СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО НАБЛЮДЕНИЯ — ПЕРСПЕКТИВЫ РАЗВИТИЯ

А. Г. Зайцев, *заместитель начальника НИЦ «Охрана» МВД России*

В измененной структуре МВД России функции вневедомственной охраны частично возложены на Департамент государственной защиты имущества, что ставит перед ним дополнительные задачи.

ПРАКТИЧЕСКИ с начала образования вневедомственная охрана России в рамках одной структуры обеспечивала одновременное выполнение трех основных функций: технической (охрана с помощью технических средств), милицейской (реагирование нарядами милиции) и страховой (возмещение материального ущерба).

Сегодня в мировой практике охранных услуг определилась устойчивая тенденция усиления роли технических средств. И это неслучайно: многочисленные исследования в области личной и имущественной безопасности показали, что широкое использование технических средств позволяет свести к минимуму либо полностью исключить негативное влияние самого ненадежного звена в системе охраны — человека, которому могут быть присущи утомляемость, невнимательность, халатность и подобные черты.

К надежности технической составляющей всегда предъявлялись повышенные требования с целью снижения затрат по двум остальным. При этом организация охраны с помощью технических средств обходится потребителю значительно дешевле. Именно поэтому все ведущие страны, включая Россию, уделяют большое внимание созданию технических средств на основе последних научных достижений, информационных и коммуникационных технологий.

Более чем 50-летний опыт работы вневедомственной охраны МВД России в этой области показал, что наиболее эффективной и экономически выгодной является централизованная охрана. Суть ее состоит в том, что информация от технических средств, установленных на территориально рассредоточенных объектах, поступает непосредственно на пульт централизованного наблюдения (ПЦН), где в автоматизированном режиме производится ее анализ, обобщение и выдача заявки на реагирование милицейскому наряду либо технической службе.

Высокая информативность современных технических средств позволяет определить, какова угроза объекту, оптимизировать силы и средства, необходимые для противодействия преступным посягательствам.

Техническую основу централизованной охраны составляют системы централизованного наблюдения (СЦН). 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.

Очевидно, этим объясняется отсутствие на нашем рынке конкурентоспособных систем иностранного 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 ПЦН.

В середине 90-х годов при создании СЦН основное внимание уделялось таким аспектам, как:

- автоматизация, которая позволяет максимально упростить процессы сдачи/взятия объектов под охрану, сократить дежурный персонал пультов централизованного наблюдения, существенно уменьшить число ложных тревог из-за неправильных действий хозорганов;
- контроль канала связи, обеспечивающий высокую достоверность передачи и исключающий потерю тревожной информации;
- разработка широкой гаммы объектовых устройств с различными функциональными и сервисными возможностями, позволяющих удовлетворить потребности самых широких слоев населения.

С учетом этих требований были разработаны и внедрены такие системы, как «Ахтуба», «Юпитер», «Приток-А», «Фобос-А», «Фобос-3» и др.

С точки зрения организации защиты объектов от несанкционированного проникновения (как по оборудованию техническими средствами охраны, так и по тактике действий дежурных служб) все перечисленные СЦН не имеют каких-либо существенных отличий, однако каждая из них обладает своими достоинствами и недостатками, которые определяют и ограничивают область их применения.

Главным же недостатком указанных систем является разнородность технических и конструкторских решений, а также закрытая архитектура построения, что не позволяет провести их объединение в универсальный комплекс технических средств централизованной охраны в пределах одного ПЦО.

В конечном счете это приводит к возникновению трудностей для всех структур вневедомственной охраны во внедрении, эксплуатации, обслуживании и ремонте разнородных технических средств, проведении единой технической политики, обеспечении должного уровня качества и надежности оборудования, а следовательно, к дополнительным финансовым затратам и увеличению тарифов на охранные услуги.

Актуальной на сегодняшний день остается проблема упорядочения парка эксплуатируемых систем централизованного наблюдения, его обновления, замены устаревшего оборудования современным, более надежным. Кроме того, в последнее время появились «квалифицированные» кражи, то есть попытки технического обхода используемых СЦН. И если сейчас известны лишь отдельные подобные случаи, то в ближайшее время это может стать массовым явлением. **Причин этому две:**

- повышение технической грамотности криминального контингента (преступники, как правило, имеют высшее или среднее техническое образование, опыт работы в отраслях, связанных с радиоэлектроникой);
- практически полная незащищенность проводных каналов.

