ТЕХНИЧЕСКОЕ ЗАДАНИЕ[1]

«Создание системы обеспечения вызова экстренных оперативных служб по единому номеру «112» на базе единых дежурно-диспетчерских служб муниципальных образований субъекта Российской Федерации»

Листов 124

2012

[1] в настоящем образце не приводятся лист утверждения, лист регистрации изменений и иные элементы оформления согласно стандартам

Подпись и дата | Инв. № дубл. | Взам. инв. № | Подпись и дата | Инв. № подл.

СОДЕРЖАНИЕ

Определения, обозначения и сокращения

Термины и сокращения	Определение
112	единый номер вызова экстренных оперативных служб на территории Российской Федерации
АРМ	автоматизированное рабочее место
ГИС	геоинформационная система
ГО и ЧС	гражданская оборона и чрезвычайные ситуации
ГУ	главное управление
ДДС	дежурно-диспетчерская служба, в настоящем ТЗ означает весь перечень экстренных оперативных служб, оперативных служб и организаций, интегрируемых в систему-112
Диспетчер	сотрудник ДДС или ЕДДС, осуществляющий прием вызовов или управление подразделениями в рамках компетенции своей службы
ЕДДС	единая дежурно-диспетчерская служба
ЕСКД	единая система конструкторской документации
ЗИП	запасные части, инструменты и принадлежности
ИБП	источник бесперебойного питания
КТС	комплекс технических средств
КСА	комплекс средств автоматизации
ЛВС	локальная вычислительная сеть
МВД России	Министерство внутренних дел Российской Федерации
Минздрав России	Министерство здравоохранения Российской Федерации
Минюст России	Министерство юстиции Российской Федерации
МЧС России	Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий
НСД	несанкционированный доступ
Оператор	сотрудник ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС, осуществляющий прием и обработку вызовов по номеру 112
ОС	операционная система
ПАК	программно-аппаратный комплекс
ПО	программное обеспечение
ПОИБ	подсистема обеспечения информационной безопасности
Пользователь	пользователь прикладного, специального программного обеспечения

Термины и сокращения	Определение
системы-112	системы-112, оператор, диспетчер, администратор, либо любой другой из тех, у кого есть учетная запись в данной системе-112
ПТК	программно-технический комплекс
региональный ЦУКС МЧС России	центр управления в кризисных ситуациях главного управления Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий по субъекту Российской Федерации
РИВП	распределенная информационно-вычислительная платформа
РСЧС	Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций
РЦОВ	резервный центр обработки вызовов, входящий в состав системы-112
СВТ	средство вычислительной техники
СГЭ	система гарантированного электроснабжения
СЗИ	средства защиты информации
система-112	система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Субъекта РФ
СНиП	строительные нормы и правила
СПО	специальное программное обеспечение
СРК	система резервного копирования
СУБД	система управления базами данных
СХД	система хранения данных
Субъект РФ	субъект Российской Федерации, в настоящем документе применяется для обозначения субъекта Российской Федерации, на территории которого создается система-112
ТЗ	техническое задание
ТПО	территориальная пожарная охрана
ТУ	технические условия
УОВЭОС	узел обслуживания вызовов экстренных оперативных служб
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦО	центр обучения
ЦОВ-АЦ	центр обработки вызовов системы-112, развертываемый в административном центре субъекта Российской Федерации
ЦОВ-ЕДДС	центр обработки вызовов системы-112 на базе единой дежурно-диспетчерской службы муниципального образования субъекта

Термины и сокращения	Определение
	Российской Федерации
ЦУКС	центр управления в кризисных ситуациях
ЧС	чрезвычайная ситуация
ЭКС	электронная карточка события
ЭОС	экстренная оперативная служба
ЭРА-ГЛОНАСС	система экстренного реагирования при авариях, основанная на применении российских средств глобальной спутниковой навигации, ГЛОНАСС, и систем спутникового мониторинга транспорта
GPRS	General Packet Radio Service — «пакетная радиосвязь общего пользования», надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. GPRS позволяет пользователю сети сотовой связи производить обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе Интернет
GPS/ ГЛОНАСС	Американская и российская глобальные навигационные системы
N+1	схема резервирования оборудования, подразумевающая установку дополнительного (резервного) устройства, аналогично основному устройству
VPN	Virtual Private Network — виртуальная частная сеть, технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с использованием средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых сообщений)
КСЗИ	комплекс средств защиты информации
ДГУ	дизельная генераторная установка

1 Общие сведения

1.1 Полное наименование автоматизированной системы и её условное обозначение

Полное наименование автоматизированной системы - система обеспечения вызова экстренных оперативных служб по единому номеру «112» на базе единых дежурно-диспетчерских служб муниципальных образований Субъекта РФ[2].

Краткое наименование автоматизированной системы - система-112.

1.2 Реквизиты контракта на создание системы-112

Шифр[3].

1.3 Наименование предприятий разработчика и заказчика системы-112

Заказчик[4].

Разработчик[5].

1.4 Перечень документов, на основании которых проектируется система-112

Перечень документов, на основании которых проектируется система-112, перечислен в приложении 1.

1.5 Предмет государственного контракта

Предметом государственного контракта является проведение технического проектирования системы-112.

1.6 Источники и порядок финансирования работ

Финансирование работ производится из бюджета Субъекта РФ.

1.7 Мероприятие, в рамках которого реализуется лот

Мероприятие[6].

1.8 Срок выполнения работы

Начало выполнения работ - со дня подписания государственного контракта.

---

[2] Субъект РФ – здесь и далее применяется для обозначения субъекта Российской Федерации, на территории которого создается система-112.
[3] указать шифр темы, реквизиты государственного контракта на выполнение работ.
[4] указать полное наименование и адрес Заказчика работы.
[5] указать полное наименование и адрес исполнителя работы.
[6] указать номер и наименование мероприятия (при наличии)

Окончание выполнения работ - определяется на конкурсной основе.

1.9 Наименования организации Исполнителя

Определяется на конкурсной основе.

1.10 Порядок оформления и предъявления заказчику результатов работ по проектированию системы

Порядок приемки работ, выполняемых в рамках данного технического задания, определен в пункте 6 настоящего ТЗ.

Исполнитель передает Заказчику документацию в соответствии с пунктом 5.1 настоящего ТЗ.

2 Назначение и цели создания системы

2.1 Назначение системы

Система-112 предназначена для информационного обеспечения единых дежурно-диспетчерских служб муниципальных образований. Она обеспечивает информационное взаимодействие органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, в том числе единых дежурно-диспетчерских служб муниципальных образований, а также дежурно-диспетчерских служб экстренных оперативных служб.

Система-112 предназначена для выполнения следующих основных функций:

прием и обработка вызовов (сообщений о происшествиях) поступающих на единый телефонный номер «112» от населения и от сигнальных систем мониторинга опасных объектов;

передача в дежурно-диспетчерские службы экстренных оперативных служб сообщений о вызовах с возможностью подключения их диспетчеров к разговорам с позвонившим лицом;

координация действий ДДС при реагировании на вызовы (сообщения о происшествиях);

организация оптимального использования сил и средств ДДС при реагировании на вызовы (сообщения о происшествиях);

поддержка единого информационного пространства для всего персонала и пользователей системы.

Система-112 предназначена для решения следующих основных задач:

прием по номеру "112" вызовов (сообщений о происшествиях);

получение от оператора связи сведений о местонахождении лица, обратившегося по номеру "112", и (или) абонентского устройства, с которого был осуществлен вызов (сообщение о происшествии), а также иных данных, необходимых для обеспечения реагирования по вызову (сообщению о происшествии);

анализ поступающей информации о происшествиях;

направление информации о происшествиях, в том числе вызовов (сообщений о происшествиях), в дежурно-диспетчерские службы экстренных оперативных служб в соответствии с их компетенцией для организации экстренного реагирования;

обеспечение дистанционной психологической поддержки лицу, обратившемуся по номеру "112";

автоматическое восстановление соединения с пользовательским (оконечным) оборудованием лица, обратившегося по номеру "112", в случае внезапного прерывания соединения;

регистрация всех входящих и исходящих вызовов (сообщений о происшествиях) по номеру "112";

ведение базы данных об основных характеристиках происшествий, о начале, завершении и об основных результатах экстренного реагирования на полученные вызовы (сообщения о происшествиях);

возможность приема вызовов (сообщений о происшествиях) на иностранных языках.

Объекты автоматизации перечислены в пункте 3 настоящего ТЗ.

2.2 Цели создания системы-112

Основными целями создания системы-112 являются:

организация вызова экстренных оперативных служб по принципу "одного окна";

организация комплекса мер, обеспечивающих ускорение реагирования и улучшение взаимодействия экстренных оперативных служб при вызовах (сообщениях о происшествиях);

реализация требований гармонизации способа вызова экстренных оперативных служб в Российской Федерации с законодательством Европейского союза.

Основной целью выполнения работ в рамках указанного в п.1.2 государственного контракта является проведение технического проектирования системы-112.

3 Характеристика объектов автоматизации

3.1 Общие сведения об объектах автоматизации

В соответствии с Положением о единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций, утвержденном постановлением Правительства Российской Федерации от 30 декабря 2004г. № 794, в территориальных органах МЧС России были организованы центры управления в кризисных ситуациях, предназначенные для координации действия по предупреждению и ликвидации чрезвычайных ситуаций. Органы повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций региона включают в себя муниципальные и межмуниципальные единые дежурно-диспетчерские службы и дежурно-диспетчерские службы ЭОС. ЕДДС являются органами повседневного управления местной (городской) подсистемы единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций. ЕДДС предназначены для координации действий ЭОС одного или нескольких муниципальных образований Субъекта РФ. На базе ЕДДС создаются центры обработки вызовов системы-112, обеспечивающие прием и обработку вызовов (сообщений о происшествиях) от населения и организаций в зоне ответственности.

Интеграции в систему-112 подлежат[7]:

служба пожарной охраны;

служба реагирования в чрезвычайных ситуациях;

служба полиции;

служба скорой медицинской помощи;

аварийная служба газовой сети;

служба «Антитеррор».

ДДС и ЕДДС Субъекта РФ входят в соответствующие организационно-штатные структуры территориальных органов федеральных органов исполнительной власти, органов исполнительной власти Субъекта РФ и органов местного самоуправления муниципальных районов, специально уполномоченных на решение задач гражданской обороны, предупреждения и ликвидации чрезвычайных ситуаций, безопасности государства, обеспечения правопорядка, безопасности жизни и здоровья граждан.

[7] Органы исполнительной власти Субъекта РФ, исходя из местных условий, вправе определять иные службы и организации, которым наряду с указанными ЭОС необходимо обеспечить интеграцию с системой-112. Соответствующий перечень формируется Исполнителем и утверждается Заказчиком на этапе формирования требований к системе-112 и разработки концепции

Для обеспечения координации взаимодействия при реагировании на вызовы (сообщения о происшествиях) вышеперечисленные объекты системы-112 должны быть обеспечены единой транспортной инфраструктурой (каналами связи) и ПТК (АРМ).

В состав системы-112 в качестве функциональных объектов должны входить ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС, а также в целях настоящего Технического задания ДДС (АРМ на объектах ДДС). РИВП предоставляет необходимые инфокоммуникационные услуги для функциональных объектов системы-112.

Решение задач системы-112 обеспечивают развернутые на функциональных объектах подсистемы (телекоммуникационная, информационно-коммуникационная, консультативного обслуживания населения, геоинформационная, мониторинга, обеспечения информационной безопасности).

Регламенты взаимодействия объектов формируются на этапе разработки рабочей документации системы-112 и утверждаются Заказчиком на стадии ввода в действие системы-112.

3.1.1 Центр обработки вызовов административного центра

ЦОВ-АЦ должен создаваться на территории административного центра Субъекта РФ, предназначен для обеспечения приема и обработки вызовов от населения административного центра Субъекта РФ и передачи на реагирование в соответствующие ДДС, взаимодействия с региональным ЦУКС МЧС России, ЦОВ-ЕДДС, ДДС, навигационно-информационным центром системы экстренного реагирования при авариях ЭРА-ГЛОНАСС, а в случае необходимости приема и обработки вызовов со всей территории Субъекта РФ.

На ЦОВ-АЦ возложены следующие основные задачи:

прием, регистрация, документирование вызовов, переадресация вызовов, поступивших по номеру «112»;

обработка массовых вызовов по поводу уже зарегистрированного происшествия;

прием, регистрация, документирование вызовов в формате SMS и электронной почты;

получение данных об абоненте и его местонахождении;

автоматический дозвон до позвонившего в случае внезапного прерывания соединения (например, если звонящий не дождался ответа оператора, находясь в очереди ожидания);

обеспечение консультативной поддержки населению при обращении по вопросам обеспечения безопасности жизнедеятельности;

при необходимости подключение к разговору с абонентом психолога или переводчика.

Должно быть предусмотрено строительство или реконструкция объектов капитального строительства, предусмотренных для размещения ЦОВ-АЦ.

ЦОВ-АЦ функционирует в круглосуточном режиме.

Оборудование ЦОВ-АЦ включает, как минимум:

автоматизированные рабочие места операторов дежурной смены;

автоматизированные рабочие места административного и обслуживающего персонала;

активное оборудование локальной вычислительной сети;

структурированную кабельную сеть;

комплект оргтехники;

средства связи;

средства оповещения;

источники гарантированного электропитания.

Должны быть приняты необходимые организационные и технические решения для обеспечения резервирования ЦОВ-АЦ в минимальном функционале автоматизированного приема и обработки вызовов с помощью размещения части операторов в РЦОВ.

Количественный состав дежурной смены должен обеспечивать возможность выполнения ЦОВ-АЦ всех своих функций, но не менее двух операторов и одного специалиста обеспечения. Должно быть обеспечено динамическое распределение вызовов между операторами дежурных смен ЦОВ-АЦ и РЦОВ.

3.1.2 Резервный центр обработки вызовов

РЦОВ должен создаваться на территории административного центра Субъекта РФ с учетом необходимости географического резервирования ЦОВ-АЦ, как правило, на базе учебно-методического центра по гражданской обороне и чрезвычайным ситуациям, с целью резервирования ЦОВ-АЦ и обучения персонала системы-112. РЦОВ должен обеспечивать выполнение всех функций ЦОВ-АЦ в полном объеме в случае выхода ЦОВ-АЦ из строя (в том числе приема и обработки вызовов от населения административного центра Субъекта РФ и передачи на реагирование в соответствующие ДДС или ЕДДС, взаимодействия с региональным ЦУКС МЧС России, ЦОВ-ЕДДС, навигационно-информационным центром системы экстренного реагирования при авариях ЭРА-ГЛОНАСС, а в случае необходимости приема и обработки вызовов со всей территории Субъекта РФ).

Должно быть предусмотрено строительство или реконструкция объектов капитального строительства, предусмотренных для размещения РЦОВ.

РЦОВ функционирует в круглосуточном режиме.

РЦОВ должен обеспечить непрерывность решения первоочередных задач системы-112 при выходе ЦОВ-АЦ из строя и вплоть до восстановления работоспособности ЦОВ-АЦ в полном объеме обеспечить полную функциональность системы-112.

Оборудование РЦОВ включает, как минимум:

автоматизированные рабочие места операторов дежурной смены;

автоматизированные рабочие места административного и обслуживающего персонала;

активное оборудование локальной вычислительной сети;

структурированную кабельную сеть;

комплект оргтехники;

средства связи;

средства оповещения;

источники гарантированного электропитания.

Минимальный состав дежурной смены – 2 оператора и специалист обеспечения.

3.1.3 Единая дежурно-диспетчерская служба

ЕДДС является подразделением муниципального образования Субъекта РФ, предназначена для приема и передачи сигналов оповещения ГО от вышестоящих органов управления, сигналов на изменение режимов функционирования муниципальных звеньев территориальной подсистемы РСЧС, приема сообщений о ЧС (происшествиях) от населения и организаций, оперативного доведения данной информации до соответствующих ЭОС и организаций (объектов), координации совместных действий ЭОС и организаций, оперативного управления силами и средствами соответствующего звена территориальной подсистемы РСЧС, оповещения руководящего состава муниципального звена и населения об угрозе возникновения или возникновении ЧС (происшествий).

Общее руководство ЕДДС муниципального образования осуществляет руководитель органа местного самоуправления, непосредственное - руководитель ЕДДС муниципального образования.

Основные задачи ЕДДС:

прием от населения и организаций сообщений о любых чрезвычайных происшествиях, несущих информацию об угрозе или факте возникновения ЧС;

анализ и оценка достоверности поступившей информации, доведение ее до ДДС, в компетенцию которых входит реагирование на принятое сообщение;

сбор от ДДС, служб контроля и наблюдения за окружающей средой и распространение между ДДС города полученной информации об угрозе или факте возникновения ЧС, сложившейся обстановке и действиях сил и средств по ликвидации ЧС;

обработка и анализ данных о ЧС, определение ее масштаба и уточнение состава ДДС, привлекаемых для реагирования на ЧС, их оповещение о переводе в высшие режимы функционирования;

обобщение, оценка и контроль данных обстановки, принятых мер по ликвидации чрезвычайной ситуации, подготовка и коррекция заранее разработанных и согласованных с городскими службами вариантов управленческих решений по ликвидации ЧС, принятие необходимых решений (в пределах установленных вышестоящими органами полномочий);

информирование ДДС, привлекаемых к ликвидации ЧС, подчиненных сил постоянной готовности об обстановке, принятых и рекомендуемых мерах;

представление докладов (донесений) об угрозе или возникновении ЧС, сложившейся обстановке, возможных вариантах решений и действиях по ликвидации ЧС (на основе ранее подготовленных и согласованных планов) вышестоящим органам управления по подчиненности;

доведение задач, поставленных вышестоящими органами РСЧС, до ДДС и подчиненных сил постоянной готовности, контроль их выполнения и организация взаимодействия;

обобщение информации о произошедших ЧС (за сутки дежурства), ходе работ по их ликвидации и представление соответствующих докладов по подчиненности.

3.1.4 Центр обработки вызовов единой дежурно-диспетчерской службы

ЦОВ-ЕДДС создаются на базе существующих ЕДДС муниципальных районов Субъекта РФ, предназначены для приема и обработки вызовов от населения, проживающего в зоне обслуживания ЕДДС, а также для взаимодействия с ЦОВ-АЦ, РЦОВ, ДДС (в рамках системы-112) и ЦОВ-ЕДДС соседних муниципальных образований Субъекта РФ.

Должна быть предусмотрена реконструкция объектов капитального строительства, предусмотренных для размещения ЦОВ-ЕДДС.

ЦОВ-ЕДДС функционирует в круглосуточном режиме.

Оборудование ЦОВ-ЕДДС включает, как минимум:

автоматизированные рабочие места операторов дежурной смены;

автоматизированные рабочие места административного и обслуживающего персонала;

активное оборудование локальной вычислительной сети;

структурированную кабельную сеть;

комплект оргтехники;

средства связи;

средства оповещения;

источники гарантированного электропитания.

Должны быть приняты необходимые организационные и технические решения для обеспечения резервированной работоспособности ЦОВ-ЕДДС в минимальном функционале автоматизированного приема и обработки вызовов и взаимодействия с ДДС в случае потери доступа к РИВП, а также возможность резервирования функционала ЦОВ-ЕДДС в полном объеме за счет ЦОВ-АЦ и РЦОВ.

Минимальный состав дежурной смены – 2 оператора.

3.1.5 Служба пожарной охраны

ДДС пожарной охраны является подразделением территориальной службы пожарной охраны, располагается, как правило, в одной из частей гарнизона пожарной охраны, в оперативном отношении подчиняется оперативному дежурному и начальнику гарнизона.

На ДДС пожарной охраны возложены следующие основные задачи:

принимать сообщения о вызовах подразделений пожарной охраны по телефонным линиям связи с номером "01";

направлять к месту вызова силы и средства подразделений пожарной охраны в соответствии с расписанием выезда (планом привлечения сил и средств),

обеспечивать в установленном порядке передислокацию дежурных смен, пожарных и аварийно-спасательных расчетов подразделений;

обобщать сведения о наличии сил и средств в подразделениях;

проверять наличие связи с подразделениями и службами жизнеобеспечения;

информировать должностных лиц об изменениях оперативной обстановки, выезде подразделений;

знать оперативную обстановку в районе (подрайоне) выезда подразделения, перечень объектов, на которые составлены планы и карточки тушения пожаров и при пожаре высылаются силы и средства подразделения по повышенному номеру (рангу) пожара, места расположения важных, взрывопожароопасных объектов, противопожарное водоснабжение, безводные участки, проезды, тактико-технические характеристики пожарной и аварийно-спасательной техники, пожарного инструмента и аварийно-спасательного оборудования, имеющегося на вооружении подразделения;

обеспечивать подразделения информацией об оперативно-тактических особенностях объекта, уровне загазованности, радиационной обстановке на месте вызова;

при необходимости в установленном порядке организовывать (обеспечивать) оповещение и сбор личного состава органов управления и подразделений к месту вызова.

3.1.6 Служба полиции

ДДС полиции является территориальным подразделением МВД России, располагается, как правило, в помещении районного органа внутренних дел, подчиняется начальнику органа внутренних дел, непосредственно подчинена начальнику дежурной части органа внутренних дел.

На ДДС полиции возлагаются следующие основные задачи:

принимать и регистрировать (в том числе в электронной форме) заявления и сообщения о преступлениях, об административных правонарушениях, о происшествиях;

передавать (направлять) заявления и сообщения о преступлениях, об административных правонарушениях, о происшествиях в государственные и муниципальные органы, организации

или должностному лицу, к компетенции которых относится решение соответствующих вопросов, с уведомлением об этом в течение 24 часов заявителя;

информировать соответствующие государственные и муниципальные органы, организации и должностных лиц этих органов и организаций о ставших известными полиции фактах, требующих их оперативного реагирования;

организовывать незамедлительное прибытие должностных лиц на место совершения преступления, административного правонарушения, место происшествия для пресечения противоправных деяний, устранения угроз безопасности граждан и общественной безопасности, документирования обстоятельства совершения преступления, административного правонарушения, обстоятельства происшествия, обеспечения сохранности следов преступления, административного правонарушения, происшествия;

организовывать оказание первой помощи лицам, пострадавшим от преступлений, административных правонарушений и несчастных случаев, а также лицам, находящимся в беспомощном состоянии либо в состоянии, опасном для их жизни и здоровья, если специализированная помощь не может быть получена ими своевременно или отсутствует;

принимать при чрезвычайных ситуациях неотложные меры по спасению граждан, охране имущества, оставшегося без присмотра, содействовать в этих условиях бесперебойной работе спасательных служб; обеспечивать общественный порядок при проведении карантинных мероприятий во время эпидемий и эпизоотий;

участвовать в мероприятиях по противодействию терроризму и в обеспечении правового режима контртеррористической операции, а также в обеспечении защиты потенциальных объектов террористических посягательств и мест массового пребывания граждан, в проведении экспертной оценки состояния антитеррористической защищенности и безопасности объектов.

3.1.7 Служба скорой медицинской помощи

ДДС скорой медицинской помощи является подразделением территориального уровня Министерства здравоохранения Российской Федерации, располагается, как правило, на территории обслуживаемого муниципального образования, непосредственно подчиняется начальнику станции скорой помощи, подчинена руководителю ЕДДС муниципального образования.

На ДДС скорой медицинской помощи возлагаются следующие основные задачи:

в режиме повседневной работы - организация и оказание скорой медицинской помощи заболевшим и пострадавшим на месте происшествия и во время их транспортировки в стационары.

в режиме чрезвычайной ситуации - по указанию окружного Территориального центра медицины катастроф направляет в зону чрезвычайной ситуации выездные бригады скорой

медицинской помощи согласно плану работы по ликвидации медико-санитарных последствий чрезвычайный ситуаций.

3.1.8 Аварийная служба газовой сети

Аварийная служба (ДДС) газовой сети является территориальным подразделением эксплуатационного управления Субъекта РФ, располагается, как правило, на территории обслуживаемого муниципального образования, подчиняется начальнику управления, непосредственно подчинена начальнику дежурной службы.

На ДДС газовой сети возложены следующие основные задачи:

прием заявок от граждан о возникновении аварийной ситуации на газовом оборудовании, газопроводах;

оперативное реагирование на заявки для локализации и ликвидации аварий, повреждений, неисправностей газового оборудования и газопроводов.

3.1.9 Служба «Антитеррор»

Дежурно-диспетчерская служба «Антитеррор» является подразделением антитеррористической комиссии Субъекта РФ.

На службу возложены следующие основные задачи:

прием заявок от граждан о фактах подготовки или проведения террористических актов;

оперативное реагирование на заявки, координация действий ЭОС.

3.1.10 Региональный Центр управления в кризисных ситуациях МЧС России

Региональный ЦУКС МЧС России является органом повседневного управления РСЧС и предназначен для обеспечения реализации функций территориальных органов МЧС России по управлению и координации деятельности сил и средств РСЧС на территории Субъекта РФ.

Основные задачи регионального ЦУКС МЧС России:

сбор, обработка и представление органам управления РСЧС оперативной информации о ЧС, организация мониторинга и прогнозирования ЧС, а также учет сил и средств, ресурсов, задействованных для ликвидации ЧС;

оперативное управление действиями подразделений при выполнении мероприятий по экстренному предупреждению и ликвидации ЧС;

координация деятельности органов повседневного управления РСЧС при угрозе возникновения ЧС;

обеспечение управления силами и средствами, предназначенными для предупреждения и ликвидации чрезвычайных ситуаций на территории Субъекта РФ;

сбор, обработка, обмен и выдача информации в области защиты населения и территорий от чрезвычайных ситуаций;

осуществление своевременного оповещения и информирования населения о чрезвычайных ситуациях в местах массового пребывания людей, а также об опасностях, возникающих при ведении военных действий или вследствие этих действий на территории Субъекта РФ;

обеспечение управления силами и средствами, предназначенными и выделяемыми для борьбы с пожарами, возникшими при ведении военных действий или вследствие этих действий на территории Субъекта РФ;

осуществление функций пункта управления Главного управления МЧС России по Субъекту РФ;

организация повседневного управления деятельностью единых дежурно-диспетчерских служб муниципальных районов и городских округов области и взаимодействия с дежурно-диспетчерскими службами органов исполнительной власти Субъекта РФ, территориальных органов федеральных органов исполнительной власти, учреждений и организаций области;

реализация государственной политики в области защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности и безопасности людей на водных объектах на территории Субъекта РФ в пределах установленных полномочий;

осуществление контроля наличия и готовности сил и средств оперативного реагирования Главного управления, его подчиненных органов управления;

сбор, обработка и представление вышестоящим, взаимодействующим и нижестоящим органам управления РСЧС оперативной информации о чрезвычайных ситуациях, прогнозной информации о тенденциях их развития и последствиях, задействованных силах, средствах и ресурсах;

оперативное управление, в пределах предоставленных полномочий, действиями подчинённых подразделений при выполнении мероприятий по предупреждению и ликвидации ЧС;

обеспечение оповещения и информирование населения о прогнозируемых и возникших ЧС мирного и военного времени, пожарах, мерах по обеспечению безопасности населения и территорий, приемах и способах защиты;

координация деятельности взаимодействующих ведомственных дежурно-диспетчерских служб при угрозе или возникновении ЧС;

информационное обеспечение работы координационных и постоянно действующих органов управления РСЧС области;

осуществление мероприятий по информированию населения о возникших и прогнозируемых чрезвычайных ситуациях и пожарах и по пропаганде безопасности жизнедеятельности.

