

□ **Валерий Крутских,**
д.ф.-м.н., Генеральный директор ЗАО «МТТ Контрол»

- Беспроводные сети

Одним из трендов последних лет является бурное развитие беспроводных технологий. Системы видеонаблюдения также не избежали этого влияния. Беспроводная передача данных, как правило, применяется в видеосистемах для организации «последней мили» – как для передачи изображения от видеокамер, так и при просмотре видео на мобильных устройствах.

Наиболее распространенными технологиями беспроводных сетей на сегодняшний день являются Wi-Fi и, выросшие на базе сетей сотовой связи, 3G и 4G. Беспроводные сети, несомненно, расширяют возможности систем видеонаблюдения, но имеют свои особенности, достоинства и недостатки. Рассмотрим их подробнее.

Сегодня на рынке широко представлены видеокамеры с возможностью передачи видео по технологии Wi-Fi. Это позволяет устанавливать видеокамеры там, где затруднена или даже невозможна прокладка проводной локальной сети. Но при этом не стоит забывать, что любой видеокамере требуется электропитание, а это необходимость прокладки провода. Поэтому автономность Wi-Fi видеокамер достаточно условна. Кроме того, технология Wi-Fi разрабатывалась для построения беспроводных локальных сетей и имеет технические ограничения на максимальную дальность передачи данных, поэтому область ее применения, как правило, ограничена одним зданием или группой рядом стоящих зданий.

Технологии 3G и 4G выросли на базе технологий сотовой связи, и «в наследство» им досталась возможность широкого покрытия территории. 3G и 4G в современных системах видеонаблюдения, как правило, применяются для просмотра видеоизображения на мобильных устройствах – ноутбуках, планшетах, мобильных телефонах. Также для просмотра может использоваться и технология Wi-Fi, но с учетом

ограниченной области покрытия.

Несмотря на очевидные достоинства, у беспроводных технологий есть и недостатки.

Прежде всего, это относительно небольшая пропускная способность, что резко ограничивает возможности построения полнофункциональных видеосистем на базе беспроводных сетей. Например, при просмотре изображений с камер необходимо смотреть их либо последовательно в нормальном разрешении, либо в режиме мультискрена, но с низким разрешением. В реальной практике хорошо работают сети 4G, позволяющие смотреть видеопоток с частотой 25 кадров в секунду. В сетях 3G приходится уменьшать либо количество кадров, либо разрешение.

Также при разработке видеосистемы на базе беспроводной сети следует уделить особое внимание созданию инфраструктуры опорной сети, поскольку одновременная передача большого количества потоков видеоданных просто «обрушит» непригодную для этих целей беспроводную сеть. Поэтому профессиональная система видеонаблюдения на нескольких объектах требует управления потоками видеоданных.

- Управление потоками видеоданных.

Современная цифровая видеокамера может одновременно поддерживать 10-20 видеопотоков, что позволяет просматривать ее 10-20 пользователями одновременно. Однако когда изображение с одной видеокамеры просматривает большое количество посетителей, камеры не выдерживают. В небольших системах видеонаблюдения данный эффект проявляется не очень сильно, но с ростом системы проблемы, связанные с большим количеством видеопотоков, возрастают многократно.

Для решения данной проблемы мы в Группе компаний «Контроль» разработали специальный программно-аппаратный комплекс — мультиплексор, который обеспечивает распределение видеопотоков на большое количество пользователей. При

проведении тестирования данный мультиплексор обеспечивал устойчивый видеосигнал для подключения к камере до 50 тыс. пользователей одновременно.

Мультиплексор также способен выполнять и обратную функцию – «собирать» потоки видеоданных от разных источников и передавать их в виде единого потока.

Таким образом, ограничения на количество потоков видеоданных в больших системах видеонаблюдения успешно решаются с помощью дополнительного элемента системы – мультиплексора.

- *Облачные технологии*

Облачные технологии являются одним из трендов последних лет. Суть их состоит в том, что такие технические задачи систем видеонаблюдения, как обработка, запись, хранение и распределение видеопотоков, выносятся из пользовательской сферы и помещаются в «облако». Обслуживанием оборудования, находящегося в «облаке», занимается специализированная компания, а пользователю предоставляется услуга видеонаблюдения.

Удаленное хранение видеоданных имеет ряд преимуществ.

Прежде всего, удаленное хранилище данных более защищено по сравнению с локальным видеоархивом. Например, злоумышленникам, которые проникли на объект, не составит труда забрать диск из стационарного видеорегистратора. А если видеoinформация дублируется в «облачное» хранилище, то видеозапись будет в сохранности. Причем хранилища данных могут быть размещены в любой точке мира, что повышает катастрофоустойчивость системы.

