Аспекты систем видеонаблюдения

Оглавление

Глава 1. Как создавать технические решения по видеонаблюдению

При проектировании видеонаблюдения необходимо найти решение семи основных задач. Данное руководство поможет читателю понимать основные варианты при решении каждой из этих задач, а также осуществлять рациональный выбор различных возможностей.

Данный обзор предназначен помочь новичкам в области видеонаблюдения. Его целью является быстрое определение ключевых аспектов при проектировании видеонаблюдения, не углубляясь при этом во множество деталей и частных случаев, какие встречаются в проектах.

Семь основных задач соответствуют следующим вопросам:

1. Какой тип видеокамер необходимо использовать?
2. Как следует подключать камеры к системам управления видеонаблюдением?
3. Какой тип системы управления видеонаблюдением нужно использовать?
4. Какой тип хранилища следует применять?
5. Какой тип видеоаналитики необходимо использовать?
6. Каким должен быть вариант отображения информации?
7. Как следует интегрировать видеосистему с другими системами?

Прим. использованы материалы с сайта http://os-info.ru

1. Видеокамеры

Образно говоря, камеры являются глазами системы видеонаблюдения. Для получения соответствующего видеоизображения камеры должны размещаться в критических областях.
При размещении камер используются два основных принципа:

- наблюдение точек прохода,
- наблюдение за наиболее ценным.

Точками прохода являются зоны, через которые люди и транспорт должны пройти для попадания в определенные области. Примерами являются дверные проемы, коридоры и проезды. Размещение камер в точках прохода является экономически оправданным способом фиксации всех, кто попадает в здание.

Ценными являются специфические объекты, которые требуют повышенной безопасности. Примерами ценного являются такие физические объекты, как сейфы, а также области, где размещаются товары; кроме того, это такие области, в которых осуществляются важные действия - например, это зоны с кассовыми аппаратами, места парковок машин или приемные. Что является ценным, определяется потребностями и приоритетами конкретной организации.

После того, как выбраны зоны наблюдения, необходимо определиться с четырьмя параметрами видеокамер.

1. Стационарная или PTZ (поворотная) камера

Камера может быть установлена для наблюдения только одного заданного ракурса, либо это может быть камера, обеспечивающая поворот, наклон и увеличение изображения (например, поворот влево или вправо, вверх или вниз, изображение ближе или дальше).

Большинство используемых в видеонаблюдения камер является стационарными. Поворотные камеры главным образом используются при широких углах обзора, и должны использоваться лишь когда ожидается, что оператор ежедневно будет активно использовать камеры. Главной причиной широкого использования стационарных видеокамер является их цена, которая в 5… 8 раз ниже цены поворотных видеокамер (стационарные видеокамеры в среднем стоят 200… 500 USD, в то время как стоимость поворотных видеокамер может превышать 2000 USD).

2. Цветные, инфракрасные или тепловизионные

В телевидении изображение может быть цветным или черно-белым. В настоящее время производство черно-белых камер для видеонаблюдения оправдано лишь тем, что они могут использоваться при очень низкой освещенности (например, в ночное время). В этих условиях инфракрасные камеры или тепловизионные камеры создают черно-белое изображение.
Для создания в темноте четкого изображения инфракрасные камеры требуют специальных ИК-осветителей; они стоят сравнительно недорого.
Для тепловизионных камер не требуется подсветка, однако они обеспечивают лишь отображение силуэтов объектов, и они являются очень дорогими (в среднем 5000… 20000

USD).
Для наблюдения в дневное время или в освещенных местах цветные камеры являются естественным выбором, поскольку преимущество цветного изображения над черно-белым очевидно.

3. Стандартное разрешение или мегапиксели

Этот выбор аналогичен выбору телевизоров. Исторически все потребители использовали камеры стандартного разрешения, однако в настоящее время пользователи все больше склоняются в сторону камер высокого разрешения. В то время как телевидение высокой четкости ограничивается 3 мегапикселами, камеры видеонаблюдения могут обеспечивать разрешающую способность до 16 мегапикселов. В 2008 году мегапиксельные камеры составляли лишь примерно 4% в общем объеме продаж видеокамер, однако их использование возрастает очень быстро.

В качестве примеров приводятся следующие изображения:

- Изображения реальной кражи, сохраненные с помощью 2-мегапиксельной камеры IQinvision
- Запись в аэропорту с помощью 16-мегапиксельной камеры Avigilon, которая демонстрирует мелкие детали вдали
- Запись в кафе аэропорта с помощью 5-мегапиксельной камеры Avigilon, которая демонстрирует мониторинг в большой области

Здесь демонстрируются довольно большие пространства – от 100 до 300 футов (примерно от 30 до 90 метров) в ширину и несколько сотен футов в глубину.

В традиционном проекте для этих целей обычно используется 3 или 4 фиксированных камеры в местах прохода и наблюдения за наиболее ценным, а также поворотная камера в центре для активного мониторинга или общего следования по предустановкам.

4. IP-камера или аналоговая

Главной тенденцией современного видеонаблюдения является переход от аналоговых камер к IP-камерам. Хотя для просмотра и записи на компьютере оцифровываются сигналы от любых камер видеонаблюдения, только в IP-камерах происходит оцифровка внутри самих камер. В то время, как большинство инфракрасных камер и тепловизионных камер по-прежнему реализуются в виде аналоговых камер, мегапиксельное разрешение достижимо лишь при использовании IP-камер. В настоящее время 20% всех продаваемых камер являются IP-камерами, и это число быстро возрастает.

В большинстве инсталляций смешиваются, сочетаются камеры различного типа. Например, на объекте могут использоваться инфракрасные фиксировано установленные аналоговые камеры для видеонаблюдения за периметром и аналоговая поворотная камера для обзора места парковки. Внутри здания может использоваться фиксированная мегапиксельная камера для наблюдения за складом и большое число фиксированных IP-камер для наблюдения за входом и коридорами.

2. Подключения

В профессиональном видеонаблюдении с целью записи и выбора отображения почти всегда камеры подключатся к системам управления видеонаблюдением. Имеются две основные характеристики, позволяющие выбрать вариант подключения.

IP или аналог

Видеоизображение может быть передано либо по компьютерной сети (IP), либо может быть передано в естественной форме аналогового видеосигнала. В настоящее время большей частью осуществляется аналоговая передача сигнала, однако переход на IP происходит достаточно быстро. С помощью технологии IP можно передавать информацию как от IP-камер, так и от аналоговых камер. IP-камеры могут быть непосредственно подключены к компьютерной сети (точно так же, как к ней подключаются компьютеры). Аналоговые камеры так подключать нельзя. Однако в этом случае для передачи аналогового сигнала по компьютерной сети можно использовать кодер (encoder). У кодера имеется вход для подключения аналоговой камеры и выходы цифрового потока для передачи по IP-сети.

Провода или беспроводное подключение

Видеосигналы можно передавать, используя кабели, либо по эфиру, вне зависимости от того, что используется – IP или аналоговое видео. Более 90% видеосигналов передается с помощью кабелей, поскольку, как правило, это наиболее простой и надежный способ передачи видео. Однако беспроводная передача является важной опцией при передаче видео, поскольку использование проводов может оказаться неприемлемым по цене для некоторых проектов, например, при наблюдении за местами парковок, заборами, удаленными зданиями.

3. Система управления видеонаблюдением (Video Management System)

Система управления видеонаблюдением является основой видеонаблюдения. Она принимает сигналы от видеокамер, сохраняет их и управляет распределением видео между наблюдателями.

Существуют четыре фундаментальных варианта системы управления видеонаблюдением. На большинстве объектов используется один из этих вариантов, однако в отдельных случаях может применяться несколько вариантов - когда необходимо иметь возможность перехода от одного варианта к другому.

• **DVR** (Digital Video Recorder - цифровой видеорегистратор) - специализированный компьютер, сочетающий в себе три составляющие: аппаратуру, программное обеспечение и видеохранилище. По определению видеорегистраторы имеют входы только для подключения аналоговых видеокамер. В настоящее время почти все видеорегистраторы поддерживают удаленное наблюдение через интернет. Видеорегистраторы очень просты в установке, однако они имеют существенные ограничены в части расширения или изменения оборудования. Вплоть до настоящего времени видеорегистраторы наиболее часто применяются среди профессионалов. Тем не менее, популярность видеорегистраторов определенно падает, и тенденцией является переход к одной из нижеследующих категорий.
• **HDVR** (hybrid DVR – гибридный видеорегистратор) – это видеорегистратор, который поддерживает и IP-камеры. Гибридные видеорегистраторы имеют полностью всю перечисленную функциональность обычных видеорегистраторов и, кроме того, они поддерживают IP-камеры и мегапиксельные камеры. Большинство

видеорегистраторов допускают обновление своего программного обеспечения, благодаря чему DVR превращается в HDVR. Возможность таких обновлений является важной, привлекательной тенденцией вследствие низкой цены такого перехода, обеспечивающего непосредственную поддержку аналоговых и IP-камер.
• **NVR** (Network Video Recorder - сетевой видеорегистратор) аналогичен обычному видеорегистратору за исключением поддерживаемых им камер. В то время, как DVR поддерживает только аналоговые камеры, NVR поддерживает только IP-камеры. Чтобы он мог поддерживать аналоговые камеры, необходимо использовать кодер (encoder).
• **Программное обеспечение для IP-видеонаблюдения** – это программное приложение, подобное Word или Excel. В отличие от DVR или NVR, программное обеспечение для IP-видеонаблюдения не поставляется с каким-то оборудованием - пользователь должен загрузить программное обеспечение в компьютер или сервер и настроить его. Это обеспечивает намного большую свободу и потенциально меньшую стоимость, чем при использовании DVR или NVR. Однако это влечет за собой существенно большую сложность и большее время для настройки и оптимизации системы. Программное обеспечение для IP-видеонаблюдения является в настоящее время главной тенденцией в системах управления видеонаблюдением – его чаще всего выбирают при большом числе камер (сотни и более).

4. Хранилище

При видеонаблюдении почти всегда осуществляется видеозапись – для последующего поиска и просмотра. Среднее время хранения записей составляет от 30 до 90 суток. Тем не менее, небольшая часть компаний хранит видеозаписи более короткое время (7 суток), а некоторые компании – очень долго (несколько лет).

Наиболее важными факторами, которые определяют время хранения записей, являются стоимость хранения и возможные угрозы безопасности фирмы.
Хотя стоимость хранения становится все ниже, видеонаблюдение требует огромных объемов памяти. Для сравнения, служба электронной почты Google предлагает бесплатно около 7 Гбайт дискового пространства. Считается, что для электронной почты это более чем достаточно. Однако для записи с одной камеры такой объем памяти может быть израсходован за одни сутки. Довольно общим фактом для систем видеонаблюдения является потребность иметь несколько терабайт памяти даже при наличии всего нескольких десятков камер. Поскольку стоимость хранения записи является важным фактором, то существует большое число технологий для оптимизации использования памяти

Тип угрозы безопасности также влияет на длительность хранения записи. Например, главной угрозой банкам является отчет о расследованиях фактов мошенничества. Эти отчеты подчас не доводятся до сведения пострадавших клиентов в течение 60… 90 дней после произошедшего инцидента. Поэтому у банков существует серьезная потребность длительного хранения видеозаписей. В отличие от этого, в казино узнают о прошедшем сразу же, и если появились проблемы, там изучают их в течение недели. Поэтому в казино очень часто используется более короткое время хранения записей (как правило, несколько недель).

Существует три основных варианта хранения записей.

1. Внутреннее хранилище – это жесткий диск внутри DVR, NVR или сервера. В настоящее время это наиболее распространенная форма хранения записей. При наличии существующих сегодня жестких дисков объемом до 1 Тбайта, внутреннее хранилище может образовывать общий объем дискового пространства до (2… 4) Тбайт. Внутреннее хранилище является наиболее дешевым вариантом, но как правило, менее надежным и масштабируемым по сравнению с другими вариантами. Тем не менее, в видеонаблюдении оно используется наиболее часто.

2. Напрямую подключенное хранилище (DAS - Directly Attached Storage) – это жесткие диски, размещенные вне DVR, NVR или сервера. Для управления жесткими дисками используются такие устройства, как NAS или SAN. Как правило, это обеспечивает большую масштабируемость, гибкость и резервирование. Однако стоимость такого решения в пересчете на терабайты обычно выше, чем у внутреннего хранилища. Наиболее часто напрямую подключенное хранилище используется в проектах с большим числом камер.

3. Кластерное хранилище – это объединенное на базе IP хранилище, ориентированное на хранении видеозаписей от большого числа камер. Множество DVR, NVR или серверов может отправлять потоковое видео на эти кластеры для хранения. Они обеспечивают эффективное, гибкое и масштабируемое хранилище для очень большого числа камер. Кластерное хранилище является наиболее важной из новых тенденций в области хранилищ.

5. Видеоаналитика

Видеоаналитика осуществляет анализ поступающих видеопотоков:

- с целью оптимизации хранения записей,
- для идентификации угроз или интересуемых событий.

Оптимизация записей – это наиболее часто используемое приложение видеоаналитики. В простейшем виде видеоаналитика проверяет видеопотоки на предмет наличия в них изменений. На основании наличия или отсутствия движения система управления видеонаблюдением может принимать решение вообще не запоминать в данный момент видео или запоминать его с малой скоростью обновления, либо с низким разрешением. Поскольку видеонаблюдение может фиксировать длительные промежутки отсутствия активности (когда, например, коридоры или лестницы, здания закрыты), с помощью анализа движения можно уменьшить использование памяти на (60… 80)% по сравнению с непрерывной памятью.

