ОБ ИСПОЛЬЗОВАНИИ АЛЬТЕРНАТИВНЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ ДЛЯ ОРГАНИЗАЦИИ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ ОБЪЕКТОВ

А. Фамильнов
начальник отдела ФГУ НИЦ «Охрана» МВД России,
Я. Зайцев
студент МЭИ (ТУ), кафедра радиоприемных устройств

Многолетний опыт работы вневедомственной охраны МВД России показал, что наиболее эффективным и экономически выгодным видом охраны является централизованная охрана объектов с помощью технических средств. Именно поэтому и многие частные охранные предприятия в настоящее время используют данный вид охраны.

Суть ее в том, что информация от технических средств, установленных на территориально рассредоточенных объектах, поступает непосредственно на центральный пульт, где в автоматизированном режиме производится ее анализ, обобщение и выдача заявки, в зависимости от ситуации, группе реагирования либо технической службе.

Основу централизованной охраны составляют системы централизованного наблюдения (СЦН).

В начале своего развития наиболее широкое применение, как у нас, так и за рубежом, нашли СЦН, использующие в качестве каналов связи телефонные линии. Это вполне объяснимо. Оборудование таких систем сравнительно дешево, а почти повсеместная телефонизация позволяет подключать к ним практически любые объекты.

Первоначально на нашем рынке почти полностью отсутствовали системы зарубежного производства. Зарубежные СЦН – это, как правило, информаторные системы, которые не требуют для своей работы установки дополнительного оборудования на АТС и передают тревожную информацию путем прямого автодозвона на пульт. Существенным недостатком таких систем является отсутствие контроля канала связи, что не позволяет обеспечить надежную охрану объектов из-за простоты их «обхода». Достаточно произвести обрыв телефонной линии, и тревожная информация будет утеряна, а сам факт обрыва не зафиксируется на пульте.

И именно поэтому одним из основных требований вневедомственной охраны является обязательное наличие контроля канала связи, несмотря на то, что система будет чуть дороже и сложнее. Хотя до сих пор даже крупные коммерческие мониторинговые компании используют информаторные системы.

Несмотря на очевидную эффективность централизованной охраны, при внедрении и эксплуатации СЦН возникают определенные проблемы, на которых хотелось бы остановиться ниже.

Первая из них связана с повышением «профессионального» уровня криминального контингента. В последнее время появились случаи «квалифицированных» краж, совершаемых путем активного, т.е. с применением специальных технических средств, вмешательства в работу оборудования и каналов связи СЦН. И если сейчас известны лишь отдельные подобные случаи, то в самое ближайшее время это может стать массовым явлением.

Единственный путь решения данной проблемы, а это, несомненно, одна из важнейших проблем самого ближайшего будущего, – применение современных методов имитостойкости аппаратуры и криптозащиты каналов связи, обеспечивающих устойчивость системы к несанкционированному вмешательству в ее работу.

Вторая проблема – это организация охраны так называемых «больших объектов». Это объекты кредитно-финансовой сферы, особой важности, повышенной опасности, жизнеобеспечения и им подобные.

В настоящее время наиболее перспективным и общепризнанным путем организации их защиты является применение интегрированных систем безопасности (ИСБ).

ИСБ в системах централизованной охраны представляет собой объектовое оборудование, однако количество информации, которое необходимо передавать на пульт и принимать со стороны пульта, в этом случае значительно возрастает.

Особенно это связано с применением в составе ИСБ телевизионных систем, которые в настоящее время широко применяются для повышения безопасности различных объектов.

В соответствии с этим, актуальной задачей является сопряжение высокоинформативного оборудования ИСБ с оборудованием СЦН.

Добиться максимальной эффективности функционирования ИСБ и систем централизованной охраны в целом возможно только повышением их информативности, которое позволяет оптимизировать действия групп задержания за счет постоянного мониторинга поведения преступника на объекте или развития других негативных ситуаций (например, пожара). В особенности это касается критически важных объектов, где оперативность принятия решений, грамотное распределение сил и средств играют первостепенную роль.

Третья и, пожалуй, самая серьезная проблема, касающаяся проводных СЦН, а они на сегодняшний день, как уже было отмечено, занимают доминирующее положение, обусловлена технической политикой компаний, предоставляющих услуги телефонной связи. Являясь в какой-то степени монополистом в своей области, необоснованно повышают цены на аренду телефонных линий и площадей на АТС, заранее не информируют охранные структуры о предстоящих реконструкциях, замене и параметрах нового оборудования на телефонных станциях.

Единственный путь решения данной проблемы – это применение альтернативных каналов связи для организации централизованной охраны. По своему принципу их можно разделить на две группы: проводные и беспроводные. До недавнего времени единственным из «альтернативных» применялся лишь выделенный радиоканал (РСПИ). В последнее время, помимо традиционного радиоканала, все активнее начинают использоваться другие альтернативные каналы (GSM, Интернет и др.). Выбор применяемого канала связи зависит от мно-

гих факторов. Рассмотрим их несколько подробнее.

