УТВЕРЖДАЮ
Начальник ДГЗИ МВД России
генерал-лейтенант милиции

В.В. Савичев

«2» 04 2008

Единые требования к системам передачи извещений и системам мониторинга подвижных объектов, предназначенным для применения в подразделениях вневедомственной охраны

СОГЛАСОВАНО
Начальник
ЦОРДВО МВД России
полковник милиции

С.Н. Голованов

«31» 03 2008

СОГЛАСОВАНО
Заместитель начальника
ФГУ НИЦ «Охрана» МВД России
полковник милиции

А.Г. Зайцев

« » 2008

Москва 2008 год

Настоящий документ определяет единые требования к системам передачи извещений и системам мониторинга подвижных объектов, порядок проведения их экспертизы на соответствие указанным требованиям, а также порядок проведения эксплуатационных испытаний с целью проверки работоспособности в реальных условиях эксплуатации[1].

I Технические требования к системам централизованного наблюдения.

Применение систем передачи извещений, удовлетворяющих изложенным ниже требованиям позволит подразделениям вневедомственной охраны :

- обеспечивать надежную охрану объектов различных форм собственности и исключить возможность использования недоброкачественной аппаратуры охранной сигнализации;
- сократить затраты на охрану (сокращение затрат на эксплуатацию, ремонт и обслуживание технических средств охраны, сокращение единовременных затрат на их приобретение и т.п.);
- осуществить укрупнение пунктов централизованной охраны (ПЦО) (например, по принципу - один пункт на отдел), что требует качественно нового подхода к построению систем централизованного наблюдения.

1 Общие требования к СЦН.

1.1 Современные средства СЦН должны соответствовать следующим требованиям:

- вся аппаратура должна удовлетворять нормам пожарной безопасности на данную категорию изделий;
- быть совместимой и сохранять преемственность с используемой на ПЦО аппаратурой;
- иметь современный дизайн и использовать последние достижения в развитии вычислительной техники и новых компьютерных технологий;

[1] Порядок проведения экспертизы и эксплуатационных испытаний представлены в приложении 1.

- обладать высокой информативностью, позволяющей разделять сигналы о проникновении и пожаре, аварии или изменении параметров линии связи и т.д.;

- обеспечивать сопряжение с оптоволоконными каналами связи, и другими цифровыми технологиями передачи информации;

- обеспечивать возможность интеграции различных устройств в единый программно-аппаратный комплекс централизованной охраны.

1.2 При разработке систем большое значение должно придаваться обеспечению информационной защищенности каналов передачи. Для исключения возможности «обхода» систем сигнализации даже с применением специальных технических средств считывания и загрузки в канал ложной информации должны применяться современные методы криптозащиты.

2 Технические требования к СЦН, работающим по проводным линиям связи.

2.1 СЦН должны строиться на основе многоуровневой иерархической структуры с обеспечением автоматизированной тактики постановки/снятия объектов под охрану

I уровень - интеграция на едином пультовом оборудовании тех систем, которые имеют принципиально несовместимые каналы передачи данных (радиоканальные и информаторные системы, а также системы, использующие выделенные проводные линии связи и вычислительные сети).

II уровень - интеграция на АТС тех систем, которые используют для связи с объектами занятые, либо переключаемые на период охраны линии связи с единым каналом передачи данных на пульт.

III уровень - интеграция объектовых (квартирных) подсистем с уменьшением общего количества каналов передачи данных на аппаратуру сбора сообщений.

Настоящий документ определяет единые требования к системам передачи извещений и системам мониторинга подвижных объектов, порядок проведения их экспертизы на соответствие указанным требованиям, а также порядок проведения эксплуатационных испытаний с целью проверки работоспособности в реальных условиях эксплуатации[1].

I Технические требования к системам централизованного наблюдения.

Применение систем передачи извещений, удовлетворяющих изложенным ниже требованиям позволит подразделениям вневедомственной охраны :

- обеспечивать надежную охрану объектов различных форм собственности и исключить возможность использования недоброкачественной аппаратуры охранной сигнализации;
- сократить затраты на охрану (сокращение затрат на эксплуатацию, ремонт и обслуживание технических средств охраны, сокращение единовременных затрат на их приобретение и т.п.);
- осуществить укрупнение пунктов централизованной охраны (ПЦО) (например, по принципу - один пункт **на** отдел), что требует качественно нового подхода к построению систем централизованного наблюдения.

1 Общие требования к СЦН.

1.1 Современные средства СЦН должны соответствовать следующим требованиям:

- вся аппаратура должна удовлетворять нормам пожарной безопасности на данную категорию изделий;
- быть совместимой и сохранять преемственность с используемой на ПЦО аппаратурой;
- иметь современный дизайн и использовать последние достижения в развитии вычислительной техники и новых компьютерных технологий;

[1] Порядок проведения экспертизы и эксплуатационных испытаний представлены в приложении 1.

- обладать высокой информативностью, позволяющей разделять сигналы о проникновении и пожаре, аварии или изменении параметров линии связи и т.д.;

- обеспечивать сопряжение с оптоволоконными каналами связи, и другими цифровыми технологиями передачи информации;

- обеспечивать возможность интеграции различных устройств в единый программно-аппаратный комплекс централизованной охраны.

1.2 При разработке систем большое значение должно придаваться обеспечению информационной защищенности каналов передачи. Для исключения возможности «обхода» систем сигнализации даже с применением специальных технических средств считывания и загрузки в канал ложной информации должны применяться современные методы криптозащиты.

2 Технические требования к СЦН, работающим по проводным линиям связи.

2.1 СЦН должны строиться на основе многоуровневой иерархической структуры с обеспечением автоматизированной тактики постановки/снятия объектов под охрану.

I уровень - интеграция на едином пультовом оборудовании тех систем, которые имеют принципиально несовместимые каналы передачи данных (радиоканальные и информаторные системы, а также системы, использующие выделенные проводные линии связи и вычислительные сети).

II уровень - интеграция на АТС тех систем, которые используют для связи с объектами занятые, либо переключаемые на период охраны линии связи с единым каналом передачи данных на пульт.

III уровень - интеграция объектовых (квартирных) подсистем с уменьшением общего количества каналов передачи данных на аппаратуру сбора сообщений.

2.2 СЦН должна иметь единый протокол обмена данными между всеми его компонентами, обеспечивающий:

2.2.1 Достаточную глубину вложения адресации к отдельным устройствам (не менее 4, вплоть до шлейфа сигнализации), что позволит получить гибкость построения системы, оптимизировать маршрутизацию информационных потоков и обеспечить возможность наращивания информационной емкости без увеличения используемых каналов передачи данных.

2.2.2 Достаточную величину адресного пространства для обеспечения совместной работы с объектовыми подсистемами большой емкости и возможностью передачи от объекта на ПЦН расширенной информации (вплоть до шлейфов сигнализации) по одному каналу передачи данных.

2.2.3 Необходимый уровень криптостойкости на всех уровнях с целью исключения возможности несанкционированного вмешательства в работу СЦН. Длина ключей шифрования должна составлять не менее 16 двоичных разрядов (количество кодовых комбинаций не менее 65536) при использовании симметричных методов кодирования. При этом недопустимо передавать одну и ту же информацию одинаковыми кодовыми блоками от посылки к посылке.

2.2.4 Возможность логического расширения без изменения структуры протокола, что позволит обеспечить дальнейшее развитие функциональных возможностей СЦН без проведения доработок ранее созданного оборудования.

2.3 Структура СЦН должна предусматривать возможность сопряжения:

2.3.1 Всех составных частей с современной аппаратурой уплотнения абонентских линий связи и с оптоволоконными линиями передачи данных в связи с внедрением электронных АТС, использующих подобные технологии.

2.3.2 С имеющимся парком технических средств охраны, широко эксплуатируемым подразделениями вневедомственной охраны и не выработавшим установленных сроков службы. Это позволит организовать

поэтапное (экономически оправданное) внедрение СЦН без кардинальной ломки сложившейся инфраструктуры охраны.