Более интересной формой видеоаналитики является выявление угроз или интересуемых событий. Действительно, как правило, если специалисты обсуждают видеоаналитику, то это соответствует их потребности в данной информации. Типичными примерами этого является нарушение периметра, оставленные предметы, подсчет людей и распознавание автомобильных номеров.

Целью этих видов видеоаналитики является проактивное выявление случаев нарушения безопасности с целью предотвращения их развития (например, нарушение периметра привлекает внимание к тому, как вор преодолевает забор, что позволяет сразу же остановить его; функция распознавания автомобильных номеров позволяет обнаруживать транспортные средства, находящиеся в розыске, что помогает задерживать их).
Эта видеоаналитика в целом разочаровала. Хотя многие наблюдатели полагают, что

видеоаналитика будет улучшаться, рынок видеоаналитики в настоящее время сокращается (в ответ на его проблемы и спад).

6. Просмотр видео

В конечном итоге, видеонаблюдение предназначено для просмотра людьми. Большая часть это видео никогда и никем не смотрится, а та часть, которая смотрится, обычно используется лишь для последующих расследований. В основном, только в розничной торговле (для обнаружения магазинных воров) и при наблюдении общественных мест (с целью выявления криминальных угроз) просмотр живого видео осуществляется непрерывно. Как правило, живое видеонаблюдение осуществляется лишь периодически - в качестве отклика на вызвавшую его угрозу или для проверки состояния удаленного объекта.

Существуют четыре основных возможности просмотра видео.

Локальное наблюдение непосредственно с выхода DVR, NVR или сервера является идеальным для мониторинга территории небольших объектов. Это позволяет использовать систему управления видеонаблюдением в качестве станции наблюдения, экономя деньги на использовании компьютера и его настройку. Такое решение чаще всего применяется в розничной торговле, банках и на предприятиях малого бизнеса.

Удаленное наблюдение с помощью компьютера применяется наиболее часто для просмотра видео. В этом случае для просмотра живого или записанного видео используются обычные компьютеры. Применяют либо установленное на компьютере специальное приложение, либо веб-браузер. Большей частью компьютерное наблюдение осуществляется с помощью специальных приложений, так как они обеспечивают наибольшую функциональность. Однако по мере совершенствования веб-приложений все больше поставщиков предлагают наблюдение именно с помощью мощного веб-приложения. Достоинством просмотра видео с помощью веб-браузера является то, что при этом не требуется установка и обновления клиентского ПО.

Мобильное наблюдение позволяет охраннику, находящемуся на территории объекта, мгновенно проверить, что отображает видеонаблюдение. Мобильное наблюдение имеет большой потенциал, поскольку группы быстрого реагирования и мобильная охрана широко распространены в индустрии безопасности. Хотя мобильные устройства доступны уже не менее 5 лет, они не становились главной тенденцией из-за решения проблем КПК и мобильных телефонов. Оптимизм и возобновление интереса к подобным устройствам вызвало появление Apple iPhone.

Видеостена - это идеальное решение для больших ситуационных центров, имеющих для просмотра сотни и тысячи камер. Видеостена образует очень большой экран, что позволяет осуществлять наблюдение сразу группе людей. Это особенно важно при чрезвычайных ситуациях. Видеостена, как правило имеет возможность переключения между камерами, а также автоматически демонстрировать изображения от камер, где произошла тревога.

7. Интеграция видеонаблюдения с другими системами

Во многих компаниях видеонаблюдение применяется самостоятельно - за счет использования клиентского приложения системы управления видеонаблюдением. Однако для больших объектов и компаний с повышенными требованиями к безопасности такое

решение является неэффективным. Взамен этого подобные организации предпочитают использовать подход, аналогичного принятому у военных в картах оперативной обстановки (COP - common operational picture), когда с помощью единого интерфейса отображается информация от нескольких систем безопасности. Имеются три способа обеспечить подобную интеграцию видеонаблюдения.

1. В качестве ядра используется система контроля доступа. Во многих организациях используется обычные электронные или IP-системы контроля доступа. Такие системы разрабатывались в течение многих лет для интегрирования их с другими системами безопасности, такими как охранные системы и видеонаблюдение. Это наиболее частый способ интегрирования видеонаблюдения, и он является сравнительно недорогим (10000 - 50000) USD. Однако системы контроля доступа зачастую имеют ограничения по количеству систем и глубине интеграции, которые они поддерживают.

2. В качестве ядра используется PSIM (physical security information management) - специализированные приложения управления информацией от систем физической защиты. Их основное назначение - собирать информацию от систем безопасности (таких, например, как видеонаблюдение) и предоставлять наиболее релевантную информацию с оптимальной стратегией отклика. Эти приложения, как правило, стоят гораздо дороже (100000 - 1000000) USD, однако они поддерживают намного более широкий диапазон систем безопасности и обеспечивают реализацию сложных функций.

3. В качестве ядра используется система управления видеонаблюдением. Все чаще системы управления видеонаблюдением допускают поддержку других систем безопасности и выполнение функций управления безопасностью. Если требуется лишь ограниченная интеграция, то существующая система управления видеонаблюдением может обеспечить недорогое (хотя и ограниченное) решение.

Результат

Если вы чувствуете себя уверенно в принятии ключевых решений при проектировании, то, возможно, вас заинтересует имеющийся анализ компаний, которые предоставляют товары для этих решений.

Глава 2. Знакомство с NVR и программным обеспечением для IP-видеонаблюдения

IP-видеонаблюдение и сетевые видеорегистраторы (NVR) – два термина, наиболее часто используемые при описании систем физической защиты на базе IP-камер и компьютерных сетей. Это маркетинговые термины, они не регулируются соответствующими стандартами, поэтому нет их официального определения, но по этому вопросу существует много различных точек зрения. В данной главе предпринята попытка зафиксировать наиболее часто принимаемые допущения и выделить наиболее часто дискутируемые моменты.

Более того, в индустрии обсуждаются вопросы о том, что привело к этим решениям. Многие используют в качестве названия таких систем NVR, в чем отражается их преемственность от DVR. Однако этот термин предполагает наличие оборудования и соответствующих приборов. Многие убеждены, что такое решение должно иметь открытую архитектуру и быть лишь программным продуктом - поэтому они не позиционируют свои продукты как NVR’ы. Довольно часто производители называют свои

продукты как системы управления IP-видеонаблюдением (IP Video Management) или системы IP-видеонаблюдения (IP Video Surveillance). Для краткости в данной книге используется сокращение NVR взамен длинных и неудобных выражений типа “Программное обеспечение для IP-видеонаблюдения” и т. п. Следует иметь ввиду, что производители не утруждают себя выбором точного названием категории своих продуктов. Я бы рекомендовал не придавать большого значения названиям категорий, а сосредоточиться на понимании разницы в тех или иных преимуществах товаров.

NVR’ы должны поддерживать IP-камеры

Практически все согласны, что обозначение NVR относится к решениям, которые должны поддерживать IP-камеры. В действительности же слово “сеть” использовано в выражении “сетевой видеорегистратор” не из-за IP-камер; обычно оно указывает на использование IP-сети для подключения IP-камер к NVR.

NVR – это лишь программное приложение (ОБСУЖДАЕТСЯ)

Большинство поставщиков NVR позиционирует свои продукты только в качестве программного обеспечения. То есть можно сказать, что, приобретая NVR, пользователь получает файлы для загрузки на выбранном им компьютере. Пользователю не требуется покупать “железо” (аппаратное обеспечение) у поставщика NVR. Это повсеместно рассматривается в качестве главного преимущества использования NVR, и это декларируется компанией Milestone Systems как побег из собственной тюрьмы. Индивидуальный выбор аппаратного обеспечения может снизить общие затраты, а также увеличить гибкость при проектировании и использовании такой системы, которая наиболее полно отвечает запросам клиента.

Тем не менее, многие поставщики NVR предлагают приборы. В IT-индустрии термин “прибор” относится к комплекту из аппаратного и программного обеспечения, которое можно купить только совместно. Простым примером прибора является сотовый телефон: здесь невозможно смешивать или сочетать программное обеспечение от одного поставщика с аппаратным обеспечением от другого поставщика. Для создания небольших систем некоторые компании (например, VideoProtein) предлагают приборы, которые позволяют упростить настройку и инсталляцию. Для крупномасштабных проектов такие компании, как Steelbox, предлагают приборы, позволяющее снизить расходы и уменьшить аппаратное обеспечение, требуемые для установки сотни камер и даже нескольких тысяч камер.

DVR’ы не могут поддерживать IP-камеры

В соответствии с общепринятым определением продукт, называемый как DVR, не поддерживает IP-камеры. Слово “цифровой” в названии “цифровой видеорегистратор” в целом отражает тот факт, что сигналы от аналоговых камер преобразуются в цифровые сигналы внутри видеорегистратора и, следовательно, не посылаются по IP-сети. По определению DVR может поддерживать только аналоговые сигналы. Следовательно, DVR может поддерживать IP-камеру только в том случае, если видеопоток от IP-камеры перед этим с помощью декодера обратно преобразуется в аналоговый сигнал.

NVR’ы поддерживают аналоговые камеры с помощью кодеров

Кодер (encoder) – это прибор, который преобразуют видеосигнал от аналоговой камеры в IP-поток, который может быть передан по компьютерной сети подобно электронной почте

или видеоролику “You Tube”. Почти все NVR’ы поддерживают кодеры. Обычно указывают следующие преимущества кодеров:

- они позволяют использовать совместно с NVR’ами существующие аналоговые камеры,
- отпадает необходимость в использовании их коаксиальных кабелей, кабелей витой пары или оптоволоконных сетей.

Некоторые системы одновременно являются DVR’ами и NVR’ами

Некоторые приборы одновременно поддерживают IP-камеры и непосредственно подключенные к ним аналоговые камеры. В частности, для поддержки аналоговых камер эти приборы не требуют использования кодеров. Аналоговые камеры могут быть непосредственно подключены к задней панели прибора – этим устраняется необходимость в кодерах. Такие приборы обычно относят к гибридным DVR’ам или NVR’ам. Главными преимуществами, приводимыми в пользу гибридных систем, является то, что они могут быть дешевле по сравнению с программных обеспечением “чистых” NVR и что они облегчают переход от аналоговых камер к IP-камерам.

Нередко обсуждается вопрос, являются ли гибридные системы действительно сетевыми видеорегистраторами или IP-системами видеонаблюдения. Главными проблемами являются блокировка камер собственным “железом” и зачастую неполная поддержка IP-камеры, а также ограниченное количество IP-камер, которые гибридная система может поддерживать.
Все NVR’ы поддерживают определенные базовые функции

Общепризнано, что все NVR’ы поддерживают определенные базовые функции:

- запись видео,
- просмотр живого видео,
- поиск записанного видео,
- просмотр записанного видео.

Эти функции можно выполнять с удаленного компьютера.

NVR’ы могут существенно различаться по уровню функциональности

В то время, как NVR’ы являются программными приложениями, функциональные возможности программного обеспечения NVR’ов могут существенно различаться. Такое различие функциональных возможностей может проявляться в продуктах различных поставщиков и даже среди разных предложений одного поставщика.

Например, компания Milestone Systems предлагает 4 категории IP-видеонаблюдения/NVR-решений, а также различные опции. Примерами таких категорий являются:

- Базовая: система для малого числа камер, функциональность базовая,
- Средняя: система для среднего числа камер, более развитое управление камерами и системой,
- Многосторонняя: система для большого числа камер с серверами во многих местах,
- Глобальная: система для сверхбольшого числа камер с преодолением отказов и центральным управлением.

В то время, как все версии предлагают такие базовые функции, как видеозапись, просмотр и поиск записи, различные версии предлагают более мощные инструменты для повышения надежности и удобства работы; кроме того, они различаются по количеству камер и поддерживаемых мест их подключения. Также могут быть существенными отличия у различных поставщиков NVR'ов по предлагаемым ими функциональности, надежности и масштабируемости.

NVR'ы также могут различаться по предлагаемым типам опций, например:

- опции для различных вертикальных рынков или приложений (розничная торговля, банки, охрана периметра),
- опции различных видов видеоаналитики (виртуальный барьер, распознавание автомобильных номеров, распознавание по лицу человека),
- опции для интеграции с системами контроля доступа, охранной сигнализацией и пр.

Не все поставщики поддерживают категории и опции. Поэтому даже среди NVR-решений покупатели должны внимательно изучать, какая комбинация характеристик наиболее подходит с точки зрения оперативности и безопасности.

Число поставщиков NVR все более возрастает

Во всем мире можно легко насчитать десятки поставщиков NVR-решений. Ожидается, что это значение будет расти:

- за счет поставщиков DVR, которые готовят предложения по NVR,
- за счет новых игроков рынка, привлеченных его ростом, которые готовят свои предложения.

Глава 3. Пропускная способность для видеонаблюдения (основные понятия)

В случае использовании IP-камер, мегапиксельных камер, NVR'ов или даже DVR'ов при планировании, проектировании и использовании систем IP-видеонаблюдения очень важным является понимание основ того, какое значение пропускной способности доступно и какая пропускная способность требуется.

Все, кто занимаются IP-видеонаблюдением, должны иметь представление об этих основах, поскольку пропускная способность – это важный фактор для видеонаблюдения.

Какое значение пропускной способности доступно?

Для вычисления того, сколько пропускной способности доступно, в первую очередь необходимо определить, между какими местами должна быть обеспечена связь. Это очень похоже на вождение автомобиля, когда имеется отправная точка и точка назначения. Например, от филиала до центрального офиса. Однако, в отличие от вождения автомобиля, доступное значение пропускной способности может варьироваться весьма существенно в зависимости от того, куда нужно передавать сигнал.

