексей Гинце, ААМ Системз

Наиболее сложный вариант, когда речь идет вообще о системе в целом. В случае реального ухода поставщика и невозможности решить вопрос путем параллельного импорта, скорее всего, потребуется ее полная замена. Если заказчик не готов терять уже функционирующий сегмент системы, то вариантов два. Первый – развертывание нового самостоятельного сегмента СКУД на основе альтернативного оборудования и ПО отечественного производителя или зарубежного поставщика, который уходить не собирается. Второй – на нашем рынке есть системы, позволяющие одновременно работать со СКУД разных производителей. Важно отметить, что второй вариант предпочтительнее, поскольку он подразумевает единое информационное пространство и управление из общего управляющего программного обеспечения (ПО), однако не факт, что именно ваша система входит в перечень поддерживаемых в ПО нового поставщика, это надо выяснять.

Параллельная работа двух СКУД без объединения их под общим управлением представляется нереальной, поскольку влечет удвоение расходов на поддержку, а самое главное – большие сложности в обмене информацией между самостоятельными сегментами СКУД на основе разного оборудования и ПО. Следует также помнить о средствах идентификации, которые в идеале должны быть совместимы, и идентификаторы из первой системы должны читаться на второй.

Если ушел поставщик контроллеров, основной вариант – заменить их на альтернативные, имеющиеся на рынке, предварительно проработав вопрос совместимости с имеющимися считывателями и идентификаторами. В этом случае вам придется заменить и управляющее ПО, с которым могут работать новые контроллеры СКУД. Для государственных структур выбор еще более узок: ПО и контроллеры должны быть отечественные.

При уходе поставщика считывателей вариантов также два: либо полная замена связки "считыватель – идентификатор", либо частичная, в том случае, когда есть возможность подобрать нового поставщика, чье оборудование совместимо с уже имеющимся. Тут надо смотреть варианты, что возможно и что выгоднее: заменить считыватели (оставив идентификаторы) или заменить идентификаторы (оставив считыватели). Если в системе несколько тысяч идентификаторов (много пользователей) и всего десяток считывателей, на которых они регистрируются, выгоднее заменить считыватели. В обратной ситуации, когда считывателей много, а идентификаторов (карт) мало, выгоднее заменить карты.

Уход с рынка поставщика ПО фактически означает замену основной части системы (ПО + контроллеры). Тем, кто собирается эксплуатировать уже установленную систему при уходе поставщика ПО, следует помнить, что обновления, скорее всего, уже не будут приходить и стабильность ее работы придется поддерживать

Максим Горяченков
Руководитель отдела технической поддержки ЗАО "НВП "Болид"

Ольга Жабрева
Заместитель генерального директора компании "АВИКС ДЦ"

Сергей Ефремов
Старший инженер по разработке и обслуживанию ООО "дормакаба Евразия"

Артем Старшинов
Pre-sale инженер компании Sigur

Сергей Сорокин
Менеджер по pre-sale и обучению компании "ТерраЛинк"

Денис Иванов
Директор по развитию компании "Итриум СПб"

собственными силами. При отсутствии кадров с необходимой для этого квалификацией это представляет собой нерешаемую задачу и возвращает к вопросу замены ПО и контроллеров.

Олег Тихонов, АРМО-Системы

По моему мнению, при ответе на этот вопрос будет правильным отталкиваться от задачи, которая стоит перед заказчиком, и если на предприятии уже действует какая-либо СКУД, то прежде всего нужно понять, есть ли необходимость в полной замене существующей системы, ведь для крупных объектов это немалые финансовые вложения. За последние полгода многие дистрибьюторы наладили параллельный импорт оборудования, и сейчас вполне реально доставить необходимое железо, но пока узким местом остается программное обеспечение. Выходом из ситуации может стать, например, активация ПО за рубежом.

Таким образом, если в компании заказчика не планируется большого роста, но нужны ЗИП (запасные части, инструменты и принадлежности) и какое-то минимальное расширение, то я бы однозначно советовал оставаться на текущем решении.

Конечно, есть клиенты, которые из-за корпоративной политики или иных соображений вынуждены менять свою СКУД целиком, здесь основной тренд – закладывать в проекты максимально доступные решения.

Самый сложный случай – это когда объект находится на какой-либо стадии производства. Тут нужно все взвесить, оценить доступность оборудования и возможные сроки его поставки. Моя рекомендация – обратить внимание на российских производителей, которые готовы выполнить интеграцию своих систем с существующим решением. Мы в таких случаях для своих клиентов всегда стараемся подобрать альтернативный интегрируемый вариант.

Отмечу также еще один важный для заказчика момент: покупать нужно не у тех компаний, кто только и умеет, что привезти "в серую", а потом бросает клиента без сопровождения, а у таких поставщиков, которые кроме возможностей логистики обладают необходимыми компетенциями и могут обеспечить поддержку на разных этапах реализации проекта.

