УТВЕРЖДАЮ
Глава муниципального образования
ЗАТО г. Североморск

_____ А.П. Абрамов

«___» _____ 2015 г.

УТВЕРЖДАЮ
ВрИО директора Североморского
муниципального казенного учреждения
«Единая дежурно-диспетчерская служба»

_____ А.А. Поляков

«___» _____ 2015 г.

АПК «БЕЗОПАСНЫЙ ГОРОД»

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «ЕДИНЫЙ ЦЕНТР ОПЕРАТИВНОГО РЕАГИРОВАНИЯ»

(ПАК ЕЦОР)

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

№ 1

на выполнение работ по проектированию АПК «Безопасный город»
программно-аппаратного комплекса «Единый центр оперативного реагирования»

(ПАК ЕЦОР)

На 85 листах

СОГЛАСОВАНО

ВрИО начальника Главного управления
МЧС России по Мурманской области

_____ А.В. Фролов

«___» _____ 2015 г.

СОГЛАСОВАНО

Председатель Комитета по обеспечению
безопасности населения
Мурманской области

_____ В.М. Воротников

«___» _____ 2015 г.

Общие сведения

1.1 Полное наименование системы и ее условное обозначение

Полное наименование системы: Программно-аппаратный комплекс «Единый центр оперативного реагирования», создаваемый на базе единой дежурно-диспетчерской службы.

Условное обозначение системы: ПАК ЕЦОР (далее – Система, Комплекс).

1.2 Шифр темы или шифр (номер) договора:

Шифр темы: ПАК ЕЦОР.

1.3 Наименование предприятий (объединений) разработчика и заказчика (пользователя) системы и их реквизиты

1.4 Перечень документов, на основании которых создается система, кем и когда утверждены эти документы

- Постановление Правительства РФ от 08.09.2010 N 697 (ред. от 19.03.2014) "О единой системе межведомственного электронного взаимодействия".
- Постановление Правительства Российской Федерации от 25 августа 2008 года № 641 "Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS".
- Указ Президента Российской Федерации от 28 декабря 2010 года № 1632 «О совершенствовании системы обеспечения вызова экстренных оперативных служб на территории Российской Федерации».
- Концепция построения и развития АПК «Безопасный город», утвержденная распоряжением Правительства Российской Федерации от 03.12.2014 г. № 2446-р.
- Постановление Правительства Мурманской области от 16.06.2015 г. № 245-ПП «Об организации и выполнении мероприятий по построению, внедрению и эксплуатации аппаратно-программного комплекса «Безопасный город» на территории Мурманской области».
- Методические рекомендации МЧС России по построению (развитию), внедрению и эксплуатации АПК «Безопасный город» от 22.02.2015 г.
- Распоряжение администрации ЗАТО г. Североморск от 07.05.2015 г. № 569-р «Об организации и выполнении мероприятий по построению, внедрению и эксплуатации на территории ЗАТО г. Североморск аппаратно-программного комплекса «Безопасный город».

1.5 Плановые сроки начала и окончания работ по созданию проекта

Плановый срок начала работ: 1-2 квартал 2016 года.

Плановый срок окончания работ: 3-4 квартал 2016 года.

1.6 Сведения об источниках и порядке финансирования работ

Источник финансирования: бюджет муниципального образования.

Порядок финансирования: в соответствии с условиями договора _____от_____ между _____ и Североморским муниципальным казенным учреждением «Единая дежурно-диспетчерская служба» (Далее СМКУ «ЕДДС»).

1.7 Порядок оформления и предъявления заказчику результатов работ

Порядок оформления и предъявления Заказчику результатов работ по созданию проекта ПАК ЕЦОР, должен в целом соответствовать требованиям комплекса стандартов и руководящих документов на автоматизированные системы:

- ГОСТ 34.003-90;
- ГОСТ 34.201-89;
- ГОСТ 34.602-89;
- ГОСТ 34.601-90;
- РД 50-34.698-90.

2 Назначение и цели создания (развития) системы

2.1 Назначение системы

ПАК ЕЦОР предназначен для построения и развития АПК «Безопасный город» в части обеспечения безопасности среды обитания и общественной безопасности.

2.2 Цели создания системы

Целями создания ПАК ЕЦОР являются:

- предупреждение кризисных ситуаций за счет внедрения систем анализа и мониторинга данных от различных существующих и перспективных систем и оконечных устройств;
- увеличение скорости реагирования при выполнении мероприятий по экстренному предупреждению и ликвидации кризисных ситуаций;
- улучшение координации оперативного взаимодействия всех дежурных, диспетчерских служб за счет интеграции соответствующих систем в единое информационное пространство.

ПАК ЕЦОР предназначен для решения следующих основных задач:

- сбор и обработка данных различных источников информации (системы мониторинга и оконечные устройства);
- оперативная оценка, анализ и прогнозирование обстановки;
- своевременная поддержка процессов принятия управленческих решений по экстренному предупреждению и ликвидации кризисных ситуаций;
- интеграция существующих и перспективных федеральных, региональных и муниципальных информационных систем, обеспечивающих безопасность жизнедеятельности населения;
- оказание информационной поддержки соответствующим службам для обеспечения экстренной помощи населению при угрозах жизни и здоровью, уменьшения социально-экономического ущерба при чрезвычайных происшествиях и чрезвычайных ситуациях;
- создание единой интеграционной платформы с возможностью подключения и управления широким спектром оконечных устройств (видеокамер, датчиков и т.д.);
- информирование граждан о событиях и результатах реагирования .

3 Характеристика объекта автоматизации

3.1 Краткие сведения об объекте автоматизации

Объектом автоматизации является управленческая деятельность единой дежурно-диспетчерской службы (ЕДДС) и информационное взаимодействие ЕДДС с ведомственными и отраслевыми дежурно-диспетчерскими службами (ДДС).

В соответствие с “Положением о единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций (РСЧС)” (в редакции постановления Правительства Российской Федерации от27.05.2005 №335) ЕДДС является органом повседневного управления РСЧС на местном (муниципальном) уровне.

Основными задачами ЕДДС в соответствие с ГОСТ Р 22.7.01-99 «Безопасность в чрезвычайных ситуациях. Единая дежурно-диспетчерская служба. Основные положения» в настоящее время являются:

- прием от населения любых сообщений о происшествиях, несущих информацию об угрозе или факте возникновения чрезвычайных ситуаций природного и техногенного характера (ЧС), их анализ и оценка достоверности, доведение поступившей информации до ДДС, в компетенцию которых входит реагирование на принятое сообщение, и контроль принятых ими мер;
- сбор от дежурно-диспетчерских служб, систем мониторинга окружающей среды и распространение между ДДС города информации об угрозе или факте возникновения ЧС, требующих совместных действий городских служб;
- обработка и анализ данных о ЧС, определение ее масштаба и состава дежурно-диспетчерских служб, привлекаемых для реагирования на ЧС, их оповещение о переводе в высшие режимы функционирования;
- оценка и контроль обстановки, подготовка вариантов управленческих решений по ликвидации ЧС, принятие необходимых решений (в пределах установленных вышестоящими органами полномочий), доведение задач до ДДС и подчиненных сил постоянной готовности, контроль их выполнения и организация взаимодействия;
- представление докладов (донесений) об угрозе или возникновении ЧС, сложившейся обстановке, возможных вариантах решений и действиях по ее ликвидации ЧС вышестоящим органам управления по подчиненности;
- информирование об обстановке и принятых мерах дежурно-диспетчерских служб, привлекаемых к ликвидации ЧС, подчиненных сил постоянной готовности;
- обобщение информации о произошедших ЧС, ходе работ по их ликвидации и представление соответствующих докладов по подчиненности.

ЕДДС является вышестоящим органом для всех ДДС города по вопросам сбора, обработки и обмена информацией о ЧС, а также координирующим органом по вопросам совместных действий ДДС в чрезвычайных ситуациях.

В рамках дальнейшего развития АПК «Безопасный город» состав задач, решаемых ЕДДС города, должен быть существенно расширен, в первую очередь, в целях обеспечения правоохранительной деятельности и безопасности среды обитания, а также эффективного предупреждения возможных кризисных ситуаций и происшествий (КСП).

При этом основными задачами ЕДДС в АПК «Безопасный город» будут являться:

- сбор и обработка данных (в том числе, данных мониторинга подвижных и стационарных объектов), необходимых для подготовки и принятия управленческих решений по предупреждению и ликвидации КСП, а также контроля их исполнения;
- прогнозирование возникновения и развития КСП на территории города, в том числе, возможных последствий аварий, катастроф и стихийных бедствий;
- оценка уже сложившейся и возможной обстановки на основе сопоставления и анализа всей имеющейся информации, в том числе, результатов прогнозирования с реальными данными, полученными от автоматических (автоматизированных) систем мониторинга, а также от вышестоящих, взаимодействующих и подчиненных организаций;
- подготовка вариантов решений на проведение мероприятий по предупреждению и ликвидации КСП и планирование их реализации, представление городской Администрации подготовленных предложений;
- доведение принятых решений, разработанных планов, сформированных команд (сигналов) до исполнителей, информирование и оповещение заинтересованных вышестоящих и взаимодействующих организаций, а также населения о сложившейся обстановке, выполняемых решениях и ходе проводимых мероприятий;
- контроль исполнения принятых решений и планов мероприятий по их реализации.

Для эффективного решения перечисленных задач ЕДДС должна поддерживать информационное взаимодействие с необходимыми городскими, а также региональными органами управления (как правило, через соответствующие дежурно-диспетчерские службы), в том числе:

- жилищно-коммунального и топливно-энергетического хозяйства;
- транспорта и связи;
- архитектуры и строительства;
- экологического надзора и промышленной безопасности;
- пожарно-спасательной службы и службы скорой медицинской помощи;
- территориальными органами МЧС России, МВД России и ФСБ России.

В рамках АПК «Безопасный город» комплексная информатизация процессов функционирования ЕДДС города во взаимодействии с местными и региональными ДДС должна обеспечить:

- своевременное представление главе Администрации заинтересованным руководителям городских органов управления полной, достоверной и актуальной информации о возникновении любых кризисных ситуаций и происшествий на территории города, оперативную подготовку дежурно-диспетчерскими службами и доведение до исполнителей обоснованных и согласованных предложений для принятия управленческих решений по предупреждению и ликвидации КСП;
- включение органов местного самоуправления, а также муниципальных организаций и предприятий, выполняющих различные задачи по обеспечению безопасности жизнедеятельности, в единое информационное пространство антикризисного управления, эффективное вовлечение региональных управленческих кадров в процессы подготовки и принятия решений по предупреждению и ликвидации КСП на муниципальном уровне;
- улучшение качества принимаемых решений и планов на основе использования аналитических и количественных методов их оценки, многовариантности и оптимизации выбора рационального варианта;
- многократность использования первичной информации, упорядочивание потоков информации, увеличение достоверности и полноты используемых данных на основе их регулярной актуализации по утвержденным регламентам;
- повышение оперативности процессов управления мероприятиями по предупреждению и ликвидации КСП, сокращение общего времени на поиск, обработку, передачу и выдачу информации;
- освобождение должностных лиц управления от рутинной технической работы с бумажными документами;
- обеспечение организационно-методической, информационно-лингвистической и программно-технической совместимости подсистем и компонентов АПК «Безопасный город».

3.2 Сведения об условиях эксплуатации объекта автоматизации и характеристиках окружающей среды

На объектах автоматизации должны отсутствовать такие воздействия, как: механический резонанс, синусоидальная вибрация, механические удары, атмосферное пониженное давление, плесневые грибы, рабочие растворы и агрессивные среды.

Электропитание на стационарных объектах эксплуатации осуществляется от электрической сети напряжением 220В, частотой 50 Гц.

Серверы, активное сетевое оборудование, рабочие станции и АТС должны размещаться в отапливаемых помещениях, в отдалении от отопительных приборов. Отапливаемые помещения должны быть оборудованы системами электроснабжения, связи, отопления, вентиляции и поддержки климатических условий:

- диапазон рабочих температур от +5°С до +35°С;
- относительная влажность до 80% при температуре +25°С;
- запыленность до 0,4 г/м3.

Требования к зданиям и помещениям, в которых располагается оборудование, входящее в состав ПАК ЕЦОР, определяются следующими стандартами:

- РД 45.120-2000 «Нормы технологического проектирования. Городские и сельские телефонные сети. НТП 112-2000, (утверждены Минсвязи РФ 12.10.2000 г.);
- СН 512-78 «Строительные нормы. Инструкция по проектированию зданий и помещений для электронно-вычислительных машин» (утверждены Постановлением Госстроя СССР от 22 декабря 1978 г. №244), (в ред. Изменения №1, утв. Постановлением Госстроя СССР от 27.02.1989 г. №33, Изменения №2, утв. Постановлением Госстроя РФ от 24.02.2000 г. №17).

На объектах ЕДДС МО в соответствии с Приказом Мининформсвязи России от 09.01.2008 г. №1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации» (зарегистрировано в Минюсте РФ 23.01.2008 г. №10993) предусматриваются мероприятия по защите информации для узлов связи I категории защищенности.

3.3 Краткая характеристика имеющихся на территории ЗАТО г. Североморск элементов ПАК ЕЦОР.

На территории ЗАТО г. Североморск в настоящее время установлены следующие элементы, подлежащие включению в единую систему АПК «Безопасный город»**:**

- местная автоматизированная система централизованного оповещения населения (МАСЦО), на базе комплекса П-166М, с возможностью управления с основного пункта управления ЕДДС и запасного пункта управления;

- система видеонаблюдения за обстановкой в общественных местах, местах проведения массовых мероприятий и др. (АПК «Безопасный город»), позволяющая выявлять правонарушения

и преступления, совершаемые в общественных местах и на улицах города, а также лиц их совершивших;

- система видеонаблюдения за дорожной обстановкой (АПК «Безопасность дорожного движения»), позволяющая контролировать дорожную обстановку, включающая в себя комплексы видеофиксации нарушений ПДД (скоростной режим);

- автоматическая система контроля за радиационной обстановкой – АСКРО (принадлежит центру мониторинга и прогнозирования Мурманской области),

- система мониторинга и контроля объектов жизнеобеспечения, позволяющая вести наблюдение за основными параметрами работы котельных МУП «Североморские теплосети» (принадлежит ФКУ «ЦУКС МЧС России по Мурманской области»),

- приобретено и планируется к установке в 2015 году оборудование и программное обеспечение «Технология системы 112».

В ходе разработки проекта ПАК ЕЦОР необходимо провести обследование всех имеющихся (на момент разработки проекта) в ЗАТО г. Североморск систем контроля и мониторинга и предусмотреть их включение в единую систему ПАК ЕЦОР с учетом возможности их дальнейшего масштабирования, наращивания, модернизации и развития.

4 Требования к системе

4.1 Требования к системе в целом

ПАК ЕЦОР является территориально распределенной автоматизированной информационно-управляющей системой. Система должна функционировать в непрерывном круглосуточном режиме и быть в постоянной готовности к обеспечению экстренного реагирования на вызовы от населения и сообщения о происшествиях.

ПАК ЕЦОР должен обеспечивать выполнение следующих функций:

- прием, обработку и переадресацию вызовов на единый телефонный номер (Технология системы «112»);
- обеспечение отображения географического положения источника вызова на электронной карте (Технология системы «112»);
- обеспечение регистрации и документирования всех входящих и исходящих вызовов (Технология системы «112»);
- обеспечение поддержки иностранных языков;
- сбор и аналитическую обработку видеосигнала с камер видеонаблюдения и фото-видеофиксации, предоставление информации на уровень принятия решений по предотвращению и (или) ликвидации последствий чрезвычайных ситуаций;
- сбор и обработку статистических данных, представление информации на уровень принятия решений по предотвращению и (или) ликвидации последствий чрезвычайных ситуаций;
- координацию, управление и поддержку межведомственного взаимодействия при реагировании на поступившие вызовы в ситуациях, требующих участия нескольких экстренных оперативных служб с отображением оперативной ситуации на электронной карте;
- информационное сопряжение с системами мониторинга критически важных объектов, оснащенных датчиками контроля параметров функционирования;
- информирование населения;
- интеграцию данных, необходимых для решения задач ПАК ЕЦОР в единое информационное пространство и обеспечение взаимодействия систем на уровне протоколов, форматов обмена данными.

Указанный функционал должен предоставляться конкретному должностному лицу в соответствии с его обязанностями, для чего должна быть предусмотрена соответствующая система распределения прав доступа.

Должна быть предусмотрена возможность доступности функционала АРМ операторов на АРМ административного и обслуживающего персонала, для чего должен быть предусмотрен гибкий механизм настройки прав доступа к объектам системы, а так же к его функциям.

Система должна иметь модульную структуру, чтобы предоставлять возможность быстрой замены компонент системы (ГИС, телефонии) на компоненты других производителей, а также предусматривать возможность масштабирования при дальнейшем увеличении объектов подлежащих контролю.

Архитектура, функциональные и технические требования ПАК ЕЦОР должны соответствовать положениям Концепции построения и развития аппаратно-программного комплекса “Безопасный город”, разработанной в рамках исполнения поручения Президента Российской Федерации от 27 мая 2014г. NПр-1175. Требуемая функциональность системы в полном объеме должна быть проработана в процессе разработки технического проекта и согласована с Заказчиком.