2.4 СЦН должна обеспечивать высокие требования к надежности функционирования своих узлов и составных частей, а также каналов связи с обеспечением, при необходимости, их резервирования вплоть до «горячего». Гарантийный срок СЦН должен составлять не менее пяти лет.

2.5 СЦН должна быть оснащена развитой системой тестирования и диагностики, позволяющей упростить процесс поиска неисправностей и сократить время восстановления ее работоспособности в случае возникновения нештатных ситуаций.

2.6 СЦН должна иметь открытую архитектуру построения на всех уровнях иерархии с целью обеспечения расширения ее функциональных возможностей, сокращения процесса разработки, внедрения новых перспективных подсистем охраны, унификации вновь создаваемого оборудования, а также обеспечения сопряжения с другими СЦН, принятыми на вооружение вневедомственной охраны.

2.7 Емкость 1 единицы ретрансляционного оборудования должна быть не менее 110 направлений (типовое значение 240), что обеспечивает минимизацию арендной платы на АТС. Для обеспечения совместной работы с электронными АТС (в частности, с «выносами») допускается создание модификаций ретрансляторов меньшей емкости.

2.8 Системы, работающие по занятым телефонным линиям, должны иметь двухсторонний обмен данными на стыке «ретранслятор - объектовое оборудование», который позволяет:

- обеспечить подтверждение на объекте процедуры постановки/снятия под охрану;

- применять эффективные методы шифрования данных, препятствующие «техническому обходу» системы и имитации сообщений;

- значительно повысить надежность функционирования системы за счет режима включения передатчика только на время обмена данными

(скважность более 100), не перегружающего каналы связи и не создающего перекрестных помех на соседние каналы.

- повысить надежность функционирования системы за счет возможности передачи данных только на время обмена, не перегружая при этом каналы связи и уменьшая перекрестные помехи на соседние каналы;

- обеспечить возможность адресного подключения нескольких объектовых устройств на одно направление, что позволит значительно увеличить информационную емкость СЦН при неизменном количестве подводимых абонентских линий связи.

2.9 СЦН должны обеспечивать охрану нескольких (не менее 2) объектов по одной абонентской линии без использования дополнительных концентраторов, что дает возможность повысить эффективность защиты малотелефонизированных объектов и увеличить фактическую емкость ретрансляционного оборудования.

2.10 Время доставки тревожного сообщения должно быть не более 15 с при загрузке системы не менее 80%. Допускается оценка данного параметра экспертным методом.

2.11 СЦН, использующие в качестве каналов передачи данных абонентские линии ГТС, должна удовлетворять требованиям органов по сертификации Минсвязи России.

2.12 Время обнаружения неисправности каналов передачи тревожной информации для СЦН всех типов не должно превышать 120 с.

2.13 СЦН должны соответствовать общетехническим требованиям к аппаратуре приборостроения, таким как надежность, устойчивость к климатическим и механическим воздействиям, вибрации, электромагнитной совместимости, требованиям к безопасности.

3 Требования к комплексам средств автоматизации (КСА) деятельности персонала подразделений вневедомственной охраны.

3.1 Типовой состав КСА должен включать, как минимум, следующие виды автоматизированных рабочих мест (АРМ):

- АРМ администратора системы, базы данных: работа с таблицами БД; установление и корректировка конфигурационных и настроечных параметров, актуализация списков пользователей и их идентификаторов и другие параметры администрирования, в зависимости от используемой СУБД.

- АРМ дежурного оператора: функции приема, передачи извещений от СЦН (РСЦН), визуального интерфейса состояния ретрансляторов (пультов), наличие статистических и сервисных функций, возможность протоколируемой службы внутренней передачи информации;

- АРМ дежурного офицера: функции контроля действий операторов, групп задержания, визуального интерфейса состояния ретрансляторов (пультов), наличие статистических и сервисных функций, возможность протоколируемой службы внутренней передачи информации, протоколирования действий групп задержания, в том числе их устных докладов;

- АРМ инженера ПЦО: ведение статистики ложных срабатываний средств ОПС, объектовых карточек, ведомостей, сроков службы средств ОПС и другой необходимой информации.

Необязательные АРМ:

- АРМ начальника дежурной смены:
- АРМ цифровой звукозаписи и воспроизведения;
- АРМ юридической службы и договорных отношений;
- АРМ инспектора технической службы;
- АРМ инспектора кадров;
- АРМ инспектора секретариата;

4 Модульная структура построения КСА.

Для возможности наращивания комплекса по мере появления новых перспективных систем охраны необходимо предусмотреть возможность подключения независимого компактного программного модуля (драйвера или сервиса). Кроме этого необходимо предусмотреть гибкое наращивание интерфейса пользователя.

4.1 Надежность программных средств КСА.

Для этих целей в комплексе должна быть предусмотрена возможность организации аппаратного и программного резервирования технических средств охраны на уровне ПЦО. Объединение компьютеров комплекса в локальную вычислительную сеть (ЛВС) должно обеспечивать как минимум два маршрута информационных потоков между любыми парами АРМов, «горячее» резервирование АРМов оперативного персонала ПЦО, применение методов диспетчеризации ресурсов КСА ПЦО, оптимального их распределения между АРМами и т.п.

Современный комплекс должен работать под управлением современных надежных операционных систем, желательно промышленного класса с применением технологии «клиент - сервер», в тоже время он должен легко перестраиваться под более простые варианты использоьания для применения на ПЦО сельской местности.

При этом, недопустимо использование недокументированных особенностей как операционных систем, так и аппаратных особенностей персонального компьютера.

В комплексе должны быть предусмотрены средства: защиты от несанкционированного доступа, резервирования, диагностики (в т.ч. и ранней диагностики отказов) и восстановления.

Информация об ошибках в системе должна бать максимально полной и адекватной.

Отказы элементов системы не должны приводить к нарушению ее работоспособности в целом, потере данных или извещений.

4.2 Протоколирование процесса функционирования КСА.

Система должна обеспечивать протоколирование на всех уровнях своей структуры.

На нижнем уровне модули системы должны вести собственные технические протоколы, предназначенные, в основном, для фиксации и последующего выявления аппаратных сбоев нижнего уровня и программных ошибок с возможностью их опционального отключения (включения).

На верхнем уровне должно быть предусмотрено протоколирование событий с формированием соответствующих выборок и информации о дате и времени:

- тревожных сообщений;
- сообщений об охране (постановленных под охрану и снятых с охраны) квартир и объектов;
- сообщений о периодах охраны с возможностью суммирования длительности периода охраны за месяц;
- сообщений о неисправностях, в том числе нарушений каналов связи;
- сообщений об отключении электропитания на объекте (квартире) с переходом объектового оборудования на работу от резервного источника электропитания;
- сообщений о неисправности резервного аккумулятора.

4.3 Масштабируемость КСА ВО.

КСА не должен иметь ограничений на количество рабочих мест. При этом в комплексе должны быть предусмотрены средства синхронизации различных экземпляров баз данных по низкоскоростным каналам связи, что необходимо, например, при территориальной разобщенности различных подразделений одного подразделения, иметь автоматическую прозрачную для оператора трансляцию извещений на любой компьютер системы в соответствии с заданным алгоритмом, вне зависимости от источника его поступления и способа подключения аппаратных средств охраны.

4 Модульная структура построения КСА.

Для возможности наращивания комплекса по мере появления новых перспективных систем охраны необходимо предусмотреть возможность подключения независимого компактного программного модуля (драйвера или сервиса). Кроме этого необходимо предусмотреть гибкое наращивание интерфейса пользователя.

4.1 Надежность программных средств КСА.

