

# КАКОВА РОЛЬ СКУД В СОСТАВЕ ИСБ? ВЗГЛЯД РАЗРАБОТЧИКОВ

**М. Куляс**

ведущий инженер компании «ЕС-Пром»,

**О. Батманов**

начальник отдела разработок компании «ЕС-Пром»,

**Ю. Суконщиков**

начальник отдела продвижения продукции компании «ЕС-Пром»

*Когда коллектив компании «ЕС-Пром» получил задание от редакции журнала «Алгоритм безопасности» подготовить статью о роли СКУД в интегрированной системе безопасности, возникла дискуссия на тему: «Насколько важна система контроля доступа в составе ИСБ? Является ее роль ведущей или вспомогательной?» В итоге обсуждения все привлеченные специалисты пришли к единодушному мнению о том, что СКУД – основа безопасности предприятия, и ее целесообразно использовать в качестве «ядра» создаваемой на объекте ИСБ, причем каждый из участников дискуссии привел свои весомые аргументы в пользу этого утверждения, из которых в итоге и родилась данная статья.*

## **Куляс Максим Олегович, ведущий инженер:**

Традиционный подход к построению ИСБ основан на теории обнаружения и локализации угроз проникновения, при этом основным рубежом защиты считается внешний периметр объекта. Существующие методики анализа эффективности систем безопасности предполагают в качестве основной угрозы нападение вооруженной группы или экстремиста-одиночки, соответственно первой по значимости системой в составе ИСБ ставится система обнаружения вторжения в составе СОП, СОТ, ОС. Такой подход актуален при анализе уязвимости особо охраняемых объектов, где действительно быстрое и достоверное обнаружение проникновения является залогом эффективности ИСБ.

Однако на большинстве предприятий, в повседневной практике, руководитель службы безопасности вряд ли столкнется с террористической угрозой, в то же время ему ежедневно приходится иметь дело с более «приземленными» событиями – это хищения, нарушения распорядка, проход на территорию посторонних лиц, выход на работу в нетрезвом состоянии.

Системы охраны, основанные на традиционных средствах обнаружения,

здесь не помогут. Нисколько не умаляя роль надежной охраны внешних границ, можно сказать, что значимость системы контроля доступа в составе комплекса безопасности на таких объектах выходит на первый план. И это подтверждается практикой – многие заказчики начинают создание интегрированной системы безопасности со СКУД, так как ее внедрение дает ряд новых возможностей, положительно сказывающихся не только на безопасности, но и на других аспектах ведения бизнеса:

- повышение трудовой и технологической дисциплины;
- рациональное расходование фонда заработной платы (оплата только реально отработанного времени);
- сокращение трудозатрат на ведение табельного учета, кадрового учета и выдачу пропусков;
- сокращение объемов хищений;
- повышение имиджа предприятия.

Обычно СКУД принято рассматривать как элемент организационной структуры, и ее роль как подсистемы безопасности, на первый взгляд, не очевидна. Для надежной защиты объекта в первую очередь необходимо обеспечить равноудовлетворенность его рубежей. И если бы на объекте не предполагалось наличие персонала, с его защитой замечательно бы

справилась система охраны периметра. На реальных объектах эта система тоже выполняет свою роль, как в плане задержания нарушителей, так и в плане сдерживания. Но наиболее уязвимым местом в системе защиты становятся точки прохода людей и проезда транспорта.

Применение СКУД актуально не только на внешних рубежах – проходных предприятия. В зданиях и помещениях СКУД обеспечивает защиту объекта днем, в рабочее время, когда другие системы охраны отключены, – отсекает посторонних людей на входе в здание, не допускает вход человека в помещение, если он не имеет соответствующих прав. При попытке нарушения правил прохода система формирует сигнал тревоги.

Обеспечение автоматического прохода персонала по электронным идентификаторам – основная функция СКУД. При этом на объект не допускаются посторонние лица, не имеющие пропуска предприятия. В современных системах, кроме этого, имеется ряд возможностей для более строгого контроля прохода, что снижает вероятность проникновения путем обмана или обхода системы.