Региональный ЦУКС МЧС России интегрируется в систему-112 либо путем установки в нем АРМ системы-112 либо выполнением интеграции соответствующего СПО регионального ЦУКС МЧС России и системы-112.

3.1.11 Узел обеспечения вызова экстренных оперативных служб

УОВЭОС - узел местной телефонной сети, обеспечивающий автоматическое установление соединения вызова от оконечных телефонных станций и узлов к экстренным оперативным службам.

УОВЭОС должен обеспечивать:

оперативность подключения;

постоянную доступность для вызова ЭОС;

расширение спектра информационно-справочных, заказных и интеллектуальных услуг, предоставляемых населению Субъекта РФ.

3.1.12 Распределенная информационно-вычислительная платформа

РИВП обеспечивает необходимый для функционирования ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС и ДДС в автоматизированном режиме комплекс инфокоммуникационных услуг в части доступа к серверам, системам хранения данных, общему и прикладному программному обеспечению, принадлежащих оператору РИВП. Предоставление указанных инфокоммуникационных услуг, обеспечивающих функциональность системы-112, включает:

предоставление услуг связи для обеспечения приема вызовов (сообщений о происшествиях) по единому номеру «112»;

предоставление необходимого для функционирования системы-112 общего и специального программного обеспечения, развернутого на оборудовании РИВП;

предоставление необходимого для функционирования указанного программного обеспечения и хранения информации оборудования РИВП;

предоставление услуг связи для обеспечения доступа пользователей ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС, ДДС к услуге.

Технологические решения РИВП и коммуникаций, обеспечивающих доступ от объектов системы-112 к РИВП, обеспечивают выполнение требований Технического задания на проектирование системы-112.

Технологические площадки РИВП территориально резервированы и располагаются на территории Российской Федерации[8].

В состав оборудования РИВП входит центр обработки данных в составе серверного оборудования и системы хранения данных, объединенных выделенной высокоскоростной вычислительной сетью. Выбор состава и параметров серверов производен на основании результатов анализа требуемой производительности оборудования для приложений или сервисов, планируемых для работы на этих серверах. Серверная платформа имеет подтвержденный производителем план существования и развития не менее чем на 5 лет с момента начала предоставления инфокоммуникационных услуг, а также совместима с другими элементами системы-112. В части серверного ядра применяются решения на базе отказоустойчивого серверного кластера и резервированного хранилища данных, объединенных в резервированную высокоскоростную вычислительную сеть с организацией гарантированного электропитания.

Технологические площадки РИВП аттестованы на соответствие требованиям безопасности информации как автоматизированная система класса 1Г и специальная информационная система персональных данных класса К1, криптографические средства защиты информации РИВП обеспечивают криптографическую защиту по уровню не ниже уровня КС2.

3.2 Адресные сведения об объектах автоматизации

Адресные сведения[9] об объектах автоматизации приведены в приложениях:

приложение № 1 – характеристика территории Субъекта РФ и объектов;

приложение № 2 – сведения об условиях эксплуатации функциональных объектов системы-112.

3.3 Общие сведения об автоматизируемых процессах

Прием и обработка вызовов (сообщений о происшествиях) в системе-112 включает:

диалог с заявителем, анализ и передачу характеристик происшествия (при необходимости перенаправление вызовов (сообщений о происшествиях)) в дежурно-диспетчерские службы соответствующих экстренных оперативных служб для непосредственного реагирования;

контроль за реагированием на происшествие, анализ и ввод в базу данных информации, полученной по результатам реагирования, уточнение и корректировку действий привлеченных дежурно-диспетчерских служб экстренных оперативных служб, информирование

8 указать местонахождение

9 фактически определяются на этапе проведения обследования и утверждаются Заказчиком

взаимодействующих дежурно-диспетчерских служб экстренных оперативных служб об оперативной обстановке, о принятых и реализуемых мерах;

размещение в информационной системе данных о ходе и об окончании мероприятий по экстренному реагированию на принятый вызов (сообщение о происшествии).

Возможность вызова экстренных оперативных служб по единому номеру «112» предоставляется пользователям телефонной связи операторами фиксированных и подвижных (мобильных) сетей телефонной связи на сети связи общего пользования. При этом операторы связи должны обеспечить прохождение вызова на номер «112» до УОВЭОС, а так же предоставить службе, принимающей эти вызовы, сведения об абонентском устройстве, с которого осуществляется вызов (номер и местоположение) и об абоненте (при необходимости), на которого зарегистрировано это устройство.

Приём вызовов (сообщений о происшествиях) осуществляется операторами ЦОВ-АЦ, РЦОВ и ЦОВ-ЕДДС по признаку территориальной принадлежности к их зоне ответственности. Все обращения в систему-112 регистрируются и, при необходимости, направляются дежурным диспетчерам соответствующих ДДС.

Взаимодействие операторов ЦОВ-АЦ, РЦОВ и ЦОВ-ЕДДС с диспетчерами ДДС в целом производится согласно регламенту информационного обмена и включает значительный объем как голосовой, так и текстовой информации (согласно унифицированной карточки информационного обмена в системе-112).

Диспетчеры ДДС при получении сообщений о происшествии выполняют меры по реагированию в соответствии с внутренними инструкциями и вводят в информационную систему (систему-112) уточненные данные по происшествию и информацию по реагированию на него.

Все действия операторов, диспетчеров и другого персонала регистрируются.

Возможность вызова экстренных оперативных служб по единому номеру «112» предоставляется круглосуточно, без выходных.

В случае ложного вызова дежурной службы заявитель несёт ответственность в соответствии с действующим законодательством.

В общем виде процесс обработки вызова экстренных оперативных служб по единому номеру «112» включает в себя следующие технологические операции:

приём и регистрация вызова (сообщения о происшествии) о происшествии и принятие решения о задействии ДДС оператором;

передача оператором унифицированной карточки информационного обмена в системе-112 в задействуемые ДДС, по необходимости подключение диспетчеров к разговору или переадресация вызова;

при необходимости уточнение оператором или диспетчером у заявителя информации по происшествию и принятие диспетчером решений по реагированию на происшествие;

направление сил и средств ДДС диспетчером на место происшествия для уточнения полученной информации, оказания помощи и ликвидации происшествия;

оказание помощи и ликвидация происшествия дежурными силами ДДС, завершение реагирования, закрытие унифицированной карточки информационного обмена в системе-112 диспетчером, после проведения контроля - оператором.

При первичном опросе заявителя оператором выясняются следующие сведения (по возможности):

характер происшествия (что случилось);

место происшествия (где случилось - адрес);

дата и время происшествия (когда случилось – дата, время);

наличие пострадавших людей (есть ли пострадавшие);

количество пострадавших (сколько пострадавших);

характер травм или проявление заболевания;

фамилия, имя, отчество позвонившего лица (кто сообщает о происшествии);

с какого абонентского устройства осуществляется вызов (номер телефона);

другие сведения, необходимые для оказания оперативной помощи.

Оператор, принимающий вызов, регистрирует сведения о вызове и о происшествии. Для получения необходимых сведений оператор задает уточняющие вопросы.

Получаемые от заявителя сведения оператор сверяет с данными об абонентском устройстве, с которого осуществляется вызов, и об абоненте, полученными от оператора связи, а так же с адресными данными геоинформационной системы.

В ходе приёма заявления оператор принимает решение о привлечении ДДС для оказания помощи заявителю, об оказании психологической помощи, помощи переводчика. В случае соответствия происшествия определенным критериям может приниматься решение о передаче информации по команде для присвоении данному происшествию статуса ЧС. Указанные решения оператор принимает самостоятельно на основании инструкций или рекомендаций соответствующего диспетчера. Подключение ДДС производится непосредственно в ходе приема заявления или сразу после его окончания путем автоматизированной передачи необходимой информации о происшествии в ДДС (на АРМ диспетчера), организации конференцсвязи, перевода вызова на ДДС.

После принятия диспетчером решения о направлении к заявителю (на место происшествия) сил и средств соответствующей ДДС для экстренной оперативной помощи диспетчер или оператор сообщают об этом заявителю, выдают ему рекомендации о необходимых действиях до

прибытия помощи и завершают телефонный вызов для обеспечения готовности к принятию следующего вызова.

На всех последующих этапах обслуживания вызова происходит отслеживание изменения обстановки и статуса реагирования на происшествие. Закрытие унифицированной карточки информационного обмена в системе-112 происходит после завершения реагирования всех привлеченных по данному происшествию ДДС.

4 Требования к системе

4.1 Требования к системе в целом

4.1.1 Требования к структуре и функционированию

4.1.1.1 Перечень подсистем, их назначение и основные характеристики

В состав подсистем системы-112 должны входить:

Телекоммуникационная подсистема, обеспечивает прохождение вызовов (сообщений о происшествиях), включая телефонные вызовы и короткие текстовые сообщения (SMS), от пользователей (абонентов) сетей фиксированной или подвижной радиотелефонной связи в систему-112, а также прохождение вызова (сообщения о происшествии) от системы-112 в ДДС Субъекта РФ.

Информационно-коммуникационная подсистема, обеспечивает хранение и актуализацию баз данных, обработку информации о полученных вызовах (сообщениях о происшествиях) и возможность получения информации о происшествии из архива в оперативном режиме, а также информационно-аналитическую поддержку принятия решений по экстренному реагированию на принятые вызовы (сообщения о происшествиях) и планированию мер реагирования. В состав указанной подсистемы входит центр обработки вызовов, в котором производится прием и обработка вызовов (сообщений о происшествиях), поступающих в систему-112.

Подсистема консультативного обслуживания, предназначена для оказания информационно-справочной помощи лицам, обратившимся по номеру «112», по вопросам обеспечения безопасности жизнедеятельности.

Геоинформационная подсистема, отображает на основе электронных карт природно-географические, социально-демографические, экономические и другие характеристики территории, местонахождение лица, обратившегося по номеру «112», и (или) абонентского устройства, с которого осуществлен вызов (сообщение о происшествии), место происшествия, а также местонахождение транспортных средств ДДС, привлеченных к реагированию на происшествие.

Подсистема мониторинга, предназначена для приема и обработки информации и сигналов, поступающих от датчиков, установленных на контролируемых стационарных и подвижных объектах, в том числе от автомобильных терминалов системы экстренного реагирования при авариях ЭРА-ГЛОНАСС и терминалов ГЛОНАСС/GPS, установленных на транспортных средствах ДДС, привлеченных к реагированию на происшествие, и транспортных средствах, перевозящих опасные грузы.

Подсистема обеспечения информационной безопасности, предназначена для защиты информации и средств ее обработки в системе-112.

4.1.1.2 Требования к структуре системы-112

Система-112 создается на базе ЕДДС муниципальных образований Субъекта РФ с децентрализованным (распределенным по районам) приемом и обработкой вызовов (сообщений о происшествиях) центрами обработки вызовов системы-112, централизованным предоставлением комплекса инфокоммуникационных услуг, обеспечивающих необходимую функциональность системы-112 (в том числе хранение информации) на базе географически резервированных технологических площадок РИВП, принадлежащих стороннему оператору. Характеристики предоставления указанной инфокоммуникационной услуги должны быть определены на стадии технического проектирования в соответствующем Регламенте.

Вызовы (сообщения о происшествиях) на номер «112» в муниципальном образовании адресуются в ЦОВ-ЕДДС, где их принимает и обрабатывает оператор системы-112. Далее оператор передает характеристики происшествия (при необходимости перенаправляет вызов) в соответствующие ДДС, персонал которых обеспечивает реагирование. Ложные вызовы должны отсеиваться на уровне ЦОВ-ЕДДС.

В административном центре Субъекта РФ вызовы (сообщения о происшествиях) на номер «112» адресуются в ЦОВ-АЦ либо РЦОВ, где их обрабатывает оператор по схожей схеме.

В случае отказа (перегрузки) ЦОВ-ЕДДС, вызов должен быть переадресован в ЦОВ-АЦ либо РЦОВ, где он должен обрабатывается с учетом того, из какого муниципального образования он поступил (т.е. для реагирования задействуются ДДС именно этого муниципального образования).

В случае отказа ЦОВ-АЦ выполнение его функций обеспечивает РЦОВ.

Автоматизированными рабочими местами системы-112 должны быть оснащены ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС, ДДС и региональный ЦУКС МЧС России.

Система-112 должна быть развернута на двух уровнях иерархии:

административного центра Субъекта РФ (ЦОВ-АЦ и РЦОВ, ДДС);

муниципальных образований (ЦОВ-ЕДДС, ДДС).

В ходе проведения разработки Технического проекта необходимо уточнить особенности реализации системы-112 исходя из характеристик объектов автоматизации, в том числе:

особенностей административно-территориального деления Субъекта РФ:

количества населения;

распределения населения на территории.

особенностей информационно-телекоммуникационной инфраструктуры административного центра Субъекта РФ:

наличия, доступности и технических характеристик имеющихся каналов связи;

готовности ЕДДС, ДДС.

Должны быть учтены (детализированы) требования по обеспечению отказоустойчивости системы-112, обеспечена минимизация расходов на создание и эксплуатацию системы-112.

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

Территориально распределенная структура системы-112 подразумевает наличие информационного обмена компонентов системы-112, находящихся в разных сегментах локальной сети.

Информационный обмен между компонентами системы-112 должен быть организован посредством:

унифицированных карточек информационного обмена;

общей базы данных;

специализированного интерфейса программирования приложений;

специализированных информационных сервисов.

Взаимодействие компонентов системы-112 с помощью специфицированных информационных сервисов должно обеспечиваться средствами протокола SOAP, при этом каждый информационный сервис должен иметь доступную для других компонентов системы WSDL-спецификацию интерфейса, и обеспечивать синтаксическую интероперабельность средствами XML формата данных, который должен соответствовать доступной для компонента XSD-схеме данных.

Решения по другим возможным вариантам информационного взаимодействия между компонентами системы-112 должны приниматься на стадии технического проектирования и быть подробно описаны в рабочей документации на систему.

Решения по регламентам и интерфейсам взаимодействия должны быть приняты на стадии технического проектирования.

4.1.1.4 Требования к характеристикам взаимосвязей создаваемой системы со смежными и внешними системами

Смежными по отношению к системе-112 являются:

система ЭРА-ГЛОНАСС;

система «Безопасный город»;

автоматизированные информационные системы ДДС.

Внешними по отношению к системе-112 являются:

АС регионального ЦУКС МЧС России;

системы обеспечения вызова экстренных оперативных служб по единому номеру «112» сопредельных субъектов Российской Федерации.

Совместимость системы-112 со смежными и внешними системами должна достигаться за счет использования:

единых общероссийских, региональных и ведомственных классификаторов;

единых коммуникационных форматов, способов кодирования и форм представления документов и данных;

стандартизированных и общепринятых технологических решений при обмене по каналам связи.

Система-112 должна обеспечивать взаимодействие с системами мониторинга ЭРА-ГЛОНАСС и ГЛОНАСС/GPS, развернутыми в Субъекте РФ. Информационное взаимодействие между подсистемой мониторинга и системой ЭРА-ГЛОНАСС должно осуществляться автоматически следующими способами:

через специализированный информационный сервис;

через API интерфейсы.

Решения по интерфейсам и регламентам взаимодействия должны быть приняты на стадии технического проектирования.

Информационное взаимодействие системы-112 с системой «Безопасный город» должно осуществляться автоматически следующими способами:

через специализированный информационный сервис;

путем регламентированного информационного обмена файлами определенного формата.

Система-112 должна обеспечивать оперативное взаимодействие с информационными системами всех ДДС. Исключение могут составлять неподдерживаемые разработчиками информационные системы, либо имеющие объективные неустранимые препятствия для интеграции в систему-112.

Информационное взаимодействие между системой-112 и автоматизированными системами регионального ЦУКС МЧС России и ДДС, системой «Безопасный город» должно осуществляться автоматически следующими способами:

путем прямого доступа АРМ к источнику данных автоматизированной информационной системы;

через специализированный информационный сервис, разработанный для интеграции с данной информационной системой;

через API автоматизированной информационной системы;

путем регламентированного информационного обмена файлами определенного формата.

Конкретные решения по способу и составу информационного обмена для обеспечения взаимодействия системы-112 с автоматизированными информационными системами регионального ЦУКС МЧС России и ДДС, системой «Безопасный город» должны быть приняты на стадии рабочего проектирования системы-112, исходя из данных, собранных при проведении обследования объектов автоматизации.

Для взаимодействия с указанными автоматизированными информационными системами на стадии технического проектирования системы-112 должны быть выданы соответствующие рекомендации.

Взаимодействие системы-112 со смежными и внешними системами должно обеспечить решение в том числе следующих задач:

получение дополнительных данных о чрезвычайных происшествиях, содержащих информацию об угрозе, территории и объекте возникновения ЧС;

анализ и оценка достоверности поступившей информации;

доведение информации о вызове (сообщении о происшествии) до ДДС в автоматизированном режиме;

получение информации в автоматизированном режиме о действиях сил и средств ДДС (организаций) по ликвидации ЧС;

обработка и анализ данных о ЧС, определение ее масштаба и уточнение состава ДДС, привлекаемых для реагирования на ЧС, их оповещение о переводе в высшие режимы функционирования;

доведение задач, поставленных вышестоящими органами РСЧС до ДДС, контроль их выполнения и организация взаимодействия;

обобщение информации о происшествиях и ЧС (за период), ходе работ по их ликвидации, а также предоставление докладов в соответствии с табелем оповещения должностных лиц.

Информационное взаимодействие между системой-112 и системами обеспечения вызова экстренных оперативных служб по единому номеру «112» сопредельных субъектов Российской Федерации должно обеспечивать обмен оперативной информацией и должно при наличии технической возможности осуществляться автоматически следующими способами:

через специализированный информационный сервис;

путем регламентированного информационного обмена файлами определенного формата.

В случае отсутствия технической возможности автоматического взаимодействия должен быть предусмотрен обмен данными с использованием имеющихся средств автоматизации под управлением оператора.

Регламенты взаимодействия с каждой системой обеспечения вызова экстренных оперативных служб по единому номеру «112» сопредельных субъектов Российской Федерации должны быть разработаны и согласованы с Заказчиком на стадии технического проектирования.

Решения по интерфейсам взаимодействия должны быть приняты на стадии рабочего проектирования системы-112.

4.1.1.5 Требования к режимам функционирования системы

Система-112 должна функционировать в режиме 24/7/365 (24 часа в сутки, 7 дней в неделю, круглый год).

Система-112 должна функционировать в следующих режимах:

штатный режим - основной режим функционирования. В данном режиме система-112 должна выполнять свои функции в соответствии с техническими и организационными инструкциями;

нештатный режим - режим, который позволяет использовать доступные ресурсы системы-112 для сохранения информации, правильного закрытия информационных массивов, работающих приложений и операционных систем. Нештатный режим должен использоваться для выполнения минимально необходимых операций в условиях аварийного энергоснабжения компонентов системы-112 или выхода из строя части оборудования.

Переход системы-112 в нештатный режим может происходить по следующим причинам:

отказ отдельных компонентов системы-112;

нарушение функционирования поддерживающей инфраструктуры - общесистемных сервисов, сетей электропитания, каналов связи и т. п.

Действия в нештатном режиме должны включать:

диагностирование инцидентов или проблем, связанных со сбоями или нештатными ситуациями в работе системы-112;

восстановление при необходимости программно-аппаратной конфигурации системы-112 (сетевого и серверного оборудования);

восстановление информации при ее утере средствами системы резервного копирования и восстановления;

расследование причин нештатной ситуации и определение причин инцидента или проблемы.

Реагирование на нештатные ситуации должно включать оповещение персонала, принятие контрмер, необходимое восстановление информации, выработку и проведение профилактических мероприятий.

Время функционирования системы-112 в нештатном режиме должно быть минимальным.

Характеристики системы-112 в штатном режиме должны соответствовать требованиям настоящего Технического задания и нормативно-правовой документации в области системы-112.

4.1.1.6 Требования по диагностированию системы

Диагностирование работоспособности системы-112 должно осуществляться специализированными программными средствами в штатном и нештатном режимах работы системы.

Диагностирование системы-112 должно обеспечивать:

мониторинг параметров работы технических и программных средств системы-112, выявление критических (угрожающих работоспособности) и аварийных компонент;

определение доступности и загруженности каналов связи между РИВП и функциональными объектами системы-112.

Объектами диагностирования должны являться:

средства вычислительной техники;

телекоммуникационное оборудование и каналы связи;

базы данных;

общесистемное программное обеспечение;

специальное программное обеспечение.

Диагностирование программно-аппаратного комплекса системы-112 должно обеспечиваться:

стандартными средствами системы управления базами данных;

встроенными средствами администрирования;

средствами мониторинга и управления сетевыми, вычислительными и информационными ресурсами объекта автоматизации.

При диагностировании должна предусматриваться возможность проведения следующих работ:

диагностирования физической и логической целостности программного обеспечения;

комплексная проверка работоспособности аппаратных и программных средств системы-112.

Средства диагностирования должны предоставлять удобный интерфейс для возможности просмотра диагностических событий, мониторинга процесса выполнения программ.

При возникновении аварийных ситуаций, либо ошибок в программном обеспечении, диагностические средства должны позволять сохранять полный набор информации, необходимой разработчику для идентификации проблемы (снимки экранов, текущее состояние памяти, файловой системы).

Диагностирование каналов связи должно осуществляться автоматически в штатном режиме функционирования системы-112.

В системе-112 должны вестись информационные файлы (log-файлы), регистрирующие работу пользователей и подсистем. Данные файлы должны предоставлять информацию о состоянии системы-112.

Система-112 должна обладать средствами контроля исключений. Данные средства должны отслеживать и уведомлять пользователя о возникших проблемах с подробным описанием сути ситуации и препятствовать потере введенных в систему данных.

Диагностирование вычислительной, сетевой и инженерной инфраструктуры системы-112 должно осуществляться обслуживающим персоналом.

4.1.1.7 Перспективы развития и модернизации системы

Под модернизацией системы-112 подразумевается модернизация технического обеспечения, операционного окружения, применение новых современных интерфейсов информационного взаимодействия, методов и протоколов передачи данных.

Система-112 должна разрабатываться с учетом перспектив ее развития, модернизации и масштабирования. Должны обеспечиваться следующие направления развития и модернизации системы-112:

расширение функциональных возможностей компонентов и подсистем в связи с изменениями полномочий должностных лиц, для автоматизации деятельности которых она предназначена;

улучшение характеристик технических и программных средств системы-112 (таких, как производительность вычислительных серверов и рабочих станций, сетевого оборудования, пропускной способности каналов связи, использование средств виртуализации);

расширение состава и актуализация справочников и классификаторов системы-112;

разработка механизмов интеграции методологического обеспечения системы-112 с системой международных и отечественных стандартов в сфере организации вызова экстренных оперативных служб по единому номеру;

развитие средств аналитической обработки информации о происшествиях и чрезвычайных ситуациях, методологии и программных средств оценки рисков в области предупреждения и ликвидации последствий ЧС и интеллектуальной поддержки принятия решений;

использование технологий ГЛОНАСС при анализе происшествий, предупреждении и контроле хода ликвидации последствий ЧС;

взаимодействие с автоматизированными системами ключевых объектов промышленной, транспортной инфраструктуры и инфраструктуры рекреации.

Должна предусматриваться возможность быстрой адаптации системы-112 при изменении положений нормативно-правовых актов, определяющих предмет автоматизации.

4.1.2 Требования к численности и квалификации персонала и режиму его работы

4.1.2.1 Общие требования

В соответствии с функциональными обязанностями персонал системы-112 подразделяется на следующие основные категории:

оперативный персонал;

эксплуатационный (обслуживающий) персонал;

административный персонал.

Также в настоящем документе определяется персонал РИВП и регионального ЦУКС МЧС России, других организаций, объектов и систем, обеспечивающий управление, функционирование и взаимодействие с системой-112.

К оперативному персоналу относятся лица, непосредственно участвующие в приёме и обработке вызовов: старшие операторы и операторы ЦОВ-АЦ, РЦОВ и ЦОВ-ЕДДС и диспетчеры ДДС.

К эксплуатационному (обслуживающему) персоналу относятся лица, обеспечивающие функционирование технических и программных средств системы-112, а так же выполнение функций защиты информации в соответствии с инструкциями по эксплуатации и обслуживанию, и выполняющие работы по техническому обслуживанию ПТК.

Обслуживающий персонал системы-112 должен состоять как минимум из следующих категорий работников, прошедших соответствующее обучение:

администраторы технологического управления системой;

администраторы по информационной безопасности;

инженер по средствам вычислительной техники;

инженер по средствам связи.

Количество и распределение обязанностей административного персонала должны обеспечить выполнение функций организации и руководства функционированием системы-112.

Оперативный персонал должен иметь навыки и уметь выполнять должностные обязанности в полном объеме. Остальной персонал системы-112, размещающийся в ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС, должен уметь выполнять обязанности оператора системы-112 в минимально допустимом объеме.

На стадии технического проектирования должны быть разработаны штатные расписания ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС.

Минимальный состав дежурных смен[10]:

ЦОВ-АЦ и РЦОВ и ЦОВ-ЕДДС – 2 оператора и специалист обеспечения;

ЦОВ-ЕДДС[11] – 2 оператора;

дежурно-диспетчерских служб пожарной охраны, реагирования в чрезвычайных ситуациях, полиции, скорой медицинской помощи; аварийной газовой сети, «Антитеррор» – 2 диспетчера;

остальных ДДС – в соответствии с их штатным расписанием.

Обеспечение требований по обслуживанию вызовов на иностранных языках с подключением к разговору переводчика обеспечить путем привлечения услуг внештатных переводчиков, предусмотреть техническую возможность и обеспечить голосовую связь с удаленными переводчиками в режиме конференции с оператором и вызывающим абонентом-иностранцем.

Обеспечение требований по оказанию психологической помощи обеспечить наличием соответствующего специалиста среди операторов ЦОВ-АЦ либо РЦОВ.