Наиболее важным фактором в определении того, сколько пропускной способности доступно для использования, является вопрос о том, требуется ли осуществлять соединение между двумя зданиями. В качестве примера:

	Типичные значения доступной пропускной способности
Внутри здания	70 Мбит /с… 700 Мбит/ с
Между зданиями	0,5 Мбит/с… 5 Мбит/с

Значение доступной пропускной способности при передаче информации от одного офиса к соседнему офису внутри здания может быть в 200 раз больше по сравнению с пропускной способностью при передаче от офиса к его филиалу, размещенному в другом квартале.

Значение доступной пропускной способности при передаче информации от одного офиса к соседнему офису внутри здания может быть в 200 раз больше по сравнению с пропускной способностью при передаче от офиса к его филиалу, размещенному в другом квартале.

Сказанное справедливо в 90% случаев (и даже более). Больше пропускной способности оказывается доступно в следующих случаях:

- здания разные, но они находятся на территории единого кампуса (университетского городка),
- в районе делового центра крупного города,
- проект реализуется для телекоммуникационной или научно-исследовательской компании.

Между зданиями

Ключевым фактором в доступности пропускной способности является стоимость используемых между зданиями сетей. Обычно это относится к WAN (Wide Area Network – глобальная сеть), этот тип трафика обычно предоставляется телекоммуникационными компаниями. Типичным примером могут служить кабельный модем или DSL, которые могут повсюду обеспечить трафик от 0,5 Мбит/с до 5 Мбит/с по цене от 50 USD до 150 USD в месяц. Другим примером является линия T1, которая предоставляет 1,5 Мбит/с по цене примерно от 300 USD до 600 USD в месяц. Для более высоких значений пропускной способности стоимость становится весьма высокой. В большинстве мест стоимость приобретения канала связи с пропускной способностью 10 Мбит/с может составлять несколько тысяч долларов в месяц.

Много говорится об оптоволокне, но широко оно не будет доступно еще многие годы. FTTH (Fiber to the home) – оптоволокно до дома или до бизнеса может существенно снизить стоимость пропускной способности. Тем не менее, использовать его очень дорого, и за последние десятилетия (даже дольше) нельзя похвастаться существенным прогрессом, разве что захватывающими дискуссиями на эту тему. Даже если все это представляется чудесным, но много ли толку в том, чем нельзя воспользоваться?

Внутри зданий

В отличие от рассмотренного, пропускная способность внутри зданий (или кампусов) достаточно высокая, поскольку стоимость использования сети довольно низкая. Пользователи даже без особых технических знаний могут легко настроить внутри здания сеть 1000 Мбит/с (известную как LAN - Local Area Networks, то есть локальную сеть), заплатив за ее монтаж менее 1000 USD, при том, что ежемесячная плата вообще

отсутствует. По сравнению с этим ежемесячная стоимость WAN с такой же пропускной способностью может составлять десятки тысяч долларов.

Стоимость использования сетей в зданиях низкая вследствие того, что затраты на них минимальны, поскольку не связаны с затратами на строительные работы. При создании сети в городе требуются разрешения на места прокладки кабелей, земляные работы, монтаж на телефонных столбах и т.д. Это огромные проекты, которые могут потребовать миллионов и даже миллиардов долларов авансовых расходов. В противоположность этому, внутри здания кабель зачастую можно быстро и легко пропустить через потолок (хоть это и не профессиональное решение, тем не менее, многие используют такой прием монтажа).

Широко обсуждаются существующие методы беспроводного подключения (WiMax, WiFi, 3G и т.п.), однако беспроводное подключение не обеспечивает ни существенно большую пропускную способность, ни намного лучшие цены по сравнению с использованием DSL или кабельного модема. По существу, беспроводное подключение не решает проблемы дороговизны и ограниченной пропускной способности при связи между зданиями. Это говорит об абсолютном превосходстве беспроводного подключения над DSL или кабельным модемом для мобильных решений и подключения к удаленным местам, но оно не может быть экономически эффективным. Просто дело в том, что будучи намного более дорогим решением, чем использование кабелей внутри зданий (при той же пропускной способности), оно не решит проблему пропускной способности между зданиями.

Сколько пропускной способности требуется IP-камерам?

Для грубой оценки пропускной способности, требуемой IP-камерой, можно использовать простое правило: 1 Мбит/с. Но кроме этого, существует много факторов, которые влияют на результирующую потребность в пропускной способности. Естественно, что поток от IP-камеры можно передавать медленно, например, 0,2 Мбит/с (200 Кбит/с), а можно быстро, например, 6 Мбит/с. Чем больше разрешающая способность и чем выше частота кадров, тем большей должна быть пропускная способность. Чем более эффективный кодек используется, тем меньше требования к пропускной способности.

Для грубой оценки пропускной способности, требуемой для мегапиксельной камеры, можно принять значения от 5 Мбит/с до 10 Мбит/с. Опять же, существует большое число факторов, влияющих на результирующую потребность в разрешающей способности. Для 1,3-мегапиксельной камеры при скорости обновления 1 кадр в секунду может потребоваться всего 0,8 Мбит/с (800 Кбит/с), в то время как для 5-мегапиксельной камеры уже может потребоваться 45 Мбит/с.

Что все это значит для проектируемой системы IP-видеонаблюдения?

Так же, как с семейным бюджетом, теперь мы можем прикинуть - “что мы можем себе позволить”.

	Имеющийся запас пропускной способности
Между зданиями	0,5 Мбит/с… 5 Мбит/с
Внутри зданий	70 Мбит/с… 700 Мбит/с

	Потребность в пропускной способности
IP-камера	1 Мбит/с
Мегапиксельная камера	5 Мбит/с… 10 Мбит/с

Используя эти таблицы, можно быстро оценить возможные комбинации из IP-камер и мегапиксельных камер при передаче сигналов внутри зданий или при связи между зданиями.

1. Внутри зданий можно легко передавать потоки от большого числа IP-камер и мегапиксельных камер.
2. При передаче между зданиями подобное практически невозможно.

Как следствие описанной ситуации, стандартная конфигурация систем IP-видеонаблюдения может выглядеть следующим образом.

• Местный регистратор в каждом здании или в удаленном месте. Местный регистратор принимает потоки камер данного здания и хранит их.
• Местный регистратор пересылает потоки (живого изображения или записанного) вне данного здания только тогда, когда пользователь действительно хочет увидеть видео. В этом случае вместо перегрузки WAN-сети сутки напролет ничем не мотивированными запросами, мы имеем пропускную способность, которая расходуется лишь в моменты, когда пользователь хочет что-то посмотреть. Обычно удаленный просмотр происходит непредсказуемо, так что в этом случае IP-видеонаблюдение мило сосуществует с дорогостоящей WAN-сетью.
• Местный регистратор для передачи потокового видео к удаленным клиентам имеет встроенные функции снижения требований к пропускной способности. Чтобы гарантировать отсутствие перегрузки сети видеосистемой и возможность удаленным наблюдателям реально видеть происходящее в другом месте, большинство систем имеют возможность снижения частоты кадров потокового видео или динамического снижения качества изображения. Обычно потока живого видео достаточно для распознавания основных угроз. В любом случае, пропускная способность, как правило, настолько дорога (особенно пропускная способность восходящего трафика, требуемого для отправки удаленному наблюдателю), что данное решение является лучшим с точки зрения экономической эффективности.

Заключение

Знание значений пропускной способности, доступной для DVR’ов и NVR’ов, а также того, сколько пропускной способности требуется для IP-камер или мегапиксельных камер - это ключевой момент при планировании и использовании реально работающих IP-видеосистем. Хотя это лишь общий обзор, но я надеюсь, он поможет в понимании значения пропускной способности для IP-видеонаблюдения.

Глава 4. Разбираемся с видеоаналитикой

Вот уже 5 лет обещания с помощью видеоаналитики пресекать попытки злоумышленников преодолевать заборы, ловить воров в магазинах, обнаруживать оставленные предметы и т.д. остаются предметом частых дискуссий.

И хотя поставщики видеоаналитики раздают грандиозные обещания, люди продолжают задаваться вопросами о целесообразности использования аналитики в реальной жизни. Естественно, что с распространением информации о проблемах видеоаналитики, риски применения ее теперь кажутся выше, чем несколько лет назад, когда новизна этой технологии увлекала всех.

В этом разделе исследуются основные проблемы, ограничивающие использование и продвижение видеоаналитики; цель его - помочь руководителям служб безопасности в лучшем понимании связанных с этим существенных вопросов.

Существуют 3 главные проблемы:

1. высокий уровень ложных тревог,
2. чрезмерная сложность эксплуатация системы,
3. слишком высокая стоимость системы.

Высокий уровень ложных срабатываний

Поскольку целью видеоаналитики является исключение человеческого участия, то для достижения этого необходимо устранение ложных срабатываний. Каждое ложное срабатывание не только требует привлечения человека для оценки произошедшего, оно создает негативные эмоции, разочарование в системе.

Многим знакомы ложные срабатывания охранных сигнализаций и разочарование в каждом таком случае. Как правило, ложные срабатывания охранных сигнализаций дома или на работе встречаются довольно редко: одно или два ложных срабатывания в месяц – это уже много. У многих клиентов месяцами не бывает ложных срабатываний охранных сигнализаций.

В отличие от этого, многие системы видеоаналитики могут формировать десятки ложных срабатываний в день. Это представляет намного большую проблему по сравнению с любой другой, относящейся к охранным сигнализациям. К тому же, если такие срабатывания случаются по многу раз в день, то они могут стать дополнительной нагрузкой в работе охраны.

Конечно, не все системы видеоаналитики создают большое число ложных срабатываний, тем не менее, многие. Эти проблемы стали главным препятствием для известных мне интеграторов и конечных пользователей, чтобы эксплуатировать или пытаться использовать системы видеоаналитики.

Чрезмерная сложность эксплуатация системы

Проблемы с эксплуатацией системы видеоаналитики зачастую упускаются из виду и даже умалчиваются. В течение недель или месяцев количество ложных срабатываний систем видеоаналитики может начать заметно расти – вследствие изменений окружающей обстановки, погоды и положения солнца (что неожиданно и непрогнозируемо может стать причиной главных проблем системы).

Но проблемой является не только увеличение числа ложных срабатываний. Постоянный риск, что в будущем система может неожиданно сломаться, уменьшает доверие к ней. Если знать, что в один прекрасный день система видеонаблюдения периметра может

перестать работать должным образом, то это говорит, что в общей системе безопасности существует серьезный изъян.

Это явилось причиной большого количества неудач в реализации систем видеоаналитики. Уже от купленных систем просто отказывались, тем самым, потеряв большие деньги, завещали другим их не покупать или просто привлекали подобным образом внимание коллег к видеоаналитике.

Это не говорит о том, что все системы видеоаналитики ведут себя подобным образом, однако следует быть осторожным, внимательно изучив информацию, подтверждающую, что данные системы длительное время работали без ухудшения параметров.

Слишком высокая стоимость системы

Если в настоящее время попытаться найти недорогие системы видеоаналитики, то такие системы могут демонстрировать проблемы №1 и №2, то есть иметь большое число ложных срабатываний, неудобство эксплуатации системы. Действительно, мой опыт говорит, что системы видеоаналитики, поставляемые бесплатно или по цене всего лишь (100… 200) USD, большей частью имели существенные проблемы в работе.

Общей особенностью реально работающих систем является то, что полная цена аппаратного и программного обеспечения для видеоаналитики обычно составляет не менее 500 USD за канал. Просто из того, что система видеоаналитики дорогая, совсем не следует, что она хорошая. Однако существуют обоснованные цены для построения системы, которая бы была надежной и хорошо бы работала в реальных условиях.

Стоимость систем видеоаналитики вытекает из необходимости создания их устойчивыми к реальным условиям окружающего мира, это не требует доказательств. Проектировщику нужно создать достаточно “интеллектуальную” систему видеоаналитики, чтобы она справлялась с изменениями освещенности, интенсивностью освещения, изменениями погоды и положения солнца и т.п. Выполнение этих требование приводит к созданию более сложных и современных программ. Такие программы почти всегда требуют для своего выполнения существенно больших аппаратных ресурсов компьютера, а также существенно больших капиталовложений в написание, тестирование и оптимизацию программ. Ясно, что все это увеличивает стоимость.

Проблема состоит в том, что все это в принципе невозможно понять из рекламной презентации, поскольку при демонстрации все системы неизменно выглядят абсолютно одинаково.
Конечно, это имеет побочный эффект - побуждает людей выбирать дешевые системы, которые, можно говорить с большой вероятностью, создают большое количество ложных срабатываний и являются неудобными в эксплуатации.

При выборе системы, которая реально работает, может оказаться трудным понять соответствие ее стоимости, если исходить из стоимости в расчете на одну камеру. Действительно, поначалу деньги на многие проекты видеоаналитики поступали в качестве государственных субсидий, по существу, делая их стоимость вторичной или не соответствующей реальной. Тем не менее, для увеличения использования видеоаналитики в частном секторе, необходимо, чтобы она не только работала, но и создавала бы финансовую прибыль.

Когда видеоаналитика позволяет сократить численность охраны или снижает существенные и частые потери, то ее использование легко оправдать. Существуют успешные в этом отношении компании (если речь идет об официально зафиксированных случаях, то лидером здесь является компания ioimage). В остальных случаях, когда участие человека не исключается, а отдельные потери малы или происходят редко, то стоимость может быть главной преградой для использования видеоаналитики.

