Техническое задание на проектирование системы обеспечения общественной безопасности города Калуги

город Калуга
2010 год

СОДЕРЖАНИЕ

АННОТАЦИЯ

В настоящем Техническом задании приведены основные назначения и цели создания, базовые технические требования к правоохранительному сегменту системы обеспечения общественной безопасности города Калуги, по его подсистемам, в том числе определены требования к организационному, информационному, программному и техническому обеспечению.

Определения, обозначения и сокращения, принятые в тексте

КТС	комплекс технических средств
АРМ	автоматизированное рабочее место;
БД	база данных
БЭК	банк электронных карт
ГУВД	городское управление внутренних дел
ДЧ	дежурная часть
ЕИТКС	единая информационно-телекоммуникационная система
ИАС	информационно-аналитическая система
ИМТПС	интегрированная мультисервисная телекоммуникационная подсистема
ИТКС	информационно-телекоммуникационная система
ВОЛС	волоконно-оптические линии связи
ШПД	широкополосный радиодоступ
КАС	комплекс аналитических систем
ОВД	органы внутренних дел
ОМ	отдел милиции
ПВН	подсистема видеонаблюдения
ПММО	подсистема мониторинга мобильных объектов
ПЭС-ГМ	подсистема экстренной связи «гражданин-милиция»
СИ	специальные исследования
СП	специальные проверки
СУБД	система управления базой данных
СУД	система управления досье
ЦМ	центр мониторинга
ЛЦМ	локальный центр мониторинга
Квитирование	уведомление отправителя пакета информации об успешном приеме данных, генерируемое получателем пакета

1 Общие положения

Настоящее техническое задание определяет требования к проектированию комплексной автоматизированной системы «Безопасный город» на территории города Калуги.
Шифр темы «Безопасный город».
Наименование Заказчика: УВД по Калужской области.
Наименование Исполнителя: УССиА УВД.
Разработка ведется на основании следующих документов:
Постановление Правительства Калужской области от 12.05.2008г. № 187 «О концепции построения комплексной системы безопасности в городах Калужской области на период до 2015 года» ;
Приказ УВД от 17.11.2008г. № 476 «О ведомственной целевой программе «Безопасный город» на 2009-2011г.г. для городских округов – г. Калуга и г. Обнинск».
Сроки выполнения работ:
Начало – _____ 2010 г.
Окончание – _____ 2010 г.

2 Цели и задачи

Целью внедрения КТС «Безопасный город» является повышение эффективности работы органов внутренних дел г. Калуги по охране правопорядка, повышение уровня безопасности личности, обеспечение гарантий собственности и минимизация причиненного материального ущерба от преступных посягательств в сфере экономики.

Цели достигаются за счет выполнения комплекса мероприятий:

- обеспечение повышенных мер безопасности в местах массового скопления людей;
- повышение эффективности работы служб правопорядка всех уровней;
- усиление информационной и технической базы правоохранительных и иных уполномоченных служб;
- повышение уровня взаимодействия органов внутренних дел с другими заинтересованными федеральными ведомствами, органами исполнительной власти.

Условия достижения цели:

- сокращение времени формирования и выдачи оперативной информации;
- сокращение времени реакции на нештатные ситуации оперативных дежурных, при выполнении ими оперативно-служебных задач;
- сокращение времени принятия решения по оперативной обстановке;
- снижение вероятности принятия ошибочных решений операторами

системы видеонаблюдения и дежурными сменами;

- максимальное снижение вероятности проведения террористического акта и криминальных действий в непосредственной близости с важными объектами, местами массового скопления людей.

Построение правоохранительного сегмента системы обеспечения общественной безопасности предполагает обеспечение комплексного подхода в реализации мер организационного, нормотворческого и технического плана, в частности - создание комплекса технических средств, решающего задачи:

- мониторинга поступающей информации о текущей обстановке (видеонаблюдение, диспетчерская связь, системы экстренного вызова и т.д.);

- позиционирования событий и реакций на них с использованием электронной карты города;

- автоматизированного определения типа события, характеризуемого принятым сигналом, сообщением, информацией о чрезвычайных, аварийных или нештатных ситуациях;

- обеспечения единой централизованной идентификации и аутентификации пользователей и поддержка иерархии доступа с системой приоритетов и полномочий доступа;

- ведения отчетности о действиях пользователей и состоянии системы в целом;

- предоставления пользователям системы единого интерфейса управления информационными ресурсами и отображения информации;

- оперативного архивирования видеоинформации;

- обеспечения возможности восстановления хода событий на основе имеющихся материалов;

- долговременного архивирования информации для последующего использования, анализа и криминалистических экспертиз.

Средствами достижения цели является проведение комплекса организационных мероприятий и оснащение подразделений органов внутренних дел, а также объектов города совокупностью взаимоувязанных комплексов технических средств и подсистем:

- городского видеонаблюдения;

- экстренной связи «гражданин-милиция»;

- мониторинга и управления подвижными объектами;

- видеофиксации нарушений правил дорожного движения и скоростного режима;

- удаленного доступа к автоматизированным банкам данных;

- защиты информации;

- автоматизированного и интегрированного управления;

- аппаратно-программных средств обработки и хранения видеоинформации;

- аппаратно-программных средств анализа и поддержки принятия решений.

3 Требования к структуре и составным частям правоохранительного сегмента обеспечения общественной безопасности

3.1 Состав правоохранительного сегмента обеспечения общественной безопасности и оснащаемых объектов Требования к структуре и функционированию

Для обеспечения общественной безопасности и правопорядка при возникновении чрезвычайных обстоятельств на территории г. Калуги - на базе ГУВД, создается единый центр мониторинга и обработки данных (ЦМ), который осуществляет управление силами и средствами правоохранительных органов, обеспечивает взаимодействие с другими силовыми структурами, органами государственной власти и экстренными службами.

Функционально центр мониторинга включает в себя:

- видеосерверы распределения видеопотоков;
- серверы хранения аудио- и видеоинформации;
- сервер системы мониторинга;
- центр обработки вызовов (экстренная связь, «02»);
- рабочие места операторов;
- рабочие места администраторов;
- вспомогательное оборудование для обеспечения работоспособности центра;
- средства отображения информации;
- инженерные системы (электроснабжение, охрано-пожарная сигнализация, контроль доступа, отопление, вентиляция, кондиционирование).

С целью обеспечения эффективного управления подчиненными силами и средствами и обеспечения взаимодействия с другими силовыми структурами, органами государственной власти и экстренными службами на территории города создается информационно-телекоммуникационная система[1], обеспечивающая руководству ЦМ возможность получать информацию о состоянии оперативной обстановки на территории города, принимать решения и передавать команды управления.

В состав информационно-телекоммуникационной системы входят:

- информационно-аналитическая подсистема;
- интегрированная мультисервисная телекоммуникационная подсистема;
- подсистема видеонаблюдения;
- подсистема экстренной связи «гражданин-милиция»;

[1] Далее – «ИТКС».

- подсистема мониторинга подвижных объектов;
- подсистема видеофиксации нарушений правил дорожного двидения;
- подсистема защиты информации.

Состав оснащаемых объектов:

В состав основных оснащаемых объектов в рамках создания сегмента системы входят:

- дежурная часть ГУВД, УВД и ее мобильные объекты;
- дежурные части территориальных отделов внутренних дел (ГОМ 1, ГОМ 2) и их мобильные объекты;
- дежурная часть и мобильные объекты управления вневедомственной охраны;
- дежурные части и мобильные объекты ГИБДД;
- дежурные части и мобильные объекты подразделений внутренних дел (ОБППСМ, ОБОиКПиО, медвытрезвитель).

Объекты на территории города - места массового скопления людей, объекты жилого сектора, здравоохранения, детские школьные и дошкольные учреждения, транспортные узлы, трассы проезда, железнодорожный и автовокзал, аэропорт (в перспективе), стратегические объекты, водозабор и территории, прилегающие к нему, а также зоны с повышенной криминогенной обстановкой: рынки, стадионы и места проведения массовых мероприятий и праздников.

На базе дежурной части УВД по Калужской области и дежурных частей подразделений УВД, создаются локальные центры мониторинга (ЛЦМ) или удаленные рабочие места.

Состав дополнительно оснащаемых в процессе создания системы объектов определяется в каждом конкретном случае.

Требования к структуре и функционированию.

Сегмент системы имеет территориально распределенную инфраструктуру, соответствующую составу и месторасположению оснащаемых объектов и пунктов наблюдения.

Сегмент системы создается с учетом возможности организации связи, взаимодействия с существующими информационными системами органов внутренних дел, действующих (дислоцированных) на территории города, а также экстренных служб города и муниципальных образований.

Предполагается возможность оперативного подключения пунктов быстрого развертывания, в том числе на основе беспроводных каналов передачи информации.

Структурно-технические решения сегмента системы обеспечивают возможность одновременного получения пользователями всех уровней информации согласно иерархии и полномочий доступа к информации.

Функционально сегмент системы включает в себя следующие компоненты:

- источники информации;
- средства трансляции цифровой видео- и аудиоинформации;
- средства отображения информации;
- средства архивирования видеоинформации;
- средства обработки информации;
- средства обмена информацией;
- средства защиты информации;
- специализированное программное обеспечение;
- проектную, техническую и эксплуатационную документацию.

3.2 Информационно-аналитическая подсистема

3.2.1. Подсистема управления включает в свой состав комплекс программно-технических средств, обеспечивающих:

- управление системой с АРМ оператора системы;
- представление информации с АРМ операторов на центральный экран центра мониторинга;
- управление протоколированием и воспроизведением аудио-видеоинформации;
- управление или мониторинг состояния инженерных систем.

3.2.2 Комплексная информационно-аналитическая система должна обеспечивать накопление, обработку и анализ получаемой информации, доступ к информационным ресурсам органов внутренних дел, выявлять связи между объектами учета, строить модели развития ситуации.

