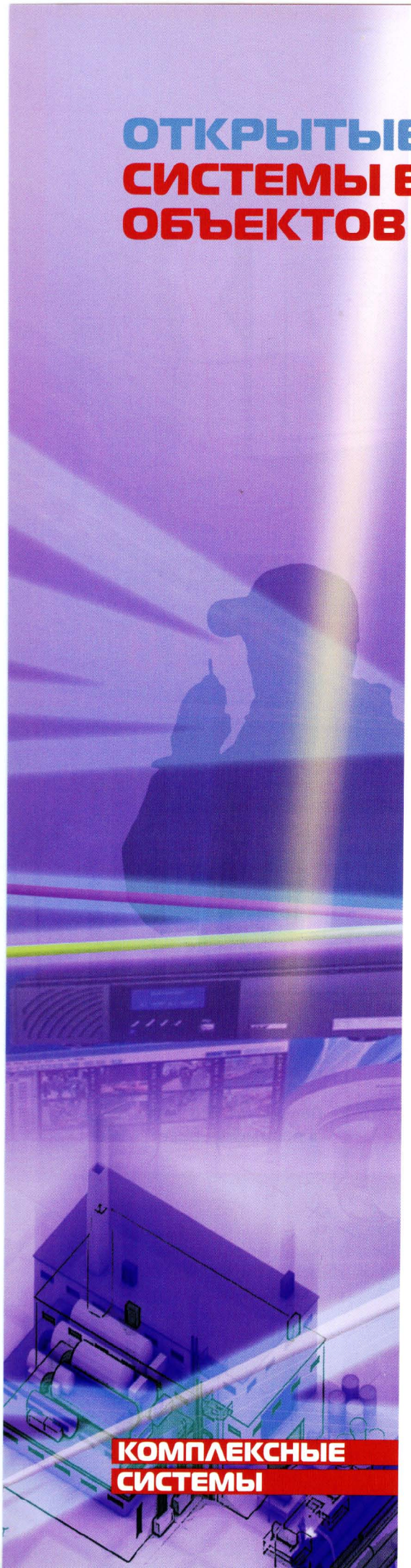
ОТКРЫТЫЕ И ЗАКРЫТЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ ОБЪЕКТОВ

Лёвин Сергей Николаевич
главный конструктор ГК СИГМА

В последнее время нередко можно услышать рассуждения и споры о «закрытости» и «открытости» систем безопасности, о преимуществах и недостатках того или иного подхода, о перспективах развития систем в сторону открытости. В этой статье я хочу поделиться своими наблюдениями на эту тему.



КОМПЛЕКСНЫЕ СИСТЕМЫ

Для начала следует определить значения прилагательных «открытая» или «закрытая» применительно к системе безопасности. Если система безопасности не разделяет никакие свои ресурсы с внешними по отношению с ней системами, то, вероятно, такую систему можно считать вполне закрытой или автономной, максимально независимой от внешних обстоятельств. В качестве ресурсов могут рассматриваться энергопитание компонентов системы безопасности, функциональное оборудование СБ, локация или размещение оборудования, коммуникационные системы для передачи данных между компонентами системы, собственно данные и ресурсы управления для интеграции и взаимодействия с внешними системами (интероперабельность), вычислительные ресурсы и оборудование для хранения данных, рабочие места сотрудников службы безопасности и, наконец, сам персонал. Если некоторые из этих ресурсов разделяются между системой безопасности и другими системами или мероприятиями, то такую систему уже нельзя в полной мере считать закрытой. Рассмотрим подробнее перечисленные ресурсы и попытаемся определить целесообразность закрытости или открытости каждого из них. Эти же факторы можно рассматривать для оценки изолированности и независимости в работе и между подсистемами в рамках общей системы безопасности. Все эти аспекты имеет смысл рассматривать как баланс между надежностью работы и стоимостью внедрения и эксплуатации системы безопасности. Как правило, разделение ресурсов должно вести к снижению стоимости и повышению эффективности эксплуатации. Впрочем, не всегда закрытость системы ведет к увеличению надежности, а открытость к снижению стоимости владения.

ЭЛЕКТРОПИТАНИЕ

С этим, наверное, разобраться проще всего. Как правило, есть нормативные документы, регламентирующие требования к электропитанию оборудования систем безопасности, в основном, к времени автономной работы в случае выхода из строя основной системы питания. Основная система электропитания является общей для различных энергопотребителей предприятия, по крайней мере, в точке ввода на объект. А вот резервную систему электропитания лучше не разделять с другими потребителями, так как в случае режима автономного питания сложно будет гарантировать заявленное время работы, так как не всегда понятно, кто сколько будет требовать от системы питания в различных режимах работы.

