

КОЛОНКА РЕДАКТОРА



Прежде всего, уважаемые коллеги, хочется поздравить вас с началом нового делового сезона: как известно, осень — самая горячая пора в нашем бизнесе. Желаю вам как можно скорее

войти в рабочий режим и ритм после сезона отпусков. И решительно взяться за дело... Но взяться не сломя голову, как это зачастую бывает, а сначала хорошенько поразмыслив о том, "куда идем" и "что делаем". Я не просто еще раз напоминаю о том, что тематику IP нужно изучать, не жалея сил и времени. Я призываю вас обратить внимание на вполне конкретные темы, важность которых нельзя недооценить. Две из них освещены в этом номере журнала. Первая посвящена системной интеграции (или интеграции систем) и призывает более внимательно, разумно и осторожно относиться к проблематике системной интеграции и даже самому термину, ее обозначающему. Вторая тема — безопасность и защищенность IP-видеонаблюдения — достойна пристальной шего внимания. Уверен, вы не раз задавались этим вопросом, и при подготовке коммерческих предложений, и при выборе оборудования, и при его установке и настройке. Дело в том, что не все так сложно, как кажется... но одновременно с этим не все так просто, как хотелось бы.

В наших статьях авторы раскрывают проблему и дают ответы на поднимаемые вопросы, но конкретные решения ваших ежедневных задач можете найти только вы. И сможете это сделать, только опираясь на прочный фундамент знаний об IP-технологиях. Мой совет — пока есть время, чтобы войти в режим, и пока заказчики возвращаются из отпусков, найдите возможность для более глубокого изучения тематики IP! Источники информации всем известны — книги, журналы, Интернет, рекламные материалы производителей... Если же вы сами только собираетесь в отпуск осенью, то не полнитесь захватить с собой учебник по сетевым технологиям (а также, конечно, журнал "Системы безопасности"). Поверьте, время, потраченное на получение новых знаний, никогда не окажется временем, потраченным впустую. Как раньше говорили в осеннюю пору сбора урожая на Руси, "осенний день весь год кормит", так и сейчас мы можем сказать, "время, потраченное на учебу, потом всю жизнь прокормит".

Е.В. Ерошин

Редактор раздела IP Security

Безопасность и надежность систем IP-видеонаблюдения: мифы и реалии

Существующему до сих пор мнению о незащищенности цифровых систем IP-видеонаблюдения автор противопоставляет весомые аргументы в пользу IP-систем, необходимую и достаточную безопасность которых обеспечивают функции защиты, встроенные в современное сетевое оборудование для корпоративных сетей. Пользователю лишь остается сделать правильный выбор сетевого оборудования



Г.А. Марков,

Технический директор компании "Технориум"

С наступлением эпохи цифровизации аудио- и видеoinформации, с массовым распространением телекоммуникационных сетей на базе протокола IP естественным шагом производителей систем видеонаблюдения стал выпуск цифровых систем видеонаблюдения для сетей IP. Эти системы уже не используют коаксиальный кабель для передачи в аналоговой форме картинки и звука, как это делают классические системы видеонаблюдения, а преобразовывают его в цифровую форму и передают по стандартным каналам связи и локальным вычислительным сетям от камер на посты наблюдения и к системам архивирования. Использование цифрового формата и стандартного для большинства сетей протокола IP позволяет строить системы IP-видеонаблюдения с недостижимыми для аналоговых систем показателями гибкости и масштабируемости. Кроме того, появляется возможность использовать в таких системах стандартное телекоммуникационное и компьютерное оборудование, что существенно снижает начальные инвестиции и стоимость сопровождения систем. Однако, по мнению некоторых адептов аналоговых систем видеонаблюдения, использование стандартного сетевого оборудования и есть одна из слабых точек систем IP-видеонаблюдения, что позволяет говорить об их общей ненадежности и незащищенности перед злоумышленниками. Для того чтобы расставить все точки над "и", рассмотрим компоненты, типовую схему построения систем IP-видеонаблюдения и механизмы обеспечения безопасности.

