УТВЕРЖДАЮ
Заместитель начальника
ГУВО МВД России
полковник полиции

_____ А.В. Грищенко

«_____»_____2012 г.

Единые технические требования к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны.

СОГЛАСОВАНО
Начальник
ФКУ НИЦ «Охрана» МВД России
полковник полиции

_____А.Г. Зайцев
«_____»_____2012 г.

Москва 2012 год

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

Технические требования к системам централизованного наблюдения.

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

– обеспечивать прирост и надежную охрану объектов различных форм собственности, квартир и других мест хранения имущества граждан, расширяя технические возможности службы по организации централизованной охраны;

– исключить возможность использования недоброкачественной аппаратуры охранной сигнализации;

– сократить затраты на охрану (на эксплуатацию, ремонт и обслуживание технических средств охраны, сокращение единовременных затрат на их приобретение и т.п.);

– осуществлять экономически обоснованное укрупнение пунктов централизованной охраны (ПЦО), что требует качественно нового подхода к построению систем централизованного наблюдения.

1 Общие требования к СЦН

1.1 Современные средства СЦН должны:

– удовлетворять нормам пожарной безопасности для данной категории изделий;

---

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

– обеспечивать передачу извещений с коэффициентом необнаруженных ошибок не более 10^{-4} (по ГОСТ Р 52435-2005);

– обеспечивать совместимость и сохранять преемственность с используемой на ПЦО аппаратурой;

– использовать последние достижения в развитии вычислительной техники и новых компьютерных технологий и иметь современный дизайн;

– обладать высокой информативностью (не менее 10 извещений), 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 методы криптозащиты не хуже класса S4 по ГОСТ Р 52435-2005.

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

1.4 СЦН должны работать по принципиально несовместимым каналам связи (проводные линии АТС, УКВ-радиоканал, каналы сотовой связи GSM, а также выделенные проводные или оптико-волоконные линии связи, локально-вычислительные сети), обеспечивая интеграцию на едином пультовом оборудовании всех своих подсистем.

1.5 Протокол обмена данными между всеми компонентами СЦН должен иметь:

- достаточную величину адресного пространства для обеспечения совместной работы с объектовыми подсистемами большой емкости с возможностью передачи на ПЦН расширенной информации (вплоть до шлейфа сигнализации) по одному каналу передачи данных;

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

1.6 СЦН должны обеспечивать высокие требования к надежности функционирования своих узлов и составных частей, а также каналов связи с обеспечением, при необходимости, их резервирования. Гарантийный срок службы СЦН должен составлять не менее пяти лет, срок эксплуатации – не менее 8 лет.

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

1.8 СЦН должны 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.

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

1.10 СЦН должны обеспечивать время доставки тревожного извещения на ПЦН не более 15 с при загрузке системы не менее 80%. Допускается оценка данного параметра экспертным методом.

1.11 СЦН должны соответствовать общетехническим требованиям к аппаратуре приборостроения, таким как надежность, устойчивость к

климатическим и механическим воздействиям, вибрации, электромагнитной совместимости, требованиям к безопасности.

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

2.1 СЦН должны иметь единый протокол обмена данными между всеми его компонентами, обеспечивающий:

- достаточную глубину вложения адресации к отдельным устройствам (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.

- 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;

- возможность интеграции на уровне ретрансляционного оборудования подсистем, работающих по занятым и переключаемым на период охраны линиям связи АТС.

2.2 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/с охраны;

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

– 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;

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

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

2.3 Системы, работающие по переключаемым на период охраны телефонным линиям, должны:

2.3.1 Обеспечивать работоспособность абонентских устройств (телефонных аппаратов, автоответчиков, телефонных аппаратов с автоматическим определителем номера, факсов и др.) с качеством по ГОСТ 7153-85 «Аппараты телефонные общего применения»;

2.3.2 Удовлетворять «Техническим требованиям на системы специальной сигнализации, использующие телефонные линии», утвержденным оперативно-техническим управлением МООП РСФСР 25 июня 1964 г. и техническим управлением Министерства связи СССР 2 июня 1964 г. и ОСТ 45.36 «Линии кабельные, воздушные и смешанные городских телефонных сетей. Нормы электрические эксплуатационные»;