В штате РЦОВ должно иметься не менее 2 преподавателей.

4.1.2.2 Требования к квалификации персонала, порядку его подготовки и контроля знаний и навыков

В процессе проведения технического проектирования должны быть определены требования к квалификации, режимам работы и порядку подготовки персонала, задействованного для обеспечения функционирования системы-112.

Численность и квалификация персонала системы-112 должны определяться с учетом следующих требований:

численность оперативного персонала системы-112 выбирается с учетом средней нагрузки за временной отрезок рабочей смены и всех задач, возлагаемых на смену данного объекта, в том числе осуществления резервирования других объектов;

структура и конфигурация системы должны быть спроектированы и реализованы с целью минимизации количественного состава персонала при сохранении надежности и оперативности работы системы-112;

структура системы-112 должна предоставлять возможность управления всем доступным функционалом системы как одному администратору, так и предоставлять возможность разделения ответственности по администрированию между несколькими администраторами;

аппаратно-программный комплекс системы не должен требовать круглосуточного обслуживания и присутствия администраторов у консоли управления.

---

[10] требования к минимальному составу и режиму функционирования ДДС и организаций, интегрированных в систему-112 дополнительно к перечисленным ниже – по указанию Заказчика

[11] могут быть совмещены функциональные обязанности (должности) операторов ЦОВ-ЕДДС и диспетчеров ЕДДС

Персонал системы-112 должен:

в части общих навыков и умений:

обладать навыками использования IBM PC совместимых компьютеров на уровне уверенного пользователя;

уметь выполнять стандартные процедуры используемой операционной системы;

ориентироваться в деловых процедурах предметной области, основных входящих и исходящих документах, материалах в рамках своей компетенции;

владеть русским языком на уровне носителя языка;

в части специфики системы-112 знать:

административную структуру Субъекта РФ и структуру системы-112, должности и фамилии руководящего состава системы безопасности зоны ответственности, адреса ДДС;

зону территориальной ответственности ЕДДС образования и зоны территориальной ответственности взаимодействующих ДДС;

дислокацию, назначение и тактико-технические данные техники, привлекаемой для ликвидации и предупреждения ЧС, размещение складов специальных средств спасения и пожаротушения в зоне ответственности;

потенциально-опасные объекты, расположенные в зоне ответственности;

назначение, задачи и тактико-технические характеристики системы-112, правила работы с оборудованием, порядок эксплуатации средств связи;

наименование объектов и населенных пунктов соседних муниципальных образований;

правила техники безопасности при использовании средств автоматизации.

Оперативный персонал ЦОВ-АЦ, РЦОВ и ЦОВ-ЕДДС должен:

знать:

функциональные обязанности и порядок работы оператора;

руководящие документы, регламентирующие работу оператора;

структуру и технологию функционирования ЦОВ-ЕДДС;

нормативные документы, регламентирующие деятельность ЦОВ-ЕДДС и ЕДДС;

документы, определяющие деятельность оператора ЦОВ-ЕДДС по сигналам ГО и другим сигналам;

правила ведения документации.

уметь:

использовать КСА и СПО системы-112;

использовать оборудование системы оповещения;

организовывать информационное взаимодействие с ДДС;

эффективно работать с коммуникационным оборудованием, основными офисными приложениями для операционной системы Microsoft Windows (Word, Excel);

безошибочно набирать на клавиатуре не менее 25 слов в минуту;

использовать гарнитуру при приёме информации;

четко говорить по радио и телефону одновременно с работой за компьютером;

применять коммуникационные навыки;

эффективно получать необходимую информацию от абонента или другого источника;

быстро принимать решения в сфере деятельности;

обрабатывать входящие вызовы в соответствии с принятыми в системе-112 стандартами, правилами и процедурами;

эффективно использовать ресурсы системы-112 (технические и информационные) для предоставления своевременной, достоверной и полной информации при обработке вызовов или выполнении запросов вышестоящих организаций или экстренных служб;

самостоятельно повышать уровень теоретической и практической подготовки;

сохранять конфиденциальную информацию, полученную в процессе выполнения своих обязанностей.

Старший оператор дополнительно должен уметь организовать работу дежурной смены.

Требования к квалификации оператора ЦОВ-АЦ, РЦОВ и ЦОВ-ЕДДС: образование высшее или среднее специальное и специальная подготовка по установленной программе без предъявления требований к стажу работы.

Дополнительное требование к квалификации старшего оператора ЦОВ-АЦ, РЦОВ и ЦОВ-ЕДДС: стаж оперативной работы не менее 1 года.

Оперативный персонал ДДС должен (в части системы-112):

знать:

функциональные обязанности и порядок работы диспетчера;

руководящие документы, регламентирующие работу диспетчера;

структуру и технологию функционирования системы-112;

нормативные документы, регламентирующие деятельность системы-112;

документы, определяющие деятельность оператора ДДС по сигналам ГО и другим сигналам;

правила ведения документации.

уметь:

использовать КСА и СПО системы-112;

поддерживать информационное взаимодействие в системе-112;

эффективно работать с коммуникационным оборудованием, основными офисными приложениями для операционной системы Microsoft Windows (Word, Excel);

безошибочно набирать на клавиатуре не менее 25 слов в минуту;

использовать гарнитуру при приёме информации;

четко говорить по радио и телефону одновременно с работой за компьютером;

применять коммуникационные навыки;

эффективно получать необходимую информацию от абонента или другого источника;

быстро принимать решения;

обрабатывать входящие вызовы в соответствии с принятыми в системе-112 стандартами, правилами и процедурами;

эффективно использовать ресурсы системы-112 (технические и информационные) для предоставления своевременной, достоверной и полной информации при обработке вызовов или выполнении запросов вышестоящих организаций или экстренных служб;

самостоятельно повышать уровень теоретической и практической подготовки;

сохранять конфиденциальную информацию, полученную в процессе выполнения своих обязанностей.

Требования к квалификации диспетчера ДДС: среднее профессиональное образование без предъявления требований к стажу работы или начальное профессиональное образование и стаж работы по специальности не менее 3 лет.

Эксплуатирующий персонал системы-112 должен:

в части настройки программно-технического комплекса системы-112:

знать основы устройства персонального компьютера и основы построения локальных вычислительных сетей;

знать принципы установки, настройки и администрирования используемых операционных систем;

знать основы администрирования используемых СУБД (настройка учетных записей, настройка прав доступа, настройка профилей безопасности, резервное копирование данных);

знать основы работы с локальными базами данных и серверами;

уметь настраивать сетевое оборудование;

уметь настраивать и обслуживать оргтехнику;

уметь устанавливать и настраивать источники бесперебойного питания.

в части настройки рабочего места пользователя системы-112:

обладать умениями и навыками установки и настройки конфигурации рабочего места пользователя;

обладать навыками разрешения аппаратно-программных конфликтов в используемых операционных системах (настройки сети и сетевых протоколов, принтера и т.п.).

в части поддержки и сопровождения системы-112:

уметь управлять распределением прав пользователей системы-112;

уметь проводить настройку интерфейса пользователя;

уметь разрешать конфликты, связанные с настройкой рабочего места пользователя;

знать и уметь применять соответствующие инструментальные средства разработки информационного комплекса.

в части обеспечения информационной безопасности системы-112:

знать законодательные акты, нормативные и методические материалы по вопросам, связанным с обеспечением защиты информации;

знать методику и технологические особенности организации комплексной защиты информации, действующей в системе-112;

владеть методами и средствами контроля охраняемых сведений, выявления каналов утечки информации;

владеть методами планирования и организации проведения работ по защите информации;

уметь разворачивать и настраивать технические средства контроля и защиты информации.

Подготовка оперативного состава ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС и преподавателей системы обучения должна проводиться в виде специально организованного курса обучения в объеме не менее 160 учебных часов, ДДС – не менее 40 учебных часов.

Организационными формами курса обучения должны являться лекции, семинары, практические занятия и самостоятельная работа. Текущий контроль занятий должен осуществляться в ходе проведения семинаров и практических занятий, итоговый контроль - путем проведения экзамена с оценкой по дисциплине. Успешно окончившим курс обучения должно быть выдано удостоверение государственного образца. Обучение должно проводиться организациями, имеющими лицензию на проведение обучения по специальности, обладающими соответствующим опытом в данной области.

4.1.2.3 Требуемый режим работы персонала АС

Штатный состав персонала системы-112 должен формироваться на основании нормативных документов Российской Федерации и Трудового кодекса.

Должна быть организована круглосуточная посменная работа персонала.

Требования к организации труда и режима отдыха персонала должны устанавливаться, исходя из требований к организации труда и режима отдыха при работе со средствами вычислительной техники.

Персонал системы-112 должен выполнять свои функции в соответствии с гигиеническими требованиями к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы на них.

Допустимый уровень шума не более 65 дБ (допустимый уровень вибрации не должен превышать по амплитуде 0,1 мм и по частоте 25 Гц).

4.1.3 Требования к информационному обмену

Информационное взаимодействие системы-112 можно условно разделить на 2 типа: между объектами внутри системы-112 и между системой-112 и смежными или внешними (интегрируемыми или взаимодействующими) системами.

Для информационного обмена должны использоваться стандартные протоколы, не зависящие от среды и способа передачи данных.

В качестве основных протоколов обмена данными в системе-112 должны использоваться:

SOAP 1.2 (http://www.w3.org/TR/soap12/);

WSDL 2.0 (http://www.w3.org/TR/wsdl20/);

XML 1.1 (http://www.w3.org/TR/xml11/);

XML Schema (XSD) 1.0 (http://www.w3.org/TR/xmlschema-0/);

JSON (http://json.org/).

Полный перечень протоколов и схемы взаимодействия и обмена информацией должны быть разработаны на стадии технического проектирования системы-112.

Для взаимодействия системы-112 со смежными и внешними системами могут быть использованы АРМ системы-112 или интеграционные компоненты с АС объектов автоматизации.

Технические решения по способам взаимодействия со смежными и внешними системами должны быть описаны в документах технического проекта системы-112 Субъекта РФ.

4.1.4 Показатели назначения

4.1.4.1 Степень приспособляемости системы к изменению процессов и методов управления, к отклонениям параметров объекта управления

В системе-112 должна обеспечиваться адаптация к требованиям, изменяющимся в процессе эксплуатации (изменениям в законодательстве, автоматизируемых процессах, методах управления и т.д.).

4.1.4.2 Допустимые пределы модернизации и развития системы

В системе-112 должна обеспечиваться возможность наращивания производительности путем увеличения производительности КТС РИВП.

4.1.4.3 Вероятностно-временные характеристики, при которых сохраняется целевое назначение Системы

Система-112 должна сохранять целевое назначение при следующих значениях вероятностно-временных характеристик:

архивное хранение данных длительностью, не менее:

не менее 5 лет - для оперативных данных (за исключением голосовых данных);

не менее 3-х лет – для остальной информации, в том числе голосовых данных.

количество ДДС, с которыми гарантируется работоспособность системы-112 - не менее 300;

количество регистрируемых обращений в систему-112 - не менее 12 000 в сутки;

режим функционирования - 24х7х365;

суммарное время функционирования системы-112 в нештатном режиме - не более 4 часов в год;

время однократного перевода системы-112 в нештатный режим функционирования:

не более 10 минут для системы-112 в целом (невозможность выполнения всех функций и задач где-либо на территории Субъекта РФ);

не более 3 часов для отдельного объекта системы-112 (при условии полнофункционального резервирования указанного объекта другими);

время функционирования КТС ЦОВ-ЕДДС и ДДС (в части функциональности системы-112) при прекращении подачи электропитания - не менее 30 мин.

Система-112 должна обеспечивать следующие показатели назначения:

постоянную доступность для осуществления экстренного вызова по прямому номеру «112» со всех терминалов фиксированных и подвижных телефонных сетей вне зависимости от эксплуатирующих их операторов связи (исключение могут составлять телефонные терминалы корпоративных сетей связи, где набору «112» может предшествовать цифра (цифры) выхода в сеть связи общего пользования);

уровень автоматизации системы-112 должен обеспечивать время реагирования (от поступления вызова до доведения команды до сил реагирования) ДДС, определяемое соответствующими нормативами;

единый пользовательский интерфейс оператора (диспетчера) в виде одного приложения для доступа к функциям системы и возможность взаимодействия с приложениями электронной картографии;

распределенную структуру: географически разнесенные РИВП, АРМ операторов, диспетчеров и администраторов должны работать в единой системе, обеспечивая заданную функциональность, необходимый уровень надежности и свободный выбор местоположения

операторов и диспетчеров, включая изменение функций без перезапуска специального программного обеспечения;

возможность смены версий специального программного обеспечения, обслуживание, подключение и отключение АРМ операторов и диспетчеров без полной остановки системы;

возможность расширения состава реализуемых функций и технологий, а также масштабирования системы-112 без повторного проектирования;

изменение конфигурации системы-112 (включая число ДДС и внешний вид информации о происшествии) без доработки программного обеспечения;

однократный ввод данных: данные о происшествиях в систему-112 должны вводиться только один раз и быть доступны для других приложений без их копирования.

4.1.5 Требования к надежности

4.1.5.1 Состав и количественные значения показателей надежности для системы в целом или ее подсистем

Технические и программные средства, входящие в состав системы-112, должны функционировать в непрерывном режиме круглосуточно. Допускается остановка отдельных компонентов для технического обслуживания и ремонта, при этом функциональность системы в целом должна сохраняться в полном объеме.

Технологические решения по созданию системы-112 должны обеспечивать выполнение следующих требований:

вероятность потери вызова – не более 0,1%;

устойчивость к сетевым перегрузкам;

предельное время ожидания ответа оператора – не более 8 сек.;

надежность с коэффициентом готовности не ниже 0,9995;

географическое резервирование основных элементов системы-112;

возможность переадресации вызовов между ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС и ДДС, а также переадресация вызовов в объекты системы-112 соседних субъектов Российской Федерации.

Уровень надежности системы-112 должен зависеть от показателей надежности следующих элементов:

КТС РИВП, включающий надежность:

вычислительных серверов;

системы хранения данных;

системы резервного копирования;

оборудования сети хранения данных;

оборудования локальной вычислительной сети;

телекоммуникационного оборудования;

системы бесперебойного питания;

общесистемного программного обеспечения;

прикладного и специального программного обеспечения системы-112;

КТС остальных (находящихся на территории Субъекта РФ) объектов системы-112, включающий надежность:

автоматизированных рабочих мест;

оборудования локальной вычислительной сети;

телекоммуникационного оборудования;

системы бесперебойного питания;

общесистемного программного обеспечения.

серверов резервирования ЦОВ-ЕДДС;

прикладного и специального программного обеспечения системы-112;

каналов передачи данных.

Надежность системы-112 должна обеспечиваться:

аппаратным резервированием:

серверного оборудования;

коммуникационного оборудования;

оборудования АРМ;

линий связи;

источников питания;

функциональной избыточностью;

наличием средств удаленной и автономной диагностики;

наличием группового комплекта запасных инструментов и принадлежностей.

Отказом для технических средств системы-112 является невозможность выполнения приема и обработки вызовов, вызванная неисправностью оборудования.

Технические средства системы-112 не должны требовать постоянного присутствия обслуживающего персонала.

Отказы технических средств или отключение электропитания не должны приводить к потере и искажению информации.

Восстановление работоспособности технических средств системы-112 допускается производить путем замены отдельных блоков или устройств в целом.

При выборе аппаратного обеспечения конкретные (фактические) количественные значения показателей надежности должны быть определены с использованием оценки надежности, основанной на требованиях и положениях нормативных документов.

4.1.5.2 Перечень аварийных ситуаций, по которым должны быть регламентированы требования к надежности

Перечень регламентируемых аварийных ситуаций:

отказы основного и резервного каналов связи;

отказ функционального объекта системы-112 в целом;

отказ аппаратного обеспечения;

отказ программного обеспечения.

импульсные помехи, сбои или прекращение подачи электропитания;

отказ АРМ.

4.1.5.3 Требования к надежности технических и программных средств

Требования к надежности технических и программных средств:

технические средства системы-112 должны обеспечивать сохранность информации при сбоях в электропитании технических средств. Сбои и отказы электропитания не должны приводить к разрушению основных технических средств и разрушению подсистемы обеспечения информационной безопасности;

центральные устройства системы-112 (вычислительные серверы, хранилища информации, основные сетевые устройства) не должны терять работоспособности при кратковременных перебоях в электропитании, для обеспечения данной функции должны использоваться источники бесперебойного питания;

для обеспечения работоспособности системы-112 в условиях длительных отключений электроэнергии необходимо предусматривать для ЦОВ-АЦ и РЦОВ системы резервного электропитания с использованием автономных электрогенераторов;

технические средства должны сохранять работоспособность и обеспечивать целостность данных за счет резервирования критических компонентов оборудования узлов и программного обеспечения, мер по обеспечению структурной избыточности, конкретные технические решения уточняются на стадии технического проектирования;

должна быть предусмотрена аппаратно-программная защита от несанкционированных действий персонала;

для обеспечения надежности функционирования системы-112 должны быть предусмотрены организационно–технические меры по поддержанию работоспособности при выходе из строя основных носителей информации и источников питания, а также средства автоматического корректного завершения работы при полном отказе по электропитанию;

характеристики надежности технических средств, входящих в состав системы-112, определяются техническими условиями на эти средства.

Надежность аппаратных средств системы-112 должна обеспечиваться:

резервированием и кластеризацией основных элементов по схеме не ниже, чем N+1;

географическим резервированием РИВП;

наличием на объектах автоматизации ЗИП[12] в соответствии с рабочей документацией.

Надежность программных средств системы-112 должна обеспечиваться:

контролем целостности данных на уровне СУБД;

сохранением целостности данных при нештатном завершении процедуры, процесса;

сохранением работоспособности программного обеспечения при некорректных действиях пользователя;

резервированием программного обеспечения и данных;

резервным копированием базы данных средствами СУБД для восстановления работоспособности системы-112 в случае ее логического или физического разрушения.

4.1.5.4 Требования к методам оценки и контроля показателей надежности на разных стадиях создания системы в соответствии с действующими нормативно-техническими документами

Оценка надежности системы-112 должна осуществляться на стадии технического проектирования, на основе анализа полноты архитектуры и технических решений по построению системы-112 и их соответствия техническим требованиям данного ТЗ.

Оценка показателей надежности должна быть проведена расчетным путем.

Требования к безопасности

Система-112 должна обеспечивать безопасность персонала при эксплуатации, техническом обслуживании и ремонте с учетом требований нормативных документов по:

электробезопасности;

пожарной безопасности (в части требований пожарной безопасности в производственных помещениях);

общим требованиям безопасности по обеспечению силового электроснабжения.

Технические средства должны отвечать действующей системе государственных стандартов безопасности труда и иметь сертификаты по электробезопасности и электромагнитной безопасности.

Факторы, оказывающие вредные воздействия на здоровье персонала со стороны всех элементов системы-112 (в том числе инфракрасное, ультрафиолетовое, рентгеновское и электромагнитное излучения, вибрация, шум, электростатические поля, ультразвук строчной частоты и т.д.), не должны превышать действующих норм.

[12] Перечень ЗИП определяется на стадии технического проектирования

4.1.6 Требования к эргономике и технической эстетике

В состав АРМ должны входить широкоформатные цветные графические жидко-кристаллические мониторы, алфавитно-цифровая клавиатура, манипулятор типа «мышь», телефонная гарнитура. Общие эргономические требования, регламентирующие организацию рабочего места, взаимное расположение средств связи в пределах рабочего места - по действующим санитарным правилам и нормам.

Размеры экрана монитора должны быть не менее 20 дюймов по диагонали для пропорции экрана 5:4. Фрагменты изображения не должны быть перенасыщены информацией и разнообразием цветовой гаммы. Рабочее место должно включать до 3 однотипных экранов, расположенных в непосредственной близости друг от друга. В таком случае отображаемая на разных мониторах информация должна быть связана между собой, при этом области ввода данных следует сосредоточить на одном из экранов и не допускать необоснованного отвлекания пользователя от выполнения текущих задач, а также переноса фокуса на другие экраны/фокусы без необходимости.

Уровни освещённости рабочих мест персонала должны соответствовать характеру и условиям труда. Должна быть предусмотрена защита от слепящего действия света и отражения (бликов).

Компоновка технических средств системы-112 должна быть рациональной, как по монтажным связям между ними, так и удобству их эксплуатации и обслуживания.

Взаимодействие персонала с системой-112 должно осуществляться посредством визуального графического интерфейса. Интерфейс должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм. 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, графических окон. Ввод-вывод данных системы-112, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном или автоматическом режимах. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям системы-112.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть, управление системой-112 должно осуществляться с помощью набора экранных меню, кнопок, значков и других графических элементов, управляемых кнопками «мыши» с дублированием управления клавиатурой. Клавиатурный режим должен использоваться, главным образом, при заполнении или редактировании текстовых и числовых полей экранных форм. Также должна обеспечиваться возможность выполнения основных

действий по приему и обработке вызова без использования манипулятора типа «мышь» (с использованием «горячих клавиш» клавиатуры).

Должна обеспечиваться корректная обработка аварийных ситуаций, вызванных неправильными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях система-112 должна выдавать пользователю соответствующие сообщения, после чего должна возвращаться в рабочее состояние, предшествовавшее неправильной (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 одних и тех же операций должны использоваться одинаковые графические значки, кнопки и другие управляющие (навигационные) элементы. Должны быть унифицированы термины, используемые для описания идентичных понятий, операций и действий пользователя;

реакция системы-112 на действия оператора (наведение указателя «мыши», переключение фокуса, нажатие кнопки) должна быть типовой для каждого действия над одними и теми же графическими элементами, независимо от их расположения на экране.

Интерактивная среда АРМ системы-112 должна обеспечивать удобный для пользователя интерфейс, отвечающий следующим требованиям:

- в части внешнего оформления:

наличие графического многооконного режима;

настройка графических элементов интерфейса, в том числе цветового оформления, в пределах возможностей операционной системы и технических средств.

- в части интерактивного взаимодействия с персоналом:

удобный и интуитивно понятный интерфейс для персонала, который хорошо знает свою предметную область, не являясь специалистом в области информационных технологий. Интерфейс должен быть оптимизирован для выполнения типовых и часто используемых прикладных операций;

взаимодействие персонала с системой должно осуществляться на русском языке, за исключением системных сообщений, не подлежащих русификации;

должно обеспечиваться предоставление контекстно-зависимой помощи;

должны быть определены требования к системе поддержки принятия решений оператором системы-112 для обеспечения наиболее быстрого и адекватного решения о переадресации разговора;

интерфейс программного обеспечения оператора должен способствовать уменьшению вероятности совершения оператором случайных либо ошибочных действий.

При ответе оператора на входящий телефонный вызов на экране оператора автоматически должна выводиться экранная форма для ввода данных. При этом оператору должен предлагаться сценарий опроса, который должен иметь древовидную структуру и отображаться в зависимости от вводимой информации. Сценарий должен содержать подсказки из вопросов, которые должны быть заданы звонящему абоненту для более точной классификации экстренной ситуации. Ввод данных должен поддерживаться текстовым анализом и выпадающими меню для нормализации введенной информации.

Пользовательский интерфейс должен выбираться в соответствии с его профилем: оператор или диспетчер. Профиль оператора должен обеспечивать его работу с вызывающими абонентами (заявителями/пострадавшими). Профиль диспетчера должен обеспечивать его работу с вызывающими абонентами и функции управления ресурсами. Диспетчеры могут иметь специальные профили, в зависимости от специфики их деятельности, например «Диспетчер скорой помощи».

Требования к эргономике очереди вызовов:

экранные элементы, представляющие очереди вызовов, должны быть размером не менее чем 250*40 пикселей (Ш*В) с возможностью горизонтального масштабирования для обеспечения безошибочного выбора манипулятором типа «мышь».

должна быть возможность для каждой очереди назначить свой звук для оповещения о добавлении вызова в очередь;

очередь вызовов должна отображаться в виде элемента интерфейса, который постоянно присутствует на экране. Элемент должен изменять свой цвет (например, с зеленого на желтый и далее на красный) в зависимости от установленных порогов допустимого времени ожидания;

у оператора АРМ должна быть возможность ответить на следующий вызов из очереди с помощью горячей клавиши.

4.1.7 Требования к транспортабельности

Требования к транспортабельности не предъявляются.

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

4.1.8.1 Условия и режим эксплуатации, которые должны обеспечивать использование технических средств системы-112 с заданными техническими показателями

КТС системы-112 в процессе функционирования должен использовать РИВП (в части потребления инфокоммуникационных услуг, обеспечивающих функциональность системы-112) и размещаться в помещениях ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС, ДДС и регионального ЦУКС МЧС России.

КТС системы-112 должен разрабатываться с учетом эксплуатации в условиях рабочих помещений, соответствующих утвержденным нормам и правилам:

по электропитанию оборудования;

по электростатической защите помещений;

по промышленной системе кондиционирования и вентиляции;

по системе автоматического пожаротушения;

по сертификация оборудования помещения в системе «Электросвязь».

Общими требованиями к эксплуатации КТС системы-112 являются требования к ежедневному и еженедельному обслуживанию программно-аппаратного комплекса РИВП, а также обслуживанию при возникновении особых ситуаций с включением работ по обслуживанию технических средств системы-112, данных в оперативных и архивных хранилищах (базах данных), потоков сообщений в электронных коммуникациях, паролей и прав доступа. Оборудование и программное обеспечение, располагающиеся на функциональных объектах системы-112, не должно требовать обязательного ежедневного обслуживания.

Электропитание должно осуществляться от сети переменного тока напряжением (220 ± 22) В с частотой (50 ±1) Гц. Технические средства системы-112 должны оснащаться источниками бесперебойного питания, которые должны обеспечивать резервное электропитание.

Оборудование инженерных систем, устанавливаемое вне помещений, и внешние коммуникации должны нормально функционировать при температуре окружающей среды от минус 35°С до плюс 35°С при относительной влажности до 85% и классе защиты от проникновения воды и пыли не ниже IP56.

Размещение оборудования системы-112 должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности и обеспечивать доступность к отдельным частям изделия для технического обслуживания и ремонта без демонтажа других составных частей изделия. Помещения объектов автоматизации системы-112 должны соответствовать требованиям технических условий на подключение объектов

автоматизации системы-112 к услугам, оказываемым на ресурсах РИВП, разработанным на стадии технического проектирования.

Для поддержания технических средств системы-112 в исправном состоянии должно обеспечиваться техническое обслуживание. Предусмотреть следующие виды технического обслуживания:

ежедневное техническое обслуживание либо контрольный осмотр;

ежемесячное техническое обслуживание;

годовое техническое обслуживание.