Состав системы IP-видеонаблюдения

Источником видеосигнала для систем IP-видеонаблюдения являются цифровые камеры, на выходе которых аудио- и видеосигнал представлен в цифровом формате (IP-пакеты) с интерфейсом подключения в виде порта FastEthernet, который непосредственно подсоединяется к такому сетевому оборудованию, как коммутатор или маршрутизатор. Это могут быть сетевые устройства, выделенные специально для систем наблюдения или совместно используемые для передачи всех корпоративных данных и подключения рабочих мест пользователей. В последнем случае может показаться, что безопасность системы видеонаблюдения зависит от действий любого пользователя компьютерной сети компании, и, если на месте пользователя окажется злоумышленник, он сможет безнаказанно нарушить ее работу. Немного позже разочаруем строящего радужные планы горе-хакера, а сейчас отметим, что при правильном выборе и настройке сетевого оборудования доступ произвольного пользователя к данным и оборудованию системы IP-видеонаблюдения невозможен.

Итак, мы получили оцифрованный сигнал от камеры, подключили камеры к сетевому оборудованию, а теперь будем использовать компьютерную сеть для передачи аудио- и видеoinформации непосредственно к посту видеонаблюдения. Этот пост может находиться как в 100 м от объекта наблюдения, так и в 2000 км от него. Замечательный показатель, который недостижим для традиционных аналоговых систем видеонаблюдения. Однако нам он интересен с точки зрения масштабов IP-сети — от расстояний и количества объектов наблюдения зависит состав и конфигурация сетевого оборудования системы IP-видеонаблюдения и меры, необходимые для обеспечения ее безопасности. Это может быть один коммутатор, к которому подключены и камеры наблюдения, и компьютеры поста наблюдения, а также несколько маршрутизаторов и коммутаторов, обеспечивающих в совокупности передачу на значительные расстояния информации, поступающей от множества камер. Заметим, что в первом случае при использовании медного кабеля максимальное удаление камер от поста наблюдения составит 200 м (ограничение стандарта FastEthernet).

Таким образом, с учетом компьютеров поста видеонаблюдения, мы можем выделить три

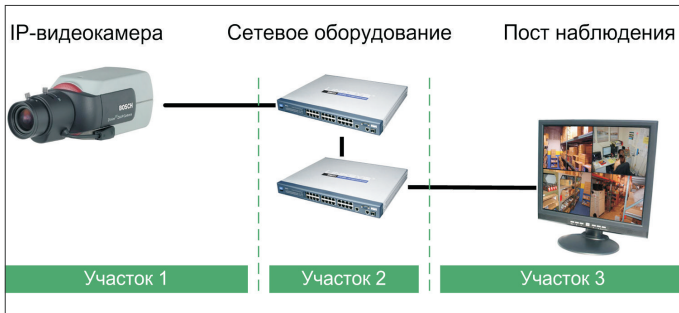


Рис. 1

участка (рис. 1) любой системы IP-видеонаблюдения, которые важны с точки зрения обеспечения безопасности:

- 1) видекамера и кабель подключения видекамеры к сетевому оборудованию — самый незащищенный физический участок;
- 2) сетевое оборудование в виде маршрутизаторов и коммутаторов, которые осуществляют передачу информации в необходимую точку расположения поста наблюдения;
- 3) зона кабельного подключения компьютеров поста наблюдения к сетевому оборудованию, которое осуществляет передачу видеосигнала. Рассмотрим механизмы защиты для каждого участка.

Системы защиты локальных систем IP-видеонаблюдения

На физических аспектах защиты первого участка останавливаться нет смысла, так как они ничем не отличаются от традиционных систем аналогового видеонаблюдения. Единственное, что может получить злоумышленник без риска быть обнаруженным (при условии свободного доступа к кабелю), — лишь картинку с камеры. При этом, однако, ему потребуется специализированный программно-аппаратный комплекс на базе ноутбука, изготовить который под силу только эксперту, разбирающемуся в компьютерных сетях, программировании и цифровой электронике одновременно. Попытка же повлиять на видеосигнал, идущий с камеры (не говоря уже о подключении какого-либо источника видеосигнала вместо видекамеры), будет мгновенно обнаружена и запротоколирована системой. Такую реакцию обеспечивают механизмы контроля целостности передаваемой информации, заложенные в сетевые протоколы FastEthernet, IP и HTTP, которые осуществляют передачу данных от видекамер по сети. Таким образом, безопасность участка подключения видекамера — кабель у систем IP-видеонаблюдения выше, чем у аналоговых систем. Рассмотрим с точки зрения безопасности участок сетевого оборудования, который абсолютно незнаком большинству специалистов по аналоговым системам видеонаблюдения. Не обладая специальными знаниями о принципах защиты информации в корпоративных сетях и необходимым для этого оборудованием, некоторые специалисты делают поспешные заявления и проводят так называемые "тест-драйвы" сетевого оборудования, которое предназначено не для создания корпоративных сетей, а для домашнего применения. Давайте же, наконец, прольем свет на этот часто используемый для спекуляций вопрос.