«Облачное» хранилище видеоданных экономически выгодно пользователю, поскольку

нет необходимости вкладывать большие средства в расширение системы. Если возникнет необходимость расширения видеосистемы, то поставщик услуги просто по факту выделит пользователю большую мощность за дополнительную плату.

Централизованное техническое обслуживание оборудования «облачной» системы видеонаблюдения позволяет значительно снизить эксплуатационные расходы. Кроме того, специализированный провайдер, как правило, имеет более подготовленный штат технических специалистов по сравнению с пользователем видеосистемы.

- Мобильные приложения для использования в интернет

«Облачные» технологии позволяют предоставлять видеонаблюдение как услугу. При этом доставку контента от «облачного» центра к конечному пользователю можно осуществлять через интернет, используя технологии Wi-Fi или 4G.

При использовании интернета для доставки видеоданных к потребителю просмотр, как правило, осуществляется на стандартных устройствах – планшетах, ноутбуках, мобильных телефонах. Есть два способа просматривать видео в таких системах видеонаблюдения – можно установить специальную клиентскую программу, либо просматривать видео в окне браузера (правда, в случае просмотра через браузер пользователь получает намного меньшую функциональность по сравнению со специализированной клиентской программой).

Однако оба этих способа просмотра очень чувствительны к задержкам в работе сети – при возникновении задержек изображение замирает, распадается на фрагменты, а то и вовсе пропадает. А в интернете задержки в работе – обычное явление. Кроме того, любая программа просмотра видео, как правило, разрабатывается под конкретный тип видеокамер, поэтому при попытке подключения дополнительных видеокамер, особенно другого производителя, возникают проблемы с просмотром видеоданных.

Как одно из решений данной проблемы, можно, в частности, использовать

вышеупомянутый мультиплексор, одной из функций которого и является подготовка потоков видеоданных для программ просмотра видео. С помощью мультиплексора в любую существующую видеосистему можно вводить любые видеокамеры. При этом мультиплексор может работать не только с собственной клиентской программой видеонаблюдения XViewision, но и с программами других производителей.

- *Значительное возрастание количества камер, проблемы просмотра и архивирования*

Системы видеонаблюдения устанавливаются для решения задач безопасности. Но таковые не ограничиваются только видеофиксацией каких-либо событий. Часто требуется не только увидеть, что человек делает, но и идентифицировать его, не только зафиксировать факт проезда машины на объект, но и проследить историю ее передвижений по номеру. Для решения таких задач используются системы распознавания лица и номеров. Поэтому в современной профессиональной видеосистеме важны не только функции просмотра, но и аналитика, интеграция с другими системами безопасности и создание больших хранилищ видеоданных.

Тенденцией последнего времени стало значительное увеличение количества видеокамер в системах видеонаблюдения. Даже на небольшом объекте их может быть установлено несколько десятков, а в системе «Безопасный город», например, видеокамер сотни и тысячи. В таких условиях остро встает вопрос об эффективности видеонаблюдения в реальном времени, а также о поиске записанной ранее информации.

Даже на небольшом объекте оператор видеонаблюдения не может долго следить за несколькими десятками камер. Его внимание теряется, глаз «замыливается». Исправить ситуацию в профессиональных видеосистемах пытались аналитикой: автоматически отслеживали пересечение линий, изменение скорости движения, использовали детектор движения. Несмотря на то, что аналитические системы активно развиваются более 10 лет, реальных улучшений в сфере безопасности не наблюдается, так как невозможно заранее точно определить место происшествия.

Новая тактика видеонаблюдения, которую мы предлагаем, и которая становится трендом последнего времени, заключается в том, что помимо визуального наблюдения за несколькими камерами, основной упор делается на том, что все видеокамеры записывают в архив все происходящее в непрерывном режиме. Архив делится на две части: архив оперативного хранения и архив долговременного хранения. Размер оперативного архива определяется технологически или с точки зрения безопасности: неделя, месяц, год. После завершения времени оперативного хранения данные в архиве обрабатываются по заданному алгоритму. Пользователь сам определяет, какие видеокadres следует оставить. Это могут быть кадры с движением, либо кадры за определенный промежуток времени, либо видеокadres, связанные с определенными событиями. Отсортированные кадры переносятся в архив долговременного хранения, размер которого также может варьироваться. Создание больших хранилищ — это сложная технологическая задача. Достаточно сказать, что их размеры уже составляют не Терабайты, а Петабайты видеоданных. Специалисты группы компаний «Контрол» разработали такие архивы. Это позволило реализовать архив общим объемом 5 Петабайт для хранения информации в течение трех лет от 500 видеоисточников.