Ремонт оборудования системы-112 в условиях эксплуатации должен обеспечиваться средствами из комплектов ЗИП.

Технологические площадки РИВП должны состоять из машинного зала и вспомогательных помещений, оснащенных оборудованием следующих типов:

информационная инфраструктура - оборудованием для обработки и хранения информации;

телекоммуникационная инфраструктура - оборудованием, обеспечивающим взаимосвязь элементов РИВП и передачу данных;

инженерным оборудованием, обеспечивающим нормальное функционирование всех систем РИВП.

Технологические площадки РИВП должны эксплуатироваться в круглосуточном, круглогодичном режиме. Все инженерные системы РИВП должны быть рассчитаны на работу по формуле 24/7/365 - 24 часа в сутки/7 дней в неделю/ 365 дней в году.

Монтаж оборудования системы-112 должен производиться в 19" серверные шкафы высотой 42U, что должно обеспечивать устойчивость работы оборудования. Использование серверного шкафа должно обеспечивать:

защиту оборудования от вредных воздействий – механических, электромагнитных, химических, гальванических и пр.;

соответствие требованиям технической эстетики;

вентиляцию;

сокращение используемой площади, требуемой для размещения серверного, сетевого и вспомогательного оборудования.

Помещения РИВП должны быть оборудованы системами кондиционирования, гарантированного электропитания, структурированной кабельной системой, системой безопасности и мониторинга, системой пожарной безопасности и отвечать следующим требованиям:

дверные проемы, лифты или лестничные пролеты, а также проходы к помещению должны быть достаточными для вноса оборудования системы-112;

необходимые размеры помещения должны определяться размером стойки с зоной обслуживания с лицевой и тыльной стороны 150 см. Размер помещения должен обеспечивать место для работы вокруг стойки, высотой 42 U. Высота помещения должна позволять установку стойки высотой 2 м с необходимым технологическим пространством над ней и вокруг для сервисного доступа. Минимальная высота помещения должна составлять 2.5 м. Минимальная допустимая площадь помещения должна составлять 6 кв.м;

пол помещения должен выдерживать нагрузку не менее 800 кг/кв.м;

помещения, где располагается КТС системы, должно быть оборудовано системой поддержания климата, которая обеспечивает кондиционирование помещения и поддержку температуры в диапазоне 18°...24°С, поддержку относительной влажности в диапазоне 30%...50%;

освещение – не менее 500 люкс (для основных светильников) горизонтальной плоскости и 200 люкс в вертикальной плоскости. Для снижения электромагнитных помех рекомендуется использовать лампы накаливания или галогенные лампы;

наличие фальшпанелей, лотков и коробов для подвода кабелей связи и электропитания;

наличие оборудования кабельного подвода.

4.1.8.2 Предварительные требования к допустимым площадям для размещения персонала системы-112

Размещение автоматизированных рабочих мест должно быть выполнено в соответствии с требованиями соответствующих нормативных документов.

Расчет потребностей в площадях помещений должен быть произведен на основе значений количества операторов дежурной смены, вычисляемого на основании статистических данных о количестве звонков в существующие ДДС в зависимости от численности населения обслуживаемого района.

Общая площадь ЦОВ-ЕДДС – не менее 65 кв.м, в том числе площадь оперативного зала 12 кв.м, площадь комнаты психологической разгрузки 12 кв.м, площадь серверной 8 кв.м, площадь административных кабинетов 18 кв.м.

Общая площадь ЦОВ-АЦ и РЦОВ – не менее 90 кв.м, в том числе площадь оперативного зала 24 кв.м, площадь комнаты психологической разгрузки 12 кв.м, площадь серверной 15 кв.м, площадь административных кабинетов 18 кв.м.

Указанные требования по общей площади ЦОВ-АЦ, РЦОВ и ЦОВ-ЕДДС не учитывают площади для размещения вспомогательного персонала (юристы, бухгалтеры и т.д.), обучаемых, преподавателей и администраторов обучения, психологов и переводчиков.

Для расчета должны быть приняты следующие параметры:

норматив площади на одно рабочее место оператора 6 кв.м;

норматив площади на одно рабочее место административного персонала 9 кв.м;

коэффициент нагрузки на вспомогательные помещения не менее 0,3.

4.1.8.3 Требования к параметрам сетей энергоснабжения

При проектировании электроснабжения, силового электрооборудования и электрического освещения технологических помещений РИВП необходимо выполнить требования:

инструкций по проектированию электроснабжения промышленных предприятий, силового и осветительного электрооборудования промышленных предприятий;

инструкций по проектированию и устройству молниезащиты зданий и сооружений;

норм и правил по проектированию искусственного освещения;

норм и правил по электротехническим устройствам.

Электроприемники должны обеспечиваться электроэнергией от двух независимых взаимно резервирующих источников питания.

Электроснабжение ЦОВ-АЦ, РЦОВ, РИВП должно быть выполнено по особой группе первой категории по обеспечению надежности электроснабжения (два независимых взаимно резервирующих источника питания, также третий резервирующий источник питания - отдельно стоящая дизель-генераторная установка с автоматическим запуском при пропадании внешнего электроснабжения).

Мощность ДГУ определяется потребностями серверного и телекоммуникационного оборудования, электрических и механических систем объекта. Время работы ДГУ от собственного топливного резервуара (топливного бака), а также технические решения по его дозаправке определяются на стадии технического проектирования, минимальное время работы ДГУ без дозаправки не менее 8 часов

Электроснабжение ЦОВ-ЕДДС, АРМ ДДС определяется на стадии технического проектирования и пообъектно согласуется с Заказчиком, и должно быть организовано наиболее надежным способом, доступным без проведения существенных объемов дополнительных работ.

Система электроснабжения оборудования ЦОВ-АЦ, РЦОВ, РИВП должна обеспечивать функционирование объекта в случае пропадания внешнего электропитания. Время автономной работы указанного оборудования должно быть не менее 30 минут (до гарантированного запуска ДГУ).

ИБП должны быть спроектированы по схеме резервирования не ниже, чем N+1. Необходимо предусмотреть отдельный щит ИБП для серверного и телекоммуникационного оборудования. Должен быть обеспечен контроль тока потребления в отдельных телекоммуникационных шкафах.

Расчет электрических нагрузок электроприемников необходимо производить с учетом коэффициентов использования и мощности (Cos φ).

Сеть штепсельных розеток для подключения вспомогательного оборудования не должна присоединяться к шинам щитов и шкафов, от которых питается телекоммуникационное и серверное оборудование.

Питающую сеть напряжением 380/220 В электроснабжения электроприемников ЦОВ-АЦ, РЦОВ, РИВП от подстанции до щита станции управления и силовых или осветительных пунктов необходимо выполнять кабелями, проводами в коробах или в скрыто проложенных винипластовых трубах.

Не должны применяться провода и кабели с изоляцией из вулканизированной резины или других серосодержащих материалов.

4.1.8.4 Требования по количеству, квалификации обслуживающего персонала и режимам его работы

Требования по количеству, квалификации персонала и режимам его работы приведены в пункте 344.1.2 настоящего ТЗ.

4.1.8.5 Требования к составу, размещению и условиям хранения комплекта запасных изделий и приборов

В системе-112 должен быть предусмотрен комплект запасных изделий и приборов.

Состав, количество и тип изделий, а также места их хранения ЗИП должны быть уточнены на стадии рабочего проектирования.

Средства вычислительной техники и связи, так же машинные носители должны храниться в упаковке на стеллажах в отапливаемых помещениях при температуре воздуха от +5 до +40˚С и относительной влажности воздуха не более 80 %. В помещении для хранения средств вычислительной техники не должно быть агрессивных примесей, вызывающих коррозию. Срок хранения – в пределах гарантийного срока эксплуатации.

4.1.8.6 Требования к регламенту обслуживания системы-112

Для системы-112 должны быть предусмотрены следующие виды периодических работ по техническому обслуживанию системы:

ежедневный осмотр;

ежемесячный технический осмотр;

эксплуатационная проверка;

внеплановое обслуживание.

Для каждого вида обслуживания на стадии рабочего проектирования должны быть определены:

состав выполняемых процедур, способ выполнения и контролируемые значения параметров;

периодичность проведения;

ответственное лицо;

порядок учета выполненных работ по техническому обслуживанию;

порядок контроля выполняемых работ.

В частности, в обслуживание должны входить работы по:

контролю и упорядочению маршрутов электронных коммуникаций;

сохранению (копированию) журналов изменений баз данных и резервных копий баз данных;

восстановлению баз данных при порче или разрушении данных;

профилактическому контролю состояния дисковых запоминающих устройств и данных на них.

Выполнение указанных требований должно обеспечивать непрерывную работу КТС системы-112. При этом резервное копирование информации может осуществляться в двух режимах:

создание полной копии базы данных;

сохранение изменений, внесенных со времени создания последней архивной копии.

Периодичность и очередность этих операций определяются отдельным распоряжением. Создание полной копии базы данных осуществляется полным копированием всех файлов указанной базы на внешние носители. При сохранении изменений, внесенных со времени создания последней архивной копии, на внешние носители переносятся только те изменения базы данных, которые были сделаны со времени последней операции архивирования (полного или частичного).

4.1.9 Требования к защите информации

Применяемые в системе-112 средства и технологии защиты информации должны обладать свойствами модульности, масштабируемости и возможности адаптации КСЗИ к различным организационным и техническим условиям.

Система защиты информации системы-112 должна обеспечивать следующие свойства защищаемой информации:

доступность информации – возможность для авторизованного пользователя за приемлемое время получить доступ к информационному ресурсу в соответствии с установленными для этого пользователя правами доступа;

целостность информации – актуальность и непротиворечивость информации, защищенность информационного ресурса от разрушения и несанкционированного изменения в процессах передачи, обработки, хранения или представления;

конфиденциальность информации – защита информационного ресурса от несанкционированного ознакомления, а также предотвращение утечки конфиденциальной информации по каналам связи.

Система-112 классифицируется [13] как специальная распределенная информационная многопользовательская система класса К1 с разграничением прав доступа с доступом к сетям связи общего пользования, требования к информационной структуре системы-112 по защите от утечек по каналам побочных электромагнитных излучений и наводок не предъявляются.

Система-112 классифицируется[14] как автоматизированная система класса 1Г и специальная информационная система персональных данных класса К1. Криптографические средства защиты информации, используемые для защиты конфиденциальных и иных охраняемых в соответствии с законодательством Российской Федерации сведений, в том числе персональных данных, обрабатываемых в системе-112, должны обеспечивать криптографическую защиту по уровню не ниже уровня КС2.

Состав и объем защищаемой информации определяется путем моделирования угроз по результатам обследования объектов подключения.

Значения показателей, а также порядок и состав мероприятий по созданию, организации и поддержке эксплуатации подсистемы информационной безопасности должны быть согласованы на стадии технического проектирования.

Должна быть организована разрешительная система доступа пользователей и эксплуатирующего персонала к техническим и программным средствам, а также информационным ресурсам системы-112.

Средства вычислительной техники, подлежащие защите, должны удовлетворять требованиям по защите информации от утечки за счет побочных электромагнитных излучений и наводок согласно нормативным документам

Система защиты информации в системе-112 должна являться неотъемлемой составной частью создаваемой автоматизированной системы и реализовываться в виде отдельной подсистемы – подсистемы обеспечения информационной безопасности. Требования к ПОИБ системы-112 приведены в пункте 4.2.6.

Требование настоящего ТЗ по защите информации могут быть скорректированы по результатам технического проектирования по согласованию с Заказчиком.

---

[13] определяется на основании разработанной на стадии формирования требований к системе-112 частной модели угроз

[14] определяется на основании разработанной на стадии формирования требований к системе-112 частной модели нарушителя

4.1.10 Требования по сохранности информации при авариях

Сохранность информации в системе-112 должна обеспечиваться при всех аварийных ситуациях.

В случае возникновения аварии или сбоя в процессе выполнения пользовательских задач должно быть обеспечено восстановление БД до состояния, актуального на момент последней завершенной системой транзакции.

В случае повреждения журналов транзакций СУБД должно обеспечиваться восстановление состояния системы на момент создания последней резервной копии данных, но не более чем за сутки до момента сбоя.

Для сохранности данных в системе должны быть предусмотрены специальные средства сопровождения БД, которые обеспечивают:

создание резервной копии данных;

восстановление данных в целостное состояние посредством резервной копии;

создание архива данных;

восстановление архива данных.

При разработке системы должен быть предусмотрен регламент, описывающий требования к средствам и способам хранения резервных копий.

Необходимо предусмотреть возможность запуска средств создания резервных копий в ручном или в автоматическом режиме.

4.1.11 Требования к защите от влияния внешних воздействий

4.1.11.1 Требования к радиоэлектронной защите средств системы-112

Средства технического обеспечения системы-112 должны быть защищены от влияния:

радиоэлектронных помех;

электромагнитных полей, электрическая составляющая которых не превышает 0,3 В на 1 $м^2$;

Электромагнитное излучение радиодиапазона, возникающее при работе электробытовых приборов, электрических машин и установок, приёмопередающих устройств, эксплуатируемых на месте размещения КТС системы-112, не должны приводить к нарушениям работоспособности подсистем.

4.1.11.2 Требования по стойкости, устойчивости и прочности к внешним воздействиям

Условия эксплуатации КТС системы-112 определяются для макроклиматических районов умеренного и холодного климата, категория размещения 4 (закрытые отапливаемые помещения с искусственно регулируемыми климатическими условиями).

Технические средства системы-112 должны выполнять свои функции и сохранять свои показатели в пределах установленных значений при следующих условиях эксплуатации:

рабочее значение температуры окружающего воздуха от +10 до +35°С, предельное верхнее значение для СВТ равно 40°С, предельное нижнее значение 3°С, возможное изменение температуры с темпом 5°С/час;

относительная влажность воздуха - от 50 до 80%, верхнее предельное значение - 90%;

атмосферное давление: верхнее рабочее значение 106.7 кПа (800 мм рт.ст.), нижнее рабочее значение 86.6 кПа (650 мм рт.ст.), нижнее предельное значение 84.0 кПа (630 мм рт.ст.);

содержание пыли в помещении не более 1,0 мг/м^3 при размере частиц не более 3 мкм;

содержание коррозийно-активных агентов в атмосфере помещения составляет 30-60% от величин, определяемых для атмосферы IV типа; сернистого газа от 20 до 250 мг/м^3 или от 0.025 до 0.31мг/м^3: хлоридов от 0.3 до 30 мг/м^3 (группа условий эксплуатации металлов и сплавов - 1);

воздействие вибрации в диапазоне частот 10-25 Гц с амплитудой до 0.1 мм;

магнитные поля постоянные и переменные с частотой 50 Гц напряженностью до 400А/м (кроме накопителей информации на основе магнитных дисков).

4.1.12 Требования к патентной чистоте

Используемое при проектировании, разработке и вводе в эксплуатацию системы-112 аппаратное обеспечение, инструменты разработки программного обеспечения и СУБД должны быть лицензионными и сертифицированы на территории Российской Федерации.

Разработчик специального программного обеспечения системы-112 должен предоставить документальные свидетельства на владение интеллектуальной собственностью и авторскими правами.

Система-112 должна соответствовать требованиям патентного законодательства Российской Федерации.

4.1.13 Требования по стандартизации и унификации

При разработке системы-112 должны быть использованы общероссийские классификаторы.

В качестве основного формата данных в интерфейсах взаимодействия со смежными и внешними системами должен использоваться стандарт XML 1.1 (http://www.w3.org/TR/xml11/) или стандарт JSON (http://json.org/).

Описания форматов данных взаимодействия должны быть представлены в документах технического проекта на внедрение системы-112 в соответствии со стандартом XML Schema 1.0 (http://www.w3.org/TR/xmlschema-0/).

4.1.14 Дополнительные требования

Прикладное программное обеспечение системы-112 должно иметь специальный режим функционирования АРМ, обеспечивающий обучение операторов и диспетчеров.

В КСА системы-112 должна обеспечиваться синхронизация таймеров (часов) ПТК и АРМ.

Подготовку персонала запланировать на базе РЦОВ, для чего предусмотреть дополнительные помещения и оборудование для обеспечения первоначальной подготовки и периодической переподготовки оперативного персонала системы-112.

4.2 Требования к функциям (задачам), выполняемым системой

Система-112 должна состоять из следующих подсистем:

телекоммуникационная подсистема;

информационно-коммуникационная подсистема;

подсистема консультативного обслуживания;

геоинформационная подсистема;

подсистема мониторинга;

подсистема обеспечения информационной безопасности.

Решение задач системы-112 обеспечивают развернутые на функциональных объектах вышеуказанные подсистемы.

4.2.1 Телекоммуникационная подсистема

Телекоммуникационная подсистема предназначена для обеспечения прохождения вызовов (сообщений о происшествиях), включая телефонные вызовы, короткие текстовые сообщения (SMS), от пользователей (абонентов) сетей фиксированной или подвижной связи в систему-112, взаимодействия объектов в рамках системы-112, а также взаимодействия с региональным ЦУКС МЧС России и с объектами системы обеспечения вызова оперативных служб по единому номеру «112» соседних субъектов Российской Федерации в части обеспечения прохождения необходимой информации.

Телекоммуникационная подсистема должна обеспечивать выполнение следующих функций:

техническое обеспечение прохождения вызовов (сообщений о происшествиях) от абонентов стационарной и мобильной телефонной связи, коротких текстовых сообщения в систему-112;

техническое обеспечение информационного обмена всеми необходимыми видами информации между объектами системы-112, а также с региональным ЦУКС МЧС России и с объектами системы обеспечения вызова оперативных служб по единому номеру «112» соседних субъектов Российской Федерации;

техническое обеспечение получения данных о местонахождении транспортного средства, оснащенного телематическим модулем GPS/ГЛОНАСС;

техническое обеспечение получения данных о местонахождении вызывающего абонентского устройства, а также иных данных от оператора связи, необходимых для обеспечения реагирования по вызову.

Технические решения должны обеспечивать поэтапный ввод в эксплуатацию системы и должны обеспечивать работоспособность системы в условиях одновременной эксплуатации новых цифровых каналов и существующих на разных направлениях.

Связь между составными частями системы-112 и со смежными (внешними) автоматизированными системами должна осуществляться в автоматическом режиме по IP-протоколам.

Присоединение системы-112 к местным телефонным сетям должно быть организовано через УОВЭОС по линиям связи с цифровым интерфейсом E1 ОКС-7 не менее чем по двум потокам или по IP-сети с применением протокола SIP.

На стадии технического проектирования системы-112 необходимо определить требования к каналам связи и проектные решения на каждом направлении, к системам привязки (последней мили) для всех объектов системы-112, к оборудованию подсистемы (технико-экономическое обоснование, в т. ч. по эксплуатационным свойствам и затратам на техническое обеспечение).

4.2.2 Информационно-коммуникационная подсистема

Информационно-коммуникационной подсистема предназначена для обеспечения хранения и актуализации баз данных, обработки информации о полученных вызовах (сообщениях о происшествиях) и возможности получения информации о происшествии из архива в оперативном режиме, а также поддержки принятия решений по экстренному реагированию на принятые вызовы и планированию мер реагирования.

Информационно-коммуникационная подсистема должна обеспечивать в автоматизированном режиме выполнение следующих функций:

прием, регистрация и документирование каждого поступившего вызова (сообщения о происшествии);

приём и обработка вызовов на единый телефонный номер «112», поступающих через операторов фиксированной и мобильной связи, в том числе с помощью e-mail, факс-сообщения, SMS (при наличии технических и иных возможностей предоставления операторами связи доступа к SMS-центру по протоколу SMPP), направление их оператору ЦОВ-АЦ (РЦОВ, ЦОВ-ЕДДС), перенаправление диспетчеру ДДС;

организацию и ведение очереди входящих вызовов;

распределение и маршрутизация вызовов между операторами ЦОВ-АЦ (РЦОВ, ЦОВ-ЕДДС);

независимую идентификацию электронных карточек всех обращений и карточек происшествий, заведенных согласно указанным обращениям;

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-112;

возможность перевода оператором вызова в систему консультативного обслуживания населения;

детектирование и обработку массовых вызовов по поводу уже зарегистрированного происшествия;

детектирование повторных обращений граждан;

регистрацию номера телефона вызывающего абонента, если эта информация поступила от оператора связи;

запись телефонного разговора при вызове;

поддержку регистрации нового происшествия, или привязку нового обращения к ранее зарегистрированному происшествию;

получение информации о месте происшествия;

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;

регистрацию информации о месте установки телефона или о местоположении вызывающего абонентского устройства в дополнение к регистрации информации об адресе места происшествия;

фиксация ложных и злонамеренных вызовов;

возможность ведения «черных» списков – списков абонентов или номеров телефонов, запросы которых обслуживаются по особому сценарию;

формирование информационного сообщения в целях принятия решений при угрозе или наступлении ЧС;

возможность автоматического голосового оповещения абонентов по заданному списку телефонов;

возможность автоматической рассылки факс-сообщений по заданному списку телефонов;

возможность автоматической рассылки SMS-сообщений по протоколу SMPP по заданному списку телефонов;

учет следующих параметров в процессе обработки телефонного вызова: дата, день недели, время, номер абонента, линия, с которой поступил вызов;

организацию автоматизированных оповещений по телефону по списку абонентов;

формирование и отправку отчета о реагировании согласно регламенту взаимодействия;

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;

оповещение администратора системы о наличии нештатной ситуации в работе и методах ее устранения в целях скорейшего возобновления нормальной работы;

информационное взаимодействие с ДДС, входящими в систему-112;

взаимосвязь с существующими и разрабатываемыми автоматизированными информационными системами экстренных оперативных служб и других участников информационного взаимодействия;

предоставление оперативной информации по происшествиям для руководства администраций муниципальных образований и входящих в их состав населенных пунктов в соответствии с их территориальной принадлежностью;

сбор, обработку и представление информации о работе системы-112 в различной форме, в том числе и с применением средств деловой графики, и в различных разрезах (временном, территориальном);

сбор и хранение информации остальных подсистем, сбор и хранение статистической информации;

хранение записанных переговоров;

контекстный поиск информации;

формирование отчетов, как за указанный период, так и отчетов реального времени;

предоставление средств редактирования информационно-консультационной базы данных;

получение отчетов касательно оперативной обстановки, расхода сил и средств, статистики по происшествиям и ЧС, по приему и обработке вызовов, по взаимодействию в рамках системы-112;

возможность хранения, наполнения и редактирования базы данных о типовых ситуациях, методах реагирования, используемой в подсистемах поддержки принятия решений и консультативного обслуживания населения;

возможность получения отчетов на основании актуальных и архивных данных;

возможность автоматического формирования группы отчетов в режиме реального времени;

возможность построения отчетов с агрегацией показателей и с их детальной расшифровкой;

разграничение прав доступа к отчетам;

автоматизацию процесса принятия решений, в том числе использование типовых сценариев реагирования на основе утвержденных ведомственных регламентов при ликвидации ЧС и происшествий;

доступ оператора к информационно-консультационной базе данных и быстрый поиск в ней для получения информации о типовых ситуациях и методах реагирования;

использование соответствующих справочников (при формировании записи о происшествии для категорий, видов и статусов происшествий) и возможность актуализации данных справочников;

учет вызовов, ЧС и происшествий;

возможность работы со списком происшествий – атрибутивный и полнотекстовый поиск, сортировка, вывод на печать;

отображение (визуализацию) информации по вызову и происшествию, в том числе номера вызывающего абонента с указанием при наличии технической возможности адрес места установки телефона или местоположения мобильного устройства, принадлежности вызывающего номера к «черному списку» для информирования о возможном ложном или злонамеренном вызове, атрибут повторности вызова, наличие уже зарегистрированных происшествий по тому же адресу (атрибут массовых вызовов);

опрос абонента по определенным заранее сценариям (наличие системы детерминированных диалогов);

привязку нескольких записей зарегистрированных вызовов к одной записи о происшествии;

возможность автоматизированной и автоматической квалификации зарегистрированных вызовов;

автоматизированный выбор состава оповещаемых экстренных служб в зависимости от типа происшествия с возможностью корректировки этого перечня оператором;

автоматический выбор способа оповещения экстренной службы в соответствии с согласованным со службой регламентом;

отображение информации о поступлении или не поступлении в соответствии с регламентом подтверждения («квитанции») о регистрации происшествия во взаимодействующей АС;

визуализацию средствами АРМ оператора информации, накопленной прочими подсистемами системы-112;

прием информации по показаниям контрольных устройств, установленных на объектах, осуществление функций контроля и управления согласно установленным регламентам, прослушивание салона автомобиля и голосовая связь с водителем.

4.2.3 Подсистема консультативного обслуживания

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

Подсистема консультативного обслуживания населения должна, как минимум, обеспечивать:

предоставление населению информации по системе-112;

информационную поддержку населения и организаций по вопросам безопасности, способам защиты от чрезвычайных ситуаций;

хранение в специальной базе данных информации, предоставляемой для консультаций;

обслуживание телефонного вызова интерактивной информационно-справочной телефонной системой (систему маршрутизации, управляемой пользователем с помощью клавиш тонального набора телефонного аппарата) для получения информации в соответствии с темой запроса, в том числе без участия оператора.

4.2.4 Геоинформационная подсистема

Геоинформационная подсистема предназначена для отображения на основе электронных карт природно-географических, социально-демографических, экономических и других характеристик территорий, местонахождение лица, обратившегося по номеру «112», и (или) абонентского устройства, с которого осуществлен вызов (сообщение о происшествии), место происшествия, а также местонахождение транспортных средств ДДС, привлеченных к реагированию на происшествие.

Геоинформационная подсистема должна обеспечивать отображение[15]:

природно-географических, социально-демографических, экономических и других характеристик территории Субъекта РФ;

местонахождения лица (или абонентского устройства), обратившегося по номеру «112», в том числе зоны (сектора) при неточном позиционировании;

места возникновения происшествия или ЧС;

мест расположения ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС, а также объектов, сил и средств подчинения ДДС и регионального ЦУКС МЧС России;

мест расположения потенциально опасных и критически важных объектов;

---

[15]ГИС должна отображать территорию и данные:
для ЦОВ-АЦ и РЦОВ - в административных границах Субъекта РФ, а также смежных муниципальных образований соседних Субъектов РФ, имеющих общую административную границу;
для ЦОВ-ЕДДС - в административных границах данного муниципального образования Субъекта РФ, а также муниципальных образований, имеющих общую административную границу с данным муниципальным образованием Субъекта РФ (в том числе муниципальными образованиями соседних Субъектов РФ)

маршрутов движения между заданными объектами (после автоматической прокладки по графу дорог с использованием информации о пробках, если такая информации доступна);

навигационной информации о составе и местонахождении, истории перемещения сил и средств реагирования (при наличии технических возможностей использования технологий ГЛОНАСС/GPS).