При построении современных корпоративных компьютерных сетей к ним предъявляются высокие требования в части надежности и безопасности передаваемых данных. Эти требования, как правило, даже выше требований к надежности и безопасности систем видеонаблюдения. Ведь зачастую информация для

служебного пользования, циркулирующая в корпоративной сетевой среде, имеет значительную большую ценность, нежели картинка с видекамеры, установленной у входа на склад. Сетевое оборудование для корпоративных сетей таких производителей, как Cisco Systems или Allied Telesis, имеет централизованную многоуровневую защиту и разграничение прав доступа на уровне пользователей и портов сетевых устройств, обеспечивает фильтрацию передаваемых данных на основе правил, заданных адми-

нать управляющую консоль коммутатора и вручную добавить свой компьютер в VLAN системы IP-видеонаблюдения. Одна задача — доступ к консоли возможен только с рабочего места администратора, но никак не с произвольного рабочего места пользователя. Круг замкнулся.

Port Security

Итак, первый рубеж защиты, блокирующий доступ произвольных пользователей компьютерной сети компании к системе IP-видеонаблюдения, установлен. Второй рубеж призван блокировать доступ посторонних лиц, не являющихся сотрудниками компании, а значит, и потенциальных злоумышленников, непосредственно к компьютерной сети и сетевому оборудованию. Этот рубеж и состоит из механизмов Port Security. Это наиболее распространенное среди производителей коммутаторов для локальных сетей название специальных функций, охраняющих каждый порт сетевого оборудования от подключения неавторизованных устройств. Ведь даже самому неграмотному хакеру известно, что свободная розетка локальной сети в офисе подключена к порту коммутатора, который можно использовать для доступа в корпоративную сеть.

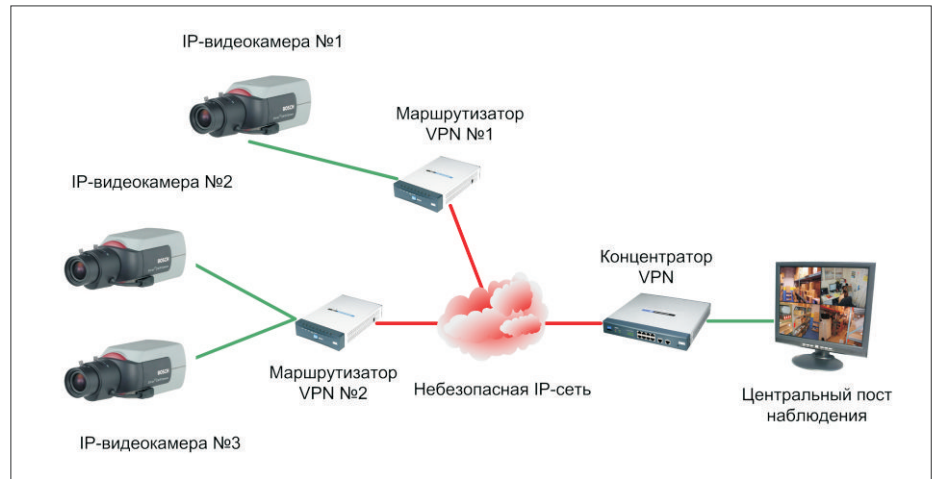


Рис. 2

нистратором. Рассмотрим подробнее такие механизмы безопасности сетевых коммутаторов, как виртуальные локальные сети VLAN, Port Security, авторизация доступа на базе 802.1x.

Технология VLAN

VLAN, как базовую и наиболее распространенную технологию ограничения доступа, поддерживают практически все коммутаторы для корпоративных сетей. Можно даже сказать, что если в коммутаторе нет поддержки VLAN, этот коммутатор явно не для сети современного предприятия.

С помощью этой технологии все устройства системы IP-видеонаблюдения выделяются в отдельную группу, изолированную от всех остальных устройств и пользователей, подключенных к сети, — виртуальную локальную сеть VLAN. Таким образом возводится барьер, который ограничивает обмен данными только в пределах одной конкретной VLAN. Пользователи, а вместе с ними и потенциальные злоумышленники, естественно, подключены к другой аналогичной VLAN; это означает, что у злоумышленника нет физического доступа к устройствам, работу которых у него есть желание нарушить. Единственный путь — взло-

Работа же механизмов Port Security состоит в идентификации подключаемых к портам коммутаторов сетевых устройств и пресечении неавторизованного доступа. В момент подключения любого сетевого устройства, например ноутбука, механизм Port Security по таким характеристикам, как MAC-адрес подключаемого устройства, его IP-адрес, однозначно определяет его как "своего" или "чужого", и в последнем случае (например, для гостей компании), разрешает доступ только к сети Интернет.

