

КОМПЛЕКСНАЯ ОХРАНА СЛОЖНЫХ СТАЦИОНАРНЫХ ОБЪЕКТОВ

А. Данг
представитель компании SYAC в РФ

Эта статья является продолжением серии публикаций на тему сложных вопросов построения высокотехнологичной системы безопасности. В прошлых статьях были рассмотрены вопросы централизации охранных комплексов видеонаблюдения, а также вопрос охраны целого города. В этой статье будет поднята задача охраны объектов, требующих повышенной надежности охранных комплексов. Будет представлено техническое решение задачи, а также разобраны два примера.

Статистические данные свидетельствуют, что преступления с каждым днем становятся все более изощренными, а преступников уже не остановить простейшими методами охраны объектов. В том случае, если речь идет о таких объектах как банки, аэропорты, школы, то надежность должна быть не просто достаточной, а максимально возможной.

Компания SYAC существует на рынке безопасности уже более 15 лет, и накопила существенный опыт в реализации различных проектов по всему миру. Одним из последних проектов, который разрабатывали инженеры компании, была программа по обеспечению безопасности всей банковской сети Unibanco. Специалисты SYAC считают своим долгом поделиться своим опытом реализации подобных проектов в свете процесса реновации, планируемыми российскими банками, тем более, что этот пример можно называть стандартным решением нестандартной масштабной задачи.

Описание задачи

Один из крупнейших в Бразилии финансовых институтов Unibanco столкнулся с серьезной проблемой большого количества случаев попыток ограбления по всей своей филиальной сети и банкоматов. С учетом того, что филиальная сеть банка состоит из 1300 отделений по всей стране, задача казалась невыполнимой. Механическое укрепление безопасности каждого отдельного отделения являлось нерациональным и дорогим решением. Очевидно, что решение проблемы заключается не в умножении числа охранников и сотрудников милиции на каждом объекте, который нуждается в охране, а в создании эффективной системы реагирования, когда любое происшествие мгновенно фиксируется, а специализированные службы выезжают на место для решения проблемы. При этом если происшествие фиксируется видеокамерой, то в процессе прибытия на объект – специалисты уже могут изучать видеоматериал, который Центр мгновенно получает посредством централизованной сети. Именно так использование комплексных высокотехнологичных средств обеспечения безопасности может помочь справиться с множеством существующих сегодня проблем. Также нельзя не учитывать то обстоятельство, что охранник не может все 24 часа в сутки внимательно изучать видеоизображение, поступающее на монитор – в этой работе ему должна помогать автоматика, например, встроенный в охранную систему детектор движения.

Детектор движения

Детектор движения на подобных сложных объектах должен быть удобным для управления. Именно это удобство и многофункциональность и определяет превосходство одних систем над другими. Представьте себе, что вы можете всего лишь парой кликов мышки указывать различные зоны. Каждой зоне присвоить свои параметры. Каждая зона может вызывать различные тревожные режимы системы для каждой из стационарных камер и каждой препозицией купольной камеры. Каждая зона детектора обладает своими параметрами по охватываемому пространству, положению и чувствительности.

Каждая зона связана со своей реакцией системы, что позволяет произвести настройки в наиболее важном для пользователя режиме. Детекция движения также может использоваться для того, чтобы купольная камера перешла на определенную заранее указанную позицию. Простой интерфейс позволяет легко установить необходимые параметры по каждой из зон:

- **Размер зоны активности:** позволяет указать объем области изменения, которой должно быть достаточно для перехода системы в тревожный режим (для успешного игнорирования небольших объектов и фиксирования лишь крупных объектов).
- **Уровень чувствительности** определяет то, насколько существенным должно быть изменение на картинке. Создано для игнорирования таких изменений как тени, отражения, видеозум и т.д.