В состав ИАС входят следующие подсистемы:

- подсистема оперативного поиска, обеспечивающая сбор, хранение и обработку оперативной информации, включая выдачу статистической информации и сводок по преступлениям, которая в свою очередь должна обеспечить интеграцию с системой ЕМАС ДЧ;
- геоинформационная подсистема, обеспечивающая сбор, хранение, обработку, отображение пространственно-координированных объектов на основе электронных карт и моделей;
- информационно-справочная подсистема, обеспечивающая сбор, хранение, представление информационных материалов о городской инфраструктуре и оперативной обстановки.

3.3 Интегрированная мультисервисная телекоммуникационная подсистема

Интегрированная мультисервисная телекоммуникационная подсистема[2] предназначена для создания транспортной среды, обеспечивающей передачу информации между объектами сегмента.

[2] Далее – «ИМТПС».

ИМТПС обеспечивает следующие виды связи:

- трансляцию видеосигнала от видеокамер в центр мониторинга и ЛЦМ подразделений ОВД, обслуживающих территорию города, а также управление видеокамерами;

- удаленный доступ абонентов к централизованным банкам данных и оперативно-справочным учетам;

- обмен служебной и оперативной информацией между дежурными частями органов внутренних дел и подразделениями УВД, а также мобильными силами правоохранительных органов, задействованных для обеспечения общественной безопасности и правопорядка на территории города;

- передачу данных о местонахождении мобильных сил правоохранительных органов в ЦМ и ЛЦМ подразделений УВД, обслуживающих территорию города;

- трансляцию видео и аудио сигналов от пунктов экстренной связи в ЦМ и ЛЦМ подразделений УВД, обслуживающих территорию города;

- передачу данных с автоматизированных комплексов видео фиксации нарушений правил дорожного движения в ЦМ и ЛЦМ ГИБДД УВД;

- связь взаимодействия ЦМ с силовыми структурами, органами государственной власти и экстренными службами, расположенными на территории города и за его пределами.

ИМТПС создается на базе, как вновь прокладываемых линий связи (ВОЛС, ШПД), так и с использованием телекоммуникационной составляющей ЕИТКС УВД.

ИМТПС, в случае необходимости, должна использовать ресурсы и интегрироваться с другими телекоммуникационными системами, развернутыми на территории города.

Применение ИМТПС позволит обеспечить интеграцию подсистем ИТКС в единую телекоммуникационную систему и создать единое информационное пространство для правоохранительных органов задействованных для обеспечения безопасности и правопорядка на территории города.

В общем случае в состав ИМТПС входят:

- стационарная телекоммуникационная система;
- система широкополосного радиодоступа;
- система подвижной радиосвязи.

Стационарная телекоммуникационная система при оперативном управлении своими элементами обеспечивает следующие виды связи:

- трансляцию видеосигнала от видеокамер в ЦМ и ЛЦМ подразделений УВД, обслуживающих территорию города;

- удаленный доступ стационарных абонентов к централизованным банкам данных и оперативно-справочным учетам;

- обмен служебной и оперативной информацией между дежурными

частями ОВД и подразделениями правоохранительных органов, задействованных для обеспечения общественной безопасности и правопорядка на территории города;

- трансляцию видео и аудио сигналов от пунктов экстренной связи в ЦМ и ЛЦМ подразделений УВД, обслуживающих территорию города;

- связь взаимодействия центра мониторинга с силовыми структурами, органами государственной власти и экстренными службами, расположенными на территории города и за его приделами.

Система широкополосного радиодоступа обеспечивает те же функции управления (аналогичные виды связи) в местах, где организация каналов стационарной телекоммуникационной системы невозможна или экономически нецелесообразна.

Система подвижной радиосвязи обеспечивает следующие виды связи:

- обмен служебной и оперативной информацией между ЦМ, ЛЦМ и мобильными силами правоохранительных органов, задействованных для обеспечения общественной безопасности и правопорядка на территории города;

- связь взаимодействия мобильных сил правоохранительных органов и мобильных сил силовых структур, органов государственной власти и экстренных служб в местах возникновения чрезвычайных ситуаций;

- удаленный доступ мобильных абонентов к централизованным банкам данных и оперативно-справочным учетам;

- передачу данных о местонахождении мобильных сил правоохранительных органов в ЦМ и ЛЦМ подразделений УВД, обслуживающих территорию города.

3.4 Подсистема видеонаблюдения

Подсистема видеонаблюдения (далее – «ПВН») предназначена для предоставления сотрудникам ЦМ и, при необходимости, ЛЦМ подразделений УВД, обслуживающих территорию города, видеоинформации об оперативной обстановке на территории города или отдельных мест в повседневной деятельности.

Применение ПВН позволит обеспечить дистанционное обнаружение и фиксацию фактов совершения криминальных действий, угроз и преступлений террористического характера, повысить уровень охраны критически важных объектов, мест массового пребывания людей.

ПВН представляет собой систему телевизионного контроля, работающую в круглосуточном режиме и построенную на основе распределенной сети телевизионных камер, размещаемых на территории города и на стратегически важных объектах.

ПВН должна поддерживать интеллектуальную аналитическую

обработку данных, а именно отбор, «вычленение» из видеопотока данных, событий, объектов, представляющих интерес с точки зрения безопасности, контроля ситуации, выявления угроз, что позволит сократить долю рутинной работы оператора.

В зависимости от поставленной задачи должны быть реализованы следующие основные функции видеоаналитики:

- обнаружение;
- различие;
- идентификация.

Целевая задача обнаружения – общее наблюдение за обстановкой на территории, обнаружение всех перемещающихся в определенном направлении объектов (лиц, транспорта), обнаружение оставленных предметов.

Целевая задача различения – контроль наличия лиц или других объектов в контролируемой зоне, фиксация их противоправных действий (вандализм, драка, ДТП и т.д.).

Целевая задача идентификации – отождествление записанного изображения с хранящимся в базе данных (узнавание незнакомого объекта контроля), получение четкого изображения лица любого человека в зоне наблюдения, позволяющее в последствии его распознать.

Внедрение указанных функций видеоаналитики позволит решить следующие задачи:

- возможность предупреждения, выявления и пресечения угроз и преступлений террористического характера, а также повышение надежности охраны критически важных объектов и мест массового пребывания людей;
- возможность централизованного отслеживания состояния различных стратегически важных объектов и территорий города;
- обнаружение и предотвращение фактов совершения криминальных действий;
- своевременная и достоверная информационная поддержка служб охраны и правопорядка всех уровней;
- обеспечение эффективного управления постами и тревожными группами органов и служб безопасности и охраны правопорядка;
- слежение за указанными подвижными объектами в автоматизированном режиме, проведение оперативной идентификации объектов (номерных знаков транспортных средств и лиц);
- фиксация видеоинформации от территориально-распределенных камер, установленных на объектах города;
- обеспечение возможности восстановления хода событий на основе записанных видеоматериалов посредством предоставления удаленного санкционированного доступа к видеоархиву сотрудникам правоохранительных органов и администрации города;
- автоматизированный анализ изображений и выделение из последовательности изображений, зафиксировавших нарушение

общественного порядка, идентифицирующих признаков фигурантов;

- дистанционная идентификация лиц и объектов;

- телеавтоматический контроль и управление дорожным движением, повышение эффективности реагирования на осложнение дорожно-транспортной обстановки со стороны оперативных служб, снижение аварийности дорожного движения.

- видеофиксация нарушений правил дорожного движения и дорожно-транспортных происшествий;

- мониторинг транспортного потока и выявление транспортных средств, находящихся в базах розыска, автоматизированными программными комплексами идентификации транспортных средств по государственным регистрационным знакам;

- фиксацию и хранение видеоинформации, поступающей от видеокамер, установленных на территории и объектах города;

- дистанционное управление видеокамерами;

- дистанционная диагностика оборудования ПВН;

В состав основных объектов видеонаблюдения входят:

- автомобильные въезды в город, улично-дорожная сеть, транспортные магистрали, перекрестки, площади, подземные переходы;

- транспортные узлы: железнодорожный и автовокзалы, аэропорт (в перспективе).

Места установки и зоны наблюдения видеокамер, а также размещение устройств обработки, хранения, печати видеоинформации подлежат согласованию с Заказчиком на этапе проектирования. Также подлежат согласованию с Заказчиком тип и параметры оборудования.

Требования к качеству видеоинформации.

Тракт системы (видеокамеры, устройства оцифровки и преобразования, передачи и хранения), алгоритмы обработки должны обеспечивать следующие показатели качества видеоизображения при соответствующем ГОСТу уровню освещенности:

- для цветного изображения разрешение не менее 470 ТВЛ и чувствительность не менее 0,5 лк;

- для черно-белого изображения разрешение не менее 540 ТВЛ и чувствительность не менее 0,01 лк;

- размер кадра в пикселах: не менее 720 точек по горизонтали и не менее 576 строк по вертикали для оцифрованного кадра;

- насыщенность изображения должна быть таковой, чтобы при его преобразовании к изображению в градациях серого, динамический, диапазон интенсивности кодировался, по крайней мере, 8 битами;

-видеоинформация представляется в виде последовательности оцифрованных и сжатых кадров с параметрами не хуже вышеуказанных;

-скорость передачи видеоинформации в реальном времени - не менее 25 кадров в секунду по каждому каналу при максимальном качестве видеоданных (в случае оперативной необходимости) и не менее 6 кадров в

секунду при контроле обстановки в рабочем режиме;

- видеокамеры должны сохранять работоспособность при наружном монтаже в диапазоне температур от -40 до +50° С;

- видеокамеры, используемые для идентификации объектов, должны выбираться с учетом предъявляемых специфических требований.

Необходимо предусмотреть установку антивандальных систем защиты, оборудования для подсветки мест наблюдения, крепление камер к поворотным устройствам и др., а также их соответствие требованиям надежности к воздействию внешних факторов. Средства защиты видеокамер от внешних воздействий (осадков, перепадов температуры, повышенной влажности, а также проявлений вандализма), требования к которым определяются характеристиками места установки:

- для уличного исполнения средства защиты должны соответствовать требованиям класса не хуже IP66 в соответствии с ГОСТ 14254-96;

- рабочий диапазон температур для уличного исполнения средства защиты должен быть не хуже -40... +50 градусов Цельсия.