Более жесткие настройки Port Security состоят в назначении администратором соответствия каждому компьютеру компании конкретному порту коммутатора, к которому он должен быть подключен, и при нарушении этого правила порт коммутатора полностью выключается до его ручного включения администратором. Безусловно, злоумышленник может установить любой MAC- и IP-адрес на свой ноутбук, однако для этого ему необходимо выяснить не только сами адреса, но и принадлежность их портам коммутатора. А эта конфиденциальная информация известна только администратору безопасности компьютерной сети компании.

Авторизация доступа на базе 802.1x

Наконец, третий рубеж, контролирующий все сетевые подключения персональных компьютеров и ноутбуков пользователей с помощью паролей, в частности, по данным их учетных записей в среде Microsoft Windows. Речь идет о протоколе 802.1X. Здесь надо отметить, что зачастую правила Port Security усложняют и увеличивают объем работ по администрированию и доставляют множество хлопот мобильным пользователям с ноутбуками. В таких случаях проектные решения сетевых решений останавливаются на варианте, состоящем из связи VLAN и протокола 802.1X. Этот протокол позволяет реализовать централизованный контроль доступа к сети компании компьютеров и пользователей в точках их подключения, на портах коммутаторов.

Для использования в локальной сети авторизации по протоколу 802.1X необходимы коммутаторы с поддержкой 802.1X и сервер авторизации RADIUS, который выполняет авторизацию либо с использованием внутренней базы данных пользователей, либо перенаправляет запрос на корпоративный сервер авторизации, например, Active Directory. При успешной аутентификации и авторизации подключения на коммутатор загружаются установленные для конкретного пользователя и его группы правила обработки сетевого трафика, которые разрешают (или блокируют) доступ пользователя к определенным частям сетевой инфраструктуры компании. Таким образом, администратор может ограничить доступ к системе IP-видеонаблюдения только с определенных компьютеров, в определенное время и определенных пользователей. Поддержка 802.1X встроена во многие операционные системы, поэтому, как правило, работа этой схемы контроля доступа прозрачна для конечного пользователя.

Необходимые и достаточные механизмы

Таким образом, в распоряжении проектировщиков и установщиков системы IP-видеонаблюдения существуют по крайней мере три механизма обеспечения безопасности, которые следует грамотно использовать. Эти механизмы необходимы и достаточны для полной защиты систем IP-видеонаблюдения как в случае выделенного сетевого оборудования для системы видеонаблюдения, так и в случае совместного использования общей компьютерной сети компании для работы системы IP-видеонаблюдения. Здесь читатель, знакомый с сетевыми технологиями, заметит, что автор никак не упомянул различные приложения для сканирования сети и атак на сетевое оборудование, например сканеры портов и IP-сетей, flood-приложения. Дело в том, что на современном уровне развития сетевого оборудования для корпоративных сетей этот вопрос уже решен и остался в прошлом. Современные сетевые устройства для корпоративных сетей умеют обнаруживать аномалии в сетевом трафике. Они отличают обычный сетевой трафик от нормальной работы пользователя от моментов сканирования или атаки на какой-либо узел сети с компьютера злоумышленника — в этих случаях порт коммутатора, к которому подключен такой враждебный компьютер, автоматически отключается до вмешательства администратора и службы безопасности

Когда нужна защита VPN

В случаях построения территориально распределенных систем IP-видеонаблюдения или вынужденного использовании небезопасных участков телекоммуникационных сетей операторов связи (таких, где нет возможности реализовать меры защиты) необходимо использовать оборудование с поддержкой шифрования передаваемых по сети данных. А именно оборудование с поддержкой технологии виртуальных частных сетей VPN (Virtual Private Network). Этот тип сетевого оборудования обеспечивает установление зашифрованных туннелей для передачи конфиденциальных данных через небезопасные сетевые соединения. Кроме шифрования оборудование поддерживает контроль целостности передаваемой информации и защиту от ее искажения злоумышленниками.