В настоящее время необходимый уровень защиты закупаемой техники в течение всего срока службы (8 и более лет) могут обеспечить только системы, использующие принципы динамического кодирования передаваемой информации. Поэтому в целях дальнейшего развития и совершенствования централизованной охраны **новые разработки должны обеспечивать:**

- имитостойкость и криптозащиту для устойчивости системы к несанкционированному «обходу», что обусловлено появлением «квалифицированных» краж;
- высокую информативность, позволяющую разделять сигналы о проникновении и пожаре, аварии или изменении параметров линии связи и т. д.;
- возможность сопряжения системы с оптоволоконными каналами связи, обусловленную внедрением предприятиями связи новых цифровых технологий передачи информации;
- унификацию создаваемых технических средств, то есть возможность интеграции различных устройств в единый программно-аппаратный комплекс централизованной охраны.

С учетом этих требований разработаны и уже внедряются система передачи извещений (СПИ) «Атлас-20» и комплекс централизованного наблюдения (КЦН) «Альтаир».

При разработке указанных систем большое значение придавалось обеспечению информационной защищенности каналов передачи. Благодаря применению современных методов криптозащиты практически полностью исключается возможность «обхода» даже с применением специальных технических средств считывания и загрузки в канал ложной информации.

Использование в подразделениях охраны СПИ «Атлас-20» и КЦН «Альтаир» позволит:

- укрупнить существующие ПЦО с уменьшением общего количества операторов за счет автоматизации СЦН с ручной тактикой работы, количества арендуемых каналов связи и сокращения затрат на охрану объектов;
- существенно снизить затраты на приобретение новой техники за счет поэтапного внедрения ее в подразделения охраны;
- обеспечить возможность работы СПИ по любым современным каналам связи (цифровое уплотнение, оптоволокно и др.);
- уменьшить количество каналов передачи данных (вследствие упорядочения структуры и повышения скорости передачи информации).

Для КЦН «Альтаир» предусматривается создание четырех новых объектовых устройств серии «Набат» с соответствующим уровнем криптозащиты.

Таким образом, можно сделать вывод, что техническая политика ВО в области создания и внедрения СЦН должна строиться с учетом повышенных требований к информативности, автоматизации, имитостойкости, криптозащите каналов передачи информации и унификации оборудования, а также с учетом возможного сопряжения с различными типами аппаратуры, используемой для организации телефонной связи (новые электронные АТС, системы цифрового уплотнения, оптоволоконные каналы связи и т. п.).

Если провести анализ используемых сегодня подразделениями вневедомственной охраны СЦН, то их можно условно разделить на три группы:

1 группа — наиболее перспективные для внедрения СЦН, в которых полностью учтены вышеназванные требования;

2 группа — СЦН, отвечающие сегодняшним требованиям, однако имеющие перспективу внедрения на ближайшие годы при условии их унификации и соответствующей модернизации;

1 группа	2 группа	3 группа
1. КЦН «Альтаир». *Изготовители: ЗАО «ЭП ЦНИТИ» (г. Ногинск, Московской обл.); АООТ «Радий» (г. Касли, Челябинской обл.)* **2. СПИ «Атлас-20».** *Изготовитель — АО «Аргус - Спектр» (г. Санкт-Петербург)*	**1. СПИ «Ахтуба».** *Изготовитель — АО «Ахтуба Плюс» (г. Волжский, Волгоградской обл.)* **2. СПИ «Юпитер».** *Изготовитель — ТОО «Элеста» (г. Санкт-Петербург)* **3. АСПИ «Приток».** *Изготовитель — ООО «Охранное бюро Сократ» (г. Иркутск)*	**1. СПИ «Фобос».** *Изготовители: ЗАО «ЭП ЦНИТИ» (г. Ногинск, Московской обл.); АООТ «Радий» (г. Касли,Челябинской обл.)* **2. СПИ «Нева-МД».** *Изготовитель — ООО «КБ систем связи» (г. Москва)* **3. СПИ «Фобос-3».** *Изготовители: ЗАО "ЭП ЦНИТИ» (г. Ногинск, Московской обл.); АООТ «Радий» (г. Касли, Челябинской обл.)*

3 группа — не имеющие перспективы, морально устаревшие СЦН, которые по большинству указанных параметров не удовлетворяют современным требованиям и дальнейшее развитие которых нецелесообразно, поскольку потребует серьезных материальных затрат.