Сенсоры, контроллеры, кнопки тревог

В итоге каждый из филиалов был оборудован системой видео/аудио мониторинга DigiEye. Система работала с камерами числом от 4 до 16 (в зависимости от размера филиала). Дополнительным преимуществом системы любого производителя является, если система уже изначально оборудована дуплексным аудио каналом и мнгозональным детектором движения. В центральном офисе при помощи системы централизации был обеспечен доступ ко всем сенсорам вибрации, установленным в банкоматах, кнопкам тревоги, инфракрасным сенсорам, контроллерам освещения, сиренам и дымовым сенсорам. Все эти приборы были установлены в отделениях банка и соединены с системой DigiEye.

Коммуникационные каналы

Продолжим дальнейшее техническое изучение проекта. После того, как решена локальная задача для каждого отдельного стационарного объекта, необходимо решать задачу объединения всей системы в единый комплекс. Для организации коммуникации между филиалами и центром мониторинга использовалась WAN Unibanco. Канал 64Kbps использовался для передачи всех изображений, аудио и финансовой информации из каждого филиала. Центральная станция мониторинга работает 24 часа в сутки и управляется опытным специально обученным персоналом, обладающим знанием, как реагировать на ситуации связанные с криминалом.

Очевидно, что все филиалы банка находились не в одном городе, и их разделяли огромные расстояния. Банкоматы разбросаны по всей стране. Именно в этом случае возникает вопрос о тех каналах связи, которые требуется использовать. Это основная проблема инсталлятора, который ограничен производителем на использование или только системы выделенного канала, или только спутниковой связи. Лучше всего в этих случаях останавливать свой выбор на тех системах, которые поддерживают любые каналы связи, например, системы работающие на основе IP протоколов. Например, DigiEye как пример наиболее "продвинутой" в этом отношении системы, предоставляет такие функциональные возможности как проигрывание записи с удаленной системы, управление PTZ устройствами, контроль входов и выходов, удаленная настройка конфигурации, удалённое обновление системы, просмотр "живого" видео или ранее записанного видеофрагмента посредством PTSN/POTS, ISDN, ADSL, HDSL, LAN. Доступ к вышеперечисленным функциям в идеальной системе должен быть обеспечен, используя самые разные методы, начиная от ПК с установленной системой MS Windows и до карманного компьютера или мобильного телефона (WAP доступ). Более подробно схема работы изложена на иллюстрации.



Центр охраны

потребуется для хранения столь важной информации. Некоторые системы позволяют использование внешних носителей информации. Аналоговые системы требуют складирования сотни и сотни видеокассет. Цифровые решения существенно упрощают эти задачи. Инженеры SYAC предлагают следующие решения для хранения информации:

- локально (на самой системе), на встроенных жестких дисках
- хранить на удаленном сервере
- использовать преимущества RAID интерфейса

Для хранения большого объема информации (месяцы видеoinформации) требуется использование RAID интерфейса, обеспечивающего повышенную надежность и высокую способность по хранению информации. Возможно использование и других интересных разработок. Например, инженеры SYAC разработали принцип "индивидуального цикла". Для определенных пользователей камер возможно выделение пространства на жестком диске (в виде процента от объема всего дискового пространства) для ведения записи в рамках отдельного индивидуального цикла хранения данных, где будут храниться видеофрагменты лишь этих камер. Принцип работы цикла аналогичен основному циклу хранения информации (информация записывает "по кругу"), однако видеoinформация в рамках индивидуального цикла хранится независимо от видеоданных основного цикла. Таким образом, пользователь может обеспечить хранение видеоданных с определенных камер более длительное время, чем в случае, если бы они хранились в рамках основного цикла записи. Например, в рамках работы охранной системы банка задействованы две камеры, одна из которых находится на входе, а другая – в хранилище, то камера в хранилище может работать в режиме индивидуального цикла хранения информации. В этом случае, видеoinформация из банковского хранилища всегда будет храниться отдельно от данных, поступающих с камеры на входе в здание.