2.3.3 Обеспечивать помехозащищенность от кратковременных неисправностей линии связи на участке «объект - ретранслятор» на время не менее 0,5 с;

2.3.4 Обеспечивать переключение абонентской линии из режима «Охрана» в режим АТС при:

- понижении напряжения питания АТС ниже 44 В;

- при коротком замыкании или обрыве абонентской линии на время более 0,5 с или отсутствии кодовой посылки от объектового устройства;

- поступлении команды «Снять» по данному направлению.

2.3.5 Обеспечивать фиксацию нарушения ШС и непрерывную передачу на ретранслятор тревожного сообщения вне зависимости от последующего, в том числе и преднамеренного, восстановления ШС.

2.4 Системы, работающие по переключаемым на период охраны телефонным линиям, не должны использовать оконечное оборудование с контролем по постоянному току;

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

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 ретрансляционного оборудования и устройств оконечных объектовых (УОО) с обязательным формированием тревожного извещения в случае санкционированного снятия объекта с охраны в непредусмотренное

«графиком охраны» время, визуального интерфейса состояния ретрансляторов (пультов), наличие статистических и сервисных функций;

– АРМ дежурного офицера: функции контроля действий операторов, групп задержания, визуального интерфейса состояния ретрансляторов (пультов), наличие статистических и сервисных функций, 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, в том числе, диагностической 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.

3.2 Для возможности наращивания комплекса по мере появления новых перспективных систем охраны необходимо предусмотреть возможность подключения независимого компактного программного модуля (драйвера или сервиса). Кроме этого не должно быть ограничение по количеству рабочих мест дежурного оператора.

3.3 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, применение методов диспетчеризации ресурсов КСА ПЦО, оптимального их перераспределения между АРМами и т.п.

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

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

В комплексе должны быть предусмотрены средства защиты от несанкционированного доступа, резервирования, диагностики и восстановления.

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

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

3.4 Должно быть предусмотрено протоколирование событий с возможностью формирования соответствующих выборок и информации о дате и времени:

– тревожных сообщений;

– сообщений об охране (поставленных 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.

3.5 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.

3.6 Резервное копирование.

В целях документирования работы СЦН должно быть предусмотрено ведение архива информационной базы данных и протоколов событий. Период хранения протокола событий – не менее одного года.

4. 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.

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

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

4.3 Радиоканальное оборудование РСПИ должно обеспечивать величину частотного разноса соседних каналов 25 КГц (с 01.01.2014 - 12,5 КГц).

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

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

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

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

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

4.9 Рекомендуется для РСПИ реализовать на базе АРМ инженера ПЦО возможность технического диагностирования наличия сигнала от каждого из устройств системы, значение коэффициента стоячей волны (КСВ), уровней сигнала и помехи в канале с отображением этих параметров на мониторе ПЭВМ.

4.10 Оборудование РСПИ должно обеспечивать возможность передачи на ПЦН не менее 17 видов извещений, среди которых должны быть следующие:

– «взят под охрану с кодом ХО» – контролируются все подключенные шлейфы сигнализации (ШС);

– «снят с охраны с кодом ХО» – объект снят с охраны, контролируется пожарный и тревожный ШС;

Где код ХО служит для идентификации ФИО хозоргана, осуществляющего взятие/снятие.

– «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;

– «снят под принуждением» – снятие объекта с охраны с одновременным формированием и передачей на ПЦН тревожного извещения;

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

– «резерв в авар. сост.» – разряд резервного аккумулятора.

5. СЦН с использованием сети GSM

СЦН с использованием каналов мобильной сотовой связи (GSM, CDMA-2000, UMTS/WCDMA, CDMA2000/IMT-MC, LTE и пр.) применяются для организации защиты нетелефонизированных объектов.