Выводы

Хотя и предвижу дальнейший успех видеоаналитики, я все же полагаю, что такой успех будет ограничен проектами для объектов, где велик уровень потерь и/или цена сокращения людских ресурсов является высокой. Хотя ясно, что аналитика будет становиться дешевле, это уменьшение стоимости потребует времени, а в переходный период точкой опоры для дальнейшего успеха аналитики могут стать дорогостоящие проекты.

Главным для принятия решения об использовании видеоаналитики является тестирование и исследование отзывов.

Глава 5. Руководство по беспроводному видеонаблюдению

В то время, как беспроводное подключение является уникальным решением для определенных задач, его использование является намного более рискованным по сравнению с использованием проводов. Важно понимать, когда стоит использовать беспроводные системы и каковы основные риски при создании таких систем. Если продуманно использовать беспроводную связь для целей видеонаблюдения, то экономическая выгода в этом случае может оказаться довольно значительной. Однако просчеты в выборе и проектировании таких систем могут привести к существенным проблемам в отношении их надежности и масштабируемости.

Главным правилом должно быть следующее: следует избегать беспроводных подключений до тех пор, пока стоимость проводного подключения в каком-то проекте не окажется существенного выше беспроводного. Причина этого в том, что применение и эксплуатация беспроводных сетей является намного более рискованным и дорогим, чем для проводных сетей. При использовании беспроводных систем возникают намного более серьезные проблемы, чем при использовании проводов, а именно: ограниченная пропускная способность, препятствия при передаче сигналов, повышенная стоимость эксплуатации и ограничения по масштабируемости.

Пропускная способность

Беспроводные сети имеют намного меньшую пропускную способность по сравнению с проводными подключениями. При использовании проводов легко достижимой может быть пропускная способность для видеонаблюдения от 70 Мбит/с до 700 Мбит/с. Для беспроводных сетей доступная пропускная способность зачастую не превышает 5 Мбит/с… 25 Мбит/с. Это является важнейшим и зачастую упускаемым из внимания аспектом при проектировании беспроводного видеонаблюдения.

Обычно беспроводное видеонаблюдение имеет существенно меньшую пропускную способность, чем это указывается в его паспортной спецификации. Причина этого в том, что метод расчета пропускной способности беспроводных систем является противоположным тому, который используется при традиционном расчете в случае

использования проводов. Например, если для проводов, говорят, что пропускная способность составляет 100 Мбит/с, то это значит, что имеется 100 Мбит/с восходящего потока и другие 100 Мбит/с нисходящего потока. В беспроводной сети пропускная способность, например, 11 Мбит/с, означает полную пропускную способность для двух потоков - восходящего и нисходящего. Некоторые беспроводные системы допускают установку половины восходящего потока и половины нисходящего потока. Это является большой проблемой для видеонаблюдения, поскольку почти вся используемая пропускная способность относится к потоку в одном направлении (восходящему). Поэтому следует быть уверенным, что данная беспроводная система в случае необходимости готова обеспечить для восходящего потока всю пропускную способность. Сказанное является общим правилом для беспроводных систем, предназначенных для передачи видео, но не является общим правилом для промышленного оборудования.

Дальнейшее снижение пропускной способности нередко оказывают окружающие условия. Беспроводные сети намного более подвержены влиянию внешних факторов по сравнению с проводными сетями. Беспроводные сети обеспечивают максимальную пропускную способность только при достаточно высоком уровне сигнала (отношении сигнал/шум). Небольшие препятствия на пути распространения сигнала или даже незначительные отклонения антенны дополнительно уменьшают пропускную способность беспроводной системы. В предыдущем примере беспроводная система с 11 Мбит/с обеспечивает пропускную способность потокового видео только 5,5 Мбит/с. Однако обычные внешние условия могут уменьшить эту пропускную способность до 2,75 Мбит/с.

Расстояние до камер

Довольно трудно настраивать многокилометровую беспроводную связь до камер видеонаблюдения. Определяющими факторами здесь являются препятствия, ограничения используемых частот, ограничения по мощности, аккуратность инсталляции.

Примечание: в данном руководстве рассматривается использование нелицензированной частоты, которая, безусловно, наиболее часто используется для беспроводных видеосистем. При использовании лицензированной частоты, когда можно применять намного большую мощность и гарантировать отсутствие помех, рассматриваемые вопросы не существенны. Однако приобретение лицензий требует времени и денег, поэтому в большинство проектов используется нелицензируемый спектр частот. Далее подразумевается использование нелицензируемых частот.

Расстояние, на которое можно передать сигнал, существенно зависит от мощности этого сигнала – в этом мы ограничены. Правительство ограничивает мощность сигнала, чтобы вы не заглушали сигнал других пользователей. Это означает, что намного труднее пробиваться среди помех и проходить большие расстояния. Это также значит, что другие пользователи на той же самой частоте могут снижать пропускную способность данного канала или блокировать ваш сигнал. Это явилось главным фактором появления диапазона 4,9 ГГц для использования в проектах видеонаблюдения, поскольку данный диапазон предназначен для общественной безопасности.

Препятствия являются серьезной проблемой для беспроводных систем видеонаблюдения. Большинство таких систем использует частотные диапазоны (от 2,4 ГГц до 5,8 ГГц), сигналы которых значительно поглощаются зданиями и деревьями. Проще говоря, если требуется передать сигнал до здания, удаленного на 100 метров, но если другое здание стоит на этом пути, то сигнал будет поглощен и связь будет невозможна. Для решения

проблемы можно и должно использовать ячеистые сети, однако это надо учитывать как фактор, влияющий на стоимость всей сети.

Очень важна аккуратность инсталляции, тем не менее, приборы могут все-таки работать неправильно, что потребует дополнительного технического обслуживания. Из-за ограничений по мощности беспроводные видеосистемы главным образом используют узконаправленные антенны, которые повышают уровень сигнала за счет концентрации его в узкой области. Это может значительно помочь в достижении больших расстояний или в преодолении помех, однако это означает, что антенны должны очень точно располагаться по одной оси. Если это условие не выполняется, то функционирование системы значительно ухудшится. Кроме того, если при эксплуатации системы антенна изменяет свое положение, работоспособность системы может совершенно неожиданно ухудшиться.

Количество камер

Количество камер беспроводной системы строго ограничивается ее пропускной способностью и расстояниями до камер. Для любого конкретного беспроводного соединения максимальное количество камер, которые могут поддерживаться системой, лежит в пределах от 5 до 15, при условии, что камеры располагаются не далее одной мили (1609 метров). Даже при “VCR”- качестве изображения (как у видеомагнитофона) и при использовании хорошего кодека потребуется поток 1 мбит/с. Это существенно при использовании беспроводных связей, которая может поддерживать только (5…20) Мбит/с. Общее число беспроводных камер может быть увеличено за счет множественных беспроводных подключений или за счет комбинации беспроводных и проводных сетей.

Разумной практикой является использование беспроводных и проводных сетей, причем доля беспроводных сетей должна быть минимальной – только в специфических случаях, когда применение проводного соединения экономически неоправданно. Типичный пример: отведение сегмента сети (от существующей сети или от телекоммуникционной компании) и развертывание беспроводного соединения от здания до места размещения камер вблизи этого здания: на столбах или заборе.

При любых рассмотренных подходах подбор кодека и выбор разрешающей способности являются ключевыми факторами в определении числа камер, которые можно использовать.
В проводной сети, при типичной пропускной способности 70-700 Мбит/с несжатое видео будет создавать серьезную нагрузку. В беспроводной сети с максимально возможной пропускной способностью 5-15 Мбит/с одна MJPEG камера стандартного разрешения может одна выбрать всю доступную пропускную способность.

Аналогично, учитывая данные ограничения пропускной способности, использование мегапиксельных камер становится серьезной задачей. Даже с различными оптимизациями мегапиксельные камеры потребляют гораздо большую пропускную способность, чем стандартные камеры (при одинаковой частоте кадров).

Вывод

Беспроводные сети могут быть решением для проектов, в которых проводные сети оказываются слишком дорогими. Отвечая потребностям дорогостоящих строительных проектов, видеонаблюдение может быть использовано в местах, где другие решения экономически неоправданны. Однако беспроводные сети – это намного большие проблемы и риски при проектировании и эксплуатации систем. По существу, четкое

понимание этих моментов, а также осознание того, когда оправдано использование беспроводных систем, будет способствовать успеху беспроводных систем видеонаблюдения.

Глава 6. API и рекомендации по системной интеграции

API (Application Programming Interface – интерфейс программирования приложений) является наиболее часто неправильно понимаемым и чрезмерно разрекламированным аспектом физической безопасности. Хотя применение API действительно может обеспечить большую выгоду, однако их использование намного сложнее того, что часто упоминается в рекламных звонках по телефону или журналах.

Целью API в системах физической безопасности является создание условий для совместной работы различных приложений. Примерами сказанного являются:

- интеграция DVR/NVR с системой контроля доступа,
- интеграция охранной сигнализации с центральной станцией мониторинга,
- интеграция IP-камер или видеоаналитики с NVR,
- создание PSIM (Physical Security Information Management – управление информацией системы физической безопасности) - системы, которая бы интегрировала все системы безопасности.

Наиболее часто можно услышать обсуждение API в предпродажных ситуациях, когда клиент или интегратор спрашивает продавца: “Ваша система работает с X?”, где в качестве X может быть любое количество систем безопасности любого производителя.

Стандартный ответ менеджера по продажам: “Конечно, ведь у нас есть API”.

Этот ответ я слышу на протяжении всего времени, пока работаю в индустрии безопасности.

Это самое опасное и лживое заявление по поводу систем физической безопасности вообще. В силу того, что подобное происходит довольно часто и является столь рискованным, стоит более подробно остановиться на API.

Урок №1. Нет такого понятия, как API

Не существует такого понятия, как API вообще. Имеется множество различных API. В больших системах существуют сотни API. В общем случае, для каждой функции в системе имеется свой API. Хотите смотреть живое видео – используйте API живого видео. Хотите устанавливать расписание – используйте API установок времени. Хотите увеличить частоту кадров при записи – используйте API частоты кадров при записи и т.д.

Урок №2. Не у всех функций есть API

Вот здесь первый подводный камень. Не для всех функций есть API.
Скажем, требуется получить список всех уведомлений о работоспособности из другого приложения. Это приложение в общем случае может иметь API, но не специальный API, который предусматривает отправку извещений о работоспособности. Легко понять: поскольку у большинства систем в настоящее время сотни функций, то нередко десятки таких функций оказываются недоступны через API.

Урок №3. Наличие API не означает, что он будет работать с данной системой

Предположим, что у Вас NVR от “Genetec” и система контроля доступа от “Software House”. В продуктах обеих этих компаний, конечно, имеются API, однако нет никаких гарантий, что указанные два продукта будут работать совместно. Для интеграции продуктов обеих компаний наличие API является необходимым, но недостаточным условием. Как минимум, обе компании должны совместно работать для обеспечения интеграции.
Многие компании заявляют, что их API работает с продуктами партнерских компаний, однако зачастую оказывается, что именно данная комбинация не поставляется изначально.

Урок 4. Интеграция требует времени

Нередко продавцы заявляют, что интеграция займет несколько недель. Так бывает, однако зачастую реализация технических деталей может потребовать значительно большего времени. Следует быть осторожным в отношении времени и денег, отпускаемых на такие проекты. Чаще всего, это непрогнозируемый риск, который невозможно оценить, пока не углубишься в технические детали того, как каждый продавец разрабатывает свои API. В общем, в конечном итоге эти проекты заканчиваются успешно, однако время и стоимость их реализации могут меняться.

Урок 5. Изменения API могут все сломать

Подобно любому продукту, с течением временем API претерпевают изменения. Разница в том, что изменения API могут вывести из строя до этого работающую систему. Причины изменения API могут быть различными: устранение ошибок, повышение производительности, добавление новых функций. При этом другая система, работа которой зависит от API, остается без изменений.

Пусть какая-то система безопасности работает с неким программным обеспечением “Vendor B” версия 3.1. Теперь, допустим, выходит “Vendor B” версии 3.2, в которой, однако, изменен API. Другими словами, новая версия несовместима со старой версией. Поэтому, если обновить “Vendor B” версия 3.1. до версии 3.2, система может неожиданно прекратить работать. В результате на экране центра управления перестает отображаться видео, или пропадает информация от системы контроля доступа либо какой-то другой системы, получившей обновление.

Урок №6. Вы заложник того, что API делает.

Если только вы не сверхкрупный клиент, то вы заложник всего того, что бы API ни делал и того, каким бы способом он это ни делал. Чаще всего, все, что вам нужно, работает прекрасно. Однако, если для в каком-то специальном случае потребуется изменение - выполнение его может оказаться непростым делом. Убедитесь, что ваши специалисты точно знают, что может и чего не может делать API, чтобы заранее предвидеть любые потенциальные проблемы. Если изменение все-таки выполнить необходимо, то, как правило, оно требует много работы и времени на тестирование. Это происходит не из-за того, что программисты такие медлительные, а потому что продавец ПО должен гарантировать, что это изменение не повредит системам безопасности на тысячах других объектов, где используется данный API.

Использование API в системах физической защиты безусловно выгодно, и их применение определенно будет расти. Понимание реалий использования API в конечном счете поможет максимально увеличивать ценность системной интеграции.

Глава 7. Как интегрировать видео с другими системами

Трудно (и становится все труднее) определить наилучший подход для интеграции видеонаблюдения с другими системами безопасности. В то время дискуссия сосредоточена на важности интеграции, задача состоит в том, чтобы сделать ее эффективно, экономично и просто.