Организация системы прав доступа

Ну и, наконец, нельзя забывать о том, что расследование большей части преступлений в банковской сфере указывало, что сотрудники банка были связаны с правонарушителями или были непосредственными сообщниками. Поэтому важно обеспечить максимальную защиту по доступу к самой системе охраны, которая может предотвратить преступление. Все функциональные возможности для надежных систем (включая доступ к информации с той или иной камеры) должны контролироваться для определенного пользователя. Для достижения максимальной безопасности права пользователя могут строго лимитироваться. Например, когда необходим централизованный контроль пользователей, DigiEye используют систему идентификации RADIUS. В этом случае процедура контроля входа в систему осуществляется внешним сервером идентификации.

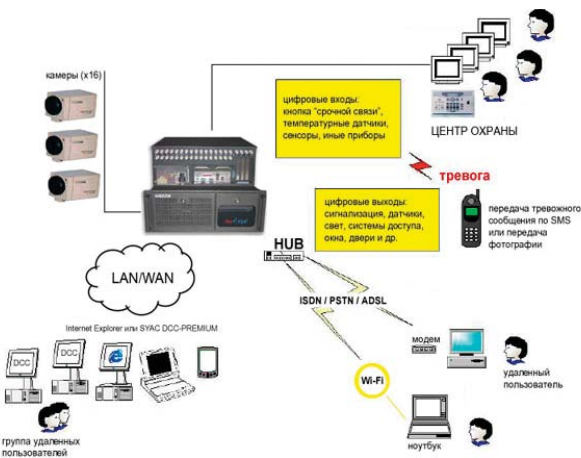
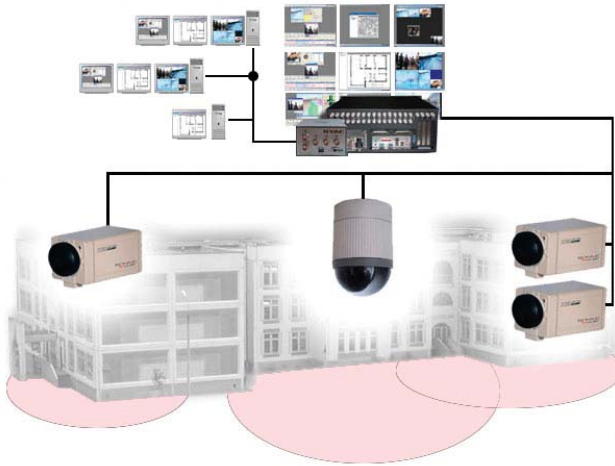


Схема организации работы локальной охраны

Хранение видеoinформации

При построении комплексной охраны сложных проектов обращайте внимание и на тот объем физической памяти, которые



Обеспечение безопасности стационарного объекта

Unibanco: результат

Вернемся к нашему примеру с сетью банков. В результате была создана уникальная полностью интегрированная структура безопасности на основе высокотехнологичного оборудования. Unibanco теперь защищен системой, которая в первый год работы существенно уменьшила ущерб от попыток ограбления. Число удавшихся ограблений снизилось в среднем на 72% по всей сети отделений банка. Это и есть вещественный результат эффективных современных охранных комплексов.

Трубопровод Европа-Магриб

Кратко можно представить и совершенно другой пример еще одного проекта SYAC. Трубопровод Европа-Магриб – это международный проект, который объединяет Алжир с Испанскими газопроводами. Газопровод длиной 2000 км проходит по террито-

рии Алжира, Марокко, Испании, Португалии и по дну Гибралтарского пролива. На 540-километровом участке газопровода находятся две крупных насосных станции: "Hassi R'Mel" на границе между Марокко и Алжиром и "Tanger" на границе между Марокко и Испанией и еще 24 небольшие насосные станции по длине всего трубопровода.

Metragaz требовалось построить централизованную систему управления безопасностью по сети, в которую было бы легко интегрировать существующую систему сигнализации, установленную на станциях. Было требование возможности управления многочисленными объектами, записи и просмотра данных, поступающих с конкретной станции, из центрального офиса. В дополнение к вышеозначенным требованиям Metragaz требовалась система, отличающаяся высокой надежностью, высокой производительностью и великолепной службой технической поддержки. Эта задача также была решена согласно тем же самым принципам, которые были кратко изложены выше.