Поворотные устройства видеокамер (по необходимости).

Видеокамера с поворотным (в том числе сетевая или IP- камера) устройством может представлять собой функционально и конструктивно законченный модуль. Поворотные устройства должны отвечать следующим требованиям:

- для уличного исполнения поворотные устройства видеокамер должны соответствовать требованиям класса не хуже IP66 в соответствии с ГОСТ 14254-96;

- рабочий диапазон температур для уличного исполнения средств защиты должен быть не хуже -40... +50 градусов Цельсия;

- максимальный угол поворота по горизонтали – не менее 300 градусов;

- максимальный угол поворота по вертикали – не менее 120 градусов;

- скорость поворота – не менее 30 градусов в секунду;

- точность позиционирования – не хуже 3 градусов;

- интерфейс управления поворотными устройствами: RS422, RS232, RS485.

Все оборудование (в том числе, предназначенное для приема аналогового сигнала с видеокамер и его цифрового преобразования), должно отвечать общим требованиям надежности и защите информации, перечисляемым ниже в соответствующих разделах данного задания.

Основное назначение подсистемы хранения и обработки - запись оцифрованной видеоинформации, поступающей от различных источников в хранилище данных, предоставление Пользователю, обеспечение обработки, в том числе выбор необходимого эпизода из архива видеозаписей, автоматическую индексацию и разметку по эпизодам и пересылку.

Требования к объему хранилища данных выбираются, исходя из требований к нормированной продолжительности хранения, количеству видеокамер, качества, в котором будет сохраняться видеоинформация, и рассчитывается на стадии рабочего проекта.

Подсистема хранения и обработки должна иметь возможность расширения и наращивания без остановки функционирования, а также отвечать требованиям к надежности и защите информации, перечисленным ниже в соответствующих разделах данного задания.

Для хранения видеоинформации в ЦМ создается видеоархив, состоящий из блоков – серверов, связанных в единый комплекс. Срок хранения информации определяется с учетом специфических особенностей оперативной обстановки на территории города.

Требования к качеству видеоинформации в видеоархиве аналогичны требованиям к самим видеокамерам.

В общем случае абонентами видеоархива могут быть:

- локальные центры мониторинга;
- удаленные АРМ подразделений УВД;
- подразделения ФСБ России, обслуживающие территорию города;
- дежурная часть Службы спасения Департамента по делам ГО и ЧС города;
- дежурная часть линейного отдела внутренних дел на транспорте.

Удаленный доступ к видеоархиву осуществляется при помощи аппаратно-программных средств, входящих в состав ИТКС.

При наличии технической возможности ПВН должна интегрироваться с другими системами видеонаблюдения, развернутыми на территории города и принадлежащим различным собственникам (МУПы, ЧОПы и т.д.).

3.5 Подсистема экстренной связи «гражданин-милиция»

Подсистема экстренной связи «гражданин-милиция» (далее - «ПЭС-ГМ») предназначена для обеспечения круглосуточной оперативной связи граждан с ЦМ и ЛЦМ подразделений УВД.

ПЭС-ГМ построена на основе распределенной сети, объединяющей пункты экстренной связи, расположенные на территории города, с терминалом, установленным в ЦМ или ЛЦМ.

ПЭС-ГМ обеспечивает функции визуального и акустического контроля оперативной обстановки, а так же регистрацию поступающей аудио и видео информации.

Применение ПЭС-ГМ позволит:

- сократить время получения информации о возникновении криминогенной ситуации и террористических угроз;
- повысить оперативность принятия управленческих решений по их пресечению;

- обнаружить и предотвратить факты совершения криминальных действий;

- обеспечить своевременную и достоверную информационную поддержку служб охраны правопорядка всех уровней и, как следствие, сократить время реагирования дежурных нарядов;

- увеличить процент раскрытия преступлений по «горячим следам»;

- своевременно предупредить и выявить угрозы и преступления террористического характера;

- обеспечить возможность восстановления хода событий на основе записанных видеоматериалов и аудиоматериалов.

ПЭС-ГМ должна обеспечивать решение следующих задач:

- предоставление гражданам круглосуточной оперативной экстренной голосовой связи с дежурным ЦМ (ЛЦМ) в опасных в криминогенном плане общественных местах;

- ручное и автоматическое управление видеокамерами наблюдения, подключенными к пункту экстренной связи, с автоматической регистрацией аудио и видео сигнала;

- многоканальную запись аудио и видео переговоров с возможностью их прослушивания и передачи в электронном виде на другие сетевые устройства;

- передачу информации, получаемой от пунктов экстренной связи, в ЦМ (ЛЦМ) или на удаленные рабочие места других подразделений УВД, обеспечивающих охрану правопорядка на территории города;

- интеграцию с системами фоноучетов и фотоучетов МВД и возможность удаленного доступа к автоматизированным банкам данных для автоматической идентификации лиц по имеющимся базам данных на предмет принадлежности голоса и изображения лица звонящего базе биометрических учетов разыскиваемых или подозреваемых лиц.

Терминалы экстренной связи должны быть в антивандальном исполнении и работать в диапазоне температур от – 30 до +50° С.

Технические характеристики аппаратуры ПЭС-ГМ должны обеспечивать выполнение требований МВД к качеству аудиоинформации и ее пригодности для проведения идентификационных исследований по голосу и речи:

- диапазон частот голосового канала связи должен быть 150-7500 Гц (частота дискретизации не ниже 11150 Гц);

- нелинейность АЧХ – не более 1%;

- должен быть обеспечен дуплексный режим работы устройства передачи голосовых данных;

- максимальное удаление говорящего от устройства экстренной связи, при котором должна обеспечиваться разборчивость речи составляет 1 метр;

- устройство передачи голосовых сообщений должно иметь заключение ЭКЦ МВД о пригодности устройства и получаемой с его помощью аудиоинформации, для проведения идентификационных

исследований по голосу и речи;

- аппаратура регистрации переговоров должна иметь заключение ЭКЦ МВД о пригодности получаемой с его помощью аудиоинформации, для проведения идентификационных исследований по голосу и речи.

3.6 Подсистема мониторинга мобильных объектов

Подсистема мониторинга мобильных объектов (далее – «ППМО») предназначена для предоставления сотрудникам ЦМ (ЛЦМ) и, при необходимости, в дежурные части подразделений УВД, обслуживающих территорию города, информации о местонахождении и состоянии:

- мобильных сил правоохранительных органов, задействованных в обеспечении общественной безопасности и правопорядка на территории города;

- личных транспортных средств граждан, оборудованных соответствующей системой.

Применение ПММО позволит:

- обеспечить эффективное управление мобильными силами правоохранительных органов;

- повысить эффективность работ «по горячим следам» за счет сокращения времени прибытия на место происшествия;

- осуществлять своевременное реагирование на происшествия, связанные с транспортными средствами, представляющими повышенную опасность для жизнедеятельности города или потенциальную привлекательность для совершения террористических действий;

- повысить эффективность борьбы с хищениями личных транспортных средств граждан.

ПММО представляет собой систему дистанционного контроля, построенную на основе распределенной сети датчиков, размещаемых на мобильных объектах, подлежащих мониторингу.

Состав и структура подсистемы мониторинга согласуется с Заказчиком и определяется при проектировании.

ПММО должна обеспечивать решение следующих задач:

- слежение за заданными подвижными объектами в автоматизированном режиме;

- определение местонахождения объекта;

- дистанционное определение состояние объекта;

- отображение на электронной карте города, расположенной в ЦМ (ЛЦМ) или дежурной части подразделения УВД, обслуживающего территорию города, в реальном времени местонахождения и состояние объекта;

- динамическое масштабирование на электронной карте города местоположения объекта;

- фиксацию и хранение информации о местонахождении и состоянии объекта;

- восстановление на основе записанных материалов маршрутов следования объекта (формирование отчета).

Передача информации от подвижного объекта в ЦМ (ЛЦМ) или подразделение УВД, обслуживающего территорию города, осуществляется при помощи аппаратно-программных средств, входящих в состав ИТКС.

ПММО должна соответствовать общим тактико-техническим требованиям к спутниковым навигационно-мониторинговым системам для органов внутренних дел Российской Федерации и внутренних войск МВД России, утвержденным приказом МВД от 31.12.2008г №1197 и иметь сертификат соответствия (приказ МВД России от 26.09.2009 №737).

При внедрении ПММО должна быть обеспечена совместимость с системами мониторинга, использующихся в УВД по Калужской области.

3.6.1. Тактико-технические требования к подсистеме.

3.6.1.1 Общие требования к подсистеме.

Подсистема должны состоять из следующих основных частей:

оборудования стационарного центра мониторинга, в том числе оборудование для хранения электронных карт, оборудование для хранения информации мониторинга, оборудование для доступа к каналам связи и прочее;

оборудования мобильных ЦМ (по специальному заказу);

оборудования удалённых рабочих мест;

бортового оборудования для установки на служебный автотранспорт;

телекоммуникационных каналов;

электронных карт;

комплекса программного обеспечения.

Подсистема должна обеспечивать возможность построения вышестоящего ЦМ, собирающего выборочную информацию от нижестоящих центров по каналам связи, с использованием интегрированной мультисервисной телекоммуникационной сети МВД России или информационно-телекоммуникационной сети внутренних войск МВД России, в защищенном виде в соответствии с решением по ЕИТКС–К ОВД, и сохраняющего ее при необходимости в своей собственной базе данных. Не допускается прохождение информации через узлы (серверы) поставщиков подсистемы.

Подсистема должна обеспечивать возможность построения единой системы мониторинга с тремя уровнями иерархии:

уровень департаментов МВД России, подразделений, непосредственно подчиненных МВД России, главных управлений МВД России по федеральным округам[3];

[3] Далее — «федеральный уровень».