ФУНКЦИОНАЛЬНОЕ ОБОРУДОВАНИЕ

Для систем охранно-пожарной сигнализации традиционно применяются специализированные средства обнаружения и приемно-контрольное оборудование, и никаких признаков разделения задач вроде бы нет. Тем не менее, все чаще встречаются решения, где задачи обнаружения признаков вторжения для систем охраны или возгорания для противопожарных систем возлагаются на средства видеонаблюдения. И хотя разделение ресурсов в данном случае происходит между подсистемами в общей системе безопасности, тем не менее, изолированность работы охраны или противопожарной защиты все равно нарушается. Как допол-

нительный признак обнаружения, такой подход выглядит привлекательным как основной — здесь много вопросов к надежности работы. Что касается приемно-контрольного оборудования, то нередко встречаются попытки использования в качестве базовых ППК универсальных программируемых контроллеров, промышленных компьютеров и т.п. Здесь обычно возникают вопросы к повторяемости заявленных характеристик системы в случае применения неспециализированных аппаратных средств. В общем случае, все же гораздо надежнее применять специализированное оборудование для решения базовых прикладных задач, по крайней мере, в ответственных решениях: в охранных системах и противопожарной защите.

РАЗМЕЩЕНИЕ ОБОРУДОВАНИЯ

Речь идет в основном о совместном размещении приемно-контрольного и серверного оборудования системы безопасности с оборудованием других систем объекта. В целом, организация единой серверной с соблюдением всех мер по физической, информационной, энергетической безопасности является хорошей идеей, если остальная IT-инфраструктура объекта находится на должном уровне. Однако, если требования режима объекта не предполагают совместное размещение, а значит и доступ постороннего персонала к оборудованию системы безопасности, единственный выход — это изолированное размещение всех компонентов с гарантированным режимом доступа.

КОММУНИКАЦИОННЫЕ СИСТЕМЫ

Здесь следует различать коммуникации внутри объекта охраны и между распределенными объектами или между объектом охраны и централизованным постом охраны.

Коммуникации внутри объекта могут быть встроены в общую СКС предприятия (структурированная кабельная система) и использовать общие как кабельную часть, так и активное коммутационное оборудование. Современная система безопасности может иметь в составе десятки и сотни IP-видеокамер высокого разрешения, которые создают сетевой трафик, сравнимый или превосходящий остальной информационный обмен предприятия. В качестве оптимизации затрат на внедрение и обслуживание использование общей локальной сети может дать значительный эффект. Вопрос только в том, насколько надежным получится такое решение. Если проект локальной сети предприятия реализован с учетом всех требований по безопасности и надежности функционирования нескольких автоматизированных систем в общей информационной среде, куда входит и система безопасности, такой подход возможен. Более того, на сложных объектах построение фактически второй локальной сети только для системы безопасности может быть вообще неосуществимо. Существующие современные технологии построения коммуникационных систем позволяют реализовать надежное и непрерывное функционирование разнородных информационных систем с заданными параметрами по пропускной способности, времени отклика и качеству обслуживания. В конце концов, можно разделять только среду передачи в виде общего использования оптоволоконных линий, да и то в этом случае для разных задач могут использоваться различные физические волокна. В любом случае все зависит от качества проекта и квалификации обслуживающего персонала.

При построении распределенной системы безопасности для связи объектов охраны между собой или с центром применение сторонних коммуникационных систем становится практически неизбежным. Каналы связи в данном случае могут представлять выделенные арендуемые каналы от специализированных провайдеров, связь через разделяемые каналы связи (GSM-связь или радиоканал) или передача данных через Интернет. В принципе, для обеспечения безопасности коммуникаций через публичные каналы связи сегодня существуют все необходимые технологии. Шифрование трафика, защита от перехвата и вмешательства в обмен данными — все это успешно применяется в самых различных отраслях, где безопасность передаваемых данных является жизненно необходимой. Поэтому само по себе использование сетей GSM или Интернета не является проблемой, главное, какие меры предприняты для обеспечения надежного и безопасного канала связи.