4.1.1 Требования к структуре и функционированию системы

4.1.1.1 Перечень подсистем, их назначение и основные характеристики

ПАК ЕЦОР должен включать в себя следующие функциональные подсистемы:

1) Подсистема поддержки принятия решений.
2) Подсистема приема и обработки обращений.
3) Подсистема комплексного мониторинга.
4) Интеграционная географическая информационная подсистема.
5) Интернет – портал.
6) Подсистема обеспечения координации и взаимодействия.
7) Подсистема комплексного информирования и оповещения.
8) Подсистема интеграции данных (интеграционная платформа).

В состав ПАК ЕЦОР также должны входить следующие обеспечивающие подсистемы:

1) Подсистема вычислительных комплексов.
2) Транспортная подсистема.
3) Подсистема хранения данных.
4) Подсистема виртуализации.
5) Подсистема резервного копирования и восстановления данных.
6) Подсистема администрирования.
7) Подсистема информационной безопасности.

4.1.1.1.1 Подсистема поддержки принятия решений

Подсистема предназначена для информационно-справочной и аналитической поддержки принятия управленческих решений, формирования аналитической и статистической отчетности.

Данная подсистема должна представлять собой полноценное приложение для интеллектуальной обработки информации, в архитектуру которого включается:

1) Хранилище данных.
2) Модули загрузки и трансформации данных .
3) Модули формирования и визуализации отчетов.

Хранилище данных пополняется данными из оперативных баз Подсистемы приема и обработки обращений. На основе фактических данных строятся различные отчёты и рассчитываются ключевые показатели работы Системы.

4.1.1.1.2 Подсистема приема и обработки обращений

Подсистема приема и обработки обращений предназначена для хранения и актуализации баз данных, обработки информации о полученных вызовах (сообщениях о происшествиях), получения информации о происшествии из архива в оперативном режиме, информационно-аналитической поддержки принятия решений по экстренному реагированию на принятые вызовы (сообщения о происшествиях), планированию мер реагирования.

В состав подсистемы должны входить следующие функциональные компоненты:

1) Компонент маршрутизации и распределения вызовов (в соответствии с технологией «112»).
2) Компонент «Нормативно-справочная информация и база знаний».
3) Компонент консультативного обслуживания.
4) Компонент контроля качества обслуживания.
5) Компонент обучения.

Функциональный компонент маршрутизации и распределения вызовов является функциональной частью Подсистемы приема и обработки обращений и предназначен для управления диспетчеризацией вызовов.

Низкоуровневые функции данной подсистемы, связанные с выполнением вызовов, организацией очередей вызовов и их обработкой реализуются средствами конкретного провайдера Телекоммуникационной подсистемы. Включение указанных функций в основные сценарии обработки вызова операторами ЕДДС/ДДС осуществляется на уровне интеграционной шины.

Функциональный компонент «Нормативно-справочная информация и база знаний» является функциональной частью Подсистемы приема и обработки обращений и предназначен для оперативной выдачи рекомендаций дежурной смене ЕДДС при принятии решений по экстренному реагированию на экстренные ситуации.

Функциональный компонент контроля качества обслуживания является функциональной частью Подсистемы приема и обработки обращений и предназначен для контроля действий операторов при обслуживании вызовов.

Функциональный компонент обучения является функциональной частью Подсистемы приема и обработки обращений и предназначен для подготовки, аттестации и переподготовки штатного персонала ЕДДС, а также может использоваться для подготовки диспетчеров ДДС.

В состав функционального компонента обучения должны входить:

1) библиотеки материалов;
2) учебный макет Системы;
3) эксплуатационная документация.

Подсистема консультативного обслуживания населения

Подсистема консультативного обслуживания населения предназначена для оказания информационно-справочной помощи лицам, позвонившим по вопросам обеспечения безопасности жизнедеятельности, в том числе, через сеть Интернет.

Подсистема должна состоять из двух логических частей:

1) база знаний, предназначенная для проведения консультирования заявителей операторами ЕДДС или ДДС;
2) интернет-портал.

База знаний должна предоставлять возможность:

- полнотекстового поиска справочных статей;
- просмотра статей;
- группировки статей;
- привязки к статье ссылки на запись в IVR;
- переадресации на запись IVR из базы знаний.

Портал должен реализовывать следующие возможности:

1) регистрация на портале;
2) просмотр информации ЕЦОР;
3) просмотр информации о предназначении портала;
4) работа со справочными статьями:
    - отображение списка статей;
    - полнотекстовый поиск статей;
    - просмотр статей;
5) работа со списком контактов:
    - отображение списка;

- поиск информации по списку;

6) отправка вопроса экспертам ЕЦОР;
7) получение ответа на вопрос на электронную почту или в личный кабинет;
8) работа с личным кабинетом:
   - предоставление возможности работы с личным кабинетом только зарегистрированным пользователям;
   - отслеживание статуса заданного вопроса;
   - возможность получения ответа на вопрос в виде сообщения в личном кабинете.

4.1.1.1.3 Подсистема комплексного мониторинга

Подсистема комплексного мониторинга предназначена для сбора и обработки информации и сигналов, поступающих от информационных систем, контролирующих работу датчиков, установленных на стационарных и подвижных объектах мониторинга, находящихся в зоне ответственности соответствующего объекта ЕЦОР.

Подсистема комплексного мониторинга должна включать в свой состав следующие функциональные компоненты:

- Компонент систем мониторинга и обеспечения безопасности;
- Компонент видеомониторинга и видеоанализа.

Компонент систем мониторинга и обеспечения безопасности должен обеспечивать:

- прием и обработку информации и сигналов, поступающих от систем контроля окружающей среды, пожарной обстановки, производственных процессов;
- формирование и передачу в другие компоненты ЕЦОР информации о внештатной ситуации на контролируемых стационарных и подвижных объектах;
- получение и регистрация текущего местоположения и состояния контролируемых транспортных средств;
- ведение статистики внештатных ситуаций по контролируемым стационарным и подвижным объектам;
- предоставление списка объектов мониторинга;
- предоставление списка обращений, поступивших по объекту мониторинга;
- предоставление списка происшествий, зарегистрированных на объектах мониторинга.

Компонент видеомониторинга должен обеспечивать:

- отображение мест расположения видеокамер, с которых поступает сигнал тревоги, на цифровой карте города для дальнейшей передачи оператору ЕЦОР

своевременных указаний на принятие мер по обеспечению безопасности в городе и на автодорогах;

- отображение направления и зон обзора камер на электронной карте;
- отображение мнемоник движущихся объектов (человек, группа людей, транспортное средство);
- возможность передачи изображения от видеокамер по цифровым каналам связи с ограниченной пропускной способностью в ЕЦОР;
- возможность интеграции с информационно-справочными ресурсами ГИБДД розыска транспортных средств, административных правонарушений в соответствии с предъявляемыми требования по безопасности и структуре запросов.
- возможность интеграции с системами экстренной связи, типа «гражданин-полиция», обеспечивающими аудио-видео связь колонн экстренной связи, размещенных на территории города.

4.1.1.1.4 Интеграционная географическая информационная подсистема

Интеграционная геоинформационная подсистема предназначена для обеспечения оперативного отображения на основе электронных карт следующих объектов и информации, относящейся к зоне ответственности объекта ЕЦОР:

1) местонахождение лица (или абонентского устройства), обратившегося по единому телефонному номеру;
2) место возникновения происшествия или ЧС;
3) отображение зон ответственности ДДС;
4) отображение мест расположения камер видеонаблюдения с обозначением направления их обзора и возможностью перехода к просмотру потока видеоинформации с выбранной видеокамеры;
5) расположения ЕДДС, взаимодействующих ДДС и подразделений экстренных служб;
6) расположение потенциально опасных и критически важных объектов;
7) информации о местонахождении и перемещении сил и средств реагирования, при наличии технических возможностей используемых технологий ГЛОНАСС;
8) характеристик территории.

4.1.1.1.5 Интернет – портал

Интернет-портал предназначен для обеспечения информационного обмена с населением и должностными лицами города и должен являться эффективным средством коммуникации в

задачах предупреждения, устранения инцидентов и чрезвычайных ситуаций и минимизации их последствий.

4.1.1.1.6 Подсистема обеспечения координации и взаимодействия

Подсистема обеспечения координации и взаимодействия должна осуществлять оперативное доведение информации до оперативных служб города с постановкой задачи на автоматический контроль исполнения.

4.1.1.1.7 Подсистема комплексного информирования и оповещения

Подсистема комплексного информирования и оповещения представляет собой организационно-техническую систему, объединяющую аппаратно-программные средства обработки, передачи и отображения аудио и видеоинформации в целях подготовки населения в области гражданской обороны, защиты от чрезвычайных ситуаций, обеспечения пожарной безопасности, безопасности на водных объектах и охраны общественного порядка, своевременного оповещения и оперативного информирования граждан о ЧС и угрозе террористических акций, мониторинга обстановки и состояния правопорядка в местах массового пребывания людей на основе использования современных технических средств и технологий.

Подсистема комплексного информирования и оповещения должна иметь доступ к средствам экстренного оповещения общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей (ОКСИОН).

4.1.1.1.8 Подсистема интеграции данных (интеграционная платформа)

Подсистема интеграции данных - составная часть Системы, обеспечивающая надежный защищенный информационный обмен разнородными данными между информационными системами – источниками Системы, компонентами Системы и доступ пользователей Системы к необходимым им ресурсам для решения задач повышения безопасности населения и городской коммунальной инфраструктуры в соответствии с Федеральным законом.

Подсистема интеграции данных должна являться центральной частью ПАК ЕЦОР. Она должна объединять все остальные используемые подсистемы в единую, согласовано работающую исполнительную среду. Данная подсистема должна быть реализована по многоуровневой архитектуре, основанной на интеграционной шине, и включать классические уровни данных, логики и представления. Шина для выполнения целевых функций должна интегрировать следующие технологические сервисы и системы:

1) Телекоммуникационная подсистема;
2) ИС ДДС ЭОС (службы 01, 02, 03, 04, Антитеррор, ЖКХ);
3) Геоинформационная система;

4) Справочные сервисы (для получения дополнительной информации по номеру абонента);
5) Подсистему Мониторинга («ГЛОНАСС/GPS»);
6) Служебные системы (SMS провайдеры, почтовые сервера и др.).

Основными задачами подсистемы интеграции данных являются:

- интеграция разнородных информационных систем в ПАК ЕЦОР;
- интеграция отдельных подсистем в составе ПАК ЕЦОР в рамках целостного процесса обработки информации;
- обеспечение доступа пользователей Системы к необходимым им ресурсам для решения задач обеспечения безопасности.

С целью решения задачи интеграции разнородных информационных систем в подсистему интеграции данных должны входить следующие функциональные компоненты:

1) Компонент ведения реестра внешних информационных систем источников информации (МРИ);
2) Компонент ведения реестра внешних информационных систем потребителей информации (МРВ);
3) Компонент реализации общей шины данных (МОШ);
4) Компонент ведения справочника метаданных информационного обеспечения Системы (ММД);
5) Компонент трансформации, контроля, очистки и нормализации (приведение к общим форматам, классификаторам и т.п.) данных из внешних информационных систем (МТД);
6) Компонент актуализации и синхронизации общесистемных справочников и классификаторов (МАС).

Компоненты подсистемы интеграции данных должны обеспечивать выполнение следующих функций:

1) Компонент ведения реестра внешних информационных систем источников информации:
   - хранение и резервное копирование данных об информационных системах источников информации;
   - поддержка целостности данных;
   - обеспечение авторизованного доступа к данным;
   - ведение протокола операций с реестром;
2) компонент ведения реестра внешних информационных систем потребителей информации:

- хранение и резервное копирование данных об информационных системах потребителей информации;
- поддержка целостности данных;
- обеспечение авторизованного доступа к данным;
- ведение протокола операций с реестром;

3) компонент реализации общей шины данных:
   - организация маршрутизации, ведение очередей и обеспечение гарантированной доставки информации, передаваемой между различными подсистемами, в масштабе контура обработки информации одного уровня конфиденциальности ПАК ЕЦОР;
   - согласование форматов файлов и данных;
   - согласование приложений при их взаимодействии с использованием различных методов и протоколов.
4) Компонент ведения справочника метаданных информационного обеспечения Системы:
   - создание и ведение единого репозитория метаданных описания информационных ресурсов Системы на основе выбранной технологии;
   - организация доступа к метаданным со стороны взаимодействующих информационных систем;
   - ведение журнала регистрации изменений;
5) компонент трансформации, контроля, очистки и нормализации (приведение к общим форматам, классификаторам и т.п.) данных из внешних информационных систем:
   - анализ структуры данных, получаемых из внешних информационных систем;
   - преобразование данных к общему формату;
   - фильтрация данных с искаженной структурой данных;
   - ведение журнала результатов контроля и преобразования данных;
6) компонент актуализации и синхронизации общесистемных справочников и классификаторов:
   - своевременное обновление общесистемных справочников и классификаторов;
   - ведение архива версий общесистемных справочников и классификаторов;
   - ведение журнала регистрации изменений.

Конкретный состав и распределение компонентов подсистемы интеграции данных определяется и уточняется на этапе технического проектирования.

4.1.1.1.9 Подсистема вычислительных комплексов

Подсистема вычислительных комплексов должна включать в свой состав следующие компоненты:

- виртуализируемые вычислительные узлы;
- выделенные вычислительные узлы.

Виртуализируемые вычислительные узлы должны формировать общий пул ресурсов для подсистемы виртуализации. Выделенные вычислительные узлы должны предоставлять вычислительные мощности для систем, виртуализация которых невозможна.

4.1.1.1.10 Транспортная подсистема

Транспортная подсистема должна включать в свой состав следующие компоненты:

1) Сегмент передачи данных:
   - активное сетевое оборудование уровня ядра;
   - активное сетевое оборудование уровня доступа.
2) Сегмент управления.

Транспортная подсистема должна иметь модульную иерархическую архитектуру, предусматривающую дальнейшее масштабирование по производительности и портовой ёмкости.

Сегмент передачи данных должен включать в себя активное сетевое оборудование уровня ядра и доступа. При необходимости, уровень ядра и уровень доступа могут быть объединены.

Уровень ядра сегмента передачи данных транспортной подсистемы должен обеспечивать маршрутизацию трафика сети передачи данных и взаимодействие с сетевым оборудованием смежных систем и комплексов. Уровень ядра сегмента передачи данных транспортной подсистемы должен обеспечивать подключение оборудования подсистемы вычислительных комплексов и подсистемы хранения данных.

Уровень доступа сегмента передачи данных транспортной подсистемы должен обеспечивать физическое подключение АРМ операторов и обслуживающего персонала, а также необходимой организационной техники ПАК ЕЦОР.

Сегмент управления должен обеспечивать доступ к сетевым интерфейсам управления вычислительных узлов, активного сетевого оборудования, централизованной системы хранения данных. Доступ в сегмент управления должен быть ограничен.

Архитектура транспортной подсистемы должна обеспечивать возможность подключения вычислительных узлов как минимум к двум различным устройствам уровня доступа, за исключением интерфейсов управления оборудованием.

Архитектура транспортной подсистемы должна обеспечивать подключение оборудования уровня доступа как минимум к двум различным устройствам уровня ядра.

Архитектура транспортной подсистемы должна обеспечивать полную работоспособность ПАК ЕЦОР при отказе единицы активного сетевого оборудования на каждом уровне иерархии.

4.1.1.1.11 Подсистема хранения данных

Подсистема хранения данных должна включать следующие компоненты:

- устройства хранения (дисковые массивы, системы хранения данных);
- сеть хранения данных.

Устройства хранения должны обеспечивать необходимый объем хранения и предоставлять функциональным и обеспечивающим подсистемам данные в допустимых временных интервалах. Устройства хранения должны обеспечивать надежное хранение данных за счет использования отказоустойчивых технологий.

Сеть хранения данных должна функционировать на базе стека протоколов FC. Сеть хранения данных должна состоять из двух функционально идентичных изолированных фабрик для обеспечения необходимого уровня отказоустойчивости. Оборудование подсистем вычислительных комплексов и хранения данных должно подключаться одновременно к обоим фабрикам сети хранения данных. Сеть хранения данных должна обеспечивать возможность дополнительного сегментирования фабрик с использованием технологий зонирования.

Требования к подсистеме хранения данных:

- управление системами хранения данных (далее – СХД) должно осуществляться через web-интерфейс и/или командную строку;
- СХД должна иметь функции мониторинга и несколько вариантов оповещения администратора о неполадках
- в подсистеме должно быть предусмотрено (по возможности) полное резервирование всех компонент (блоков питания, путей доступа, процессорных модулей, дисков, кэша и т.д.);
- подсистема хранения данных должна обеспечивать доступность данных. (использование технологии RAID, создание полных и мгновенных копий данных внутри дисковой стойки, реплицирование данных на удаленную СХД и т.д.);
- должна предусматривать возможностью добавления (обновления) аппаратуры и программного обеспечения в горячем режиме без необходимости остановки всего комплекса;
- подсистема хранения данных должна обеспечивать достаточную производительность для работы Системы;
- подсистема должна обеспечивать масштабируемость;
- подсистема не должна иметь единой точки отказа;

- СХД должна обеспечивать файловый доступ к данным по протоколам NFS и CIFS(SMB);
- СХД должна поддерживать пулы хранения данных.

Подсистема хранения данных должна обеспечивать полезный объем необходимый для хранения всей поступающей видеоинформации в формате h.264 в течение 30 дней.