Данная проблема расширяется, и она не сводится лишь к стандартным задачам выбора технологии и проектирования. Несколько лет назад возможные варианты были достаточно ясными (поскольку они были чрезвычайно ограничены). Или, выражаясь более точно, довольно ясным был следующий вариант: в качестве центра управления работала бы система контроля доступа (СКД), а другие системы, такие как видеонаблюдение, поставляли бы информацию для платформы на базе СКД.

В настоящее время имеются три категории или, если угодно, три кандидата на роль основного приложения в системах безопасности:

1. Система контроля доступа (классический подход).
2. PSIM-система: появившаяся тенденция использования специального приложения, которое управляет традиционными системами безопасности.
3. Система видеонаблюдения: результат растущего стремления продавцов видеонаблюдения с помощью своего продукта управлять другими системами.

Какую из этих систем выбрать? Какая из них лучше? Какая из них победит?

Система контроля доступа

Системы контроля доступа являются наиболее развитыми в части доступных опций, востребованных в последнее десятилетие. Большинство систем контроля доступа может интегрироваться с большим числом систем управления видеонаблюдением. Главным преимуществом является то, что системы контроля доступа используются практически повсюду, а введение в них дополнительных интерфейсов сравнительно недорого. Основной недостаток использования систем контроля доступа в качестве центральной платформы является стремление ограничить поддержку систем сторонних производителей кроме тех, которые наиболее полно способствуют их скорым продажам. В качестве главных игроков, поддерживающих данные тенденции, в первую очередь упоминаются компании GE, Tyco (Software House) и Honeywell. Кстати, одни системы контроля доступа практически никогда не поддерживают другие системы контроля доступа, так что если требуется поддержка сразу нескольких СКУД, то такое решение, как правило, не работает.

PSIM-система

Термин PSIM символизирует концепцию управления информацией в системах физической безопасности; в то же время он относится к группе компаний, которые создают специальные приложения, предназначенных исключительно для управления системами безопасности, такими как системы контроля доступа и системы управления видеонаблюдением. Известными поставщиками здесь являются Orsus

http://www.orsus.com/ , Proximex http://www.proximex.com/ и Vidsys http://vidsys.com/ . Поскольку эти компании не принадлежат поставщикам систем контроля доступа или видеонаблюдения и не контролируются ими, то они могут предлагать (и предлагают) разнообразную поддержку различных производителей. Кроме того, они оптимизируют свое решение не как просто расширение существующей системы контроля доступа, а скорее как решение для полномасштабного управления безопасностью. Обратной стороной медали является необходимость приобретения нового, недешевого (от 100 тыс. до 1 млн. и более) USD и неизвестного в использовании продукта.

Система управления видеонаблюдением

Все более и более поставщики систем управления видеонаблюдением добавляют в свои системы функции PSIM. Например, компания VideoNEXT http://www.videonext.com/ , традиционный поставщик систем управления видеонаблюдением, в настоящее время предлагает на рынке (видео + PSIM)-решения. Такие продукты, как Nextiva от компании Verint и Ocularis от OnSSI имеют в себе такие черты PSIM, как создание графических планов объекта, интеграция с другими системами, управление рабочим процессом и т.д. Главным преимуществом является простое и дешевое добавление функций в пользовательский интерфейс, который в данное время, быть может, уже используется. Однако частичная поддержка (или отсутствие поддержки) других видеосистем – это серьезный недостаток. Еще больше запутывает ситуацию тот факт, что компании Orsus и Proximex (два поставщика PSIM-систем) предлагают мощные решения по управлению видеонаблюдением, которые обеспечивают лучшее наблюдение в системах большого масштаба, чем многие поставщики систем управления видеонаблюдением

Рекомендации

Принятие данного решения является непростым, так как не существует какого-то одного подхода, который может использоваться повсеместно. Начинать следует с изучения возможностей существующей системы контроля доступа. Возможно, это будет наиболее дешевый и простейший способ интеграции систем. Если с этим подходом имеются сложности (а они, конечно, могут быть – ведь данный подход имеет свои ограничения), то в таком случае можно порекомендовать изучение предложений от поставщиков PSIM-систем. Они будут дорогими и сложными, однако, скорей всего, они позволят интегрировать все необходимые системы.

Глава 8. Стоит ли использовать IP-камеры?

Рынок безопасности принял IP-камеры. Тем не менее, большинство используемых видеокамер по-прежнему остается аналоговыми, а большая часть систем управления видеонаблюдением продолжает строиться на базе цифровых видеорегистраторов. Когда и как следует переходить на IP? Насколько быстрым будет этот переход. В какой момент руководитель службы безопасности, производитель или интегратор поймет необходимость такого перехода?

Хотя в целом картина кажется ясной, все же в большинстве случаев, когда речь заходит о конкретном переходе на IP, о том, как его выполнять и как управлять этим переходом – такое бизнес-решение становится чрезвычайно важным.

Важнейшие стратегические моменты

Чтобы легче определиться с переходом на IP, ниже представлены три важнейших стратегических момента, которые определяют скорость и порядок осуществления этого перехода.

- Чем большим является охраняемый объект, тем более выгоден скорейший переход на IP-камеры.
- Чем более совершенными становятся мегапиксельные камеры, тем скорее следует переходить на IP-камеры.
- DVR'ы продолжат реализацию функций NVR'ов, и этим они будут продлевать жизнь аналоговых систем.

В данном разделе рассматриваются эти важнейшие стратегические моменты, а также специальные рекомендации для интеграторов и конечных пользователей.

Стратегический момент №1. Размер объекта

Чем большим является охраняемый объект, тем более выгоден скорейший переход на IP-камеры. При этом не так важно, сколько объектов - важен размер каждого отдельного объекта. Из-за ограничений, присущих коаксиальному кабелю, в случае очень больших объектов стоимость инсталляции системы с коаксиальным кабелем резко возрастает. Речь идет о бизнес-центрах, корпоративных кампусах, военных базах. Использование дешевых коаксиальных кабелей не решает эти проблемы. Здесь требуется использование собственных сетей.

Возможность отказа от собственных сетей является одним из преимуществ IP-камер, которое перевешивает все остальные, и привело к развитию IP-камер/кодеров. Все это справедливо для случая, когда решение принимается только из соображений бизнеса.

На больших проектах видеонаблюдения можно сэкономить от 1000 USD до 4000 USD в пересчете на одну камеру по сравнению с системами передачи на большие расстояния аналоговых видеосигналов. Если при этом удастся избежать земляных работ, то выигрыш может быть намного большим.

Не удивительно, что большинство крупнейших систем с использованием IP-камер реализовано в школах, корпоративных кампусах, муниципалитетах, в армии. Нельзя сказать, что IP-камеры применяются повсюду, однако многие, если не большинство крупнейших проектов успешно реализованы с их помощью там, где имелись большие расстояния между камерами.

Так же не следует удивляться и тому, что рестораны быстрого питания, филиалы банков, объекты малого и среднего бизнеса, а также другие организации, размещенные на небольших площадях, не спешат использовать IP-камеры. Здесь и с коаксиальными кабелями все работает прекрасно, а экономически обосновать IP достаточно трудно.

Стратегический момент №2. Все большее развитие мегапиксельных камер

Если подходить практически, то улучшение качества изображения IP-камер стандартного разрешения по сравнению с качеством аналоговых камер, записанных DVR'ом, является минимальным. Конечно, качество изображения, получаемого с помощью IP-камер, выше, однако не настолько, чтобы с его помощью во много раз увеличилась бы раскрываемость преступлений. Без очевидного и существенного улучшения таких параметров качество IP-камер не сможет влиять на распространение IP (это не означает, что IP не будет

распространяться, однако более вероятным является распространение IP под влиянием стратегического момента №1, прекрасным дополнением к которому является высокое качество изображения).

В отличие от сказанного, мегапиксельные камеры безусловно создают предпосылки для раскрытия большего числа преступлений. Мы наблюдаем начало этого процесса при использовании мегапиксельных камер в казино. Благодаря их возможности отображать мелкие детали, недостижимой для аналоговых камер, предотвращаются или, по крайней мере, уменьшаются потери, что создает фирмам дополнительную ценность их бизнесу.

Однако бизнес мегапиксельных камер только набирает силу, поскольку их использование увеличивает полную стоимость системы. По-прежнему остается совсем неясно, когда и каким образом все эти затраты и сложности могут быть преодолены и начнется повсеместное использование мегапиксельных камер.

Хотя у мегапиксельных камер имеются хорошие перспективы, однако пока что они не реализованы. Они будут способствовать переходу к мегапиксельным камерам, вопрос лишь в том, когда и каким образом?

Стратегический момент №3. DVR'ы продолжат реализацию функций NVR'ов

Один их наиболее интересных и неодооцененных моментов в переходе к IP-камерам - как на этот переход реагируют производители DVR'ов. Несомненно, что производство DVR'ов продолжится, что продлит жизнь аналоговых камер.

Существует 5 областей применения DVR'ов, где они традиционно проигрывали в сравнении с NVR'ами и где они смогли сократить это отставание.

- Поддержка IP-камер. Почти все популярные DVR'ы превратились в гибридные системы, поддерживающие большое многообразие IP-камер. Данная тенденция сохранится, так как техническая реализация этого не столь трудна, а клиенты четко обозначили свою потребность в гибком решении. Хотя гибридные DVR'ы не способны поддерживать такое количество брендов камер, как это делают NVR'ы, однако для большинства пользователей ассортимент поддерживаемых камер скорей всего является вполне достаточным. И накопленная база гибридные DVR'ов зачастую будут иметь экономическое превосходство над системами с IP-камерами или кодерами.

- Удаленный доступ. Если ранние модели DVR'ов могли быть ограничены в части дистанционного доступа, то в настоящее время все DVR'ы предлагают множество способов и функций для удаленного доступа, включая доступ по локальной сети и интернету. С точки зрения клиента различие между DVR'ами и NVR'ами становится все менее заметным.

- Масштабируемость. Хотя в этой области исторически NVR'ы имели преимущество, однако для современных DVR'ов уже нормой является возможность управлять системой из тысяч камер. DVR'ы обеспечивают диагностику функционирования, централизованное управление, создание виртуальных матриц и многое другое. Это не доказывает, что DVR'ы лучше или что они могут каким-то образом вытеснить NVR'ы. Просто в DVR'ах учтены прежние основные недостатки, поэтому IP трудно их победить лишь только по этому вопросу.

- Интеграция приложений. DVR'ы всегда хорошо интегрировались с системами контроля доступа, охранными сигнализациями, кассовыми терминалами, банкоматами и т.д. Мне кажется, заявления любой из сторон по этому вопросу являются скорее маркетинговыми приемами, нежели говорят о реальных отличиях. Думаю, большинство клиентов смогут убедиться, что каждое из этих решений отвечает их требованиям.

- Аналитика. С возрастанием числа гибридных систем, а также непрерывным увеличением скорости процессоров, DVR'ы становятся мощными аналитическими платформами. Тот факт, что DVR'ы являются гибридными системами, теперь означает, что они могут поддерживать такие же камеры компаний OV или Io Image, какие могут поддерживать NVR'ы. Тот факт, что за минимальную стоимость в DVR'ах могут быть установлены высокоскоростные процессоры, означает, что внутри своей системы DVR приобретает черты непрерывной аналитики. Поскольку двухядерные и четырехядерные процессоры становятся обычным явлением, то экономически оказывается очень выгодным (по отношению к IP-камерам) выполнение аналитики в DVR'ах

Итак, многие важные достоинства IP-камер реализованы в DVR'ах. Конечно, это не остановит распространение IP-камер, однако сделает его более сложным, а также повысит важность принимаемого решения о существовании или замене аналоговых камер.

Рекомендации

Начнем с основных рекомендаций, которые применимы ко всей отрасли, а затем отдельно рассмотрим рекомендации для конечных пользователей и интеграторов.

Общая рекомендация №1. **Прогресс начинается на крупных объектах**

Если вы стремитесь к росту отдачи от вложений в новых областях, то такими областями определенно будут большие объекты. Почему? Потому что IP-камеры меняют бизнес-модель использования камер на крупных объектах, на больших территориях. Там, где прежде использование камер было слишком дорогим, IP предоставляет новый вариант их использования.

Наверняка мы увидим, как это развивается в школах, корпоративных кампусах, муниципалитетах, на удаленном оборудовании – повсюду, где большие расстояния отделяют камеры от станций наблюдения и видеозаписи.

Общая рекомендация №2. **Полный отход от аналоговых камер и DVR'ов будет медленным**

Поскольку DVR'ы совершенствуются, а аналоговые камеры остаются хорошим решением для небольших объектов, следует рассчитывать на медленный отход от использования аналоговых камер и DVR'ов. Другими словами, весьма маловероятно, что мы увидим массовый исход этих приборов из видеосистем в ближайшие 5 лет. Для этого должна возрасти ценовая конкуренция IP-камер, а решения на базе NVR должны стать проще в установке и управлении. Однако этот процесс требует развития в течение ряда лет.

Общая рекомендация №3. **Пристальное внимание к мегапиксельным камерам**

Пока что мегапиксельные камеры – это “темная лошадка”. Когда совокупная стоимость владения мегапиксельных камер (камера, пропускная способность, хранилище) приблизится к аналоговым камерам, тогда появится мощный финансовый стимул перехода на IP. Прямо сейчас трудно сказать, когда и как это произойдет. Однако, если вы стремитесь получить прибыль от этого перехода, сфокусируйте свои усилия на осознании и предугадывании момента, когда он произойдет.

Рекомендации для руководителя службы безопасности

Те 10% или 20% читателей, кто уже используют IP, могут переходить к следующей главе.