Аркадий Гамбург, Семь печатей

Вариантов немного: либо оставить все как есть (вдруг рассосется, то есть или поставщик вернется, или, на худой конец, обходные каналы поставок наладятся), либо менять всю систему. Третьего не дано: расширить систему, интегрировать ее с новым оборудованием (например, с той же биометрией), или с какими-то своими приложениями без адекватного поставщика практически невозможно.

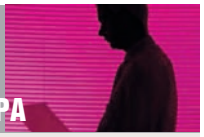
При замене системы надо искать такую СКУД, которая позволит использовать по максимуму старое оборудование (считыватели, замки, турникеты...) и при этом с наименьшими издержками впишется в действующую интегрированную структуру обмена данными предприятия.

Замену систем можно осуществлять постепенно, на какое-то время установив новую СКУД параллельно старой.

И повторю мой всегдашний совет при выборе СКУД: опираться только на объективные характеристики системы, в том числе обязательно посетить (или хотя бы обзвонить) объекты, где рассматриваемая система работает. Ни в коем случае не выбирать по принципу "это есть у моего знакомого" и уж тем более отсекать тех, кто что-то лоббирует по шкурной заинтересованности...

Максим Горяченков, НВП "Болид"

ПО зарубежных вендоров в ряде случаев может быть заменено на российское. За последние годы было представлено достаточно много отечественного ПО верхнего уровня для монито-



КОЛОНКА РЕДАКТОРА

СКУД на крупных объектах: игроков меньше, задачи сложнее

В большинстве инженерных систем, и системы безопасности не являются в этом плане исключением, есть разделение, связанное с их мощностью и способностью выдерживать тяжелые нагрузки. Все это справедливо также и для СКУД. Действительно, СКУД для решения задач доступа в офис на 2–4 двери, где может даже не быть выделенного компьютера, и СКУД крупного холдинга с объектами в разных городах, тысячами точек доступа, сотнями управляющих компьютеров и серверов, десятками тысяч карт похожи друг на друга не более, чем легковая "Лада" и карьерный БЕЛАЗ.

Сложности, связанные с внедрением СКУД на крупных объектах, в настоящее время существенно усугубляются уходом части зарубежных вендоров и усложнением логистики для тех, кто продолжает работать, в том числе по схеме параллельного импорта. Ко всему прочему, число компаний, работающих в рыночном сегменте крупных СКУД, всегда было меньше тех, кто ориентировался на массовый рынок. Поэтому уход даже нескольких значимых мировых игроков сильно повлиял на текущий расклад отечественного рынка СКУД. Многие серьезные потребители встали перед дилеммой: полностью заменить установленные зарубежные системы на отечественные аналоги, что влечет большие материальные издержки, или рискнуть и продолжить эксплуатацию имеющихся зарубежных технических средств и ПО в случае сохранения части связей и каналов поставки, с риском потерять все при полном их перекрытии. Безусловно, такая картина не является полной и существует масса промежуточных решений, позволяющих минимизировать шоковый эффект от описанных выше полярных вариантов.

В этом номере журнала вы можете ознакомиться с мнением ведущих экспертов и представителей авторитетных на рынке систем контроля и управления доступом компаний, которые предложат варианты решения задач СКУД для крупных заказчиков в нынешней непростой для всех ситуации. Коллеги также делятся собственным видением вариантов развития отрасли на ближайшую перспективу и называют ключевые технологии, которые будут формировать основной вектор развития СКУД в России.

Алексей Гинце

Редактор раздела "Системы контроля и управления доступом", директор по связям с общественностью компании "ААМ Системз"

ринга и управления интегрированными системами безопасности, которое может работать с контроллерами СКУД различных, в том числе зарубежных, производителей. Поэтому, если контроллеры объекта входят в число поддерживаемых российским ПО, серьезных проблем возникнуть не должно.

Те контроллеры, которые официально перестали поставляться в Россию, теоретически могут быть ввезены через третьи страны. Но пока трудно сказать, насколько такие схемы поставок реально заработали. В случае ухода с рынка поставщика контроллеров более перспективным видится их замена на российское оборудование. Отечественные производители сегодня предлагают аппаратные и программно-аппаратные решения для СКУД любого масштаба.

Считыватели можно назвать наименее проблемной частью СКУД. Зачастую они подключаются к контроллерам по стандартным интерфейсам Wiegand или OSDP, поэтому их замена на отечественные или азиатские аналоги не будет вызывать больших трудностей. Исключением могут быть системы с собственными решениями по защите от копирования идентификаторов. В этом случае со временем может потребоваться замена всех считывателей и карт доступа.

Ольга Жабрева, АВИКС ДЦ

На нашем рынке существует большое количество российских сильных профессиональных игроков среди производителей СКУД. Большинство из них более чем с 15-летней историей. За эти годы компаниями были решены различные интеграции с контроллерами и системами зарубежных производителей, и не только. Российские системы давно уже шагнули за пределы задач чистой СКУД. На сегодняшний день это большие интеграционные платформы.

Поэтому, по моему мнению, дальнейшее развитие существующих иностранных СКУД на объектах заказчика могут взять на себя российские производители и это произойдет "бесшовно" (учитывая опыт производителя). Заказчики не потеряют имеющийся функционал, а лишь приобретут новые функциональные модули, разработанные под специфику их отрасли.

