Тенденции интеграции СОТ в ИСБ

Александр Крахмалев,
К.т.н., проф., акад. ВАНКБ,
нач. отдела НИЦ «Охрана» МВД России
Илья Свирин,
генеральный директор ООО «Нордавинд»,

В рамках проведенной в НИЦ «Охрана» НИР были рассмотрены возможности применения телевизионных систем в охранной сигнализации и определен круг задач телевизионных систем (систем охранного телевидения – СОТ по терминологии ГОСТ Р 51558-2000), исходя из требований обеспечения безопасности и учета всей структуры охраны объекта:

1. **Оперативные задачи** по охране (автоматизированная охранная сигнализация с максимальной обработкой информации для немедленного реагирования) - построение системы охранного телевидения (СОТ) в составе ИСБ объекта или жесткая связь видеокамер с охранными извещателями или детекторами движения.
2. **Наблюдение** за охраняемым объектом с помощью операторов – основное решение по определению состояния объекта принимается человеком (оператором). Такие системы можно назвать «телевизионные системы наблюдения» (ТСН). Основная задача таких систем - предоставить оператору качественное изображение во всех условиях эксплуатации и обеспечить комфортную работу оператора для принятия им правильного решения.
3. **Видеозапись** (видеорегистрация) – основная задача системы видеорегистрации, последующий анализ видеоинформации для расследования противоправных действий или критических ситуаций на объекте.

Все три задачи могут быть также реализованы в рамках одной системы.

При решении **оперативных задач** следует учитывать, что принятие решения жестко ограничено временными рамками. В автоматизированных системах централизованной охраны, когда на пульт централизованного наблюдения (ПЦН) приходится **сотни и тысячи** охраняемых объектов, время доставки тревожного сообщения не должно превышать десятков секунд (с учетом контроля канала связи для радиосистем допускается норма – не более **двух минут**). При этом должно быть обеспечено время прибытия наряда на объект, охраняемый данным ПЦН, **три – пять** минут после получения сигнала тревоги. Как видно это достаточно жесткие нормы и они могут быть выполнены только с учетом внедрения автоматизации в деятельность ПЦН. Одна из основных проблем здесь это ложные сигналы тревоги. Современные системы передачи извещений (СПИ) и первичные средства об-

наружения проникновений (автоматические охранные извещатели), обладают достаточно высокой надежностью, обнаружительной способностью и низким уровнем ложных тревог, однако полностью ложные тревоги исключить нельзя. Применение телевизионных систем могло бы помочь в решение задачи **снижения ложных тревог** (например, при срабатывании охранного извещателя включается телекамера, позволяющая дополнительно оценить ситуацию на охраняемом объекте). Однако нужно учитывать, что в этом случае решение полностью перекладывается на оператора, со всеми присущими ему человеческими факторами, о которых было сказано выше. К тому же это может привести к увеличению времени реагирования на сигнал тревоги. Кроме того, нужно учитывать технические возможности каналов передачи видеоизображения. Наиболее широко в настоящее время в СПИ, применяемых в централизованной охране массовых объектов, используются телефонные линии ГТС и радиоканал. Несмотря на современные достижения в удаленной передаче видеоданных, возможность применения телевидения в данном случае требует индивидуального подхода и соответствующего технико-экономического обоснования. Например, при охране периметра объекта. Современные периметровые извещатели сами по себе достаточно дорогие изделия. По принципу действия большинство из них имеет зону охраны порядка сотен метров и не позволяет точно определить место проникновения нарушителя. Кроме того, уровень ложных тревог для периметровых средств охраны достаточно высок. Применение телевизионных средств в данном случае просто необходимо. Следует также учитывать, что охрана периметра, как правило, применяется на объектах особой важности и повышенной опасности, которые должны быть надежно защищены от террористических угроз. В этом случае телекамеры, включаемые по сигналу периметровых извещателей, позволят оператору оценить опасность угрозы (один нарушитель лезет через забор, или это вооруженная группа с применением технических средств) и вызвать соответствующие силы реагирования.