Для этих целей в комплексе должна быть предусмотрена возможность организации аппаратного и программного резервирования технических средств охраны на уровне ПЦО. Объединение компьютеров комплекса в локальную вычислительную сеть (ЛВС) должно обеспечивать как минимум два маршрута информационных потоков между любыми парами АРМов, «горячее» резервирование АРМов оперативного персонала ПЦО, применение методов диспетчеризации ресурсов КСА ПЦО, оптимального их распределения между АРМами и т.п.

Современный комплекс должен работать под управлением современных надежных операционных систем, желательно промышленного класса с применением технологии «клиент - сервер», в тоже время он должен легко перестраиваться под более простые варианты использования для применения на ПЦО сельской местности.

При этом, недопустимо использование недокументированных особенностей как операционных систем, так и аппаратных особенностей персонального компьютера.

В комплексе должны быть предусмотрены средства: защиты от несанкционированного доступа, резервирования, диагностики (в т.ч. и ранней диагностики отказов) и восстановления.

Информация об ошибках в системе должна бать максимально полной и адекватной.

Отказы элементов системы не должны приводить к нарушению ее работоспособности в целом, потере данных или извещений.

4.2 Протоколирование процесса функционирования КСА.

Система должна обеспечивать протоколирование на всех уровнях своей структуры.

На нижнем уровне модули системы должны вести собственные технические протоколы, предназначенные, в основном, для фиксации и последующего выявления аппаратных сбоев нижнего уровня и программных ошибок с возможностью их опционального отключения (включения).

На верхнем уровне должно быть предусмотрено протоколирование событий с формированием соответствующих выборок и информации о дате и времени:

- тревожных сообщений;
- сообщений об охране (постановленных под охрану и снятых с охраны) квартир и объектов;
- сообщений о периодах охраны с возможностью суммирования длительности периода охраны за месяц;
- сообщений о неисправностях, в том числе нарушений каналов связи;
- сообщений об отключении электропитания на объекте (квартире) с переходом объектового оборудования на работу от резервного источника электропитания;
- сообщений о неисправности резервного аккумулятора.

4.3 Масштабируемость КСА ВО.

КСА не должен иметь ограничений на количество рабочих мест. При этом в комплексе должны быть предусмотрены средства синхронизации различных экземпляров баз данных по низкоскоростным каналам связи, что необходимо, например, при территориальной разобщенности различных подразделений одного подразделения, иметь автоматическую прозрачную для оператора трансляцию извещений на любой компьютер системы в соответствии с заданным алгоритмом, вне зависимости от источника его поступления и способа подключения аппаратных средств охраны.

4.4 Пользовательский интерфейс.

Все программные компоненты комплекса средств автоматизации должны иметь «дружественный» пользовательский интерфейс, обеспечивающий понятность и простоту, наглядность и удобство как инсталляции программных средств, так и работы с ними, электронную контекстно-привязанную помощь с подробной инструкцией о работе АРМ.

5 Информаторные СЦН.

Основным недостатком информаторных систем является отсутствие постоянного контроля каналов связи с пультовым оборудованием. Поскольку вневедомственная охрана выполняет и страховые функции, использование подобных систем без организации дополнительной защиты каналов недопустимо. В то же время системы такого типа могут найти применение там, где использование классических систем централизованного наблюдения невозможно (при организации телефонных каналов по оптоволоконным линиям связи, через устройства высокочастотного уплотнения, выносные концентраторы).

Выходом из сложившейся ситуации может быть применение систем, в которых объектовос оборудование связано между собой или с ТЩН дополнительным каналом обмена информацией.

При этом устройства пультовые оконечные (УПО), работающие по коммутируемым телефонным линиям, должны' удовлетворять следующим требованиям.

5.1 Соответствие требованиям ГОСТ 25007-81.

5.2 Определение номера вызывающего абонента.

5.3 Непрерывный контроль исправности телефонной линии, сигнализацию о нарушении ее работоспособности в течение времени не более 120с.

5.4 Наличие источника резервного питания для внешних (не встраиваемых в ПЭВМ) УПО, возможность работы при отключении

первичного электропитания, прием и просмотр принимаемых извещений в этом режиме, возможность передачи в компьютер извещений, принятых в автономном режиме, при восстановлении электропитания.

5.5 УПО должно обеспечивать контроль собственной работоспособности, достоверности принимаемых извещений и диагностику ошибок.

5.6 Уровень радиопомех, создаваемых УПО, не должен превышать значений, указанных в ГОСТ Р 50009 и соответствовать отраслевым нормам Минсвязи России (Нормы 9-93).

6 Радиоканальные СЦН.

Радиоканальные СЦН (радиоканальные системы передачи извещений - РСПИ) не отличаются по основным тактико-техническим требованиям от СЦН, использующих проводные каналы связи. В то же время специфика используемого канала связи вносит следующие дополнительные требования.

6.1 Предприятие-изготовитель РСПИ должно иметь разрешение на использование рабочих частот для серийного производства данной системы, выданное Государственной комиссией по радиочастотам Российской Федерации.

6.2 Радиоканальное оборудование РСПИ должно соответствовать требованиям ГОСТ 12252-86 «Радиостанции с угловой модуляцией сухопутной подвижной службы. Типы, основные параметры, технические требования и методы измерений».

6.3 РСПИ должна обеспечивать контроль канала связи с каждым из охраняемых объектов и определять факт нарушения связи за время не более 120 секунд.

6.4 Время доставки тревожных извещений от объектового оборудования до ПЦН не должно превышать 5 секунд.

6.5 Время доставки служебных извещений от объектового оборудования до ПЦН не должно превышать 120 секунд.

6.6 Время доставки сигналов управления от ПЦН до объектового оборудования не должно превышать 5 секунд.

6.7 Время доставки служебных извещений от ПЦН до объектового оборудования не должно превышать 120 секунд.

6.8 ПЦН РСПИ должен обеспечивать техническое диагностирование наличия сигнала от каждого из объектов, его уровня и уровня помехи в канале.

6.9 Оборудование РСПИ должно обеспечивать возможность передачи на ПЦН не менее 16 видов извещений, среди которых должны быть следующие:

- «взят под охрану» - контролируются все подключенные шлейфы сигнализации (ШС);

- «снят с охраны» - объект снят с охраны, контролируется пожарный и тревожный ШС;

- «вход» - нарушение ШС «Вход» во время действия временной задержки;

- «проникновение» - нарушение ШС «Вход» и не выполнение действий для перевода объектового оборудования в режим «снят с охраны»;

- «периметр» - нарушение ШС, включенных в группу «Периметр»;

- «объем» - нарушение ШС, включенных в группу «Объем»;

- «пожар» - нарушение ШС, включенных в группу «Пожар»;

- «взлом» - нарушение целостности корпуса объектового оборудования;

- «вызов милиции» - нажатие кнопки тревожной сигнализации;

- «патруль» - сигнал о прибытии группы задержания;

- «переход на резерв» - переход на электропитание от резервного источника;

- «резерв в аварийном состоянии» - разряд резервного аккумулятора.

7 СЦН с использованием сети GSM.

СЦН с использованием каналов мобильной сотовой связи (GSM, CDMA-2000 и пр.) применяются для организации защиты нетелефонизированных объектов.

7.1 Требования к системным параметрам СЦН с использованием сети GSM:

- системы должны обеспечивать передачу извещений по голосовому тракту в формате ADEMCO CONTACT ID. Допускается использование других протоколов, улучшающих качество (надежность, скорость, информативность, помехоустойчивость) передачи извещений по каналам GSM (CSD, GPRS и SMS), либо CDMA-2000 (DATA, SMS);

- при наличии «обратного» канала должна обеспечиваться возможность передачи команд «Запрос состояния», «Перевзятие». При этом в объектовом оборудовании должны быть предусмотрены меры, предотвращающие несанкционированное или не авторизованное управление приемно-контрольным прибором.

- устройство должно иметь альтернативный резервный канал передачи извещений (радиоканал, двухпроводный канал и т.п.).