Сергей Ефремов, дормакаба Евразия

В случае считывателей ситуация наименее болезненная, найти альтернативного поставщика будет несложно, так как большое число систем использует стандартные интерфейсы Wiegand и OSDP. В случае проблем с поставками ПО или контроллеров единственный выход – искать альтернативного поставщика и прорабатывать возможность интеграции новой системы с существующей, то есть разворачивать параллельно новую систему, обеспечить интеграцию и постепенно, по мере выхода из строя старого оборудования, переводить объект под контроль новой системы. Главное в этом процессе – хорошо проработанная интеграция и детальная дорожная карта перехода на новую систему.

Артем Старшинов, Sigur

В первую очередь следует проанализировать текущую ситуацию и понять, сколько осталось ЗИП и какое время может безаварийно функционировать объект.

Исходя из результатов анализа можно сделать выводы, как срочно необходима замена оборудования (полная или частичная). В любом случае стоит найти альтернативные варианты, которые смогут объединить решения ушедшего бренда и другие, которые остались на рынке, чтобы переход был плавным.

Следует обращаться к проверенным решениям, которые стабильны на рынке и подходят под политику импортозамещения.

Если времени достаточно, то стоит рассмотреть возможность интеграции текущего решения с новым или полной замены на новое оборудование.

Сергей Сорокин, ТерраЛинк

Первоначально нужно оценить, какие компоненты системы безопасности "ушедшего" поставщика используются в настоящий момент, насколько они критичны для бесперебойной работы, насколько технологичны и современны, есть ли аналоги. Рассмотреть возможность экономической и технологической целесообразности вариантов частичной замены оборудования и ПО на аналоги или же полной модернизации системы с переходом на более технологичные и функциональные решения от новых поставщиков. По результатам анализа искать поставщика нового решения или частичной замены компонентов системы.

Денис Иванов, Итриум СПб

Единственный верный путь – составлять стратегический план максимально полного перехода на отечественные решения и затем его выполнять. Ни один из иностранных производителей (разработчиков) не ушел с рынка на 100%: есть параллельный импорт, остались компетентные специалисты и т.д. То, чего больше всего опасались – что владельцы систем на базе иностранных решений останутся полностью у разбитого корыта, не случилось. Но очевидно, что о досанкционном уровне поддержки и сопровождения (в том числе непосредственно от производителя) говорить уже не приходится, да и с некоторыми компонентами действительно сложности очень высоки.

Другой фактор – понимание властью того, что иностранные решения надо заменять. Существует Указ Президента Российской Федерации от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации". В соответствии с ним "с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры".

Опять же, имеет место подрыв доверия к иностранной продукции: то, что сегодня еще доступно по каким-то "параллельно-перпендикулярным" схемам, завтра может доступным уже не быть. И в том числе где гарантии, что в системе нет каких-то бэкдоров, через которые все, что было "параллельно закуплено", завтра не выключат извне?

Резюмирую: бережно относиться к тому, что уже в эксплуатации, но в дальнейшем планировать

На какие технологии идентификации следует обратить внимание потребителю в текущей ситуации для крупных распределенных СКУД?

Алексей Гинце, ААМ Системз

Наиболее перспективными представляются бесконтактные биометрические СКУД (если будут решены правовые вопросы), а также классические RFID-технологии (как карточные, так и идентификация по смартфону).

Что касается наиболее распространенных карточных RFID, то следует обратить внимание прежде всего на смарт-идентификацию (13,56 МГц) как наиболее защищенную. Классика вроде Proximity давно не соответствует базовым требованиям по безопасности и защите от копирования.

Олег Тихонов, АРМО-Системы

В этом контексте выделять какую-то одну из технологий идентификации я бы не стал. Все они по-прежнему доступны: и RFID, и биометрия, и мобильный доступ. Выбор здесь зависит от предпочтений и нужд заказчика. Есть некоторые сложности с производством чипов для карт-идентификаторов, что существенно увеличивает сроки их поставки, поэтому при реализации СКУД с использованием карт этот момент надо учитывать. В случае RFID-идентификаторов я бы посоветовал также обратить внимание на защищенные решения.

Если в системах контроля доступа планируется применять идентификацию с помощью мобильных телефонов, рекомендую тщательно выбирать производителя такой СКУД (подходящая схема лицензирования, покрытие "парка" смартфонов, сервер в России).

Что касается биометрического контроля доступа, то здесь могу отметить, что больше всего запросов к нам приходит на решения с идентификацией по лицу, это сейчас главный тренд в данной сфере.

Аркадий Гамбург, Семь печатей

Думаю, что нынешний уровень технологии распознавания лиц вполне позволяет рекомендовать заказчикам переходить на этот способ идентификации.

Плюсы очевидны:

- идентификатор (то есть лицо) всегда при себе и его невозможно подделать;
- при желании (а для определенного рода предприятий это и необходимое условие) может быть включена многофакторная идентификация;
- возможность решать задачи дополнительного контроля (температура, маска, QR-код и все, что еще может возникнуть).