Сотовая сеть стандарта GSM сейчас имеет широчайшую зону покрытия, что делает ее весьма привлекательной для организации централизованной охраны. Учитывая, что основная цель ее создания – это передача речевых сообщений, основной канал, имеющий определенные приоритеты – это голосовой канал. Помимо голосового канала, в GSM-сети существует цифровой канал данных, канал GPRS (EDGE) и с недавнего времени высокоскоростной канал 3G. При использовании каждого из указанных каналов для целей охраны необходимо понимать их особенности.

В голосовом канале существует явление «хендовер». Так называется любое переключение на другой канал или таймслот одной и той же соты. Такое переключение происходит при резком увеличении нагрузки на сотовую сеть, например, после футбольного матча или при приземлении самолета. При таком переключении происходит изменение спектра передаваемого сигнала, что является допустимым для передачи речи и неприемлемо для передачи цифровой информации. А ведь для целей охраны по голосовому каналу будет передаваться именно «цифра». То есть при возникновении такого явления канал связи становится крайне неустойчивым.

Для передачи цифровой информации в сетях GSM существует специальный канал цифровых данных. Скорость передачи невелика, но достаточна для передачи сообщений в небольшом объеме, схожем по информативности с Contact-ID. Сообщения передаются без искажений. Но передача информации через цифровой канал данных будет доступна лишь, если сеть не будет загружена, поскольку в существующих GSM-сетях общего пользования приоритет отдается голосовому каналу.

Эта проблема частично решается путем использования канала GPRS (EDGE). В этом случае применяется протокол TCP/IP. Операторы предлагают специальные тарифы, при использовании которых канал будет доступен вне зависимости от загруженности сотовой сети. Но для использования GPRS уровень сигнала GSM должен быть стабильно высоким. Также на качество и скорость цифровой передачи влияют «индустриальные помехи», которые часто присутствуют в городе.

Использование 3G схоже с GPRS, но значительно повышена информативность. Однако покрытие сетей 3G пока невелико, а оборудование заметно дороже.

Но самой главной проблемой использования GSM-каналов является достаточно простая возможность подавления сигнала (с помощью так называемых «глушилок»), а осуществлять надежный контроль канала, например, с помощью специально предназначенных для корпоративных клиентов виртуальных корпоративных сетей – достаточно дорого.

Другая привлекательная сеть, которая имеет всеобщее распространение – это Интернет. Сегодня получить доступ к сети возможно многими способами. При этом применяются как проводные, так и современные беспроводные технологии. Но здесь возникает потенциальная опасность несанкционированного доступа к данным и внесения компьютерных вирусов. Кроме того, исследования показали, что неоднократно в течение суток возникают пропадания связи на время от десятков секунд до нескольких минут. Причиной этого является, как правило, перегрузка сервера провайдера, которая может быть вызвана длительной информационной загруженностью одного из каналов в сети, проведением «хакерской» атаки и рядом других причин. Причем по-

влиять на этот процесс практически невозможно. Так устроена аппаратура цифровых каналов.

Для того чтобы избежать негативных последствий использования открытых сетей общего пользования (GSM, Интернет), необходимо использовать их с применением закрытых выделенных каналов или создавать свои независимые сети.

В условиях городской застройки для этого подходит современный стандарт беспроводной связи WiMax. На сегодняшний день в Москве уже развернуты две коммерческие сети. Они созданы для доступа к Интернету, цифровому телевидению и IP-телефонии. В будущем возможно их использование для централизованной охраны, поскольку эта технология позволяет выделить независимый закрытый канал внутри развернутой сети общего пользования. Протокол, используемый в WiMax, позволяет надежно осуществлять контроль канала без дополнительных затрат, в отличие от GSM, а канал передачи данных обладает высокой пропускной способностью, что особенно важно для организации связи с объектами, где необходима большая информативность. Стоимость оборудования для доступа к сети уже сейчас сравнима со стоимостью GSM-модема, что не создает дополнительных препятствий для его внедрения. На самом деле использовать современный стандарт беспроводного доступа для организации охраны можно уже и сегодня.

Однако, несмотря на появление массовых технологий беспроводного доступа, еще длительное время будут сохранять свое значение как специализированный класс оборудования радиосистемы передачи извещений (РСПИ). В основе этого лежат как экономические факторы, так и стремление большинства поставщиков услуг к созданию собственной, независимой от внешних обстоятельств, сети передачи данных.

Рассматривая тенденции развития РСПИ российского производства, нельзя не отметить постепенный переход от односторонних способов обмена информацией (от объектового оборудования к пультовому) к двухсторонним.

Такой переход, по мнению авторов статьи, обусловлен следующими факторами:

- появлением сравнительно дешевой элементной базы, серийно выпускаемых микросхем с функциями приемопередающего радиотракта;
- необходимостью экономного отношения к использованию частотных ресурсов (при организации дисциплины опроса всегда можно увеличить количество обслуживаемых абонентов, но не при отсутствии таковой);
- возможностью предоставления специальных и сервисных функций, реализуемых только при возможности диалога между центральным оборудованием и оборудованием, установленным на объекте.

Кроме вышеуказанных преимуществ, переход к двухстороннему способу обмена информацией позволил значительно повысить информативность систем. Если раньше количество видов информации было достаточно жестко ограничено (как правило, «Взят под охрану», «Снят с охраны», номера и типы нарушенных/восстановленных шлейфов сигнализации, информация о состоянии электропитания и т.п.), то теперь эти ограничения связаны только с границами фантазии разработчика. К сожалению, фантазия большинства российских разработчиков не пошла дальше старого доброго формата «Contact ID».

С другой стороны, резкое увеличение информативности общения между объектовым и пультовым оборудованием в радиоканальных системах привело к возникновению еще одной интересной тенденции. А именно, к интеграции с объектовыми подсистемами других производителей. Продавая свое радиоканальное оборудование, изготовитель заинтересован в том, чтобы его оборудование позволило решить наибольшее количество задач, возникающих в реальной жизни. Наиболее коротким путем к такой универсализации является обеспечение возможности подключения максимального количества подсистем «нижнего» уровня с сохранением их полной информативности. Например, изготовитель РСПИ не может качественно реализовать подсистему сбора информации от беспроводных извещателей или биометрическую систему контроля доступа. Это лучше умеют другие. Но он может договориться о сопряжении протоколов обмена информацией. И в этом случае оба партнера получают взаимную выгоду.

В целом такие изменения носят положительный характер. Поскольку конечный потребитель остается только в выигрыше, получая улучшенные сервисные функции за ту же цену.

Наиболее актуальными проблемами для совершенствования РСПИ являются две, на первый взгляд, несовместимые задачи. Уменьшение используемой полосы рабочих частот и повышение скорости обмена информацией в радиоканале. Использование полос рабочих частот шириной 25 кГц уже сейчас становится анахронизмом. А в дальнейшем, при усилении контроля над пользованием радиочастотного спектра, станет экономически нецелесообразным. С другой стороны, непрерывное развитие объектовых подсистем, в том числе систем охранного телевидения, постоянно повышает требования к пропускной способности канала связи между объектовой и пультовой частью. Это противоречие оставляет широчайший простор для творчества.

В настоящее время количество частных охранных предприятий и мониторинговых компаний только растет, что влечет все большую конкуренцию между ними. В условиях отсутствия единой технической политики в области организации централизованной охраны, определяющей требования по надежности применяемых СЦН, некоторые компании идут по пути уменьшения затрат в ущерб надежности. Это приводит к снижению качества оказываемых услуг, т.е. к общему снижению уровня безопасности и защищенности. На чем же они экономят?

В последние годы грань между городом и областью постепенно стирается: одни переезжают жить подальше от шумного мегаполиса, другие проводят загородом большую часть своего времени, и все больше людей хотят защитить не только свои квартиры, но и недвижимость за пределами города. В таких условиях большинство мониторинговых компаний используют, как правило, каналы сотовой связи GSM. А, как говорилось выше, осуществление контроля сотового канала – вещь достаточно затратная. На пульте не будет информации о том, что система выключена, сломалась или была умышленно выведена из строя до 12 часов, а заявка технической службе поступит лишь после 72 часов «молчания» системы. О какой надежности такой организации охраны можно говорить?

Подводя итог всему вышеизложенному, если мы говорим о создании надежной централизованной охраны различных объектов, можно определить следующие приоритетные направления в создании и развитии СЦН:

1. Системы должны иметь модульную структуру с полным комплектом устройств, позволяющим обеспечивать работу по любым имеющимся на сегодняшний день (и даже перспективным) каналам связи, возможность стыковки с уже существующими системами, а также сопряжения с различными типами аппаратуры, используемой для организации телефонной связи (новые электронные АТС, системы цифрового уплотнения, оптоволоконные каналы связи и т.п.). Все эти возможности должны быть реализованы на единой программно-аппаратной платформе.
2. Протоколы обмена, используемые для передачи тревожных и служебных извещений, должны быть защищены от несанкционированного вмешательства в работу системы с помощью специальных средств снятия и внесения ложной информации в каналы связи.
3. Информативность систем должна обеспечивать уровень мониторинга состояния объекта, максимально повышающий оперативность реагирования групп задержания.

На наш взгляд, такая стратегия создания и развития систем централизованного наблюдения позволит более эффективно решать вопросы организации охраны самых разнообразных объектов.