При решении задачи **наблюдения** за охраняемым объектом телевизионную систему наблюдения (ТСН) в данном случае нельзя отнести к автоматизированным системам, хотя некоторые элементы автоматизации там, безусловно, присутствуют. В соответствии с этим в ТСН полностью проявляется влияние человеческого фактора, что и необходимо учитывать при проектировании системы охраны объекта и планировании действий службы, отвечающей за безопасность. При этом должны быть предусмотрены нормы по загрузке операторов ТСН, обучение операторов, четкие инструкции, контроль действий и т.д. Основная проблема здесь в том, что физические возможности человека по наблюдению за экраном видеомонитора, крайне ограничены. Поэтому при проектировании ТСН необходимо опираться на нормы, обоснованные с учетом требований инженерной психо-

логии. Такие нормы могут войти в стандарты по применению ТСН, учитывая то, что разработка подобных стандартов по системам безопасности, в настоящее время, признана актуальной и работа в этом направлении ведется, как за рубежом, так и в России. Существующие нормативные документы были разработаны достаточно давно и требуют переработки. В НИЦ «Охрана», например, были разработаны рекомендации Р 78.36.002-99 «Выбор и применение телевизионных систем видеоконтроля» и Р 78.36.008-99 «Проектирование и монтаж систем охранного телевидения и домофонов». В этих документах можно найти упоминание, касающееся норм загрузки видеооператоров:

«Следует особо отметить, что анализировать изображения, поступающие с нескольких мониторов одновременно, оператор практически не в состоянии – очень высока вероятность ошибки. Поэтому устанавливать для одного оператора более 4-х мониторов не рекомендуется. Да и в этом случае целесообразно, чтобы он внимательно наблюдал один монитор, а на другие – переключал внимание при возникновении нештатных ситуаций».

Таким образом, задача построения ТСН состоит в том, чтобы обеспечить максимальную комфортность работы оператора для того, чтобы сосредоточить его внимание на решение основной задачи – обеспечение безопасности охраняемого объекта. Современное состояние развития технических средств видеонаблюдения предоставляет в распоряжение проектировщика и соответственно оператора все необходимые возможности: видеокамеры высокой чувствительности и высокого разрешения; высококачественные цветные видеомониторы; средства коммутации видеосигнала; средства удаленной передачи видеоданных; средства автоматизации управления видеокамерами (поворотные устройства с дистанционным и программным управлением, скоростные купольные камеры и т.д.). Имеется также широкая номенклатура различных аксессуаров, обеспечивающих работу современных ТСН. Еще большая эффективность ТСН может быть обеспечена при работе ее в составе ИСБ.

Системы **видеозаписи** (СВЗ) напрямую не предназначены для охраны объекта от несанкционированного проникновения. Однако их роль в расследовании преступлений и тревожных ситуаций трудно переоценить. Кроме того, использование видеозаписей важно не только для того, чтобы, имея хорошо различимые изображения нарушителей, облегчить их дальнейшую идентификацию и юридическую легитимность действий правоохранительных органов, последующий анализ ситуации важен также для оценки качества работы системы безопасности объекта и эффективности действий службы охраны. Выводы, полученные в результате этого анализа, могут быть использованы для повышения эффек-

тивности системы безопасности и, соответственно, могут сыграть определенную роль в профилактике и предотвращении преступлений на данном объекте.

Новый этап развития систем видеорегистрации связан с применением **цифровой обработки** видеосигнала и появлением цифровых систем видеозаписи. Можно отметить два основных направления в развитии цифровых систем видеорегистрации – цифровые видеорегистраторы - **ЦВР** (Digital Video Recorder – **DVR**), как отдельно законченные конструктивные устройства (без применения компьютера) и цифровая видеорегистрация, реализованная на программном уровне в составе цифровых систем видеонаблюдения – **ЦСВ** на базе компьютера. На рис. 1 приведена структурна схема построения СОТ на базе современного многофункционального DVR.