Но надо понимать и относительные минусы такого подхода:

1. Высокая стоимость решения по сравнению с классическими технологиями. Но для крупных организаций это вряд ли большая проблема.
2. Меньшая скорость реакции системы (по сравнению с картой), которая зависит даже не столько от скорости самого устройства, сколько от времени позиционирования лица. Во внутренних помещениях это не особенно важно, а на проходных проблема решается увеличением количества турникетов и постепенного привыкания персонала к "правильному" проходу.
3. При программной реализации распознавания снижается надежность системы. Это может происходить при использовании серверной видеоаналитики или при работе с терминалами через управляющее ПО.

Проблема обходится при аппаратном подключении терминалов распознавания, что позволит работать системе в автономном режиме. А почему этот режим важен – смотрите мой ответ на четвертый вопрос.

Максим Горяченков, НВП "Болид"

Последние годы казалось, что наиболее перспективным видом идентификации является биометрия. Технологии идентификации по шаблонам лиц стремительно развивались, в России было внедрено множество собственных наработок, широко использовались также решения азиатских поставщиков. То есть санкции не столь значительно повлияли на этот сегмент. Но государственное регулирование этой сферы может затормозить и изменить естественные пути развития биометрической идентификации.

Если говорить о классической идентификации при помощи карт, то необходимо помнить, что для российских производителей наиболее проблемными остаются считыватели самых защищенных карт семейства MIFARE Plus. Компании NXP и STMicroelectronics, являющиеся основными производителями чипов, используемых при работе с упомянутыми картами, полностью прекратили прямую работу с российскими производителями. Азиатские производители чипов пока могут предложить решения с сильно ограниченным функционалом, поддерживающие только уязвимую технологию Crypto-1.

Ольга Жабрева, АВИКС ДЦ

На мой взгляд, биометрическая идентификация на сегодняшний момент предоставляет более надежный способ идентификации пользователей, а также позволяет избежать мошенничества. Второй плюс: вы не несете постоянных дополнительных затрат на идентификаторы (карты доступа), носителем идентификатора является сам человек. Уровень технологий ведущих производителей данных решений позволяет оперировать большим количеством пользователей без значительных потерь скорости обработки.

Сергей Ефремов, дормакаба Евразия

Стандартно – RFID: карты доступа никуда не денутся и все еще являются основным средством идентификации, имеет смысл изучить рынок производителей чипов для карт, чтобы понять, какие производства локализованы, и сфокусироваться на соответствующих типах карт.

Далее – Face Recognition. Это перспективная технология, в России есть хорошие алгоритмы распознавания, вероятно со временем она вытеснит все другие виды биометрической идентификации.

Биометрическая идентификация на сегодняшний момент предоставляет более надежный способ идентификации пользователей, а также позволяет избежать мошенничества. Второй плюс: вы не несете постоянных дополнительных затрат на идентификаторы (карты доступа), носителем идентификатора является сам человек. Уровень технологий ведущих производителей данных решений позволяет оперировать большим количеством пользователей без значительных потерь скорости обработки

Вероятно, Face Recognition со временем вытеснит все другие виды биометрической идентификации

Mobile Identification также удобный способ идентификации, хорошая защита от передачи пропуска третьим лицам. К преимуществам мобильной идентификации также можно отнести возможность удаленно передавать права доступа на телефон, что может быть очень полезным в случае территориально удаленных объектов, не имеющих постоянной связи с "большой землей".

Идентификация по картам MIFARE Plus, DESFire становится все сложнее из-за проблем с их поставками от производителя NXP Semiconductors. На данный момент возможно использование решений от EM Marine или MIFARE Classic, но есть существенный минус: они не защищены от копирования

Артем Старшинов, Sigur

Идентификация по картам MIFARE Plus, DESFire становится все сложнее из-за проблем с их поставками от производителя NXP Semiconductors. На данный момент возможно использование решений от EM Marine или MIFARE Classic, но есть существенный минус: они не защищены от копирования.

Сегодня повышенный интерес вызывают биометрические технологии и виртуальные идентификаторы, например идентификация по смартфону.

Отсутствие физического идентификатора обладает большим набором преимуществ, таких как защита от копирования, меньшая вероятность потерять его, удобство использования и т.д.

Для посетителей крупных объектов набирает популярность отправка QR- или штрихкода посетителю. Это удобно, но менее безопасно. Поэтому, с учетом юридической обстановки относительно биометрии, самый оптимальный способ – идентификация по смартфону, а там, где нельзя ее использовать, – идентификационные карты.