5.1 Требования к системным параметрам СЦН с использованием сети GSM:

– системы должны обеспечивать возможность передачи извещений по основным каналам связи с использованием технологий VPN GPRS или CSD;

– системы должны обеспечивать возможность запроса текущего состояния и удаленного управления объектовым оборудованием;

– устройства системы должны иметь альтернативный резервный канал передачи извещений (радиоканал, телефонная сеть общего пользования, каналы с использованием сети Ethernet и т.п.).

5.2 Требования к устройствам оконечным объектовым (УОО):

– УОО должно обеспечивать возможность работы не менее, чем с двумя SIM-картами.

– 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 обеспечивать контроль регистрации связи с ПЦН и передавать по резервному каналу соответствующее извещение при отсутствии связи в течение 120 с и более. Кратковременные (менее 120 с) сбои связи не должны вызывать тревожных извещений;

– УОО должно обеспечивать передачу сообщений, предназначенных для контроля канала связи. Период передачи контрольных сообщений зависит от вида используемого канала. Период передачи должен программироваться при настройке УОО;

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

5.3 Время доставки тревожных извещений от объектового оборудования до ПЦН и время доставки сигналов управления от ПЦН до объектового оборудования по основным каналам связи не должно превышать 15 секунд.

5.4 Время доставки извещений от объектового оборудования до ПЦН по резервным каналам связи не должно превышать 120 секунд.

5.5 ПЦН должен обеспечивать техническое диагностирование наличия сигнала от каждого объектового устройства, уровня сигнала в канале с отображением этих параметров на АРМ инженера, а также по возможности количества базовых станций, доступных для обслуживания.

6. СЦН с использованием сети Ethernet в том числе с использованием PON-технологий

СЦН, использующие в качестве каналов связи сети Ethernet, могут применяться для организации охраны объектов, квартир и мест хранения имущества граждан с обязательным использованием резервного канала связи.

6.1 Требования к системным параметрам СЦН с использованием сети Ethernet:

– сопряжение устройства с сетью передачи данных (физический уровень) должно соответствовать спецификации IEEE 802.3 10BaseT/100BaseT/1000BaseT;

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

– в технических условиях на объектовое оборудование должна быть предусмотрена полноценная проверка работоспособности по сети Ethernet, например, подключением к компьютеру или какой-либо контрольной аппаратуре;

– связь между АРМ и объектовым оборудованием должна быть двухсторонней, то есть АРМ должен обнаруживать потерю связи или неисправность объектового оборудования.

6.2 Объектовое оборудование должно:

– иметь альтернативный резервный канал передачи извещений на ПЦН (GSM-канал, радиоканал и т.п.), а также возможность автоматического перехода с основного канала на резервный и обратно при восстановлении основного;

– отображать полную потерю связи с АРМ;

– 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;

– иметь неизменяемый пользователем MAC-адрес из диапазона, выделенного IEEE Organization предприятию-изготовителю. Устройство должно иметь возможность использования как фиксированного, так и динамического IP адреса;

– 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);

– 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 120 секунд и более.

6.3 СЦН должна обеспечивать идентификацию УОО программным обеспечением ПЦН с целью исключения возможности подмены УОО.

6.4 Устройства коммуникации, непосредственно подключенные к УОО на объекте (свичи, маршрутизаторы, а для gpon - устройство ont и т. д.) должны быть обеспечены резервным электропитанием, продолжительность работы от которого должна быть сопоставима со временем работы самого УОО на резервном электропитании.

6.5 Общие требования к организации связи между УОО и ПЦН:

– работа с помощью стандартных IP пакетов;

– наличие резервного канала связи (как со стороны прибора, так и со стороны ПЦН);

– подключение ПЦН к сети Ethernet должно быть осуществлено через маршрутизатор, выполняющий функции межсетевого экрана (firewall);

– подключение ПЦН к сети Ethernet должно быть осуществлено через двух или более провайдеров.

6.6 Требования к каналу связи от объектового оборудования 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 объектового оборудования.

6.7 Требования к серверу, выполняющему роль ретранслятора:

– резервное питание должно быть рассчитано на автономную работу не менее 3 часов;

– возможно применение двух сетевых интерфейсов для разделения работы «вниз» и «вверх»;

– периодический контроль канала связи до каждого объектового оборудования;

– защита от DoS атак (Denial of Service – отказ в обслуживании) со стороны Сервера – ретранслятора;

– наличие «белого» списка идентификаторов приборов, зарегистрированных на ПЦН.