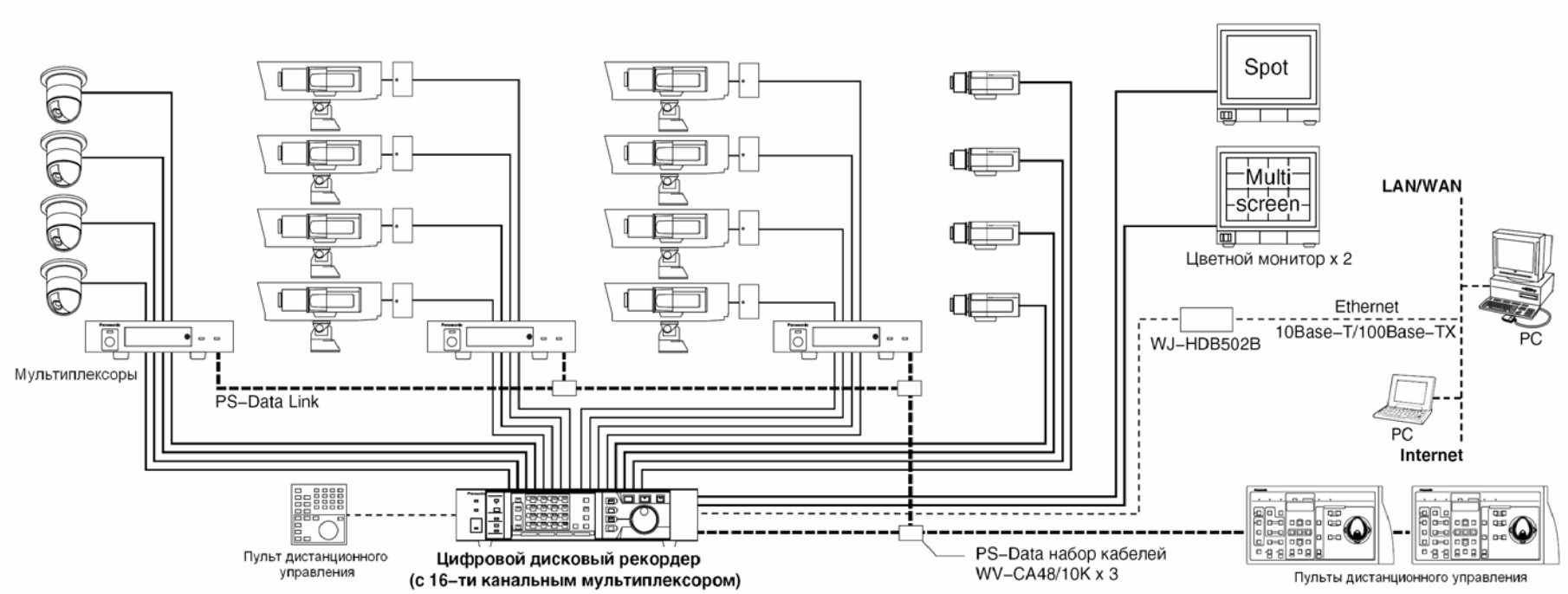

Рисунок 1 СОТ на базе цифрового видерегистратора

(упростить рисунок и дать с максимальным разрешением макс. dpi)

Изучение отечественного и зарубежного опыта применения, тенденций и перспектив развития средств безопасности, которое постоянно проводится в НИЦ «Охрана» МВД России, показывает, что для обеспечения безопасности различных объектов, в особенности объектов особой важности и повышенной опасности, наилучшим образом подходят интегрированные системы безопасности (ИСБ), в составе которых телевидение играет значительную роль. Кроме того, эффективность применения СОТ в составе ИСБ значительно повышается.

Среди задач, решаемых СОТ можно отметить особую роль **видеорегистрации.** Первые две из трех задач СОТ, в настоящее время, имеют определенный набор проблем, затрудняющих их эффективное применение.

Для решения оперативных задач (автоматизированная охранная сигнализация - обнаружение проникновения) в составе СОТ применяются детекторы движения, которые по надежности, эффективности и по соотношению цена/эффективность уступают традиционным охранным извещателям.

Задача наблюдения за охраняемым объектом требует привлечения значительных людских ресурсов и соответственно имеет все недостатки «человеческого фактора».

Видеорегистрация, хотя и непосредственно не решает вопросы охраны, может сыграть существенную роль (и уже есть этому многочисленные примеры из практического опыта) в раскрытии преступлений и противоправных действий, а широкое внедрение телевизионных систем с мощными средствами видеорегистрации может способствовать профилактике и предупреждению противоправных действий.

Прогресс в данном направлении подтверждается наличием современных технических средств, постоянным их совершенствованием при тенденции снижения цен, что делает их доступными для широкой сферы применения – от квартирных видедомофонов, до систем безопасности крупных объектов типа аэропортов, а также создания проектов для оснащения видеосистемами целых районов и городов.