Сергей Сорокин, ТерраЛинк

Общий тренд – бесконтактные технологии идентификации. С точки зрения перспективности использования идентификаторов следует обратить внимание на биометрию (в частности, на аутентификацию по лицу) и использование смартфонов. При этом нужно рассматривать варианты использования на смартфоне как постоянных меток для сотрудников, так и временных QR-кодов для посетителей. Использование RFID-карт с различной технологией защиты данных от копирования в настоящее время очень сильно распространено. Они будут применяться еще на многих объектах какое-то время. Но в использовании RFID-карт есть ряд проблемных моментов. Например, если у заказчика есть задача, связанная с учетом рабочего времени, то сложно исключить передачу личной RFID-карты другому сотруднику. И как результат, данные в системе учета рабочего времени (УРВ) будут неактуальны. Очень часты также случаи утери и поломки RFID-карт. Если эти моменты рассматривать в сравнении с использованием личного мобильного телефона в качестве идентификатора, то к сохранности личного смартфона и данных на нем люди относятся более внимательно.

Денис Иванов, Итриум СПб

Очевидно, потребителям нужно обращать внимание на те технологии, которые не являются проприетарными иностранными, то есть доступ к которым не может быть внезапно ограничен. Можно вспомнить уход с рынка одного из ведущих производителей считывателей и карт, у которого была возможность закрепить за потребителем определенный формат карт; теперь такой потребитель не знает, что ему делать. Но здесь, помимо технологии идентификации, интересным фактом являются еще и попытки распространить использование OSDP для связи контроллеров СКУД с периферийным оборудованием (в первую очередь считывателями, но технически можно также работать и с замками, и с герконами) – OSDP как раз проприетарная технология с ограниченной доступностью средств разработки и развития.

Как вы оцениваете текущую правовую ситуацию в области биометрической идентификации в крупных проектах? Готовы посоветовать биометрию потребителю?

В разделах нормативных документов касательно использования биометрии в СКУД важно обратить внимание на необходимые параметры защиты и шифрования шаблона лица, используемого в системе на различных этапах, защиты данных на биометрических считывателях и контроллерах в случае их воровства

Алексей Гинце, ААМ Системз

Основными законами, которые затрагивают сферу биометрии, являются 152-ФЗ (о персональных данных) и 149-ФЗ (о защите информации). Настоятельно рекомендую с ними ознакомиться (для начала), поскольку незнание норм не освобождает от ответственности. Важно также следить за всеми дополнительными подзаконными актами и разъяснениями Минцифры. В целом ситуацию оцениваю как не полностью прозрачную в правовом плане и рекомендую внимательно и придирчиво проверять каждую новую систему перед ее внедрением на предмет максимального соответствия правовым нормам. Рекомендую привлекать на этапе проектирования не только технических экспертов, но и грамотных юристов, дабы избежать правовых коллизий в будущем.

Олег Тихонов, АРМО-Системы

Биометрические решения мы не только советуем, но и активно применяем в проектах наших заказчиков. Если оценивать правовую сторону, то полной ясности по этому вопросу мы пока не обрели. Но определенно можно сказать, что существует весьма большое число объектов, на которых возможна реализация биометрических СКУД без дополнительных действий клиента в плане их приведения в соответствие законодательной базе. Это системы контроля доступа, предназначенные для внутренних нужд предприятий, и здесь достаточно простого согласия пользователей на использование биометрических методов идентификации.

Максим Горяченков, НВП "Болид"

Пока не вполне понятен порядок применения положений 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных" к СКУД. Закон содержит ст. 13, регламентирующую биометрическую идентификацию и аутентификацию при проходе на территорию ряда предприятий, связанных с оборонно-промышленным комплексом (ОПК), атомной и химической промышленностью, ТЭК, транспортной инфраструктурой и т.п. с использованием Единой биометрической системы (ЕБС). Проход на гражданские объекты явным образом законом не регламентирован. При этом ст. 15 запрещает сбор биометрических персональных данных для любых целей, кроме передачи этих данных в ЕБС в установленном порядке.

Будут ли положения этого закона распространяться на все объекты, оборудованные СКУД, покажет ближайшее время. Если да, то рынок ждет серьезная трансформация.

Сергей Ефремов, дормакаба Евразия

Правовые вопросы лежат вне моих компетенций, но в целом я пока еще с некоторым подозрением отношусь к возможности полного перехода на биометрию в крупных проектах. Как мы все знаем, биометрия – это вероятностный признак, и чем больше база персонала, тем больше шансов на ошибку.

Артем Старшинов, Sigur

На текущий момент государство пытается внедрить контроль безопасности персональных данных, в частности биометрических идентификаторов.

Такой подход в целом оправдан для защиты персональных данных граждан, но дело в том, что крупные негосударственные организации в любом случае несут ответственность за хранение персональных и биометрических данных своих сотрудников. Поэтому, на наш взгляд, не совсем корректно ограничивать их в хранении этих данных.

Сейчас возникает действительно много вопросов: какие будут санкции для предприятий, не выполняющих требования ЕБС, но защищающих свои данные самостоятельно, будет ли ситуация касаться СКУД, не изменится ли время идентификации.

Биометрия все еще является удобной и актуальной с точки зрения СКУД, с совершенствованием алгоритмов распознавания ее возможное применение будет только расти.

Мы считаем, что должен быть баланс между удобством использования биометрии и безопасностью хранения персональных данных. Если условие безопасности выполняется, то в таком случае да, биометрия – отличный вариант.