4.1.1.1.12 Подсистема виртуализации

Подсистема виртуализации должна включать в свой состав следующие компоненты:

- гипервизоры;
- виртуальные машины (серверы);
- управляющий модуль.

Подсистема виртуализации должна строиться с применением технологий обеспечения высокой доступности виртуальных машин.

Подсистема виртуализации должна поддерживать интеграцию с централизованной системой хранения данных.

Подсистема виртуализации должна обеспечивать возможность вывода в режим технического обслуживания любого из вычислительных узлов подсистемы вычислительных комплексов или разделов централизованной системы хранения данных. При этом не должно происходить прерывания в работе затрагиваемых виртуальных серверов.

Основным компонентом платформы виртуализации должен являться программный гипервизор первого типа («bare-metal» гипервизор, устанавливаемый непосредственно на аппаратную составляющую серверного оборудования).

Гипервизор должен устанавливаться на хост-серверы (виртуализируемые вычислительные узлы подсистемы вычислительных ресурсов).

4.1.1.1.13 Подсистема резервного копирования и восстановления данных

Подсистема резервного копирования и восстановления данных должна обеспечивать выполнение следующих функций:

- периодическое архивирование различных массивов данных;
- извлечение данных из архива и запись их в соответствующий массив;
- хранение и учет копий данных.

Подсистема резервного копирования и восстановления данных должна включать в свой состав следующие компоненты:

- управляющий модуль;
- клиентские модули;
- узел хранения резервных копий;

Подсистема резервного копирования и восстановления данных предназначена для минимизации потери информации при сбоях оборудования, программного обеспечения и ошибках обслуживающего персонала.

Подсистема резервного копирования и восстановления данных должна строиться по клиент-серверной архитектуре.

Подсистема резервного копирования и восстановления данных должна быть совместима с используемым в смежных подсистемах аппаратным и программным обеспечением.

Подсистема резервного копирования и восстановления данных должна иметь возможность масштабирования при увеличении объема защищаемых данных.

Подсистема резервного копирования и восстановления данных должна использовать технологии дедупликации и сжатия данных.

4.1.1.1.14 Подсистема администрирования

Подсистема администрирования предназначена для установки, изменения и контроля основных параметров ПАК ЕЦОР в процессе его эксплуатации.

Подсистема администрирования должна обеспечивать выполнение следующих функций:

- администрирование операционных систем, сетевого и инструментального программного обеспечения, входящего в ПАК ЕЦОР;
- контроль исправности основных элементов Системы;
- сбор и хранение данных о параметрах функционирования основных элементов Системы;
- оперативное вмешательство в работу программно-технических средств Системы.

4.1.1.1.15 Подсистема информационной безопасности

Подсистема обеспечения информационной безопасности предназначена для защиты информации и средств ее обработки в ЕЦОР.

Подсистема информационной безопасности должна обеспечивать требуемый уровень защиты информации от внешних и внутренних угроз.

К объектам защиты ЕЦОР относятся:

- технические средства;
- программные средства;
- информация, содержащая охраняемые сведения, в том числе регламенты и процедуры работы объектов ЕЦОР и взаимодействующих ДДС;
- помещения, предназначенные для обработки и хранения информации.

В ЕЦОР циркулирует конфиденциальная информация, относящаяся к следующим типам:

а) персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

б) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

в) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами.

Для решения задач подсистемы обеспечения информационной безопасности должен быть предусмотрен комплекс программно-технических средств и организационных (процедурных) решений по защите информации от несанкционированного доступа, определяемый на основании требований настоящего документа и с учетом модели угроз и нарушителя.

Информационный обмен между компонентами ПОИБ должен осуществляться с использованием каналов связи локальной вычислительной сети, не выходящих за пределы контролируемой зоны. При этом под контролируемой зоной понимается пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей Заказчика.

Для организации информационного обмена с использованием каналов связи, выходящих за пределы контролируемой зоны, требуется использовать средства криптографической защиты информации, которые в установленном порядке прошли процедуру оценки соответствия требованиям безопасности информации ФСБ России. Криптографическая защита информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны, должна обеспечиваться с использованием криптоалгоритма ГОСТ 28147-89. Используемые средства криптографической защиты информации должны обеспечивать криптографическую защиту по уровню не ниже КС2.

В соответствии с Приказом ФСТЭК России от 05.02.2010 года №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» для обеспечения безопасности персональных данных при их обработке в ИСПДн целесообразно использовать мероприятия по обеспечению безопасности ПДн. Для реализации данных мероприятий необходимо создание следующих функциональных компонентов:

- Компонент управления доступом;
- Компонент регистрации и учета;

- Компонент обеспечения целостности;
- Компонент обеспечения безопасного межсетевого взаимодействия;
- Компонент анализа защищенности;
- Компонент обнаружения вторжений;
- Компонент антивирусной защиты.

4.1.1.2 Требования к способам и средствам связи для информационного обмена между компонентами системы

Технологические решения должны строиться на использовании существующей и создаваемой в рамках ПАК ЕЦОР телекоммуникационной сети, позволяющей использовать одни и те же каналы связи для передачи всех видов данных (в том числе голосовых и видео).

Телекоммуникационная сеть должна отражать существующее деление телекоммуникационной структуры Единой сети электросвязи России на магистральные (транспортные) сети и сети доступа.

Для информационного обмена могут использоваться сети электросвязи следующих категорий:

- сеть связи общего пользования;
- выделенные сети связи;
- технологические сети связи, присоединенные к сети связи общего пользования;
- сети связи специального назначения.

Конкретные схемы связи существующей и создаваемой в рамках ПАК ЕЦОР телекоммуникационной сети должны быть определены по согласованию с Заказчиком при техническом проектировании.

Взаимодействие компонентов программного обеспечения в Системе должно осуществляться на основе стандартов на архитектуру построения системных сервисов (служб) и взаимно-совместимых приложений (стандарты типа CORBA, DCOM, SOAP/XML, RPC, RMI или JSON).

4.1.1.3 Требования к характеристикам взаимосвязей создаваемой системы со смежными системами

ПАК ЕЦОР должен поддерживать информационное взаимодействие с информационными системами городских, а также региональных органов управления, в том числе:

- жилищно-коммунального и топливно-энергетического хозяйства;
- транспорта и связи;

- архитектуры и строительства;
- экологического надзора и промышленной безопасности;
- пожарно-спасательной службы и службы скорой медицинской помощи;
- территориальными органами МЧС России, МВД России и ФСБ России.

Информационная совместимость ПАК ЕЦОР со смежными информационными системами должна обеспечиваться возможностью использования в них одних и тех же форматов данных и протоколов обмена данными между информационными системами.

Взаимодействие ПАК ЕЦОР со смежными разнородными информационными системами должно определяться:

- специальными стандартами – протоколами взаимодействия;
- типовым синтаксисом сообщений, именами элементов данных, операциями управления и состояния;
- типовыми пользовательскими сервисами и межсистемными интерфейсами электронного информационного взаимодействия;
- типовыми протоколами электронного взаимодействия.

Протоколы взаимодействия должны представлять собой наборы правил взаимодействия функциональных блоков смежных систем на основе сетевой модели взаимодействия открытых систем.

Синтаксис сообщения, имена элементов данных, операции управления и состояния должны быть реализованы на основе гипертекстовых языков разметки (текста) типа SGML(XML).

Пользовательские сервисы и интерфейсы электронного информационного взаимодействия должны определять способы взаимодействия, правила передачи информации и сигналы управления передачей информации (примитивы).

Межсистемные интерфейсы должны реализовываться на базе международных стандартов на электронные документы, включая:

- стандарты UN/EDIFACT, разработанные Европейской Экономической Комиссией ООН (ЕЭК ООН) и принятые в качестве международных стандартов;
- стандарты ISO серии 8613 «Обработка информации. Текстовые и учрежденческие системы. Архитектура, ориентированная на обработку учрежденческих документов (ODA), и формат обмена»;
- стандарты ISO серии 10021 «Информационная технология. Передача текстов. Системы обмена текстами в режиме сообщений (MOTIS)»;
- стандарты TCP/IP, SGML и др.

Основными процедурами управления передачей информации должны являться: запрос-ответ, авторизация, индикация.

Процедуры запрос-ответ должны быть реализованы на основе использования клиент-серверной архитектуры ПАК ЕЦОР.

Программы клиентов могут использовать протоколы прикладного уровня стандарта OSI HTTP, FTP и SMTP по схеме «запрос-ответ».

Процедуры авторизации должны представлять собой процесс, а также результат процесса проверки установленных параметров пользователя ПАК ЕЦОР (логина и пароля) и предоставление ему или группе пользователей ПАК ЕЦОР определенных полномочий на выполнение действий, связанных с доступом к ресурсам ПАК ЕЦОР. Должно обеспечиваться ведение журнала авторизации пользователя.

Процедуры индикации должны представлять собой процессы отображения результатов мониторинга управления обмена информацией в ПАК ЕЦОР с применением обеспечивающих эти процессы программных и технических устройств отображения.

4.1.1.4 Требования к режимам функционирования системы

Годовой цикл эксплуатации ПАК ЕЦОР – ежедневно, без выходных, при условии, что серверы и коммуникационное оборудование работают круглосуточно.

Система должна функционировать в следующих режимах: штатном, автономном.

Штатный режим является основным режимом функционирования Системы, при котором поддерживается выполнение всех заявленных функций. В этом режиме Система должна обеспечивать работу всех пользователей.

Автономный режим является вспомогательным режимом функционирования отдельных элементов Системы, когда все или отдельные их функции становятся недоступными для пользователей Системы. В этом режиме осуществляются техническое обслуживание, реконфигурация, модернизация и совершенствование компонентов Системы, а также резервное копирование информационного наполнения и конфигурационных файлов.

4.1.1.5 Требования по диагностированию системы

Должны быть предусмотрены организационно-методические и технические меры по автоматизированному контролю и диагностированию сбоев в работе аппаратно-программных комплексов для всех структурных компонентов системы, а также оперативному восстановлению их работоспособности.

Под организационно-методическими мерами понимаются мероприятия по разработке структуры эксплуатационных подразделений, соответствующей территориально-распределенному характеру системы и способной производить своевременную диагностику функционирования элементов Системы, а также принимать адекватные меры по устранению критических ситуаций. В методические меры необходимо включить мероприятия по подготовке и обучению персонала, а

также подготовку и выпуск рабочих и эксплуатационных документов по способам диагностики функционирования различных элементов системы и устранения сбоев, критических и аварийных ситуаций.

В качестве технических мер ПАК ЕЦОР должен предоставлять инструменты диагностирования основных компонентов Системы.

Диагностические инструменты должны предоставлять удобный интерфейс для возможности просмотра диагностических событий, мониторинга процесса выполнения программ.

Диагностирование Системы должно осуществляться посредством анализа различных журналов системы (например, журнала запуска и остановки, журнала возникновения исключительных ситуаций в Системе и т.д.) и информационных (log) файлов системы.

Объектами диагностирования должны являться:

- средства вычислительной техники;
- телекоммуникационное оборудование и каналы связи;
- средства гарантированного электропитания;
- базы данных;
- общее программное обеспечение;

Диагностирование компонент ПАК ЕЦОР должно осуществляться во всех режимах её функционирования.

Организационно-методические и технические мероприятия по диагностированию системы должны применяться централизованно, по согласованию с организацией-оператором Системы.

4.1.1.6 Перспективы развития, модернизации системы

Система должна предусматривать поэтапное развитие. Развитие и модернизация и должны обеспечиваться без нарушения ее работоспособности, для этих целей при создании ПАК ЕЦОР должен быть обеспечен не менее чем 30% резерв технических, технологических и телекоммуникационных возможностей Системы.

Развитие и модернизация Системы могут идти в следующих направлениях:

- расширения состава объектов автоматизации;
- развития функциональной архитектуры Системы за счет создания дополнительных функций подсистем, расширяющих ее возможности;
- создание новых типов комплексов средств автоматизации;
- повышения технических характеристик технических средств Системы (производительность серверов, пропускная способность каналов связи);
- усовершенствование действующих типов ПТК, включая их адаптацию к развивающейся инфраструктуре, средств связи и передачи данных.

В ходе работ по проектированию и разработке ПАК ЕЦОР должны быть предусмотрены организационно-методические и технические меры, обеспечивающие возможности развития и модернизации Системы:

- возможность масштабирования:
- добавление дополнительных сервисов и подсистем;
- увеличение количества конечных пользователей;
- увеличение количества автоматизированных рабочих мест (АРМ);
- подключение новых каналов связи;
- расширение состава предоставляемой информации.
- возможность модернизации технических и программных средств (в части развития функциональности) без вывода системы из постоянной эксплуатации и без потери данных.

4.1.2 Требования к численности и квалификации персонала системы и режиму его работы

Персонал ПАК ЕЦОР должен состоять из:

- пользователей Системы;
- персонала, осуществляющего эксплуатацию (обслуживающего персонала).

Численный состав пользователей является переменным и определяется руководством объекта автоматизации.

Все пользователи должны быть разделены по группам (ролям) в соответствии с функциональностью, которую они используют при работе с Системой.

Каждый пользователь должен иметь одну (единую) учетную запись в Системе.

Численный состав персонала, обслуживающего компоненты Системы, устанавливается штатным расписанием организации-оператора ПАК ЕЦОР.

Численность обслуживающего персонала Системы должна определяться с учетом следующих требований:

- структура и конфигурация Системы должны быть спроектированы и реализованы с целью минимизации количественного состава обслуживающего персонала и обеспечения работоспособности Системы во всех режимах функционирования;
- аппаратно-программные средства Системы не должны требовать круглосуточного обслуживания и постоянного присутствия администраторов у консоли управления;
- структура Системы должна предоставлять возможность управления всем доступным функционалом Системы как одному администратору, так и предоставлять

возможность разделения ответственности по администрированию между несколькими администраторами;

- для администрирования Системы к администратору не должны предъявляться требования по знанию всех особенностей функционирования элементов, входящих в состав администрируемых компонентов Системы.

Для обслуживающего персонала Системы должны быть определены следующие основные роли:

- системный администратор;
- инженер по обслуживанию средств сетевой и вычислительной техники, а также периферийного оборудования;
- администратор информационной безопасности.

Требования к численности и составу обслуживающего персонала Системы подлежат уточнению при техническом проектировании и должны быть включены в эксплуатационную документацию на каждый сегмент.

Основными квалификационными требованиями к персоналу Системы является возможность самостоятельной работы:

- наличие соответствующих юридически правильно оформленных документов с необходимыми квалификационными характеристиками (допуски для работы);
- необходимый стаж самостоятельной работы;
- подтверждение квалификационных характеристик в течение испытательного срока;
- самостоятельная работа с современным серверным оборудованием, сетевым оборудованием, периферийным оборудованием, ленточными библиотеками, дисковыми массивами, сканерами, коммутационным оборудованием.

Подготовка (переподготовка, повышение квалификации) и контроль знаний персонала должны осуществляться в плановом порядке с выдачей соответствующих свидетельств и удостоверений.

Режим работы персонала Системы должен соответствовать требованиям Трудового кодекса Российской Федерации, включая работу в условиях аварийных ситуаций, в том числе:

- требования к организации труда и режима отдыха персонала должны устанавливаться, исходя из требований к организации труда и режима отдыха при работе с персональными компьютерами;
- все специалисты должны работать с нормальным графиком работы не более 8 часов в сутки;
- для обеспечения максимальной работоспособности и сохранения здоровья профессиональных пользователей на протяжении рабочей смены должны

устанавливаться регламентированные перерывы: через 2 часа после начала рабочей смены и через 1,5 – 2,0 часа после обеденного перерыва продолжительностью 15 минут каждый или продолжительностью 10 минут через каждый час работы;

- продолжительность непрерывной работы персонала с разрабатываемой системой и персональными компьютерами без регламентированного перерыва не должна превышать 2 часа;
- деятельность персонала по эксплуатации средств Системы должна регулироваться должностными инструкциями.

4.1.3 Показатели назначения

Целевое назначение Системы должно сохраняться на протяжении всего срока ее эксплуатации. Срок эксплуатации Системы определяется сроком устойчивой работы аппаратных средств вычислительных комплексов, своевременным проведением работ по замене (обновлении) аппаратных средств, по сопровождению программного обеспечения Системы и его модернизации.

ПАК ЕЦОР должен сохранять работоспособность при увеличении количества пользователей в пределах, поддерживаемых вычислительной инфраструктурой.

Технологические решения по созданию системы должны обеспечивать выполнение следующих требований:

- предельное время ожидания ответа оператора – не более 8 сек.;
- вероятность потери вызова – не более 0,1%;
- устойчивость к сетевым перегрузкам;
- возможность дальнейшего развития системы в направлении расширения функционала, производительности, масштабируемости существующих служб и возможности реализации новых служб;
- возможность взаимодействия между ЕЦОР ЕДДС и ДДС, а также взаимодействия с региональным ЦУКС МЧС России.

Специальные требования к вероятностно-временным характеристикам, при которых сохраняется целевое назначение Системы, не предъявляются.

4.1.4 Требования к надежности

Под надёжностью Системы понимается ее комплексное свойство сохранять во времени, в установленных нормативно-технической и (или) конструкторской документацией пределах, значения параметров, характеризующих способность Системы выполнять свои функции, определяемые её назначением, режимами и условиями эксплуатации.

В качестве показателей надёжности Системы должны использоваться показатели, характеризующие надёжность реализации ее функций.