6.8 Требования к каналу связи от сервера до ПЦН, осуществленной по локальной сети 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 Ethernet.

7. 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.

7.1 Общими требованиями, предъявляемыми к объектовому оборудованию любой группы, являются:

– соответствие нормативным документам: ГОСТ 52435-2005, ГОСТ Р 52436-2005, ГОСТ Р 50775-95, ГОСТ Р 50009-2000, ГОСТ Р МЭК 60065-2009, ГОСТ 26342-84, ГОСТ 27990, РД 78.36.006-2005, НПБ 57-97 и НПБ 75-98;

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

– современный и эргономичный дизайн корпуса;

– удобство монтажа и простота в эксплуатационном обслуживании.

7.2 УОО должны обеспечивать выполнение следующих основных функций:

– прием и отображение (световое, звуковое) извещений от охранных извещателей (о нормальном состоянии, о тревоге, о маскировании, о неисправности, о снижении напряжения электропитания, о вскрытии корпуса, о снятии с поверхности установки, об ограничении зоны обнаружения);

– прием и отображение (световое, звуковое) извещений от датчиков угроз различных видов (утечки газа, воды);

– прием и отображение (световое, звуковое) извещений от пожарных извещателей;

– 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

– индикацию исправности канала связи с ПЦН;

– индикацию на УОО факта начала контроля состояния прибора АРМом ПЦН при взятии УОО под охрану;

– для УОО со встроенным источником резервного питания рекомендуется иметь индикатор, отображающий оставшийся заряд аккумуляторной батареи.

7.3 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.

7.4 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.

7.5 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.

7.6 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).

7.7 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).

7.8 УОО должны быть защищены от несанкционированного снятия с охраны в режиме охраны. В УОО должно быть исключено применение ключей Touch Memory без использования секретных кодов, защищающих их от копирования.

7.9 УОО должны обеспечивать возможность подключения выносных элементов 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.

ПРИЛОЖЕНИЕ 1

1. Порядок проведения экспертизы СЦН, применяемых в подразделениях вневедомственной охраны

1.1 Техническая экспертиза СЦН проводится в целях:

– проверки соответствия единым техническим требованиям;

– анализа тактико-технических характеристик;

– проверки функциональных возможностей;

– оценки стоимостных показателей;

– сравнения с аналогами, применяемыми в подразделениях вневедомственной охраны.

1.2 Экспертизе повергаются серийно выпускаемые СЦН, разработанные в инициативном порядке (без технического задания, утвержденного ГУВО 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 ГУВО МВД России, указав в нем наименование и область применения СЦН, ее основные особенности, краткие технические характеристики и стоимостные показатели с приложением копий сертификатов.

1.4 Экспертиза проводится ФКУ НИЦ «Охрана» МВД России (Исполнитель) на платной основе по письменному обращению ГУВО 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 характеристиках 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 ГУВО 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 ФКУ НИЦ «Охрана» МВД России.

1.10 Калькуляция, договор и соглашение о договорной цене.

На основании программы и методики проведения технической экспертизы СЦН, 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 ГУВО 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 ГУВО МВД России.

2 Порядок сертификации СЦН, предназначенных для применения подразделениями вневедомственной охраны

Сертификация проводится в ФКУ ЦСА ОПС МВД России 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

Эксплуатационные испытания СЦН 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 проводятся на объектах, охраняемых подразделениями вневедомственной охраны и определенных ГУВО МВД России. Продолжительность испытаний не менее 1000 часов со дня ввода в эксплуатацию.

3.2 Программа и методика испытаний.

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

– краткую характеристику систем с учетом заключения специалистов ФКУ 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 ГУВО 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.

Ввод СЦН 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 о соответствии СЦН 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 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 ГУВО МВД России.

ПРИЛОЖЕНИЕ 2

Термины, применяемые в настоящем документе и их определения

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