уровень МВД, ГУВД, УВД по субъектам Российской Федерации[4];

уровень отделов (управлений) внутренних дел по районам, городам и иным муниципальным образованиям;[5]

а также должна быть реализована дополнительно возможность информационного взаимодействия между уровнями иерархии системы, доступ к справочной и служебной информации с различных уровней иерархии системы, предоставление справочной и служебной информации для различных уровней иерархии системы.

Подсистема должна обеспечивать возможность определения, передачи и отображения на ЭК местности навигационных параметров служебных ТС с установленным бортовым оборудованием, а также доставку и отображение на бортовом оборудовании (в специальном варианте исполнения) служебного автотранспорта текстовой и графической информации, передаваемой из ЦМ.

Способ распределения условных номеров комплектов бортового оборудования должен обеспечивать уникальность присвоенного номера каждому ТС (номер состоит из 7 разрядов: два разряда – номер региона, следующие пять разрядов – номер бортового оборудования).

Подсистема должна осуществлять автоматизированную поддержку актуальности справочной информации по ТС на всех уровнях реализации. Изменения должны вступать в силу во всех ЦМ на всех уровнях иерархии не позднее двух суток.

Тревожные и служебные извещения, формируемые бортовым оборудованием ТС, должны поступать и фиксироваться в ЦМ органа внутренних дел, обеспечивающего наблюдение на данной территории. Отображение поступившей информации должно сопровождаться отображением местоположения ТС на ЭК местности.

При перемещении ТС с установленным бортовым оборудованием одной из аналогичных систем между зонами обслуживания, оборудование ЦМ подсистемы должно обеспечивать возможность автоматизированной передачи процесса обслуживания данного ТС, установление информационного обмена и взятие на контроль (с голосовым информированием экипажа ТС — по специальному заказу).

Подсистема должна обеспечивать возможность автоматизированной трансляции информации, поступившей от ТС, и данных о его местоположении в ЦМ других систем, а также в вышестоящие ЦМ в соответствии с принятой иерархией.

Подсистема должна обеспечивать передачу команд управления бортовым оборудованием ТС из ЦМ, обеспечивающего текущее наблюдение за этим подвижным объектом.

Подсистема должна обеспечивать квитирование прохождения информации между бортовым оборудованием и ЦМ, а также между ЦМ на

[4] Далее — «региональный уровень».

[5] Далее — «территориальный уровень».

всех уровнях реализации (при передаче навигационных отметок по каналу ультракоротких волн[6] квитирование может не применяться).

В подсистеме должны использоваться электронные карты, представленные в векторной форме (в виде набора векторов заданной длины и ориентации). Должна обеспечиваться возможность конвертации сторонних ЭК в программное обеспечение[7] систем — совместимость форматов используемых ЭК с форматом MapInfo и форматом SXF. Должна обеспечиваться поддержка адресного слоя в ЭК (поиск объекта по адресу).

Подсистема должна обеспечивать возможность использования навигационных сигналов системы ГЛОНАСС либо совместно сигналов систем ГЛОНАСС/GPS.

Шкалы времени подсистемы должны быть синхронизированы с национальной шкалой координированного времени Российской Федерации UTC (SU) с погрешностью не более 0,01 секунды.

Подсистема, а также используемые ЭК и навигационная аппаратура потребителей глобальных навигационных спутниковых систем должны быть сертифицированы в установленном в Российской Федерации порядке. Навигационные приёмники должны быть сертифицированы как средство измерений в организации, аккредитованной в области данного вида измерений.

Подсистема должна обеспечивать резервное копирование информации и её восстановление после сбоя.

3.6.1.2 Технические требования к подсистеме.

Подсистема должна обеспечивать круглосуточное бесперебойное обслуживание не менее 1000 ТС для ЦМ территориального уровня.

Подсистема должна обеспечивать возможность получения выборочной информации о ТС вышестоящими ЦМ от ЦМ нижестоящего уровня.

Подсистема должна обеспечивать определение местоположения каждого из обслуживаемых ТС и отображение его на ЭК с предельной погрешностью (при доверительной вероятности 0,997) не более ±30 метров.

Подсистема должна обеспечивать идентификацию информации, полученной от каждого из комплектов бортового оборудования с отображением в ЦМ следующих основных параметров:

идентификационный номер комплекта в системе;

государственный регистрационный номер ТС;

идентификационный номер ТС (VIN);

торговую марку ТС;

модель ТС;

цвет кузова ТС;

---

[6] Далее — «УКВ».

[7] Далее — «ПО».

принадлежность к подразделению и условный номер;

позывные радиообмена;

телефонный номер SIM (R-UIM)-карты, установленной в ТМ.

Подсистема должна обеспечивать формирование бортовым оборудованием ТС и доставку в ЦМ следующих основных извещений:

«Занят» — предупреждение о выполнении ранее полученного указания;

«Свободен» — подтверждение о выполнении указания;

«Прибыл на место» — подтверждение прибытия в указанное место;

«Приступил к исполнению» — подтверждение полученного указания;

«Взят под охрану» — система автомобильной сигнализации включена;

«Снят с охраны» — система автомобильной сигнализации отключена;

«Тревога-вторжение» — несанкционированный доступ внутрь ТС и (или) сработала система автомобильной сигнализации;

«Тревога-нападение» — сигнал тревоги подан экипажем ТС;

«Несанкционированное вскрытие» — вскрытие корпуса ТМ или другие несанкционированные действия при попытках вывести бортовое оборудование из строя;

«Выход из зоны наблюдения» — при выходе автомобиля из заданной зоны;

«Вход в зону наблюдения» — при входе автомобиля в заданную зону;

«Нет навигации» — бортовое оборудование не принимает навигационные сигналы от спутников;

«Нет связи с объектом» — на ЦМ не принимаются сигналы от бортового оборудования;

«Переход на резервное электропитание» — переключение бортового оборудования на электропитание от внутреннего резервного источника;

«Критическое состояние резервного электропитания» — исчерпан ресурс внутреннего резервного источника электропитания бортового оборудования.

Подсистема должна обеспечивать возможность постановки ТС под охрану как водителем ТС, так и оператором ЦМ.

Подсистема должна обеспечивать передачу и выполнение не менее двух команд управления бортовым оборудованием ТС из ЦМ (в зависимости от решаемых задач).

Подсистема в специальном варианте исполнения должна обеспечивать передачу из ЦМ, отображение на бортовом оборудовании ТС, формирование бортовым оборудованием ТС и доставку в ЦМ текстовых сообщений, состоящих из 64 произвольных текстовых символов (включая кириллицу) и более.

Подсистема должна обеспечивать получение в ЦМ информации от не менее 6 ТС за секунду в канале УКВ.

Подсистема, при наличии устойчивого канала связи, должна обеспечивать доставку информации от бортового оборудования в ЦМ, а также доставку служебной информации или команд управления из ЦМ до бортового оборудования за время не более 10 секунд.

Подсистема, при наличии устойчивого канала связи, должна обеспечивать периодичность получения в ЦМ информации о местоположении и текущем состоянии ТС:

при несении дежурства — не менее чем 1 раз за 10 секунд;

при возникновении тревожной ситуации — не менее чем 1 раз за 5 секунд.

Подсистема, при наличии устойчивого канала связи, должна обеспечивать периодичность проверки работоспособности бортового оборудования, формирование и передачу информации о текущем состоянии («сигнал жизни»):

при несении дежурства — не менее чем 1 раз за 60 секунд;

в режиме «Взят под охрану» — в интервале от 2 до 720 минут;

в режиме «Снят с охраны» — в интервале от 2 до 24 часов.

3.6.1.3 Технические требования к оборудованию и программному обеспечению центров мониторинга подсистемы.

Программное обеспечение подсистемы должно иметь модульный принцип построения.

Оборудование и ПО ЦМ должны обеспечивать выполнение следующих основных функций:

защиту от несанкционированного доступа и утечки информации по техническим коналам;

прием, обработку и отображение навигационных параметров и текущего состояния всех автомобилей, оснащённых комплектами бортового оборудования, входящими в состав подсистемы;

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

постоянное накопление и обработку поступающей информации с целью привлечения внимания оператора при возникновении ситуаций, требующих его действий;

документирование, систематизацию и хранение поступающей информации.

Оборудование и ПО ЦМ в специальном варианте исполнения должны обеспечивать выполнение следующих дополнительных функций:

прием, обработку и отображение фото (видео) информации от бортового оборудования ТС, обеспечивающего передачу фото (видео)

изображения;

прием запросов от бортового оборудования ТС, обеспечивающего удаленный доступ к информационным базам данных, их обработку и отправку ответов;

возможность корректировки и настройки геоинформационных баз данных (электронной карты местности с адресными данными).

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

Оборудование и ПО ЦМ должны обеспечивать отображение местоположения каждого автомобиля, оснащённого комплектом бортового оборудования, входящим в состав подсистемы, а также траектории его движения на фоне ЭК местности, в виде ломаной линии и(или) набора точек (по выбору оператора), как в отдельном окне, так и в текущем. Линии должны иметь стрелки, указывающие направление движения ТС, точки должны иметь порядковые номера. По желанию оператора рядом с каждой точкой маршрута на ЭК должно указываться время определения НП в данной точке.

Синхронизация шкал времени компьютеров ЦМ должна осуществляться по сигналам спутниковой группировки ГЛОНАСС путём подключения к одному из компьютеров локальной сети ЦМ приёмника сигналов системы ГЛОНАСС. Синхронизация должна осуществляться один раз в 5 минут с погрешностью не более 0,01 секунды. Погрешность выдачи сигналов времени используемым приёмником ГЛОНАСС должна составлять не более 0,01 секунды.

Оборудование и ПО ЦМ должны обеспечивать разделение уровней доступа операторов и обслуживающего персонала к управлению и получению информации в соответствии с выполняемыми служебными обязанностями, с протоколированием и хранением запросов в архиве.

Оборудование и ПО ЦМ должны обеспечивать возможность оперативной настройки параметров получения, отображения и обработки информации в соответствии с условиями эксплуатации (изменение перечня отображаемых на ЭК транспортных средств, отображение патрульных автомобилей разных групп отметками разной формы и цвета, изменение перечня отображаемых сведений о ТС).

ПО ЦМ должно отображать признак неактуальности (устаревания) НП ТС с указанием времени вычисления последних действительных НП и причины их неактуальности (потеря связи с бортовым оборудованием, отсутствие приёма навигационным приёмником сигналов от спутников).

ПО ЦМ территориального уровня должно обеспечивать отображение векторных ЭК с величиной временной задержки при изменении масштабов и сдвигов не более 3-х секунд. ЭК должны выводиться на экран операторов в зависимости от текущей ситуации в автоматическом режиме. При этом

картографическое обеспечение должно поддерживать возможность нанесения на ЭК условных обозначений (постов, мест происшествий).

Должна обеспечиваться возможность одновременного открытия нескольких окон (не менее 6-ти) с ЭК разных регионов, в каждом из которых должна устанавливаться центровка по одному ТС или автоматическое масштабирование по группе ТС.

В ПО ЦМ должны быть средства вычисления расстояний на ЭК («электронная линейка» с точностью ±10%) и средства поиска объектов ЭК по адресу.

При просмотре истории движения ТС должен обеспечиваться быстрый и удобный поиск местоположения ТС в заданное время, а также поиск момента времени, в которое ТС находилось в заданном месте, с возможностью ручного пошагового перемещения отметки ТС по траектории вперёд и назад.

ПО ЦМ должно обеспечивать возможность быстрого и удобного создания и редактирования контрольных зон, закрепления этих зон за конкретными ТС, анализа времени нахождения ТС в зоне/вне зоны, пересечения границ зоны.

ПО ЦМ должно обеспечивать возможность контроля соблюдения графика движения ТС.

Оборудование и ПО ЦМ должны обеспечивать возможность накопления информации в архиве со сроком хранения не менее 6 месяцев, поиск информации, сохраненной в архиве, по различным признакам, формирование отчета о движении ТС или группы ТС в графической (на фоне ЭК), текстовой и табличной форме с указанием величины пробега и времени простоя за указанный промежуток времени, количества отработанного времени, событий, происходивших с ТС (срабатывание датчиков, превышение скорости, обрывы связи), времени нахождения ТС в зоне и вне зоны контроля, процента патрулирования зоны контроля (отношение времени движения ТС в зоне к общему времени нахождения в зоне).

ПО ЦМ должно обеспечивать возможность переназначения (изменения имен) датчиков, подключенных к входам бортового оборудования, и исполнительных устройств, подключенных к выходам бортового оборудования.

Оборудование и ПО ЦМ должны обеспечивать резервное копирование (в том числе на внешние носители информации) 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.

3.6.1.4 Требования к применяемым электронным картам.

В состав подсистемы должны входить ЭК Российской Федерации (масштаб 1:1000000), региона (республики, края, автономного округа, области) Российской Федерации (масштаб 1:100000), населённых пунктов субъекта Российской Федерации (масштаб 1:10000).

ЭК Российской Федерации должна содержать города, федеральные трассы, железнодорожные пути, реки, озёра, названия республик, краёв, автономных округов, областей и городов (с численностью населения не менее 1000 человек), а также названия федеральных трасс.

ЭК региона Российской Федерации должна содержать населённые пункты, автодороги федерального и регионального значения, железнодорожные пути, гидрографию, мосты, земельные участки, зеленые насаждения, названия районов области, населённых пунктов (с численностью населения не менее 100 человек) и автодорог.

ЭК населённого пункта Российской Федерации должна содержать дороги, улицы и тротуары, железнодорожные пути, гидрографию, мосты, строения, земельные участки, зеленые насаждения, названия улиц, площадей, скверов, парков, автокооперативов, садоводческих товариществ, стадионов, кладбищ, номера домов и корпусов (с названиями учреждений и организаций, располагающихся в этих зданиях), названия микрорайонов, округов и районов населённого пункта.

3.6.1.5 Технические требования к бортовому оборудованию подсистемы.

Бортовое оборудование ТС должно обеспечивать следующие режимы работы:

«Активный» — выполняется определение навигационных параметров и осуществляется передача данных в ЦМ;

«Ждущий» — выполняется определение навигационных параметров, передача данных в ЦМ не осуществляется;

«Спящий» — навигационный приёмник выключен, данные в ЦМ не передаются, осуществляется контроль всех шлейфов сигнализации;

«Взят под охрану» - осуществляется контроль всех шлейфов сигнализации, формирование соответствующих извещений, прием и выполнение команд из центра контроля и управления;

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

«Черный ящик» — выполняется определение навигационных параметров и их запись во внутреннюю энергонезависимую память без передачи информации в эфир;

«Сервис» — перепрограммирование ТМ дистанционно (по высокоскоростным каналам связи) либо путём подключения его к персональному компьютеру с целью изменения параметров его работы или версии встроенного прикладного ПО.

Бортовое оборудование должно обеспечивать выполнение следующих основных функций:

определение НП по сигналам системы ГЛОНАСС или ГЛОНАСС/GPS;

передачу НП в ЦМ и (или) их запись во внутреннюю энергонезависимую память через заданный оператором ЦМ промежуток времени (от 1 до 3600 секунд), расстояния (от 10 до 1000 метров), угла поворота (от 10 до 180 градусов);

ежесекундный подсчет пробега ТС, а также его передачу в ЦМ и сохранение в энергонезависимой памяти;

формирование и передачу в ЦМ и (или) запись во внутреннюю энергонезависимую память информации о текущем состоянии в соответствии с параметрами выбранного режима работы;

контроль состояния подключенных шлейфов сигнализации;

прием и выполнение команд, поступающих из ЦМ;

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

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

подключение элементов управления, обеспечивающих идентификацию водителя (считыватель пластиковых карт, Touch Memory и т. п.);

формирование и передачу в ЦМ текстовых сообщений и формализованных извещений;

прием, обработку и отображение текстовых сообщений и команд, поступающих из ЦМ;

передачу фото или видеоизображений с места нахождения ТС в ЦМ;

удаленный доступ к информационным базам данных;

согласованность с ЕИТКС–К.

Бортовое оборудование должно обеспечивать первое определение навигационных параметров при «холодном» старте за время не более 120 секунд.

Бортовое оборудование должно сохранять работоспособность при напряжении питания от 10,8 до 30 V. Мощность, потребляемая ТМ, не должна превышать 5 Вт (в «спящем» режиме — не более 0,5 Вт).

Бортовое оборудование должно иметь разъём для подключения к бортовой сети и защиту от изменения полярности при подключении к источнику электропитания.

Бортовое оборудование должно иметь защиту от повреждения в случае короткого замыкания или заземления на корпус антенных входов или любых входных/выходных портов на время до 5 минут, а также в случае отключения антенн.

ТМ должен иметь внутренний (встроенный) резервный источник электропитания. Время автономной работы ТМ в активном режиме от

внутреннего резервного источника электропитания должно составлять не менее 2 часов.

Все сообщения, передаваемые бортовым оборудованием в ЦМ, должны быть синхронизированы со временем в координированной шкале времени UTC(SU) с погрешностью не более 0,01 секунды. При отсутствии приема сигнала с навигационных спутников должна быть предусмотрена возможность работы от внутренних часов ТМ (время работы от внутренних часов — не менее 24 часов).

Бортовое оборудование в различных вариантах исполнения должно обеспечивать:

передачу информации по каналам конвенциальной радиосвязи с использованием УКВ-радиостанций, принятых на снабжение в МВД России;

поддержку цифровых транковых сетей;

передачу информации по каналам GSM, CDMA (с использованием технологий передачи данных GPRS, EV-DO, SMS, Data-call), и другим каналам связи.

В бортовом оборудовании должна быть возможность передачи тревожных извещений по любому доступному каналу связи. В случае если тревожное извещение не доставлено в ЦМ по основному каналу связи, оно должно отправляться последовательно по остальным имеющимся каналам связи.

Бортовое оборудование должно обеспечивать возможность подключения не менее пяти шлейфов сигнализации и двух исполнительных устройств для выполнения команд из центра мониторинга.

Бортовое оборудование должно обеспечивать определение следующих состояний каждого из шлейфов сигнализации, с формированием и передачей соответствующей информации в ЦМ: «Норма», «Тревога», «Обрыв», «Замыкание на массу», «Замыкание на питание».

Бортовое оборудование должно обеспечивать возможность подключения элементов индикации, оповещающих о текущем режиме работы. При формировании и передаче извещения «Тревога-вторжение» элементы индикации не должны изменять своего текущего состояния.

Бортовое оборудование должно обеспечивать возможность сохранения во внутренней энергонезависимой памяти не менее 8640 последовательно зарегистрированных событий, отражающих его состояние за последние 24 часа.

Сохранение событий во внутренней энергонезависимой памяти должно осуществляться либо автоматически при пропадании связи, либо в соответствии с установками, заданными оператором. Выгрузка содержимого энергонезависимой памяти при восстановлении связи — либо автоматически при восстановлении связи, либо по требованию оператора, с возможностью ручного прерывания процесса выгрузки.

Бортовое оборудование должно обеспечивать возможность считывания содержимого внутренней энергонезависимой памяти путём подключения технологических устройств через специальный разъём или с использованием ближнего радиоканала.

Конструкция бортового оборудования должна обеспечивать возможность скрытного размещения его элементов внутри ТС, защиту от механических и электромагнитных воздействий. При этом должен сохраняться доступ обслуживающего персонала к разъёму для считывания содержимого внутренней энергонезависимой памяти

Конструкция ТМ должна иметь исполнение «всё в одном», то есть плата управления, спутниковый навигационный приёмник, приёмо-передающие устройства (кроме мощных радиопередатчиков), внутренний аккумулятор должны быть интегрированы в один корпус, к которому подключаются питание, антенны, исполнительные устройства и датчики, дисплеи, считыватели магнитных или радиометок, индикаторы и другие внешние устройства.