Надёжность Системы должна характеризоваться:

- по отдельным составляющим надёжности – единичными показателями;
- по нескольким составляющим надёжности – комплексными показателями надёжности.

В качестве единичных показателей надёжности ПАК ЕЦОР должны использоваться следующие показатели:

- средняя наработка Системы на отказ - не меньше 3 000 часов;
- средний срок службы Системы – не менее 30 000 часов;
- среднее время восстановления работоспособного состояния Системы после отказа - не более 4 часов.

В качестве комплексного показателя надёжности ПАК ЕЦОР должен использоваться коэффициент готовности (отношение времени штатного функционирования к общему времени работы), который должен составлять не менее 0.99, что соответствует менее 7 часов простоя в месяц.

Критерием предельного состояния следует считать моральное старение Системы, не соответствие её текущим задачам, когда моральное старение невозможно устранить посредством технического надзора и плановым ремонтом.

Числовые значения заданных показателей надёжности для ПАК ЕЦОР в целом и её отдельных компонентов оцениваются на основе требований к надёжности поддерживаемых ими рабочих процессов и проверяются на этапе ввода в постоянную эксплуатацию Системы. Допускаются экспериментальные методы оценки показателей надёжности Системы (моделирование работы и отказов).

Деятельность по оценке и контролю показателей надёжности должна проводиться в комплексе работ по управлению качеством и испытаниями Системы. Оценка показателей надежности должна проводиться согласно ГОСТ 27.301-95, ГОСТ 27.402-95, ГОСТ 27.410-87.

Надежность ПАК ЕЦОР должна обеспечиваться:

- использованием технических средств повышенной отказоустойчивости и их структурным резервированием;
- наличием на объектах автоматизации запасных изделий и приборов (ЗИП);
- защитой технических средств по электропитанию путем использования источников бесперебойного питания;
- дублированием носителей информационных массивов.

В процессе проектирования ПАК ЕЦОР должны быть определены наиболее критичные, с точки зрения надежности, участки информационно-технологического цикла и перечни возможных аварийных ситуаций, представлены решения по обеспечению надежности критичных участков.

Под отказом ПАК ЕЦОР понимается событие, заключающееся в нарушении автоматического режима функционирования Системы (прекращения выполнения хотя бы одной из функций), при котором для восстановления работоспособности требуется перезагрузка программного обеспечения с исходного носителя, проведение специальных процедур информационного восстановления, ремонта или замены отказавшего оборудования.

Кратковременное нарушение функционирования Системы (до десяти минут), устраняемое автоматически или по командам оператора путем проведения реконфигурации, перезагрузки, информационного восстановления, рестартов и не приводящее к потере информации, не является отказом.

Оборудование и ПО должны проектироваться для круглосуточной работы, позволять осуществлять резервирование и восстановление Системы после сбоев.

Система в целом должна обеспечивать выполнение целевых функций в режиме 24х365 (24 часа в день, 365 дней в году) за исключением периодов технического обслуживания, предусмотренных технической документацией. Критерием выполнения данного требования является значение коэффициента готовности.

Гарантийный срок эксплуатации применяемого оборудования определяется политикой производителя оборудования.

К критическим компонентам ПАК ЕЦОР относятся:

- средства обработки и хранения данных;
- средства телекоммуникации и информационного взаимодействия компонентов Системы;
- средства и компоненты обеспечения информационной безопасности.

Для выполнения поставленных требований к надёжности Системы в целом и её компонентов должно быть:

- обеспечено отсутствие нерезервированных точек отказа критических компонентов Системы: создание отказоустойчивых кластеров серверов, использование высоконадежных систем хранения данных, дублирование каналов связи (топологически разными путями);
- обеспечена возможность «горячей» замены элементов (например, горячая замена компонентов серверов, источников питания и т.п.);

Конкретные технические решения и список компонентов, подлежащих резервированию, уточняются при техническом проектировании.

Характеристики надёжности технических средств, входящих в Систему, определяются техническими условиями (технической документацией) на эти средства.

Сбои в работе ПО и КТС, телекоммуникационной инфраструктуры или сетей электроснабжения не должны приводить к внесению искажений в первичные данные, получаемые и хранимые в БД, и в хранимые результаты обработки первичных данных. Сохранность информации должна обеспечиваться на аппаратном, системно-техническом, общесистемном программном и организационном уровнях.

При выработке проектных решений по обеспечению высокой надежности необходимо использовать свойства применяемой аппаратной платформы, СУБД, функциональные свойства специализированного общесистемного и прикладного программного обеспечения, а также соответствующие организационные меры.

Уточнения по составу и значению показателей надежности должно быть проведено на этапе технического проектирования Системы.

4.1.5 Требования безопасности

Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление в соответствии с ГОСТ 12.1.030-81 и «Правилами устройства электроустановок» (ПУЭ).

Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также аварийное ручное отключение.

Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование. В случае возгорания не должно выделяться ядовитых газов и дымов. После снятия электропитания должно быть допустимо применение любых средств пожаротушения.

Факторы, оказывающие вредные воздействия на здоровье со стороны всех элементов системы (в том числе инфракрасное, ультрафиолетовое, рентгеновское и электромагнитное излучения, вибрация, шум, электростатические поля, ультразвук строчной частоты и т.д.), не должны превышать действующих норм (СанПиН 2.2.2./2.4.1340-03 от 03.06.2003 г.).

4.1.6 Требования к эргономике и технической эстетике

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав системы должно осуществляться посредством визуального графического интерфейса (GUI). Навигационные элементы должны быть выполнены в удобной для пользователя форме. Средства редактирования информации должны удовлетворять принятым соглашениям в части использования функциональных клавиш, режимов работы, поиска, использования оконной

системы. Ввод-вывод данных системы, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям системы.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов. Клавиатурный режим ввода должен используется главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на русском языке.

Система должна обеспечивать корректную обработку ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Экранные формы должны проектироваться с учетом требований унификации:

- все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;
- для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы. Термины, используемые для обозначения типовых операций (добавление информационной сущности, редактирование поля данных), а также последовательности действий пользователя при их выполнении, должны быть унифицированы;
- внешнее поведение сходных элементов интерфейса (реакция на наведение указателя «мыши», переключение фокуса, нажатие кнопки) должны реализовываться одинаково для однотипных элементов.

Система должна соответствовать требованиям эргономики и профессиональной медицины при условии комплектования высококачественным оборудованием (ПЭВМ, монитор и прочее оборудование), имеющим необходимые сертификаты соответствия и безопасности Росстандарта.

4.1.7 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Эксплуатация Системы должна производиться в соответствии с эксплуатационной документацией и Регламентом технического обслуживания.

Условия эксплуатации, хранения, а также виды и периодичность обслуживания технических средств компонентов ПАК ЕЦОР должны соответствовать требованиям по эксплуатации, техническому обслуживанию, ремонту и хранению, изложенным в документации на них завода-изготовителя.

Обслуживание Системы должно производиться обслуживающим персоналом.

Допускается использование специализированных служб или подразделений на объектах внедрения, для обслуживания и ремонта оборудования.

Должно быть предусмотрено текущее ежедневное техническое обслуживание Системы. При возникновении неисправностей, должно осуществляться оперативное техническое обслуживание, временные регламенты которого не должны превышать указанных значений времени восстановления.

Регламент технического обслуживания должен быть определен в составе эксплуатационной документации.

Размещение технических средств и организация автоматизированных рабочих мест должны быть выполнены в соответствии с требованиями ГОСТ 21958-76 «Система «человек-машина». Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования».

Для электропитания технических средств должна быть предусмотрена однофазная сеть 220 В (+10-15)% частотой 50 Гц (+1-1) Гц. Каждое техническое средство запитывается однофазным напряжением 220 В частотой 50 Гц через сетевые розетки с заземляющим контактом.

Техническое обслуживание ПАК ЕЦОР должно осуществляться эксплуатационным персоналом. Требования к численности, режиму работы и функциям эксплуатационного персонала определены в разделе 4.1.2 настоящего документа.

Регламент технического обслуживания и порядок ремонта оборудования ПАК ЕЦОР определяется на стадии создания проектной документации.

Ремонт оборудования Системы должен допускать возможность замены его типовых элементов без приостановки деятельности ПАК ЕЦОР.

4.1.8 Требования к защите информации от несанкционированного доступа

Информационная безопасность Системы должна осуществляться подсистемой обеспечения информационной безопасности, реализуемой организационными мерами и программно-

техническими средствами. Требования к подсистеме информационной безопасности приведены в разделах 4.1.1.1.8 и 4.2.8.

Требования к защите информации от несанкционированного доступа разрабатываются на этапе разработки проектной документации.

4.1.9 Требования по сохранности информации при авариях

В ПАК ЕЦОР должна быть обеспечена сохранность информации при авариях и сбоях в электропитании системы, отказов в работе серверного оборудования и сетевого оборудования.

В Системе должны быть предусмотрены средства для резервного копирования информации. В состав эксплуатационной документации должен входить регламент, определяющий процедуры резервного копирования, восстановления данных и программного обеспечения.

Система должна включать следующие средства обеспечения сохранности информации:

- средства создания резервной копии базы данных;
- средства восстановления базы данных из резервной копии при возникновении событий, приведших к повреждению базы данных;
- резервные серверы (функционально дублирующие серверы);
- резервные АРМ управления;
- резервные коммутаторы;
- источники бесперебойного питания.

Программное обеспечение ПАК ЕЦОР должно автоматически восстанавливать свое функционирование при корректном перезапуске технических средств. Должна быть предусмотрена возможность организации автоматического или ручного резервного копирования с использованием стандартных программных и аппаратных средств, входящих в состав ПАК ЕЦОР.

Обеспечение надежности хранения и восстановления данных должно осуществляться на основе:

- быстрого сброса cache памяти в случае отказа внешнего электропитания;
- использования глобальных дисков горячей замены;
- упреждающего резервирования дисков;
- изоляции диска в случае его сбоя;
- постоянной проверки целостности персональных данных о пассажирах в фоновом режиме;
- возможности переноса данных внутри системы без остановки приложений;
- использования технологии RAID, обеспечивающей защиту от одновременного выхода из строя двух дисков.

Регламент работы системы должен предусматривать создание резервных копий баз данных и сопутствующей информации. Процесс создания резервных копий должен быть автоматизирован с минимальными функциями оператора и удобным пользовательским интерфейсом.

4.1.10 Требования к защите от влияния внешних воздействий

Технические средства должны отвечать требованиям ГОСТ 19542-83, ГОСТ 29339-92, ГОСТ Р 50628-2000, требованиям Госкомсвязи России «Автоматизированные системы управления аппаратурой электросвязи» 1998г. по электромагнитной совместимости и помехозащищенности.

ТС должны удовлетворять требованиям по электромагнитной совместимости, определенным в ГОСТ 22505-97 и ГОСТ 51275-99.

Иных специальных требований по защите от влияния внешних воздействий в части радиоэлектронной защиты не предъявляется.

Требования по устойчивости к таким воздействиям как: механический резонанс, синусоидальная вибрация, механические удары, атмосферное пониженное давление, плесневые грибы, рабочие растворы и агрессивные среды в ПАК ЕЦОР не предъявляются.

4.1.11 Требования к патентной чистоте

Проектные решения Системы должны отвечать требованиям по патентной чистоте согласно действующему законодательству Российской Федерации.

В соответствии с ст. 773 Гражданского кодекса Российской Федерации Исполнитель обязан гарантировать Заказчику передачу полученных по договору результатов, не нарушающих исключительных прав других лиц.

Готовые, настраиваемые компоненты должны быть лицензированы согласно лицензионному соглашению фирмы-производителя.

4.1.12 Требования по стандартизации и унификации

Процесс разработки Системы должен соответствовать требованиям к созданию АС, регламентированных стандартами:

- ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

Компоненты Системы должны быть разработаны в соответствии с требованиями национальных стандартов (ГОСТ), Единой системы конструкторской документации, Единой системы программной документации и других руководящих и нормативных правовых документов по созданию АС, в том числе, АС в защищенном исполнении, а также требованиями нормативно-методических и руководящих документов ФСТЭК России и ФСБ России.

В Системе должны использоваться типовые проектные решения, унифицированные формы управленческих документов, общероссийские классификаторы технико-экономических и социальных показателей и классификаторы других категорий, унифицированные методы реализации функций системы, стандартные технические и программные средства общего назначения, общепринятые (стандарты де-факто) языки и процедуры информационного взаимообмена.

Реализация требований по стандартизации и сертификации должна включать:

- стандартизацию типовых проектных решений по компонентам, функциональным и обеспечивающим подсистемам Системы;
- стандартизацию информационных протоколов и документооборота, использование государственных, ведомственных и локальных классификаторов;
- сертификацию оборудования и программных средств, используемых в вычислительной системе и реализующих принцип открытости Системы.

На АРМ и серверах для реализации однотипного функционала должны использоваться одинаковые методы обработки данных и унифицированные программные средства.

При разработке и внедрении Системы должны быть реализовано:

- создание компонента на основе применения типовых проектных решений с учетом особенностей объектов Системы;
- средства классификации и кодирования Системы должны соответствовать федеральным и отраслевым классификаторам, словарям, регистрам и реестрам;
- состав и структура баз данных Системы должны быть унифицированы по составу показателей, их размерности, периодичности представления, формам и форматам представления.

4.2 Требования к функциям (задачам), выполняемым системой

Функции (задачи) Системы реализуются функциональными компонентами ПАК ЕЦОР и входящими в их состав функциональными подсистемами.

Определенные настоящим техническим заданием требования к функциям (задачам), выполняемым Системой, уточняются на этапах технического проектирования и разработки проектной документации ПАК ЕЦОР.

4.2.1 Подсистема поддержки принятия решений

Подсистема поддержки принятия решений должна выполнять следующие функции:

1) опрос абонента по определенным заранее сценариям (наличие системы детерминированных диалогов);
2) автоматизацию процесса принятия решений, в том числе использование типовых сценариев реагирования на основе утвержденных ведомственных регламентов при ликвидации ЧС и происшествий;
3) сбор и хранение информации остальных подсистем, сбор и хранение статистической информации;
4) построение аналитических и статистических отчетов с минимальными временными затратами и без нагрузки на транзакционную часть системы:
   - сбор, обработку и представление информации о работе ЕЦОР в различной форме, в том числе и с применением средств деловой графики, и в различных разрезах (временном, территориальном);
   - формирование отчетов за указанный период;
   - возможность получения отчетов на основании актуальных и архивных данных;
   - возможность построения отчетов с агрегацией показателей и с их детальной расшифровкой;
   - расчет основных показателей функционирования Системы;
   - отчеты по приёму и обработке вызовов, как по отдельно взятой ЕДДС, ДДС, так и по совокупности;
   - отчеты по событиям (превышение пороговых значений, устанавливаемых в настройках подсистемы и т.п.).
5) разграничение прав доступа к отчетам;
6) автоматическое формирования стандартных аналитических и статистических отчетов по заданному расписанию.