Все остальные в своих решениях должны учитывать следующие два фактора.

1. Размеры охраняемых объектов. Если это небольшие рестораны быстрого питания или бутики розничной торговли, выделите время на изучение IP, не торопитесь. Если же объекты большие, вам нужно энергично двигаться в направлении IP.

2. Возможности вашего DVR. Оцените достижения поставщика вашего DVR. Если это новинки, например, такие, что DVR гибридный, поддерживает аналитику, обеспечивает центральное управление и т.д., то, вероятно, с ним не будет проблем в течение многих лет. Если же DVR не поддерживает данные функции, то вы можете пропустить волну нового поколения, которая обеспечивает уменьшение трудозатрат и сокращение потерь. В этом случае начните изучать возможности перехода на новую IP-систему.

Глава 9. Важность гибридных DVR’ов/NVR’ов

Практически все руководители служб безопасности используют DVR’ы. Кое-кто перешел на NVR’ы, а некоторые до сих пор эксплуатируют видеомагнитофоны, однако 80% всех руководителей служб безопасности в настоящее время используют DVR’ы. В таком случае, что же делать с этими самыми DVR’ами и куда двигаться дальше? – это очень непростой вопрос. Возможным решением могут быть гибридные системы.

Гибридный NVR/DVR – это прибор (специализированный компьютер), который может одновременно поддерживать как IP-камеры, так и непосредственно подключенные к нему аналоговые камеры. Этим обеспечивается простота и гибкость решения. Клиенты могут начать с уже существующих аналоговых камер и не спеша переходить на IP-камеры. Особенно, в отличие от “чистого” NVR, при использовании гибридного NVR’а/DVR’а отпадает необходимость в отдельном видео кодере для подключения аналоговых камер.

В настоящее время почти все традиционные поставщики NVR’ов/DVR’ов предлагают гибридные NVR’ы/DVR’ы. Однако у многих специалистов возникает вопрос: соответствует ли это потребностям клиентов или происходит лишь от того, что традиционным поставщикам DVR’ов реализовать это несложно?

Как бы то ни было, но гибридный NVR/DVR – это довольно разумное решение, часто он играет главную роль в самых различных проектах видеонаблюдения:

- в настоящее время более 80% камер являются аналоговыми, и большинству из них предстоит еще много лет работы;
- во многих приложениях (возможно, не менее, чем в 30% систем), ограничения по пропускной способности заставляют клиентов размещать видеорегистраторы удаленно от поста наблюдения, вблизи камер.

В этих условиях системы на базе гибридных NVR'ов/DVR'ов будут весьма привлекательными. А поскольку подобные условия являются достаточно типичными, то это будет основным фактором как для многих руководителей служб безопасности, так и для всей отрасли в целом. Чтобы понять, почему этот фактор является главным, рассмотрим главные преимущества NVR'а и выясним, почему в данных условиях они уменьшаются.

Основным достоинством "чистого" NVR'а является объединение в нем функций управления видеонаблюдением и хранилища. Вместо того, чтобы управлять сигналами от десятков камер на объектах фрагментами по 16 или 32 канала, можно использовать объединяющие серверы и кластерные хранилища. Эти серверы и кластерные хранилища позволяют снизить стоимость оборудования, энергопотребление и затраты на обслуживание. Действительно, вначале многие последователи NVR'ов и IP-видеосистем добивались этого благодаря отмеченному достоинству.

Наибольшую проблему для отмеченного объединения создают ограничения пропускной способности. Это объединение функций требует, чтобы сигналы камер из различных частей объекта (объектов) передавались бы на центральный пункт (или пункты) наблюдения. Для этого требуется достаточная пропускная способность. Внутри локальный сети (как правило, внутри здания) в наличии достаточная пропускная способность, а сам трафик довольно дешевый. Что же касается централизованного хранилища и управления видеонаблюдением в глобальной сети WAN, то вот это может потребовать затрат в сотни, а то и тысячи долларов в месяц; этим сводятся на нет все достоинства объединения функций.

При наличии многих распределенных объектов, имеющих от 4 до 32 камер, компании будут вынуждены осуществлять управление локальными сигналами и хранение записей в соответствующих помещениях объектов. Конечно, здесь нет ничего нового, поскольку это уже давно применяется с DVR'ами. Однако это оказывает влияние на NVR-бизнес и побуждает использовать гибридные NVR/DVR-системы.

Экономическое сравнение гибридного NVR/DVR'а с "чистым" NVR'ом

При использовании менее 32 камер и необходимости запоминать и управлять сигналами от этих камер на объекте экономические показатели гибридных NVR/DVR'ов намного лучше, чем у чистых NVR'ов.

Гибридный NVR/DVR среднего класса (от 16 до 32 каналов) стоит примерно от 6000 USD до 8000 USD (для всех оценок используются данные из Google). Гибридный NVR/DVR осуществляет кодирование видео, хранение, управление и обслуживание, "все в одном", причем, настройки его являются простейшими и они могут осуществляться на самом объекте.

По сравнению с этим, решение на базе "чистого" NVR может быть на (20… 50)% дороже гибридной системы, и оно является более сложным в настройке и обслуживании. Повышенные затраты образуются:

1. за счет необходимости приобретения автономных кодеров для преобразования аналоговых камер в IP-камеры (от 200 USD до 300 USD в расчете на одну камеру),

2. приобретением лицензий на программное обеспечение для NVR (от 100 USD до 150 USD в расчете на одну камеру),

3. приобретением персонального компьютера/сервера с хранилищем (от 75 USD до 125 USD в расчете на одну камеру).

Кроме того, необходимо установить сервер, загрузить в него программное обеспечение, настроить операционную систему, сконфигурировать кодеры, установить соединения между кодерами и NVR. Это также требует дополнительной площади, дополнительных IP-адресов, а поскольку теперь имеется множество систем, то возрастают риски, связанные с их интеграцией и проблемы с последующим обслуживанием.

Использование NVR'а является намного более сложным и времязатратным по сравнению с гибридным NVR'ом/DVR'ом, который можно считать сравнительно близким к plug and play. В крупномасштабных проектах, где объединены сотни камер, экономия средств зачастую может служить оправданием дополнительной сложности и затратам времени на установку. Однако в проектах с небольшим числом камер затраты являются достаточно существенным фактором.

Гибридные NVR'ы/DVR'ы обеспечивают постепенный переход

Любому клиенту больше всего хотелось бы получить гибридный NVR/DVR от того же поставщика, у которого он до этого приобретал DVR. Даже если клиенту не особенно нравится данный продавец DVR'ов, однако весь его персонал обучен на использовании клиентского программного обеспечения этих DVR'ов. Более того, часто все DVR'ы приобретаются у одного продавца, так что персонал не должен волноваться, какое клиентское программное обеспечение будет использовать. Обычно для гибридных систем может быть использовано то же клиентское программное обеспечение, что и для DVR'ов. Это позволяет сделать переход безболезненным и прозрачным для пользователей. Клиенты хотят осуществлять переход, однако по мере его приближения главным фактором реализации существующих процессов и продуктов является удобство работы персонала.

Недостаток гибридных DVR'ов/NVR'ов

Самым большим недостатком гибридных DVR'ов/NVR'ов является то, что в реальности многие из них не являются гибридными. Истинно гибридные приборы должны быть одинаково гибкими, как для IP-, так и для аналоговых камер. Стандартом должна быть возможность работы с различными IP- и аналоговыми камерами в различных сочетаниях. Также стандартной должна быть поддержка различных IP- и мегапиксельных камер. Хорошим примером реального гибрида может служить продукция компании Exacq.

Проблемой является то, что существует большое число якобы гибридных систем, которые обеспечивают лишь кажущуюся поддержку одновременного использования различных IP-камер. Частым приемом является рекламирование работы с 16 аналоговыми входами, в дополнение к которым можно подключать только несколько IP-камер, лишь одного или двух поставщиков. Примером фальшивого гибрида может служить модель Symdec производства GE.

Предполагается, что гибридные системы обеспечат гибкость в переходе на IP. Однако указанный подход скорее рекламный трюк, нежели реальная выгода покупателю.

Быть открытым – это тренд, в то время, как недостаточно ясное понятие “открытость”, объявленная всеми, в реальности труднодостижима.

Это надо хорошо понимать еще до того, как приобретать систему управления видеонаблюдением или составлять ее спецификацию.

Не так давно я беседовал с одним из наиболее известных и уважаемых специалистов в области CCTV. Он выразил свое разочарование и беспокойство в том, что поставщик утверждал, что их система является открытой, а на практике все оказалось совсем не так. Это нанесло серьезный удар по его проекту системы. И если уж такой специалист попался на этом, то подобное может произойти с любым из нас.

И здесь я вижу три основных проблемы:

- размытость термина “открытость” (что это означает на самом деле?),
- каждый заявляет, что его система открытая (даже если это не так),
- открытую систему создать трудно (однако обычно это воспринимается как нечто простое).

По этим причинам можно так и не узнать правды о системе и оказаться в ловушке.

Размытость термина “открытость”

В простейшем случае под открытой системой понимается система, которая может работать с другими системами различных производителей. Однако с каким числом других систем данная система должна нормально работать, чтобы называться открытой? И с каким числом различных производителей?

Авторитетные лидеры индустрии часто определяют открытость, как способность работать с системами одного или двух производителей одной категории. Конечно, это похоже на открытую систему, только вот достаточно ли она открытая? Для большинства пользователей, увы, нет, и такая система представляет большой риск, а когда придет пора интегрировать ее с другой системой, может оказаться, что она просто не будет с ней работать

Каждый заявляет, что его система открытая

Мне кажется, что вот это – наиболее опасный момент в дискуссии об “открытости”. Простой пример: политики осознали, что расизм не приемлем. Привело ли это к тому, что среди политиков не стало расистов? Конечно, нет. Результатом стало лишь то, что политики понимают, что надо избегать расистских высказываний, и заявляют о равенстве всех наций. Подобная ситуация и с системами видеонаблюдения.

Вне зависимости, насколько система закрыта, специалисты по продажам и маркетингу знают, что должны заявлять, что система открыта.

Официально заявлять клиенту, что система не является открытой, очень рискованно; чтобы снять эту проблему производители говорят, что система открытая. А поскольку повсеместно используемое определение открытости является столь расплывчатым, то подобные заявления делать довольно легко, без каких-либо оговорок.

Открытую систему создать трудно

Такое впечатление, что продавцы выдают желаемое за действительное (как если бы само заявление о том, что система открытая, уже делало бы ее открытой).

Это подкрепляется абсурдным заявлением “У нас есть API”. И хотя Вам действительно требуется API, но само по себе наличие API совершенно недостаточно. Это как если бы заявить, что вы – шеф-повар, хотя умеете готовить лишь гамбургеры.

В реальности же, наличие действительно открытой системы, накладывает на продавца огромные обязательства. Это означает оптимизацию API, делая ее максимально простой для самых разных пользователей. Это означает возможность интеграции самими пользователями с целью поддержки разных клиентов, которые используют данную технологию – в противном случае подобную систему нельзя назвать открытой. И быть может, самое главное – это означает огромные усилия разработчиков по реальной поддержке сотен устройств на самых различных объектах.

Один из моих любимых вопросов: “Какие продукты вы реально поддерживаете в настоящее время?”. Это позволяет разоблачать пиар и недобросовестную рекламу в отношении “открытых систем”. Большинство продавцов используют такой прием: если их систему теоретически возможно интегрировать с другими продуктами, то они заявляют, что система поддерживает и данный продукт. Будьте осторожны! Уточняйте подробности и добивайтесь истины.

Вывод

В первую очередь нам следует быть внимательными относительно правильного толкования понятия “открытость”. Я даже думаю, что может быть следует начать поиск более подходящих оценок и определений того, какую систему можно назвать открытой.

Глава 11. Опасность коробочных решений

Опасным и требующим больших усилий по продвижению является для компаний продажа коробочных решений систем видеонаблюдения. Продавая в одном комплекте камеры, кодеры и системы управления IP-видеонаблюдением, поставщики надеются соблазнить клиента интегрированным и законченным решением.

Самое смешное, что пока все на словах выступают за открытые платформы, индустрия явственно движется в сторону все более тесно увязанных комплектов. Мне это кажется весьма рискованным, а потому следует ясно представлять опасность приобретения подобных “решений” “коробок”. Сначала я действительно называл их решениями, но теперь полагаю, что это неудачное выражение. Поэтому и поменял его на “коробки”, что лучше отражает суть данного явления.

Кто продает коробочные решения? Компании Verint, March, American Dynamics, Pelco, Cisco, DvTel, Bosch, IndigoVision, Avigilon. Что-то подобное теперь можно заметить у Axis с экспансией их Cam Station Вот уже и Panasonic, анонсировав это, двинулся в сторону продаж “решений”, то бишь, коробок Сейчас проще сказать, кто не торгует коробками (Наиболее крупным игроком рынка является Milestone). И что интересно, 5 лет назад большинство этих компаний специализировалось лишь на системах управления или камерах. Как видим, тенденция усиливается.

Продавцам нравится идея продажи коробок, поскольку она содержит возможность увеличения дохода (за счет перекрестных продаж) и увеличения прибыли (за счет

комплектования товаров). Кроме того, они могут говорить о себе, что они развивают рынок и создают новые ценности и т.д. и т.п.

Я не сомневаюсь, что отдельные продавцы действительно это делают, однако если существуют десятки продавцов практически одних и тех же коробок, то все мы оказываемся в довольно рискованной ситуации.