7.2 Требования к устройствам оконечным объектовым (УОО):

- УОО должно иметь уникальный идентификатор объекта и передавать его на ПЦН;

- извещения, передаваемые от УОО ' на ПЦН, должны иметь информативность не менее 5 (сообщения - постановка на охрану, снятие с охраны, тревога, неисправность, тест канала связи);

- УОО должно иметь возможность дублирование передаваемых на ПЦН событий в виде SMS на мобильный телефон пользователя;

- УОО должно обеспечивать непрерывный контроль регистрации в сети GSM и передавать соответствующее извещение при отсутствии регистрации в течение 5 минут и более. Кратковременные (менее 5 минут) сбои при регистрации в сети не должны вызывать тревожных извещений;

- УОО должно обеспечивать контроль финансовых средств на счету SIM-карты и выдавать соответствующее предупреждение (пользователю или ПЦН) при снижении баланса ниже заданного критического уровня;

- УОО должно обеспечивать передачу сообщений, предназначенных для контроля канала связи. Период передачи контрольных сообщений зависит от используемого канала (голосовой, GSM CSD, GPRS, SMS). Период передачи должен программироваться при настройке УОО.

7.3 Требования к каналу связи от УОО до ПЦН.

УОО может работать в одном (или нескольких) режимах:

- дозвон;

- дозвон и передача данных с помощью сигналов DTMF;

-SMS;

- GPRS.

Настройка контроля канала связи должна иметь диапазон не менее:

- для SMS и автодозвона: 1 мин - 12 часов;

-для GPRS: 5с.

8 СЦН с использованием сети Ethernet.

СЦН с использованием сети Ethernet применяются для организации охраны нетелефонизированных объектов.

8.1 Требования к системным параметрам СЦН с использованием сети Ethernet:

- сопряжение устройства с сетью пер'едачи данных (физический уровень) должно соответствовать спецификации IEEE 802.3 10BaseT/100BaseT/l000BaseT;

- физическое подключение ППК к сети Ethernet должно производиться через стандартный интерфейс, например 10/100 BaseT с соблюдением всех требований стандарта (тип разъема, разводка контактов, уровни сигналов и проч.);

- в ТУ на ГОЖ должна быть предусмотрена полноценная проверка работоспособности по сети Ethernet, например подключением к компьютеру или какой-либо контрольной аппаратуре;

- связь между АРМ и ППК должна быть двухсторонней, то есть АРМ должен обнаруживать потерю связи или неработоспособность ППК настолько быстро, чтобы сохранялась возможность предотвращения кражи после преднамеренного нарушения связи. В свою очередь ППК должен отображать потерю связи с АРМ;

- протокол взаимодействия АРМ и ППК должен обеспечивать защиту от несанкционированной замены ППК на аналогичный или на какой-либо имитатор. Протокол должен быть криптостойким для защиты от получения сведений о функционировании охраняемого объекта в случае перехвата (сканирования) обмена;

- устройство должно использовать стек протоколов TCP/IP, обязательна поддержка протоколов ARP, ICMP. Для связи с ПЦН может быть использован протокол TCP или UDP. Весь трафик между УОО и ПЦН должен быть зашифрован;

- устройство должно иметь неизменяемый пользователем MAC-адрес из диапазона, выделенного IEEE Organization предприятию-изготовителю. Устройство должно иметь возможность использовать фиксированный IP адрес, допускается использование динамического адреса, полученного от сервера DHCP (в зависимости от настройки), при условии, что устройство является в сети клиентом;

- устройство может иметь возможность конфигурирования, диагностики и управления через Web-интерфейс (протокол HTTP), при этом должна быть обеспечена защита от несанкционированного доступа не хуже Digest Access Authentication (RFC 2617);

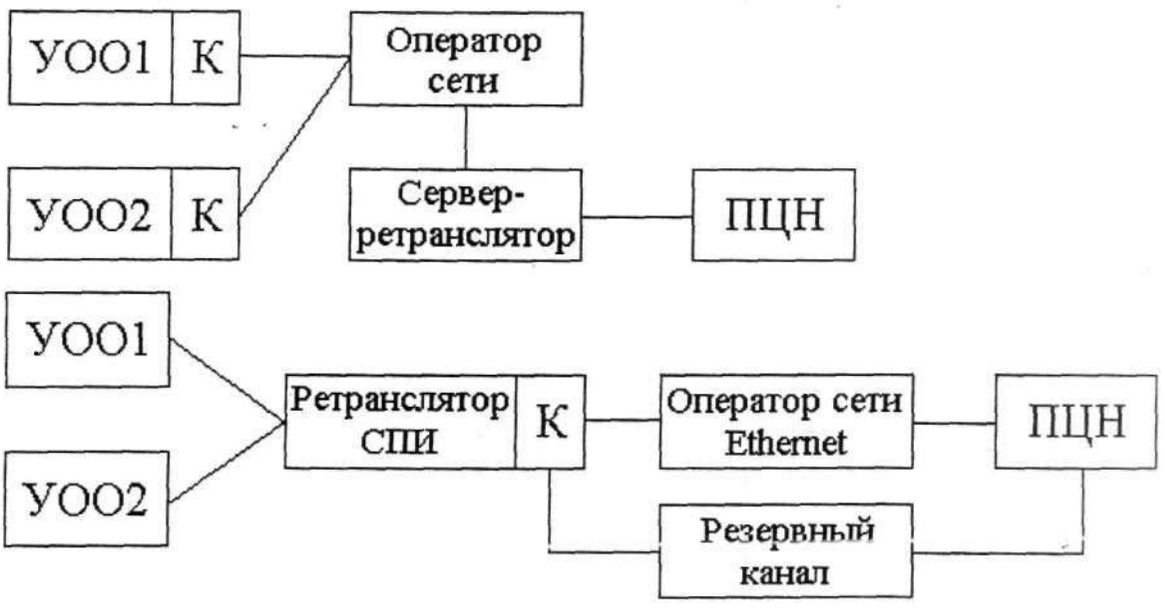
- устройство должно обеспечивать индикацию связи с сервером ПЦН и диагностику ошибок соединения. Устройство и программное обеспечение ПЦН не должны фиксировать неисправность при нарушениях связи

длительностью 30 секунд и менее, и должны фиксировать разрыв связи при ее отсутствии в течение 2 минут и более;

- устройство должно иметь альтернативный резервный канал передачи извещений (Ethernet с другим провайдером, GSM-канал, радиоканал, двухпроводной канал и т.п.), а также возможность автоматического перехода с основного канала на резервный и обратно при восстановлении основного;

- идентификация УОО программным обеспечением ПЦН должна исключать возможность подмены УОО.

8.2 Принцип построения СЦН по каналам Ethernet.



здесь: УОО - устройство оконечное объектовое,

К - коммуникатор,

ПЦН - пульт централизованного наблюдения,

Оператор - оператор Ethernet сети.

Таким образом, СЦН состоит из следующих основных узлов:

1.УОО(или ППК).

2. Коммуникатор.

3. Канал связи от коммуникатора до сервера, выполняющего роль ретранслятора.

4. Канал связи от сервера, выполняющего роль ретранслятора, до ПЦН.

5.АРМ ПЦН.

ППК должен иметь сменный модуль коммуникации с ПЦН в зависимости от среды передачи данных, в том числе для использования резервного канала связи.

Требования к коммуникатору:

- работа с помощью стандартных IP пакетов;
- наличие резервного канала связи.

Требования к каналу связи от ППК до сервера, выполняющего роль ретранслятора:

- защита от модификации передаваемых сообщений с помощью шифрования ключом не меньше 128 бит;
- защита от взлома ключа шифрования его динамической модификацией не реже чем раз в час;
- защита от подмены прибора при передаче однотипной информации (например, с помощью гаммирования) с повторяемостью не менее 3 года;
- защита от подмены прибора формированием и проверкой специальных запросов «свой-чужой»;
- защита от DoS атак (Denial of Service - отказ в обслуживании) со стороны ППК.