Конструкция корпуса ТМ должна исключать доступ к SIM-карте и разъёмам снаружи без вскрытия корпуса.

В ТМ для подключения датчиков, исполнительных устройств и электропитания должны использоваться разъёмы, в которых контакты разделены диэлектрическими перегородками.

ТМ должен поддерживать запрос PIN-кода SIM–картой и его автоматический ввод (после предварительного программирования ТМ) в целях защиты от несанкционированного использования SIM–карты.

Бортовое оборудование должно обеспечивать электромагнитную совместимость и устойчивость к воздействию электромагнитных помех в соответствии с требованиями действующих в Российской Федерации стандартов.

Бортовое оборудование должно удовлетворять требованиям назначения при воздействии климатических факторов для исполнения умеренного и холодного климата и соответствующей категории размещения по ГОСТ 15150-69 и ГОСТ 16019-2001. Диапазон рабочих температур для блоков, работающих в сетях сотовой связи, должен составлять не менее чем от –25 до +55 ^{o}C, для блоков, работающих с использованием штатных радиостанций — не менее чем от –40 до +55 ^{o}C.

Бортовое оборудование должно удовлетворять требованиям назначения после воздействия механических факторов в условиях транспортирования Ж по ГОСТ 23216-78.

Конструкция составных частей бортового оборудования должна обеспечивать защиту от попадания внутрь твердых тел (пыли) и (или) от попадания внутрь воды. Степень защиты оболочек частей бортового оборудования должна быть не хуже степени IP 51 в соответствии с ГОСТ 14254-96.

Бортовое оборудование должно удовлетворять требованиям безопасности по ГОСТ Р МЭК 60065-2005.

Габаритные размеры корпуса ТМ должны быть не более (Ш х В х Г) — 188х58х166 миллиметров.

Масса ТМ должна быть не более 1600 грамм.

3.6.1.7 Требования к документации на подсистему.

Спутниковая навигационно-мониторинговая система и оборудование должны иметь следующую документацию (на русском языке):

технические условия;

руководство по эксплуатации — документ, содержащий сведения о конструкции, принципе действия, характеристиках (свойствах) изделия и его составных частей, программного обеспечения, указания по правильной и безопасной эксплуатации изделия (использования по назначению, технического обслуживания, текущего ремонта, хранения и транспортирования), оценке его технического состояния для определения необходимости отправки в ремонт, а также сведения по утилизации изделия и его составных частей;

паспорт — документ, содержащий сведения, удостоверяющие гарантии изготовителя, значения основных параметров и характеристик (свойств) изделия, а также сведения о сертификации и утилизации изделия;

формуляр (по специальному заказу, взамен паспорта) — документ, имеющий формализованные поля для отражения сведений о хранении, закреплении и движении аппаратуры при эксплуатации, учёта работы по годам, технического обслуживания и неисправностей, сведений об установленной категории, о ремонте, об изменениях в конструкции аппаратуры и её основных частях во время эксплуатации и ремонта, сведений о результатах проверки инспектирующими лицами.

3.7 Подсистема видеофиксации нарушений правил дорожного движения и скоростного режима

Подсистема видеофиксации нарушений правил дорожного движения предназначена для автоматической фиксации нарушений правил дорожного движения, скоростного режима на улицах города и его окрестностях, регистрации государственных регистрационных знаков транспортных средств, проверки их по базам данных, передачи полученных данных в ЦМ и ЛЦМ ГИБДД УВД для анализа и принятия решений.

Места установки и тип оборудования согласуются с Заказчиком на стадии проектирования.

Подсистема должна обеспечивать следующие функции:

- контроль дорожной обстановки и автоматическое детектирование фактов нарушений ПДД: превышение разрешенного скоростного режима,

выезд на встречную полосу, движение задним ходом, проезд на запрещающий сигнал светофора, нарушение пропускного режима, другие нарушения, тип (типы) нарушения ПДД, фиксируемых комплексами в составе системы, определяются исходя из реальных условий организации движения в зонах контроля. Возможность фото- видео фиксации факта нарушения ПДД не менее чем с двух точек обзора;

- фотофиксация и считывание номерных знаков ТС, попавших в зону контроля;

- фотофиксация распознанного номерного знака ТС, нарушившего ПДД;

- комплексная проверка движущегося транспортного средства на предмет его розыска, а также на предмет запрета эксплуатации по причине непройденного техосмотра;

- оперативная передача информации о нарушителе (карточка нарушения), розыске транспортного средства и его документов, а также запрете эксплуатации транспортного средства на АРМ;

- распечатка карточки нарушения, содержащей информацию о владельце ТС и фото (видео) фрагментов нарушения с указанием адреса расположения оборудования на стационарном АРМ (форма карточки согласовывается с УГИБДД УВД);

- система должна быть построена на основе масштабируемых технологических решений, должна обеспечивать увеличение количества комплексов фиксации, АРМ, ЦУП, работающих в составе системы;

- централизованное администрирование системы и архивирование информации в ЦМ и УГИБДД УВД;

- контроль и управление доступом в систему с регистрацией всех обращений пользователей, защиту информации от несанкционированного доступа и стирания;

- бесперебойное функционирование 24 часа в сутки, возможность дистанционного проведения профилактического обслуживания элементов системы.

3.8 Подсистема защиты информации

Под подсистемой защиты информации понимается система технических, организационных и других мер, направленных на обеспечение информационной безопасности.

Подсистема защиты информации обеспечивает решение следующих задач:

- защита информации от несанкционированного доступа;

- защита циркулирующей информации от преднамеренных воздействий с целью нарушения целостности при передаче по каналам связи;

- защита от проникновения компьютерных вирусов;

- ввод и проверка электронной подписи для идентификации информации;

- контроль целостности программного обеспечения и данных, защищенности конфигурации ресурсов;

- обеспечение сохранности, достоверности, полноты и актуальности к обрабатываемой хранимой информации (целостности информации);

- обеспечение резервного копирования, восстановления данных и программного обеспечения;

- контроль и мониторинг конфигурации (изменений и модификаций) программно-технических средств;

- управление доступом, включая аппаратно-программные средства и решения;

- разграничение доступа к ресурсам, сегментам и ЛВС, взаимодействующих с подсистемами;

- аутентификация и авторизация пользователей;

- администрирование пользователей, управление и хранение учетных данных о пользователях;

- анализ передаваемой информации;

- регистрация и учёт активности пользователей и программного обеспечения;

- контекстный контроль и архивирования передаваемой информации;

- распределение программного обеспечения, мониторинг работоспособности и управления компонентами и подсистемами;

- криптографическая защита, включая контроль целостности информации, контроль и проверка электронной цифровой подписи.

Комплекс организационно - режимных мероприятий, документированных процедур, программных и технических средств защиты, а также технологий их применения определяются политикой информационной безопасности в соответствии с моделью угроз и нарушителя.

Подсистема не подключается ни на аппаратном, ни на программном уровне к другим компьютерным сетям общего пользования без применения сертифицированных по требованиям информационной безопасности средств защиты информации в соответствии с требованиями Указа Президента РФ № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена».

При создании подсистемы используются только сертифицированные ФСТЭК России средства защиты информации, а в случае применения криптографических средств защиты, сертифицированные так же ФСБ России.

Защита информации при работе с другими подсистемами.

При работе с другими подсистемами необходимо предусмотреть:

- защиту каналов передачи данных от нарушения конфиденциальности и целостности передаваемой информации;

- создание защищенного узла доступа к серверным, пользовательским и иным информационным ресурсам за счет строгой двухфакторной

аутентификации по цифровым сертификатам на основе российских сертифицированных криптографических алгоритмов;

- обеспечение гарантии авторства документов, файлов, сообщений и их неотказуемости за счет встраивания российских криптографических алгоритмов электронной цифровой подписи в системы обмена и распределения информации и управления потоками работ;

- разграничение доступа к данным информационно-справочных и аналитических систем средствами сертифицированными по требованиям информационной безопасности СУБД.

Каналы передачи данных сетей общего пользования необходимо защищать с использованием средств криптозащиты. Средства криптозащиты имеют гарантированную стойкость, необходимые сертификаты и предписания для обеспечения полной совместимости на уровне форматов ключей шифрования, сертификатов электронной цифровой подписи, служебных команд территориально-распределенных систем безопасности. Для этого используются средства криптографической защиты, применяемые в Единой системе информационной безопасности (ЕСИБ) ЕИТКС МВД России.

Тип аппаратуры криптозащиты определяется уполномоченными подразделениями МВД России.

Категорирование, техническая паспортизация и аттестация подсистемы для обсуждения и обработки информации различной степени секретности производятся в рамках аттестации подсистемы по требованиям информационной безопасности в целом на этапе создания или ввода подсистемы или отдельных составляющих в эксплуатацию.

Перечень необходимых мер защиты информации может быть определен по результатам предварительного обследования объекта защиты, специальных проверок (СП) и специальных исследований (СИ) технических средств, инструментальных объектовых исследований на этапе аттестационных испытаний.

Все мероприятия по защите информации должны быть согласованы с Заказчиком.

4. Общие требования к системе

Система должна обеспечивать:

- широкие возможности интеграции, способность объединить в единый комплекс системы, оборудование и приборы различных производителей;

- централизованный, удаленный контроль и управление;

- способность масштабирования. Возможность расширения и модернизации;

- эффективность, надежность, устойчивость и бесперебойность работы

системы в круглосуточном режиме.

4.1. Требования к численности и квалификации персонала

Рекомендуемая численность персонала, необходимого для обеспечения круглосуточной эксплуатации системы видеонаблюдения, и требования к уровню его квалификации должны определяться Подрядчиком и Заказчиком на этапе проектирования.

Штатная численность персонала определяется и обеспечивается Заказчиком с учетом проектных рекомендаций Подрядчика.