4.2.2 Подсистема приема и обработки обращений

Подсистема должна обеспечивать следующие функции:

1) приём и обработка (регистрация и документирование) вызовов на единый телефонный номер, поступающих через операторов фиксированной и мобильной связи, направление их оператору ЕЦОР (ЕДДС), перенаправление диспетчеру ДДС;
2) автоматическое заполнение электронной карточки вызова данными, получаемыми от оператора связи (АОН, др. данные);

3) ручное (диспетчером, оператором) заполнение соответствующих полей электронной карточки;
4) дополнительный прием, регистрация, документирование вызовов поступающих в формате: e-mail, SMS (при наличии технических и иных возможностей предоставления операторами связи доступа к SMS-центру), обращений через портал, направление их оператору ЕЦОР, перенаправление диспетчеру ДДС;
5) регистрацию номера телефона вызывающего абонента, если эта информация поступила от оператора связи;
6) получение информации о месте установки телефона для вызовов, поступивших от абонентов телефонной сети фиксированной связи, или определение местоположения абонентского устройства сети мобильной связи при наличии технических и иных возможностей предоставления операторами связи информации о месте установки телефона или о местоположении вызывающего абонентского устройства;
7) регистрацию информации о месте установки телефона или о местоположении вызывающего абонентского устройства в дополнение к регистрации информации об адресе места происшествия;
8) получение информации о месте происшествия;
9) фиксация ложных и злонамеренных вызовов;
10) детектирование повторных обращений граждан;
11) обработка массовых вызовов по поводу уже зарегистрированного происшествия;
12) возможность выполнения сценариев при обработке входящих вызовов;
13) возможность просмотра истории вызовов;
14) возможность ведения «черных» списков – списков абонентов или номеров телефонов, запросы которых обслуживаются по особому сценарию;
15) учет следующих параметров в процессе обработки телефонного вызова: дата, день недели, время, номер абонента, линии, с которой поступил вызов;
16) получение информации о типичных проблемах и средствах их решения, а так же структурированной справочной информации (адреса, телефоны, режимы работы основных служб и т.п.) в соответствии с обрабатываемым вызовом;
17) оповещение администратора системы о наличии нештатной ситуации в работе и методах ее устранения в целях скорейшего возобновления нормальной работы;
18) взаимосвязь с существующими и разрабатываемыми автоматизированными информационными системами (АИС) экстренных оперативных служб и других участников информационного взаимодействия;

19) использование соответствующих справочников (при формировании записи о происшествии для категорий, видов и статусов происшествий) и возможность актуализации данных справочников;
20) возможность работы со списком происшествий – атрибутивный и полнотекстовый поиск, сортировка, вывод на печать;
21) автоматизированный выбор состава оповещаемых экстренных служб в зависимости от типа происшествия с возможностью корректировки этого перечня оператором;
22) автоматический выбор способа оповещения экстренной службы в соответствии с согласованным со службой регламентом;
23) отображение информации о поступлении или не поступлении в соответствии с регламентом подтверждения («квитанции») о регистрации происшествия во взаимодействующей АС;
24) при переадресации вызова др. оператору (диспетчеру), передача ранее полученной информации об источнике вызова и случившемся событии;
25) голосовое самообслуживание абонентов (InteractiveVoiceResponse) со следующими функциями:
    - возможность переадресации входящих вызовов на голосовое меню;
    - навигация по голосовому меню с помощью DTMF-набора;
    - навигация по голосовому меню, при помощи функции распознавания речи;
    - поддержка преобразования текста в речь (для автоматического озвучивания текстовых документов);
    - автоматическая переадресация абонента из очереди на компонент голосового самообслуживания, при превышении времени ожидания в очереди или переполнении очереди;
26) автоматическая переадресация абонента из модуля голосового самообслуживания на ДДС, в соответствии с результатами тонального набора или распознавания речевой информации, полученной от абонента;
27) организация групп операторов
28) организация рабочего места операторов группы “Обычный оператор” со следующими функциями:
    - регистрация на рабочем месте с правами “Обычный оператор”;
    - прием входящих вызовов с отображением информации о номере вызывающего абонента и номере вызываемой службы;

- получение информации об абоненте и его местонахождении из внешних баз данных (адрес местожительства, возраст, пол, домашний и мобильный (при предоставлении оператором связи) телефоны вызывающего абонента);
- возможность принудительного разъединения вызова;
- перевод вызова на другого оператора внутри одной группы операторов;
- перевод вызовов в другие группы операторов;
- переадресация входящего вызова на внешний номер или на подсистему самообслуживания (автоинформатор);
- постановка на удержание;
- передача вызова, конференция, консультация;

29) организация рабочего места операторов группы “Старший оператор (супервизор)” со следующими функциями:
- регистрация на рабочем месте с правами “Старший оператор (супервизор)”;
- возможность приема и обработки входящих вызовов аналогично, как “Обычный оператор”;
- возможность мониторинга текущего состояния своей группы “Обычных операторов”;
- возможность администрирования операторских ресурсов в «горячем» режиме;
- возможность прослушивания разговоров “Обычных операторов” в реальном времени, а также ранее записанных;
- возможность блокировки, вывода из системы “Обычных операторов”;
- возможность блокировки “Обычных операторов” своей группы;
- передача сообщений операторам различных групп;
- возможность просмотра статистики по операторам своей группы (групп);
- возможность оказания, в случае необходимости, психологической поддержки путем переадресация вызовов психологу в двух режимах (с отключением оператора ЕДДС от разговора и с участием оператора ЕДДС в разговоре) в случаях, когда требуется вмешательство психолога;
- подключение переводчика в случаях, когда абонент разговаривает на языке, отличном от русского и оператор не владеет этим языком;

30) организация рабочего места администратора подсистемы со следующими функциями:
- регистрация на рабочем месте с правами администратора;

- предоставление гибкого интерфейса для настройки подсистемы в целом и всех составляющих модулей, в том числе:
  - настройка маршрутизации вызовов во всех МО;
  - настройка групп операторов ЕДДС, ДДС;
  - привязка групп операторов к службам;
  - настройка рабочих мест операторов;
  - настройка статистики и отчетности;
  - настройка модуля записи телефонных переговоров;
  - наличие возможности мониторинга работы всей подсистемы в целом так и отдельных модулей.

4.2.2.1 Функциональный компонент маршрутизации и распределения вызовов

Функциональный компонент маршрутизации и распределения вызовов должен обеспечивать выполнение следующих функций:

1) организация очереди входящих вызовов к операторской группе с возможностью настройки различных алгоритмов распределения вызовов между операторами (циклическое распределение вызовов, выбор наиболее свободного оператора, выбор наименее занятого диспетчера, др.) и с учётом следующих критериев:
   - информация АОН;
   - число вызовов, ожидающих в очереди к данной группе операторов;
   - квалификация оператора;
2) переадресацию вызова в двух режимах (с отключением оператора от разговора и с участием оператора в разговоре) на ДДС, другого оператора, группу операторов, эксперта, специалиста, психолога, переводчика, должностное лицо во всех возможных вариантах взаимодействия объектов Системы;
3) возможность автоматического голосового или SMS оповещения абонентов по заданному списку телефонов;
4) возможность выполнения оператором исходящих (в ТФОП) вызовов.

4.2.2.2 Функциональный компонент «Нормативно-справочная информация и база знаний»

Функциональный компонент «Нормативно-справочная информация и база знаний» должен обеспечивать выполнение следующих функций:

1) возможность хранения, наполнения и редактирования базы данных о типовых ситуациях, методах реагирования, используемой в системах поддержки принятия решений и консультативного обслуживания населения;
2) поддержание максимальной актуальности информации и сформированных знаний;
3) контекстный поиск с учетом атрибутов хранения данных, типов документов, возможность использования фильтров и шаблонов;
4) централизованное управление изменениями информационных объектов, контроль логической целостности и публикации;
5) выстраивание взаимосвязей между информационными объектами;
6) использование типовых сценариев реагирования на основе утвержденных ведомственных регламентов при ликвидации происшествий;
7) предоставление средств редактирования информационно-консультационной базы данных;
8) доступ оператора к информационно-консультационной базе данных и быстрый поиск в ней для получения информации о типовых ситуациях и методах реагирования.

4.2.2.3 Функциональный компонент консультативного обслуживания

Компонент консультативного обслуживания населения должен обеспечивать выполнение следующих функций:

1) размещение на общедоступном Портале ЕЦОР в сети Интернет документов нормативно-правового обеспечения по вопросам предупреждения и ликвидации чрезвычайных ситуаций;
2) информирование абонентов системы средствами системы голосового самообслуживания (InteractiveVoiceResponse):
   - автоматическое озвучивание текстовых документов;
   - навигация по голосовому меню с помощью DTMF-набора;
   - навигация по голосовому меню, при помощи функции распознавания речи.

4.2.2.4 Функциональный компонент контроля качества обслуживания

Функциональный компонент контроля качества обслуживания должен обеспечивать выполнение следующих функций:

1) поддержка записи и хранения телефонных разговоров операторов при обработке вызовов со следующими функциями:
   - централизованная запись телефонных разговоров;
   - централизованное управление и общая настройка подсистемы;

- запись всех переговоров операторов ЕДДС и ДДС;
- возможность записи не только аудиоинформации, относящейся к вызову, но и компьютерных экранов, которые оператор открывал на дисплее во время обслуживания вызова (опционально);
- резервирование серверов записи аудиоинформации, для записи IP телефонов по схеме N+N (“один к одному”) и N+M (“один к нескольким”);
- запись телефонных разговоров как с IP-телефонов, так и аналоговых аппаратов с единым интерфейсом для поиска и воспроизведения вызовов;

2) наличие собственной подсистемы отчётности для построения хронологических отчётов по статистикам записанных вызовов
3) возможность прослушивания записанных переговоров.

4.2.2.5 Функциональный компонент обучения

Функциональный компонент обучения должен обеспечивать выполнение следующих функций:

- хранение и предоставление доступа к библиотеке материалов;
- хранение и предоставление доступа к эксплуатационной документации;
- предоставление доступа к программным и техническим средствам для обучения.

4.2.3 Подсистема комплексного мониторинга

Основными функциями подсистемы комплексного мониторинга является следующие:

1) сбор и анализ параметров состояния контролируемых объектов от автомобильных терминалов системы экстренного реагирования «ЭРА-ГЛОНАСС»:
   - получение информации о произошедших ДТП;
   - получение географических координат ДТП;
   - получение данных о пострадавших;
   - передача отчетов о ходе реагирования в систему «ЭРА-ГЛОНАСС»;
2) сбор и анализ параметров состояния контролируемых объектов от терминалов «ГЛОНАСС/GPS», установленных на транспортных средствах экстренных оперативных служб, привлеченных к реагированию на происшествие и транспортных средствах, перевозящих опасные грузы:
   - получение информации о географических координатах объекта;
   - получение информации о параметрах вектора скорости объекта;
   - получение информации о метке времени (если информация передается терминалом ГЛОНАСС);

- получение сигнала о возникновении внештатной ситуации;

3) сбор параметров состояния контролируемых объектов:
   - отслеживание с привязкой к объекту и реальному времени работы как в событийном режиме, так и в режиме периодического опроса по инициативе с диспетчерского центра, в том числе и автоматически по заданному алгоритму;
   - автоматическая регистрация событий, происходящих на контролируемых объектах, с их привязкой к объекту, географическим координатам и реальному времени (в режиме «черный ящик»);
   - аварийная и предупредительная сигнализация о возникновении внештатных ситуаций на контролируемых объектах;
   - отображение в реальном масштабе времени перемещения (места) и состояния мобильного объекта на плане города (карте местности);
4) формирование и передача в другие компоненты Системы вызова по внештатной ситуации на контролируемых стационарных и подвижных объектах;
5) взаимодействие со следующими компонентами Системы:
   - подсистемой ГИС в части передачи географических координат подвижных объектов;
   - АРМ оператора ЕДДС в части сигнализации о возникновении внештатных ситуациях на объектах мониторинга;
6) осуществление мониторинга контролируемых объектов в реальном масштабе времени;
7) предоставление мониторинговой и необходимой архивной информации допущенным пользователям в реальном масштабе времени;
8) создание и поддержание архивной базы данных, запись мониторинговой информации в архив;
9) администрирование базы учетных данных (ведение карточек объектов, зарегистрированных в системе);
10) разграничение прав доступа пользователей к базе данных;
11) квитирование всех проходящих через «интегрирующий узел» сообщений;
12) работы в режиме "уточненных" координат (дифференциальный режим).

4.2.3.1 Компонент систем мониторинга и обеспечения безопасности

Компонент систем мониторинга и обеспечения безопасности должен обеспечивать решение следующих задач:

- прием и обработка информации и сигналов, поступающих от датчиков (соответствующих автоматизированных систем), установленных на контролируемых стационарных и подвижных объектах, в том числе терминалов ГЛОНАСС/GPS, установленных на следующих транспортных средствах:
- экстренных оперативных служб, привлеченных к реагированию на происшествие;
- городских служб, привлеченных к реагированию на происшествие;
- осуществляющих перевозку детей;
- перевозящих опасные грузы;
- муниципальный маршрутный городской транспорт, осуществляющий пассажирские перевозки.

2) интеграция с системой видеоанализа с целью обеспечения следующих возможностей:
   - автоматическое уведомление оператора ЕЦОР о событиях выявленных системами видеоидентификации и видеоанализа с привязкой события к электронной карте с автоматическим заполнением регистрационной карточки события;
   - автоматически уведомление оператора ЕЦОР об активации сигнала тревоги при регистрации микрофоном, установленном на камере звука выше критического уровня с привязкой события к электронной карте с автоматическим заполнением регистрационной карточки события;
   - отображение на электронной карте мест расположения камер видеонаблюдения с указанием направлений обзора;
   - переход из электронной карты к видеопотоку выбранной оператором камеры.
3) интеграция с системами пожарной безопасности, системами охранной сигнализации и системами мониторинга природной и техногенной безопасности с целью обеспечения следующих возможностей:
   - автоматическое уведомление оператора ЕЦОР о событиях, выявленных системами;
4) отображение на электронной карте мест срабатывания датчиков систем.

4.2.3.2 Компонент видеомониторинга и видеоанализа

Программное обеспечение подсистемы видеонаблюдения и видеоанализа, должно обладать следующими функциями:

1) представление всех обнаруженных целей (человек, автомобиль, группа людей) и событий в реальном времени как на общем плане наблюдаемого объекта, так и на детализированных планах;
2) оператору должна предоставляться общая картина происходящего на объекте таким образом, чтобы при необходимости, оператор мог иметь возможность повысить уровень детализации в интересующем месте и получить более детальную информацию о месте возникновения происшествия;
3) отображение областей видимости обзорных камер на планах подсистем с возможностью выбора камеры для просмотра посредством ее выделения на плане;
4) иерархическая организация видеоисточников, аналитических регистраторов, устройств управления. Распределение прав пользователей по доступу к источникам видео и событий по аппаратному или логическому принципу. Каждый оператор должен иметь полномочия по доступу к источникам на просмотр, модернизацию параметров, получение текущего состояния, просмотр архива с указанием глубины и т. д. в соответствии с его служебными полномочиями;
5) установка степени важности тревог с определением группы операторов-получателей;
6) оперативное уведомление оператора о сложившихся нештатных ситуациях с предоставлением информации о времени, месте, характере ситуации, автоматическим предоставлением видеоинформации одновременно в записи и реального времени, а так же поддержкой режима оценки оператором каждой из ситуаций;
7) система приоритетов по доступу к источникам и исполнительным устройствам. Администраторы системы должны определять приоритеты управления поворотными и прочими исполнительными устройствами для всех операторов;
8) мониторинг состояния всех элементов системы в реальном времени из любой точки сетевой среды. Операторы должны получать информацию о работоспособности системы в реальном времени. При отказе узла должны получать тревожное сообщение;
9) унифицированный интерфейс настройки сетевых источников видеосигнала с возможностью оперативного доступа. Система должна позволять из единого центра администрировать все распределенные источники видеосигнала и

видеорегистраторы с аналитикой при помощи единого приложения с мгновенным применением результатов в режиме работы системы на всех уровнях иерархии;

10) распознавание целей (люди, автомобили, оставленный предмет, дым, огонь) и тревожных ситуаций в режиме реального времени по видеоизображению, получаемому от неподвижных видеокамер (Master-камер);
11) задание одного из режимов работы поворотных:
    - цикличное патрулирование предустановленных зон;
    - управление по командам оператора;
    - автоматическое наведение на обнаруживаемые цели.
12) патрулирования поворотной камерой путем циклической смены зон наблюдения в автоматическом режиме и реализации функций видеорегистрации, и обнаружения нештатных ситуаций для каждой зоны обзора;
13) управление поворотными камерами следующими способами:
    - виртуальный джойстик;
    - указание интересующей области на видеоизображении;
    - указание интересующей области на электронной карте.
14) автоматическое наведение поворотных камер на обнаруженные цели (человек, ТС, группа людей) с оптическим увеличением и сопровождением по видеоизображению с обзорной камеры;
15) формировать по каждому событию короткометражный видеоролик для оперативного анализа и реагирования;
16) при наличии двух и более камер с пересекающимися секторами обзора, должен быть предусмотрен режим передачи сопровождаемой цели от одной камеры к другой.
17) выбор режима сопровождения целей (сопровождение целей, вызвавших тревогу, сопровождение всех обнаруженных целей);
18) указание интересующей области для оптического увеличения при помощи поворотной камеры, посредством плана объекта и видеоизображения сопряженной с ней неподвижной камеры;
19) формирование в режиме реального времени базы данных распознанных целей;
20) привязка зон обзора неподвижных видеокамер к карте охраняемого объекта, проекции мнемоник движущихся целей на карту объекта;
21) выдача аудиовизуального сигнала оператору в случае возникновения тревожной ситуации;
22) оперативное уведомление оператора о сложившихся нештатных ситуациях с предоставлением информации о времени, месте, характере ситуации,

автоматическим предоставлением видеоинформации одновременно в записи и реального времени, а так же поддержкой режима оценки оператором каждой из ситуаций;

23) обеспечение круглосуточного наблюдения за ситуацией в зонах наблюдения;

24) обеспечение просмотра архива с возможностью поиска видеофрагментов по определенным условиям (дата, время, камера, тип цели и т.д.).

4.2.3.2.1 Требования к подсистеме видеонаблюдения и видеоанализа

Видеокамеры или кодеры (преобразователи аналогового сигнала в цифровой) должны поддерживать интерфейс ONVIF версии 1.02 или выше, тип устройства передатчик сетевого видео (NVT), профиль Profile S. Передатчики сетевого видео, включая камеры и видеосервера, должны поддерживать компрессию H.264 MainProfile, MJPG MainProfile для передачи потокового видео и JPEG для передачи отдельных кадров. Видеоаналитические сервера, подключаемые к сетевым камерам, должны на выходе поддерживать интерфейс ONVIF версии 2.2 или выше, тип устройства аналитика сетевого видео (NVA) для передачи видео и результатов работы видеоаналитики от сервера к другим компонентам.

4.2.3.2.2 Требования к аналитическим функциям подсистемы видеоанализа

Подсистема видеоанализа должна обладать возможностью реализации следующих нижеперечисленных аналитических функций.

Ситуационные:

- обнаружение скопления людей, в том числе в несанкционированных местах;
- оценка плотности потока людей на значимых для города объектах;
- выявление фактов неадекватного движения человека;
- индексирование событий в условиях дорожного движения (плотность потока, заторы, массовое скопление автотранспорта), в том числе в парковочных зонах;
- детектор оставленных предметов и их владельцев;
- детектор повышенной активности людей в контролируемой зоне;
- детектор запрещенного или нетипичного движения автотранспорта, людей;
- детектор задымления и открытого огня;
- детектор фактов пересечения запрещенной зоны (проезд, проход);
- детектор исчезнувших предметов;
- реагирование на проход людей в заданном направлении (входы, выходы, переходы, коридоры и т.п.);
- появление человека или автомобиля в зоне наблюдения (улицы, площади, перекрестки, парки).