Требования к серверу; выполняющему роль ретранслятора:

- резервное питание должно быть рассчитано на автономную работу не менее 3 часов;
- два сетевых интерфейса для разделения работы «вниз» и «вверх»;
- периодический контроль канала связи до каждого ППК;
- защита от DoS атак (Denial of Service - отказ в обслуживании) со стороны Сервера - ретранслятора;
- наличие «белого» списка IP адресов для соединения с ПЦН.

Требования к каналу связи от сервера до ПЦН:

- шифрование всего TCP трафика ключом не менее 128 бит;

- защита от взлома ключа шифрования его динамической модификацией не реже чем раз в час;

- защита от подмены ретранслятора при передаче однотипной информации (например, с помощью гаммирования);

- защита от DoS атак (Denial of Service - отказ в обслуживании) со стороны Интернет.

9 Повышение надежности доставки тревожных сообщений.

В отличие от широко распространенных проводных систем передачи извещений, использующих переключаемые и занятые абонентские линии городских телефонных сетей, информаторные системы, а также системы с использованием GSM- и Ethernet-каналов связи не обеспечивают должного уровня надежности доставки тревожных сообщений.

Так, информаторные системы, не обеспечивают необходимого уровня контроля канала связи.

Системы с использованием GSM-каналов связи легко подавляются широко распространенными и доступными средствами. Кроме того, ограниченная пропускная способность каналов связи базовых станций приводит к резкому ухудшению работы системы при пиковых нагрузках.

Системы с использованием Ethernet-технологий, как показывает общемировая практика, слабо защищены от DoS атак как со стороны ППК, так и со стороны сервера (такие технологии взлома общеизвестны и также легкодоступны).

Учитывая изложенное, применение перечисленных каналов связи допустимо только в случае их дублирования, что позволит повысить надежности работы систем передачи извещений.

10 Требования к объектовому оборудованию.

Все многообразие объектового оборудования и задачи по его унификации можно условно разбить на 3 группы - оборудование для малых, средних и крупных объектов.

Общим требованием, предъявляемым к объектовому оборудованию любой группы, является:

- соответствие нормативным ГОСТам: 26342-84, 12997-84, 27990-88, 50775-95, 51089-97, МЭК 60065-2002, НПБ 57-97 и НПБ 75-98; РД 78.36.006-2005;

- обязательность применения имитостойких методов кодирования передаваемой на ретрансляторы и пульты информации;

- современный дизайн корпуса;

- удобство монтажа и простота в эксплуатационном обслуживании.

Устройства объектовые оконечные (УОО) должны обеспечивать выполнение следующих основных функций:

- прием извещений от извещателей и других устройств, включенных в шлейфы сигнализации;

- формирование извещений для передачи на ПЦН;

- контроль исправности шлейфов сигнализации и каналов связи;

- управление средствами отображения информации, а также по возможности световыми и звуковыми оповещателями или другими объектовыми устройствами;

- управление постановкой на охрану и снятием с охраны.

- для УОО со встроенным источником резервного питания рекомендуется иметь индикатор, отображающий оставшуюся емкость аккумуляторной батареи.

Информативность УОО должна быть установлена в ТУ на приборы конкретного вида в зависимости от возможности работы с конкретным видом СЦН.

Рекомендуемая информативность УОО - не менее десяти извещений.

Для УОО, работающих совместно с СЦН, информативность которых ниже информативности УОО, допускается передавать на ПЦН обобщенный сигнал тревоги. При этом УОО должно иметь возможность отображения информации на выносном табло для определения места нарушения на охраняемом объекте.

Для УОО, предназначенных для работы совместно с СЦН, имеющих обратный канал передачи данных, должно быть предусмотрено отображение на УОО извещения со стороны СЦН о взятии под охрану или снятии с охраны (квитирование взятия/снятия).

УОО должны выдавать извещения о проникновении при нарушении шлейфов охранной сигнализации длительностью от 500 мс (короткое замыкание, обрыв, срабатывание извещателя) и не должны выдавать указанных извещений при длительности 300 мс и менее.

УОО могут обеспечивать по цепям шлейфа или линии связи электропитание извещателей (например, двухпроводные пожарные и охранные извещатели). При этом в ТУ на УОО должны быть указаны допустимые значения напряжения и тока в ШС, при которых обеспечивается работа таких извещателей.

Для УОО со встроенным источником резервного электропитания (аккумуляторная батарея) должны дополнительно отображаться:

- наличие сетевого питания;
- наличие резервного питания;
- неисправность резервного питания (разряд или неисправность аккумуляторной батареи).

УОО должны обеспечивать управление взятием под охрану и снятием с охраны. Для этого могут использоваться как встроенные, так и внешние устройства управления взятием/снятием (в том числе - шифроустройства).

УОО должны быть защищены от несанкционированного снятия с охраны в режиме охраны. При разработке новых УОО исключить

применение ключей Touch Memory без использования секретных кодов, защищающих их от копирования.

Для УОО рекомендуется иметь возможность подключения выносных элементов контроля состояния ШС и цепи контроля наряда: световой индикатор и датчик контроля (электроконтактный или другого типа), формирующий соответствующее извещение (например, «Прибытие наряда»).

Допускается совмещать световой индикатор контроля наряда с внешним световым оповещателем.

Все объекты классифицируются в зависимости от количества шлейфов сигнализации.

10.1 Малые объекты.

Для оборудования малых объектов и мест хранения личного имущества граждан должны использоваться приборы и оконечные устройства с возможностью контроля до 4-х шлейфов сигнализации. Отличия могут заключаться в блоках сопряжения с выбранным типом СЦН.

Технически допустима разработка недорогих устройств этого класса под выбранный тип СЦН при условии соблюдения единых требований к тактике их работы, питанию, организации контроля за шлейфами сигнализации, возможности подключения тех или иных извещателей, оповещателей и т.д.

10.2 Средние объекты.

Средние объекты требуют для организации охраны от 5 до 20 шлейфов сигнализации и не имеют внутреннего автономного пульта охраны.

Такие объекты имеют, как правило, несколько помещений и оборудуются средствами не только охранной, но и пожарной сигнализации. Для них предусматривается возможность независимой постановки под охрану различных помещений и т.п.

Объектовое оборудование такого типа должно разрабатываться как под конкретный тип СЦН, так и быть универсальным с оснащением соответствующими коммуникаторами.

10.3 Крупные объекты.

Крупные объекты требуют для организации своей защиты более 20 шлейфов сигнализации. Такие объекты, как правило, имеют собственную службу безопасности и внутренний круглосуточный пост охраны. Для организации комплексной защиты таких объектов, необходима разработка семейства объектовых подсистем вплоть до интегрированных систем безопасности.

Являясь с одной стороны автономными, с другой стороны такие системы должны объединяться в единый комплекс централизованного наблюдения через коммуникаторы более высокого уровня.

К оборудованию для объектов среднего и крупного уровня можно отнести домовые (подъездные) концентраторы для охраны квартир в пределах одного дома (подъезда). Такие концентраторы могут иметь автономный пульт охраны (например, у консьержки), и предназначены для охраны слаботелефонизированных объектов и квартир граждан.

II Технические требования к системам мониторинга подвижных объектов, предназначенным для применения в подразделениях

1 Общие требования к системам мониторинга подвижных объектов.

1.1 Системы мониторинга подвижных объектов (далее Системы), используемые в настоящее время подразделениями вневедомственной охраны, предназначены для контроля местоположения и состояния автотранспортных средств (АВТС), оснащенных бортовым оборудованием одной из этих систем.

1.2 Системы должны состоять из следующих основных частей:

- оборудование диспетчерского центра контроля и управления (ДЦ);
- бортовое оборудование для организации охраны АВТС;

- бортовое оборудование для установки на служебном автотранспорте подразделений вневедомственной охраны (автомобилях групп задержания).