Стремительный прогресс развития СОТ в системах безопасности требует значительного увеличения пропускной способности каналов передачи данных. Это требуется для качественной передачи видеоинформации. Наличие такого высокоинформативного канала передачи данных дает возможность передавать по этим каналам и другую информацию в системах безопасности (объемы этой информации значительно меньше, чем водеоданных). Из этого можно сделать вывод, что именно СОТ становится базовой основой построения ИСБ, а поскольку перспектива самих телевизионных систем это цифровая обработка видеосигнала, то в качестве выбора основных каналов и технологий связи для по-

строения ИСБ – это использование IP сетей, технологий Internet, беспроводных компьютерных сетей, сетей мобильной связи и современных достижений IT-индустрии.

Структура ИСБ на базе использования IP сетей и подсистемы СОТ с применением цифровых видеорегистраторов приведена на рис. 2.

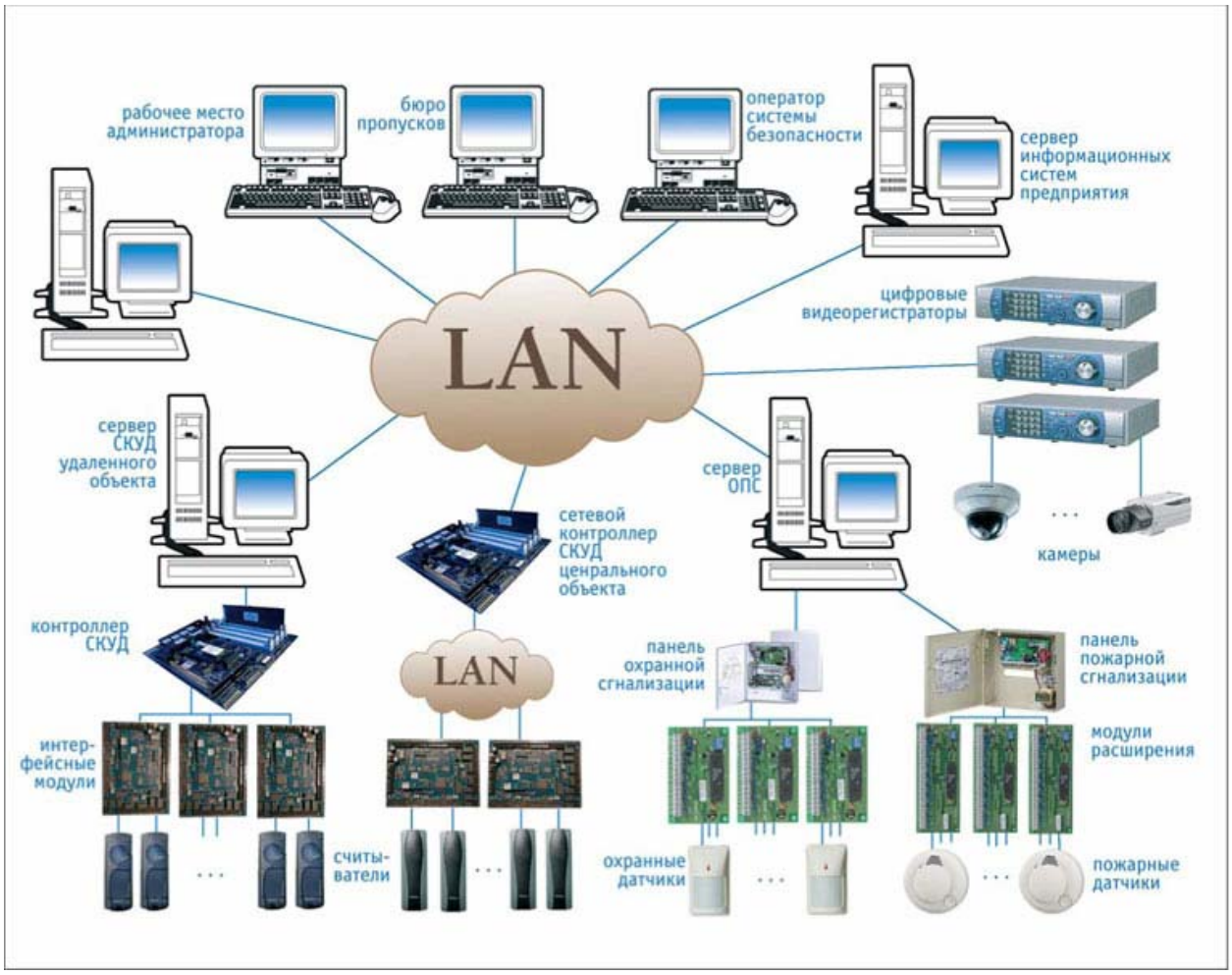

Рисунок 2 ИСБ с использованием IP-сетей
(упростить рисунок и дать с
максимальным разрешением макс. dpi)