Опасность №1. Параметры коробок являются слишком общими

У покупателей видеосистем самые различные требования. Однако большинство коробок позиционируется для "горизонтального" рынка (то есть они не могут быть оптимальными для любого специфического использования). Коробки могут ограничивать гибкость и адаптируемость к различным вариантам их использования. Поэтому надо быть внимательным, чтобы понимать, соответствует ли данная коробка исходным требованиям.

Опасность №2. Можно оказаться скованным, если выбрать устаревшую на рынке коробку

Поскольку коробками торгует большое число продавцов, то есть среди них и аутсайдеры. Трудно предположить, что из десятков компаний, предлагающих в общем-то один и тот же товар, все из них одинаково успешны. Если приобрести коробки неудачников рынка, то вместе с такими коробками можно получить и проблемы. Будет очень трудно расширить возможности коробочного решения, и можно оказаться в ловушке из-за его ограничений.

Опасность №3. Вы под контролем, если выбрали коробку лидера рынка

С момента, как вы приобрели коробку, вы становитесь в зависимости от милости продавца. Вот почему так много враждебности в отношении таких компаний, как GE Security или Tyco. Вы покупаете их коробку, а они покупают вас (и знают об этом). Ваши просьбы о поддержке продуктов третьей стороны или о новых желательных функциях слишком слабы и нежелательны, чтобы быть реализованными (даже если вы сверхважный клиент). Все это делает решения с IP-видео похожими на те, с проблемами которых мы боролись последнее десятилетие.

Я не говорю, что не следует покупать коробки. Некоторые из них мне кажутся чрезвычайно сильным решением (особенно в той мере, в какой они сосредоточены на каком-то вертикальном рынке). Однако при такой покупке следует четко представлять сопутствующие действия и степень риска при этом.

Глава 12. Как читать маркетинговые материалы

Практически вся информация по IP-видео – это продающие тексты. Для принятия правильного решения такой материал следует анализировать и читать критически.

Сначала я не верил, что большая часть информации - это маркетинговые материалы продавцов. Очевидно, что информация на сайтах и в пресс-релизах является маркетинговым материалом, однако есть ведь еще статьи и отчеты в журналах. Однако почти все статьи, найденные мною в десятках журналов, написаны продавцами (как правило, руководителями маркетинговой службы). Более того, большинство из этих статей без сомнения являются рекламными текстами, используемыми продавцами для их коммерческих предложений. Они декларируют достоинства новых технологий на фоне

рекламы своих компаний, игнорируя при этом критические взгляды. Даже свежие отчеты являются обычными копиями или выдержками из пресс-релизов.

Таким образом, вам по-настоящему нужно быть внимательным и понимать, ради чего написан текст, который вы читаете. Я приучил себя относиться критически к тому, что я читаю, это помогает осознавать, насколько логична данная публикация. Если вы хотите принимать верные решения и быстро понимать реальную ценность того, что вы читаете, я приглашаю вас воспользоваться моими приемами, которыми хочу здесь поделиться.

Лучший анализ такой информации сможет реально уберечь вас от ошибок и проблем в будущем.

В то же время я надеюсь, что продавцы будут менять свое отношение к маркетинговым материалам. Мне кажется, честная информация выгодна всем – об этом я говорю всегда и повсюду.

Вот мои основные рекомендации по чтению маркетинговых материалов:

- определяйте, насколько хорошо работает то, что вам предлагают,
- определяйте, какие преимущества дает данное предложение по сравнению с наилучшей альтернативой,
- - определяйте цену данного предложения.

1. Насколько хорошо это работает

В маркетинговых материалах, как правило, в восторженных тонах рассказывается о том, для чего предназначено данное предложение. Это прекрасно для установления потенциальных возможностей продукта, что является необходимым для дальнейших коммуникаций. Это первый шаг к пониманию того, что клиенты могут ожидать от данного предложения и в чем его разница по сравнению с аналогами.

Однако проблема в том, что все это описывается настолько расплывчато, что читатель не в силах понять, насколько это соответствует его требованиям. Самое главное, очень редко в маркетинговом материале обсуждается, насколько хорошо работает то, что предлагается, и насколько хорошо это может работать в других приложениях. Я наблюдал, как подобное происходило по двум причинам:

- когда продавец не уверен, какой сегмент рынка соответствует его товару,
- когда продавец хочет создать максимально широкую сеть сбыта, не потеряв ни одного потенциального клиента.

В любом случае, читателю очень трудно понять, насколько предложение соответствует его задаче.

Я думаю, что в конечном итоге это никому не выгодно. В краткосрочной перспективе продавец может выиграть за счет сюиминутной продажи. Однако даже для продавца это может создавать проблемы. Если реализация проекта некачественная (а она часто бывает такой, если товар плохо подходит задаче), мала вероятность повторных продаж или привлечения партнеров. По существу, это повышает себестоимость реализованной продукции и ограничивает рост продаж в долгосрочной перспективе.

Как читатель, вы должны четко спросить себя, насколько хорошо это будет работать? Рассмотрите, какие производственные проблемы или внешние условия могут помешать проекту. Поскольку вряд ли вы получите от продавца четкий и ясный ответ, вам нужно сделать это самому, чтобы не ошибиться в выборе решения.

2. Ближайшая наилучшая альтернатива

В большинстве маркетинговых материалов приукрашиваются преимущества их систем. Например, поставщики NVR'ов обычно заявляют о таких их достоинствах, которые имеются даже у бюджетных DVR'ов. Продавцы мегапиксельных камер строят предположения о возможностях использования их камер, которые почти никогда не используются на практике. По существу, при сравнении они делают перекос в сторону увеличения положительных свойств своих товаров. (Примечание: это является обычным для любой категории товаров, просто в настоящее время NVR'ы и мегапиксельные камеры - два больших продуктовых направления).

Это вызывает путаницу в конкретных отличиях предлагаемых продуктов. Действительно инновационные решения могут потеряться в огромных перечнях традиционных свойств и функциональных возможностей. Конечных пользователей могут подталкивать к покупке более сложных и дорогих продуктов, которые в реальности не приносят их проектам лучших показателей.

3. Цена вопроса

Продавцы редко обсуждают стоимость своих предложений. Как правило, озвучиваются расплывчатые заявления вида "существенная ROI" (Return on Investment – окупаемость инвестиций) или "значительно возросшая ценность". Продавцы обоснованно беспокоятся, что кто-то может вмешаться в их дилерскую политику цен для конечных пользователей. Кроме того, зачастую они беспокоятся, что разглашение цены отпугнет некоторых покупателей, поэтому лучше акцентировать внимание на тех преимуществах, которые они получат, а цену сообщать клиенту лишь когда тот согласится на покупку.

Огромным недостатком неразглашения цен является то, что читатели не могут определить "ценность" или "ROI". По определению, не имея представления о цене, вы не можете рассчитать финансовую отдачу. И это не просто математическая проблема. Это весьма практический вопрос, поскольку читатели не могут понять, является ли данное предложение приемлемым для их бюджетов. Подобное я вижу постоянно в статьях, посвященных RAID, QoS, IP multicast, избыточным серверам. Цены на такие возможности/продукты могут быть очень высокими. Тем, кто пытаются оценить, подходит ли данное решение, трудно это сделать, не зная даже порядка цены.

Было бы весьма ценно, если бы продавцы сообщали хотя бы приблизительную цену своих продуктов. Не требуется знание какой-то договорной цены; прекрасно, если будет известна хотя бы рекомендованная производителем розничная цена. Например, цена за вашу мегапиксельную камеру ближе к 500 USD? к 1000 USD? К 1500 USD? к 2000 USD? Предоставление приблизительного диапазона цен будет достаточным, чтобы читатель мог оценить, насколько это соответствует его бюджету, и сколько товаров нужно заказать.

Если во время чтения маркетингового материала вы будете держать в голове перечисленные пункты, вы сможете лучше определять истинную ценность предложений. До тех, пока маркетинговые материалы не станут более ясными (если такое вообще

возможно), применение этих рекомендаций должно помочь в оценке подобной информации.

Глава 13. Как оценить новую технологию

В большинстве случаев, вывод на рынок новых технологий заканчивается провалом; зато в случае успеха достигаемое преимущество может быть огромным. Вопрос лишь в том, как эффективно определять, какая из новых технологий является реальной – это позволит не только избежать беды, но и получить драгоценные вознаграждения.

Наверняка вы знаете десятки компаний. Каждая новая перспективная технология спешит пробиться во многие компании в надежде быть ими принятой. При этом происходит не просто оценка самой технологии – это еще и выяснение, у каких компаний уже имеется выигрышное решение.

Как правило, вы не можете провести подобную оценку, опираясь исключительно на собственные знания. Большая часть времени при оценке новой технологии уходит на поиск недостающих специфических знаний в этой области. Поэтому требуется выбрать тактику и методы, дающие вам, как проектировщику, наилучшие шансы для победы.

В данной главе рассматриваются 5 основных рекомендаций, созданных мною на протяжении многих лет работы в качестве интегратора и производителя. Итак:

1. Убедитесь, что маркетинговые материалы содержат технические подробности.
2. Задавайте конкретные вопросы о возможных проблемах данного продукта.
3. Убедитесь, что ваш продавец не является патологическим лгуном.
4. Спросите продавца, насколько хорошо его продукт будет работать со всеми элементами вашей системы.
5. Проведите тестирование под большой нагрузкой.

Содержат ли маркетинговые материалы технические подробности?

Первое, что следует сделать в самом начале, это проверить технический уровень маркетинговых материалов. Вам не требуется знание технической терминологии. Для начала просто просмотрите маркетинговый материал и оцените, сколько в нем обычного текста, а сколько аббревиатур, цифр, диаграмм и т.д.

Недостаток технических подробностей является точным индикатором того, что либо это концептуальный товар, либо несуществующий в природе. Нередко недостаток технических подробностей - следствие того, что компания продвигает саму идею, но у компании мало ресурсов для ее инженерной реализации. В некоторых случаях инженерный состав компании сильный, но продукт еще настолько незрелый, что у них просто нет достаточного количества технических подробностей для представления товара.

Я вообще решил отказаться рассматривать материалы компаний, которые не отвечают этому критерию. С другой стороны, только то, что в материалах данной компании содержатся технические подробности, совсем не означает, что все это точно будет работать (компания может быть особенно изощренной в маркетинге, а могут здесь быть и другие проблемы). Поэтому просто воспринимайте сказанное в качестве первого испытания.

Задаете ли вы конкретные вопросы о возможных проблемах?

Большинство людей вам явно не лгут, однако при этом и не говорят всю правду. Поскольку для большинства людей вранье является дискомфортным, то чаще всего они просто стараются избегать обсуждения неприятных вопросов. Если спросить: “Сколько компаний используют ваш продукт в своей деятельности?”, то большинство продавцов дадут ответ, близкий к истине. Ежели вы ничего не спросите, то практически никто из продавцов по собственной инициативе вам не сообщит, что их продукт никогда не использовался или используется всего лишь на одном-двух объектах. Строго говоря, они вам не лгут, однако результат при этом такой же, поскольку он заставляет вас делать неправильные выводы относительно основных моментов в процессе принятия решения. Если для зрелых продуктов многому можно доверять, то для продуктов новых технологий это является большим риском.

Дело в том, что у продуктов новых технологий всегда имеются проблемы. Это не значит, что такие продукты не следует использовать, однако надо точно знать, каковы эти проблемы. Поэтому прямо задайте свои вопросы, например, такие:

- На скольких объектах используется ваш продукт?
- Если взять три последних отказа вашего продукта на объектах - что явилось их причиной?
- В чем была причина отказов продукта предыдущих пилотных версий? (всех или хотя бы некоторых из них)
- Вы мне можете дать ссылки? (Не принимайте оправдания, что они не могут делиться информацией в силу ее особой важности для безопасности объектов. Для любого успешного продукта можно найти несколько клиентов, готовых об этом поговорить, особенно, если вы являетесь руководителем службы безопасности).

Просто помните, что ничего нельзя принимать на веру, задавайте вопросы.

Является ли продавец патологическим лгуном?

Патологические лгуны, занятые продвижением продуктов новых технологий, представляют собой большую опасность. Каждый раз такие продавцы упорно “вкручивают мозги”, уходя от обсуждения каких-то проблем или критики. Они могут быть настолько хороши, что вы ослабите свою бдительность, а ваш восторг от возможных преимуществ будет игнорировать проблемы. Это вдвойне опасно: во-первых, это лишает вас должной осмотрительности, а во-вторых, что намного хуже, у патологических лгунов, как правило, плохие продукты, поскольку они слишком заняты “вкручиванием мозгов”, чтобы создавать что-нибудь ценное.

Подобное было со мной, когда я работал интегратором. Мы участвовали в совещаниях, и подобный парень постоянно “вкручивал мозги” с предложением для нас, отклонял любые законные вопросы и старался создать при этом ощущение огромных преимуществ для нас без какого-то риска. В какой-то момент клиент задал ему технический вопрос, что-то вроде: “Вы используете протокол X?”, и этот парень тут же парировал: “Конечно”. Клиент, который был неплохим специалистом, и я – мы оба были захвачены врасплох. К сожалению, мой коллега не знал, что это был устаревший протокол, который уже никто не хотел использовать. После того, как мы покинули совещание я спросил этого парня, зачем он так сказал. И тот ответил мне: “Я пытался говорить им то, что они хотели услышать”.

Помните о том, что продавцы неспроста говорят вам именно то, что, как они считают, вы хотите услышать.