Сергей Сорокин, ТерраЛинк

Требуется более качественная проработка как технической, так и организационной составляющей нормативных документов по защите и использованию персональных данных. В частности, в разделах нормативных документов касательно использования биометрии в СКУД важно обратить внимание на необходимые параметры защиты и шифрования шаблона лица, используемого в системе на различных этапах, защиты данных на биометрических считывателях и контроллерах в случае их воровства.

Сейчас уже на многих объектах используется биометрическая идентификация. Это закономерный шаг в развитии способа идентификации как таковой. Есть много поставщиков и аппаратно-программных средств для биометрической идентификации. Главное – при выборе внимательно оценить параметры надежности, скорости работы, защищенности предлагаемого решения, а также надежность поставщика и его положение на рынке.

Денис Иванов, Итриум СПб

Со своей точки зрения в случае биометрии: у большого количества клиентов мы часто наблюдаем плохое понимание того, с чем они фактически имеют дело. Биометрия в системе может не храниться, так как в реальности используются биометрические шаблоны – некоторые математические модели, из которых сам биометрический признак не восстановить. Кроме того, часто возникают вопросы о соответствии оборудования или программного обеспечения (ПО) требованиям законодательства в части обработки персональных данных (ПД), хотя ни контроллер, ни считыватель, ни ПО не являются операторами ПД, да и биометрический шаблон сам по себе, без привязки к конкретному человеку, вряд ли является ПД.

Поэтому выдача любых рекомендаций по применению биометрии требует предварительной длительной разъяснительной работы. Дополнительно отмечу, что сама применимость биометрических технологий может сталкиваться с существенными ограничениями. Так, пандемия COVID-19 показала, что многие биометрические решения в ее условиях оказались плохо применимы. Отпечатки пальцев требуют контактной идентификации. Сканированию вен ладоней мешает требование использовать перчатки. Эффективность распознавания лиц значительно снижается при ношении масок (или вовсе перестает работать, если к маске добавить еще очки и низко надвинутую шапку). Сканирование сетчатки или радужной оболочки глаза – пока скорее дорогие уникальные решения со своими ограничениями и сложностями.

Существует весьма большое число объектов, на которых возможна реализация биометрических СКУД без дополнительных действий клиента в плане их приведения в соответствие законодательной базе. Это системы контроля доступа, предназначенные для внутренних нужд предприятий, и здесь достаточно простого согласия пользователей на использование биометрических методов идентификации

Новое семейство многофункциональных контроллеров СКУД и ОТС – БОРЕЙ

Представляет ООО "Итриум СПб" www.itrium.ru

ИТРИУМ
Создаём историю инноваций с 1994 года

Решаемые задачи

Контроллеры БОРЕЙ производятся более 10 лет и отлично зарекомендовали себя в системах самого разного размера и назначения, от больших офисов до международных аэропортов и промышленных предприятий с сотнями точек доступа, на необслуживаемых объектах и в высоконагруженных системах. Весь наработанный опыт решения разнообразных задач, в том числе уникальных, был учтен при разработке семейства контроллеров БОРЕЙ нового поколения.

Появление на рынке	2023 г.
Ценовой сегмент	Средний и высокий

Конкурентные преимущества

Новый БОРЕЙ обладает значительно большими вычислительными ресурсами и обеспечивает еще большую гибкость и адаптацию под процессы конкретного предприятия. Стали проще монтаж и обслуживание, расширен спектр решаемых задач СКУД, управления ОТС, интеграции и других – любой сложности, специфики и масштаба. Современный кросс-платформенный HTTP-API позволяет просто и эффективно решать самые разнообразные, в том числе уникальные, интеграционные задачи. Разработаны готовые интегрированные решения для задач автоКПП, шлюзового доступа, биометрической идентификации и взаимодействия с системами управления предприятием.

Что оценят покупатели

- Наличие операционной системы и всех необходимых веб-приложений "на борту".
- От 1 до 34 точек доступа, от 8 до почти 200 охранных шлейфов.
- Встроенный сетевой коммутатор, обеспечивающий большую свободу выбора топологии сети передачи данных.
- Возможность модернизации существующих систем с сохранением кабельной инфраструктуры.
- Встроенный веб-сервер для настройки, конфигурирования и управления.
- Встроенные средства автоматического межконтроллерного взаимодействия.
- Построение систем любого масштаба путем простого добавления контроллеров.
- Возможность настройки уникальных алгоритмов доступа любой сложности и серьезной модификации.
- Открытая платформа, обеспечивающая управление внешними устройствами (ключница, АКХ, Modbus и т.д.) и создание новых приложений.
- Возможность работы без применения специального серверного программного обеспечения.
- "Из коробки" готов к работе в составе КСБ НЕЙРОСС, в том числе совместно с контроллерами предыдущего поколения. ■

см. стр. 127 "Ньюсмейкеры"

Что наиболее критично для правильного функционирования распределенных СКУД – программное обеспечение или аппаратная часть (контроллеры)?