Значительное снижение стоимости услуг доступа к ресурсам глобальной компьютерной сети Internet и развитие сетей мобильной связи позволяют говорить о переходе IT-индустрии в новую эру распределенных решений.

Охранные системы традиционно использовали самые передовые и прогрессивные технологии, поэтому распределенные решения могут в скором времени войти в этот сектор рынка, дав импульс к переходу на очередной качественный уровень.

Традиционные охранные системы, которыми, в настоящее время оборудовано значительное число реальных объектов, представляют собой совокупность разрозненных компонентов, образующих набор слабо связанных подсистем с децентрализованным

управлением и мониторингом (охранное телевидение, охранно-пожарная сигнализация, средства контроля доступа). Такие системы создаются на основе проектного решения. Эффективность работы таких систем во многом определяется квалификацией обслуживающего их персонала и проработанностью проекта, в который, как правило, разработчики проекта – проектно-монтажные организации, имеющие большой опыт работы, закладывают элементы интеграции (интеграция на проектном уровне). Более высокая степень интеграции систем – это применение ИСБ аппаратно - программного уровня интеграции, которые создаются на базе специализированных локальных вычислительных сетей (ЛВС) и используют IT-технологии, что позволяет перейти на новый качественный уровень обеспечения безопасности объектов. Такие ИСБ, в настоящее время широко и успешно применяются.

Современные системы охранного телевидения предоставляют широкие возможности по построению распределенных «клиент-серверных» решений. Ориентация таких решений на работу в IP-сетях, которыми является подавляющее большинство локальных вычислительных сетей, позволяет разработчикам, а также интеграторам таких систем, говорить о возможности их функционировании в глобальной компьютерной сети Internet.

Хотя здесь необходимо отметить, что широкие возможности, которые дает Internet, требуют взвешенного подхода к построению систем безопасности на базе применения каналов Internet, исходя, прежде всего из задач обеспечения безопасности.

Технические возможности для этого есть, но необходимо учитывать некоторые дополнительные факторы:

- «клиент» должен обладать достаточно высокой вычислительной мощностью, чтобы обеспечить эффективное декодирование видео потока;
- канал подключения к глобальной компьютерной сети Internet со стороны «клиента», и тем более со стороны сервера, должен иметь достаточную пропускную способность;
- сервер системы охранного телевидения должен обязательно иметь выделенный IP-адрес.

Эти дополнительные факторы приводят к следующим проблемам. Высокие требования к вычислительной мощности клиента ограничивают применение современных мобильных платформ ноутбуками и достаточно производительными карманными ПК, оставляя «за бортом» самую распространенную на сегодняшний день клиентскую платформу – мобильный телефон.

Высокие требования к пропускной способности каналов доступа в Internet ставят жирный крест на dial-up клиентах и сравнительно узких GPRS и GSM каналах, являющихся зачастую единственными экономически оправданными решениями для загородных объектов.

Необходимость наличия собственного выделенного IP-адреса для сервера накладывает дополнительные требования на провайдера услуг доступа к Internet и, что, наверное, даже более важно, делает видеосервер уязвимым по отношению внешним сетевым атакам.

Решение данных проблем требует кардинального пересмотра целевых платформ и совершенствования существующей технологической базы (средств и языков разработки, протоколов, алгоритмов сжатия и т.п.) для построения распределенных охранных систем.

Уже сейчас на Российском рынке представлены законченные технические решения и опытные образцы изделий для построения распределенных систем охранного телевидения, ориентированные на использование мобильных Java-enabled платформ в среде глобальной компьютерной сети Internet.

Открытая технология EyeOn™ (patent pending), разработанная и внедряемая Российской компанией Нордавинд, испытания которой проводятся в НИЦ «Охрана» МВД России, позволяет решать следующие задачи:

- предоставление удаленного доступа к видеорегистраторам и видеосерверам, не имеющим выделенного IP-адреса в пространстве адресов Internet, через специальные сервера-ретрансляторы EyeOn, расположенные в Internet;
- синхронная передача видеоданных Java-enabled мобильным клиентам, обеспечивающим возможность управления качеством получаемого потока с учетом пропускной способности канала и объема доступных вычислительных ресурсов клиента.

Охранные системы, использующие технологию EyeOn, обеспечивают возможность подключения мобильных клиентов (Java-enabled мобильные телефоны, портативные и карманные ПК) к удаленным видеорегистраторам и видеосерверам без выделенного IP-адреса. Решения на базе технологии EyeOn носят бюджетный характер и поэтому могут быть эффективно использованы для построения охранных систем загородных домов и небольших офисных помещений.

Технология синхронной ретрансляции EyeOn предполагает размещение в сети Internet выделенного сервера-ретрансляции. Предоставляется услуга использования существующих серверов-ретрансляции EyeOn за абонентскую плату.

Рисунок 3 Мобильный телефон с установленным программным обеспечением EyeScreamME

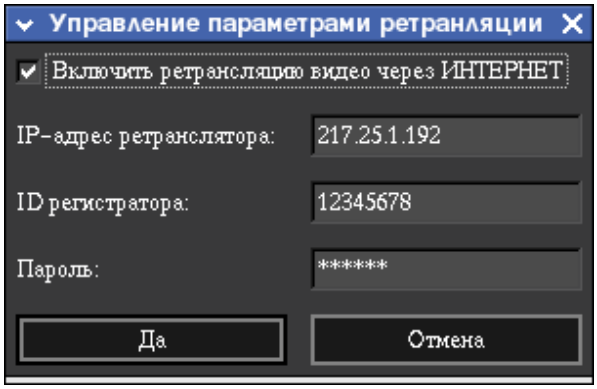

Рисунок 4 Диалог настройки параметров ретрансляции системы охранного телевидения, реализующей технологию EyeOn

Предполагается, что видеорегистратор и мобильные клиенты не имеют выделенного адреса в сети Internet. Подключение услуги ретрансляции заключается в получении идентификационных параметров для доступа к функциям ретранслятора (выделенный IP-адрес ретранслятора, уникальный идентификатор видеорегистратора и пароль для доступа к учетной записи видеорегистратора на ретрансляторе). После загрузки указанных параметров в видеорегистратор, выполняется периодическое подключение к ретранслятору. Очевидно, что подключение в обратном направлении невозможно, т.к. только ретранслятор имеет выделенный IP-адрес. При каждом подключении видеорегистратора к ретранслятору выполняется процедура аутентификации и чтение признака запроса данных (DRF – Data Required Flag). Вместе с установленным признаком DRF регистратору возвращаются требуемые параметры видеопотока, определяемые клиентом в зависимости от пропускной способности канала, разрешающей способности собственного дисплея и т.п.

При получении признака DRF видеорегистратор передает ретранслятору фрагмент видеопотока, отвечающий запрашиваемым параметрам.

Ретранслятор EyeOn обеспечивает возможность подключения нескольких мобильных клиентов на получение данных от одного видеорегистратора. Мобильный клиент с установленным программным обеспечением EyeScreamME™ подключается к ретранслятору по его выделенному IP-адресу в сети Internet и в числе прочих параметров запроса передает идентификатор видеорегистратора, от которого требуется получение данных. Ретранслятор выставляет признак DRF и удерживает сетевое соединение до момента очередного подключения требуемого видеорегистратора или до истечения таймаута.

Таким образом, реализуется синхронный обмен данными между видеорегистратором и мобильными клиентами.

Проблемы информационной безопасности являются одними из самых серьезных и актуальных при построении распределенных решений в глобальной компьютерной сети Internet. Применительно к охранным системам требования безопасности особенно актуальны, т.к. нарушение механизмов информационной защиты позволит злоумышленнику влиять на физическую безопасность охраняемого объекта.

В теории информационной безопасности выделяются следующие виды угроз безопасности информации: угрозы конфиденциальности, целостности и доступности. Предотвращение реализации данных угроз требует применения комплексных мер защиты на доступных уровнях взаимодействия с видеорегистратором и ретранслятором, начиная с сетевого уровня, реализуемого операционной системой, и заканчивая уровнем приложений.