Наилучший способ разобраться, как оно на самом деле, это в сторонке от потенциального лгуна задать вопросы другому представителю продавца (обычно, это технический специалист). Сейчас большинство людей знает, являются ли их коллеги лгунами, однако сами они довольно неохотно говорят об этом напрямую. Поговорите с ними о рабочих проблемах и задайте этим людям конкретные вопросы. Этим способом вы довольно быстро получите правильное понимание проблем и поймете расхождение во взглядах представителей продавца.

Как это влияет на элементы вашей системы?

Продукты новой технологии обычно отказывают из-за непредвиденных проблем эксплуатации. В целом, это довольно просто обнаружить, когда технология используется для решения бизнес-проблем. С другой стороны, чрезвычайно трудно понять, какие эксплуатационные проблемы вы приобрели вместе с продуктом, разместив и используя на объекте данную технологию.

Это является наиболее важным моментом в оценке продуктов новых технологий. Вне зависимости от того, что бы ни было сказано или обещано, независимо от потенциальных возможностей - в зависимости от того, как технология влияет на систему, это делает ее или работоспособной, или убивает систему. Очень часто технология сказывается на скрытом возрастании стоимости, а может быть и просто не способной работать совместно с существующими системами или процедурами.

Вы должны быть уверены, что понимаете, как новая технология будет взаимодействовать с существующими системами. У вас имеются работающие системы, и вы хотите, чтобы эти системы продолжали работать. Однако нередко обнаруживается, что эта технология не работает совместно с основными компонентами вашей существующей системы. Работая интегратором, я как-то при проектировании системы видеоаналитики приобрел себе головную боль из-за того, что не интегрировал видеоаналитику с существующим у клиента матричным коммутатором. Это была незначительная техническая подробность, которая привела к очень серьезной проблеме в работе системы. Пройдитесь по всем аспектам функционирования вашей системы и убедитесь, что среди них нет скрытых несовместимостей в работе.

Аналогичным образом - довольно легко подсчитать прямые затраты на продукт новой технологии, однако следует быть внимательным в отношении косвенных затрат, которые может повлечь за собой использование данного продукта.

Часто в новой технологии содержатся требования, которым не просто соответствовать при существующей системе. Такая технология может требовать намного большей пропускной способности или намного более мощных по сравнению с существующими компьютеров, или необходимости дополнительных тренингов и техподдержки. При анализе ваших затрат будьте готовы оценить, какими могут быть косвенные затраты - они нередко делают перспективный проект вообще нереализуемым.

Технология может быть хороша сама по себе, но при этом недостаточно хорошей для конкретных задач бизнеса. Вы должны быть уверены, что она действительно хорошая, в противном случае можно получить серьезную проблему функционирования системы. Зачастую технология существует для того, чтобы автоматизировать существующие процессы ручного труда. Довольно часто новая технология может заменить труд человека на (90… 95)%. Однако во многих случаях, с точки зрения функционирования или технической поддержки недостаток оставшихся (5… 10)% может создавать существенные

проблемы для бизнеса. Если вы используете систему распознавания по лицу человека для проверки входящих в дверь (верификация совместно с СКУД) и если система распознавания делает за время работы всего лишь 5% ошибок, то это может быть 5 или даже 20 человек в день, которых эти ошибки выводят из себя. Это может быть очень хорошая система с совершенной технологией, однако она может недостаточно хорошо соответствовать другим задачам бизнеса или вообще вашей компании.

Если вы тщательно оценили взаимодействие систем, их косвенные расходы а также соответствие бизнес-задачам и все эти требования удовлетворяются, то скорей всего, вас ждет удача.

Как это работает при большой нагрузке?

Одним из основных способов определения того, какое влияние оказывает новая технология на работоспособность системы, является создание пробного проекта. Пробные проекты используются часто, поэтому я здесь дам лишь пару советов.

Первое – убедитесь, что пробный проект оказывает на существующую систему наивысшую из возможных нагрузку. Часто тестирование проводится в лаборатории или в вашем офисе – это очень плохая идея. Офисный или лабораторный тест скрывает возможные проблемы и работает в пользу недобросовестных продавцов.

Насколько новый продукт способен выдерживать экстремальные условия и нагрузки – в этом главная разница между новыми и зрелыми продуктами. Нужно потратить много времени и сил, чтобы продукт отвечал реальным мировым задачам и был оптимизирован для работы в экстремальных условиях.

Поставить продукт в самые тяжелые условия работы – вот лучший способ оценить, насколько продукт готов для использования в системе. При таком подходе любые дефекты проявляются очень быстро (а не месяц спустя, когда проект уже запущен и проводить какие-то настройки очень трудно).

Использование продуктов новых технологий является наиболее мощным средствам создания конкурентного преимущества. Если вы руководитель службы безопасности, то это поможет вам реально отличиться и продвинуться в своей карьере. Если вы интегратор, это может привести к невероятному профессиональному росту. Я являюсь ярым пропагандистом использования продуктов новых технологий.

Очень важным является принятие правильных решений относительно продуктов новых технологий. Используйте рассмотренные приемы, и я надеюсь, что они помогут вам, не тратя времени, принимать наилучшие решения.

Глава 14. Как рассчитать окупаемость инвестиций (ROI) в видеонаблюдении

Расчеты ROI являются мощным инструментом, однако они могут оказаться искаженными. Хотя они и предназначены для объективного определения ценности решения, сами расчеты зачастую могут затемнять истину.

Цель данной публикации заключается в том, чтобы помочь руководителю службы безопасности лучше понимать расчеты ROI поставщика, а также помочь руководителю изменять или уточнять расчеты с целью получения точных и реалистических результатов.

Использование данных принципов может оказаться полезным также интеграторам и производителям.

Для выполнения качественных расчетов ROI требуется не только знание математики или финансов, но и детальное понимание работы систем. Если вы разберетесь в деталях работы, то и математика, и финансы для вас окажутся намного более простыми.

Вот четыре принципа подготовки к выполнению расчета ROI:

- знать альтернативное решение по отношению к предлагаемому решению (требующему инвестиций),
- знать полную стоимость,
- осознавать возможность технологических недоработок в инвестируемом решении,
- проверять корректность предположений о работе системы.

Принцип №1. Альтернативы

Наиболее частый трюк имитации ROI-анализа заключается в выборе альтернативы, которая по определению хуже, но при этом не соответствует вашей задаче. Этим грешат большинство продавцов. Вот жизненный пример с NVR'ами. Зачастую продавцы NVR'ов заявляют, что NVR'ы повышают рентабельность инвестиций за счет возможности централизованного мониторинга, а также возможности их интеграции с приложениями типа кассовых терминалов и СКУД. Хотя это абсолютная правда, но это не имеет отношения к ROI, поскольку то же самое делают и DVR'ы. Руководителю службы безопасности нет смысла сравнивать NVR с видеомагнитофоном или вообще непонятно с чем, поскольку у каждого руководителей имеется DVR и в качестве альтернативы NVR'у он будет рассматривать DVR. Для создания бизнес-предложения по NVR'у его следует сравнить с DVR'ом.

Например, если NVR стоит 10000 USD, а DVR стоит 8000 USD, инвестиции при расчете ROI будут равны 2000 USD (наценка для NVR по отношению к DVR). В то же время, продавец NVR'а мог бы заявить только о возврате инвестиций от возможностей, которые являются уникальными для NVR'а по сравнению с DVR'ом, исключив таким образом из рассмотрения такие аспекты, как централизованный мониторинг и интеграция приложений. Если вы не будете использовать подобный подход, а просто будете рассчитывать ROI от использования NVR'а в сравнении с видеомагнитофоном, вы просто выбросите деньги, заплатив лишнее за NVR, в то время как DVR мог бы работать у вас не хуже.

Примечание. Я считаю, что зачастую NVR'ы оказываются более ценными, чем DVR'ы, так что сказанное не является критикой сетевых видеорегистраторов. Здесь содержится критика самого процесса, часто используемого для оправдания решения в пользу приобретения NVR'а.

Поставщики мегапиксельных камер часто пропагандируют уменьшение числа камер, однако при этом расчеты ROI могут искажаться. Например, недавно в авторитетном докладе рассматривался вариант, по которому 13 аналоговых камер могли быть заменены на две 3-мегапиксельные камеры, обеспечивая при этом уличное видеонаблюдение с полем зрения 30 метров. В документе делается вывод, что решение с мегапиксельными камерами реально дешевле. Подобное допущение вводит в заблуждение, поскольку реальной альтернативой здесь является использование 2… 3 аналоговых камер. Это то, что в настоящее время использует большинство руководителей службы безопасности, и

если в качестве альтернативы использовать такое соотношение, то стоимость варианта с мегапиксельной камерой оказывается существенно выше варианта с аналоговыми камерами.

Примечание. Использование мегапиксельных камер в этом варианте, благодаря их высокому качеству, может обеспечить намного более высокий возврат инвестиций за счет возможности решения ранее недоступных задач. Здесь я возражаю не против использования их в данном проекте, а лишь уточняю метод финансового обоснования такого решения.

Руководитель службы безопасности и продавец мегапиксельных камер должны сосредоточиться на рассмотрении увеличившейся отдачи, получаемой конкретно за счет возросшего качества изображения. В частности, при рассмотрении ROI для мегапиксельных камер должны учитываться только проблемы, разрешаемые исключительно мегапиксельной камерой и которые не могут быть решены рассматриваемой в качестве альтернативы аналоговой камерой. Если при решении какой-то задачи решающим является распознавание автомобильных номеров, то здесь мегапиксельная камера имеет преимущество. Однако если для решения проблемы достаточно определять, что, к примеру, машина – белая Honda Civic, то для этого достаточно использовать и аналоговую камеру, а мегапиксельная камера не будет иметь преимущества.

Обычно такое разграничение размывается, однако если вы действительно хотите правильно определять ROI, то это является решающим фактором.

Принцип №2. Знайте полную стоимость

Часто в указываемом продавцом расчете возврата инвестиций не указываются косвенные затраты. Они становятся скрытыми затратами, которые в дальнейшем могут существенно снизить реальное значение ROI.

Одной из скрытых затрат видеоаналитики является необходимость мониторинга. В зависимости от уровня ложных срабатываний, возможно, потребуются соответствующие ресурсы для оценки и проверки тревог. Такие расходы могут оказаться весьма существенными. Вы можете получить технологию, работающую так, как обещалось в рекламе, однако чтобы довести ее до этого уровня, возможно, потребуется выделить дополнительные рабочие ресурсы. Убедитесь, что вы осознаете, что могут потребоваться какие-то косвенные расходы, и что вы это учитываете.

Другим примером косвенных затрат являются мегапиксельные камеры. При их использовании надо учитывать не только повышенную стоимость самих камер, но и повышенную стоимость хранилища и пропускной способности. Почти все мегапиксельные камеры в своей работе используют менее эффективную компрессию, (приводящую к качеству изображения, хуже), чем у аналоговых камер (текст в скобках добавлен мной. Ю.Г.). Итак, если вам от мегапиксельной камеры действительно нужно повышенная разрешающая способность, то это приведет к последующему росту расходов на хранилище (а зачастую и расходов на оплату сети).

С другой стороны, оба вида этих вида затрат могут быть оправданы, однако объективный анализ должен включать практически все дополнительные расходы.

Принцип №3. Технологические недоработки

Когда продавец рассчитывает вам ROI, как правило, он предполагает, что технология будет работать так, как им обещано в рекламе. Новая технология иногда отказывает. Также, случается, что технология работает, но не в тех условиях, которые требуются.

В этом, в частности, одна из основных проблем видеоаналитики. Легко заявить, что контроль периметра позволяет существенно снизить потери. Однако это зависит от того, насколько хорошо работает система. Если в условиях сильного снегопада объект перестает контролироваться, значит в таких условиях система не может работать должным образом. Это может сможет снизить заложенные в проекте возможности в отношении борьбы с материальными потерями. Аналогичным образом, возможно, вы захотите использовать мегапиксельную камеру для распознавания автомобильных номеров или лиц в очень плохо освещенном месте, ночью. Многие мегапиксельные камеры плохо работают в условиях низкой освещенности. Если в проекте вы заложили решение этих задач в темное время суток, то реально это может не работать.

Также, система может не работать по причине того, что она слишком сложна при эксплуатации, поэтому операторы ошибаются в всех случаях, которые только могут создаваться системой.

Внимательно проверьте все прогнозы поставщика и убедитесь, что возможные технологические недоработки отражены в расчете ROI.

Принцип №4. Предположения о работе системы

Поставщики могут только строить догадки о реальных условиях работы службы безопасности. Зачастую эти догадки слишком оптимистические или вообще не соответствуют ситуации на объекте. Примерами таких предположений являются материальные потери в расчете на одно происшествие, количество происшествий в месяц, количество происшествий, которые система позволит предотвратить.

В первую очередь вы должны задать вопрос и получить ответ, какие из этих предположений о работе системы нашли отражение в предоставленном продавцом расчете ROI. Сравните их с вашей реальной статистикой и пересчитайте для получения соответствующих значений. Сколько времени система действительно охраняет объект? Сколько происшествий в год можно реально предотвратить с новой системой (таких происшествий, которых нельзя было предотвратить с помощью прежней системы)?

Вероятно, все это будет отличаться от предположений поставщика, так что будьте готовы внести коррективы в расчеты рентабельности инвестиций.

Проблемами для всех финансовых моделей являются сделанные допущения. С использованием этих четырех принципов вы сможете лучше оценивать и определять допущения, делая это корректно. Определяйте скрытые затраты и проблемы, которые могут игнорироваться в теоретическом расчете ROI – это заставит ваших поставщиков быть честными перед вами.

Распутывайте частую путаницу и искажения в ROI, и вы будете награждены точным расчетом рентабельности инвестиций, обеспечивая прозрачность и подлинную ценность бизнеса.