Использование копий (клонов) действующих карт доступа – распространенная сегодня проблема, «чистые» карты можно купить и запрограммировать совершенно свободно. Проблема решается двумя путями – обнаружение по особым признакам клонированных карт при входе или применение карт с более совершенной технологией защиты внутренних данных, например, смарт-карт Mifare® вместо распространенных и дешевых EM-Marine®.

Такая функция, как фотоидентификация (отображение фотографии владельца), позволяет обнаружить попытки прохода по чужим картам. Немаловажное значение для проходных предприятия имеет функция запрета повторного прохода, или «anti-pass-back». Во-первых, исключаются попытки провести с собой «друга» по одной и той же карте, а во-вторых – становится возможным обнаружить и пресечь некорректные последовательности входа и выхода, которые зачастую связаны с другими, более серьезными нарушениями.

Примеры из реального опыта эксплуатации систем контроля доступа отлично показывают эффективность СКУД в решении повседневных задач поддержания безопасности. На одном из предприятий, при проведении плановых работ на производственном оборудовании, обнаружилась пропая силовой кабеля, который был отрезан и похищен, будучи в обесточенном состоянии. На следующий день на проходной охрана задержала сотрудника, которого система не пропустила на работу, так как он не выходил через турникет вечером преды-

дущего дня. При выяснении причин отказа в доступе обнаружилось, что сотрудник через проходную действительно не выходил (что было проверено по архиву системы видеонаблюдения). Перед лицом объективных фактов сотрудник признался в хищении кабеля, с которым он в тот день покинул территорию через дыру в ограждении. Поскольку внедрение СКУД привело к повышению оперативного внимания к попавшим таким образом в поле зрения работников, воровство на предприятии значительно сократилось.

Как видно из этого примера, важную роль в поддержании безопасности имеет интеграция СКУД с системами видеонаблюдения, которые позволяют восстанавливать события в точках прохода при проведении расследований.

Необходимая функция СКУД – протоколирование событий входа и выхода, а также действий персонала охраны проходных по ручному управлению точками прохода. В совокупности с информацией систем наблюдения это позволяет обнаружить, например, несанкционированный выезд транспорта через КПП (что обычно также связано с хищениями). Кроме того, протокол событий позволяет контролировать перемещение сотрудников по территории объекта.

Так, один из работников подозревался в регулярных хищениях дорогостоящих материалов. При анализе протокола событий СКУД (рис. 1) выяснилось, что время от времени этот сотрудник выходил через проходную гораздо позже, чем покидал свое рабочее место. В один из таких дней работник был задержан в удаленной точке территории при передаче сообщникам похищенных ценностей через забор.

Помимо решения задач, связанных с контролем прохода и регистрацией собы-

тий, СКУД защищает здания и помещения в нерабочее время. Аппаратные возможности контроллеров доступа позволяют легко реализовать функции приемно-контрольного прибора охранной сигнализации. Практически все современные СКУД имеют возможность подключения охранных шлейфов. Это позволяет одновременно обеспечивать контроль доступа и охрану помещения на базе одного прибора, что снижает затраты на создание ИСБ. При этом СКУД и ОС создаются одновременно, что сокращает время монтажа, снижает стоимость оборудования, упрощает пусконаладку и последующую эксплуатацию системы безопасности.

Контроллер доступа имеет весь набор возможностей, необходимых для прибора охранной сигнализации, – входы для подключения датчиков (в том числе с контролем сопротивления шлейфа), источник резервного питания, выходы для управления оповещателями и линиями ПЦН. Постановка и снятие помещений с охраны может выполняться как с помощью карт доступа, так и дистанционно с выносных пультов или с компьютеров дежурной смены службы безопасности. При этом возможна интеграция с системами видеонаблюдения, как на программном, так и на аппаратном уровнях.