1.3 Системы должны обеспечивать возможность построения единой системы мониторинга с тремя уровнями иерархии:

- федеральный (Межрегиональный координационный центр МВД России);

- региональный (республиканские, краевые, областные управления вневедомственной охраны);

- территориальный (подразделения вневедомственной охраны районного звена).

2 Технические требования к системам мониторинга подвижных объектов.

2.1 Системы должны обеспечивать поддержку единых информационных протоколов обмена данными между ДЦ, независимо от типа системы и предприятия-изготовителя. Способ распределения условных номеров комплектов бортового оборудования между Системами должен обеспечивать уникальность присвоенного номера каждому АВТС.

2.2 Системы должны осуществлять автоматизированный обмен информацией между ДЦ с целью обновления баз данных по АВТС в соответствии с уровнями иерархии. Изменения должны вступать в силу во всех ДЦ на всех уровнях иерархии за время'не более 30 минут после внесения изменения.

2.3 При перемещении АВТС, с установленным бортовым оборудованием одной из систем, между зонами обслуживания, оборудование ДЦ унифицированных систем этих зон должно обеспечивать автоматизированную передачу процесса обслуживания данного АВТС и установление информационного обмена без потери контроля за АВТС.

2.4 Тревожные или служебные извещения, формируемые бортовым оборудованием охраняемых АВТС, должны поступать и фиксироваться в ДЦ

одной из Систем, обеспечивающей наблюдение на данной территории. Отображение поступившей информации должно производиться одновременно с отображением местоположения АВТС на электронной карте местности.

2.5 Системы должны обеспечивать возможность автоматизированной трансляции информации, поступившей от АВТС и данных о его местонахождении, в ДЦ других систем в соответствии с принятой иерархией.

2.6 Системы должны обеспечивать определение, передачу и отображение информации о местоположении служебного автотранспорта подразделений вневедомственной охраны, с установленным бортовым оборудованием, а также доставку и отображение на бортовом оборудовании служебного автотранспорта необходимой информации, передаваемой из диспетчерского ДЦ при условии, если бортовое оборудование поддерживает необходимую функциональность.

2.7 Системы должны предусматривать возможность защиты от внешнего подавления канала связи между бортовым оборудованием и оборудованием ДЦ.

2.8 Системы должны предусматривать возможность защиты от внешнего вмешательства (криптостойкость передаваемой информации и имитостойкость оборудования) в канал связи между бортовым оборудованием и оборудованием ДЦ, а также между диспетчерскими ДЦ различных уровней.

2.9 Картографическое обеспечение систем должно быть совместимым по форматам используемых электронных карт, отображать электронные план-схемы городов, областей, регионов.

2.10 Системы должны обеспечивать возможность использования навигационного оборудования систем «ГЛОНАСС» или «ГЛОНАСС/GPS».

2.11 Системы должны обеспечивать круглосуточное бесперебойное обслуживание следующего количества абонентов:

для ДЦ территориального уровня:

- по числу охраняемых АВТС - не менее 10 000;

- по числу патрульных автомобилей - не менее 255;

для ДЦ регионального уровня:

- по числу охраняемых АВТС - не менее 65 000;

- по числу патрульных автомобилей - не менее 1 000;

для ДЦ федерального уровня:

- по числу охраняемых АВТС - не менее 10 000 000;

- по числу патрульных автомобилей - не менее 100 000.

2.12 Системы должны обеспечивать идентификацию информации, полученной от каждого из комплектов бортового оборудования с отображением в ДЦ следующих параметров:

для охраняемых АВТС:

- идентификационный номер в системе;

- государственный регистрационный номер;

- идентификационный номер автомобиля (VIN);

- торговую марку;

- тип модели;

- цвет кузова;

- данные владельца автомобиля (Ф.И.О., домашний адрес, контактные телефоны и т.п.);

для служебного автотранспорта:

- идентификационный номер в системе;

- принадлежность к подразделению и условный номер;

- государственный регистрационный номер;

- позывные радиообмена.

2.13 Системы должны обеспечивать формирование бортовым оборудованием охраняемых АВТС и доставку в ДЦ следующих извещений:

- «взят под охрану» - система автомобильной сигнализации включена;

- «снят с охраны» - система автомобильной сигнализации отключена;

- «снят с охраны под принуждением» - система автомобильной сигнализации вынужденно отключена владельцем, при условии, если сигнализация поддерживает эту функцию;

- «тревога-предупреждение» - система автомобильной сигнализации сработала, но вскрытия корпуса АВТС не было при условии, если сигнализация поддерживает эту функцию;

- «тревога-вторжение» - система автомобильной сигнализации сработала и вскрыт корпус АВТС при условии, если сигнализация поддерживает эту функцию;

- «тревога-нападение» - сигнал тревоги подан владельцем АВТС;

- «неисправность» - техническая неисправность бортового оборудования;

- «переход на резервное электропитание» - переключение бортового оборудования на электропитание от резервного источника;

- «критическое состояние резервного электропитания» - исчерпан ресурс источника резервного электропитания бортового оборудования.

2.14 Системы должны обеспечивать формирование бортовым оборудованием патрульных автомобилей и доставку в диспетчерский ДЦ следующих формализованных извещений:

- «приступил к исполнению» - подтверждение полученного указания;

- «прибыл на место» - подтверждение прибытия в указанное место;

- «свободен» - подтверждение о выполнении ранее полученного указания;

- «занят» - предупреждение о выполнении ранее полученного указания;

- «выход из зоны наблюдения» - при выходе автомобиля за пределы заданной зоны;

- «тревога» - сигнал тревоги подан членом экипажа патрульного автомобиля;

- «несанкционированный демонтаж» - вскрытие корпусов бортового оборудования или другие несанкционированные действия при попытках вывести бортовое оборудование из строя;

- «переход на резервное электропитание» - переключение бортового оборудования на электропитание от резервного источника;

- «критическое состояние резервного электропитания» - исчерпан ресурс источника резервного электропитания бортового оборудования.

2.15 Системы, при наличии устойчивого канала связи, должны обеспечивать доставку информации от бортового оборудования в ДЦ, обеспечивающий текущий контроль АВТС, за время, не более 10 сек.

Системы, при наличии устойчивого канала связи, должны обеспечивать периодичность получения информации о местонахождении и текущем состоянии (при нахождении в зоне действия каналов связи):

- для охраняемых АВТС (при возникновении тревожной ситуации) - не менее чем 1 раз за 10 сек.;

- для патрульных автомобилей (при несении дежурства) - не менее чем 1 раз за 30 секунд.

2.16 Системы, при наличии устойчивого канала связи, должны обеспечивать периодичность проверки работоспособное!и бортового оборудования, формирование и передачу информации о текущем состоянии:

- для охраняемых АВТС, в режиме «взят под охрану» - в интервале от 2 минут до 12 часов, в режиме «снят с охраны» - в интервале от 2 до 24 часов;

- для патрульных автомобилей - не менее чем 1 раз за 30 секунд.

2.17 Требования к бортовому оборудованию Систем.

2.17.1 Бортовое оборудование охраняемых АВТС должно обеспечивать выполнение следующих основных функций:

- определение текущего местоположения АВТС или формирование сигналов для его определения;

- контроль состояния подключенных шлейфов сигнализации с извещателями и дополнительного оборудования;

- формирование и передачу в ДЦ информации о текущем состоянии в соответствии с параметрами выбранного режима работы;

- прием и выполнение команд, поступающих из ДЦ;

- диагностирование работоспособности собственного и подключенного оборудования, с формированием и передачей соответствующей информации вДЦ;

- контроль состояния электропитания, переключение на резервный источник электропитания и обратно, с формированием и передачей соответствующей информации в ДЦ;

2.17.2 Бортовое оборудование охраняемых АВТС должно обеспечивать следующие режимы работы:

- «взят под охрану» - осуществляется контроль всех шлейфов сигнализации, формирование соответствующих извещений, прием и выполнение команд из ДЦ;

- «снят с охраны» - осуществляется контроль шлейфов сигнализации с подключенной тревожной кнопкой и формирование соответствующих извещений;

2.17.3 Бортовое оборудование охраняемых АВТС должно обеспечивать возможность подключения не менее четырех шлейфов сигнализации и двух исполнительных устройств, для выполнения команд из ДЦ.