Перечень и объем информации, предоставляемый на разные типы АРМ (операторов, диспетчеров), определяется на стадии технического проектирования.

Пользовательский интерфейс подсистемы должен предоставлять следующие дополнительные 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;

прокладку маршрутов движения транспортных средств между выбранными объектами;

поиск свободных сил и средств, задействованных ДДС в районе происшествия для организации реагирования;

отображение статуса привлекаемых сил и средств ДДС;

нанесения необходимой информации на карту[16];

редактирование информации, нанесенной на карту.

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

Подсистема должна иметь механизмы взаимодействия с уже имеющимися геоинформационными системами ДДС, в том числе обеспечивать поддержку основных стандартов форматов используемых карт.

4.2.5 Подсистема мониторинга

Подсистема мониторинга предназначена для приема и обработки информации и сигналов, поступающих от датчиков, установленных на контролируемых стационарных и подвижных объектах, в том числе от автомобильных терминалов системы экстренного реагирования при авариях ЭРА-ГЛОНАСС и терминалов ГЛОНАСС/GPS, установленных на транспортных средствах ДДС, привлеченных к реагированию на происшествие и транспортных средствах, перевозящих опасные грузы.

Подсистема мониторинга должна решать задачи сбора информации от разнообразных устройств объектов мониторинга, обработки и квалификации нештатной ситуации на объектах мониторинга, предоставления пользователям подсистемы целостной и актуальной информации о

[16] Перечень информации определяется на этапе технического проектирования

положении дел на объектах мониторинга, передачи информации об экстренных ситуациях на объектах мониторинга в другие подсистемы системы-112.

Подсистема мониторинга должна также обеспечивать формирование и передачу в другие компоненты системы-112 вызова по внештатной ситуации на контролируемых стационарных и подвижных объектах.

4.2.6 Подсистема обеспечения информационной безопасности

Подсистема обеспечения информационной безопасности должна обеспечивать защиту компонентов, объектов подключения и информации, находящейся в зоне ответственности системы-112 от потенциальных злоумышленников, непроизвольных действий и прочих угроз информационной безопасности.

Целью реализации ПОИБ является снижение вероятного ущерба от реализации угроз ИБ и выполнение требований законодательства Российской Федерации в части защиты информации.

ПОИБ предназначена для защиты конфиденциальной информации, включая персональные данные, ПО и технические средства системы-112.

ПОИБ должна обеспечивать необходимую и достаточную защиту информационных ресурсов системы-112 от характерных угроз безопасности, определенных на основе разработанных модели угроз и модели нарушителя, соответствующих нормативно-правовой документации в области защиты информации ФСБ России и ФСТЭК России.

ПОИБ должна предусматривать следующие меры [17] по противодействию актуальным угрозам системе-112:

Актуальная угроза	Описание угрозы	Меры противодействия	
		Технические	Организационные
Угрозы несанкционированного доступа к информации			
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн			
Кражи, модификации, уничтожения информации	Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы Системы-112 и средства защиты, а так же происходит работа пользователей	Создание СЗПДн с помощью средств, сертифицированных ФСТЭК России, пропускной режим, крепкие двери, решетки на окнах, опечатывание помещений, наличие сейфов	Подбор персонала, ознакомление с ответственностью
Несанкционированное отключение	Угроза осуществляется путем НСД внешними и	Создание СЗПДн с помощью средств,	Подбор персонала, ознакомление с

[17] определяется на основании разработанной на стадии формирования требований к системе-112 частной модели угроз

Актуальная угроза	Описание угрозы	Меры противодействия	
		Технические	Организационные
средств защиты	внутренними нарушителями в помещения, где расположены средства защиты ИСПДн	сертифицированных ФСТЭК России	ответственностью, разработка инструкций
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).			
Действия вредоносных программ (вирусов)	Угроза осуществляется при помощи программно-математического воздействия (действие программ-вирусов)	Установка средств антивирусной защиты, сертифицированных ФСТЭК России	Разработка инструкций по антивирусному контролю
Установка ПО, не связанного с исполнением служебных обязанностей	Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей Системы-112 или ее элементов	Установка и настройка СЗИ, сертифицированных ФСТЭК России, разграничение прав доступа пользователей	Разработка инструкций, ознакомление с ответственностью
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.			
Непреднамеренная модификация (уничтожение) информации сотрудниками	Угроза осуществляется за счет действия человеческого фактора пользователей Системы-112, которые нарушают положения принятых правил работы с Системой-112 или не осведомлены о них	Установка и настройка СЗИ, сертифицированных ФСТЭК России, разграничение прав доступа пользователей	Разработка инструкций, ознакомление с ответственностью
Непреднамеренное отключение средств защиты	Угроза осуществляется за счет действия человеческого фактора пользователей системы, которые нарушают положения принятых правил работы с Системой-112 и средствами защиты или не осведомлены о них	Установка и настройка СЗИ, сертифицированных ФСТЭК России, разграничение прав доступа пользователей	Разработка инструкций, ознакомление с ответственностью
Угрозы преднамеренных действий внутренних нарушителей			

Актуальная угроза	Описание угрозы	Меры противодействия	
		Технические	Организационные
Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Угроза осуществляется путем НСД внутренних нарушителей в помещения, где расположены элементы системы и средства защиты, а так же происходит работа пользователей	Создание СЗПДн с помощью средств, сертифицированных ФСТЭК России, пропускной режим, крепкие двери, решетки на окнах, опечатывание помещений	Подбор персонала, разработка инструкций, ознакомление с ответственностью
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Угроза осуществляется за счет действия человеческого фактора пользователей системы, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.		Подбор персонала, разработка инструкций, ознакомление с ответственностью
Угрозы несанкционированного доступа по каналам связи.			
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:			
Перехват за переделами контролируемой зоны	Угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, циркулирующие за пределами контролируемой зоны, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль	Установка средств межсетевого экранирования, сертифицированных ФСТЭК России. Установка средств криптографической защиты, сертифицированных ФСБ России. Использование средств обнаружения вторжений и анализа защищенности, сертифицированных ФСТЭК России	Разработка инструкций
Перехват в пределах контролируемой зоны внешними нарушителями	угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль	Пропускной режим, крепкие двери, решетки на окнах, опечатывание помещений, использование средств межсетевого экранирования	Разработка инструкций

Актуальная угроза	Описание угрозы	Меры противодействия	
		Технические	Организационные
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	угроза заключается в передаче запросов сетевым службам хостов Системы-112 и анализе ответов от них	Установка средств межсетевого экранирования, сертифицированных ФСТЭК России. Установка средств криптографической защиты, сертифицированных ФСБ России. Использование средств обнаружения вторжений и анализа защищенности, сертифицированных ФСТЭК России	Разработка инструкций
Угрозы выявления паролей по сети	Угроза может быть реализована с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing)	Установка средств межсетевого экранирования, сертифицированных ФСТЭК России. Установка средств криптографической защиты, сертифицированных ФСБ России. Использование средств обнаружения вторжений и анализа защищенности, сертифицированных ФСТЭК России	Разработка инструкций
Угрозы навязывания ложного маршрута	Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы	Установка средств межсетевого экранирования, сертифицированных ФСТЭК России. Установка средств криптографической защиты, сертифицированных ФСБ России. Использование средств обнаружения вторжений и анализа защищенности, сертифицированных ФСТЭК России	Разработка инструкций
Угроза подмены доверенного объекта	Угроза заключается в передаче служебных	Установка средств межсетевого	Разработка инструкций

Актуальная угроза	Описание угрозы	Меры противодействия	
		Технические	Организационные
в сети	сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных	экранирования, сертифицированных ФСТЭК России. Установка средств криптографической защиты, сертифицированных ФСБ России. Использование средств обнаружения вторжений и анализа защищенности, сертифицированных ФСТЭК России	
Угрозы внедрения ложного объекта сети	Угроза основана на использовании недостатков алгоритмов удаленного поиска и заключается в передаче по сети специальных запросов и получении на них ответов с искомой информацией	Установка средств межсетевого экранирования, сертифицированных ФСТЭК России. Установка средств криптографической защиты, сертифицированных ФСБ России. Использование средств обнаружения вторжений и анализа защищенности, сертифицированных ФСТЭК России	Разработка инструкций
Угрозы типа «Отказ в обслуживании»	Угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты	Использование лицензионного ПО. Установка средств межсетевого экранирования, сертифицированных ФСТЭК России. Установка средств криптографической защиты, сертифицированных ФСБ России. Использование средств обнаружения вторжений и анализа защищенности, сертифицированных ФСТЭК России	Разработка инструкций
Угрозы удаленного запуска приложений	Угроза заключается в стремлении запустить на	Установка средств межсетевого	Разработка инструкций

Актуальная угроза	Описание угрозы	Меры противодействия	
		Технические	Организационные
	хосте Системы-112 различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста	экранирования, сертифицированных ФСТЭК России. Установка средств криптографической защиты, сертифицированных ФСБ России. Использование средств обнаружения вторжений и анализа защищенности, сертифицированных ФСТЭК России	
Угрозы внедрения вредоносных программ по локальной вычислительной сети	Угроза осуществляется за счет внедрения вредоносных программ, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей	Установка средств межсетевого экранирования, сертифицированных ФСТЭК России. Установка средств криптографической защиты, сертифицированных ФСБ России. Использование средств обнаружения вторжений и анализа защищенности, сертифицированных ФСТЭК России	Разработка инструкций

Соответственно средствами ПОИБ должны выполняться следующие задачи, направленные на обеспечение требуемых свойств информации:

защита информации от несанкционированного доступа;

регистрация и учёт активности пользователей и программного обеспечения;

защита циркулирующей информации от несанкционированной модификации при передаче по каналам связи, хранении и обработке на СВТ системы-112;

контроль сетевого доступа к ресурсам системы-112;

обеспечение конфиденциальности информации при передаче по каналам связи с использованием криптографических методов;

защита от проникновения компьютерных вирусов;

анализ передаваемой информации с целью обнаружения несанкционированного воздействия на ПО системы-112;

обнаружение уязвимых версий или ошибок конфигурации ПО, используемого в системе-112.

Средства защиты, входящие в состав ПОИБ, должны иметь развитые средства регистрации критических системных событий в электронных журналах и средства оперативного оповещения об этих событиях администраторов безопасности.

Структура ПОИБ системы-112 должна включать в себя следующие функциональные подсистемы:

управления доступом;

регистрации и учета;

обеспечения целостности;

межсетевого экранирования;

криптографической защиты информации;

антивирусной защиты;

обнаружения вторжений;

анализа защищенности.

ПОИБ должна обеспечивать независимость функционирования каждой из входящих в ее состав структурных подсистем защиты. Нарушение функционирования любой подсистемы защиты не должно приводить к нарушению функционирования других подсистем защиты.

ПОИБ системы-112 должна использовать следующие средства защиты:

собственные «наложенные» СЗИ (СЗИ, входящие в состав только ПОИБ);

механизмы защиты, встроенные в ПО функциональных подсистем системы-112;

сервисы ИБ, предоставляемые сторонними и смежными (внешними) подсистемами, эксплуатируемыми Заказчиком.

ПОИБ системы-112 должна строиться на основе ограниченного числа типов и версий используемого программного обеспечения, а также типов и конфигураций аппаратно-программных средств защиты, уточняемых на стадии технического проектирования.

ПОИБ системы-112 должна максимально использовать сервисы ИБ, предоставляемые смежными и внешними системами, эксплуатируемыми Заказчиком.

Собственные «наложенные» СЗИ ПОИБ системы-112, предаваемые в эксплуатацию Заказчику, должны быть совместимы с СЗИ, эксплуатируемыми Заказчиком.

С целью снижения стоимости владения при разработке решений в части состава собственных «наложенных» СЗИ ПОИБ системы-112 предпочтение должно отдаваться оборудованию и ПО, уже находящемуся в эксплуатации у Заказчика.

Используемые в составе ПОИБ СЗИ должны в установленном порядке пройти процедуру оценки соответствия требованиям информационной безопасности (сертификации) в системе ФСБ России или ФСТЭК России.

Состав и структура ПОИБ должна определяться требованиями данного ТЗ и требованиями к объектам, подключаемым к системе-112, сформированными на основе актуальных типовых моделей нарушителя и угроз.

4.3 Требования к видам обеспечения

4.3.1 Требования к математическому обеспечению

Математическое обеспечение должно определять модели и алгоритмы обработки информации, алгоритмы управления прикладными процессами.

Алгоритмы обработки информации должны описывать алгоритмы, осуществляющие сервисные функции при обработке информации (сортировка, фильтрация, выполнение арифметических операций над массивами данных и др.), алгоритмы оперативного контроля и управления.

Разработанные алгоритмы должны обеспечивать высокую оперативность исполнения (минимальное количество ветвлений, условных переходов и прерываний) при разумной их длине. Разработанные алгоритмы управления прикладными процессами должны обладать высокой надежностью и устойчивостью.

4.3.2 Требования информационному обеспечению

4.3.2.1 Требования к составу, структуре и способам организации данных

Информационное обеспечение системы-112 по содержанию и полноте должно быть достаточно для комплексного представления всех основных вопросов.

При разработке системы должны предусматриваться современные технологии обработки данных, в том числе:

перемещение по иерархии данных;

агрегацию и детализацию данных для проведения анализа;

расчет аналитических показателей по согласованным методикам.

В рамках обеспечения информационного взаимодействия с другими информационными системами в системе-112 должна быть обеспечена совместимость с действующими и создаваемыми смежными и внешними информационными системами посредством открытых программных API интерфейсов, файлового обмена и доступа при помощи технологии Web-сервисов в едином согласованном формате на основе XML, XSL.

Организация данных в системе-112 должна включать в себя:

операционные данные - структурированную динамическую информацию, порождаемую и используемую в ходе осуществления основных процессов деятельности;

электронные документы - неструктурированные данные, порождаемые в процессах деятельности, а так же получаемые извне, после преобразования в электронный вид;

служебную информацию - структурированную информацию, обеспечивающую функционирование компонентов и системы-112 в целом;

внешние информационные ресурсы - структурированную информацию, получаемую из автоматизированных систем организаций и ведомств согласно соглашениям об информационном обмене и техническим условиям обмена;

нормативно-справочную информацию - условно-постоянную информацию, используемую в процессах деятельности, которая в структурированной части должна формироваться на основе единой системы классификации и кодирования и которая включает в себя международные, общегосударственные, ведомственные и отраслевые классификаторы, нормативы и справочники, а также неструктурированную нормативно-справочную документацию;

метаданные - структурированную, понимаемую автоматизированную системой информацию о характеристиках и множествах принимаемых значении хранимых данных, которая описывает, в частности, информационное наполнение (структуру) базы данных и рабочие процессы;

картографическую и адресную информацию - структурированную графическую информацию, предназначенную для реализаций функций геоинформационной системы.

Сущности предметной области деятельности должны выделяться на основе устойчивых объектов предметной области, а не на основе формализации документов, подверженных частым изменениям.

Сущности предметной области должны предусматривать атрибуты для идентификации.

Все подсистемы системы-112 должны использовать единые, ведущиеся централизованно метаданные, НСИ и классификаторы, обеспечивать возможность формирования локальных справочников, поддерживать историчность (версионность) метаданных и НСИ для обеспечения возможности проведения анализа с использованием данных за предшествующие временные периоды.

Разрозненные данные должны быть интегрированы в едином централизованном хранилище информации.

Состав, структура и способы организации данных в базах данных, а также состав и структура НСИ должны быть уточнены на стадии технического проектирования.

4.3.2.2 Требования к информационному обмену между компонентами системы

В системе-112 возможны следующие виды информационного обмена между компонентами:

сбор информации, содержащейся в текстовых журналах;

обмен информацией между компонентами системы-112, расположенными в одной ЛВС;

обмен информацией между компонентами системы-112, расположенными в разных ЛВС.

Информационный обмен между компонентами системы-112 должен осуществляться с учетом требований пункта 4.1.1.2 настоящего ТЗ.

4.3.2.3 Требования к информационной совместимости со смежными и внешними системами

В системе-112 возможны следующие виды информационного обмена со смежными и внешними системами:

получение информации из смежных (внешних) информационных ресурсов;

отправка информации в смежные (внешних) информационные ресурсы;

межведомственный обмен информационными ресурсами.

Взаимодействие со смежными и внешними информационными ресурсами должно осуществляться с учетом требований пункта 4.1.1.4 настоящего ТЗ.

Детальные требования к видам информационного обмена со смежными и внешними системами и состав данных для осуществления информационного обмена по каждой системе должны быть сформированы на стадии технического проектирования системы-112.

Система-112 должна поддерживать возможность экспорта данных в смежные и внешние системы через файлы данных или информационные сервисы, а также обеспечивать возможность загрузки данных, получаемых от смежных (внешних) систем.

4.3.2.4 Требования по использованию общесоюзных и зарегистрированных республиканских, отраслевых классификаторов, унифицированных документов и классификаторов

Структуры баз данных подсистем должны поддерживать кодирование хранимой и обрабатываемой информации в соответствии с общероссийскими классификаторами (там, где они применимы).

Система, по возможности, должна использовать классификаторы и справочники, которые ведутся в Единой системе классификации и кодирования.

Требования к составу и содержанию общих справочников и классификаторов должны быть сформированы на стадии технического проектирования и уточнены на этапе разработки рабочей документации системы-112.

4.3.2.5 Требования по применению систем управления базами данных

Для хранения данных подсистем системы-112 должны использоваться современные реляционные или объектно-реляционные СУБД. Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД (индексы, хранимые процедуры, триггеры и т.п.).

Средства СУБД, а также средства используемых операционных систем должны обеспечивать документирование и протоколирование информации, циркулирующей в системе-112.

Структуры и состав прикладных баз данных подсистем должны определяться таким образом, чтобы обеспечить полноту хранимой информации, выполнение технологических операций, совместимость с другими базами данных и формирование выходных документов на бумажных носителях.

Структуры и состав прикладных баз данных подсистем уточняются на этапе разработки рабочей документации системы-112.

4.3.2.6 Требования к структуре процесса сбора, обработки, передачи данных в системе и представлению данных

Должны быть регламентированы следующие процессы сбора данных:

получение данных из электронных форм пользовательского интерфейса системы-112, заполняемых персоналом;

получение данных, регистрируемых автоматическими компонентами системы-112;

получение данных от смежных систем;

получение данных от внешних систем.

Данные, поступающие в систему-112, должны проходить обработку средствами форматно-логического контроля. В случае нарушения правил форматно-логического контроля данных пользователь должен уведомляться об обнаруженных нарушениях, должна предоставляться возможность исправления нарушений.

В системе-112 запрещается передача данных с использованием открытых информационных каналов связи, за исключением данных, обрабатываемых подсистемой консультационного обслуживания.

Представление данных пользователям системы-112 должно осуществляться через специализированные графические пользовательские интерфейсы (GUI) в соответствии с правами разграничения доступа.

Прямой доступ персонала к БД системы-112 должен быть ограничен в соответствии с должностными инструкциями.

4.3.2.7 Требования к защите данных от разрушений при авариях и сбоях в электропитании

При возникновении аварийных ситуаций, связанных со сбоями электропитания, информация в базах данных системы-112 должна сохраняться.

4.3.2.8 Требования к контролю, хранению, обновлению и восстановлению данных

К контролю данных предъявляются требования:

доступ к данным должен предоставляться только авторизованным пользователям в соответствии с их служебными полномочиями, а также с учетом категории запрашиваемых данных;

в системе-112 должны протоколироваться все события, связанные с изменением своего информационного наполнения и обеспечиваться возможность, в случае сбоя в работе, восстановления состояния, с использованием ранее запротоколированных изменений данных.

К хранению данных предъявляются требования:

технические средства, обеспечивающие хранение информации, должны использовать современные технологии, позволяющие обеспечить повышенную надежность хранения данных и оперативную замену оборудования (распределенная избыточная запись/считывание данных, зеркалирование, независимые дисковые массивы, кластеризация);

должно обеспечиваться хранение данных в установленные сроки;

резервные копии данных должны храниться в СХД, предназначенных для долгосрочного хранения данных.

В системе-112 должны быть предусмотрены функции резервного копирования данных, которые должны обеспечивать резервное копирование и восстановление после сбоев в работе БД и параметров всех подсистем системы-112.

В системе-112 должны применяться методы инкрементального, дифференциального и полного резервного копирования.

Регламенты резервного копирования должны быть разработаны на этапе разработки рабочей документации.

4.3.2.9 Требования к процедуре придания юридической силы документам, продуцируемым техническими средствами системы-112

Придание юридической силы документам, продуцируемым с использованием системы-112, осуществляется в соответствии с действующим законодательством Российской Федерации.

4.3.3 Требования к лингвистическому обеспечению

4.3.3.1 Требования к применению языков программирования высокого уровня

Используемые при разработке языки программирования высокого уровня должны обеспечивать решение всех задач по реализации функций системы-112.

Допускается использование стандартных языков программирования высокого уровня, отвечающих требованиям реализации задач предметной области.

Перечень требований уточняется на стадии технического проекта и согласовывается протоколами с Заказчиком.

4.3.3.2 Требования к применению языков подготовки отчетов

В составе системы-112 должен использоваться язык для подготовки отчетов, позволяющий производить модификацию существующих и создание новых отчетов. Язык для подготовки отчетов должен иметь встроенные средства создания графических представлений (диаграмм, графиков и т.п.), а также обеспечивать экспорт результатов в форматы широкого применения (текстовый, ODF, XLS, DOC и т.п.).

Перечень требований к применению языков подготовки отчетов может уточняться в процессе разработки проекта и согласовываться протоколами с Заказчиком.

4.3.3.3 Требования к способам организации диалога с персоналом

Для организации диалога системы-112 с персоналом и пользователями должен применяться графический пользовательский интерфейс.

Информационно-лингвистическая совместимость подсистем системы-112 и смежных (внешних) информационных систем должна обеспечиваться централизованным ведением кодификаторов, справочников и классификаторов.

В системе-112 должны обеспечиваться хранение и обработка текстовой информации на русском и английском языках[18].

Специальное программное обеспечение системы-112 для организации взаимодействия с пользователем должно использовать русский язык.

Способ организации диалога с персоналом должен обеспечивать:

уменьшение вероятности совершения оператором случайных ошибочных действий;

предусматривать логический контроль ввода данных;

возможность изменения и сохранения индивидуальных настроек пользователя Системы;

Общение оператора с лицами, обратившимися по номеру «112» должно осуществляться посредством гарнитуры (включающей наушники и микрофон), предназначенной для профессионального использования.

При поступлении вызовов (ситуационных карточек) в ДДС на АРМ оператора (диспетчера) должно воспроизводиться звуковое оповещение.

4.3.3.4 Требования к средствам описания предметной области (объекта автоматизации)

В составе комплексов разработки должны быть средства описания предметной области и объекта автоматизации, обеспечивающие автоматизированный процесс прямого и обратного проектирования баз данных и подсистем, а так же документирование полученных результатов.

Языки манипулирования данными должны отвечать требованиям стандарта ANSI SQL-92 и поддерживать реляционную модель баз данных, а также стандарт ODBC/JDBC.

---

[18] конкретный перечень определяется на этапе проведения обследования и согласуется Заказчиком

Для внешнего взаимодействия должны использоваться структуры XML или JSON.

Допускается выдача сообщений от приобретаемых компонентов общесистемного программного обеспечения системы-112 на английском языке.

Вся документация, разрабатываемая в рамках создания системы-112, должна быть представлена на русском языке за исключением документов, носящих международный характер.

4.3.4 Требования к программному обеспечению

Используемые программные средства должны поддерживать реализацию системы-112 на различных современных платформах, обеспечить поддержку современных стандартов функционирования программного обеспечения.

Программное обеспечение должно быть обеспечено поддержкой производителя на срок не менее 5 лет и быть совместимым с решениями, используемыми МЧС России.

Программные средства системы-112 состоят из:

общесистемного программного обеспечения;

специального программного обеспечения.

4.3.4.1 Общесистемное программное обеспечение

Общесистемное обеспечение должно обеспечивать:

создание и поддержку единой информационно-телекоммуникационной инфраструктуры;

обеспечение решения информационных и функциональных задач подсистем, входящих в состав системы-112;

функционирование оборудования и аппаратного обеспечения системы-112, а также обеспечивать подключение технических средств различного назначения;

целостность информационных ресурсов системы-112 на уровне используемых операционных систем и систем управления базами данных;

поддержку механизмов кластеризации;

распределенное хранение данных;

единые принципы, методы, технологии хранения, обработки и представления данных пользователям системы-112;

достоверность и однозначность данных;

реализацию в заданных режимах задач и функций, возложенных на систему-112;

предоставление необходимой и достаточной скорости обработки данных;

безопасный авторизованный доступ.

Структура общесистемного программного обеспечения:

операционные системы;

системы управления базами данных;

средства виртуализации;

средства управления и мониторинга;

общесистемное ПО АРМ.

4.3.4.1.1 Операционные системы

Серверная операционная система должна обеспечивать:

высокую производительность;

поддержку кластерных технологий;

высокую степень устойчивости и надежности;

поддержку обменов информации по используемым сетям;

удобный и понятный пользователю графический интерфейс, простоту и эффективность использования;

возможность работы с мультимедиа;

возможность конфигурирования под конкретные условия использования;

поддержку многозадачного или псевдомногозадачного режима;

модульность, гибкую конфигурируемость;

малое время реакции, многоуровневую, основанную на приоритетах, обработку прерываний и присвоение меток времени зафиксированным событиям;

развитые средства коммуникации (поддержка стандартных сетей, а также различных интерфейсов ввода-вывода).

управление программами - ОС осуществляет загрузку в оперативную память всех программ, передает им управление в начале их работы, выполняет различные действия по запросу выполняемых программ и освобождает занимаемую программами оперативную память при их завершении. В рамках функции управления программами ОС также осуществляет:

параллельное исполнение нескольких задач (поддержка многозадачного режима работы);

распределение ресурсов компьютера между задачами;

организацию взаимодействия задач друг с другом;

обеспечение работы с устройствами долговременной памяти, такими как магнитные диски, ленты, оптические диски и т.д., управление свободным пространством на этих носителях и структурирование пользовательских данных;

управление периферийными устройствами (стандартный доступ к различным устройствам ввода/вывода, таким как терминалы, модемы, печатающие устройства и т.п., обеспечение во взаимодействии пользовательских программ с нестандартными внешними устройствами);

организацию межмашинного взаимодействия и разделение ресурсов в ЛВС;

защиту системных ресурсов, данных и программ пользователя, исполняющихся процессов и самой себя от ошибочных и враждебных действий пользователей и их программ.

