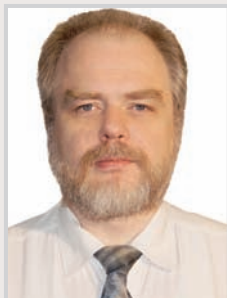


КОЛОНКА РЕДАКТОРА

Первая скрипка



В условиях постоянного роста террористических угроз в мире роль СКУД трудно переоценить. Если посмотреть правде в глаза, то из известного "трио" СКУД + ОПС + ССТV фактически именно СКУД способна ока-

зать активное противодействие террористической угрозе: не пустить кого не надо куда не надо. Это не означает, что другие системы чем-то плохи, просто для ССТV и ОПС основная задача – обнаружить и зафиксировать (задокументировать) событие – нарушение, тогда как для СКУД главным будет обеспечить на объекте совершение исключительно легитимных (санкционированных) действий.

Разумеется, это не значит, что СКУД решает все, – кофе она не сварит и от хакерской атаки вряд ли защитит. Зато эффективно решит вопросы, связанные с перемещением персонала, посетителей, транспортных средств и иногда грузов. Особенно важна роль СКУД в вопросах защиты объектов, которые обеспечивают бесперебойное функционирование целых городов и даже регионов, а также объектов, связанных с опасными производствами. Простейший пример – станция водозабора, химкомбинат, атомная электростанция и пр. Конечно, защита такого объекта – сложный комплекс технических и организационных мер, но одна из первых скрипок в этом оркестре у СКУД. Недаром реализованных терактов на таких объектах во всем мире немного, даже с учетом до конца не подтвержденных случаев, вроде взрыва на химическом заводе AZF под Тулузой в 2001 г.

Следует отдельно отметить современный тренд на глубокую интеграцию СКУД не только с классическими системами безопасности, вроде ССТV и ОПС, но и с системами информационной безопасности (логический доступ), с системами управления предприятием (ERP), системами учета рабочего времени (УРВ) и пр. Фактически, на современном этапе развития СКУД можно рассматривать не только как элемент интегрированной системы безопасности (ИСБ) компании, но и как важную составляющую системы жизнедеятельности объекта в целом. Нельзя обойти вниманием удобство современных систем доступа, обеспечивающих идентификацию по различным биометрическим признакам, идентификацию по смартфону, идентификацию транспорта на большом расстоянии с помощью меток, по номеру и пр. СКУД становятся понятнее, ближе и удобнее людям, и это, безусловно, радует.

Алексей Гинце

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

СКУД как часть антитеррористической защиты критически важных объектов

Приходится констатировать: классические технические средства безопасности почти всегда запаздывают против грубой силы. Так, видеозапись события поможет при расследовании, но не предотвратит само событие. Охранная сигнализация успешно известит об уже произошедшем взрыве. Способна ли СКУД дать достойный отпор чуме XXI века?



Алексей Омелянчук

Начальник КБ "Рубикон"
ГК "Сигма"

Прямо скажем, реально бороться с терроризмом можно лишь оперативно-разыскными, агентурными и пропагандистскими мерами. Досмотровые системы – и металлоискатели на вокзалах, и рентген-аппараты в аэропортах – это по сути вспомогательные инструменты для оперативно-разыскной деятельности. Они прилагаются к специально обученным людям, осуществляющим по большей части неформально-

психологический скрининг человеческого потока. СКУД – единственная подсистема, которая реально предупреждает преступления, в том числе и террористического характера.

Нет так эффективно, зато эффективно

Да, СКУД также имеет очень ограниченное применение в случае террористической угрозы. Самые распространенные – публичные теракты в местах массового скопления людей – практически невозможно предотвратить в автоматическом режиме. Однако можно противодействовать менее эффективным, но чреватых значительно более катастрофическими последствиями попыткам воздействия на опасные предприятия (особенно многочисленным химическим), объекты жизнеобеспечения (в первую очередь водопровод) и другие особо важные объекты.

В новейшей истории не случилось успешных попыток террористических атак на химические предприятия. Неудачная была в прошлом году во Франции (Гренобль) и, предположительно, планировалась в Великобритании. По сообщениям ФСБ, в 2009 г. были предотвращены попытки атаки на московский водопровод. По сравнению с длинным перечнем громких



СКУД позволяет успешно противодействовать попыткам воздействия на объекты жизнеобеспечения



Служебные двери в аэропортах оснащены средствами СКУД, что не позволяет обойти металлоискатели и рентген-аппараты

взрывов и обстрелов это немного. Однако реализация любой из этих угроз могла бы на порядок превзойти самые страшные на сегодня события 11 сентября 2001 г.

Враг не пройдет

Чем же может помочь СКУД в борьбе с террористической угрозой? Как и всегда, СКУД держит двери на замке. Обратите внимание, в том же аэропорту большое количество людей занято борьбой с террористами, ведется сплошной досмотр пассажиров. При этом рядом имеются служебные двери, через которые можно обойти и металлоискатели, и рентген-аппараты. Но на любой из них стоит считыватель или кодонаторник. В результате один охранник обеспечивает контроль двадцати дверей, а иначе пришлось бы к каждой приставить отдельного охранника.

Конечно, это вопрос денег. И не говорите, что жизни людей бесценны, — можно измерять затраты не деньгами, а человеко-днями, результат тот же — если выделить дополнительные две сотни охранников на каждую станцию водоподготовки, то тогда на эти несколько тысяч человек придется уменьшить, скажем, штат механиков-лифтеров, проверяющих исправность лифтов. Это тоже жизни, тоже бесценные.

Еще серьезнее тот факт, что, призвав на помощь тысячи охранников, вы сами увеличиваете вероятность, что на объект попадет злоумышленник. Чем больше там сотрудников, тем труднее их всех проверить.

Защита объекта: не экономьте на спичках

Итак, система контроля доступа помогает повысить защиту объекта. Какая система для этого нужна? Не стоит гнаться за новинками, но уместно применять средства с повышенной защитой. Например, карты



Призыв на помощь тысячи охранников, вы сами увеличиваете вероятность, что на объект попадет злоумышленник

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

ПРИЕМНО-КОНТРОЛЬНЫЙ ПРИБОР С КОНТРОЛЕМ ДОСТУПА



C2000-4

4096
пользователей

15
окон времени

- Управление однонаправленной точкой доступа (вход по идентификатору, выход по кнопке)
- Полноценные охранные, пожарные и технологические шлейфы
- Поддержка считывателей с двойной идентификацией (Proximity-карта и PIN-код)
- Управление доступом и взятием/снятием при помощи одного идентификатора
- Интеллектуальный контроль двери при помощи геркона (контроль взлома и блокировки; подтверждение прохода; оптимизация времени управления замком)

BOLID

bolid.ru

2 дня, 180 брендов, Groteck
www.all-over-ip.ru
конвергенция индустрий,
внушительная база знаний,
CEO SUMMIT, ИНТЕЛЛЕКТУАЛЬНОЕ ЗДАНИЕ
ОТКРЫТЫЕ ПЛАТФОРМЫ
УПРАВЛЕНИЕ ИДЕНТИФИКАЦИЕЙ
ОБЛАЧНЫЕ РЕШЕНИЯ
день Bosch,
5000 покупателей,
5 конференций, ИНТЕРНЕТ ВЕЩЕЙ
БОЛЬШИЕ ДАННЫЕ
УМНЫЙ ГОРОД
100 спикеров,
лидеры IP-отрасли,
технологии будущего,
зарубежные гуру,
знаковые тренды,
академия Dahua,
ключевые заказчики,
основные партнеры,
взрывные новинки,
The Next Big Thing

9

23-24.11.2016



ALL-OVER-IP

ТОЛЬКО БИЗНЕС - НИЧЕГО ЛИШНЕГО

СЕТЕВАЯ ИНФРАСТРУКТУРА
 ВИДЕОНАБЛЮДЕНИЕ
 КОНТРОЛЬ ДОСТУПА
 ХРАНЕНИЕ ДАННЫХ
 ВИДЕОАНАЛИЗ
 МАШИННОЕ ЗРЕНИЕ
 КОММУНИКАЦИИ



СКУД затрудняет доступ. Окончательно остановить человека может только человек

с защищенным каналом обмена, которые нельзя незаметно "прочитать" в кармане у настоящего сотрудника и сделать копию. Разумеется, террористы (как и все те люди, которые склонны решать свои проблемы силой) не отличаются интеллектом. Как пример – угонщики автомобилей почти никогда не применяют средства радиоперехвата секретных кодов управления, им проще набить морду хозяину и просто отобрать ключ. Однако в последние годы минимально защищенные карты (обычно на базе MIFARE) стоят совсем ненамного дороже простых, незащищенных, и, конечно, нет причин заранее отсеять саму возможность копирования карт. Для особо важных объектов в последний год начали применяться отечественные карты высокой степени защиты, например электронная карта военнослужащего. Конечно, использование карт такой степени защиты на гражданских объектах вряд ли уместно, но может рассматриваться в рамках общегосударственных программ.

**Пока они едины,
они непобедимы**

Важно, чтобы СКУД работала как единое целое с системой охранной сигнализации. И то, и другое по отдельности хорошо, но вместе они представляют особенно могучую силу. Как обычно происходил процесс в старые недобрые времена? Ответственный за помещение на проходной расписывается в журнале, получает ключ, охранник снимает это помещение с охраны, и человек пошел на рабочее место. Что химзаводы, что станции водоснабжения – весьма немаленькие по территории. Человек может полчаса добираться до рабочего места, а помещение стоит снятым с охраны.

Как это происходит в интегрированной системе? Да, разумеется, расписаться в журнале – это святое. Однако помещение снимается



Дверь должна держать удар. Не стоит вставлять железную дверь в гипсокартонную перегородку

с охраны, только когда человек в него вошел. И ставится, когда он вышел, ну, скажем, в соседнюю комнату. И снова снимается, когда он вернулся. Помещение на охране, а человеку это даже незаметно, не отвлекает. И правильно, нечего отвлекать от прямых обязанностей ответственного человека.

Кадры пока что решают все

Что еще важно учесть? Оперативность контроля и управления. Контроллеры, способные работать автономно при обрыве связи с центральным процессором, – это хорошо. Однако для ответственных помещений недопустимо осуществлять проходы без постоянного контроля из операторской. Кратковременный сбой связи – это одно, а неожиданные запросы доступа в поставленном на охрану и закрытом на ночь помещении – совсем другое, на них обязательно должен реагировать охранник.

Я в начале сказал, что СКУД – единственный вид техники, способный именно остановить преступника. Но на самом деле СКУД способна только задержать, затруднить доступ. Окончательно остановить человека может только другой человек.

Против лома есть прием

Важна защищенность от грубой силы. Не в том смысле, как это слово употребляют спецы по компьютерной безопасности (они имеют в виду прямой подбор кода, пароля), а буквально. Дверь должна держать удар. Провода к замку не следует прокладывать снаружи на виду у всех. Даже если вы не хотите, чтобы контроллер работал автономно и пропускал по карте, пусть он стоит внутри защищаемого помещения, и его блок питания вместе с резервным аккумулятором тоже. Эти простые решения существенно затруднят проникновение.

Ну и, конечно, не стоит вставлять железную дверь в гипсокартонную перегородку. Впрочем, такие вопросы – вопросы инженерной укреплённости – не относятся напрямую к СКУД. Их правильно решать совместно с архитектурными решениями. Так, можно поставить тяжелые ворота, усиленные стальными тросами, в конце переулка, на котором КамАЗ успевает разогнаться до 150. А можно – за поворотом, и тогда не надо их особо усиливать.

Меньше "бантиков", больше надежность

Еще один важный момент – защищенность самой системы. Компьютерную сеть необходимо изолировать от Интернета, охранник не должен знать пароля администратора. Набирают популярность системы на основе не Windows, а более защищенных "отечественных" операционных систем – МСВС, "Астра-Линукс". Это хорошо. Это действительно хорошо.

Мне не раз приходилось видеть, как охранники играют в "игрушки" на компьютере с АРМ системы охраны. Даже обычный Linux значительно снизит вероятность, что неспециалист сможет запустить на нем "игрушку". А использование АРМ охраны не по назначению – это не только риск вирусов и доступа извне, это просто повышает вероятность того, что система подвиснет в самый ответственный момент. Да, большинство Linux-программ не столь красиво выглядят, как программы под Windows. Зато они работают, и, как правило, именно за счет уменьшенного количества "бантиков", работают надежно.

Разумный выбор разумных решений

Резюмируя вышесказанное, можно кратко сказать так: СКУД (и любая аппаратура сама по себе) не в силах победить терроризм. Но применение СКУД на опасных объектах значительно затруднит планирование действий террористов и поможет специалистам, которые с ними реально борются. Необязательно на всех объектах применять системы "военного" класса (обычно называются "для Особо Ответственных Объектов"), однако в реальности системы повышенной защиты стоят ненамного дороже, зато свободны от многих смешных недостатков дешевой аппаратуры. И, конечно, даже на стадии проектирования главное – человек, его разумный выбор разумных решений. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

КОНТРОЛЛЕР ДОСТУПА



C2000-2

32768
пользователей

100
уровней
доступа

100
окон
времени

- Управление дверьми, турникетами, шлагбаумами, шлюзами
- Подключение двух считывателей с интерфейсом Touch Memory, Wiegand, ABA TRACK II
- Запрет повторного прохода (antipassback)
- Временные графики доступа
- Двойная идентификация (Proximity карта + PIN-код)
- Доступ по правилу двух (трех) лиц
- Управление доступом и взятием/снятием при помощи одного идентификатора

C2000-2 вер.2.20

- Доступ под принуждением
- Взятие под охрану датчика контроля двери
- Больше возможностей в настройке уровней доступа и шлейфов сигнализации

**Новая
версия 2.20**



BOLID

bolid.ru