**Батманов Олег Анатольевич, начальник отдела разработок:**

За последние годы системы КУД получили широкое распространение. Значительно увеличилось количество помещений, оснащаемых контролем прохода, стандартной стала задача оснащения проходных предприятий системой электронной идентификации, возрос функционал и мощность предлагаемых на рынке систем. Сейчас привычными и

Рис. 1. Протокол событий СКУД. Слишком большое время между уходом из цеха и выходом с территории – повод для привлечения внимания к сотруднику

Фамилия	Имя	Событие	Время	Источник события
Ильина	Ирина	Штатный вход	26.12.2013 10:05:38	Проездная
Ильина	Ирина	Штатный вход	26.12.2013 10:59:50	Проездная
Ильина	Ирина	Штатный вход	26.12.2013 10:59:55	10 Цех
Мисеев	Павел	Предоставление доступа на выход	26.12.2013 11:02:20	10 Цех
Мисеев	Павел	Штатный выход	26.12.2013 11:02:20	10 Цех
Мисеев	Павел	Предоставление доступа на выход	26.12.2013 11:02:38	Проездная
Мисеев	Павел	Штатный выход	26.12.2013 11:02:38	Проездная
Николаев	Тимофей	Штатный вход	26.12.2013 10:55:13	Проездная
Николаев	Тимофей	Штатный вход	26.12.2013 10:55:13	10 Цех
Николаев	Тимофей	Предоставление доступа на выход	26.12.2013 11:04:53	10 Цех
Николаев	Тимофей	Штатный выход	26.12.2013 11:04:53	10 Цех
Николаев	Тимофей	Предоставление доступа на выход	26.12.2013 11:04:55	Проездная
Николаев	Тимофей	Штатный выход	26.12.2013 11:04:55	Проездная
Петров	Константин	Штатный вход	26.12.2013 12:07:12	Проездная
Петров	Константин	Штатный вход	26.12.2013 10:11:53	10 Цех
Петров	Константин	Штатный вход	26.12.2013 11:15:12	Проездная
Прокофьев	Виталий	Отказ в доступе на выход - нет прав	26.12.2013 10:39:02	10 Цех
Прокофьев	Виталий	Штатный выход	26.12.2013 10:45:12	10 Цех
Прокофьев	Виталий	Штатный выход	26.12.2013 12:22:12	Проездная
Фролов	Игорь	Штатный выход	26.12.2013 10:45:12	10 Цех
Фролов	Игорь	Штатный выход	26.12.2013 10:48:41	Проездная
Фролов	Игорь	Штатный вход	26.12.2013 10:51:31	Проездная

востребованными стали функции учета рабочего времени, контроля последовательности прохода, подготовки и печати отчетов с фильтрацией и группировкой результатов по множеству критериев. В то же время, другие подсистемы безопасности также развивались.

Средства охранной сигнализации стали функциональнее и удобнее. Ушла в прошлое обязательная необходимость управления режимом охраны нажатием кнопки на приборах или набором кода на пультах управления. Идентификация пользователя и управление постановкой/снятием с охраны с графического плана объекта сейчас может выполняться по предъявлению бесконтактного идентификатора оператором, автоматически по заданным временным расписаниям или событиям в других зонах охраны.

Массово начали внедряться видеосистемы, число доступных зон видеоконтроля резко увеличилось, изменились технологии реализации устройств обработки и каналы передачи информации, возросло качество изображения, увеличились объемы видеоархивов и длительность непрерывной записи. Современные системы видеонаблюдения выполняют разнообразные задачи оперативной аналитики, включающей распознавание номеров автомобилей, идентификацию по изображению лица, детекторы оставленных и исчезнувших предметов, постоянно совершенствуются ставшие уже привычными детекторы движения.

Изменило ли текущее состояние функционала средств безопасности ведущую роль СКУД в ИСБ? Общий взгляд на наиболее известные представленные на рынке продукты позволяет по-

ложительно ответить на этот вопрос. Но так ли это на самом деле?

Для более глубокой оценки ситуации необходимо еще раз сформулировать главные задачи ИСБ:

- Предоставление оператору достоверной, оперативной и достаточной для анализа ситуации информации с привязкой к месту возникновения события (рис. 2).
- Обеспечение возможности быстрого доступа к дополнительной информации, полученной от других подсистем ИСБ и позволяющей принять более эффективные решения по противодействию угрозам.
- Повышение удобства расследования произошедших инцидентов за счет формирования информативных отчетов по событиям с различными критериями отбора, а так же обеспечение быстрого доступа к соответствующим архивным видеозаписям.

Первая задача решается использованием в качестве основного источника событий подсистем с минимальным уровнем ложных тревог и пропусков цели, предоставлением оператору единого пользовательского интерфейса для всех подсистем, отображением места тревоги на плане объекта, формированием понятных текстовых описаний источника события, развитыми алгоритмами взаимодействий подсистем при возникновении событий, отображением списка рекомендуемых действий.