Первичная подготовка и обучение персонала эксплуатации и использованию средств системы видеонаблюдения должны осуществляться до ввода системы в опытную эксплуатацию, на этапе монтажа системы, Подрядчиком, в рамках заключенного с Заказчиком договора.

Последующая подготовка и обучение персонала организуется Заказчиком.

Допуск персонала к самостоятельной эксплуатации (использованию) средств системы видеонаблюдения, а также текущий контроль знаний и навыков персонала, осуществляется Заказчиком.

Требования по численности и квалификации персонала могут быть уточнены в ходе проектирования и создания системы.

4.2. Требования к надежности

Надежность системы должна обеспечиваться на основе:

- применения высоконадежного и отказоустойчивого оборудования;

- принятия специальных технологических решений, включая резервирование, обеспечивающих высокую отказоустойчивость и живучесть наиболее ответственных и жизненно важных систем;

- применения унифицированных технических средств, как в рамках отдельных систем, подсистем и комплексов, так и системы в целом;

- наличием ЗИП достаточной комплектности.

Надежность кабельных систем должна обеспечивать требования нормативно-технических документов по пожаростойкости и пожаробезопасности и соответствовать международным стандартам.

Надежность системы электропитания должна обеспечиваться применением системы бесперебойного питания, кроме того, все основные элементы системы должны быть защищены своими локальными источниками бесперебойного питания, способными автономно поддерживать их нормальный режим работы.

Надежность активного оборудования ЛВС должна обеспечиваться выполнением следующих требований:

- обеспечения возможности замены в «горячем» режиме всех

интерфейсных модулей и блоков питания центрального коммутатора;

- поддержка коммутаторами технологий резервирования линий - STP (IEEE 802.1d), HSRP, Ether Cannel;

- применение системы управления ЛВС, позволяющей, в том числе, проводить оперативный контроль за работой активных компонент ЛВС и ее компонентов;

- дублирование каналов связи между основными узлами.

Повышение надежности серверов должно обеспечиваться за счет:

- применения внутренних RAID-контроллеров или внешних дисковых массивов данных с реализацией аппаратного или программного RAID;

- применения резервных источников питания по схеме N+1;

- применения ПО для ИБП, позволяющего информировать о неисправности сети электропитания;

- применения удалённой диагностики и управления серверами с одной или нескольких специализированных рабочих станций, служащих единой серверной консолью;

- использования технологии «горячей» замены компонента;

- организации кластеров или установки систем высокой доступности для хранения особо важных сетевых данных;

- применения сетевых операционных систем, обеспечивающих высокую доступность, надёжность и масштабируемость решений, позволяющих минимизировать плановые и внеплановые простои и подключать новые компоненты серверов или внешние устройства без перезагрузки системы;

- применения программ для резервного копирования и архивирования особо важных данных и соответствующих аппаратных решений.

Системы должны обеспечивать показатели надежности в соответствии с ГОСТ 27.002 «Надежность в технике. Основные понятия. Термины и определения» и ГОСТ 27.003 «Надежность в технике. Состав и общие правила задания требований по надежности».

Требования к надежности системы при проектировании должны быть регламентированы для отказов оборудования.

На всех стадиях пусконаладочных работ и испытаний системы должен проводиться анализ отказов и неисправностей системы.

При проектировании системы должны быть реализованы требования по надежности в случае отключения электропитания от промышленной сети, а также требования по восстановлению работоспособности в случае выхода из строя аппаратно-технических или программных средств.

Отказом системы (элемента системы) должен считаться случай, когда система (элемент системы) не в состоянии выполнять свои функции.

Наиболее критичные при отказах аппаратно-технические и программные средства системы должны быть резервированы, в соответствии с требованиями Заказчика по такому резервированию. Объем резерва определяется Заказчиком на этапе проектирования системы и согласовывается с Разработчиком.

Требования к надежности могут быть уточнены в ходе проектирования.

4.3. Требования по безопасности

Комплекс систем должен удовлетворять общим требованиям безопасности по ГОСТ 12.2.007.0 «Изделия электротехнические. Общие требования безопасности» и ГОСТ 12.2.006 «Безопасность аппаратуры электронной сетевой и сходных с ней устройств, предназначенных для бытового и аналогичного общего применения. Общие требования и методы испытаний».

Монтаж и эксплуатация ТС, требующих электропитания, должны отвечать требованиям безопасности по ГОСТ 12.2.003 «Оборудование производственное. Общие требования безопасности».

Система должна удовлетворять общим требованиям пожарной безопасности по ГОСТ 12.2.006.

Уровни излучений системы должны соответствовать нормам и требованиям безопасности, установленным ГОСТ 12.1.006 «Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля», ГОСТ 12.1.040.

При проектировании и создании системы видеонаблюдения должны быть обеспечены требования по безопасности при монтаже, наладке, эксплуатации, обслуживании и ремонте аппаратно-технических средств системы, включая защиту от воздействий электрического тока, электромагнитных полей, акустических шумов и др., а также требования по допустимым уровням освещенности, вибрационных и шумовых нагрузок, при необходимости.

Требования по обеспечению безопасности при наладке, эксплуатации, обслуживании и ремонте аппаратно-технических средств системы должны быть изложены в соответствующей эксплуатационно-технической документации, разрабатываемой исполнителями на создаваемые подсистемы.

Все технические средства ПГВН должны быть сертифицированы на предмет соответствия обязательным требованиям по безопасности. Система сертификации ГОСТ Р:

- ГОСТ Р МЭК 60950-2002 «Безопасность оборудования информационных технологий»;

- ГОСТ Р 51318.22-99 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационных технологий»;

- ГОСТ Р 51318.24-99 «Совместимость технических средств электромагнитная. Устойчивость оборудования информационных технологий к электромагнитным помехам»;

- ГОСТ Р 51317.3.2-99 «Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам»;

- ГОСТ Р 51317.3.3-99 «Совместимость технических средств электромагнитная. Колебания напряжения и фликер, вызываемые техническими средствами, подключаемыми к низковольтным системам электроснабжения»;

- ГОСТ 26329-84 «Машины вычислительные и системы обработки данных. Допустимые уровни шума технических средств и методы их определения».

Требования по безопасности могут быть уточнены в ходе проектирования и создания системы.

4.4. Требования по эргономике и технической эстетике

По эргономике и технической эстетике система должна соответствовать ГОСТ 30.001-83 «Система стандартов эргономики и технической эстетики. Основные положения».

Рабочие места должны обеспечивать возможность непрерывной работы операторов в течение смены в соответствии с требованиями СанПИН 2.2.2.542 «Гигиенические требования к видеодисплейным терминалам и персональным ЭВМ и организация работ» от 14.07.1996 г.

Терминальные средства должны обеспечивать деятельность в условиях внешней освещенности экрана, уровней акустических шумов и вибраций в помещениях и параметров микроклимата в соответствии с санитарно-гигиеническими требованиями.

Места для отдыха операторов дежурной смены предусматриваются Заказчиком.

АРМ системы видеонаблюдения, их компоновка и размещение должны обеспечивать удобство и комфортность работы персонала в круглосуточном режиме, при дневном и искусственном освещении, с учетом специфики помещений, в которых они размещаются.

Места размещения АРМ и другого оборудования системы видеонаблюдения определяет Заказчик на этапе проектирования системы и выдает соответствующие исходные данные Подрядчику.

Стационарные аппаратно-технические средства системы видеонаблюдения, их монтаж и размещение в помещениях должны обеспечивать удобство их эксплуатации, обслуживания и ремонта

персоналом, с учетом специфики помещений, в которых они размещаются.

Освещение, кондиционирование и вентиляцию помещений, в которых размещаются средства системы видеонаблюдения обеспечиваются Заказчиком.

Требования по эргономике и технической эстетике могут быть уточнены в ходе проектирования и создания системы.

4.5. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению

Система должна быть рассчитана на длительную непрерывную круглосуточную работу с короткими перерывами на техническое обслуживание.

Аппаратно-технические средства системы должны обслуживаться в соответствии с эксплуатационно-технической документацией, разрабатываемой Подрядчиком.

Состав эксплуатационно-технической документации должен соответствовать требованиям ГОСТ 2.601-95 «Эксплуатационные документы». Объем документации согласовывается на этапе проектирования системы.

Эксплуатация системы должна осуществляться персоналом Заказчика (Пользователя, в том числе органы внутренних дел), прошедшим необходимую подготовку. При необходимости, к эксплуатации могут привлекаться Подрядчик или специализированные организации на основе договоров, заключаемых с Заказчиком.

Подготовка персонала системы должна осуществляться на этапе создания системы, до ввода ее в опытную эксплуатацию. Первичную подготовку персонала организует Заказчик в рамках договора с Подрядчиком. В дальнейшем подготовку персонала в период эксплуатации системы и контроль уровня его подготовленности осуществляет Заказчик.

Требования к количеству и уровню подготовки персонала для системы должны определяться в проектной документации.

Кадровое обеспечение системы необходимым персоналом осуществляет Заказчик.

Гарантийное и техническое обслуживание системы в период гарантийного срока организует Подрядчик, послегарантийное и сервисное - Заказчик.

Вопросы финансирования эксплуатации системы, включая послегарантийное и сервисное обслуживание, решаются Заказчиком.

Состав ЗИП для обеспечения эксплуатации системы согласовывается Заказчиком на этапе проектирования системы.

Стационарные средства системы должны быть рассчитаны на эксплуатацию и хранение в отапливаемых помещениях.

Стационарные средства системы, устанавливаемые вне помещений (камеры, приемопередающие устройства), должны быть рассчитаны на

эксплуатацию в условиях воздействия окружающей среды (температура –40°С/+50°С, влажность до 100%).

Требования по эксплуатации, техническому обслуживанию, ремонту и хранению могут быть уточнены в ходе проектирования.

4.6. Требования по обеспечению информационной безопасности

При создании системы должны быть выполнены в необходимом объеме требования Заказчика по обеспечению информационной безопасности, в соответствии с действующим законодательством Российской Федерации.

Организационно-технические меры, обеспечивающие защиту хранящейся в базах данных системы информации от несанкционированного доступа, разрабатываются при проектировании.

В системе должно обеспечиваться сохранение и восстановление информационных массивов.

В системе должна обеспечиваться защита данных от разрушения при авариях и сбоях в системе электропитания.

При проектировании системы должны быть предусмотрены меры по защите оборудования и программного обеспечения от ошибочных действий персонала.

Требования по электронной защите системы определяются, при необходимости, Заказчиком, в соответствии с нормативно-технической документацией, действующей в системе МВД России.

Аудит безопасности проектируемой комплексной системы обязателен при участии профильных подразделений ФСБ России.

Требования по обеспечению информационной безопасности могут быть уточнены в ходе проектирования и создания системы.

4.7. Требования по обеспечению патентной чистоты

При создании системы должна быть обеспечена патентная чистота в отношении Российской Федерации и государств СНГ, в соответствии с действующим законодательством Российской Федерации.

Программное обеспечение, распространяемое на основе лицензий производителей, используемое в системе, должно иметь соответствующие лицензии, приобретенные в установленном порядке.

Требования по обеспечению патентной чистоты могут быть уточнены в ходе проектирования.

4.8. Требования к стандартизации и унификации

При создании системы должны приниматься к руководству действующие в Российской Федерации стандарты, а также отраслевые

стандарты МВД России, в части, не противоречащей действующему законодательству Российской Федерации.

Технические средства, используемые при создании системы, должны использовать стандартные электрические стыки, интерфейсы, технологии и протоколы передачи данных.

Технические средства, используемые при создании системы, подлежащие обязательной сертификации и/или декларированию соответствия в соответствии с действующим законодательством Российской Федерации, должны иметь соответствующие сертификаты и/или декларации о соответствии.

Технические средства, используемые при создании системы, должны быть сертифицированы в системе сертификации вооружения, военной и специальной техники МВД РФ.

Технические средства, используемые при создании системы должны иметь заключение ЭКЦ МВД РФ о проведении апробации оборудования и вывод о пригодности аудиовизуальных материалов, получаемых с оборудования для проведения криминалистических экспертиз.

Требования к стандартизации и унификации могут быть уточнены в ходе проектирования и создания системы.

4.9. Дополнительные требования

Обучение персонала должно производиться с использованием эксплуатационно-технической документации производителей оборудования, а также, разрабатываемой Исполнителем.

Требования к оснащению системы устройствами для обучения персонала и документацией на них могут быть уточнены в ходе проектирования.

В составе системы должны быть предусмотрены (при необходимости) сервисная аппаратура для проверки элементов системы в объеме, обеспечивающем ее техническое обслуживание и ремонт.

Конкретный состав сервисной аппаратуры для проверки элементов системы определяется на этапе проектирования.

4.10. Требования к системе, связанные с особыми условиями эксплуатации

При проведении работ по развертыванию правоохранительного сегмента системы обеспечения общественной безопасности города необходимо обеспечить участие представителей органов внутренних дел не только в межведомственных комиссиях по приемке работ, но и на начальных стадиях, в том числе при проектировании, выработке технических решений, разработке тактико-технических требований к закупаемой аппаратуре, оборудованию доставки и обработки информации. Представителям органов внутренних дел на местах целесообразно

выступать не только в качестве пользователей, но и в качестве технических экспертов предполагаемых работ.

В целях реализации единой технической политики в органах внутренних дел закупка оборудования для оснащения объектов должна осуществляться согласно перечня технических средств, принятых на снабжение органов внутренних дел и внутренних войск или прошедшие соответствующие сертификационные испытания.

Техническое регулирование

Контроль за реализацией общих требований к создаваемым в УВД аппаратно - программным комплексам технических средств контроля за состоянием правопорядка на улицах, объектах транспорта, в других общественных местах осуществляет УССиА УВД, а также ГУ НПО «СТиС» МВД России в соответствии с приказом МВД РФ от 16.08.2007 г. №731, п. 18.2.

В соответствии с приказом МВД РФ от 16.08.1999 г. № 609 на ГУ НПО «СТиС» МВД России возложено решение вопросов в части проведения испытаний и сертификации указанных видов техники для органов внутренних дел.

Вопросы участия в организации и проведении работ по созданию новых и модернизации существующих технических средств обеспечения безопасности дорожного движения, разработке требований и других нормативных документов, также выполнение функций Технического комитета по стандартизации (ТК-278) «Безопасность дорожного движения», а также органа по сертификации в сфере обеспечения безопасности дорожного движения возложены на НИЦ БДД МВД России.

Вопросы выработки новых подходов к организации охраны имущества физических и юридических лиц, разработки рекомендаций и методических пособий по вопросам организации и осуществления государственной защиты имущества, создания средств охранной сигнализации, а также принятия мер по внедрению новых охранных технологий в деятельность органов внутренних дел и внутренних войск возложены на ФГУ НИЦ «Охрана» МВД России.

Вопросы организационно-методического руководства экспертно-криминалистическими центрами в системе МВД России, а так же непосредственное использование технико-криминалистических средств и методов в предупреждении, раскрытии и расследовании преступлений, в том числе проведение экспертиз и исследований; организация, проведение и координация прикладных научных исследований в области экспертно-криминалистической деятельности возложены на ЭКЦ МВД России.

Вопросы сертификации аппаратуры охранно-пожарной сигнализации возложены на Центр сертификации аппаратуры охранно-пожарной сигнализации МВД России (ЦСА ОПС МВД России).

В связи с осуществлением эксплуатации системы, силами специализированных организаций, привлекаемых на договорной основе,

Заказчиком должны быть проработаны вопросы по своевременному заключению необходимых договоров с привлекаемыми специализированными организациями.

Помещения и места для размещения оборудования в ходе создания системы обеспечиваются Заказчиком.

Требования к системе, связанные с особыми условиями эксплуатации, могут быть уточнены в ходе проектирования и создания системы.

4.11. Требования к видам обеспечения

4.11.1. Информационное обеспечение

Должны быть разработаны классификаторы технико-экономической информации, нормативно-справочная информация, форма представления и организации данных в системе, в том числе формы документов, массивов и логические интерфейсы (протоколы обмена данными).

4.11.2. Программное обеспечение

Должны быть разработаны программы, необходимые для реализации всех функций системы в объеме, предусмотренном техническим заданием. Максимально должны быть использованы существующие программные продукты, необходимые для реализации всех функций системы в объеме, предусмотренном техническим заданием.

4.11.3. Техническое обеспечение

Должны быть разработаны комплексы технических средств, необходимые для реализации функций системы: средства получения, ввода, подготовки, обработки, хранения (накопления), регистрации, вывода, отображения, использования, передачи информации и средства реализации управляющих воздействий.

4.11.4. Организационное обеспечение

Должны быть разработаны документы, определяющие функции подразделений управления, действия и взаимодействие персонала системы.

4.11.5. Правовое обеспечение

Должны быть разработаны нормативные документы, определяющие правовой статус системы и персонала, правил функционирования системы и нормативы на автоматически формируемые документы, в том числе на машинных носителях информации.

Требования к видам обеспечения могут быть доработаны в ходе

проектирования и создания системы.

5 СОСТАВ И СОДЕРАЖНИЕ РАБОТ ПО СОЗДАНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Состав и содержание работ определяется в соответствии с ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы» Часть 5 «Состав и содержание работ по созданию системы».

По согласованию Сторон отдельные этапы и стадии могут быть исключены, добавлены либо в них могут быть внесены корректировки.

5.1. Сроки выполнения работ.

Стадия	Содержание работ	Исполнитель	Отчетность

5.2. Перечень организаций исполнителей работ

Определяется путем проведения открытого конкурса (аукциона).

5.3. Перечень документов, предъявляемых по окончании соответствующих стадий и этапов работ

Перечень документов, предъявляемых по окончании соответствующих стадий и этапов работ, определяется на этапе создания рабочего проекта при согласовании с Заказчиком и в соответствии с требованиями ГОСТ 34.201-89.

5.4. Вид и порядок проведения экспертизы технической документации

Стадия, этап, объем проверяемой документации, организация экспертиз согласовываются Заказчиком совместно с Подрядчиком.

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

По завершении работ Исполнитель предоставляет Заказчику утвержденный рабочий проект и другую исполнительную документацию. Разработка проектных решений системы и его частей должно осуществляться в соответствии с данным техническим заданием и исходными данными, предоставляемыми Заказчиком. В случае необходимости представители Исполнителя проводят обследование объекта с участием представителей Заказчика. Результаты проведенного обследования фиксируются в протоколе, подписываемом представителями Заказчика и Исполнителя.

Исполнитель разрабатывает рабочий проект и передает его Заказчику в ___ экземплярах.

Заказчик рассматривает предоставленный Исполнителем рабочий проект и утверждает его либо передает Исполнителю замечания к рабочему проекту.

При наличии замечаний рабочий проект должен быть доработан Исполнителем с учетом замечаний Заказчика в согласованные с Заказчиком сроки.

7. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

При создании рабочего проекта допускается объединение и разбиение документации в один или несколько томов для нескольких систем и подсистем. Каждый том проекта должен содержать следующие документы:

- пояснительную записку;
- рабочие чертежи основного комплекта;
- таблицы соединений и подключений (для отдельных систем);
- спецификацию оборудования, изделий и материалов.

Перечень документации, а также её содержание должны учитывать требования ГОСТ систем СПДС и ЕСКД.

Документация на систему и входящие в него системы должна быть передана Заказчику в двух экземплярах – один в виде альбомов и книг, второй на магнитных носителях.

8. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

Дополнения, уточнения или изменения к настоящему ТЗ могут вноситься по согласованию сторон и должны оформляться в виде частных технических заданий (ЧТЗ). ЧТЗ являются неотъемлемой частью

настоящего технического задания.