Операционная система АРМ должна обеспечивать:

высокую производительность;

высокую степень устойчивости и надежности;

поддержку обменов информации по используемым сетям;

удобный и понятный пользователю графический интерфейс, простоту и эффективность использования;

возможность работы с мультимедиа;

возможность конфигурирования под конкретные условия использования;

поддержку многозадачного или псевдомногозадачного режима;

модульность, гибкую конфигурируемость;

малое время реакции, многоуровневую, основанную на приоритетах, обработку прерываний и присвоение меток времени зафиксированным событиям;

развитые средства коммуникации (поддержка стандартных сетей, а также различных интерфейсов ввода-вывода).

управление программами - ОС осуществляет загрузку в оперативную память всех программ, передает им управление в начале их работы, выполняет различные действия по запросу выполняемых программ и освобождает занимаемую программами оперативную память при их завершении. В рамках функции управления программами ОС также осуществляет:

параллельное исполнение нескольких задач (поддержка многозадачного режима работы);

распределение ресурсов компьютера между задачами;

организацию взаимодействия задач друг с другом;

обеспечение работы с устройствами долговременной памяти, такими как магнитные диски, ленты, оптические диски и т.д., управление свободным пространством на этих носителях и структурирование пользовательских данных;

управление периферийными устройствами (стандартный доступ к различным устройствам ввода/вывода, таким как терминалы, модемы, печатающие устройства и т.п., обеспечение во взаимодействии пользовательских программ с нестандартными внешними устройствами);

организацию межмашинного взаимодействия и разделение ресурсов в ЛВС;

защиту системных ресурсов, данных и программ пользователя, исполняющихся процессов и самой себя от ошибочных и враждебных действий пользователей и их программ.

4.3.4.1.2 Система управления базами данных

ПО СУБД должно обеспечивать:

предоставление встроенных средств удаленного администрирования;

высокую производительность;

возможность построения распределенной базы данных;

масштабируемость (наращивание производительности при увеличении числа пользователей и объемов данных);

систему разграничения доступа, интегрированную с системой разграничения доступа ОС (применение пользователей и групп ОС);

распределенное хранение данных;

возможность удаленного доступа к данным;

прозрачность расположения данных - обеспечение высокой скорости доступа к данным, поддержку кластерных технологий, поддержку распределенного хранения данных;

гетерогенность – должна обеспечиваться работа с данными, которые хранятся в системах с различной архитектурой и производительностью;

сетевую прозрачность - поддержку одинаковой работоспособности в условиях разнородных сетей, удаленный доступ;

поддержку распределенных запросов - обеспечение возможности объединения данных из баз, размещённых в разных системах;

поддержку распределенных изменений - обеспечение возможности изменения данных в базах, размещенных в разных системах, в пределах предоставленных пользователю прав;

поддержку распределенных транзакций - выполнение транзакции, выходящих за рамки одной вычислительной системы, поддержка целостности распределенной БД при возникновении отказов в отдельных системах или в сети;

безопасность - обеспечение защиты от несанкционированного доступа;

универсальность доступа - обеспечение единой методики доступа ко всем данным.

4.3.4.1.3 Средства виртуализации ПО

Средства виртуализации программного обеспечения должны обеспечивать:

управление виртуальными ресурсами системы-112;

перераспределение виртуальных ресурсов, динамическую балансировку нагрузки;

консолидацию инфраструктурных серверов, консолидацию до 10 и более виртуальных машин на одном физическом процессоре;

защиту непрерывности процессов с использованием единой платформы для аварийного восстановления виртуальных машин в случае аппаратного сбоя;

упрощенную инициализацию инфраструктуры;

централизованный и распределенный контроль использования аппаратных ресурсов системы-112;

перемещение приложений на новые аппаратные средства (перемещение операционных систем и программного обеспечения на виртуальные серверы, работающие на новом оборудовании);

разделение одного физического сервера на несколько автономных и независимых друг от друга виртуальных машин;

полноценную виртуализацию ресурсов процессоров, памяти, ресурсов хранилищ и сетевых ресурсов;

использование каждой отдельной виртуальной машиной до 4-х физических процессоров;

группировку физических серверов, хранилищ или сетевых компонентов в унифицированные логические ресурсы;

защиту виртуальной инфраструктуры от аппаратных сбоев и угроз безопасности;

клонирование, копирование и создание шаблонов виртуальных машин;

формирование отчетов о производительности процессоров, памяти и операций ввода-вывода;

централизованное администрирование и управление службами виртуальной инфраструктуры;

инициализацию, мониторинг и управление виртуальной ИТ-средой с помощью единого интерфейса;

перенос виртуальных машин между отдельными физическими серверами;

работоспособность приложений независимо от используемого оборудования и операционных систем;

мониторинг состояния физических серверов, готовности и степени использования виртуальных машин на основе единого интерфейса;

интеграцию с продуктами управления системами через API-интерфейсы веб-служб;

управление ресурсами виртуальных машин, динамическое выделение ресурсов;

энергосберегающую оптимизацию ресурсов;

высокую детализацию управления доступом, формирование контрольных данных;

управление пользовательскими ролями и разрешениями, сеансами, управление исправлениями.

4.3.4.1.4 ПО средств управления и мониторинга

Программное обеспечение средств управления и мониторинга должно обеспечивать:

удаленную одновременную установку обновлений программного обеспечения;

автоматическую настройку и обновление системы безопасности;

разбиение КТС на отдельные группы с возможностью независимого управления группами;

удаленное выполнение консольных команд;

поддержание единой конфигурации ОС и ПО;

мониторинг системных параметров с возможностью автоматического исправления ошибок;

удаленное управление вычислительными серверами;

централизованный мониторинг сбоев отдельных компонентов;

обработку и отображение событий, произошедших на управляемых объектах;

совместную работу планировщика заданий и обработчика событий;

возможность упреждающего управления с использованием прогнозирования событий на основе прошлых и настоящего состояний системы.

4.3.4.1.5 ПО автоматизированных рабочих мест

ПО АРМ должно обеспечивать выполнение следующих функций:

создание новых документов;

внесение изменений в документы и их оформление;

сохранение документов в виде файлов;

поиск и открытие уже имеющихся документов;

вывод документов на печать, на средства отображения информации;

антивирусную защиту.

4.3.4.2 Специальное программное обеспечение

Специальное программное обеспечение должно обеспечивать персоналу функциональность согласно вышеприведенным требованиям, а также:

автоматическое или ручное заполнение унифицированных карточек информационного обмена (карточек ЧС и происшествий);

возможность идентификации сообщения с уже существующим ЧС или происшествием;

классификацию ЧС или происшествия с помощью ключевых слов;

классификацию события с помощью иерархического справочника;

объединение нескольких вызовов по одному событию;

возможность просмотра в реальном режиме времени заполняемых оператором системы-112 (диспетчером ДДС) унифицированных карточек информационного обмена и прослушивание соответствующих переговоров диспетчером ДДС (оператором системы-112, диспетчером иной ДДС) в зависимости от типа происшествия;

передача информации по вызовам (в различных формах представления) в ДДС и контроль реагирования;

фильтрацию журнала учета ЧС и происшествий (событий) в зависимости от типа события, его состояния, времени регистрации, местоположения, оператора и т. д.;

отображение справочников адресных данных (городов, населенных пунктов, улиц, объектов);

предоставление справочника объектов системы-112;

предоставление справочника ресурсов для реагирования;

подготовку планов реагирования с описанием действий оператора ДДС, вариантов оповещения ДДС;

заполнение вышеуказанных справочников, описаний объектов, а также разработку слоев электронных карт и привязку объектов;

запись, архивирование, поиск и воспроизведение переговоров.

СПО должно предоставлять следующие дополнительные функции управления вызовами:

распределение поступающих вызовов между операторами должно обеспечиваться в соответствии с настройками Системы;

возможность настройки схем эскалации неотвеченных вызовов за заданное время дополнительным операторам, всем операторам соответствующего ЦОВ-ЕДДС и относящихся к нему ДДС, всему персоналу Системы;

возможность настройки разных схем распределения для разных типов вызовов;

распределение вызовов между операторами в соответствии с их загрузкой (по времени обработки диспетчером последнего вызова);

возможность установки специального периода для завершения операторами работы над вызовом перед передачей ему нового вызова;

должна обеспечиваться возможность создания нескольких очередей для разных типов (внутренних, внешних, от подсистемы мониторинга) вызовов;

должна обеспечиваться возможность постановки разных типов вызовов в общую очередь;

обеспечиваться обновление данных на экранах остальных операторов при ответе оператором на вызов;

должна предусматриваться возможность для контроля администратором длины очереди и времени обработки вызовов;

СПО должно предоставлять следующие функции организации совместной работы:

подключение любого количества служб (участников) к происшествию;

занесение (изменение) информации о вызовах в систему и автоматическое обновление на экранах участвующих в обработке события операторов (диспетчеров) информации о вызове, при переходе оператором (диспетчером) на другое поле экранной формы ввода либо его неактивности в течение более чем 5 секунд в процессе занесения (изменения) такой информации одним из операторов (диспетчеров);

возможность подключения новых участников до завершения обработки предыдущим с немедленным предоставлением введенных данных и немедленным отображением изменений;

обеспечение участникам работы по происшествию возможности прослушивания записи вызовов, относящихся к происшествию;

агрегирование в одной записи о происшествии информации, поступающей от разных служб;

представление информации по происшествию свое для каждой службы;

однократное введение информации (поля данных) используемой в представлениях для нескольких служб;

должна обеспечиваться возможность прикрепления к происшествию любых документов в виде файлов;

раскрытие или ограничения доступа к информации служб на основе системы разграничения доступа.

СПО должно предоставлять следующие дополнительные функции:

подсказки (предложения) оператору о привязке поступившего вызова к ранее зарегистрированному (и не завершенному) вызову на основании совпадения телефонного номера заявителя, места происшествия и т. д.;

автоматизированная и автоматическая квалификация зарегистрированных вызовов на основе справочников для категорий, видов и статусов происшествий с возможностью актуализации справочников;

любое количество уровней в иерархическом классификаторе происшествий;

возможность создания собственных классификаторов для каждого вида ДДС;

формирование перечня вопросов для интервью заявителя и/или регистрации информации по реагированию в зависимости от иерархического классификатора типов происшествий;

автоматическое изменение перечня вопросов интервью в зависимости от ответов на предыдущие вопросы;

автоматическое изменение классификации происшествия в результате использования ответов на вопросы интервью;

формирование подсказок для действий оператора по результатам интервью;

автоматическое определение ДДС, к зоне ответственности (географической и функциональной) которой (которых) относится данное происшествие;

автоматическое определение перечня объектов повышенного риска, находящихся в зоне происшествия;

автоматизированный поиск свободных сил и средств ДДС, находящихся в районе происшествия для реагирования (в зависимости от имеющегося оборудования и навыков экипажей);

создание типовых сценариев реагирования операторов, диспетчеров на происшествие, экстренную или чрезвычайную ситуацию;

автоматический выбор сценария реагирования в зависимости от классификации происшествия, результатов интервью, места происшествия, номера абонента;

создание специальных сценариев реагирования, привязанных к объекту повышенного риска, для ликвидации происшествий в зоне этого объекта.

СПО должно предоставлять следующие дополнительные функции в части геоинформационной подсистемы:

возможность автоматического (без выполнения оператором специально направленных на это действий) присоединения к происшествию «снимка» карты с районом происшествия;

плавное масштабирование карты;

возможность выбора сил и средств на карте (выбор символа ресурса на карте и назначение через контекстное меню задачи на реагирование на происшествие);

возможность отображения местоположения ресурсов по карте вручную.

Указанный функционал должен предоставляться конкретному должностному лицу системы-112 в соответствии с его обязанностями. При изменении обязанностей должностного лица, или изменении лица, работающего на АРМ, перенастройка АРМ или изменение набора установленного на нем ПО не должно требоваться.

Функционал АРМ оператора и диспетчера (в части информационно-коммуникационной подсистемы) должен реализовываться единым приложением. Доступные через это приложение функционал должен определяться правами и обязанностями лица и (возможно) выбранным рабочим заданием.

Должна быть предусмотрена возможность распространения функционала АРМ операторов (диспетчеров) на АРМ административного и обслуживающего персонала.

СПО должно предоставлять возможности «свободного» расположения операторов, т. е. функциональные возможности всех АРМ соответствующего типа, входящих в сиситему-112, и выполняемые задачи должны определяться исключительно параметрами входа пользователя в систему, а не местом расположения АРМ в пределах системы-112.

4.3.4.3 Требования к независимости программных средств от используемых средств вычислительной техники и операционной среды

Программные средства должны обеспечивать совместимость со средствами вычислительной техники, построенными по архитектуре x86 (32 бита) и x64 (64 бита).

Совместимость программных продуктов с используемыми СВТ должна определяться в соответствии с рекомендациями фирм производителей этих программных продуктов (согласно спискам совместимости аппаратных средств фирм-производителей).

4.3.4.4 Требования к качеству программных средств, а также к способам его обеспечения и контроля

Надежность программных средств должна обеспечиваться использованием сертифицированных операционных систем, общесистемных программных средств и инструментальных программных систем, используемых при разработке СПО. Надежность СПО должна обеспечиваться комплексом мероприятий, осуществляемых для управления качеством создания ПО на всех этапах жизненного цикла.

Надежность программных средств должна обеспечиваться за счет:

надежности общесистемного и разрабатываемого СПО;

проведения комплекса мероприятий отладки, поиска и исключения ошибок;

ведения журналов системных сообщений и ошибок по подсистемам для последующего анализа и изменения конфигурации.

На каждом этапе разработки программных средств должна проводиться проверка правильности принятых решений по разработке и применению готовых программных средств.

В системе-112 должно обеспечиваться автоматическое (без перерыва функционирования системы-112) обновление программного обеспечения.

Система автоматического обновления программного комплекса должна обеспечивать:

постоянный контроль версионности компонентов программного комплекса;

проверку инфраструктурных условий, при выполнении которых, обновление будет произведено успешно;

возможность, в случае неудачной попытки обновления, отката к текущей версии программного комплекса системы.

Надежность специального программного обеспечения должна подтверждаться путем проведения функционального и нагрузочного тестирования.

Уточнение требований к системе обновления программного комплекса должно производиться на стадии технического проектирования.

4.3.4.5 Требования по необходимости согласования вновь разрабатываемых программных средств с фондом алгоритмов и программ

Необходимость согласования вновь разрабатываемых программных средств с фондом алгоритмов и программ отсутствует.

4.3.5 Требования к техническому обеспечению

4.3.5.1 Требования к видам технических средств, в том числе к видам комплексов технических средств, программно-технических комплексов и других комплектующих изделий, допустимых к использованию в системе

4.3.5.1.1 Требования к видам технических средств

Комплекс технических средств системы-112 должен размещаться на базе РИВП, территориально разнесенных и объединенных общей сетью передачи данных с пропускной способностью каналов на менее 512 Мбит/с, а также на базе объектов автоматизации системы-112, подключенных к РИВП через резервируемые каналы передачи данных.

В качестве технического обеспечения комплекса технических средств системы-112 должны применяться следующие виды технических средств:

Состав КТС системы-112, размещенный на базе РИВП:

вычислительные серверы;

система хранения данных;

система резервного копирования;

высокоскоростная сеть передачи данных;

телекоммуникационное оборудование;

локальная вычислительная сеть;

структурированная кабельная система;

система гарантированного электроснабжения;

комплекс средств защиты информации.

Состав КТС системы-112, размещенный на объектах автоматизации системы-112 на территории Субъекта РФ:

автоматизированные рабочие места;

телекоммуникационное оборудование;

локальная вычислительная сеть;

структурированная кабельная система;

система гарантированного электроснабжения;

комплекс средств защиты информации;

серверы резервирования ЦОВ-ЕДДС.

Количественный и качественный состав КТС системы-112 уточняется на стадии технического проектирования в ходе обследования и определения уровня технической оснащенности объектов автоматизации.

Вычислительное ядро системы-112 должно базироваться на РИВП.

4.3.5.1.2 Требования к видам программно-технических комплексов

Требования к видам программно-технических комплексов должны быть определены на стадии технического проектирования после согласования с Заказчиком типа используемой платформы, определения перечня основных поставщиков (изготовителей оборудования и разработчиков программного обеспечения).

4.3.5.1.3 Требования к программному и аппаратному обеспечению в части обеспечения информационной безопасности системы

Общие требования к типам операционных систем, типам серверов и ПЭВМ, а также технических средств защиты, которые должны быть задействованы в КСЗИ, не должны противоречить требованиям технической политики, проводимой Заказчиком.

Применяемые программно-аппаратные решения должны обеспечивать возможность гибкой модификации структуры и масштабирования ресурсов КСЗИ. Программное обеспечение, предлагаемое к использованию в КСЗИ, должно соответствовать современным мировым требованиям по функциональному назначению, поддерживать основные протоколы совместимости и обмена.

Специальное программное обеспечение, предлагаемое к использованию в КСЗИ, должно иметь документацию и поддерживаться производителями на основе долгосрочного договора.

4.3.5.2 Требования к функциональным, конструктивным и эксплуатационным характеристикам средств технического обеспечения системы-112

4.3.5.2.1 Общие требования к КТС

Архитектура решения должна иметь возможность масштабирования и должна соответствовать последним тенденциям развития ИТ-архитектуры с обеспечением необходимых требований, таких как надежность, простота в обслуживании, низкое потребление энергии, минимальное время восстановления после сбоев, защищенность.

Общие требования, предъявляемые к техническому обеспечению РИВП:

использование технологий виртуализации для объединения вычислительных и других системных ресурсов, а также для их динамического перераспределения;

возможность масштабирования;

резервирование и стекирование всего телекоммуникационного оборудования;

функционирование в режиме 24x7x365.

Общие требования, предъявляемые к КТС системы-112:

серверное оборудование, а также вычислительное и коммутационное оборудование ЛВС, СКС и других систем КТС должно размещаться в 19-дюймовых стоечных шкафах;

вся информация, необходимая для мониторинга технического состояния оборудования комплекса технических средств, должна выводиться на пульт дежурного РИВП;

должна быть обеспечена возможность администрирования оборудования КТС с единой консоли управления;

расположение оборудования должно осуществляться таким образом, чтобы обеспечить беспрепятственный доступ для его обслуживания;

все места подключения интерфейсов должны иметь дополнительную фиксацию, для предотвращения их самопроизвольного отключения во время транспортировки и эксплуатации;

оборудование должно быть новое, не восстановленное, должно иметь заводскую сборку и выпускаться серийно;

техническая документация должна быть выполнена на русском языке;

оборудование должно поставляться вместе с комплектом запасных частей;

должен предоставляться единый федеральный номер службы поддержки, поддержка по данному номеру должна оказываться круглосуточно;

гарантия на оборудование должна быть не менее 1 года.

4.3.5.2.2 Требования к вычислительным серверам

Требования к составу, количеству и характеристикам вычислительных серверов системы-112 должны быть уточнены на стадии технического проектирования и согласованы с Заказчиком, быть достаточными для поддержания функционирования системы-112 в пределах заданных в данном Техническом задании характеристик.

Вычислительные серверы должны обеспечивать функционирование общесистемного, прикладного и СПО системы-112, ПО СУБД и резервного копирования.

Вычислительные серверы должны обеспечивать высокую степень надежности и отказоустойчивости в сочетании с высокой производительностью.

Резервирование всех функциональных компонентов серверов должно осуществляться по схеме не ниже, чем N+1.

Серверы, входящие в состав системы-112, могут быть реализованы в виде виртуальных машин в отказоустойчивой среде виртуализации, установленной не менее чем на двух физических серверах с общей системой хранения данных.

Вычислительные серверы должны иметь документацию на русском языке и гарантийную поддержку производителя.

4.3.5.2.3 Требования к серверам резервирования ЦОВ-ЕДДС

Требования к составу, количеству и характеристикам серверов резервирования ЦОВ-ЕДДС системы-112 должны быть уточнены на стадии технического проекта и согласованы протоколами с Заказчиком.

Серверы резервирования ЦОВ-ЕДДС должны обеспечивать функционирование ОПО и СПО, ПО СУБД и резервного копирования для обеспечения базовой функциональности системы-112.

Серверы резервирования ЦОВ-ЕДДС должны обеспечивать высокую степень надежности и отказоустойчивости в сочетании с высокой производительностью.

Резервирование всех функциональных компонентов серверов резервирования ЦОВ-ЕДДС должно осуществляться по схеме не ниже, чем N+1.

Серверы резервирования ЦОВ-ЕДДС могут быть реализованы в виде виртуальных машин в отказоустойчивой среде виртуализации, установленной не менее чем на двух физических серверах с общей системой хранения данных.

Серверы резервирования ЦОВ-ЕДДС должны иметь документацию на русском языке и гарантийную поддержку производителя.

4.3.5.2.4 Требования к системе хранения данных

Система хранения данных должна обеспечивать высокую степень надежности и отказоустойчивости в сочетании с высокой производительностью.

Резервирование всех функциональных компонентов СХД должно осуществляться по схеме не ниже, чем N+1.

СХД должна иметь:

адаптеры для подключения к системе хранения данных и системе резервного копирования через высокоскоростные интерфейсы;

поддержку аппаратных уровней 0, 1, 3, 5, 10, 30 и 50 и обеспечивать организацию виртуальных RAID-массивов уровней 0,1,5;

централизованную систему управления;

возможность расширения дискового пространства;

документацию на русском языке и гарантийную поддержку со стороны производителя;

возможность «горячей» замены:

контроллеров;

жестких дисков;

вентиляторов;

блоков питания.

Объем СХД должен рассчитываться в зависимости от нагрузочной способности системы.

В СХД должны применяться жесткие диски обеспечивающие возможность их «горячей» замены.

Каждый элемент СХД должен быть выполнен в конструктиве для установки в стандартный 19" телекоммуникационный шкаф.

Программное обеспечение для управления СХД должно включать опции для обеспечения выполнения вышеприведенных требований, обладать интуитивно понятным интерфейсом для работы с СХД и сопровождаться необходимыми лицензиями и комплектом документации.

4.3.5.2.5 Требования к системе резервного копирования

Система резервного копирования должна обеспечивать высокую степень надежности и отказоустойчивости в сочетании с высокой производительностью.

Резервирование всех функциональных компонентов СРК должно осуществляться по схеме не ниже, чем N+1.

СРК должна иметь:

адаптеры для подключения к системе хранения данных и системе резервного копирования через высокоскоростные интерфейсы.

документацию на русском языке и гарантийную поддержку производителя.

Объем СРК должен рассчитываться в зависимости от:

объема данных системы хранения;

объема данных, предназначенных для резервного копирования;

применяемых аппаратных уровней дисковых массивов (RAID);

степени доступности (готовности) резервируемых данных.

Каждый элемент СРК должен быть выполнен в конструктиве для установки в стандартный 19" телекоммуникационный шкаф.

В качестве проектного решения должны быть разработаны регламенты архивного хранения информации.

Программное обеспечение СРК должно включать необходимые лицензии, а также опции для удаленного управления, должна обеспечиваться совместимость с программными комплектами производителей приложений для систем резервного копирования.

4.3.5.2.6 Требования к высокоскоростной сети передачи данных

Высокоскоростная сеть передачи данных должна:

обеспечивать высокоскоростной обмен между вычислительными серверами, системой хранения данных и системой резервного копирования;

обеспечивать резервирование всех функциональных компонентов высокоскоростной сети передачи данных по схеме не ниже, чем N+1.

Все элементы высокоскоростной сети передачи данных должны быть выполнены в конструктиве для установки в стандартный 19" телекоммуникационный шкаф, оборудование должно иметь документацию на русском языке и гарантийную поддержку производителя.

4.3.5.2.7 Требования к телекоммуникационному оборудованию

Телекоммуникационное оборудование должно:

обеспечивать высокую степень надежности и отказоустойчивости в сочетании с высокой производительностью;

обеспечивать резервирование всех функциональных компонентов по схеме не ниже, чем N+1.

иметь документацию на русском языке и гарантийную поддержку производителя.

Серверные шкафы необходимые для установки оборудования КТС должны иметь ширину 19".

Место в серверных шкафах должно быть рассчитано с учётом возможности масштабирования компонент КТС.

Серверные шкафы должны оставляться, как минимум, в следующей комплектации:

дверцы и боковые панели под один ключ;

крепеж для соединения элементов шкафов;

опоры с регулировкой горизонтальности;

монтажные компоненты;

предварительно установленные ролики, боковые панели;

установленная документация.

Серверные шкафы должны быть выполнены в едином дизайне.

4.3.5.2.8 Требования к локальной вычислительной сети

Локальная вычислительная сеть должна строиться на базе коммутаторов второго и третьего уровней с интерфейсами Ethernet поддерживающими режим полный дуплекс при скорости обмена 100/1000 BaseT.

Подключения сетевого оборудования к вычислительным серверам должны быть резервированы.

Активное сетевое оборудование системы-112 должно использовать:

отказоустойчивую архитектуру;

технологии коммутации интерфейсов Ethernet при построении ЛВС;

оборудование и решения, обеспечивающие масштабируемость ЛВС без необходимости замены оборудования.

ЛВС функциональных объектов системы-112 должна соответствовать следующим требованиям:

построение с применением технологии VLAN;

использование протокола IPv4;

класс обслуживания – real-time;

доступность каналов связи – 99,995 % в месяц;

процент потерянных пакетов (PE-to-PE) в среднем в месяц – не более 0,25%;

односторонние сетевые задержки на наземных каналах (PE-to-PE) в среднем за месяц – не более 75 мсек;

колебания сетевой задержки на наземных каналах (PE-to-PE) / джиттер – не более 50 мсек.

Подключение функциональных объектов системы-112 к РИВП должно осуществляться по каналам связи с пропускной способностью из расчета не ниже 512 Кбит/с на одно АРМ системы-112 с учетом требований технических решений и СПО к каналам связи.

Активное сетевое оборудование системы-112, используемое в качестве центрального, реализующего функции основной транспортной магистрали, должно иметь модульную архитектуру и поддерживать отказоустойчивые конфигурации за счет:

дублирования блоков питания;

дублирования модулей управления и маршрутизирующих модулей;

поддержки технологий резервирования каналов.

ЛВС должна иметь сегмент, обеспечивающий высокоскоростной обмен данными между вычислительными серверами, системой хранения данных и системой резервного копирования.

Каждый элемент ЛВС должен быть выполнен в конструктиве для установки в стандартный 19" телекоммуникационный шкаф.

Проектные решения по ЛВС должна приниматься с учетом использования современных средств защиты информации и возможностью интеграции в нее других средств и систем защиты информации.

Проектными решениями должна предусматриваться возможность автоматического переключения с основных на резервные каналы передачи данных.

Оборудование ЛВС должно иметь документацию на русском языке и гарантийную поддержку производителя.