2.17.4 Бортовое оборудование охраняемых АВТС должно обеспечивать возможность подключения элементов управления, обеспечивающих идентификацию владельца автомобиля. При наличии нескольких владельцев должны обеспечиваться идентификация каждого из них, с передачей уточняющей информации в ДЦ.

2.17.5 Бортовое оборудование патрульных автомобилей должно обеспечивать выполнение следующих основных функций:

- определение текущего местоположения АВТС или формирование сигналов для его определения;

- контроль состояния подключенного шлейфа сигнализации (тревожная кнопка) и дополнительного оборудования;

- диагностирование работоспособности собственного и подключенного оборудования, с формированием и передачей соответствующей информации в ДЦ;

- контроль состояния электропитания, переключение на резервный источник электропитания и обратно, с формированием и передачей соответствующей информации в ДЦ.

2.17.6 Бортовое оборудование патрульных автомобилей в специальном варианте исполнения должно обеспечивать выполнение следующих дополнительных функций:

- формирование и передачу в ДЦ текстовых фрагментов, а так же формализованных извещений;

- прием, обработку и отображение текстовых фрагментов и команд, поступающих из ДЦ;

- передачу фото- и видеоизображений с места нахождения на ДЦ;

удаленный доступ к ннформацйилпым базам данных.

2.17.7 Бортовое оборудование Систем должно иметь защиту от вскрытия. При вскрытии корпуса должно выдаваться извещение о несанкционированном вскрытии или о тревоге.

2.17.8 Бортовое оборудование Систем должно обеспечивать возможность сохранения в энергонезависимой памяти до 1000 последовательно зарегистрированных событий для охраняемых АВТС и до 2000 последовательно зарегистрированных событий для патрульных автомобилей, отражающих его состояние за последние 12 часов.

2.17.9 Бортовое оборудование Систем должно обеспечивать соответствие следующим требованиям: ГОСТ Р 50789, ГОСТ 14254 (IP 51), ГОСТ 15150, ГОСТ 12.2.007.0, ГОСТ РМЭК 60065, ГОСТ 12.1.004.

2.18 Требования к оборудованию и программному обеспечению (ПО) диспетчерских центров контроля и управления Систем.

2.18.1 Оборудование и ПО ДЦ в непрерывном круглосуточном режиме работы должны обеспечивать выполнение следующих основных функций:

- прием, обработку и отображение информации о местоположении и текущем состоянии всех автомобилей (при одновременном текущем отображении на экране не менее 30 АВТС), оснащенных комплектами бортового оборудования и входящими в состав системы;

- контроль работоспособности собственного оборудования, а так же всех комплектов бортового оборудования, входящих в состав системы;

- постоянное накопление и обработку поступающей информации, привлечение внимания оператора при возникновении ситуаций, требующих его действий и формирование при необходимости очереди таких событий;

- документирование, систематизацию и хранение поступающей информации.

2.18.2 Оборудование и ПО ДЦ (в специальном варианте исполнения) должны обеспечивать выполнение следующих дополнительных функций:

- прием, обработку и отображение фото- видеоинформации с

обеспечивающего передачу фото- и видеоизображения;

- прием запросов с автомобилей, оборудованных комплектами бортового оборудования, обеспечивающего удаленный доступ к информационным базам данных, их обработку и отправку ответов.

2.18.3 Оборудование и ПО ДЦ должны обеспечивать возможность подключения ДЦ других Систем, с выделением потоков информации и приоритетов управления, относящихся к этому центру. Каналы связи между центрами должны иметь защиту от несанкционированного доступа.

2.18.4 Оборудование и ПО ДЦ должны обеспечивать отображение местоположения каждого автомобиля, оснащенного комплектом бортового оборудования, входящим в состав системы, или траектории его движения на

фоне карты местности, в виде, удобном для операторов.

2.18.5 Оборудование и ПО ДЦ должны обеспечивать разделение уровней доступа операторов и обслуживающего персонала к управлению и получению информации, в соответствии с выполняемыми служебными обязанностями.

2.18.6 Оборудование и ПО ДЦ должны обеспечивать возможность своевременной настройки параметров получения, отображения и обработки информации в соответствии с условиями эксплуатации. Внесение изменений в настройки оборудования, изменение программного обеспечения электронных карт местности, просмотр архивов событий и запуск других подпрограмм, входящих в комплект поставки ДЦ, не должны влиять на работоспособность ПО, обеспечивающего прием и накопление поступающей информации.

2.18.7 Оборудование и ПО ДЦ должны обеспечивать возможность корректировки и настройки геоинформационных баз данных (карты или плана местности).

2.18.8 ПО ДЦ должно обеспечивать отображение электронных план-схем с величиной временной задержки при изменении масштабов и сдвигов не более 3-х секунд. Электронные план-схемы должны выводиться на экран операторов в зависимости от текущей ситуации в автоматическом режиме. При этом картографическое обеспечение должны поддерживать работу с базой данных электронных план-схем не менее 90 регионов и входящих в них городов.

2.18.9 Оборудование и ПО ДЦ должны обеспечивать возможность накопления информации в архив со сроком хранения не менее 6 месяцев, поиска информации, сохраненной в архиве, по произвольному запросу и отображение полученной информации на фоне карты местности и в виде отчетов.

2.18.10 Оборудование и ПО ДЦ должны обеспечивать резервное копирование и восстановление информации и программного обеспечения,

регистрацию и обработку ситуаций по выходу оборудования из строя, сбор и обработку статистической информации, удаление неактуальной информации из архива.

ПРИЛОЖЕНИЕ 1

1 Порядок проведения экспертизы СЦН и систем мониторинга подвижных объектов, применяемых в подразделениях вневедомственной охраны.

1.1 Техническая экспертиза СЦН и систем мониторинга подвижных объектов проводится в целях:

- проверки соответствия единым техническим требованиям;
- анализа тактико-технических характеристик;
- проверки функциональных возможностей;
- оценки стоимостных показателей;
- сравнения с аналогами, применяемыми в подразделениях вне ведомственной охраны.

1.2 Экспертизе повергаются серийно выпускаемые СЦН и системы мониторинга подвижных объектов, разработанные в инициативном порядке (без технического задания, утвержденного ЦОРДВО МВД России) и освоенные в серийном производстве предприятиями (далее Заявителями), предлагаемые для применения в службе вневедомственной охраны, и имеющие:

- сертификат соответствия в системе сертификации ГОСТ Р Ростехрегулирования России, выданный уполномоченным органом по сертификации (для изделий охранной сигнализации);
- сертификат пожарной безопасности системы сертификации в области пожарной безопасности, выданный уполномоченным органом по сертификации (для изделий охранно-пожарной сигнализации);
- сертификат соответствия или декларация соответствия требованиям Федерального агентства связи (для СЦН, работающих по линиям АТС и/или имеющих в своем составе радиоканальные устройства);
- разрешительные документы на использование рабочих частот (для СЦН с использованием радиоканальных устройств);

- другие сертификаты и лицензии, обусловленные их функциональными особенностями.

1.3 Для принятия решения о целесообразности проведения экспертизы Заявитель должен направить письмо в ЦОРДВО МВД России, указав в нем наименование и область применения СЦН или системы мониторинга подвижных объектов, ее основные особенности, краткие технические характеристики и стоимостные показатели с приложением копий сертификатов.

1.4 Экспертиза проводится ФГУ НИЦ «Охрана» МВД России (Исполнитель) на платной основе по письменному обращению ЦОРДВО МВД России. Оплата работ по проведению экспертизы проводится Заявителем на основании договора, заключаемого между Исполнителем и Заявителем.