Сервисные:

- расфокусировка видеокамеры;
- загрязнение объектива видеокамеры;
- изменение фона;
- изменение зоны обзора, отворачивание камеры;
- заслонение объектива камеры.

4.2.3.2.3 Требования к пороговым условиям срабатывания алгоритмов подсистемы видеоанализа

Компонент должен обеспечить следующее качество распознавания:

- вероятность распознавания чистых контрастных регистрационных номеров транспортных средств (удовлетворяющих требованиям ГОСТ Р 50577-93, ГОСТ 3207-77 и Венской конвенции о дорожном движении) - более 99%;
- вероятность распознавания в реальном транспортном потоке - более 95%;
- максимально допустимая скорость движения транспортного средства в зоне контроля - 150 км/ч (потоковая версия) или 20 км/ч (паркинговая версия);
- размер номерной пластины в кадре: высота больших символов — 14–27 пикселов; ширина пластины — 120–180 пикселов;
- чувствительность - не менее 50 лк;
- угол наклона камеры - по вертикали до 30°, по горизонтали до 30°;
- допустимый интервал следования легковых автомобилей - 3 м (угол наклона камеры по вертикали 30°);
- допустимый интервал следования грузовых автомобилей - 7 м (угол наклона камеры по вертикали 30°).

4.2.3.2.4 Требования к транспортным алгоритмам подсистемы видеоанализа

Минимальный размер изображения ТС, за которым ведётся наблюдение, с элементами аналитики должен соответствовать 10x10 пикселов.

Относительная погрешность определения скорости ТС по видеоданным: не более 20%.

4.2.3.2.5 Требования к алгоритмам «Обнаружения движения/прохода» подсистемы видеоанализа

Минимальный размер целей, детектируемых и классифицируемых алгоритмами должен составлять: 6 пикселей в высоту, 4 пикселя в ширину.

4.2.3.2.6 Требования к алгоритму «Оставленный предмет» подсистемы видеоанализа

Минимальный размер предмета, детектируемого алгоритмами должен составлять 20 пикселей.

4.2.3.2.7 Требования к алгоритму «Возгорание» подсистемы видеоанализа

Минимальный размер возгорания, детектируемого алгоритмами, должен составлять 20 пикселей. Минимальный размер ауры огня не более 8х8 пикселей.

4.2.3.2.8 Требования к алгоритму «Скопление людей» подсистемы видеоанализа

Минимальный размер человека должен составлять не менее 4 х 15 пикселей. Минимальное кол-во людей считаемых скоплением не менее 4.

4.2.3.2.9 Требования к алгоритму «Подсчет людей» подсистемы видеоанализа

Минимальный линейный размер человека на изображении должен составлять 16 пикселей.

4.2.3.2.10 Требования к алгоритму «Шагающий мастер» и алгоритмам на поворотных видеокамерах подсистемы видеоанализа

Требования к размерам целей аналогичны стационарным камерам. Время нахождения в каждой препозиции не менее 7 секунд. Для алгоритмов обнаружения оставленных предметов, возгорания время нахождения в каждой препозиции не менее 30 секунд.

4.2.3.2.11 Требования к клиентскому приложению подсистемы видеоанализа для операторов ЕЦОР

Клиентское приложение подсистемы видеоанализа для операторов ПАК ЕЦОР должно обеспечивать следующее:

- прием и обработку потока информации, поступающей от объектового оборудования;
- обработку цветного изображения;
- управление отображением видеоинформации;
- формирование мультиэкранного изображения с возможностью одновременного просмотра до 64 видеокамер;
- возможность экспорта или распечатки выбранного кадра («стоп-кадр»);
- взаимодействие со средствами архивирования видеоинформации для просмотра архивов;
- возможность просмотра изображения с видеокамер или архива в полноэкранном режиме;

- возможность просмотра архивного изображения в выбранных зонах наблюдения при одновременном контроле текущей ситуации в других зонах;
- просмотр архива событий (фильтрация по типу событий, дате и другим параметрам).
- поддержку автоматического звукового (должна быть предусмотрена возможность программного отключения данной функции администратором) и визуального оповещения о срабатывании детектора движения независимо для каждой видеокамеры с автоматическим включением записи;
- возможность дистанционного управления исполнительными устройствами;
- аутентификацию оператора;
- протоколирование всех действий оператора на АРМ;
- сохранение работоспособности при кратковременном пропадании электропитания.

4.2.4 Интеграционная географическая информационная подсистема

Интеграционная геоинформационная подсистема должна иметь механизмы взаимодействия с уже имеющимися геоинформационными подсистемами ДДС, либо удовлетворять требованию заменимости.

Объем и распределение предоставляемой информации по рабочим местам должностных лиц определяется на этапе технического проектирования ЕЦОР.

В подсистеме должен быть предусмотрен механизм регулярного обновления электронных карт подсистемы для обеспечения актуальности картографической информации.

Пользовательский интерфейс подсистемы должен предоставлять следующие функциональные возможности:

- атрибутивный поиск на карте объектов классифицированных типов;
- указание и уточнение местоположения объектов, связанных с происшествием, как с помощью визуальных графических средств, так и с помощью прямого ввода координат;
- прокладка маршрутов движения между заданными объектами;
- определение загруженности дорог.

Интеграция Подсистемы приема и обработки обращений и Интеграционной геоинформационной системой происходит на двух уровнях:

1) на уровне интеграционной шины для подготовки географической информации в автоматическом режиме;
2) на уровне АРМ оператора для предоставления оператору возможности работы с картой on-line (приближение, перемещение, измерение и т.д.).

Общие функции интеграционной геоинформационной системы:

1) отображение картографических слоев многослойного цифрового плана города (здания, границы кварталов, зеленые массивы, водные объекты, железные дороги, мосты, улицы и т.д.) в произвольном масштабе с возможностью настройки параметров отображения (порядок отображения слоев, цвета и стили линий и заливок, шрифты надписей, использование условных знаков и т.д.);
2) обеспечение по завершении ввода заявки о пожаре (ЧС) отображение фрагмента карты с центром в точке соответствующей центроиду объекта пожара (ЧС);
3) выполнение пространственных измерений;
4) вычисление прямоугольных или географических координат объекта по его почтовому адресу и наоборот (поддержка геокодирования);
5) поиск объекта по его почтовому адресу, телефону, наименованию;
6) справка об объектах под курсором с получением информации по базам данных;
7) поиск объекта по таблице с отображением на карте;
8) поиск объекта по названию, включая определение его адреса или координат; при визуализации плана (карты) он(а) должна панорамироваться к этому объекту, объект должен при этом быть подсвечен;
9) оперативное отображение картографической информации и объектов учета и мониторинга на АРМ оператора ЕДДС:
   - местоположение абонента;
   - место возникновения происшествия (при наличии информации о географическом местоположении);
   - критически важные объекты, находящиеся под наблюдением системы мониторинга;
   - подчиненные и задействованные мобильные силы и средства (только при получении такой информации от соответствующих ДДС);
   - природно-географические, социально-демографические, экономические и другие характеристики территории;
   - соседние ДДС;
10) для каждого ДДС отображение объектов учета и мониторинга, входящих в зону ответственности данного ДДС;
11) атрибутивный поиск на карте объектов классифицированных типов;
12) указание и уточнение местоположения объектов, связанных с происшествием, как с помощью визуальных графических средств, так и с помощью прямого ввода координат;
13) прокладка маршрутов движения между заданными объектами.

4.2.5 Интернет – портал

Интернет-портал должен предоставлять пользователям сети Интернет следующие возможности:

1) предоставлять актуальную информацию о событиях, напрямую или косвенно связанных с обеспечением безопасности жизнедеятельности, а так же о допустимых к общему доступу инцидентах и заявках с обозначением их статуса и с привязкой к местности (обозначением на электронной карте города);
2) информировать оператора ПАК ЕЦОР о зарегистрированных, посредством Интернет – портала, событиях с автоматической регистрацией и постановкой заявки на контроль исполнения;
3) предоставление пользователям сети Интернет актуализированной информации о событиях, связанных с безопасностью жизнедеятельности;
4) предоставление информации о статусах исполнения обращений граждан с отображением на электронной карте города;
5) возможность присоединения мультимедийной информации к сообщению о событии;
6) определение устройства пользователя, обращающегося на интернет портал с автоматическим предоставлением соответствующей версии интернет портала (для мобильных устройств – мобильную версию);
7) фильтрация зарегистрированных событий, отображаемых на электронной карте интернет портала по следующим критериям:
   - завершенные события;
   - обрабатываемые события;
   - категории событий;
   - события по заданному периоду времени.

Веб-клиент должен работать в интернет-браузерах таких как InternetExplorer, MozillaFirefox, GoogleChrome, Safari, Opera, OperaMini.

4.2.6 Подсистема обеспечения координации и взаимодействия

Подсистема обеспечения координации и взаимодействия должна выполнять следующие функции:

1) организация межведомственного взаимодействия в работе служб оперативного/экстренного реагирования при реагировании на чрезвычайные ситуации;
2) обеспечение возможности управления статусами инцидентов в многопользовательском режиме;

3) автоматизированное формирование поручений на основе заранее подготовленных шаблонов и сценариев реагирования;
4) контроль хода исполнения поручения и автоматический запуск сценариев информирования при угрозе срыва срока исполнения поручения.

4.2.7 Подсистема комплексного информирования и оповещения

Основной функцией подсистемы комплексного информирования и оповещения является объединение в организационно-техническую систему аппаратно-программных средств обработки, передачи и отображения аудио и видеоинформации в целях:

- подготовки населения в области гражданской обороны, защиты от чрезвычайных ситуаций;
- обеспечения пожарной безопасности;
- безопасности на водных объектах;
- охраны общественного порядка;
- своевременного оповещения и оперативного информирования граждан о КСП и угрозе террористических акций;
- мониторинга обстановки и состояния правопорядка в местах массового пребывания людей на основе использования современных технических средств и технологий.

4.2.8 Подсистема информационной безопасности

ПИБ должна представлять комплекс из организационных мер и программно-технических средств и должна обеспечивать:

- управление доступом к информационным ресурсам ПАК ЕЦОР;
- обеспечение безопасности при межсетевом взаимодействии;
- регистрацию и учет работы пользователей;
- обеспечения целостности информации;
- антивирусную защиту;
- обнаружения вторжений;
- криптографическую защиту, передаваемых данных.

4.2.8.1 Функциональный компонент управления доступом

Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Должна осуществляться идентификация терминалов, узлов сети, каналов связи, внешних устройств по логическим именам.

Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

4.2.8.2 Функциональный компонент регистрации и учета

Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная - несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке.

Должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ.

Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный - несанкционированный).

Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

- идентификатор субъекта доступа;
- спецификация защищаемого файла.

Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)].

Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

Учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

4.2.8.3 Функциональный компонент обеспечения целостности

Должна быть обеспечена целостность программных средств ПОИБ, а также неизменность программной среды.

Целостность ПОИБ проверяется при загрузке системы по контрольным суммам компонент системы защиты.

Целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

Должна осуществляться физическая охрана технических средств (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации, особенно в нерабочее время.

Должно проводиться периодическое тестирование функций ПОИБ при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД.

Должны быть в наличии средства восстановления ПОИБ, предусматривающие ведение двух копий программных средств ПОИБ и их периодическое обновление и контроль работоспособности.

4.2.8.4 Функциональный компонент обеспечения безопасного межсетевого взаимодействия

В связи с наличием подключения ИСПДн к сетям связи общего пользования данный функциональный компонент должен быть реализован путем использования средств межсетевого экранирования, соответствующих 3 (третьему) классу защищенности в соответствии с РД ФСТЭК «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». В целях выполнения требований законов и подзаконных нормативных актов, регламентирующих вопросы защиты конфиденциальной информации, в том числе персональных данных, используемые межсетевые экраны как средства защиты информации должны в установленном порядке пройти процедуру оценки соответствия ФСТЭК России.

4.2.8.5 Функциональный компонент анализа защищенности

Средства анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему. В целях выполнения требований законов и подзаконных нормативных актов, регламентирующих вопросы защиты конфиденциальной информации, в том числе персональных данных, используемые средства анализа защищенности как средства защиты информации должны в установленном порядке пройти процедуру оценки соответствия ФСТЭК России.

4.2.8.6 Функциональный компонент обнаружения вторжений

Данный компонент должен быть реализован путем использования в составе ИСПДн сертифицированных программных или программно-аппаратных средств (систем) обнаружения вторжений.

4.2.8.7 Функциональный компонент антивирусной защиты

В составе ИСПДн на рабочих станциях и серверах должны применяться сертифицированные средства антивирусной защиты в целях защиты ПДн и программно-технических средств от воздействия вредоносного программного обеспечения.

Указанный перечень функциональных компонентов может быть уточнен и изменен по согласованию с Заказчиком на этапе технического проектирования.

Для программных средств, используемых при защите информации в ИСПДн, должен быть обеспечен четвертый уровень контроля отсутствия НДВ. Все программное и аппаратное обеспечение, реализующее функционал защиты информации, должно быть сертифицировано в системе сертификации ФСТЭК России.

4.3 Требования к видам обеспечения

4.3.1 Требования к математическому обеспечению

В состав математического обеспечения Системы входят алгоритмы и проектные процедуры, на основе которых разрабатываются функциональные подсистемы ПАК ЕЦОР.

Описание моделей, процессов, алгоритмов и процедур должны включать:

- логику и способы формирования результатов решения с указанием последовательности этапов алгоритма, необходимых расчетных и (или) логических формул;
- указания о точности вычисления (при необходимости);
- описание связей между частями и операциями алгоритма (процедуры).

Математическое обеспечение должно предусматривать все ситуации (логические ветви алгоритма), которые могут возникнуть в процессе решения задач функциональными подсистемами.

Алгоритмы (процедуры) могут быть представлены одним из следующих способов:

- графический (в виде схемы);
- табличный;
- текстовой;
- смешанный (графический или табличный с текстовой частью).

Способ представления алгоритма выбирает разработчик, исходя из сущности описываемого алгоритма и возможности формализации его описания.

4.3.2 Требования к информационному обеспечению

Информационное обеспечение Системы – это совокупность форм документов, классификаторов, нормативной базы (компоненты информационного обеспечения) и реализованных решений по объемам, размещению и формам существования информации, применяемой при функционировании Системы.

Решения по объемам, размещению и формам существования информации, должны быть реализованы в информационной базе Системы.

Информационное единство в ПАК ЕЦОР должно обеспечиваться использованием общих информационных ресурсов, в том числе единой системы кодирования и классификации информации, а также алгоритмами функционирования программно-технических средств.

Единая система кодирования и классификации информации должна обеспечивать:

- централизованное ведение словарей и классификаторов, использующихся в информационном взаимодействии;
- выполнение необходимых технологических функций, в том числе предоставление возможности обмена данными с внешними по отношению к ЕЦОР системами.

Для общероссийских классификаторов должен обеспечиваться импорт обновлений из файлов, полученных от организации, ответственной за ведение этого классификатора.

Процессы сбора, обработки, передачи данных в ПАК ЕЦОР и предоставлению данных должны быть реализованы в операциях:

- однократного ввода данных в Систему и многократного их использования при решении задач обеспечения безопасности населения и безопасности городской коммунальной инфраструктуре на различных уровнях ПАК ЕЦОР;
- формирования, ведения, применения баз данных ПАК ЕЦОР;
- настройки программного обеспечения;
- хранения, обновления информации о событиях;
- репликации информации по компонентам ПАК ЕЦОР;
- обмена информацией в режиме импорта-экспорта в соответствии с регламентами информационного обмена, реализуемого прикладным программным обеспечением;
- обеспечения информационной совместимости ПАК ЕЦОР с информационными системами субъектов на всех уровнях.

Процессы сбора, обработки и передачи данных в Системе должны определяться ведомственными нормативно-техническими документами и быть отражены в должностных инструкциях сотрудников подразделений – пользователей Системы.

4.3.3 Требования к лингвистическому обеспечению

Лингвистическое обеспечение Системы (ЛО) – это совокупность средств и правил для формализации естественного языка, используемых при общении пользователей и эксплуатационного персонала при функционировании Системы.

Лингвистическое обеспечение должно быть направлено на формализацию смыслового содержания информации на естественном языке с целью автоматизации ее обработки, хранения, редактирования и поиска.

Для формализации и значительного сжатия информации должны применяться автоматизированные процедуры индексирования и классификации (рубрицирования) текстов - Web-серверная технология, а также традиционные способы обработки, хранения, редактирования и поиска информации для решения конкретных информационных задач по ведению различных классификаторов, словарей, нормативно - справочной информации и т.п. с использованием механизма запросов к СУБД.

Способы организации диалога с пользователем Системы должны обеспечивать уменьшение вероятности совершения оператором случайных ошибок, предусматривать логический контроль ввода данных, формирование запросов на обновление информации и решение расчетно-информационных задач.

Общение пользователя с Системой должно происходить в интерактивном режиме путем работы с интерфейсом системы (экранными формами, встроенных меню и пр.).

В целом ЛО должно удовлетворять потребности пользователей Системы в языковых средствах.

Лингвистическое обеспечение должно обеспечивать:

- текстовый и графический способы общения субъектов и пользователей Системы со средствами автоматизации;
- диалоговый режим общения пользователей со средствами автоматизации с возможностью конструирования диалогов в интересах пользователей;
- формирование запросов с АРМ пользователей Системы и запуск задач;
- защиту от ошибок и некорректных действий пользователей системы.