4.3.5.2.9 Требования к структурированной кабельной системе

Структурированная кабельная система (СКС) должна обеспечить коммутацию оборудования комплекса технических средств.

Проектные решения по СКС должны строиться на использовании медного неэкранированного витого парного (UTP) и волоконно-оптического (FO) кабеля.

В проводном сегменте СКС должен использоваться UTP-кабель не ниже 5-й категории.

СКС должна иметь возможность увеличения количества соединительных портов не менее чем на 20%.

Коммутационная зона должна располагаться в непосредственной близости от главного кросса.

4.3.5.2.10 Требования к системе гарантированного электроснабжения

Электроснабжение ЦОВ-АЦ, РЦОВ и РИВП должно соответствовать требованиям особой группы первой категории по классификации ПУЭ (Правила устройства электроустановок). В качестве дополнительных независимых источников должны применяться ИБП и ДГУ.

При построении системы энергоснабжения допускается использование шинной технологии.

Источники бесперебойного питания должны обеспечивать функционирование комплекса технических средств системы-112 при полном или частичном отключении внешних источников электропитания на время, необходимое для запуска ДГУ.

Уровень суммарных гармонических искажений на входе системы при полной нагрузке не должен превышать 5%.

Аккумуляторные батареи должны быть рассчитаны на срок эксплуатации не менее 3 лет.

Должна обеспечиваться возможность выполнения профилактических и ремонтных работ без отключения нагрузки.

Архитектура системы должна обеспечивать быстрое масштабирование мощности и уровня эксплуатационной готовности, без вывода всего комплекса из режима основной работы.

Система гарантированного электроснабжения должна состоять, как минимум, из следующих компонентов:

распределительный щит СГЭ;

источник бесперебойного питания с аккумуляторной батареей;

кабельные линии подключения ИБП к вводному и распределительному щитам и АКБ;

распределительная сеть: магистраль от главного распределительного щита до вводного щита СГЭ и кабельных линий от распределительного щита СГЭ до групповых щитов потребителей;

групповые щиты.

Проектные решения по СГЭ должны приниматься исходя из максимальной конфигурации КТС без необходимости проведения каких-либо доработок системы. СГЭ должна иметь запас мощности не менее 25%.

4.3.5.2.11 Требования к автоматизированным рабочим местам

АРМ должны обеспечить пользователям обработку данных и автоматизацию управленческих функций в области функциональности системы-112, а также автоматизацию выполнения вспомогательных (обеспечивающих) функций.

АРМ операторов (диспетчеров) системы-112, как минимум, должны включать:

персональный компьютер;

два монитора;

источник бесперебойного питания;

телефонный аппарат или гарнитуру;

возможность подключения к сети и сетевому принтеру;

общесистемное программное обеспечение;

специальное программное обеспечение системы-112.

АРМ системных администраторов КТС, как минимум, должны включать:

персональный компьютер;

монитор;

источник бесперебойного питания;

телефонный аппарат или гарнитуру;

возможность подключения к сети и сетевому принтеру;

общесистемное программное обеспечение;

программное обеспечение мониторинга состояния оборудования КТС.

4.3.5.2.12 Требования к комплексу средств защиты информации

Комплекс средств защиты информации системы-112 должен включать:

сертифицированные средства защиты информации в соответствии с классами защищенности, выбранными для реализации системы-112;

общесистемное, специальное программное обеспечение, включающее штатные средства (встроенные функции) защиты информации от НСД, либо имеющее соответствующие сертифицированные дополнения в виде средств защиты информации от НСД;

средства обеспечения:

конфиденциальности, целостности, достоверности и доступности информации;

защиты информации от утечки по техническим каналам связи и доступа;

сопряжения средств защиты информации с используемым в создаваемых информационных системах общим и специальным программным обеспечением.

Средства межсетевого экранирования должны обеспечивать контролируемое подключение системы-112 к общедоступным сетям и развязку отдельных сетевых сегментов в рамках самой системы-112. Средства экранирования должны обеспечивать управление информационными

потоками между сегментами системы-112 и контроль информационных потоков, направленных, как в систему-112, так и из нее.

4.3.6 Требования к метрологическому обеспечению

Требования к метрологическому обеспечению:

отсутствие ошибки округления при расчетах:

отсутствие ошибок округления и отсутствие накопление ошибок расчетов при пересчетах по процентному содержанию.

Дополнительных требований к метрологическому обеспечению не предъявляется.

4.3.7 Требования к организационному обеспечению

Организационное обеспечение системы-112 должно быть достаточным для эффективного выполнения персоналом возложенных на него обязанностей по эксплуатации системы-112.

Организационное обеспечение должно включать инструкции по каждому виду деятельности и точное определение выполняемых функций для каждой штатной единицы персонала системы.

Должностные инструкции сотрудников, деятельность которых связана с функционированием системы-112, должны быть дополнены функциями, связанными с эксплуатацией данной системы.

4.3.7.1 Организационное обеспечение процесса создания системы-112

Для повышения качества управления проектом создания системы-112 могут применяться средства автоматизации операций календарно-ресурсного планирования и управления документами.

4.3.7.2 Требования к защите от ошибочных действий персонала

Система должна обеспечивать защиту от ошибочных действий персонала и исключать возможность нарушения функционирования от неправильных действий персонала, обеспечивая стопроцентное сохранение данных системы при любых действиях персонала и одиночных отказах программно-технических средств.

Должны быть определены должностные лица, ответственные за:

выполнение основных функций системы-112;

администрирование системы-112;

обеспечение информационной безопасности системы-112;

управление работой персонала по обслуживанию системы-112.

4.3.8 Требования к методическому обеспечению

Методическое обеспечение системы-112 должно быть направлено на обеспечение персонала инструкциями по выполнению действий, совершаемых ими в соответствии со своими должностными обязанностями в процессе работы с системой-112.

При разработке методического обеспечения системы-112 должны быть учтены нормативно-правовые акты, регулирующие автоматизируемые системой-112 процессы, в том числе нормативно-правовые акты Российской Федерации и Субъекта РФ, ведомственные приказы и регламенты.

Методическое обеспечение системы-112 должно включать следующие виды документов:

проекты основных нормативных правовых документов;

учебные и методические материалы;

технологические инструкции.

Перечень основных нормативных правовых документов и их проекты должны быть разработаны Исполнителем и согласованы с Заказчиком на стадии ввода в действие системы-112.

Учебные и методические материалы должны быть разработаны Исполнителем на стадии ввода в действие системы-112. Учебные и методические материалы предназначены для обучения сотрудников работе с системой-112 или отдельными ее компонентами. Учебные и методические материалы должны быть разработаны для каждой функциональной роли всех подсистем системы-112.

Методическое обеспечение системы-112 в части разработки детальных пошаговых инструкций по выполнению административных процессов с использованием компонент системы-112 разрабатывается Исполнителем и утверждается Заказчиком. Технологические инструкции должны представлять собой детальное пошаговое описание выполнения административных процессов с использованием компонентов системы-112. Данные инструкции должны содержать конкретные действия, выполняемые каждым сотрудником (ролью), участвующим в процессе. Технологические инструкции должны разрабатываться для каждой из подсистем системы-112 в соответствии с их функциональными и архитектурными особенностями. Перечни и инструкции для каждой из подсистем должны быть разработаны на этапе разработки рабочей документации системы-112.

4.3.9 Специальные требования

Проектирование системы-112 должно проводиться с использованием опыта создания и эксплуатации аналогичных систем, эксплуатируемых или находящихся на стадии внедрения в странах Европейского Союза, субъектах Российской Федерации.

В рамках работ по настоящему техническому заданию Исполнитель должен:

разработать технический проект системы-112 на территории Субъекта РФ.

развернуть макет системы-112.

На момент сдачи технический проект системы-112 должен удовлетворять требованиям действующего законодательства.

РИВП, обеспечивающий функциональность системы-112, должен предоставлять соответствующие инфокоммуникационные услуги, отвечающие требованиям, указанным в разделах 2 и 4 настоящего технического задания и соответствующие Регламенту предоставления инфокоммуникационной услуги, обеспечивающей функциональность системы-112, на базе распределенной информационно-вычислительной платформы, разрабатываемому на стадии технического проектирования. При этом использование ресурсов РИВП должно строиться с применением технологий виртуализации.

Макет системы-112 должен обеспечить проведение анализа возможностей эффективного функционирования системы-112 в соответствии с решениями, заложенными в техническом проекте. В состав макета должны входить АРМ операторов ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС выбранного муниципального района, диспетчеров сопрягаемых ДДС административного центра Субъекта РФ и выбранного муниципального района. Территориально макет системы-112 должен развертываться на базе определенного Заказчиком муниципального района.

Указанный макет должен позволить оценить выполнение требований к системе-112, описанных в настоящем Техническом задании, в том числе:

реализацию комплексной поддержки обработки вызовов, возможности управления силами и средствами со стороны операторов ЦОВ-АЦ, РЦОВ, ЦОВ-ЕДДС, диспетчеров ДДС в соответствии с концепцией системы-112;

координацию действий при происшествиях и несчастных случаях;

интеграцию поддержки действий персонала системы-112 в рамках единого информационного и технологического подхода;

идентификацию ЧС или происшествия с помощью системы иерархических справочников;

поддержку принятия решения при организации комплексного реагирования различных ведомств с помощью базы планов действий;

контроль реагирования ДДС со стороны ЦОВ-АЦ, РЦОВ и ЦОВ-ЕДДС с помощью планов действий;

формирование статистической, аналитической и оперативной отчётности о событиях, ситуациях и действиях персонала объектов системы-112 по различным информационным срезам.

В рамках реализации макета должны быть выполнены следующие работы:

доработка и настройка интерфейсов пользователя прикладного программного обеспечения;

подготовка и загрузка фрагментов баз данных по объектам;

настройка интерфейса с системой видеонаблюдения;

моделирование звонков и сигналов от оборудования пожарной безопасности, контроля доступа и другого оборудования систем безопасности;

моделирование подвижных объектов;

ввод фрагментов исходных данных по объектам, силам и средствам, штатному расписанию, планам реагирования и т.д.;

подготовка, настройка и тестирование внутренних интерфейсов системы;

установка и тестирование оборудования, общего программного обеспечения, системы управления базами данных, прикладного программного обеспечения;

подготовка инструкции оператору по работе с макетом;

консультации специалистам по работе с макетом системы-112.

Указанные АРМ макета должны подключаться к РИВП в соответствии с техническими условиями, разработанными на стадии проектирования.

Все предоставляемые исполнителем услуги, необходимые для обеспечения функционирования макета системы-112, предоставляются на срок до выполнения обязательств по контракту.

5 Состав и содержание работ по созданию системы-112

5.1 Перечень этапов работ и документов, предъявляемых по окончании работ

При разработке технического проекта системы-112 для обеспечения условий ее функционирования, при которых гарантируется соответствие предъявленным настоящим требованиям, должны быть реализованы этапы, перечисленные в таблице 1.

Таблица 1. Этапы разработки технического проекта системы-112

Номер этапа работ	Требования к работам и содержанию отчетной документации и материалов
1. Разработка технического проекта на создание системы-112	В состав документов технического проекта на создание системы-112 должны входить[19]: Ведомость технического проекта; Пояснительная записка к техническому проекту; Технический проект подсистемы информационной безопасности; Схема функциональной структуры; Описание автоматизированных функций; Схема организационной структуры; Схема структурная комплекса технических средств; Описание комплекса технических средств; Описание информационного обеспечения; Описание программного обеспечения; Описание алгоритма; Ведомость оборудования и материалов; Проектная оценка надежности системы; Схема организации связи; Регламент предоставления инфокоммуникационной услуги, обеспечивающей функциональность системы-112, на базе распределенной информационно-вычислительной платформы; Рекомендации по интеграции системы-112 с выявленными смежными и внешними автоматизированными системами; Частное техническое задание на макет системы-112; Программа и методика испытаний макета системы-112. Акт выполненных работ по первому этапу.
2. Развертывание макета системы-112	Перечень муниципальных образований и перечень объектов автоматизации системы-112, на базе которых необходимо развернуть макет системы-112, согласованный с Заказчиком. Развертывание макетов системы-112 должно осуществляться на основании частного технического задания, разработанного Исполнителем и включать поставку, монтаж (установку) и настройку оборудования (телекоммуникационного оборудования и АРМ), обеспечивающего подключение АРМ системы-112 к РИВП (комплект отгрузочных документов на поставленные товары, акт

[19] представлен минимально необходимый перечень документов, полный перечень определяется Заказчиком

Номер этапа работ	Требования к работам и содержанию отчетной документации и материалов
	выполненных работ), предоставление в пользование специального программного обеспечения на АРМ пользователей (операторов ЦОВ-ЕДДС, диспетчеров ДДС), включая установку, настройку и техническую поддержку (акт выполненных работ), обучение пользователей по работе с системой-112 (акт выполненных работ), подключение АРМ системы-112 к РИВП (акт выполненных работ). Проведение испытаний макета (протокол проведения испытаний, акт проведения испытаний) Акт выполненных работ по второму этапу. Акт выполненных работ по Государственному контракту.

6 Порядок контроля и приемки работ

6.1 Общие требования к приемке работ

Выполненные работы (оказанные услуги) должны приниматься Заказчиком по акту сдачи-приемки исполнения обязательств по этапу Государственного контракта. При приемке, в том числе, должно проверяться соответствие объема и качества выполненных работ (оказанных услуг) требованиям Государственного контракта.

Перед представлением государственному заказчику отчетные материалы по работе должны быть согласованы с МЧС России: Технический проект системы-112 должен иметь согласование межведомственной рабочей группы Субъекта РФ, заключение ФГБУ ВНИИ ГОЧС (ФЦ) о соответствии требованиям существующих нормативных и типовых документов и согласование секции по системе-112 при Межведомственном координационном научном совете при Правительственной комиссии по предупреждению и ликвидации чрезвычайных ситуаций и обеспечению пожарной безопасности.

В течение 10 (десяти) дней с момента предоставления подготовленной и подписанной Исполнителем отчетной документации, Приемочная комиссия Государственного заказчика должна проверить качество результатов исполнения обязательств по Государственному контракту (по этапу Государственного контракта) на предмет соответствия выполненных работ (оказанных услуг) и представленной отчетной документации требованиям и условиям настоящего Государственного контракта. Для проверки соответствия качества выполненных работ (оказанных услуг) установленным требованиям могут привлекаться независимые эксперты.

Поставленное оборудование (товары), передаются Заказчику вместе с комплектом отгрузочных документов.

При несоответствии результатов работы требованиям технического задания Заказчик направляет Исполнителю перечень замечаний, которые последний обязан устранить в согласованные с Заказчиком сроки и представить доработанную документацию на повторное рассмотрение.

6.2 Требования к испытаниям

Испытания системы-112 должны проводиться в соответствии с нормативными документами, определяющими требования к испытаниям автоматизированных систем.

Апробация функциональных подсистем системы-112 должна проводиться на основе утвержденной «Программы и методики испытаний». При проведении апробации должна быть организована техническая поддержка всех организаций, участвующих в апробации.

Предварительные испытания системы-112 проводятся для определения ее работоспособности и решения вопроса о возможности приемки системы-112 в опытную эксплуатацию.

Предварительные испытания следует выполнять после проведения разработчиком отладки и тестирования поставляемых программных и технических средств и представления им соответствующих документов об их готовности к испытаниям, а также после ознакомления персонала системы-112 с эксплуатационной документацией.

Приемочные испытания системы-112 проводят для определения соответствия системы техническому заданию, оценки качества опытной эксплуатации и решения вопроса о возможности приемки системы-112 в постоянную эксплуатацию.

При проведении испытаний, проверке или аттестации в ней подвергают:

комплекс программных и технических средств;

персонал;

эксплуатационную документацию, регламентирующую деятельность персонала при функционировании системы-112;

систему в целом.

При испытаниях системы-112, прежде всего, проверяют:

качество выполнения комплексом программных и технических средств автоматических функций во всех режимах функционирования системы-112 согласно техническому заданию на создание системы-112 субъекта Российской Федерации и конкурсной документации;

знание персоналом эксплуатационной документации и наличие у него навыков, необходимых для выполнения установленных функций во всех режимах функционирования системы-112;

полноту содержащихся в эксплуатационной документации указаний персоналу по выполнению им функций во всех режимах функционирования системы-112;

количественные и (или) качественные характеристики выполнения автоматических и автоматизированных функций системы-112 в соответствии с техническим заданием;

другие свойства системы-112, которым она должна соответствовать по техническому заданию.

Испытания системы-112 следует проводить на объектах автоматизации. По согласованию между заказчиком и разработчиком предварительные испытания и приемку программных средств системы-112 допускается проводить на технических средствах разработчика при создании условий получения достоверных результатов испытаний.

Допускается последовательное проведение испытаний и сдача частей (компонент, модулей, подсистем) системы-112 в опытную и постоянную эксплуатацию в соответствии с частными техническими заданиями на данные компоненты, модули, подсистемы.

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

Должен быть предусмотрен следующий перечень мероприятий по развертыванию системы-112:

развертывание ЦОВ-АЦ;

развертывание РЦОВ;

развертывание ЦОВ-ЕДДС;

интеграция ДДС в систему-112;

создание телекоммуникационной инфраструктуры системы-112;

обучение преподавательского состава;

обучение персонала системы-112;

обучение персонала взаимодействующих ДДС;

организация взаимодействия между объектами системы-112;

организация взаимодействия с региональным ЦУКС МЧС России и с объектами системы обеспечения вызова оперативных служб по единому номеру «112» соседних субъектов Российской Федерации.

Также должны быть предусмотрены первоначальное подключение к РИВП и последующее наращивание мощностей РИВП соответственно вводу в эксплуатацию функциональных объектов системы-112.

Кроме непосредственного развертывания ПТК системы-112 на объектах автоматизации, необходимо проработать вопросы информационного и иных форм взаимодействия экстренных оперативных служб в рамках системы-112. В том числе, к моменту ввода в опытную эксплуатацию должна быть сформирована нормативно-правовая база, обеспечивающая функционирование системы-112 и взаимодействие экстренных оперативных служб. Исполнители по всем стадиям (этапам) создания системы-112, по требованию Заказчика, должны принимать участие в разработке нормативно-правовой документации, обеспечивающей работу системы-112 и в ее согласовании.

8 Требования к документированию

8.1 Перечень подлежащих разработке комплектов и видов документов

Состав и структура документов, разрабатываемых в рамках данной работы, определены требованиями комплекса стандартов на автоматизированные системы.

8.2 Требования к составу и содержанию документов

В состав отчетной документации по результатам работ должны входить документы, приведенные в разделе 5.1.

Состав и объем разрабатываемой технической документации может быть дополнительно уточнен по согласованию с Заказчиком.

Сроки выполнения работ определяются календарным планом. Сроки выполнения работ могут быть дополнительно уточнены и согласованы в процессе проведения обследования объектов автоматизации.

Документация должна быть оформлена в соответствии с требованиями единой системы конструкторской документации.

Язык отчетных материалов - русский.

Отчетные материалы должны быть представлены на бумажном носителе (на листах формата А4 и А3 в трех экземплярах) и в электронной форме. На титульном листе должно быть помещено наименование отчетного материала, учетные реквизиты, подписи Исполнителя и Соисполнителей, скрепленные печатями.

Отчеты в электронной форме должны быть представлены на оптическом диске, исключающем возможность изменения информации (CD-R, DVD-R, DVD+R). Форматы представления информации - pdf. Представляемые в составе отчетных материалов оптические диски маркируются несмываемыми водой фломастерами или наклейками, не ухудшающими их использование, и помещаются в защитные коробки.

9 Источники разработки

9.1 Основные нормативные и правовые документы, регулирующие создание системы-112

Федеральный закон от 21 декабря 1994 года № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (в ред. ФЗ от 28.10.2002 № 129-ФЗ, от 22.08.2004 № 122-ФЗ, от 04.12.2006 № 206-ФЗ, от 18.12.2006 № 232-ФЗ, от 30.10.2007 № 241-ФЗ, от 30.12.2008 № 309-ФЗ, от 07.05.2009 № 84-ФЗ, от 25.11.2009 № 267-ФЗ, от 19.05.2010 № 91-ФЗ, от 27.07.2010 № 223-ФЗ, от 28.12.2010 № 412-ФЗ, от 29.12.2010 № 442-ФЗ, от 01.04.2012 № 23-ФЗ);

Постановление Правительства Российской Федерации от 31 декабря 2004 года № 894 «Об утверждении перечня экстренных оперативных служб, вызов которых круглосуточно и бесплатно обязан обеспечить оператор связи пользователю услугами связи, и о назначении единого номера вызова экстренных оперативных служб» (в ред. от 06.10.2011);

ГОСТ Р 22.7.01-99 Государственный Стандарт Российской Федерации. Безопасность в чрезвычайных ситуациях. Единая дежурно-диспетчерская служба;

Распоряжение Правительства Российской Федерации от 25 августа 2008 г. № 1240-р «Об утверждении Концепции создания системы-112»;

Указ Президента Российской Федерации от 28 декабря 2010 года № 1632 «О совершенствовании системы обеспечения вызова экстренных оперативных служб на территории Российской Федерации»;

Постановление Правительства Российской Федерации от 21 ноября 2011 года № 958 «О системе обеспечения вызова экстренных оперативных служб по единому номеру «112» (в ред. от 04.09.2012);

Распоряжение Правительства Российской Федерации от 04 мая 2012 года № 716-р «Об утверждении Концепции федеральной целевой программы "Создание системы обеспечения вызова экстренных оперативных служб по единому номеру "112" в Российской Федерации на 2012 - 2017 годы";

Постановление Правительства Российской Федерации от 11 июля 2009 года № 549 «О федеральном сетевом операторе в сфере навигационной деятельности»;

Методические материалы по созданию системы-112 на территории Российской Федерации МЧС России;

нормативные акты, протоколы заседаний администрации и иные документы администрации субъекта Российской Федерации[20].

9.2 Общие документы

Федеральный закон от 21 июля 1997 года № 116-ФЗ «О промышленной безопасности опасных производственных объектов» (в ред. ФЗ от 07.08.2000 г. № 123-ФЗ, от 10.01.2003 г., № 15-ФЗ, от 22.08.2004 г. № 122-ФЗ, от 09.05.2005 г. № 45-ФЗ, от 18.12.2006 г. № 232-ФЗ, от 30.12.2008 г. № 309-ФЗ, от 30.12.2008 г. № 313-ФЗ, от 27.12.2009 г. № 374-ФЗ, от 23.07.2010 г. № 171-ФЗ, от 27.07.2010 г. № 226-ФЗ, от 27.07.2010 г. № 227-ФЗ, от 01.07.2011 г. № 169-ФЗ, от 18.07.2011 г. № 242-ФЗ, от 18.07.2011 г. № 243-ФЗ, от 19.07.2011 г. № 248-ФЗ, от 28.11.2011 г. № 337-ФЗ, от 30.11.2011 г. № 347-ФЗ, от 25.06.2012 г. № 93-ФЗ);

Федеральный Закон от 07 июля 2003 года № 126-ФЗ "О связи" (ред. от 28.07.2012);

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации от 27 июля 2006 года № 152 «О персональных данных» (в ред. Федеральных законов от 25.11.2009 № 266-ФЗ, от 27.12.2009 № 363-ФЗ, от 28.06.2010 № 123-ФЗ, от 27.07.2010 № 204-ФЗ, от 27.07.2010 № 227-ФЗ, от 29.11.2010 № 313-ФЗ, от 23.12.2010 № 359-ФЗ, от 04.06.2011 № 123-ФЗ, от 25.07.2011 № 261-ФЗ);

Указ Президента Российской Федерации от 17 марта 2008 года N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

Постановление Правительства Российской Федерации от 24.03.1997 года № 334 «О порядке сбора и обмена в Российской Федерации информацией в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (в ред. от 22.12.2011);

Постановление Правительства Российской Федерации от 10 ноября 2003 г. № 677 «Об общероссийских классификаторах технико-экономической и социальной информации в социально-экономической области» (в ред. Постановления Правительства Российской Федерации от 04.08.2005 N 493, распоряжения Правительства Российской Федерации от 23.11.2006 № 1615-р, Постановления Правительства Российской Федерации от 08.12.2008 №917, Постановления Правительства Российской Федерации от 02.09.2010 г. № 659);

Постановление Правительства Российской Федерации от 30 декабря 2003 г. № 794 «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций» (в ред. Постановлений Правительства Российской Федерации от 27.05.2005 года № 335, от 03.10.2006 года № 600, от 07.11.2008 года № 821, от 10.03.2009 года № 219, от 16.07.2009 года №

[20] перечислить

577, от 02.09.2010 года № 659, от 08.09.2010 года № 702, от 04.02.2011 года № 48, от 04.02.2011 года № 50, от 31.03.2011 года № 226, от 22.12.2011 года № 1101, от 18.04.2012 года № 340, от 04.09.2012 года № 882, от 22.10.2012 года № 1082, от 01.11.2012 года № 1128, от 19.11.2012 года № 1179);

Постановление Правительства Российской Федерации от 25 мая 2005 года № 328 "Об утверждении правил оказания услуг подвижной связи" (в ред. от 06.10.2011);

Приказ Мининформсвязи России от 17 ноября 2006 года № 142 "Об утверждении и введении в действие Российской системы и плана нумерации" (Зарегистрирован в Минюсте России 08.12. 06 г. № 8572) (в ред. от 15.06.2012);

9.3 Нормативные и правовые документы служб реагирования в чрезвычайных ситуациях

Федеральный закон от 21 декабря 1994 № 68-ФЗ "О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера" (в ред. ФЗ от 28.10.2002 № 129-ФЗ, от 22.08.2004 № 122-ФЗ, от 04.12.2006 № 206-ФЗ, от 18.12.2006 № 232-ФЗ, от 30.10.2007 № 241-ФЗ, от 30.12.2008 № 309-ФЗ, от 07.05.2009 № 84-ФЗ, от 25.11.2009 № 267-ФЗ, от 19.05.2010 № 91-ФЗ, от 27.07.2010 № 223-ФЗ, от 28.12.2010 № 412-ФЗ, от 29.12.2010 № 442-ФЗ, от 01.04.2012 № 23-ФЗ);

Указ Президента Российской Федерации от 28 августа 2003 года № 991 "О совершенствовании единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций" (с изм. и доп. от 11 июля 2004 г.);

Указ Президента Российской Федерации от 11 июля 2004 года № 868 "Вопросы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий" (с изм. и доп. от 21 октября 2005 г., от 13.11.2012 г.);

Постановление Правительства Российской Федерации от 10 мая 1995 года № 457 "О создании государственного унитарного авиационного предприятия Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий" (с изм. и доп. от 22 апреля 1997 г.);