В технологии EyeOn предусмотрены средства защиты информационных потоков. Имеется два типа информационных потоков: управляющая информация и целевой видеопоток. Оба потока должны быть защищены при передаче через глобальную компьютерную сеть Internet, но целевой видеопоток должен быть защищен дополнительно от ретранслятора, который осуществляет прозрачную передачу видеофреймов, как бинарных блоков данных, что гарантирует конфиденциальность и целостность целевого видеопотока при передаче через транзитные узлы-ретрансляторы и линии связи.

Технические решения, которые позволяют защитить канал взаимодействия компонентов охранной системы, построенной с использованием технологии EyeOn, основаны на следующих принципах:

- аутентификация видеорегистратора на ретрансляторе – в базовом варианте EyeOn аутентификация осуществляется путем проверки соответствия указанного видеорегистратором идентификатора предъявленному паролю;
- предотвращение несанкционированного доступа к трафику между компонентами охранной системы – осуществляется с использованием технологии Secure Socket Layer (SSL) путем применения асимметричного шифрования, что гарантирует конфиденциальность и целостность потока управляющей информации и целевого видеопотока от внешних угроз, но потенциально сохраняется угроза съема информации с ретранслятора, где целевой видеопоток находится в открытом виде;
- предотвращение съема целевой видеоинформации с ретранслятора – в ретранслятор и во все мобильные клиенты загружаются ключи симметричного шифрования, которые используются для шифрования данных на видеорегистраторе и дешифрования непосредственно на клиентах. Таким образом, передаваемый целевой видеопоток находится в зашифрованном виде, вплоть до его получения клиентом. Это не ограничивает возможности ретранслятора, т.к. целевой видеопоток рассматривается как последовательность неформатированных

блоков и перенаправляется без изменений в соответствии с сопровождающей его управляющей информацией.

- взаимная криптографическая аутентификация видеорегистратора и ретранслятора позволит избежать подмены абонента взаимодействия. Это позволит исключить возможность подмены одного видеорегистратора другим, направив клиентам ложный (например, неактуальный) поток данных, а также исключить возможность подмены одного ретранслятора другим, т.е. осуществить активный перехват информации;
- средства электронно-цифровой подписи позволят абонентам (клиентам) быть уверенными, что данные получены именно от запрашиваемого видеорегистратора.

В настоящее время в разработке находится технология EyeOnSecure, которая является защищенной версией технологии EyeOn.

В заключение можно отметить, что развитие техники СОТ и в частности систем видеорегистрации идет активными темпами, появляются новые технологии построения систем СОТ, использующие современные достижения IT-индустрии и методы защиты данных, что имеет немаловажное значение для систем безопасности. Появление на рынке множества новых продуктов СОТ как аппаратных так и программных средств, ставит на одно из первых мест перед пользователем и заказчиком проблему правильного и оптимального выбора систем и решений. Этому должна помочь современная нормативная база для проведения сертификации и применения распределенных решений в области охранных систем в государственных и военных структурах. Однако на настоящий момент требования к таким системам на сегодня отсутствуют и диктуются только потребностями рынка, которые зачастую не учитывают специфику построения систем безопасности объектов.

Развитие нормативной базы для распределенных охранных систем, использующих в качестве транспортной среды глобальную компьютерную сеть Internet и мобильные сети связи, позволит акцентировать внимание разработчиков на наиболее важных проблемах построения распределенных систем и повысить престиж России на мировом рынке охранных систем.

Работа над созданием такой нормативной базы проводится в НИЦ «Охрана» МВД России в рамках технического комитета по стандартизации МТК/ТК-234 «Технические средства систем охраны и безопасности», а также в рамках разработки технических регламентов в области антитеррористической и противокриминальной защиты.

Список использованных источников

1. А.К. Крахмалев. Перспективы использования цифровых видеорегистраторов в автоматизированных системах охранной сигнализации. («Системы цифровой видеорегистрации (DVR)-2006». Выпуск I), Москва, Изд. «Гротек».
2. ГОСТ Р 51558-2000. Системы охранные телевизионные. Общие технические требования и методы испытаний.
3. Закон Российской Федерации № 2446-1 от 5 марта 1992 г.: О безопасности.
4. ГОСТ Р 51275-99. Защита информации. Объект информации. Факторы, воздействующие на информацию.
5. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Архитектура защиты информации.