ДАННЫЕ И РЕСУРСЫ УПРАВЛЕНИЯ

Система безопасности может быть интегрирована с другими системами предприятия. Как правило, это касается противопожарной защиты. Системы диспетчеризации и жизнеобеспечения могут получать извещения о пожаре и изменять режимы работы в соответствии с обстановкой на объекте. Если говорить о производственных предприятиях, то автоматизированные системы управления технологическими процессами (АСУ ТП) и системы противоаварийной защиты (ПАЗ) в обязательном порядке интегрируются с системой противопожарной защиты (СПЗ) и постоянно учитывают данные от СПЗ в собственных алгоритмах работы. События от охранной сигнализации о постановке на охрану может использоваться системой жизнеобеспечения для изменения режима управления климатом, отключения ненужного освещения. Данные от систем контроля и управления доступом используются для контроля рабочего времени сотрудников, местоположения персонала на объекте в каждый момент времени. В данных примерах система безопасности используется как источник событий для внешних систем, что в принципе не предполагает возможность вмешательства в управление техническими средствами охраны. Тем не менее, интерфейсы и протоколы обмена данными при организации взаимодействия систем представляют серьезную потенциальную уязвимость, и этот факт должен обязательно учитываться при интеграции.

ВЫЧИСЛИТЕЛЬНЫЕ РЕСУРСЫ И СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ

Применение облачных вычислений и хранение данных в облаке распространяется чрезвычайно широко и захватывает сегодня все новые сферы применения. SaaS (Software-as-a-Service — программное обеспечение как услуга), это одна из форм облачных вычислений, модель обслуживания, при которой пользователям предоставляется готовое прикладное программное обеспечение, полностью обслуживаемое провайдером. Поставщик в этой модели самостоятельно управляет приложением, предоставляя заказчикам доступ к функциям с клиентских устройств, как правило, через веб-браузер. По такой модели уже сейчас предлагаются сервисы для организации систем охранного телевидения, контроля и управления доступом. Более того, сейчас на рынок выходит модель «Инфраструктура как услуга» (IaaS — Infrastructure-as-a-Service). В данном варианте заказчику предоставляется в аренду вся вычислительная структура для предприятия. Потребитель, как правило, приобретает серверное время, умноженное на количество задействованных виртуальных процессоров и виртуальных объемов памяти, а также пространство хранения (возможно, с различной тарификацией в зависимости от производительности), заданную сетевую пропускную способность. Конечно, для адептов традиционного подхода к организации инфраструктуры системы безопасности такие варианты работы — это страшный сон, и хуже не придумаешь. Но прогресс не остановить, облачная модель организации IT-инфраструктуры будет продолжать развиваться и задач систем безопасности это также коснется.

РАБОЧИЕ МЕСТА СОТРУДНИКОВ СЛУЖБЫ БЕЗОПАСНОСТИ

Традиционно пост охраны организуется на объекте или, в случае централизованной охраны, на ПЦН. И для выполнения

основных задач обеспечения безопасности это правильно. Однако в парадигме построения современного «Умного дома» все инженерные системы, обеспечивающие функционирование объекта, должны сводиться в единую диспетчерскую, откуда осуществляется общий мониторинг и управление. Если это не режимный объект с особыми требованиями к обеспечению безопасности, то такой подход выглядит вполне разумным.

ПЕРСОНАЛ

Как уже говорилось выше, функции дежурной смены службы безопасности могут выполняться как выделенным персоналом, так и в рамках единой диспетчерской. Что касается технического обслуживания системы безопасности, то с учетом уровня сложности современного оборудования и программного обеспечения, самое правильное решение — это с самого начала закладывать в бюджет расходы на услуги специализированной организации. Как правило, попытки сэкономить на качественном обслуживании, привлекая собственный технический персонал, приводит к тому, что через 2–3 года система постепенно перестает в полной мере выполнять свои функции. В итоге, восстановление работоспособности выливается в гораздо большие расходы, чем своевременные профилактические работы.

ЧТО В ИТОГЕ?

Подход в построении современной системы безопасности по принципу натурального хозяйства, где «все свое» постепенно будет заменяться неким пакетом ресурсов, услуг и сервисов, предоставляемых специализированными компаниями. В эпоху глобализации рынков и виртуализации IT-решений для конечного потребителя это вполне логичный и ожидаемый сценарий развития технических средств и систем обеспечения безопасности.

СОБЫТИЯ

«ДИАН-СБ» ИЗ ТУЛЫ СТАЛА ОФИЦИАЛЬНЫМ ИНСТАЛЛЯТОРОМ «ВИДЕОГЛАЗА»

Тульская компания «Диан-СБ» стала партнером крупного столичного дилера — компании «Видеоглаз». По условиям франшизы компания получила новый сайт с полным каталогом партнерских товаров, с интернет-магазином и расширенным функционалом. Сюда входит online-расчет стоимости работ, автоматическое сохранение истории заказов в личном кабинете, составление коммерческих предложений прямо на сайте и т.п.