Постановление Правительства Российской Федерации от 3 августа 1996 года № 924 "О силах и средствах Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций" (вместе с "перечнем сил постоянной готовности федерального уровня единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций") (ред. от 23.12.2004, от 23.12.2011);

Постановление Правительства Российской Федерации от 22 февраля 1997 года № 193 "Об уточнении функций Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и Министерства труда и социального развития Российской Федерации" (с изм. и доп. от 15 декабря 1998 г.);

Постановление Правительства Российской Федерации от 4 сентября 2003 года № 547 "О подготовке населения в области защиты от чрезвычайных ситуаций природного и техногенного характера" (с изм. и доп. от 1 февраля 2005 г., от 08.09.2010);

Постановление Правительства Российской Федерации от 30 декабря 2003 года № 794 "О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций" (в ред. Постановлений Правительства Российской Федерации от 27.05.2005 года № 335, от 03.10.2006 года № 600, от 07.11.2008 года № 821, от 10.03.2009 года № 219, от 16.07.2009 года № 577, от 02.09.2010 года № 659, от 08.09.2010 года № 702, от 04.02.2011 года № 48, от 04.02.2011 года № 50, от 31.03.2011 года № 226, от 22.12.2011 года № 1101, от 18.04.2012 года № 340, от 04.09.2012 года № 882, от 22.10.2012 года № 1082, от 01.11.2012 года № 1128, от 19.11.2012 года № 1179);

Постановление Правительства Российской Федерации от 16 мая 2005 года №303 "О разграничении полномочий федеральных органов исполнительной власти в области обеспечения биологической и химической безопасности Российской Федерации" (с изм. и доп. от 23 марта 2006 г., от 01.11.2012);

Постановление Правительства Российской Федерации от 1 декабря 2005 года № 712 "Об утверждении Положения о государственном надзоре в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, осуществляемом Министерством Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий" (в ред. от 22.04.2009);

Постановление Правительства Российской Федерации от 21 мая 2007 года № 304 "О классификации чрезвычайных ситуаций природного и техногенного характера" (в ред. от 17.05.2011);

Постановление Правительства Российской Федерации от 26 ноября 2007 года №804 «Об утверждении Положения о гражданской обороне в Российской Федерации»;

Приказ МЧС России и Росгидромета от 2 августа 1999 года № 416/79 "О взаимодействии МЧС России и Росгидромета в области прогнозирования, предупреждения и ликвидации чрезвычайных ситуаций";

Приказ МЧС России от 28 января 2002 года № 32 "Об утверждении Положения о поисково-спасательной службе Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий";

Приказ МЧС России от 18 марта 2002 года № 116 "Об утверждении Схемы организации управления МЧС России";

Приказ МЧС России от 6 августа 2004 года № 372 "Об утверждении Положения о территориальном органе Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий - органе, специально уполномоченном решать задачи гражданской обороны и задачи по предупреждению и ликвидации чрезвычайных ситуаций по субъекту Российской Федерации" (с изм. и доп. от 24 октября 2006 г., 2 июля, 6 августа 2007 г., 11.01.2012);

Приказ МЧС России от 1 октября 2004 года № 458 "Об утверждении Положения о территориальном органе Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий - региональном центре по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий" (с изм. и доп. от 24 октября 2006 г., 19 февраля 2007 г., 11.01.2012);

Приказ МЧС России от 20 декабря 2004 года № 590 "Об утверждении норм обеспечения территориальных органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий";

Приказ МЧС России от 2 мая 2006 года № 270 "Об утверждении инструкции о порядке приема, регистрации и проверки сообщений о преступлениях и иных происшествиях в органах государственной противопожарной службы министерства российской федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий" (Зарегистрировано в Минюсте России 02.06.2006 №7904) (в ред. от 22.06.2010);

Приказ МЧС России от 29 июня 2006 года № 386 "Об утверждении Административного регламента Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий по исполнению государственной функции по организации информирования населения через средства массовой информации и по иным каналам о прогнозируемых и возникших чрезвычайных ситуациях и пожарах, мерах по обеспечению безопасности населения и территорий, приемах и способах защиты, а также пропаганде в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности и безопасности людей на водных объектах";

Приказ МЧС России от 24 июля 2006 года № 418 "Об утверждении Регламента Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий" (в ред. от 18.04.2012);

Приказ МЧС России от 05 декабря 2006 года № 712 "О квалификационных требованиях к профессиональным знаниям и навыкам, необходимым для исполнения должностных

обязанностей федеральными государственными гражданскими служащими центрального аппарата и территориальных органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий" (Зарегистрировано в Минюсте России 28.12.2006 №8705);

Приказ МЧС России от 16 марта 2007 года № 139 "Об утверждении Инструкции о порядке согласования нормативных документов, которые принимаются федеральными органами исполнительной власти и устанавливают или должны устанавливать требования пожарной безопасности";

Приказ МЧС России от 26 июля 2007 года № 403 "Об утверждении Порядка работы комиссий Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и его территориальных органов по соблюдению требований к служебному поведению федеральных государственных гражданских служащих и урегулированию конфликта интересов";

Постановление Федеральной службы государственной статистики от 28 января 2005 года № 5 "Об утверждении статистического инструментария для организации МЧС России статистического наблюдения за деятельностью в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности и безопасности людей на водных объектах, в том числе в области социальной защиты граждан".

9.4 Нормативные и правовые документы службы пожарной охраны

Федеральный закон от 21 декабря 1994 года № 69-ФЗ "О пожарной безопасности" (с изм. и доп. от 22.08.1995 года № 151, от 18.04.1996 года № 32, от 24.01.1998 года № 13, от 07.11.2000 года № 135, от 06.08.2001 года № 110, от 30.12.2001 года № 196, от 25.07.2002 года № 116, от 10.01.2003 года № 15, от 10.05.2004 года № 38, от 29.06.2004 года № 58, от 22.08.2004 года № 122, от 01.04.2005 года № 27, от 09.05.2005 года № 45, от 02.02.2006 года № 19, от 25.10.2006 года № 172, от 04.12.2006 года № 201, от 18.12.2006 года № 232, от 26.04.2007 года № 63, от 18.10.2007 года № 230, от 22.07.2008 года № 137, от 14.03.2009 года № 32, от 19.07.2009 года № 198, от 09.11.2009 года № 247, от 25.11.2009 года № 267, от 23.07.2010 года № 173, от 28.09.2010 года № 243, от 29.12.2010 года № 442, от 18.07.2011 года № 242, от 18.07.2011 года № 243, от 19.07.2011 года № 248, от 08.11.2011 года № 309, от 30.11.2011 года № 345);

Федеральный закон от 25 июля 2002 № 116-ФЗ "О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с совершенствованием государственного управления в области пожарной безопасности" (с изм. и доп. от 27.12.2002 года № 184, от 30.06.2003 года № 86, от 20.08.2004 года № 113, от 22.08.2004 года № 122, от 29.12.2004 года № 189, от 04.12.2006 года № 201, от 24.07.2009 года № 213, от 28.12.2010 года № 390, от 07.02.2011 года № 3, от 29.11.2004 года № 141, от 18.07.2011 года № 242);

Указ Президента Российской Федерации от 9 ноября 2001 года №1309 "О совершенствовании государственного управления в области пожарной безопасности" (с изм. и доп. от 8 мая 2005 г., от 27.10.2011 г.);

Постановление Правительства Российской Федерации от 12 февраля 2001 года № 103 "О территориальных подразделениях Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий" (с изм. и доп. от 8 августа 2003 г.);

Постановление Правительства Российской Федерации от 20 июня 2005 года № 385 "О федеральной противопожарной службе" (в ред. от 29.12.2009 года № 1107, от 20.06.2011 года № 484);

Положение об экспертном совете управления государственного пожарного надзора МЧС России (утв. Главным государственным инспектором Российской Федерации по пожарному надзору 8 декабря 2004 г.);

Нормы пожарной безопасности НПБ 204-99 "Порядок создания территориальных подразделений государственной противопожарной службы на основе договоров с органами государственной власти субъектов Российской Федерации, органами местного самоуправления" (с изм. и доп. от 27 декабря 2002 г., 30 июня 2003 г., 20, 22 августа, 29 ноября, 29 декабря 2004 г., 4 декабря 2006 г.);

«Методические рекомендации по действиям подразделений федеральной противопожарной службы при тушении пожаров и проведении аварийно-спасательных работ» от 22 июня 2010 года № 5427-5-1-2.

9.5 Нормативные и правовые документы службы полиции

Федеральный закон "О полиции" от 2 февраля 2011 года № 3-ФЗ (с изм. и доп. от 01.07.2011 года № 169, от 01.07.2011 года № 170, от 19.07.2011 года № 247, от 21.11.2011 года № 329, от 30.11.2011 года № 340, от 30.11.2011 года № 342, от 03.12.2011 года № 389, от 06.12.2011 года № 410, от 25.06.2012 года № 88);

Указ Президента Российской Федерации от 12 февраля 1993 года № 209 "О милиции общественной безопасности (местной милиции) в Российской Федерации" (с изм. и доп. от 2 декабря 1998 г.);

Постановление Правительства Российской Федерации от 7 декабря 2000 года № 926 "О подразделениях милиции общественной безопасности" (с изм. и доп. от 26 июля 2001 г., 10 августа 2005 г., 22 февраля, 29 мая 2006 г.);

Приказ МВД России от 20 ноября 1992 года № 420 "Об утверждении Временной инструкции по организации работы внештатных сотрудников милиции";

Приказ МВД России от 18 января 1993 года № 17 "О мерах по совершенствованию организации патрульно-постовой службы милиции";

Приказ МВД России от 13 апреля 1993 года № 166 "О совершенствовании организации охраны общественного порядка и обеспечения общественной безопасности" (с изм. и доп. от 17 июля 1996 г., 10 марта 1999 г., 22 декабря 2000 г., 25 августа 2003г.);

Приказ МВД России от 19 марта 1997 года № 162 "О дополнительных мерах по совершенствованию деятельности отрядов милиции особого назначения органов внутренних дел Российской Федерации" (с изм. и доп. от 22 декабря 2000 г., 7 марта 2001 г., 11 мая 2006 г.);

Приказ МВД России от 22 июня 1999 года № 456 "О мерах по совершенствованию деятельности милиции общественной безопасности по борьбе с правонарушениями в сфере потребительского рынка товаров и услуг";

Приказ МВД России от 31 декабря 1999 года № 1105 "О мерах по усилению контроля органами внутренних дел за частной детективной и охранной деятельностью" (в ред. от 30.08.2011);

Приказ МВД России от 14 июня 2000 года № 642 "Об утверждении Норм положенности организационной, криминалистической, специальной техники и средств связи для подразделений дознания милиции общественной безопасности органов внутренних дел Российской Федерации";

Приказ МВД России от 16 сентября 2002 года № 900 "О мерах по совершенствованию деятельности участковых уполномоченных милиции" (с изм. и доп. от 3 мая 2003 г., 30 марта 2006 г., 12 апреля 2007 г.);

Приказ МВД России от 4 мая 2010 года № 333 «Об утверждении «Инструкции о порядке приема, регистрации и разрешения в органах внутренних дел Российской Федерации заявлений, сообщений и иной информации о происшествиях» (в ред. от 17.05.2011).

9.6 Нормативные и правовые документы скорой медицинской помощи

Основы законодательства Российской Федерации об охране здоровья граждан от 22 июля 1993 года № 5487-1 (с изм. и доп. от 02.03.1998 года № 30, от 20.12.1999 года № 214, от 02.12.2000 года № 139, от 10.01.2003 года № 15, от 27.02.2003 года № 29, от 30.06.2003 года № 86, от 29.06.2004 года № 58, от 29.12.2004 года № 122, от 01.12.2004 года № 151, от 07.03.2005 года № 15, от 21.12.2005 года № 170, от 31.12.2005 года № 199, от 02.02.2006 года № 23, от 18.10.2007 года № 258, от 24.07.2007 года № 214, от 18.10.2007 года № 230, от 23.07.2008 года № 160, от 08.11.2008 года № 203, от 25.12.2008 года № 281, от 30.12.2008 года № 309, от 24.07.2009 года № 213, от 25.11.2009 года № 267, от 27.12.2009 года № 365, от 27.07.2010 года № 192, от 28.09.2010 года № 243, от 18.07.2011 года № 242, от 07.12.2011 года № 420);

Постановление Правительства Российской Федерации от 31 декабря 2005 года № 871 "Об обеспечении в 2006 году машинами скорой медицинской помощи и реанимобилями учреждений скорой медицинской помощи и санитарной авиации";

Приказ Минздрава СССР от 20 мая 1988 года № 404 "О мерах по дальнейшему совершенствованию скорой медицинской помощи населению" (с изм. и доп. от 15 декабря 1988 г., 26 марта 1999 г.);

Приказ Минздрава России от 25 января 1999 года № 25 "О мерах по улучшению медицинской помощи больным с нарушениями мозгового кровообращения";

Приказ Минздрава России от 26 марта 1999 года № 100 "О совершенствовании организации скорой медицинской помощи населению Российской Федерации" (с изм. и доп. от 16 ноября 2004 г., 10 июня 2010 г.);

Приказ Минздрава России от 14 августа 2002 года № 265 "Об организационно-методическом отделе станции скорой медицинской помощи";

Приказ Минздрава России от 14 октября 2002 года № 313 "Об утверждении отраслевого стандарта "Салоны автомобилей скорой медицинской помощи и их оснащение. Общие технические требования"";

Приказ Минздрава России от 11 марта 2003 года № 93 "Об отраслевой программе "Скорая медицинская помощь";

Приказ Минздравсоцразвития России от 01 ноября 2004 года № 179 "Об утверждении порядка оказания скорой медицинской помощи" (в ред. от 30.01.2012);

Приказ Минздравсоцразвития России от 13 октября 2005 года № 633 "Об организации медицинской помощи";

Приказ Минздравсоцразвития России от 10 мая 2007 года № 323 "Об утверждении Порядка организации работ (услуг), выполняемых при осуществлении доврачебной, амбулаторно-поликлинической (в том числе первичной медико-санитарной помощи, медицинской помощи женщинам в период беременности, во время и после родов, специализированной медицинской помощи), стационарной (в том числе первичной медико-санитарной помощи, медицинской помощи женщинам в период беременности, во время и после родов, специализированной медицинской помощи), скорой и скорой специализированной (санитарно-авиационной), высокотехнологичной, санаторно-курортной медицинской помощи" (в ред. от 09.09.2009);

Приказ Минздравсоцразвития России от 2 декабря 2009 года № 942, утверждающий «Статистический инструментарий станций (отделений), больницы скорой медицинской помощи»;

Письмо Федеральной службы по надзору в сфере здравоохранения и социального развития от 17 июня 2005 года № 01И-267/05 "Об автомобилях скорой медицинской помощи".

9.7 Нормативные и правовые документы службы «Антитеррор»

Федеральный закон от 31 марта 1999 года № 69-ФЗ "О газоснабжении в Российской Федерации" (с изм. и доп. от 22 августа 2004 г., 23 декабря 2005г., 2 февраля, 18 декабря 2006 г., 26 июня 2007 г., 7 ноября 2011 г.).

Указ Президента Российской Федерации от 15 февраля 2006 года № 116 "О мерах по противодействию терроризму" (в ред. от 02.09.2012);

Соглашение между Правительством Российской Федерации и Содружеством Независимых Государств об условиях пребывания на территории Российской Федерации Антитеррористического центра государств - участников Содружества Независимых Государств (Москва, 21 октября 2003 года, с изм. и доп. от 9 июня 2005 года);

Регламент Антитеррористической комиссии в субъекте Российской Федерации (утв. Национальным антитеррористическим комитетом 7 июля 2006 года);

Положение об Антитеррористической комиссии в субъекте Российской Федерации (утв. Национальным антитеррористическим комитетом 7 июля 2006 года);

Приказ ФСБ России от 16.05.2006 года № 205 "Об утверждении инструкции по организации в органах Федеральной Службы Безопасности приема, регистрации и проверки сообщений о преступлениях и иной информации о преступлениях и событиях, угрожающих личной и общественной безопасности" (зарегистрирован в Минюсте РФ 09.10.2006 года №8364).

9.8 Нормы и стандарты

ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на 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 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Стадии создания;

ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы»;

ГОСТ 12.1.00-89 «Техническое задание на создание автоматизированной системы»;

ГОСТ 34.603-92. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем;

ГОСТ 50571.20-2000. Электроустановки зданий;

РД 50 34.698-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Методические указания. Требования к содержанию документов;

ГОСТ 12.1.004-76 ССБТ «Система стандартов безопасности труда. Пожарная безопасность. Общие требования»;

ГОСТ 12.1.030-81 ССБТ «Система стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление» (в ред. от 01.03.1987);

ГОСТ 12.2.003-91 ССБТ «Оборудование производственное. Общие требования безопасности при обслуживании системы в процессе эксплуатации»;

ГОСТ 12.2.007.0-75 ССБТ «Изделия электротехнические. Общие требования безопасности» (в ред. от 01.06.1988);

ГОСТ 12.2.007.13-2000 ССБТ «Лампы электрические. Требования безопасности»;

ГОСТ 12.4.124-83 ССБТ «Средства защиты от статического электричества. Общие технические требования»;

ГОСТ 27.002-89 «Надежность в технике. Основные понятия, термины и определения»;

ГОСТ 27.301-95 «Надежность в технике. Расчет надежности. Основные положения».

ГОСТ 45.63-96 «Обеспечение надежности средств электросвязи. Основные положения»;

ГОСТ 15150-69 «Машины, приборы и другие технические изделия исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды»;

ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение»;

ГОСТ 21958-76 «Система «Человек-машина». Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования»;

ГОСТ 25861-83 «Машины вычислительные и системы обработки данных. Требования по электрической и механической безопасности и методы испытаний»;

ГОСТ Р 51322.1-99 (МЭК 60884-1-94) «Соединители электрические штепсельные бытового и аналогичного назначения. Часть 1. Общие требования и методы испытаний» (ГОСТ Р 51322.1-2011 (МЭК 60884-1:2006));

«Требования о защите информации, содержащейся в информационных системах общего пользования», утверждены Приказом ФСБ/ФСТЭК №416/489 от 31.08.2010 г.;

ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;

ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

ГОСТ Р 54620-2011 «Глобальная навигационная спутниковая система. СИСТЕМА ЭКСТРЕННОГО РЕАГИРОВАНИЯ ПРИ АВАРИЯХ. Автомобильная система вызова экстренных оперативных служб. Общие технические требования»;

ГОСТ Р 54619-2011 «Глобальная навигационная спутниковая система. СИСТЕМА ЭКСТРЕННОГО РЕАГИРОВАНИЯ ПРИ АВАРИЯХ. Протокол обмена данными автомобильной

системы вызова экстренных оперативных служб с инфраструктурой системы экстренного реагирования при авариях»;

ГОСТ Р 54721-2011 «Глобальная навигационная спутниковая система. СИСТЕМА ЭКСТРЕННОГО РЕАГИРОВАНИЯ ПРИ АВАРИЯХ. Общий порядок оказания системой базовой услуги»;

«Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», (утверждено Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119);

Руководящий документ Гостехкомиссии России (ФСТЭК России) «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации» (1992 г.);

Руководящий документ Гостехкомиссии России (ФСТЭК России) «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (1992 г.);

Руководящий документ Гостехкомиссии России (ФСТЭК России) «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (1997 г.);

Руководящий документ Гостехкомиссии России (ФСТЭК России) «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (1997 г.);

«Положение о сертификации средств защиты информации по требованиям безопасности информации». Приказ Председателя Гостехкомиссии России от 27.10.1995 г. №199. Зарегистрировано Госстандартом России в Государственном реестре 20.03.1995 г. (Свидетельство №РОСС 1Ш.0001.01БИОС MS Windows SPR);

Руководящий документ Гостехкомиссии России (ФСТЭК России). «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» от 30 марта 1992 г.;

Руководящий документ Гостехкомиссии России (ФСТЭК России). «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», 1992 г.;

Руководящий документ Гостехкомиссии России (ФСТЭК России). «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;

Выписка из «Требований к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» (ФСБ России, 2007 г.);

«Порядок проведения классификации информационных систем персональных данных» (утвержден Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года № 55/86/20);

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2008 г.);

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2008 г.);

«Положение о методах и способах защиты информации в информационных системах персональных данных» (утверждено Приказом ФСТЭК России);

«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (ФСБ России, 2008 г.);

«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСБ России, 2008 г.);

ГОСТ Р 51275–2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию»;

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

ГОСТ Р 50739-95. «Средства вычислительной техники. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования»;

ГОСТ Р 34.11-94. «Информационная технология. Криптографическая защита информации. Функция хеширования»;

ГОСТ 12.2.032-78. «ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования»;

РД 78.143-92. Руководящий документ. Системы и комплексы охранной сигнализации. Элементы технической укрепленности объектов. Нормы проектирования;

Приложение № 3 к РД 78.143-92 «Группы охраняемых объектов по степени необходимой защиты от преступных посягательств техническими средствами укреплённости и прочими инженерно-техническими мероприятиями по усилению охраны»;

Приложение № 5 к РД 78.143-92 «Основные требования к помещениям охраны»;

РД 78.145-93 «Системы и комплексы охранной пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ»;

Пособие к РД 78.145-93;

РД 78.147-93. Единые требования по технической укрепленности и оборудованию сигнализацией охраняемых объектов;

ГОСТ Р 50009-92. Совместимость технических средств охранной, пожарной и охранно-пожарной сигнализации электромагнитная. Требования, нормы и методы испытаний на помехоустойчивость и индустриальные радиопомехи;

СНиП 2.04.05-91;

Стандарт IEEE 802.3. Спецификация параметров и требований технологии передачи «Ethernet» (Local Area Networks): Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - ETHERNET;

Стандарт IEEE 802.3u. Спецификация параметров и требований технологии передачи «Fast Ethernet» (Local and Metropolitan Area Networks-Supplement - Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units and Repeater for 100Mb/s Operation, Type 100BASE-T);

Стандарт IEEE 802.3z. Спецификация параметров и требований технологии передачи «Gigabit Ethernet» (Media Access Control Parameters, Physical Layers, Repeater and Management Parameters for 1,000 Mb/s Operation, Supplement to Information Technology - Local and Metropolitan Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications);

Стандарт IEEE 802.1p. Спецификация параметров и требований технологии классификации трафика и динамической широковещательной фильтрации (Standard for Local and Metropolitan Area Networks&Supplement to Media Access Control (MAC) Bridges: Traffic Class Expediting and Dynamic Multicast Filtering);

Стандарт IEEE 802.1Q. Спецификация параметров и требований мостовой передачи виртуальных сетей (Standard for Virtual Bridged Local Area Networks);

ГОСТ 14254-96 (МЭК 529-89) (LGA BW 8995.01 / DIN EN 60529-2000);

СН-512-78. Технические требования к зданиям и помещениям для установки средств вычислительной техники (ред. от 24.02.2000);

Правила устройства электроустановок;

ГОСТ Р 50571.22-2000 (МЭК 60364-7-707-84) «Электроустановки зданий. Часть 7. Требования к специальным электроустановкам. Раздел 707. Заземление оборудования обработки информации»

Инструкция по устройству сетей заземления и зануления в электроустановках;

ГОСТ 12.1.004-91 «ССБТ. Пожарная безопасность. Общие требования».

Нормы пожарной безопасности НПБ 110-99 (ред. от 01.08.2001);

СНиП 2.04.09-84. Пожарная автоматика зданий и сооружений (с изм. и доп. от 21.02.1997);

Правила устройства и безопасной эксплуатации сосудов, работающих под давлением ПБ10-115-96;

ISO/IEC 11801:2002 (E). Международный стандарт. Информационные технологии - структурированные кабельные системы для помещений заказчика;

ВНП-001-95. Ведомственные нормы проектирования. Здания учреждений;

СанПиН 2.2.2/2.4.1340-03 (с изм. и доп. от 25.04.2007, 30.04.2010, 03.09.2010);

СанПИН 2.2.4.1294-03 «Гигиенические требования к аэроионному составу воздуха производственных и общественных помещений»;

Приказ Минсвязи РФ от 08.08.2001 N 183 (ред. от 25.02.2004) "О Системе сертификации "Связь";

РД 45.120-2000 «Нормы технологического проектирования. Городские и сельские телефонные сети»;

ГОСТ 2.105-95 «ЕСКД. Общие требования к текстовым документам», ГОСТ 2.106-96 «ЕСКД. Текстовые документы».

Приложение 1

Характеристика территории Субъекта РФ и объектов

Численность населения в муниципальных образованиях Субъекта РФ

Муниципальные районы и городские и сельские округа	Численность населения, человек		
	всего	в том числе:	
		городское	сельское
Всего по Субъекту РФ			
Муниципальные районы:			
Городские округа:			
Сельские округа:			

Информация о региональном ЦУКС МЧС России

№ п/п	Наименование	Адрес

Информация о ЕДДС в Субъекте РФ

№ п/п	Наименование ЕДДС	Вышестоящая организация	Муниципальное образование (перечень МО)	Адрес ЕДДС	Перечень подчиненных ДДС

Информация о ДДС в Субъекте РФ

№ п/п	Наименование ДДС	Вышестоящая организация	Муниципальное образование (перечень МО)	Адрес ДДС

Приложение 2

Сведения об условиях эксплуатации функциональных объектов системы-112

Информация о помещениях объекта автоматизации

№ п/п	Наименование объекта автоматизации	Общая площадь помещения	Площадь помещений под рабочие места операторов	Площадь помещений под вычислительное и коммуникационное оборудование	Наличие систем кондиционирования воздуха в помещениях под оборудование	Наличие резервных линий электропитания

Информация о каналах связи объекта автоматизации

№ п/п	Наименование объекта автоматизации	Пропускная способность Интернет-каналов (Кбит/с)	Тип/марка средств информационной защиты Интернет-каналов	Наличие прямых каналов связи

Информация о техническом оснащении объекта автоматизации

№ п/п	Наименование объекта автоматизации	Наличие свободных мест в стоечных шкафах (кол-во U)	Наличие возможности установки стоечного шкафа	Тип/марка средств обеспечения бесперебойного питания	Тип/марка средств сетевой коммутации	Тип/марка цифровых АТС операторов службы

Информация об обслуживающем и оперативном персонале

№ п/п	Наименование объекта автоматизации	Численность обслуживающего персонала (чел.)	Из них операторы службы (чел.)	Из них технический обслуживающий персонал (чел.)	Укомплектованность персоналом (%)

Статистическая информация о количестве обращений

№ п/п	Наименование объекта автоматизации	Количество обращений в сутки (по данным предыдущего календарного года)		
		среднее (шт.)	максимальное (шт.)	ложных и/или несущественных обращений (шт.)