1.5 Для проведения экспертизы Заявитель, должен представить исполнителю образец системы с объектовым оборудованием в количестве не менее трех образцов имеющихся типов (допускается для сложных изделий один образец) и документацию в следующем составе:

- пояснительная записка, содержащая информацию об основных тактико-технических ха"акте"истиках системы;

- технические условия на систему и на ее составные части;

- эксплуатационную- документацию (руководство по эксплуатации, паспорт, технические описания, этикетки и т.д.)'на изделие и его составные части;

- программное обеспечение (при работе изделия с компьютером);

- руководство по работе с программным обеспечением;

- отзывы эксплуатирующих организаций (при их наличии).

При необходимости Заявитель предоставляет справку-объективку о своем предприятии по установленной форме.

1.6 Экспертиза начинается после оплаты работ по договору.

1.7 Срок проведения экспертизы должен устанавливаться в договоре и

не должен превышать 45 рабочих дней, его изменение возможно только по согласованию с ЦОРДВО МВД России.

1.8 Экспертиза должна включать в себя следующие работы:

- разработка программы и методики экспертизы;

- изучение конструкторской и эксплуатационной документации на предмет соответствия требованиям ГОСТ, достаточности заложенных требований и полноты проверок для серийного производства;

- анализ конструктивных и схемотехнических особенностей, качества и технологии изготовления изделия. Оценка уровня применяемой элементной базы;

- проверка тактико-технических характеристик и функциональных возможностей с проведением лабораторных испытаний, а при необходимости дополнительных испытаний с привлечением сторонних организаций. Сравнение технико-экономических показателей с аналогами, применяемыми в подразделениях вневедомственной охраны, в форме таблицы;

- проверка режимов работы с превышением параметров (на 10%), указанных в технических условиях, при воздействии дестабилизирующих факторов (климатических, механических, электропитания и т.п.);

- оформление результатов экспертизы.

1.9 Программа и методика проведения экспертизы изделия должна разрабатываться с использованием соответствующих методик стандартов и других нормативных документов, ранее разработанных методик испытаний, опыта эксплуатации аналогов подразделениями вневедомственной охраны. Программу и методику утверждает руководитель ФГУ НИЦ «Охрана» МВД России.

1.10. Калькуляция, договор и соглашение о договорной цене.

На основании программы и методики проведения технической экспертизы СЦН и систем мониторинга подвижных объектов, разрабатывается сметная калькуляция ее стоимости, включающая затраты на проведение работ по п. 1.8, а также затраты на материалы, амортизацию

оборудования и оплату работы смежных организаций.

На основании калькуляции составляется договор и протокол соглашения о договорной цене на проведение работ по экспертизе. В договоре предусматриваются, в том числе:

- принципы оплаты работ по договору;
- сроки проведения экспертизы;
- возможность привлечения к проведению сторонних организаций;
- другие сведения, необходимые для проведения экспертизы.

1.11 Проведение экспертизы:

- работы по проведению экспертизы проводятся по утвержденной Программе и методике с соблюдением Правил и норм техники безопасности.
- результаты технической экспертизы оформляются в виде заключения и отчета о проведенной экспертизе. Экспертное заключение должно быть направлено в ЦОРДВО МВД России, а Заявителю - отчет о проведенной экспертизе не позднее 10 суток после окончания работ.

На основании экспертного заключения принимается решение о целесообразности проведения эксплуатационных испытаний заявленного изделия в подразделениях вневедомственной охраны.

При необходимости устранения выявленных замечаний, экспертное заключение Заявителю направляет ЦОРДВО МВД России.

2 Порядок сертификации СЦН и систем мониторинга подвижных объектов, предназначенных для применения подразделениями вневедомственной охраны.

Сертификация проводится в ФГУ ЦСА ОПС МВД России и (или) в другом уполномоченном органе по сертификации в соответствии действующим законодательством Российской Федерации.

Изделия, предназначенные для применения в подразделениях вневедомственной охраны должны иметь сертификат соответствия в системе сертификации ГОСТ Р Ростехрегулирования России, выданный

уполномоченным органом по сертификации (для изделий охранной сигнализации) и другие необходимые сертификаты в соответствии с п. 1.2.

3 Порядок организации и проведения эксплуатационных испытаний СЦН и систем мониторинга подвижных объектов.

Эксплуатационные испытания СЦН и систем мониторинга подвижных объектов проводятся с целью проверки работоспособности и соответствия основным техническим требованиям технических условий СЦН в реальных условиях эксплуатации с развертыванием на ПЦО подразделений вневедомственной охраны и установкой оконечных устройств на конкретных объектах.

3.1 Место и время испытаний.

Испытания СЦН и систем мониторинга подвижных объектов проводятся на объектах, охраняемых подразделениями вневедомственной охраны и определенных ЦОРДВО МВД России. Продолжительность испытаний не менее 1000 часов со дня ввода в эксплуатацию.

3.2 Программа и методика испытаний.

Испытания изделий проводятся по разработанной ФГУ НИЦ «Охрана» МВД России и утвержденной ЦОРДВО МВД России программе и методике, которая должна включать:

- краткую характеристику систем с учетом заключения специалистов ФГУ НИЦ «Охрана» МВД России;
- цель испытаний;
- условия и последовательность проведения испытаний;
- виды и методы проверок.

Установка и техническое обслуживание СЦН возлагается на территориальное подразделение вневедомственной охраны. Контроль за ходом эксплуатационных испытаний осуществляется специалистами ЦОРДВО МВД России и регионального УВО.

Во время проведения испытаний ведется журнал, находящийся на ПЦО ОВО. Журнал должен иметь следующие разделы:

- информацию о ложных срабатываниях и их причинах: (дата, время, номер ложного срабатывания, причина срабатывания или предполагаемая причина);

- дефекты, выявленные в ходе эксплуатационных испытаний;

- подстройка и регулировка, проведенные в процессе эксплуатации: (дата, причины, величина параметра до и после);

- результаты контрольных проверок работоспособности: (дата, вид проверки, результаты).

Записи в журнале подтверждаются подписями лиц, осуществляющими эксплуатационное обслуживание СЦН или систем мониторинга подвижных объектов.

Ввод СЦН и систем мониторинга подвижных объектов в эксплуатацию оформляется актом, который подписывается ответственными представителями УВО (ОВО) при МВД, ГУВД, УВД по субъектам Российской Федерации.

3.3. Результаты испытаний оформляются протоколом, в котором даётся заключение с соответствий СЦН или систем мониторинга подвижных объектов заявленным тактико-техническим требованиям, а также вносятся сведения об удобстве монтажа, ремонта, эксплуатационного обслуживания и предложения по улучшению конструктивных и эксплуатационных параметров. В протоколе отмечаются также возникшие во время испытаний отказы и нарушения работоспособности СЦН или систем мониторинга подвижных объектов с указанием причин их вызвавших. Протокол подписывается лицами, проводившими испытания и осуществлявшими за ними контроль, и утверждается руководителем УВО (ОВО) при МВД, ГУВД, УВД по субъектам Российской Федерации.

3.4. Протокол испытаний в срок не позднее 10 дней со дня окончания испытаний направляется в ЦОРДВО МВД России.

ПРИЛОЖЕНИЕ 2

Термины, применяемые в настоящем документе и их определения

Термин	Определение
СЦН	Система централизованного наблюдения
РСПИ	Радиоканальная система передачи извещений
ПИК	Прибор приемно-контрольный
ПЦО	Пункт централизованной охраны
ПЦН	Пульт централизованного наблюдения
ГТС	Городская телефонная сеть
КСА	Комплекс средств автоматизации
АРМ	Автоматизированное рабочее место
БД	База данных
ЛВС	Локально вычислительная сеть
УПО	Устройстве пультовое оконечное
УОО	Устройство объектовое оконечное
ШС	Шлейф сигнализации
ДЦ	Диспетчерский центр контроля и управления