«ПРОСОФТ-БИОМЕТРИКС» ОСНАСТИЛА БИОМЕТРИЧЕСКИМИ СЧИТЫВАТЕЛЯМИ ЧЕШСКИЕ ДАТА-ЦЕНТРЫ

Компания BioSmart, s.r.o., ставшая европейским представительством ООО «Прософт-Биометрикс», объявила о завершении крупного проекта по созданию безопасного контрольно-пропускного режима. Считывателями биометрических данных по рисунку вен ладоней и отпечаткам пальцев оснащены крупные дата-центры компании Master Internet, s.r.o., предоставляющей услуги в области хранения данных и интернет-сервисов.

РАЗВЕРНУТА СИСТЕМА IP-ВИДЕОНАБЛЮДЕНИЯ «ЛИНИЯ» НА 3000 КАМЕР

В магазинах торговой сети «Командор» Красноярского края начало эксплуатации «Линии» с подключением первых трех тысяч IP-камер подтвердило эффективность решения. Система позволяет развернуть безлимитное количество удаленных клиентов, интегрирована с лучшими POS-системами, что существенно улучшает функционал IP-видеонаблюдения в ритейле. Возможность бесплатного использования online-сервиса «Линия Облако».

«АРМО-СИСТЕМЫ» И WAGNER ПОДПИСАЛИ ДИСТРИБЬЮТОРСКИЙ ДОГОВОР

«АРМО-Системы» подписала договор о партнерстве с Wagner Group GmbH, производителем аспирационного оборудования для сверхраннего обнаружения возгораний и систем пожаротушения, включая аспирационные дымовые извещатели для общих помещений, «чистых комнат» и серверных. Все извещатели Wagner Titanus имеют высокое качество исполнения, продолжительный срок службы и низкое число ложных тревог.

СИСТЕМА HYPERPOD ПОЛУЧИЛА НАГРАДУ КОНКУРСА DCS AWARDS 2018

Компания Schneider Electric удостоилась престижной награды — система контейнеризации HyperPod стала победителем конкурса DCS Awards 2018 в номинации «Инновация года для дата-центров». Это интегрированное решение заводского исполнения для распределения воздуха, электроэнергии и организации кабелей, где самонесущая конструкция для изоляции холодного или горячего коридора легко монтируется в машинном зале ЦОДа.

ВЫРУЧКА HIKVISION ВЫРОСЛА НА 26,92%

Общий оборот компании Hikvision, ведущего мирового поставщика инновационных продуктов и систем безопасности, за 1-ое полугодие 2018 года составил 20,88 млрд юаней. Рост выручки в годовом исчислении составил 26,92%, а чистая прибыль, приходящаяся на акционеров, составила 4,15 млрд. юаней — рост на 26,00%. В течение первой половины 2018 года компания создала более 10 новых региональных офисов за рубежом.

4122 IP-КАМЕРЫ ПОД УПРАВЛЕНИЕМ MACROSCOP В ОХРАНЕ ФСИН РОССИИ

К июлю 2018 года системы охранного видеонаблюдения ФСИН России объединяют 4122 камер LTV под управлением ПО Macroscop. Видеосистема объединяет более десятка объектов УФСИН РФ во Владимирской области и Республике Мордовия. На каждом установлено порядка 400 камер, данные с которых обрабатываются 5 серверами и отображаются на нескольких постах для операторов. В каждом учреждении организован также главный пост видеонаблюдения.

БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ НА YOTA ARENA

Для контроля доступа и учёта рабочего времени Yota Arena выбирает систему APACS Bio на базе программного комплекса разработки ААМ «Системз» и биометрических устройств Suprema. Suprema — один из мировых лидеров в производстве оборудования для биометрической идентификации. Компания ААМ «Системз» является лучшим глобальным партнером Suprema за 2017 год и эксклюзивным дистрибьютором оборудования данного бренда в России.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПРИЕМА ПЛАТЕЖЕЙ ISBC ДЛЯ АВТОДОРОГИ БИШКЕК–ОШ

Стартовал этап тестирования работы автоматизированной системы приема платежей за проезд через тоннели с электронным шлагбаумом на посту «Сосновка» (81 км) автодороги Бишкек–Ош в Кыргызской Республике. Консорциум «КБМ-Акфорта-Дельта Профи» построил решение на RFID-технологиях ISBC. На посту установлены датчики, определяющие габариты транспортного средства. Камеры видеонаблюдения обеспечивают распознавание номеров.