Схема подключения VPN

В большинстве случаев типовой схемой подключения для сетей VPN является схема "точка-точка" с выделенным сетевым центром, в котором устанавливается так называемый концентратор VPN. К нему подключаются и с ним взаимодействуют маршрутизаторы VPN, установленные на объектах наблюдения. Маршрутизаторы VPN обеспечивают защиту передаваемых данных по безопасному туннелю от необходимого числа IP-видеокамер на пост наблюдения, в котором размещен концентратор VPN. В то же время никаких физических ограничений на размещение и число концентраторов VPN нет.

Конфигурация сети, состоящей из устройств VPN, может быть такой, какой требуется из соображений безопасности и географии размещения объектов наблюдения.

Концентраторы и маршрутизаторы

В качестве концентраторов VPN используются специализированные устройства, выпускаемые такими производителями, как Cisco Systems, Linksys, Allied Telesis и многими другими. В то же время стандартные маршрутизаторы для IP-сетей могут быть дополнены аппаратными модулями шифрования VPN и выступать в роли центрального узла сети VPN, в частности, такой возможностью обладают маршрутизаторы ISR компании Cisco Systems. Речь идет о маршрутизаторах Cisco серий 800, 1800, 2800 и 3800, которые можно использовать для построения не только небольших сетей VPN из десятка узлов, но и крупных, насчитывающих десятки и сотни узлов территориально распределенных сетей. Важной особенностью маршрутизаторов ISR является возможность использования модулей шифрования, поддерживающих криптографические алгоритмы по российским стандартам ГОСТ и имеющих соответствующие сертификаты Гостехкомиссии, ФСБ и ФСТЭК, что позволяет применять их при установке IP-видеонаблюдения на режимных объектах государственных заказчиков в РФ.

В местах установки IP-видеокамер или в точке их подключения к небезопасной сети устанавливаются маршрутизаторы VPN, которые обеспечивают безопасное подключение одной или нескольких IP-видеокамер к концентратору VPN. Так же как и IP-видеокамера,

маршрутизатор VPN имеет один или несколько интерфейсов FastEthernet, что позволяет подключать к нему IP-видеокамеры напрямую, то есть без каких-либо дополнительных устройств. В качестве маршрутизатора VPN для подключения одной или двух камер рационально использовать, например, такие модели, как Cisco 850 ISR или Linksys RV042, а для подключения десятка камер будут оптимальны такие модели, как Cisco 870 ISR или Linksys RV016.

И концентраторы и маршрутизаторы VPN, рассчитанные на использование в корпоративных сетях, поддерживают достаточно сильные алгоритмы шифрования 3DES или AES, стойкость к взлому которых сегодня более чем достаточна для защиты систем IP-видеонаблюдения. Задержка шифрования, как правило, не превышает 100 мс в случае аппаратного шифрования/дешифрования. Этот важный момент необходимо учесть при выборе оборудования, поскольку не все производители устанавливают аппаратный криптографический процессор, и — как следствие — при больших потоках данных возможны существенные задержки в передаче видеoinформации. Что касается масштабируемости, то, например, такой концентратор VPN, как Cisco ASA 5505, сможет обработать данные с 10 точек подключения IP-видеокамер.

Резюме

При правильном выборе сетевого оборудования и его настройке процесс обеспечения безопасности сети для IP-видеонаблюдения принципиально ничем не отличается от корпоративной компьютерной сети, и, более того, эти сети могут сосуществовать в пределах одной корпоративной компьютерной сети.

Системы IP-видеонаблюдения не только не уступают аналоговым системам по показателям безопасности, но и при условии проектирования и установки квалифицированными специалистами значительно более защищены от воздействий как неопытных хакеров, так и достаточно квалифицированных злоумышленников. В любом случае задача взлома или нарушения работы системы IP-видеонаблюдения при использовании описанных в статье систем защиты является нетривиальной.

Для защиты систем IP-видеонаблюдения, сосредоточенных на небольшой территории, достаточно использовать механизмы защиты, встроенные в коммутаторы корпоративного уровня таких производителей, как Cisco Systems, Allied Telesis, Linksys и некоторых других. При выборе оборудования следует удостовериться в поддержке технологий VLAN, Port Security и 802.1X. Как минимум, необходима поддержка VLAN.

Для защиты территориально распределенных систем IP-видеонаблюдения необходимо использовать технологии и оборудование сетей VPN. При выборе оборудования следует удостовериться в поддержке аппаратного шифрования/дешифрования по стандартам 3DES или AES. ■

Ваши мнение и вопросы по статье направляйте на

ss@groteck.ru