Преимуществом данного подхода является то, что мы никогда не пропустим какое-либо событие. Не надо заботиться о том, включилась запись или нет, был оператор на месте или нет. Из минусов стоит выделить большой объем видеоархивов, а также большой объем информации, который следует анализировать. Вручную просматривать такой объем данных без предварительной информации об инциденте невозможно. Чтобы просмотреть все видеокамеры системы уровня города, понадобится не одна неделя, что лишает смысла сам поиск. В качестве решения было предложено использовать для поиска специальные алгоритмы метаданных. Метаданными называется любая информация, связанная с видеоданными. Это могут быть результаты работы детектора движения, сигналы тревоги, информация о срабатывании датчиков, команды оператора, информация от смежных систем безопасности, например, системы контроля доступа или системы распознавания номеров автомобилей. Особо важная роль отводится интеграции различных систем, которая дает дополнительную информацию для метаданных. Системы контроля доступа, системы защиты информации, системы документооборота, электронная почта, телефония и другие системы привлекаются к поиску по архиву с помощью метаданных.

Во время записи видеомассив размечается с помощью метаданных — иными словами, каждому элементу метаданных ставится в соответствие один или несколько связанных с ними видеофрагментов. Таким образом, поиск становится более эффективным и быстрым. Такой архив метаданных, например, нами был реализован в линейке продуктов системы видеонаблюдения XViewision.

- Организация диагностики, централизованной технической поддержки и обслуживания, повышение надежности

При построении больших профессиональных систем видеонаблюдения возрастает роль таких факторов, как надежность, возможность диагностики, восстановление после сбоев, организация технической поддержки и обслуживания. Не последнюю роль играет и эффективная защита системы от злоумышленников, а также потерь данных из-за ошибок пользователей.

Для профессионалов важна надежность больших хранилищ видеоданных. В блоках видеоархивов, разработанных нашими специалистами, например, работоспособность блока сохраняется при выходе из строя до трех жестких дисков одновременно, замена неисправных дисков может производиться в «горячем» режиме без остановки работы блока. Кроме того, для повышения надежности системы производится стартовая диагностика всех элементов и непрерывная диагностика параметров блоков в процессе работы. Для поддержания работоспособности системы видеонаблюдения в любой момент времени в наших системах реализованы подсистемы мониторинга электропитания и мониторинга параметров среды. Для исключения потерь данных создан механизм восстановления системы после сбоев с помощью снапшотов (моментальных снимков системы и данных), используется система защиты от модификации данных. С целью исключения влияния человеческого фактора разработано клиентское рабочее место, жесткий диск которого находится в охраняемом помещении, с возможностью удаленной загрузки и с защитой от модификации. Управление и администрирование системой видеонаблюдения осуществляется централизованно с возможностью удаленной настройки и загрузки рабочих мест.

- Видеонаблюдение для защиты информации

По данным агентства Bloomberg*, с 2009 года было совершено более 555 миллионов случаев потери/кражи данных, в том числе персональных. Наибольшую угрозу представляют хакеры, человеческий фактор и физическая кража оборудования. Традиционные средства защиты имеют ряд недостатков: они направлены в основном на защиту от внешних угроз; система защиты является частью охраняемого объекта; защита осуществляется в виртуальном, а не физическом пространстве. Поэтому мы

разработали новый программно-аппаратный комплекс Xvmatic для противодействия внешним и внутренним угрозам, включающий информационную и физическую защиту данных.

Прежде всего, мы предлагаем разделять оперативный массив дисков и клиентских рабочих мест операторов видеонаблюдения, которые загружаются с сервера при каждом включении. Клиентский образ создается из «золотой» копии операционной системы с установленными программами. При завершении работы клиентский образ стирается, уничтожая все внесенные при работе вирусы и зловреды. В отличие от традиционных систем с «тонкими» клиентами, вычисления выполняются непосредственно на рабочем месте, используя его процессор, 3d-ускоритель и всю периферию. При этом диска в системном блоке рабочего места нет.

Благодаря разделению дискового пространства на оперативное и долговременное, обеспечивается защита от программных закладок «нулевого дня». В оперативном дисковом пространстве работа ведется в течение одной-двух недель. В случае аварии можно быстро восстановить систему после сбоя. В долговременном дисковом пространстве работа ведется в течение года. В каждый момент времени задействован только один сервер. Поэтому в «нулевой день» данные на большей части оборудования недоступны для атаки.

Включая в систему защиты технические средства охраны – видеонаблюдение, контроль доступа, биометрию и сигнализацию, – можно однозначно идентифицировать сотрудника не только в виртуальном, но и в физическом пространстве. Дополнительно осуществляется видеонаблюдение в помещениях, регистрируются изображения на мониторах рабочих мест.

Активно в защите информации мы применяем так называемый Сценарий «4-х глаз», когда на одном рабочем месте ведется одновременная работа двух сотрудников, один из которых оператор, а другой — контролер. Если контролер или оператор покинет помещение, в котором находится рабочее место, сеанс автоматически прерывается. При этом отключается только монитор, клавиатура и мышь, а исполняемая программа не прерывается. Контролируется присутствие обоих сотрудников как раз за счет видеокамеры у монитора компьютера, непрерывно распознающей лица людей.

Интересным является режим работы под контролем дежурного службы безопасности.

Постоянный мониторинг действий пользователя осуществляется посредством видеокамеры, расположенной перед оператором, и устройства захвата изображения на экране компьютера. В дежурной службе отображается: текущий экран, фотография сотрудника из базы данных и реальное изображение, полученное с видеокамеры. Если у оператора дежурной службы возникают какие-либо подозрения или сомнения в правомерности действий пользователя рабочего места, он может удаленно отключить клавиатуру, монитор и мышь и в дальнейшем разобраться в инциденте.

За счет систем видеонаблюдения может происходить также удаленный контроль руководителем. Причем он может осуществляться за действиями как операторов рабочих мест, так и дежурной службы в экстренных ситуациях.

Технология непрерывного мониторинга парольной защиты также непосредственно связана с видеонаблюдением. Режим распознавания лица служит не только для биометрической идентификации сотрудника при входе в систему, но и для периодического распознавания лица с целью подтверждения личности оператора. Кроме этого, на рабочее место оператора настроен детектор присутствия системы видеонаблюдения. Если оператор покидает рабочее место, через заданный временной интервал клавиатура, мышь и монитор отключаются от системного блока, и рабочее место блокируется.

- *Монетизация систем видеонаблюдения:*

Классический подход к установке системы видеонаблюдения предназначает ее исключительно для целей безопасности. Но мы можем поднять экономическую привлекательность внедрения, если будем предлагать видеонаблюдение как интегрированный компонент для получения дополнительных доходов. Монетизация – сегодня один из основных трендов использования современных систем видеонаблюдения. Поясним на примерах.

- *Средства объективного контроля бизнес-процессов*

Средства контроля бизнес-процессов, как правило, сводятся к оформлению бухгалтерских документов, которые не всегда объективно отражают действительность. Наличие системы видеонаблюдения позволяет регистрировать объективную «картинку» происходящего. Например, если при въезде на предприятие система видеонаблюдения регистрирует автомобили и распознает их номера, то появляется объективный фактор для учета пребывания автомобиля на территории и взимания платы за стоянку.

С помощью распознавания QR-кода, можно организовать эффективную систему учета рабочего времени, а наличие системы видеонаблюдения исключает влияние человеческого фактора, когда один сотрудник может передать свой пропуск другому.

- ***Контроль технологических процессов***

Можно использовать систему видеонаблюдения для контроля технологических процессов, например, в денежных хранилищах. Камеры фиксируют не только перемещение сотрудников, но и номера банкнот при пересчете денег.

При маркировке QR-кодом деталей или изделий на конвейере можно фиксировать время ее нахождения на ленте, а также нарушение технологии.

- ***Реклама***

В супермаркетах, торговых центрах, бутиках, аптеках, кафе, ресторанах, отелях широко применяется гибкий маркетинговый инструмент Indoors TV – система демонстрации видеоматериалов информационного и рекламного характера на мониторах и видеопанелях. Это позволяет выводить на экран информацию из любого источника: видеофайла, видеочамеры, сетевого потока, аудиофайла.

- ***Маркетинг***

В маркетинге есть возможность отслеживать средствами видеонаблюдения наиболее популярные пути прохода посетителей, фиксировать время нахождения перед

рекламой, оценивать пол, возраст и эмоции посетителей.

Исходя из нашей практики, основные трудности монетизации систем видеонаблюдения состоят в необходимости их интеграции с соответствующими прикладными программами, системами бухгалтерского учета, а также адаптации программ к особенностям бизнес-процессов. Но иметь такое решение весьма полезно. В частности, соединяя видеонаблюдение с разработанной в «МТТ Контрол» системой контроля и управления доступа IDmatic и с системой интеграции XVmatic, мы предлагаем нашим заказчикам возможность не просто распознавания номеров автомобилей, но и одновременное получение сведений об имени водителя, наличии у него действующих пропусков, об используемых тарифах оплаты.

- Выводы

Резюмируя сказанное выше, можно констатировать, что «нет средней температуры по больнице». Возможности, которые сегодня технологии предоставляют пользователю, многообразны и позволяют подобрать оптимальный вариант системы видеонаблюдения конкретно к задачам, которые она должна решать – с учетом ее масштабности и масштабируемости, степени защищенности данных и сроков их хранения, глубине интеграции в других бизнес-процессов. Главное – это четко для себя понять и сформулировать, чтобы потом, обратившись к профессионалам, реализовать все с максимальным эффектом.

[Источник](#)