Представители систем по группам представлены в таблице.

При дальнейшей эксплуатации СЦН в ближайшее время может возникнуть еще одна серьезная проблема. Минсвязи России выпущен новый документ, запрещающий работу любого дополнительного оборудования, устанавливаемого на АТС, на несущих частотах ниже 30 кГц. Эксплуатирующиеся сейчас системы работают, как известно, на частоте 18 кГц, то есть входят в прямое противоречие с этими требованиями. Чем это грозит вневедомственной охране — объяснять не нужно. В связи с этим планируется провести разработку новых узлов для обеспечения работы КЦН «Альтаир» на рабочих частотах 36 кГц.

Другими приоритетными задачами технической политики в области развития централизованной охраны являются следующие.

Во-первых, разработка единых требований на системы централизованного наблюдения, что при многообразии существующих и вновь появляющихся предприятий — разработчиков и производителей средств охранно-пожарной сигнализации позволит унифицировать стыки систем передачи извещений, как вновь разрабатываемых, так и уже находящихся в эксплуатации.

Во-вторых, расширение функциональных возможностей комплексов средств автоматизации (КСА) ПЦО в части решения неоперативных задач (документооборот, статистика, техническое обслуживание, регламентные работы ТС ОПС, договорная работа и т. п.), которые составляют значительную долю в работе подразделений.

Анализ работы КСА ПЦО показал, что ни один из них, решая прямые задачи оперативного управления работой ПЦО, не охватывает в должной мере большого круга неоперативных задач. Проведение указанных работ позволит значительно упростить и облегчить работу персонала ПЦО и ОВО в целом.

В последние годы особое внимание уделялось созданию и развитию радиосистем передачи извещений (РСПИ). **Внедрение охранных систем, использующих радиочастотные каналы связи, позволяет:**

- расширить сферу деятельности подразделений ВО путем организации охраны объектов, не имеющих линии телефонной связи;
- повысить надежность систем охраны особо важных объектов за счет дублирования телефонных каналов связи;
- обеспечить при необходимости срочную установку оборудования на объекте, нуждающемся в охране.

Деятельность НИЦ «Охрана» в данной области была направлена на удешевление оборудования радиосистем с целью повышения его доступности для населения. В то же время качество систем в отношении потребительских свойств, надежности и защищенности передаваемой информации должно постоянно повышаться.

С этой целью в 2004 году были продолжены работы по созданию радиосистемы малой емкости со сниженной стоимостью объектового оборудования и улучшенными тактико-техническими и эксплуатационными параметрами. Это достигается за счет применения нового подхода к структурному построению системы, современного пультового, ретрансляционного и объектового оборудования. При этом одним из основных условий данной работы является совместимость новой системы с ранее установленным радиоканальным объектовым оборудованием серии «Струна».

Перспективы развития РСПИ рассматриваются НИЦ «Охрана» как составная часть создания единого унифицированного комплекса технических средств охраны. Поэтому важнейшим свойством новых систем является «открытость» архитектуры. Под этим подразумевается обеспечение технической возможности для сопряжения с любыми типами объектового оборудования и другими системами охраны.

Сопряжение с охранными, охранно-пожарными и пожарными приборами, а также интегрированными системами достигается путем создания приемно-передающих устройств с универсальным интерфейсным входом коммуникатора.

В рамках дальнейшего развития РСПИ в 2005–2006 гг. планируется создание радиосистем большой емкости (10 тысяч и более охраняемых объектов) с организацией контроля канала связи в течение не более 2 мин.

Поскольку создание РСПИ большой емкости, отвечающей требованиям по защищенности канала связи, возможно только на базе двухстороннего синхронного канала связи, следует считать это направление наиболее перспективным при создании радиосистемы для средних и больших городов.

Полная реализация изложенных направлений позволит уже в ближайшее время значительно повысить надежность охраны имущества и будет способствовать снижению краж на охраняемых объектах.