Выводы

На сегодняшний день можно смело утверждать, что в первый же год инвестиции в высокотехнологичную систему охраны окупились, и теперь банк представляет собой одно из самых безопасных мест города, а трубопровод охраняется по последнему слову техники. Для этого потребовалось использование самых современных систем безопасности и опыта многих компаний, в том числе и опыт инженеров компании SYAC. Очевидно, что борьба с преступлениями – это комплексный процесс, в котором обмен опытом имеет ключевое значение. Общими усилиями можно сделать мир безопаснее. В следующей статье мы более подробно осветим принципы охраны мобильных объектов.

НОВОСТИ

ЗАО "Компания Безопасность" представляет новую линейку оборудования для работы по IP сетям – VCS, компании Bosch Security Systems. Номенклатура VCS включает: классическую серию: VIP 10, VideoJet 10, VideoJet 10i; профессиональную серию: VIP 1000, VideoJet 1000, VideoJet 8000, VideoJet Xpro. Основные составляющие номенклатуры VCS: передатчики/приемники видео по IP сетям; запись, поиск и воспроизведение видео и звука по IP сетям; ПО для программирования и просмотра; цифровой 160-канальный коммутатор для интеграции видео. Широкие возможности удаленного доступа с персонального компьютера: просмотр, запись и управление видео с ПК; передача речи через Интернет; управление поворотной камерой. Дистанционная работа с системой: просмотр на стандартном CCTV мониторе; передача речи через Интернет; поддержка клавиатур с RS232 протоколом; PTZ управление камерой; управление матрицей и DVR. Получение информации о тревогах: видео по детекции с превосходным качеством и intercom audio; связь по тревоге; дистанционное управление PTZ, матрицей, Divar; запись видео и звука на ПК по тревогам. Цифровая запись видео сигналов: запись от 18 часов до 1 недели; независимый просмотр с разным качеством, программирование и воспроизведение через Web и / или ПО VIDOS; сетевой видеомаягнитофон VIDOS-NVR; запись 64 камер на сервер в течение 1 месяца; отказоустойчивость – запись продолжается даже при отсутствии связи в сети. Масштабируемость и гибкость: любая камера на любой монитор, запись любой камеры, воспроизведение на любом мониторе; много пользователей, удаленные посты, удаленная запись; низкая стоимость при наращивании системы: VideoJet XPro. Гибкость и расширяемость обеспечивается ПО "VIDOS". Настраиваемый интерфейс.

Вышла первая версия программного обеспечения TRASSIR™ для совместной работы с компактным IP видеосервером Lanser, позволяющая построить действительно полноценную распределенную систему видеонаблюдения на базе TCP/IP сетей. Lanser поступил в продажу в ноябре прошлого года и поставлялся до сих пор только в комплекте с собственным программным обеспечением Lanser Light, имеющим ограниченное число функций, таких как постоянная запись получаемого видеонаблюдения и подключение только одного устройства. Возможность оценить все достоинства видеосервера появилась только сейчас, в составе системы цифрового видеонаблюдения TRASSIR™. Применение видеосервера Lanser в комплекте с ЦСВН TRASSIR™ особенно целесообразно на объектах с большой площадью или распределенных территориально: в гостиницах, промышленных предприятиях, офисных зданиях, автозаводах, локальных домовых сетях для централизованной охраны городских кварталов. Построение системы с передачей изображения в цифровом формате на базе существующей инфраструктуры.

Компания "Вокорд Телеком" выпустила новый продукт PHOBOS IPtel – комплекс мониторинга, записи и обработки соединенный IP-телефонии и другой телематической информации. PHOBOS IPtel – это комплекс технических средств, предназначенный для записи, хранения, репликации, анализа и сортировки соединений IP-телефонии и другой телематической информации, передаваемой по протоколу TCP/IP. Основные области применения PHOBOS IPtel: системы документирования диспетчерских переговоров, построенные на основе технологий IP-телефонии Cisco, Avaya. системы мониторинга для операторов IP-телефонии.