Алексей Гинце, ААМ Системз

Важным будет и программная, и аппаратная составляющая, однако первая мне представляется более важной. Можно даже сказать, что для СКУД крупных и особенно крупных распределенных систем критически важными будут характеристики именно программного обеспечения. В таких системах недостаточно будет обойтись простой синхронизацией баз данных отдельных филиалов. ПО для такой системы должны обеспечивать:

- единое пространство администрирования (настройка рабочих мест и оборудования в удаленных филиалах);
- единое кадровое пространство (актуальность данных сотрудников в филиалах, назначение прав доступа в филиалы из центрального офиса);
- единое информационное пространство (получение отчетов о событиях в любой точке системы);
- общее пространство управления (управление из центра оборудованием в удаленных филиалах);
- единое пространство мониторинга (мониторинг событий в удаленных филиалах).

Что касается контроллеров, то они прежде всего должны соответствовать требуемой мощности для использования в крупной распределенной СКУД. Контроллеры должны иметь базовый набор интерфейсов связи и обладать необходимой защитой от перехвата трафика как между отдельными устройствами, так и между филиалами.

Олег Тихонов, АРМО-Системы

В распределенной системе все важно: и ПО, и железо, я бы даже сказал, что одно без другого не живет. А критическая ситуация может сложиться в любом узле системы. На мой взгляд, здесь наиболее актуальна организация стабильного канала связи, наличие которого существенно облегчает решение всех задач, возникающих при реализации распределенных проектов.

Аркадий Гамбург, Семь печатей

Надежность программно-аппаратного комплекса обеспечивается прежде всего именно его аппаратной составляющей.

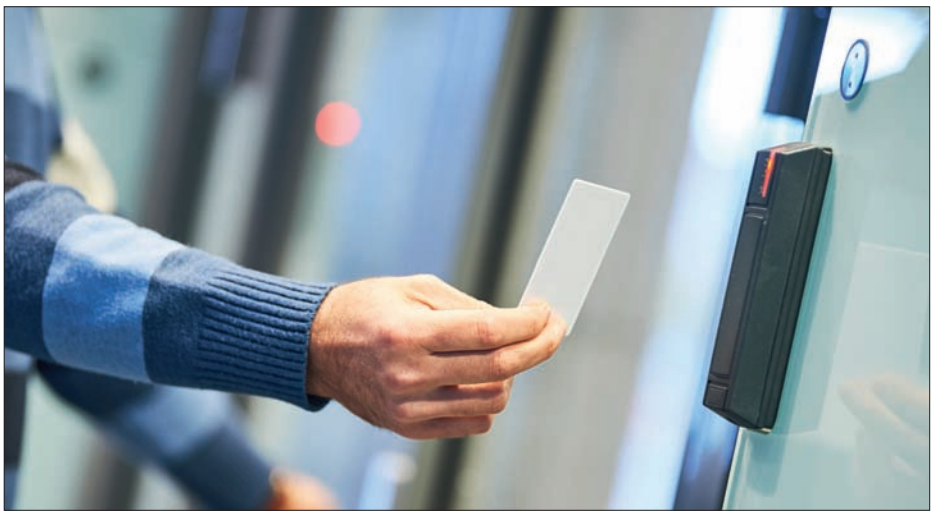
Работоспособность системы в комплексном режиме (то есть под управлением программного обеспечения) зависит от многих факторов: линий связи, локальной вычислительной сети (ЛВС), компьютеров, их операционных систем, специалистов, обслуживающих все это хозяйство... Естественно, что при возникновении проблем в одном из этих звеньев вся система рушится.

Автономный же режим зависит (точнее, должен зависеть) только от работоспособности одного управляющего устройства – контроллера. Контроллер (точнее, *правильный* контроллер) имеет память ключей и событий, хранит временные и пространственные ограничения и принимает решение о допуске как минимум по алгоритму "кого, куда и когда пускать", то есть полностью управляет "своими" пунктами прохода без серверного ПО.

Несомненно, программное обеспечение в современных системах очень важно – это онлайн-мониторинг, ввод данных, аналитика, интеграция. Но для всего этого кратковременный сбой – минуты и даже часы не столь критичен.

А вот аналогичный и даже еще более кратковременный сбой для организации доступа недопустим: все пункты прохода на объекте будут заблокированы. И чем система крупнее, тем недопустимее эта ситуация.

Поэтому заказчик обязательно должен требовать от поставщика СКУД обеспечения именно автономности проходов, с демонстрацией и с периодической проверкой этого режима.



В случае выбора RFID следует обратить внимание на смарт-идентификацию (13,56 МГц) как наиболее защищенную

Максим Горяченков, НВП "Болид"

На мой взгляд, качество и ПО, и контроллеров является одинаково важным фактором.

Если ПО работает идеально (прописывает идентификаторы в контроллеры, собирает с них данные и т.п.), а сами контроллеры не могут обеспечить должную пропускную способность или просто работают нестабильно, то, с точки зрения рядового пользователя, такая система будет неработоспособна.

Если контроллеры работают идеально, а ПО, например, теряет часть событий от контроллеров или не может корректно прописать в них новых пользователей и т.п., то такую систему тоже нельзя назвать работоспособной.

Все компоненты должны качественно решать свои задачи.

Ольга Жабрева, АВИКС ДЦ

Я думаю, что и программное обеспечение, и аппаратная часть имеют решающее значение для правильного функционирования распределенных систем управления доступом. Без совместной работы обоих компонентов система не сможет функционировать должным образом. Но монтаж и пусконаладка также играют важную роль для дальнейшего функционирования системы. Я все больше склоняюсь к мнению, что главное – качественный монтаж с соблюдением всех требований производителя и квалифицированная настройка. И тогда заявленный функционал системы будет обеспечен.

Вы можете купить ПО, контроллеры и периферию от самых топовых производителей. Но если установить это все с использованием неквалифицированной рабочей силы ("кривых рук"), то у вас в системе будут появляться "глюки". Например, из-за вибраций может отходить контакт, что, в свою очередь, будет приводить к потере связи ПО с элементами СКУД, перезагрузке некоторых элементов системы, одним словом система начнет работать нештатно. Вы будете грешить на систему, а виной всему отходящий кабель. Выловить причины такой работы – это занимает время, силы, а также накаляет атмосферу между заказчиком и производителем. Как говорил Генри Форд, "разочарование от низкого качества длится дольше, чем радость от низкой цены".

Сергей Ефремов, дормакаба Евразия

Распределенная СКУД настолько надежна, насколько надежен самый слабый ее элемент. И архитектура программного обеспечения, и контроллеры должны изначально создаваться с учетом особенностей распределенных систем – потенциальных проблем на линиях связи, проблем с синхронизацией данных. В действительно распределенной системе на каждом из уровней должны быть реализованы механизмы резервирования и нормального функционирования при отключении головного компонента соответствующего уровня.

Артем Старшинов, Sigur

Для правильного функционирование распределенной СКУД должно быть качественное взаимодействие между программным обеспечением и аппаратной частью.

Очень многое завязано на функционале, который требуется от СКУД на конкретном предприятии. Если это вопрос только обеспечения доступа, без бизнес-логик и их отработки, то это решается силами аппаратной части, и она обязана функционировать автономно.

Если же на объекте основным функционалом СКУД является взаимодействие с верхнеуровневыми системами, которые обеспечивают выполнение бизнес-процессов предприятия, то тут главную роль играет программное обеспечение, которое обеспечивает связь и конвертацию бизнес-задач в понятные требования СКУД для аппаратных устройств.

Сейчас мы наблюдаем, что все больше ответственности переходит на сторону ПО, так как это отвечает задачам бизнеса.

Сергей Сорокин, ТерраЛинк

Все зависит от объекта и задач заказчика по обеспечению безопасности. В целом одинаково важно использовать и надежные идентификаторы, и считыватели, и контроллеры, и сетевую инфраструктуру, и программное обеспечение.

И программное обеспечение, и аппаратная часть имеют решающее значение для правильного функционирования распределенных систем управления доступом. Без совместной работы обоих компонентов система не сможет функционировать должным образом. Но монтаж и пусконаладка также играют важную роль

Денис Иванов, Итриум СПб

Для любой системы, а в особенности для распределенной, критичен правильный выбор всех элементов, в частности контроллеров и ПО (на самом деле не только их). Начнем с контроллеров. Допустим, ошиблись с их выбором. Вероятны минимум две возможные проблемы:

- задержки при массовых проходах и/или больших базах пропусков из-за низкой производительности контроллеров;
- невозможность настроить логику работы контроллера в соответствии со специфическими требованиями, регламентами и процедурами предприятия. Ошибка при выборе контроллеров потребует менять уже регламенты и бизнес-процессы, возможно с ущербом для безопасности.

Неправильный подбор ПО приводит к следующему:

- неготовность ПО к работе в распределенной системе (например, всегда должен быть один и только один сервер, или же серверов может быть несколько, но невозможно задать их иерархию, определить правила синхронизации данных и т.д.) – это серьезно ограничивает возможности управления пропусками и режимом, может негативно влиять на надежность системы, предъявлять повышенные требования к каналам связи и т.д.;
- неготовность к встраиванию в бизнес-процессы предприятия (отсутствие документированных интерфейсов информационного взаимодействия или готовых модулей для системной интеграции) серьезно снижает экономическую эффективность внедрения СКУД и объем получаемой от нее пользы;
- неготовность к работе с большими объемами данных (распределенные системы, как правило, крупномасштабные) – результатом будет медленная или нестабильная работа и снижение эффективности всех бизнес-процессов, связанных со СКУД: получения пропусков в бюро пропусков, работы с отчетностью и т.д.

Распределенная СКУД настолько надежна, насколько надежен самый слабый ее элемент. И архитектура программного обеспечения, и контроллеры должны изначально создаваться с учетом особенностей распределенных систем – потенциальных проблем на линиях связи, проблем с синхронизацией данных