Должны быть унифицированы диагностические сообщения, выдаваемые пользователю на АРМ пользователя Системы, сообщения о несанкционированных действиях пользователей.

В состав лингвистического обеспечения должны входить:

- языковые средства пользователей;
- словари терминов;
- правила формализации данных, включая методы сжатия и развертывания текстов, представленных на естественном языке.

Языковые средства пользователей должны обеспечивать:

- ввод, обновление, просмотр и редактирование информации;
- идентификацию и адресацию входной информации;
- поиск, просмотр и выдачу подготовленной информации на устройства отображения и печати;

- возможность представления информации в сообщениях в виде, позволяющем производить их автоматическую обработку (в том числе синтаксический и семантический контроль);
- исключение неоправданной избыточности и неоднозначности;
- формализацию документальных данных.

Языки ввода-вывода данных должны поддерживать реляционную и объектно-реляционную базы данных.

Словари терминов должны быть разработаны для реализации процессов информационного обмена на основе единого для всех компонентов Системы языка.

Словари терминов должны содержать лексику, дополненную при необходимости общепринятыми терминами с указанием смысловых связей между терминами.

4.3.4 Требования к программному обеспечению

Программное обеспечение ПАК ЕЦОР должно представлять собой совокупность общего программного обеспечения (ОПО) и специального программного обеспечения (СПО).

Программное обеспечение Системы должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в состав средств информатизации новых объектов Системы.

Программное обеспечение, технология (включая нормативно-техническую документацию) его разработки должны обеспечивать возможность согласованной разработки унифицированного (типового) программного обеспечения силами нескольких разработчиков.

Программное обеспечение должно быть сертифицировано по требованиям безопасности информации.

4.3.4.1 Требования к общему программному обеспечению

ОПО должно представлять собой совокупность программных средств со стандартными интерфейсами Российской Федерацией, предназначенных для организации и реализации информационно-вычислительных процессов в Системе. Состав ОПО формируется при проектировании конфигурации ПТК интегрируемых информационных систем.

ОПО должно обеспечить:

- выполнение информационно-вычислительных процессов совместно с другими видами обеспечения;
- управление вычислительным процессом и вычислительными ресурсами с учетом приоритетов пользователей;

- коллективное использование технических, информационных и программных ресурсов;
- обмен неформализованной и формализованной информацией между компонентами Системы, а также между Системой и пользователями с протоколами информационно-логического взаимодействия;
- ведение учета и регистрации передаваемой и принимаемой информации;
- ввод в базы данных информации с клавиатуры АРМ и с машинных носителей, а также информации, поступающей через телекоммуникационные средства;
- автоматизированный контроль и диагностику функционирования технических и программных средств, а также тестирование технических средств;
- создание и ведение баз данных с обеспечением контроля, целостности, сохранности, реорганизации, модификации и защиты данных от несанкционированного доступа;
- создание и ведение словарей, справочников, классификаторов и унифицированных форм документов, параллельный доступ пользователей к ним;
- поиск по запросам информации в диалоговом режиме и представление ее в виде документов;
- выполнение распределенных запросов к данным;
- синхронизацию корректировки данных и контроль за изменением документов в базах документов;
- разработку, отладку и выполнение программ, формирующих распределенные запросы к данным;
- формирование и ведение личных архивов пользователей;
- организацию решения функциональных задач СПО;
- наращивание состава общего программного, а также специального программного, информационного и лингвистического обеспечения;
- обработку (формирование, контроль, просмотр, распознавание, редактирование, выдачу на средства отображения и печати) текстовой, табличной и графической информации;
- восстановление работоспособности ПО и баз документов (из резервных копий) после сбоев и отказов технических и программных средств.

ОПО должно поддерживать функционирование выбранных типов ПЭВМ и периферийных устройств на уровне операционных систем (ОС), утилит и драйверов. Операционные системы должны выбираться исходя из перспектив развития аппаратно-программных платформ в мире, с учетом поддержания преемственности версий и редакций, условий и порядка их обновления,

предлагаемых фирмой - разработчиком. Количество ОС, их версий и редакций в Системе должно быть минимизировано.

ОПО может включать следующие основные компоненты:

- графические 32 (64 и более) - разрядные многозадачные (многопроцессорные) операционные системы;
- сетевые операционные системы;
- системы управления базами данных;
- телекоммуникационные программные средства, включая средства электронной почты;
- средства архивирования файлов;
- инструментальные средства для создания и ведения текстовых и графических документов, электронных таблиц и т.д.;
- средства поддержки Internet и Intranet -технологий;
- средства управления выводом данных на устройства отображения информации группового и коллективного пользования;
- технологические программные средства.

Должно быть обеспечено ведение депозитария для всего ПО, а также создание дистрибутивов для любого ПТК Системы и распространение программного обеспечения на все компоненты Системы.

Поставляемое ПО, если это предусмотрено существующей нормативной правовой базой, должно быть сертифицировано (в том числе по требованиям безопасности информации) или иметь соответствующие сертификаты. Вопросы его использования и тиражирования должны регулироваться соответствующими соглашениями или сублицензионными договорами.

4.3.4.1.1 Требования к системам управления базами данных

Используемая в ПАК ЕЦОР система управления базами данными (СУБД) должна быть промышленного изготовления с необходимыми лицензиями.

СУБД должна представлять собой комплекс программ и языковых средств, предназначенных для создания, ведения и использования баз данных.

СУБД в общем должна обеспечивать контроль, обновление (ввод и корректировку) и восстановление данных об обращениях, событиях, а также обмен информационными ресурсами между базами данных субъектов ПАК ЕЦОР, связанных между собой по иерархии программ с участием специального программного обеспечения (СПО) и общего программного обеспечения (ОПО).

Общими требованиями к СУБД являются:

- применение русского языка на уровнях пользовательского интерфейса и системных сообщений;
- поддержка реляционной или объектно-реляционной модели базы данных;
- автоматическое восстановление базы данных;
- совместимость с различными операционными системами серверов БД;
- поддержка сетевых протоколов TCP/IP;
- возможность контроля доступа к данным;
- централизованное управление учетными записями пользователей;
- оптимизация запросов.

4.3.4.2 Требования к специальному программному обеспечению

Специальное ПО подсистем ПАК ЕЦОР должно быть реализовано на базе отечественных программных разработок.

При разработке задач СПО должно быть обеспечено использование всех возможностей, предоставляемых средствами ОПО (системными сервисами) по обработке данных.

Для обеспечения возможности наращивания функциональности СПО должна быть разработана нормативно-техническая документация, содержащая описания принятых в системе протоколов и интерфейсов, выполнение которых позволит задаче нормально функционировать в операционной и информационной среде Системы.

Для обеспечения принципов сохранения ранее вложенных инвестиций и соблюдения преемственности функциональной наполненности ПТК информационных систем субъектов Системы создаваемое СПО должно по возможности функционировать в среде текущего состояния ОПО.

СПО должно быть спроектировано и реализовано таким образом, чтобы обеспечивались:

- функциональная полнота - реализация всех, подлежащих автоматизации функций объектов автоматизации;
- возможность адаптации и настройки программных средств с учетом специфики каждого объекта;
- эргономичность - обеспечение удобства и унификации пользовательского интерфейса Российской Федерации;
- защита от ошибочных действий оператора (пользователя);
- контроль и защита от некорректных исходных данных.

4.3.5 Требования к техническому обеспечению

Техническое обеспечение ПАК ЕЦОР – это совокупность всех технических средств, используемых при эксплуатации ПАК ЕЦОР.

Техническое обеспечение представляет собой основу ПАК ЕЦОР и должно включать:

- средства вычислительной техники;
- средства коммуникационной техники;
- средства организационной техники.

Средства вычислительной техники должны обеспечивать реализацию комплексных технологий обработки и хранения информации и являться базой интеграции всех современных технических средств обеспечения управления информационными ресурсами.

Коммуникационная техника должна обеспечивать реализацию технологий передачи данных и предполагает как автономное функционирование, так и функционирование в комплексе со средствами компьютерной техники.

Организационная техника должна обеспечивать реализацию технологий хранения, представления и использования информации, а также выполнение различных вспомогательных операций в рамках тех или иных технологий информационной поддержки управленческой деятельности.

В целом техническое обеспечение ПАК ЕЦОР должно отвечать следующим требованиям:

- базироваться на сертифицированных образцах средств вычислительной техники, средств коммуникационной техники, средств организационной техники;
- обладать информационной, программной и технической совместимостью, адаптируемостью к условиям функционирования, возможностью расширения с целью подключения новых устройств;
- обеспечивать устойчивую управляемость, надежное хранение информации, оперативность ее обработки, малое время отклика при большом количестве запросов, а также резервное копирование и восстановление информации, наличие источников бесперебойного питания;
- комплектация автоматизированных рабочих мест (АРМ) с повышенными требованиями по информационной безопасности согласуется Заказчиком отдельно;
- вся поставляемая электронно-вычислительная техника должна соответствовать или превышать требования технических спецификаций по производительности и эргономическим показателям;
- рабочие станции, серверы, системы хранения данных поставляются, по возможности, от одного производителя;

Вся электронно-вычислительная техника ПАК ЕЦОР должна функционировать при следующих условиях: параметры электропитания - качество электрической энергии в сети переменного тока должно соответствовать требованиям ГОСТ 13109; после воздействия повышенной относительной влажности окружающей среды (98%) при температуре 25°С; в условиях воздействия рабочей пониженной температуры окружающей среды 5°С; в условиях воздействия рабочей повышенной температуры окружающей среды 40°С; после пребывания в условиях пониженной температуры окружающей среды минус 50°С; после пребывания в условиях повышенной температуры окружающей среды 50°С; за исключением особо оговоренных в спецификациях случаев уровень шума при работе отдельных устройств не должен превышать 30 дБ в полосе частот 50-3000 Гц на расстоянии 1 м;

Средства вычислительной техники должны быть максимально приспособлены для последующей модернизации.

Исполнитель должен обеспечить обслуживание компьютеров в течение гарантийного срока на КТС в целом и всего срока службы (не менее 3 лет) своими силами, либо по договору с другими организациями на всей территории Российской Федерации как на период гарантийного, так и послегарантийного обслуживания.

Гарантийное обслуживание должно обеспечиваться в соответствии с программой обеспечения надежности либо сервисными центрами Исполнителя/Оператора, либо сервисными центрами, работающими по договору с Заказчиком. Поддержка и обновление лицензионного ПО определяются условиями соглашения между Заказчиком и Исполнителем.

4.3.5.1 Требования к видам технических средств, в том числе к видам комплексов технических средств, программно-технических комплексов

4.3.5.1.1 Дежурно диспетчерские службы (ДДС)

Оборудование ДДС включает, как минимум:

- автоматизированные рабочие места оперативного дежурного и диспетчера дежурной смены;
- активное оборудование локальной вычислительной сети;
- структурированную кабельную сеть;
- средства связи;
- источник гарантированного электропитания.

4.3.5.2 Требования к функциональным, конструктивным и эксплуатационным характеристикам средств технического обеспечения системы.

Выбор технических средств ПАК ЕЦОР должен строиться на основе ориентации на отечественный рынок ИКТ, использования совокупности научно обоснованных оценочных критериев, состав которых предопределен целями, составом функций и структурой ПАК ЕЦОР.

Исходными данными для выбора технических средств являются:

- характеристики функциональных задач ПАК ЕЦОР;
- характеристики задач обеспечения информационной безопасности ПАК ЕЦОР;
- заявленные производителем технические характеристики оборудования.

Формирование КТС ПАК ЕЦОР должно изначально осуществляться на основе использования АРМ пользователей существующих информационных систем, (с проведением необходимых организационно-технических мероприятий по обеспечению информационной безопасности), а в дальнейшем увеличения числа АРМ и улучшения их технических характеристик, оснащения ЛВС активным сетевым оборудованием, серверами баз данных, техническими и программно-аппаратными средствами защиты информации.

Развитие КТС ПАК ЕЦОР должно осуществляться эволюционно с поэтапной заменой морально устаревающего оборудования при условии поддержания совместимости и преемственности сохранения работоспособности программного обеспечения. При этом в части замены системных блоков АРМ, серверов и мониторов должна сохраняться ориентация на платформы, выпускаемые к моменту поставки заводами-изготовителями, при соблюдении гарантийных обязательств не менее 3-х лет с момента поставки.

Поставщик оборудования должен представить сертификаты или другие документы, подтверждающие совместимость компьютеров применяемым операционным системами другому общему программному обеспечению.

Каждая поставляемая позиция оборудования и программного обеспечения должна иметь Руководство пользователя на русском языке. Техническая документация по каждой поставляемой позиции может быть на русском или английском языках. Поставщик оборудования должен представить сертификаты соответствия Российской Федерации на всю поставляемую электронно-вычислительную технику.

4.3.6 Требования к организационному обеспечению

Создание Системы осуществляется с учетом использования существующих нормативной правовой базы, проектных и конструкторских решений, информационных ресурсов, программно-технической и телекоммуникационной инфраструктуры, а также вновь создаваемых перспективных систем органов исполнительной власти, участвующих в создании ПАК ЕЦОР.

Первоочередными мероприятиями организации работ по созданию Системы должны быть:

- проведение работ по исследованию путей построения Системы и согласование состава ее опытного образца;
- проектированию комплекта средств опытного образца Системы, в рамках которых должны быть выработаны предложения по практической реализации положений проекта Концепции, в том числе разработка проектов частных технических заданий на отдельные самостоятельные элементы;
- разработка прикладного программного обеспечения решения функциональных задач в рамках опытного образца Системы;
- разработка типовых соглашений и регламентов по обеспечению информационно-технического сопряжения ПАК ЕЦОР с взаимодействующими автоматизированными и информационными системами и их реализация в рамках опытного образца;
- проведение изыскательских, проектных и строительно-монтажных работ по оборудованию помещений, предназначенных для размещения ПТК опытного образца Системы, инженерными системами, а также по оборудованию их по требованиям защиты информации;
- создание опытного образца Системы и проведение ее опытной эксплуатации.

В процессе опытной эксплуатации опытного образца Системы могут быть определены (скорректированы):

- состав источников информации и пользователей;
- состав и структура показателей;
- состав и формы входных и выходных документов;
- требования технического задания на Систему;
- типовые решения, подлежащие тиражированию при развёртывании Системы в полном объёме.

4.3.7 Требования к методическому обеспечению

Методическое обеспечение Системы должно включать совокупность документов, описывающих технологию функционирования Системы, методы выбора и применения пользователями технологических приемов для получения конкретных результатов при функционировании Системы.

5 Состав и содержание работ по созданию системы

Перечень работ по созданию ПАК ЕЦОР должны соответствовать основным нормативным документам, в том числе ГОСТ 34.601-90 «Информационная технология. Автоматизированные системы. Стадии создания» и включать стадии «Техническое и рабочее проектирование» (РД), «Ввод ПАК ЕЦОР в постоянную эксплуатацию».

В общем случае состав и содержание работ по созданию внедрению ПАК ЕЦОР представлен в таблице (Таблица 1).