Для решения второй задачи необходимо обеспечить формирование событий по каждому факту нарушения, отображение сопутствующих событий, фиксацию точного времени возникновения события и возможность оперативного получения видеоизображения из тревожной зоны.

Третья задача решается за счет развитых средств формирования отчетов с фильтрацией и группировкой информации по времени, типу устройства, идентификатору пользователя и т.п., с возможностью просмотра архивных видеозаписей для каждого выбранного события с привязкой по времени и с учетом размещения видеокамер на объекте.

Теоретически, каждая из основных современных подсистем ИСБ – КУД, ОПС, видеонаблюдения может быть ведущей, однако, оптимальной будет та из них, которая более органично вписывается в задачи интеграции. Для определения этого необходимо оценить ключевые параметры каждой из систем.

Система видеонаблюдения обладает самой высокой информативностью, так как в реальном времени позволяет проследить развитие ситуации, оценить степень угрозы или идентифицировать нарушителя при расследовании. В процессе работы система может формировать события от детекторов движения и других модулей аналитики, позволяя инициировать выполнение взаимодействий в других подсистемах.

Различные детекторы нарушений хорошо работают в закрытых зонах и помещениях с достаточным уровнем освещения, где по умолчанию нет движущихся объектов, а их появление вызывает тревогу. При ухудшении условий видимости, при плохой освещенности, в туман, дождь или снег, а так же при наличии в зоне детекции постоянно присутствующих или случайных движущихся объектов, таких как ветки деревьев, яркие отблески автомобильных фар, возникает либо большое количество ложных тревог, либо, при снижении чувствительности, большая вероятность пропуска цели. Высокая информативность системы оказывается бесполезной при отсутствии привязки к конкретному промежутку времени и видеоканалу, так как постоянное эффективное наблюдение за несколькими десятками видеоизображений или последовательный просмотр видеоархива в поисках нарушителя практически невозможны.

Невысокая достоверность формируемых событий делает использование видеосистемы в качестве ведущей подсистемы в составе ИСБ нецелесообразной, однако ее наличие значительно повышает общую эффективность решения.

Системы ОПС обладают максимальной достоверностью, так как, при правильно выбранных извещателях, грамотном определении места их установки и надежности каналов передачи извещений, вероятность ложных тревог или пропуска цели стремится к нулю. Даже системы охраны периметра, на которые воздействуют различные погодные факторы, содержат необходимые алгоритмы

Рис. 2. С ростом масштабов и возможностей современных средств безопасности вопросы интеграции как никогда актуальны



минимизации помех и обеспечивают достаточные параметры достоверности. С другой стороны, информативность охраняемых систем не очень высока. Можно получить информацию о факте и месте нарушения, но никаких дополнительных сведений система не сформирует.

Также стоит учесть тот факт, что подсистемы ОПС рассчитаны на охрану помещений в нерабочее время, либо там, где не требуется постоянного присутствия персонала. Программное обеспечение подсистем ОПС обычно имеет хорошие возможности по протоколированию событий и формированию отчетов. Для них также важно обеспечение отображения информации на графическом плане объекта, так как точное определение места тревоги существенно повышает скорость реакции персонала охраны и эффективность принимаемых мер.

Дальнейшее повышение эффективности может быть достигнуто за счет получения видеoinформации с ближайших к месту события видеокамер, как в режиме оперативного наблюдения, так и при анализе ситуации в процессе расследования. В результате, подсистема ОПС вполне может быть ведущей в ИСБ объекта, на котором отсутствует или используется простая подсистема СКУД или установлена система видеонаблюдения.

СКУД является одной из наиболее сложных подсистем безопасности объекта. Ее информативность несколько ниже по сравнению с подсистемами видеонаблюдения, а достоверность соизмерима с подсистемами ОПС. Главное отличие СКУД от остальных подсистем заключается в круглосуточном контроле состояния точек прохода и обеспечении идентификации персонала. При этом точки доступа полноценной СКУД, оснащенные датчиками открытия, не только позволяют отследить фактический проход, но и обеспечивают формирование тревоги при нештатном преодолении или удержании в открытом состоянии преграждающего устройства. Кроме этого, профессиональные СКУД позволяют фиксировать и предотвращать попытки прохода в запрещенные зоны, отслеживать нарушения последовательности прохода (защита от передачи пропуска или «anti-pass-back»), нарушения разрешенного интервала времени входа и выхода. В особо ответственных зонах можно реализовать контроль и оповещение оператора о фактах прохода под принуждением.

Так как все события, сформированные системой, включая штатные, в обязательном порядке протоколируются, интенсивность поступления информационных сообщений и объем протокола событий в СКУД является максимальными среди всех рассмотренных подсистем.

В рабочее время, если не учитывать средства охраны периметра и закрытых для доступа персонала зон, СКУД является единственной системой, позволяющей организовать необходимую безопасность объекта. Совместно с подсистемами ОПС и видеонаблюдения можно значительно повысить общий уровень безопасности за счет развитых взаимодействий, таких как вывод изображений с заданных камер по тревогам и нарушениям правил прохода, разблокировку точек доступа при пожаре, ограничения доступа при получении тревожного события, постановку или снятие с охраны заданных зон или разделов при предъявлении отдельных категорий пропусков.

Для базового программного обеспечения СКУД важно иметь возможность отображения точек доступа на графическом плане объекта для оперативного управления их режимами работы оператором системы. С учетом сложности реализации алгоритмов доступа, высоких требований к аналитическим возможностям модулей подготовки отчетов и значительного объема обрабатываемых данных можно сделать вывод, что применение подсистем контроля доступа в качестве основы ИСБ наиболее эффективно вследствие возможности использования имеющихся в программном обеспечении наработок не только для СКУД, но и для других подсистем.

Если рассматривать программные продукты независимых интеграторов, то при их создании максимальный объем работ возникает именно при интеграции подсистем КУД. Причем, чем мощнее и гибче интегрируемая подсистема, тем сложнее реализация имеющихся в системе функций. Интеграция же других подсистем, как правило, проще, при условии, что уровень функционала, с учетом категории подсистем, приблизительно одинаков.

#### **Суконщиков Юрий Геннадьевич, начальник отдела продвижения продукции:**

Не стоит забывать, что создание и внедрение интегрированной системы безопасности не является самоцелью. Главная, если не единственная задача, стоящая перед ИСБ, – обеспечение эффективного функционирования предприятия в условиях нестабильности внешней и внутренней среды. Решение этой задачи реализуется за счет воздействия на угрозы – потенциальные или реальные действия, события.

Повышение эффективности работы предприятия может достигаться как за счет экономии потребляемых ресурсов (сокращение текущих затрат), так и через более продуктивное использование действующего капитала и новых капиталовложений. Так как же ИСБ может рабо-

тать на повышение эффективности предприятия?

Предполагая соблюдение принципа экономической целесообразности при создании системы безопасности предприятия, можно прийти к выводу, что внедрение ИСБ не влечет сокращения текущих затрат и воздействовать на эффективность предприятия система безопасности может только в направлении увеличения КПД используемых средств.

Самый прямой путь повысить эффективность капиталовложений в безопасность – использовать ресурсы ИСБ для совершенствования управления предприятием. И в этом вопросе потенциал СКУД значительно превышает возможности остальных подсистем, главным образом за счет воздействия на организацию и дисциплину труда.

Под дисциплиной труда понимается обязанность работника соблюдать нормы и правила, регулирующие его трудовые отношения с работодателем и непосредственно сам процесс труда. В своей трудовой деятельности работник должен соблюдать три вида дисциплины:

- трудовая дисциплина – соблюдение норм трудового законодательства и правил внутреннего распорядка;
- технологическая дисциплина заключается в необходимости выполнения технологических инструкций, правил и стандартов, обеспечивающих качество производимой продукции;
- производственная дисциплина – обязанность соблюдения правил техники безопасности.

Главнейшая функция СКУД, гарантирующая этой системе встраивание в процесс обеспечения дисциплины труда, – наличие механизма задания строго определенного маршрута перемещения работника по предприятию. Большинство инструкций и правил представляют собой регламентированную последовательность действий, которые необходимо выполнить в определенном порядке, т.е. соблюдая заданный «маршрут». СКУД, должным образом настроенная, позволяет обеспечить неукоснительное (с протоколированием попыток отклонения!) соблюдение установленных правил.

Приведем в качестве иллюстрации несколько примеров из нашего опыта работы.

*Пример 1.* Простейший путь решения задачи по недопущению на территорию предприятия нетрезвых сотрудников (трудовая дисциплина, производственная дисциплина) – выявление лиц в состоянии алкогольного опьянения еще на проходной предприятия, фиксация и разбор случаев прохода на работу в нетрезвом виде. СКУД, как подсистема ИСБ, дополненная пороговыми алкотестерами (рис. 3) и запрограммированная на предоставление права на проход по двум



**Рис. 3.** Проходная, оснащенная средствами тестирования на алкоголь. Проход разрешается только после получения подтверждающего сигнала от алкотестера

признакам (персональный идентификатор и разрешающий сигнал алкотестера), в полной мере гарантирует соблюдение дисциплины труда в части избежания последствий, вызванных принятием алкоголя.

**Пример 2.** Приказом Министерства здравоохранения и социального развития РФ от 12.04.2011 № 302н утверждены перечни вредных и опасных производственных факторов и работ, при выполнении которых проводятся обязательные медицинские осмотры (норма трудового законодательства – трудовая дисциплина). Для предприятий, подпадающих под этот Приказ, выходом может служить использование СКУД, в «маршрут» которой включено обязательное посещение медкабинета. Попытка избежать такого осмотра приведет к возникновению события «нару-

шение последовательности прохода» и недопущению работника в зону проведения работ. Немаловажно и то, что зафиксированный в протоколе ИСБ список штатных проходов и попыток нарушения является надежной основой для оценки руководством предприятия и/или контролирующими органами соблюдения дисциплины труда.

**Пример 3.** Для автотранспортных предприятий и логистических компаний актуальна задача соблюдения порядка выезда автомобилей на линию (технологическая дисциплина, производственная дисциплина). Решение задачи обеспечивается установкой контроллеров СКУД в обязательных пунктах с программированием контроллеров для выполнения установленной последовательности технологического процесса в АТП.

**Таблица**

Вид нарушений		Количество нарушений	Суммарная недоработка, дни	Экономия ФОТ, руб.
Опоздания и ранние уходы	от 10 до 20 минут	574	11,96	17 467,00
	от 20 до 30 минут	939	39,13	57 148,00
	от 30 до 40 минут	467	29,19	42 631,00
	от 40 до 50 минут	601	50,08	73 141,00
	от 50 минут до часа	411	42,81	62 523,00
Прогулы		72	72	105 154,00
<b>Общая экономия по итогам одного месяца</b>				<b>358 064,00</b>

**Пример 4.** На многих предприятиях используется повременная заработная плата в зависимости от времени работы сотрудника и его квалификации. При наличии такой системы вопрос соблюдения трудового распорядка относится уже не только к дисциплине труда, но и к расходованию потребляемых ресурсов – фонда оплаты труда (ФОТ). Использование информации, полученной из протокола СКУД, о фактическом времени прихода и ухода работников позволяет исключить необоснованные выплаты заработной платы.

В качестве примера можно привести таблицу, основанную на фактических данных, предоставленных в службу технической поддержки нашей компании промышленным предприятием с численностью персонала около 5000 человек, и макроэкономическом параметре «среднемесячная номинальная начисленная заработная плата», который на дату написания статьи был равен 30 670 рублям.

Таким образом, СКУД не только позволяет улучшить управление предприятием, но и повысить его эффективность за счет экономии потребляемых ресурсов!

#### Вместо заключения

*Все озвученные в статье мнения сходятся на том, что СКУД в современных системах безопасности занимает центральное место. Однако, СКУД сама по себе, без взаимосвязи с другими системами, не способна полностью обеспечить безопасное состояние защищаемого объекта. Все другие технические подсистемы безопасности не менее важны, направлены на сокращение времени обнаружения угроз нападения/проникновения и, как следствие, к сокращению величины ущерба. По сути – вложение средств в безопасность работает как «страховка» для собственника. И только СКУД, благодаря своим уникальным возможностям, позволяет создать полноценную интегрированную систему безопасности, задействованную в основных бизнес-процессах предприятия.*