Таблица 1 - Состав и содержание работ

№ п/п	Стадии	Содержание работ	Результат
1.	Обследование	– Определение информационно-телекоммуникационной инфраструктуры объектов автоматизации. – Обследование и анализ деятельности дежурно-диспетчерских служб экстренных оперативных служб, единых дежурно-диспетчерских и центров обработки вызовов. – Изучение действующей нормативно-правовой базы. – Разработка документа «Отчет об обследовании». – Разработка ТЗ на создание опытного образца ПАК ЕЦОР.	– Согласованный документ «Отчет об обследовании»; – ТЗ на создание опытного образца ПАК ЕЦОР.
2.	Техническое и рабочее проектирование	– Разработка проектных решений по системе и её частям. – Разработка и оформление комплекта документов Технорабочего проекта	– Утвержденный комплект документов Технического проекта в составе: • Схема организации связи; • Пояснительная записка к Схеме организации связи; • Ведомость технического проекта; • Пояснительная записка к техническому проекту; • Описание автоматизируемых функций; • Схема функциональной структуры; • Схема организационной структуры; • Описание организационной структуры; • Схема автоматизации; • Описание программного обеспечения; • Схема структурная комплекса технических средств; • Описания комплекса технических средств; • Ведомость оборудования и материалов; • Описание средств

№ п/п	Стадии	Содержание работ	Результат
			информационной безопасности; • Модель угроз ПАК ЕЦОР; • Расчет затрат на техническое обслуживание ЕЦОР; • Модели рабочих процессов (Описание алгоритма); • Описание информационного обеспечения; • Описание массива информации
3.	Создание опытного образца ПАК ЕЦОР первой очереди	– Разработка специального программного обеспечения ПАК ЕЦОР первой очереди. – Разработка и оформление эксплуатационной документации. – Разработка спецификации на оборудование и ОПО ПАК ЕЦОР первой очереди.	– Специальное ПО ПАК ЕЦОРпервой очереди, развернутое на стенде разработчика; – Комплект эксплуатационной документации в составе: • Руководство пользователя, • Руководство администратора. – Спецификация оборудования и материалов.
4.	Ввод в действие опытного образца ПАК ЕЦОР первой очереди	– Подготовка объектов автоматизации к вводу в действие ПАК ЕЦОР первой очереди. – Проведение обучение и инструктажа персонала ПАК ЕЦОР. – Комплектация ПАК ЕЦОР первой очереди необходимым оборудованием и ОПО. – ПНР. – Опытная эксплуатация ПАК ЕЦОР первой очереди. – Доработка документации и специального программного обеспечения ПАК ЕЦОР первой очереди по результатам опытной эксплуатации. – Приемо-сдаточные испытанияПАК ЕЦОР первой очереди.	– Акт выполненных работ (о подготовке объекта автоматизации к вводу в действие ПАК ЕЦОР первой очереди); – Комплект организационно-распорядительных и методических материалов для сотрудников объектов автоматизации. – Программа обучения. – Заполненный журнал инструктажа сотрудников, принимающих участие в опытной эксплуатации. – Программа опытной эксплуатации. – Заполненные журналы опытной эксплуатации с объектов автоматизации. – Акт выполненных работ (об устранении замечаний). – Акт приемо-сдачи работ первой очереди.
5.	Создание опытного образца ПАК ЕЦОР полного состава	– Разработка специального программного обеспечения ПАК ЕЦОР полного состава. – Доработка эксплуатационной документации. – Разработка спецификации на оборудование и ОПО ПАК ЕЦОР полного состава.	– Специальное ПО ПАК ЕЦОР полного состава, развернутое на стенде разработчика; – Доработанный комплект эксплуатационной документации в составе: • Руководство пользователя, • Руководство администратора. – Спецификация оборудования и материалов.
6.	Ввод в действие опытного образца ПАК ЕЦОР полного состава	– Подготовка объектов автоматизации к вводу в действие ПАК ЕЦОР полного состава. – Проведение обучение и инструктажа персонала ПАК ЕЦОР полного состава. – Комплектация ПАК ЕЦОР полного состава необходимым оборудованием и ОПО. – ПНР. – Опытная эксплуатация ПАК ЕЦОР	– Акт выполненных работ (о подготовке объекта автоматизации к вводу в действие ПАК ЕЦОР полного состава); – Комплект организационно-распорядительных и методических материалов для сотрудников объектов автоматизации. – Программа обучения. – Заполненный журнал инструктажа сотрудников, принимающих

№ п/п	Стадии	Содержание работ	Результат
		полного состава. – Доработка документации и специального программного обеспечения ПАК ЕЦОР полного состава по результатам опытной эксплуатации. – Приемо-сдаточные испытания ПАК ЕЦОР полного состава. – Передача ПАК ЕЦОР в промышленную эксплуатацию.	участие в опытной эксплуатации. – Программа опытной эксплуатации. – Заполненные журналы опытной эксплуатации с объектов автоматизации. – Акт выполненных работ (об устранении замечаний). – Акт приемо-сдачи работ полного состава.

Изменения в составе проектной и рабочей документации, форма отчетных материалов, состав предложений по структуре и содержанию нормативных правовых и организационно-распорядительных документов ПАК ЕЦОР согласовываются с Заказчиком.

6 Порядок контроля и приемки системы

6.1 Виды, состав, объем и методы испытаний системы и ее составных частей

Виды, состав, объем и методы испытаний Системы, и ее составных частей определяются в ГОСТ 34.603-92.

Согласно п. 1.3 ГОСТ 34.603-92 для ПАК ЕЦОР устанавливают следующие основные виды испытаний:

- предварительные;
- опытная эксплуатация;
- приемочные.

Допускается дополнительно проведение других видов испытаний ПАК ЕЦОР и ее компонентов.

Предварительные испытания Системы проводятся для определения ее работоспособности и решения вопроса о возможности приемки Системы в опытную эксплуатацию.

Предварительные испытания Системы проводятся в соответствии с программой и методикой испытаний, путем выполнения тестовых сценариев. Программа и методика разрабатываются Исполнителем на стадии «Рабочая документация» и согласовывается с Заказчиком. Содержание отдельных проверок должно определяться в соответствующей графе программы и методики испытаний для каждой проверяемой функции.

Режим испытаний должен определяться местом и сроками проведения испытаний, режимом работы и правилами эксплуатации технических средств, используемых при проведении испытаний, согласно Программе и методике испытаний.

В программе предварительных испытаний ПАК ЕЦОР или частей ПАК ЕЦОР указывают:

- перечень объектов испытания;
- состав предъявляемой документации;
- описание проверяемых взаимосвязей между объектами испытаний;
- очередность испытаний частей Системы;
- порядок и методы испытаний, в том числе состав программных средств и оборудования, необходимых для проведения испытаний, включая специальные стенды.

Результаты испытаний отражают в протоколе. Работу завершают оформлением акта приемки в опытную эксплуатацию.

Постоянную эксплуатацию ПАК ЕЦОР проводят в рамках опытного образца Системы с целью определения фактических значений количественных и качественных характеристик Системы и готовности персонала к работе в условиях функционирования Системы, определения

ее фактической эффективности, корректировке (при необходимости) документации и специального программного обеспечения.

Приемочные испытания Системы проводят для определения ее соответствия техническому заданию, оценки полноты и качества выполнения функций Системы и решения вопроса о возможности приемки Системы в постоянную (промышленную) эксплуатацию.

Приемочные испытания проводят в соответствии с программой и методикой, в которой указывают:

- перечень объектов, выделенных в системе для испытаний и перечень требований, которым должны соответствовать объекты;
- критерии приемки системы и ее частей;
- условия и сроки проведения испытаний;
- средства для проведения испытаний;
- фамилии должностных лиц объектов автоматизации, ответственных за проведение испытаний;
- методику испытаний и обработки их результатов;
- перечень оформляемой документации.

Для проведения приемочных испытаний должна быть предъявлена следующая документация:

- техническое задание на создание Системы;
- программа и методика испытаний.

Проверку комплектности и качества эксплуатационной документации следует проводить путем анализа документации на соответствие требованиям нормативно-технических документов и ТЗ.

Результаты испытаний объектов, предусмотренных программой, фиксируют в протоколах, содержащих следующие разделы:

- назначение испытаний и номер раздела требований ТЗ на АС, по которому проводят испытание;
- состав технических и программных средств, используемых при испытаниях;
- указание методик, в соответствии с которыми проводились испытания, обработка и оценка результатов;
- условия проведения испытаний и характеристики исходных данных;
- состав и порядок использования контрольной (тестовой) информации при проведении испытаний;
- обобщенные результаты испытаний;

- выводы о результатах испытаний и соответствии созданной системы или ее частей определенному разделу требований ТЗ на АС.

Протоколы испытаний объектов по всей программе обобщают в едином протоколе, на основании которого делают заключение о соответствии системы требованиям ТЗ на АС и возможности оформления акта приемки АС в постоянную эксплуатацию.

Работу завершают оформлением акта о приемке АС в постоянную эксплуатацию.

Испытания ПАК ЕЦОР следует проводить на объекте Заказчика. По согласованию между Заказчиком и Исполнителем предварительные испытания и приемку программных средств Системы допускается проводить на технических средствах разработчика при создании условий получения достоверных результатов испытаний.

Допускается последовательное проведение испытаний и сдача частей (сегментов, подсистем) ПАК ЕЦОР в постоянную эксплуатацию.

6.2 Общие требования к приемке работ по стадиям

Сдача-приёмка работ должна производиться поэтапно в соответствии с календарным планом к государственному контракту.

По факту выполнения работ Исполнитель представляет Заказчику результаты работ в соответствии с данным техническим заданием вместе с Актом сдачи-приемки выполненных работ и Перечнем отчетной документации.

Заказчик в семидневный срок со дня получения акта сдачи-приемки выполненных работ принимает одно из следующих решений:

- в случае если представленные результаты работ в полной мере соответствуют обязательствам, принятым Исполнителем по Договору, Заказчик принимает результат работ, подписывает и утверждает акт сдачи-приемки выполненных работ;
- в случае если представленные результаты работ содержат отклонения от условий Договора, Заказчик составляет перечень замечаний и необходимых доработок.

Замечания к результатам работ подлежат доработке Исполнителем в сроки, установленные Заказчиком или, если такие не установлены, в течении7 (семи) дней с момента подписания Заказчиком перечня разногласий. Доработка результатов работ осуществляется Исполнителем за свой счет без последующей компенсации этих расходов Заказчиком.

Акт сдачи-приемки выполненных работ подписывается в двух экземплярах, один из которых передается Исполнителю, а второй находится у Заказчика.

Не подписание Заказчиком в срок акта сдачи-приемки выполненных работ при отсутствии замечаний к результатам работ является фактом признания полного выполнения Исполнителем своих обязанностей по настоящему Договору надлежащим образом и в срок.

7 Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие

Для создания условий функционирования объектов автоматизации Системы, при которых гарантируется соответствие разработанной Системы требованиям, содержащимся в настоящем техническом задании и возможности эффективного использования Системы на объектах автоматизации, Заказчиком должны быть проведены следующие мероприятия:

- приведение поступающей в систему информации к виду, пригодному для обработки с помощью ЭВМ;
- изменения, которые необходимо осуществить в объекте автоматизации;
- создание условий функционирования объекта автоматизации, при которых гарантируется соответствие создаваемой Системы требованиям, содержащимся в данном ТЗ;
- создание необходимых для функционирования Системы подразделений и служб;
- определение подразделения и должностных лиц, ответственных за проведение опытной эксплуатации и постоянной эксплуатации.

7.1 Приведение поступающей в Систему информации к виду, пригодному для обработки с помощью ЭВМ

Для приведения поступающей в Систему информации к виду, пригодному для обработки с помощью ЭВМ должны быть проведены системно-аналитические мероприятия по формализации, категоризации, описания атрибутивного состава документов и форм документов аналитического и статистического учета.

Должны быть разработаны и утверждены отчетные и экранные формы компонентов системы.

В рамках функционирования ПАК ЕЦОР необходимо приводить информацию к виду, пригодному для обработки при помощи ЭВМ, следующим путем:

- путем передачи информации из смежных систем с использованием установленных протоколов и средств интеграции;
- путем ручного ввода данных с использованием электронных форм ввода данных.

Для обеспечения первого способа используется средства, разработанные Исполнителем. Для обеспечения второго способа используется персонал объектов автоматизации Заказчика.

7.2 Изменения, которые необходимо осуществить в объекте автоматизации

Изменения в организационной структуре должны осуществляться согласно требованиям ГОСТ 24.209-80.

Подготовка помещений на объектах автоматизации для размещения ПАК ЕЦОР должна осуществляться согласно требованиям СНиП 3.05.07-85.

Нормы и правила, определенные СНиП 3.05.07-85, распространяются на производство и приемку работ по монтажу и наладке систем автоматизации технологических процессов и инженерного оборудования на строительстве новых, расширении, реконструкции и техническом перевооружении действующих предприятий, зданий и сооружений.

Монтажу систем автоматизации должна предшествовать подготовка в соответствии со СНиП 3.01.01-85 и СНиП 3.05.07-85. Помещения для развертывания систем автоматизации оборудуются по требованиям обеспечения безопасности информации и режимных мероприятий с учетом требований нормативных документов.

Приемку технологической готовности к монтажу систем автоматизации следует осуществлять поэтапно по отдельным законченным частям объекта.

Организацию дополнительных компьютерных рабочих мест необходимо осуществлять с учетом требований СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

8 Требования к документированию

На различных стадиях создания ЕЦОР должна быть разработана документация в соответствии с:

- ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»
- ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем»
- РД 50-34.698-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы требования к содержанию документов»
- ГОСТ 24.301-80 «Система технической документации на АСУ. Общие требования к выполнению текстовых документов»
- ГОСТ 2.105-95 «Единая система конструкторской документации. Общие требования к текстовым документам»
- ГОСТ 2.104-2006 «Единая система конструкторской документации. Основные надписи»

В исключительных случаях, допускаются отступления от требований ГОСТ по согласованию с Заказчиком.

8.1 Требования к перечню подлежащих разработке комплектов и видов документов

Документация на ПАК ЕЦОР должна разрабатываться в соответствии с требованиями ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем», РД 50-34.698-90 «Методические указания. Автоматизированные системы. Требования к содержанию документов» и ЕСПД.

Перечень подлежащих разработке комплектов и видов документов на стадиях технического проекта и рабочей документации следующий:

Перечень подлежащих разработке комплектов и видов документов:

1) Согласованный документ «Отчет об обследовании»;
2) Утвержденный комплект документов Технорабочего проекта в составе:
   - Схема организации связи;
   - Пояснительная записка к Схеме организации связи;
   - Ведомость технического проекта;

- Пояснительная записка к техническому проекту;
- Описание автоматизируемых функций;
- Схема функциональной структуры;
- Схема организационной структуры;
- Описание организационной структуры;
- Схема автоматизации;
- Описание программного обеспечения;
- Схема структурная комплекса технических средств;
- Описания комплекса технических средств;
- Ведомость оборудования и материалов;
- Описание средств информационной безопасности;
- Модель угроз ПАК ЕЦОР;
- Экономическое обоснование (сметная документация) затрат на построение и внедрение ПАК ЕЦОР;
- Расчет затрат на техническое обслуживание ПАК ЕЦОР;
- Модели рабочих процессов (Описание алгоритма);
- Описание информационного обеспечения;
- Описание массива информации;
- Программа и методика испытаний.

3) Комплект эксплуатационной документации в составе:
   - Руководство пользователя;
   - Руководство администратора.
4) Спецификация оборудования и материалов.
5) Комплект организационно-распорядительных и методических материалов (состав комплекта разрабатывается и согласовывается с Заказчиком на стадии создания опытного образца ПАК ЕЦОР).
6) Программа обучения.
7) Программа опытной эксплуатации.
8) Образец журнала опытной эксплуатации.
9) Образцы актов:
   - Акта выполненных работ (о подготовке объекта автоматизации к вводу в действие ПАК ЕЦОР первой очереди);
   - Акта выполненных работ (об устранении замечаний);
   - Акта приемо-сдачи работ;

– Акта ввода ПАК ЕЦОР в промышленную эксплуатацию.

Перечень комплектов и видов документов может быть уточнен по результатам технического проектирования и разработки рабочей документации по согласованию с Заказчиком.

8.2 Требования к форме представления документации

Вся разработанная документация должна быть выполнена на русском языке, представлена Заказчику на бумажном и электронном (компакт-диск) носителях.

Документы технического проекта и рабочей документации комплектуют в папки, книги или альбомы по признаку принадлежности к одному структурному элементу Системы.

Разрабатываемая документация подлежит нормоконтролю на предприятии-изготовителе.

8.3 Требования к микрофильмированию документации

Требования к микрофильмированию документации не предъявляются.

8.4 Требования к документированию комплектующих элементов

Программное обеспечение и технические средства сторонних производителей должны быть снабжены сопроводительной документацией, входящей в поставляемый производителем комплект соответствующих комплектующих элементов.

9 Источники разработки

При создании Системы должны быть использованы следующие нормативные, правовые, методические документы и документы по стандартизации:

Доктрины, Стратегии и Федеральные целевые программы:

- Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации от 9 сентября 2000 г. № Пр-1895;
- Стратегия развития информационного общества в Российской Федерации, утвержденная Президентом Российской Федерации 7 февраля 2008 г. № Пр-212);
- постановление Правительства Российской Федерации от 20 августа 2001 г. №587 «О федеральной целевой программе «Глобальная навигационная система»;
- Комплексная программа обеспечения безопасности населения на транспорте, утвержденная распоряжением Правительства Российской Федерации от 30 июля 2010 г. № 1285-р.

Федеральные законы и нормативные акты:

- Гражданский кодекс Российской Федерации;
- Федеральный закон Российской Федерации от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании»;
- Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
- Федеральный законРоссийской Федерацииот 27 июля 2006 г.№152-ФЗ «О персональных данных»;
- Федеральный законРоссийской Федерацииот 27 июля 2006 г.№149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Государственные стандарты, регламенты и руководящие документы:

- ГОСТ 2.114-95. «Единая Система Конструкторской Документации. Технические условия»;
- ГОСТ 19.102-77. «Единая Система Программной Документации. Стадии разработки»;
- ГОСТ 24.202-80. «Требования к содержанию документа «Технико-экономическое обоснование создания АСУ»;
- ГОСТ 34.003-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;

- ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ 34.401-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Средства технические периферийные автоматизированных систем дорожного движения. Типы и технические требования»;
- ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания»;
- ГОСТ 34-602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- РД 50-680-88. «Методические указания. Автоматизированные системы. Основные положения»;
- РД 50-682-89. «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения»;
- РД 50-34.698-90. «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»;
- ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;
- ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»;
- ГОСТ Р 51241-98. «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»;
- РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», решение председателя Гостехкомиссии России от 30 марта 1992г.;
- РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», решение председателя Гостехкомиссии России от 25.07.1997 г.;
- РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля

отсутствия недекларированных возможностей», Приказ Председателя Гостехкомиссии России №114 от 4 июня 1999 г.;

- приказ ФСТЭК России, ФСБ России, Мининформсвязи России №55/86/20 от 13 февраля 2008 г. «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- приказ ФСТЭК России от 5 февраля 2010 г. №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»;

СОСТАВИЛИ

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата
Североморское муниципальное казенное учреждение «Единая дежурно-диспетчерская служба»	Старший оперативный дежурный	Поляков А.А.		
Североморское муниципальное казенное учреждение «Единая дежурно-диспетчерская служба»	Инженер 1 категории	Веселов Д.М.		

СОГЛАСОВАНО

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата