

**Министерство Российской Федерации
по делам гражданской обороны, чрезвычайным ситуациям
и ликвидации последствий стихийных бедствий**



МЕТОДИЧЕСКОЕ ПОСОБИЕ

**по разработке организационных документов по созданию
и развитию аппаратно-программного комплекса
«Безопасный город»**



Москва – 2016

Методическое пособие разработано в целях реализации Концепции построения и развития аппаратно-программного комплекса «Безопасный город» (далее – АПК «Безопасный город»), утвержденной распоряжением Правительства Российской Федерации от 03.12.2014 № 2446-р, и обобщения опыта работы органов государственной власти и местного самоуправления при выполнении всего комплекса мероприятий по созданию и внедрению АПК «Безопасный город» в муниципальных районах и городских округах.

В данном пособии систематизирован практический материал, который необходимо использовать при организации и проведении мероприятий по созданию, внедрению и развитию АПК «Безопасный город».

Методическое пособие разработано коллективом ФГБУ ВНИИ ГОЧС (ФЦ) под общим руководством доктора технических наук, профессора С.А. Качанова.

СОДЕРЖАНИЕ

Содержание	3
Определения	7
Обозначения и сокращения.....	9
Введение.....	12
1. Предложения по интеграции действующих информационно-аналитических, управляющих и других систем в области природно-техногенной и общественной безопасности в аппаратно-программный комплекс «Безопасный город»	14
1.1. Общие положения.....	14
1.2. Перечень функций (задач), ранее созданных и действующих автоматизированных информационно-управляющих систем различной ведомственной принадлежности, интегрируемых в состав АПК «Безопасный город»	31
1.2.1 Место АПК «Безопасный город» в структуре РСЧС	31
1.2.2 Перечень действующих АС различной ведомственной принадлежности, интегрируемых в состав АПК «Безопасный город».....	32
1.2.3 Перечень функций (задач) и назначение подсистем в составе АПК «Безопасный город».....	36
1.3 Требования к категориям и содержанию информации, передаваемой из действующих автоматизированных информационно-управляющих систем в системы АПК «Безопасный город».....	38
1.3.1 Определение перечня категорий передаваемой информации.....	38
1.3.2 Определение требований к содержанию информации, передаваемой от действующих АС в АПК «Безопасный город»	40
1.4 Алгоритм информационного обмена действующих автоматизированных систем с АПК «Безопасный город».....	54

1.4.1	Техническая основа информационного обмена.....	54
1.4.2	Алгоритм информационного обмена	55
1.5	Требования к организации обмена данными между действующими АС различной ведомственной принадлежности на муниципальном и региональном уровне и системами в составе АПК «Безопасный город».	56
2	Предложения по применению действующих информационно-аналитических управляющих и других систем для предупреждения и ликвидации чрезвычайных ситуаций и происшествий, обеспечения правопорядка в составе АПК «Безопасный город»	63
2.1	Анализ действующих и перспективных автоматизированных информационно-управляющих систем различной ведомственной принадлежности на муниципальном и региональном уровне на предмет соответствия их функциональных характеристик требованиям, указанным в Концепции построения и развития АПК «Безопасный город»	63
2.1.1	Исходные данные анализа.....	63
2.1.2	Функциональные подсистемы АПК "Безопасный город"	65
2.1.3	Функциональная схема АПК «Безопасный город».	102
2.1.4	Функциональные задачи организаций, задействованных в информационном обмене в АПК «Безопасный город».....	105
2.2	Анализ возможности и условий сопряжения действующих автоматизированных информационно-управляющих систем различной ведомственной принадлежности на муниципальном и региональном уровне с системами АПК «Безопасный город»	105
2.2.1	Общие положения	105
2.2.2	Требования к Единому стеку открытых протоколов информационного взаимодействия АПК «Безопасный город»	106
2.2.3	Требования к протоколу информационно-технического взаимодействия АПК «Безопасный город»	115

2.2.4	Требования к программным средствам поддержки информационно взаимодействия (интеграционной шине).....	116
2.3	Модель взаимодействия действующих информационно-управляющих систем и систем в составе АПК «Безопасный город».....	1255
2.3.1	Общие положения по взаимодействию	1255
2.3.2	Модель информационного взаимодействия.....	12930
3	Проект архитектуры решений АПК «Безопасный город»	1322
3.1	Требования к архитектуре АПК «Безопасный город».....	1322
3.2	Функциональные сегменты, системы и подсистемы (типовой вариант) АПК «Безопасный город», их функции и технические характеристики, предложения по сопряжению.	1333
3.2.1	Архитектура АПК «Безопасный город»	1333
3.2.2	КСА «Региональная платформа».....	1354
3.2.4	КСА Единый центр оперативного реагирования	1422
3.2.5	КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»	159
3.2.6	КСА функционального блока «Безопасность на транспорте»	177
3.2.7	КСА функционального блока «Экологическая безопасность»	189
3.3	Основные технические требования к параметрам оборудования АПК «Безопасный город».....	201
3.3.1	Требования к надежности	201
3.3.2	Требования безопасности.....	204
3.3.3	Требования к эргономике и технической эстетике	206
3.3.4	Требования к эксплуатации, техническому обслуживанию и ремонту.....	207
3.3.5	Требования по сохранности информации при авариях	2088
3.3.6	Требования к защите от влияния внешних воздействий	2099

3.3.7	Требования к патентной чистоте	209
3.3.8	Требования по стандартизации и унификации	209
3.4	Предложения по режимам функционирования, диагностирования и работы АПК «Безопасный город»	212
	ЗАКЛЮЧЕНИЕ	21414
	СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	21616
	СПИСОК НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ	217

ОПРЕДЕЛЕНИЯ

Абонент	Лицо, пользующееся средствами связи и осуществившее передачу информации в Систему
АПК «Безопасный город»	Аппаратно-программный комплекс технических средств «Безопасный город»
Заявитель Злонамеренный вызов	Абонент, обратившийся с сообщением о происшествии Событие, в основе которого лежит заведомо неверная информация
Интерфейс сопряжения (Сопряжение)	Граница взаимодействия разнородных автоматизированных систем, посредством которой они обмениваются информацией.
Карточка	Интерфейс для отображения информации по зарегистрированному событию
Классификатор/ Справочник	Систематизированный перечень наименованных объектов или один объект, которому в соответствие дан уникальный код
Консультация	Оказание пояснительно-информационных услуг Заявителю
Конференция	Телефонный вызов, охватывающий трех и более абонентов
Критически важный объект	Объект, значимость которого определяется органами государственной власти Российской Федерации, ее субъектов или местного самоуправления с целью определения мер по защите интересов государства, юридических и физических лиц от преступных посягательств и предотвращения ущерба, который может быть нанесен природе и обществу, а также от возникновения чрезвычайной ситуации
Ложный вызов	Событие, обработка по которому выявила факт ошибочности вызова
Область ответственности ДДС	Участок территории и/или перечень объектов, на которой конкретная ДДС осуществляет деятельность по предназначению, определенную законодательством РФ и/или уставными документами органа управления или организации, формирующей ДДС
Обращение	Факт сообщения о происшествии в ЕДДС
Обучение	Процесс подготовки, переподготовки и повышения квалификации диспетчеров ЦУКС, ЕДДС и ДДС
Объект мониторинга	Природный, техногенный или природно-техногенный объект или его часть, в пределах которого по определенной программе осуществляются регулярные наблюдения за окружающей средой с целью контроля за её состоянием, анализа и оценки происходящих в ней процессов, выполняемых для своевременного выявления и прогнозирования их изменений и оценки

Обработка происшествя/ Действия по обработке	Действия, совершенные бригадой реагирования для осуществления мер по устранению происшествя
Интеграция	Процесс объединения автоматизированных систем единое в целое.
Интеграционная шина	Программно-техническое решение, обеспечивающее сопряжение, интеграцию и/или информационное взаимодействие разнородных автоматизированных систем.
Интернет - Портал	Интернет-ресурс для граждан, представителей организаций и заинтересованных служб, предоставляющий доступ к информационным материалам, базе знаний консультативного обслуживания и сервисам для регистрации заявки о КСП
Инцидент	Происшествие или ситуация, зарегистрированное в ЕДДС Процесс обмена данными, находящимися в составных частях автоматизированной информационно-управляющей системы.
Информационное взаимодействие	
Регламент	Совокупность правил, определяющих порядок работы
Оперативная обстановка	Совокупность действий, событий, происшествя, кризисных ситуаций, ЧС на территории муниципального образования за определенный период времени, ведущих к изменению уровня рисков общественной безопасности, правопорядка, безопасности среды обитания.
Силы и средства реагирования	Специально подготовленные силы и средства федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, организаций и общественных объединений, предназначенные и выделяемые (привлекаемые) для предупреждения и ликвидации чрезвычайной ситуации
Событие	Зарегистрированный в Системе факт обращения
Специалист	Лицо, сведущее в любой профессиональной области и оказывающее консультационные услуги
Стационарный объект мониторинга	Объект мониторинга, на котором установлен датчик мониторинга ситуации
Статус (автоматический или ручной) (инцидента)	Этап в процессе обработки инцидента
Факсимильное сообщение	Графическое сообщение, передаваемое по телефонным сетям с помощью специального аппарата
Черный список	Список номеров телефонов абонентов, отмеченных в злоумышленных или ложных вызовах

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

HTML	HyperTextMarkupLanguage — язык разметки гипертекста
IVR	InteractiveVoiceResponse — интерактивные голосовые сообщения
PDF	PortableDocumentFormat — межплатформенный формат электронных документов, созданный фирмой AdobeSystems
SMS	ShortMessageService — технология, позволяющая осуществлять приём и передачу коротких текстовых сообщений сотовым телефоном
XLS,XLSX	Формат файла программы MS Excel
АБД ГИС	Автоматизированная база данных на основе геоинформационных технологий
АС РСЧС	Автоматизированная информационно-управляющая система Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций
АРМ	Автоматизированное рабочее место
АСКАВ	Автоматизированная система контроля аварийных выбросов на химически опасных объектах
АСКРО	Автоматизированная система контроля радиационной обстановки
АСКОС	Автоматизированная система контроля окружающей среды
АС	Автоматизированная система
АХОВ	Аварийно-химически опасные вещества
БД ЭПТ	База данных электронных паспортов территорий
ГИС	Геоинформационная система
ГЛОНАСС/GPS	Глобальная навигационная спутниковая система
ГОСТ	Государственный стандарт
ДДС	Дежурно-диспетчерская служба
ЕДДС	Единая дежурно-диспетчерская служба
ИГИП	Интеграционная географическая информационная подсистема
ИС	Информационная система
ИУС	Информационно-управляющая система
ИСПДн	Информационная система персональных данных
КСА	Комплекс средств автоматизации
КСОБЖН	Комплексная система обеспечения безопасности жизнедеятельности населения
КСЭОН	Комплексная система экстренного оповещения населения об угрозе возникновения или о возникновении чрезвычайных ситуаций
КСП	Кризисные ситуации и происшествия, а именно ситуации и происшествия, сложившиеся на определенной территории или акватории, в результате аварий, природных явлений, противоправных действий и иных факторов, которые при отсутствии необходимой профилактики могут привести к возникновению чрезвычайной ситуации.
ЛИДАР	Автоматизированная система дистанционного мониторинга окружающей среды

ЛСО	Локальная система оповещения
МГПО	Местный гарнизон пожарной охраны
МЧС России	Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий
НДВ	Не декларированные возможности
НПА	Нормативно-правовые акты
ОДС	Оперативная дежурная смена
ОМПЛ	Объект массового пребывания (постоянного и/или временного нахождения) людей
ОКСИОН	Общероссийская комплексная система информирования и оповещения населения в местах массового пребывания людей
ОС	Операционная система
ОПО	Общее программное обеспечение
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПОО	Потенциально-опасный объект
ПСЧ	Пункт связи пожарной части
ПТ	Паспорт территории
ПТК	Программно-технический комплекс
КТС	Комплекс технических средств
ПДн	Персональные данные
ПЭМИН	Побочные электромагнитные излучения и наводки
РСЧС	Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций
РЦОВ	Резервный центр обработки вызовов
РФ	Российская Федерация
Система-112	Система обеспечения вызова экстренных оперативных служб по единому номеру «112»
СКУД	Система контроля и управления доступом
СС ТМК	Система сбора результатов технического мониторинга и контроля объектов транспортной инфраструктуры
СУБД	Система управления базами данных
ТЗ	Техническое задание
ТУ	Технические условия
ФОИВ	Федеральный орган исполнительной власти
ЦОВ	Центр обработки вызовов
ЦОВ-112	Центр обработки вызовов Системы-112
ЦОД	Центр обработки данных
ЦППС	Центральный пункт пожарной связи
ЦУКС	Центр управления в кризисных ситуациях
ИКТ	Информационно-коммуникационные технологии
ЦУКС ГУ МЧС	Федеральное казенное учреждение «Центр управления в кризисных ситуациях ГУ МЧС России по Республике Саха (Якутия)»
ЧС	Чрезвычайная ситуация
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

ЭПТ

Электронные паспорта территорий

ВВЕДЕНИЕ

К настоящему времени в рамках развития системы обеспечения общественной безопасности, правопорядка и безопасности среды обитания в муниципальных образованиях внедрены различные аппаратно-программные комплексы (АПК). В целом, существующие АПК справляются с решением возложенных на них задач, продемонстрировав высокую эффективность. В тоже время высокий уровень рисков ЧС сохраняется. Более того, ряд причин, включая усиливающуюся тенденцию урбанизации, способствуют возрастанию рисков ЧС и тем, самым, создают угрозы для создания устойчивого социально-экономического развития и роста инвестиционной привлекательности муниципальных образований. Линейное наращивание состава АПК безопасности на уровне субъекта Российской Федерации и муниципального образования уже не дает желаемого роста эффективности, а ведет к чрезмерному росту сложности системы безопасности муниципальных образований, существенному увеличению затрат, затрудняет эксплуатацию и управление этими системами, что в конечном итоге не создает предпосылок к эффективному и адекватному управлению возрастающими рисками ЧС.

Эти обстоятельства выдвигают новые требования к функциональному наполнению систем безопасности и обуславливают необходимость комплексирования имеющихся автоматизированных, информационных систем на уровне субъекта Российской Федерации и муниципального образования в многоуровневую систему обеспечения общественной безопасности, правопорядка и безопасности среды обитания.

Комплексирование имеющихся автоматизированных систем в многоуровневая систему обеспечения общественной безопасности, правопорядка и безопасности среды обитания позволит сформировать единое информационное пространство, позволяющее использовать современные подходы к мониторингу, прогнозированию, предупреждению правонарушений, происшествий и чрезвычайных ситуаций и реагированию на них.

Работа выполнялась на основании технического задания на НИР «Разработка организационных документов по созданию и развитию аппаратно-программного комплекса «Безопасный город» (НИР «АПК Безопасный город») и проводится в соответствии с пунктом № 2-1-3-11/Б5 изменений в План научно-исследовательских и опытно-конструкторских работ МЧС России на 2015 и направлений перспективных научных исследований до 2020 года, утвержденных приказом МЧС России от 28.09.2015 №519 на 2015 год.

Результаты, полученные в рамках выполнения данной НИР рекомендуется использовать при построении и развитии АПК «Безопасный город» в муниципальных образованиях субъектов Российской Федерации.

1. Предложения по интеграции действующих информационно-аналитических, управляющих и других систем в области природно-техногенной и общественной безопасности в аппаратно-программный комплекс «Безопасный город»

1.1. Общие положения

Большинство современных автоматизированных систем состоят из следующих компонентов:

- Платформа, на которой функционируют остальные компоненты системы, включающая в себя аппаратуру (железо) и системное ПО.
- Данные, с которыми работает система. Состоят из СУБД и баз данных.
- Приложения, реализующие бизнес-логику по работе с данными системой. Состоят из компонентов бизнес-логики, пользовательского интерфейса, вспомогательных компонентов (фрэймворк) и сервера приложений, который обеспечивает хранение и доступ к компонентам приложения.
- Бизнес-процессы, представляющие из себя сценарии работы пользователей с системой.

Поэтому, интеграция информационных систем заключается в интеграции одного или нескольких компонентов интегрируемых информационных систем (объектов интеграции):

- интеграция платформ;
- интеграция данных;
- интеграция приложений;
- интеграция бизнес-процессов.

Целями интеграции платформ является:

- обеспечение возможности взаимодействия между приложениями, работающими на различных программно-аппаратных платформах (например, между приложениями, работающими на серверах Windows, Solaris, Linux и др;
- обеспечение возможности работы приложений, разработанных для одной программно-аппаратной платформы, на других программно-аппаратных

платформах (например, приложений Windows на платформах Linux, Solaris и др.).

Существует несколько подходов, направленных на достижение этих целей:

- удаленный вызов процедур (RPC, CORBA, DCOM, Web-сервисы);
- ПО промежуточного слоя (Microsoft.Net, Java Runtime);
- виртуализация.

Технологии удаленного вызова процедур (в широком смысле под процедурой понимается некоторая функциональность приложения) позволяют опубликовать процедуру и обеспечить возможность ее вызова (передачи входящих параметров и получения выходных результатов) для приложений, работающих на других платформах. Элементами таких технологий обычно являются: общий для всех платформ язык описания интерфейсов процедур (IDL, WSDL), «адаптер» (переходник) процедуры, который транслирует внешние вызовы во внутренние и передает результаты обратно (стабы) и менеджеры, отвечающие за доставку запросов и результатов между платформами в сети (брокеры). Примерами технологий удаленного вызова процедур являются: RPC, CORBA, DCOM, Web-сервисы.

Концепция программного обеспечения промежуточного слоя (framework, среда исполнения, виртуальная машина) состоит в разработке прикладного ПО не с использованием сервисов конкретной операционной системы (например, Windows API), а с использованием сервисов ПО промежуточного слоя. Разработчиками ПО промежуточного слоя создаются ее реализации под различные операционные системы, которые транслируют вызовы соответствующих функций фрейворка в вызовы соответствующей операционной системы. Типичным примером является технология Java Runtime Environment. Приложения, разработанные для этой технологии работают на любых программно-аппаратных платформах (Windows, Linux и др.) без каких-либо доработок самих приложений. Аналогичные возможности предоставляет среда Microsoft .Net Framework.

Интересной и современной концепцией является «виртуализация». К интеграции платформ она имеет отношение постольку, поскольку позволяет существенно упростить использования различных платформ и, соответственно, использование систем, требующих для своего функционирования наличия конкретных платформ. Если без виртуализации возможно одновременное функционирование N операционных сред на N серверов, то применение технологий виртуализации позволяет обеспечить функционирование N операционных сред на M серверов. Если $N > M$ – это позволяет сократить расходы на аппаратное обеспечение путем его более эффективного использования. Если $N < M$ – это простой путь увеличения производительности систем. Например, виртуализация позволяет развернуть и одновременно использовать на одном физическом сервере несколько операционных систем: Windows, Linux и др. На каждом из таких «виртуальных» серверов могут быть развернуты соответствующие системы, которые будут доступны одновременно.

По определению информационная система работает с данными. В подавляющем большинстве случаев система имеет в своем составе базу данных для их хранения. Интеграция на уровне данных предполагает совместное использования данных различных систем. Интеграция данных может оказаться проще, чем интеграция приложений, т.к. промышленные СУБД, в которых обычно хранят данные информационные системы, имеют развитые возможности программного доступа к данным из других приложений. Сами приложения при этом могут иметь весьма ограниченные возможности программного (вне собственного пользовательского интерфейса) использования своей функциональности внешними системами.

Подходы к интеграции данных:

- универсальный доступ к данным;
- хранилища данных.

Технологии универсального доступа к данным позволяют обеспечить единообразный доступ к данным различных СУБД. Посредником для работы с конкретной СУБД в данном случае является драйвер для соответствующей

СУБД. Это позволяет абстрагироваться от специфики конкретных СУБД и легко осуществлять интеграцию данных, хранящихся в различных СУБД. Наиболее распространенные технологии этого класса: ODBC, JDBC.

Концепция хранилищ данных состоит в создании корпоративного хранилища данных. Хранилище данных – база данных, хранящая в себе данные, собираемые из баз данных различных информационных систем, для целей их дальнейшего анализа. Для создания хранилищ данных используются технологии (OLAP), отличные от технологий создания оперативных БД (OLTP). В основном это делается для повышения производительности выполнения сложных аналитических запросов по многим параметрам (многомерные запросы). Подходы к созданию и наполнению хранилищ данных отражены в парадигме ETL (extraction, transformation, loading = извлечение, преобразование и загрузка). Технологии и инструментальные средства анализа больших массивов данных с целью выявления закономерностей предметной области объединяются понятием «Data Mining». Термин для совокупности технологий хранилищ данных и инструментальных средств и – «Business Intelligence».

Интеграция данных включает объединение данных, находящихся в различных источниках, и предоставление данных пользователям в унифицированном виде. Роль интеграции данных возрастает, когда увеличивается объём и необходимость совместного использования данных.

Системы интеграции данных могут обеспечивать интеграцию данных на физическом, логическом и семантическом уровне. Интеграция данных на физическом уровне с теоретической точки зрения является наиболее простой задачей и сводится к конверсии данных из различных источников в требуемый единый формат их физического представления.

Интеграция данных на логическом уровне предусматривает возможность доступа к данным, содержащимся в различных источниках, в терминах единой глобальной схемы, которая описывает их совместное представление с учетом структурных и, возможно, поведенческих (при использовании объектных моделей) свойств данных. Семантические свойства данных при этом не

учитываются. Поддержку единого представления данных с учетом их семантических свойств в контексте единой онтологии предметной области обеспечивает интеграция данных на семантическом уровне.

Процессу интеграции препятствует неоднородность источников данных, в соответствии с уровнем интеграции. Так, при интеграции на физическом уровне в источниках данных могут использоваться различные форматы файлов. На логическом уровне интеграции может иметь место неоднородность используемых моделей данных для различных источников или различаются схемы данных, хотя используется одна и та же модель данных. Одни источники могут быть веб-сайтами, а другие — объектными базами данных и т. д. При интеграции на семантическом уровне различным источникам данных могут соответствовать различные онтологии. Например, возможен случай, когда каждый из источников представляет информационные ресурсы, моделирующие некоторый фрагмент предметной области, которому соответствует своя понятийная система, и эти фрагменты пересекаются.

При создании системы интеграции возникает ряд задач, состав которых зависит от требований к ней и используемого подхода. К ним, в частности, относятся:

- разработка архитектуры системы интеграции данных.
- создание интегрирующей модели данных, являющейся основой единого пользовательского интерфейса в системе интеграции.
- разработка методов отображения моделей данных и построение отображений в интегрирующую модель для конкретных моделей, поддерживаемых отдельными источниками данных.
- интеграция метаданных, используемых в системе источников данных.
- преодоление неоднородности источников данных.
- разработка механизмов семантической интеграции источников данных.

Архитектуры систем интеграции:

а) Консолидация. В случае консолидации данные извлекаются из источников, и помещаются в Хранилище данных. Процесс заполнения Хранилища состоит из трех фаз — извлечение, преобразование, загрузка (Extract, Transformation, Loading — ETL). Во многих случаях именно ETL понимают под термином «интеграция данных». Еще одна распространенная технология консолидации данных — управление содержанием корпорации (enterprise content management, сокр. ECM). Большинство решений ECM направлены на консолидацию и управление неструктурированными данными, такими как документы, отчеты и web-страницы.

Консолидация — однонаправленный процесс, то есть данные из нескольких источников сливаются в Хранилище, но не распространяются из него обратно в распределенную систему. Часто консолидированные данные служат основой для приложений бизнес-аналитики (Business Intelligence, BI), OLAP-приложений.

При использовании этого метода обычно существует некоторая задержка между моментом обновления информации в первичных системах и временем, когда данные изменения появляются в конечном месте хранения. Конечные места хранения данных, содержащие данные с большими временами отставания (например, более одного дня), создаются с помощью пакетных приложений интеграции данных, которые извлекают данные из первичных систем с определенными, заранее заданными интервалами. Конечные места хранения данных с небольшим отставанием обновляются с помощью оперативных приложений интеграции данных, которые постоянно отслеживают и передают изменения данных из первичных систем в конечные места хранения.

б) Федерализация. В федеративных БД физического перемещения данных не происходит: данные остаются у владельцев, доступ к ним осуществляется при необходимости (при выполнении запроса). Изначально федеративные БД предполагали создание в каждом из n узлов $n-1$ фрагментов кода, позволяющего обращаться к любому другому узлу.

При использовании медиатора создается общее представление (модель) данных. Медиатор — посредник, поддерживающий единый пользовательский интерфейс на основе глобального представления данных, содержащихся в источниках, а также поддержку отображения между глобальным и локальным представлениями данных. Пользовательский запрос, сформулированный в терминах единого интерфейса, декомпозируется на множество подзапросов, адресованных к нужным локальным источникам данных. На основе результатов их обработки синтезируется полный ответ на запрос. Используются две разновидности архитектуры с посредником — Global as View и Local as View.

Отображение данных из источника в общую модель выполняется при каждом запросе специальной оболочкой (wrapper). Для этого необходима интерпретация запроса к отдельным источникам и последующее отображение полученных данных в единую модель. Сейчас этот способ также относят к федеративным БД.

Интеграция корпоративной информации (Enterprise information integration, сокр. ЕИ) — это пример технологии, которая поддерживает федеративный подход к интеграции данных.

Изучение и профилирование первичных данных, необходимые для федерализации, несильно отличаются от аналогичных процедур, требуемых для консолидации.

в) Распространение данных. Приложения распространения данных осуществляют копирование данных из одного места в другое. Эти приложения обычно работают в оперативном режиме и производят перемещение данных к местам назначения, то есть зависят от определенных событий. Обновления в первичной системе могут передаваться в конечную систему синхронно или асинхронно. Синхронная передача требует, чтобы обновления в обеих системах происходили во время одной и той же физической транзакции. Независимо от используемого типа синхронизации, метод распространения гарантирует доставку данных в систему назначения. Такая гарантия — это ключевой отличительный признак распространения данных. Большинство технологий

синхронного распространения данных поддерживают двусторонний обмен данными между первичными и конечными системами. Примерами технологий, поддерживающих распространение данных, являются интеграция корпоративных приложений (Enterprise application integration, сокр. EAI) и тиражирование корпоративных данных (Enterprise data replication, сокр. EDR). От федеративных БД этот способ отличает двустороннее распространение данных.

г) Сервисный подход. Сервисно-ориентированная архитектура SOA (Service Oriented Architecture), успешно применяемая при интеграции приложений, применима и при интеграции данных. Данные также остаются у владельцев и даже местонахождение данных неизвестно. При запросе происходит обращение к определённым сервисам, которые связаны с источниками, где находится информация и ее конкретный адрес.

Интеграция данных объединяет информацию из нескольких источников таким образом, чтобы ее можно было показать клиенту в виде сервиса. Сервис — это не запрос в традиционном смысле обращения к данным, скорее, это извлечение некоторой бизнес-сущности (или сущностей), которое может быть выполнено сервисом интеграции через серию запросов и других сервисов. Подход SOA концентрируется, в первую очередь, на определении и совместном использовании в форме сервисов относительно ограниченного количества самых важных бизнес-функций в корпорации. Следовательно, сервис-ориентированные интерфейсы в довольно большой степени строятся на ограниченном количестве запросов на необходимую информацию, которую нужно представить потребителю.

Имея соответствующие учетные данные системы безопасности, потребитель может осуществить выборку любых данных из источника через почти неограниченное количество различных запросов SQL. Но для этого потребитель должен иметь представление о модели источника данных и способе создания результата с использованием этой базовой модели. Чем сложнее модель источника данных, тем более сложной может оказаться эта задача.

Вне зависимости от выбранных технологии и метода интеграции данных, остаются вопросы, связанные с их смысловой интерпретацией и различиями в представлении одних и тех же вещей. Именно, приходится разрешать несоответствие схем данных и несоответствие самих данных.

Типы несоответствия схем данных:

- Конфликты неоднородности (используются различные модели данных для различных источников);
- Конфликты именованя (в различных схемах используется различная терминология, что приводит к омонимии и синонимии в именовании);
- Семантические конфликты (выбраны различные уровни абстракции для моделирования подобных сущностей реального мира);
- Структурные конфликты (одни и те же сущности представляются в разных источниках разными структурами данных).

Структурные и семантические конфликты выливаются в следующие проблемы:

- Различие в типах данных. Некоторый домен в одном источнике может представляться числом, в другом — строкой фиксированной длины, в третьем — строкой переменной длины;
- Различие в единицах измерения. В одной БД указана величина в сантиметрах, в другой — в дюймах;
- Различие в множестве допустимых значений;
- Различие «домен-отношение». Домен в одной БД (например строковое значение) соответствует таблице в другой БД (записи из таблицы-справочника);
- Различие «домен — группа доменов». В одном источнике адрес записывается одной строкой, в другом — отдельные поля для улицы, дома, строения, квартиры;
- Различие «данные-схема». Данные одной БД соответствуют схеме (метаданным) другой. В одной БД «инженер» — значение атрибута «должность»

отношения «работник», в другой «инженеры» — отношение, содержащее некоторых работников, в то время как «бухгалтеры» содержит других;

- Отсутствующие значения. В каком-то из источников может отсутствовать информация, имеющаяся в большинстве других.

Разрешение этих несоответствий часто выполняется вручную.

Интеграция на уровне приложений подразумевает использование готовых функций приложений другими приложениями.

Стоит упомянуть следующие подходы к интеграции приложений:

- интерфейсы прикладного программирования;
- обмен сообщениями (Корпоративная шина сервисов);
- сервис-ориентированная архитектура;
- интеграция пользовательских интерфейсов.

Интерфейс прикладного программирования конкретной системы представляет из себя «опубликованный» функционал этой системы, который может быть использован извне. Функционал может публиковаться в виде набора функций (пример – Windows API) или в виде объектной модели (объекты со свойствами и методами, пример – объектные модели приложений Microsoft Office).

В большинстве случаев интеграция нескольких систем заключается в передаче информации между ними, например, в форме запрос-ответ. Если системы функционируют в гетерогенных распределенных средах, то принципиальное значение имеет обеспечение гарантированности, безопасности, управляемости доставки информации между приложениями. Эти и другие принципы реализуются в корпоративных системах обмена сообщениями. В данном случае речь идет об обмене сообщениями между приложениями, а не людьми, как, например, в случае E-mail или ICQ. Функциональность этих систем достаточно прозрачна – прием сообщения от одного приложения, транспортировка по заданным правилам и передача этого сообщения другому приложению. При этом может производиться шифрование сообщений (для невозможности прочтения данных в процессе транспортировки), цифровая

подпись (для защиты от умышленного изменения данных во время пути сообщения), настройка подписки (для отправки одного сообщения сразу нескольким приложениям), определение метаданных для сообщений (для облегчения использования сообщений со сложной структурой содержимого) и др [http://en.wikipedia.org/wiki/Enterprise_service_bus].

Сервис-ориентированная архитектура (SOA) является современной парадигмой. Она является логическим продолжением концепции Web-сервисов, которая состоит в публикации функциональных блоков какого-либо приложения в виде, позволяющем получить к ним доступ другим приложениям через Web. Web (протокол HTTP) в данном случае привлекателен ввиду возможности его использования и, соответственно, использования опубликованных в Web приложений на любых программно-аппаратных платформах. Web-сервис – небольшая программная надстройка над функционалом приложения, преобразующая вызовы, получаемы через Web во внутренние вызовы функций приложения и возвращающая результаты обратно.

Публикация функционала корпоративных приложений в виде Web-сервисов. Упорядочивание опубликованных сервисов в виде каталога.

Построение на основе Web-сервисов новых приложений путем их комбинации.

Понятно, что в данном случае создания новых приложений на основе существующих Web-сервисов будет существенно ниже, чем разработка приложений «с нуля» или обширная интеграция с другими системами.

Также часто используется следующий подход – интеграция пользовательских интерфейсов. Например, для создания приложений «одного окна». Простейший пример – фреймы в вэб-странице. Внутри каждого фрейма при этом содержится отдельное вэб-приложение. Благодаря фреймам, все эти приложения отображаются на экране одновременно. Пользовательские интерфейсы вэб-приложений очень легко интегрируются, однако, существуют возможности интегрировать и «классические» пользовательские интерфейсы и их фрагменты (ActiveX).

Наиболее целостным подходом к интеграции систем является интеграции на уровне бизнес-процессов. В рамках интеграции бизнес-процессов происходит и интеграция приложений, и интеграция данных и, что не менее важно, людей, вовлеченных в этот бизнес-процесс. Интеграция на уровне бизнес-процессов является наиболее «естественной» для организаций, т.к. их деятельность состоит, прежде всего, именно из бизнес-процессов, а не приложений, баз данных и платформ.

Идеи, лежащие в основе интеграции бизнес-процессов, достаточно просты и включают следующие шаги:

- составить сценарий некоторого бизнес-процесса, происходящего в организации;
- описать в нем операции взаимодействия пользователей с различными системами и систем между собой.

Таким образом, бизнес-процесс является элементом, логически интегрирующим различные системы. Сценарий создается при помощи специализированного программного продукта, который далее будет управлять ходом этого бизнес-процесса согласно сценарию.

Операции взаимодействия с системами в рамках бизнес-процесса детально описываются в терминах информационного обмена: форматы обмена, используемые сервисы, приложения, события, правила, политики и т.п.

К интегрирующему программному обеспечению, при помощи которого описан сценарий бизнес-процесса, подключаются посредством адаптеров интегрируемые системы, вовлеченные в бизнес-процесс. Таким образом, становится возможным автоматизированный информационный обмен между системами.

Готовый к выполнению бизнес-процесс выводится на «пульт управления» менеджера, при помощи которого, он может запускать и останавливать бизнес-процессы, отслеживать их состояние, вводить данные и принимать решения на отдельных операциях бизнес-процессов, требующих участия человека и др.

Взаимодействия между системами, не требующее участия человека осуществляется автоматически интегрирующим ПО.

Существует большое количество программных продуктов для интеграции систем: коммерческий и бесплатных, с закрытыми исходниками и Open Source, дорогих и дешевых, с различной функциональностью, рассчитанных на различный масштаб бизнеса пользователей.

Можно выделить следующие классы продуктов для интеграции систем:

- реализующие идеологию SOA;
- реализующие идеологию Messaging (промежуточное ПО);
- корпоративные шины сервисов;
- средства интеграции на уровне бизнес-процессов (BPEL, Business Process Execution Language);
- средства интеграции данных.

Серьезные продукты для интеграции корпоративных приложений от солидных вендоров включают в себя компоненты сразу нескольких классов из перечисленных выше. В настоящем обзоре ограничимся продуктами от трех вендоров: Microsoft, Oracle и IBM.

Microsoft BizTalk Server.

BizTalk Server представляет собой программный продукт для интеграции приложений и бизнес-процессов. Архитектура BizTalk Server, основана на идеологии обмена сообщениями между приложениями.

Центральной частью системы является механизм обмена сообщениями (Engine), который состоит из двух частей:

- Messaging – транспортный уровень (прием, хранение и отправка сообщений между приложениями), подключение к обмену различных систем, функционирующих на различных платформах, использование учетных записей для подключения к системам и др.;
- Orchestration – правила (логика) обработки сообщений. Например, при помощи визуального дизайнера можно определить алгоритм, в соответствии с которым, получив сообщение от терминала необходимо создать сообщение для

CRM-системы и бухгалтерской системы с целью дальнейшей обработки факта продажи.

«Надстройки» над BizTalk Server Engine (Business Activity Monitoring и Services) предоставляют возможности управления бизнес-процессами в организации на основании информации, собираемой в процессе «общения» интегрированных приложений.

Реализованная в продукте идея заключается в регистрации некоторой необходимой информации (Tracking, задается при настройке правил обработки сообщений в Engine) для целей дальнейшего мониторинга бизнес-процессов. Например, можно описать бизнес-процесс продажи, включающий несколько стадий (заказ, оплата, отгрузка и т.п.). Далее при получении сообщения от соответствующей системы (POS, бухгалтерия, склад и т.п.), отражающего факт изменения стадии конкретной продажи, это регистрируется и становится доступным для просмотра текущего состояния и анализа исторических данных.

Также следует отметить, что Microsoft BizTalk Server позиционируется вендором как продукт для B2B-интеграции. Это означает, что интегрируемые бизнес-процессы и приложения не обязательно должны находиться в рамках одной компании, а могут затрагивать несколько взаимодействующих компании, например, в цепочке поставок. В этом случае каждая такая компания использует Microsoft BizTalk Server для интеграции внутренних процессов и приложений и взаимодействует с BizTalk-серверами других компаний для внешнего обмена [<http://www.microsoft.com/rus/biztalk/>].

Microsoft SQL Server.

Общеизвестная СУБД Microsoft SQL Server является также примером платформы для интеграции данных. Функции интеграции реализуются в MS SQL Server следующими компонентами: Integration Services и Analysis Services.

Integration Services является ETL-инструментом, позволяющим [<http://www.microsoft.com/sqlserver/2008/ru/ru/default.aspx>]:

- Собрать данные из различных источников (например, реляционных БД, текстовых файлов, RSS-каналов в Интернете, вэб-сервисов и др.);

- Преобразовать их из исходных форматов в необходимые с использованием промежуточных хранилищ или без них. Правила преобразование и консолидации задаются разработчиками хранилища;

- Поместить результат в информационное хранилище, в котором они становятся доступными потребителям интегрированной информации.

Analysis Services поддерживает процесс интеграции данных на следующих этапах, а именно:

- Создание OLAP-хранилищ, в которое стекаются данные из различных источников в процессе интеграции, и хранение многомерных данных;

- Обеспечение доступа к OLAP-данным, выполнения многомерных запросов. Типичный пример – работа с данными при помощи Pivot Table.

- Интеллектуальный автоматизированный анализ данных (Data Mining).

Oracle SOA Suite.

Данный продукт от Oracle похож по своей функциональности на BizTalk сервер от Microsoft. Он разработан на технологиях Java, поэтому может работать на различных платформах (Windows, Solaris, HP-UX, Linux).

Также, в отличие от BizTalk Server Oracle SOA Suite представляет из себя не один программный продукт, а набор относительно программных компонентов, некоторые из которых могут использоваться по отдельности [<http://www.oracle.com/global/ru/ip/10g/as/bpel.html>]:

Oracle BPEL Process Manager – средство создания (при помощи визуального дизайнера), «хостинга» и управления бизнес-процессами, включающими в себя взаимодействие между людьми и интегрируемыми ИТ-приложениями.

Oracle Business Activity Monitoring – панель управления (dashboard) интегрированными бизнес-процессами. Позволяет просматривать различные показатели бизнес-процессов (например, KPI), сервисов и их компонентов в «одном окне».

Oracle Business Rules – средство описания бизнес-правил и политик, используемых в интегрированных бизнес-процессах.

Oracle Service Bus – «транспортный уровень», корпоративная шина сервисов (ESB), обеспечивает взаимодействия между различными приложениями в организации.

Oracle Web Services Manager – инструмент централизованного доступа к веб-сервисам, существующим в организации, обеспечивающий создание учетных записей и политик для приложений, использующих администрируемые веб-сервисы.

Oracle JDeveloper – среда разработки на Java от Oracle.

Connectivity – набор адаптеров (более 300) для подключения к различным программным продуктам и технологиям, используемым в организации.

Oracle SOA Suite входит в состав продуктов middleware, для которых вендор использует обобщающее название Oracle Fusion.

IBM WebSphere.

IBM WebSphere – это middleware от IBM, аналог Oracle Fusion. В составе IBM WebSphere есть продукты, обеспечивающие интеграцию систем в парадигме SOA (по аналогии с Oracle SOA Suite). Состав и функционал продуктов похож на аналогичное ПО других вендоров [<http://www.ibm.com/products/ru/ru/>]:

WebSphere Business Modeler – средство визуального описания интегрирующих бизнес-процессов.

WebSphere Process Server – хостинг и исполнение бизнес-процессов.

WebSphere Integration Developer – среда разработки сервисных компонентов.

WebSphere Business Monitor – инструмент мониторинга бизнес-процессов

WebSphere Enterprise Service Bus – система, обеспечивающая взаимодействие между сервисами, реализованным в компании в рамках SOA.

WebSphere MQ – система обмена сообщениями между приложениями, в т.ч. в рамках SOA.

Интеграция данных включает объединение данных, находящихся в различных источниках, и предоставление данных пользователям в унифицированном виде. Этот процесс становится существенным как в коммерческих задачах (когда двум похожим компаниям необходимо объединить их базы данных), так и в научных (комбинирование результатов исследования из различных биоинформационных репозиториях, для примера). Роль интеграции данных возрастает, когда увеличивается объём и необходимость совместного использования данных.

Итоги сравнения интеграционных решений приведены в «Приложении И». В этом приложении показано, что сравнивались 16 интеграционных продуктов, которые доступны на российском рынке. Альтернативы сравнивались по следующим критериям:

- Функциональность, технологичность и соответствие современным взглядам;
- Устойчивость к "Санкциям" и др. политическим демаршам;
- Информационная безопасность;
- Масштабность и сложность выполненных Проектов, особенно с Госструктурами;
- Простота представления, изложения и понимания архитектуры (сути) решений;
- Сертификация;
- Возможности доработки, гибкость;
- Наличие исходных кодов и документации;
- Наличие адаптеров взаимодействия с подсистемами АПК «БГ».

1.2. Перечень функций (задач), ранее созданных и действующих автоматизированных информационно-управляющих систем различной ведомственной принадлежности, интегрируемых в состав АПК «Безопасный город»

1.2.1 Место АПК «Безопасный город» в структуре РСЧС

1.2.1.1 Согласно Концепции построения и развития аппаратно-программного комплекса «Безопасный город» возросшие требования к функциональному наполнению систем безопасности обусловили необходимость формирования на уровне субъекта Российской Федерации и муниципального образования комплексной многоуровневой системы обеспечения общественной безопасности, правопорядка и безопасности среды обитания, базирующейся на современных подходах к мониторингу, прогнозированию, предупреждению правонарушений, происшествий и чрезвычайных ситуаций и реагированию на них.

Целью построения и развития аппаратно-программного комплекса «Безопасный город» является повышение общего уровня общественной безопасности, правопорядка и безопасности среды обитания за счет существенного улучшения координации деятельности сил и служб, ответственных за решение этих задач, путем внедрения на базе муниципальных образований комплексной информационной системы, обеспечивающей прогнозирование, мониторинг, предупреждение и ликвидацию возможных угроз, а также контроль устранения последствий кризисных ситуаций и правонарушений.

На АПК «Безопасный город» муниципального образования возлагаются задачи автоматизации процессов взаимодействия территориальных и функциональных подсистем РСЧС, а также ведомственных подсистем на территории муниципального образования.

Кроме того, за счет интеграции с существующими информационными системами всех уровней, компоненты АПК «Безопасный город» должны обеспечивать:

- формирование информационно-коммуникационной платформы для органов местного самоуправления с целью устранения рисков обеспечения безопасности среды обитания, общественной безопасности и правопорядка на базе межведомственного взаимодействия;
- обеспечение информационного обмена на региональном и муниципальном уровне через единое информационное пространство с учетом разграничения прав доступа к информации разного характера;
- создание дополнительных инструментов на базе муниципальных образований для оптимизации работы существующей системы обеспечения общественной безопасности;
- построение и развитие систем ситуационного анализа причин дестабилизации обстановки и прогнозирования существующих и потенциальных угроз для обеспечения безопасности населения муниципального образования.

1.2.2 Перечень действующих АС различной ведомственной принадлежности, интегрируемых в состав АПК «Безопасный город».

Перечень функций (задач) ранее созданных и действующих АС различной ведомственной принадлежности, интегрируемых в состав АПК «Безопасный город» определен на основе анализа технических заданий муниципальных образований по созданию АПК «Безопасный город». Всего было проанализировано около 140 технических заданий. В результате анализа составлен перечень систем, интеграция которых предусматривается посредством АПК «Безопасный город» муниципального уровня:

1. Сегмент обеспечения правопорядка и профилактики правонарушений на территории муниципального образования в составе КСА следующих подсистем:

Подсистемы мониторинга

а) подсистема интеллектуального видеонаблюдения, обеспечивающая автоматическое детектирование (видеообнаружения, видеоидентификации и видеораспознавания) определенных событий с целью мониторинга, предупреждения и профилактики правонарушений;

б) подсистема оценки качества деятельности представителей территориальных органов федеральных органов исполнительной власти, ответственных за обеспечение правопорядка и профилактики правонарушений на территории муниципального образования;

в) подсистема позиционирования мобильным персоналом органов исполнительной власти, ответственных за правопорядка и профилактики правонарушений на территории муниципального образования;

г) подсистема обеспечения экстренной связи;

Подсистемы управления

д) подсистема управления мобильным персоналом органов исполнительной власти, ответственных за правопорядка и профилактики правонарушений на территории муниципального образования;

е) подсистема управления территориальными органами федеральных органов исполнительной власти, ответственных за обеспечение правопорядка и профилактики правонарушений на территории муниципального образования;

ж) подсистема управления видеонаблюдением и видеопотоками.

сегмент обеспечения защиты от чрезвычайных ситуаций природного и техногенного характера и пожаров в составе КСА следующих подсистем:

Подсистемы мониторинга

а) подсистема мониторинга критически важных объектов;

б) подсистема мониторинга потенциально опасных объектов;

в) подсистема мониторинга социально значимых объектов;

г) подсистема мониторинга пожарной безопасности объектов;

Подсистемы управления

- д) подсистема управления твердыми бытовыми отходами;
- е) подсистема управления технического обеспечения и ремонтного обслуживания критически важных объектов;
- ж) подсистема управления технического обеспечения и ремонтного обслуживания потенциально опасных объектов;
- з) подсистема управления технического обеспечения и ремонтного обслуживания социально значимых объектов;
- и) подсистема позиционирования и управления мобильными подразделениями сил РСЧС, привлекаемыми к ликвидации ЧС и пожаров, в том числе, пожарно-спасательными и пожарными подразделениями;
- к) подсистема поддержки принятия решений по предупреждению и ликвидации ЧС природного и техногенного характера, снижению рисков возникновения ЧС и пожаров;
- л) подсистема информирования и оповещения населения.

2. Сегмент обеспечения безопасности инфраструктуры жилищно-коммунального комплекса в составе КСА следующих подсистем:

Подсистемы мониторинга

- а) мониторинга и управление работой по предупреждению и ликвидации чрезвычайных ситуаций, вызванных сбоями в работе коммунальной инфраструктуры;
- б) подсистема мониторинга сбоев в работе сети водоснабжения;
- в) подсистема мониторинга сбоев в работе сети газоснабжения;
- г) подсистема мониторинга сбоев в работе сети теплоснабжения;
- д) подсистема мониторинга сбоев в работе сети электроснабжения;
- е) подсистема мониторинга, предупреждения и ликвидации чрезвычайных ситуаций, возникающих при нарушении правил пожарной безопасности;
- ж) обеспечения безопасности охраняемых объектов, придомовых территорий и объектов социального назначения;
- з) обеспечения экстренной связи;

и) управления ремонтными работами на объектах муниципальной (коммунальной) инфраструктуры;

Подсистемы управления

к) подсистема управления технического обеспечения и ремонтного обслуживания сети водоснабжения;

л) подсистема управления технического обеспечения и ремонтного обслуживания сети газоснабжения;

м) подсистема управления технического обеспечения и ремонтного обслуживания сети теплоснабжения;

н) подсистема управления технического обеспечения и ремонтного обслуживания сети электроснабжения;

о) подсистема информирования и оповещения населения;

п) подсистема моделирования предпосылок и оценка последствий чрезвычайных ситуаций.

3. Сегмента обеспечения безопасности имущественного комплекса, в составе КСА следующих подсистем:

а) подсистема управления дежурного плана города;

б) подсистема поддержки принятия решений при управлении муниципальными активами;

в) подсистема обеспечения социальной безопасности;

г) подсистема управления земельным муниципальным реестром;

д) подсистема управления реестром электросетей;

е) подсистема управления реестром сетей и сооружений водоснабжения;

ж) подсистема управления реестром тепловых сетей;

з) подсистема управления реестром дорог;

и) подсистема управления реестром телекоммуникаций;

к) подсистема управления социальным реестром;

л) подсистема управления реестром мест обработки и утилизации отходов;

м) подсистема управления реестром природоохранных и рекреационных зон и паркового хозяйства.

1.2.3 Перечень функций (задач) и назначение подсистем в составе АПК «Безопасный город»

1.2.3.1 Функции интеграции в АПК «Безопасный город» выполняет подсистема обеспечения координации и взаимодействия (ПОКВ), предназначенная для обеспечения создания и поддержки единой информационной среды между взаимодействующими органами управления и которая обеспечивает хранение и маршрутизацию интегрируемых данных, предоставляет взаимодействующим системам сервисы доступа к интегрируемым данным, а также средства доступа к сервисам настройки и поддержки функционирования бизнес-процессов.

ПОКВ в целях обеспечения требований предназначения должна включать следующие необходимые функциональные средства:

- формирования модели данных АПК «Безопасный город»;
- формирования хранилищ данных в соответствии с заданной моделью данных;
- доступа к данным в соответствии с правами доступа;
- доступа к сервисам взаимодействия с поддержкой синхронного и асинхронного способа вызова сервисов;
- обмена сообщениями с гарантированной доставкой;
- статической и алгоритмической маршрутизации сообщений;
- обработки и преобразования сообщений (трансформация данных между форматами);
- оркестровки и хореографии сервисов;
- набор готовых адаптеров для обеспечения доступа к данным из сторонних информационных систем;

- централизованного управления безопасностью и политиками доступа к данным;

- аудита, протоколирования и т.п.

В состав ПОКВ должны входить необходимые функциональные элементы:

- хранилище данных;

- средства доступа к данным;

- средства поддержки формирования и выполнения бизнес-процессов.

Данные функциональные элементы должны обеспечивать:

- программные интерфейсы (сервисы интеграции), обеспечивающие информационное взаимодействие автоматизированных систем в составе АПК «Безопасный город»;

- сквозное управление бизнес-процессами интегрируемых систем, средствами унифицированного событийно-ориентированного механизма взаимодействия;

- организацию структурированных разделяемых данных («мастер»-справочников);

- ведение нормативно-справочной информации;

- разграничение доступа пользователей взаимодействующих систем к циркулирующим данным;

- формирование и поддержку функционирования модели данных хранилища интегрируемых данных интеграционной шины.

1.2.3.2 Подсистема комплексного мониторинга объектов (ПКМО), предназначенная для сбора и комплексной обработки сообщений от автоматических (автоматизированных) систем мониторинга стационарных и подвижных объектов, для поддержки интеграции в АПК «Безопасный город» должна включать в свой состав (для каждой системы мониторинга) агенты взаимодействия с ПОКВ, обеспечивающие обмен данными с ПОКВ.

Агенты взаимодействия с ПОКВ в составе систем мониторинга должны функционировать в составе АПК «Безопасный город» в соответствии с соответствующим протоколом информационно-технического взаимодействия.

1.2.3.3 Подсистема комплексного информирования и оповещения (ПКИО), предназначенная для комплексного информирования и оповещения населения с использованием всех имеющихся для этого систем и средств, для поддержки интеграции в АПК «Безопасный город» должна включать в свой состав (для каждой системы информирования и оповещения населения) агенты взаимодействия с ПОКВ, обеспечивающие обмен данными с ПОКВ. Агенты взаимодействия с ПОКВ в составе систем информирования и оповещения населения должны функционировать в составе АПК «Безопасный город» в соответствии с соответствующим протоколом информационно-технического взаимодействия.

1.2.3.4 Подсистема поддержки принятия решений (ПППР), предназначенная для аналитического и количественного обоснования вариантов возможных управленческих решений и планов их реализации, для поддержки интеграции в АПК «Безопасный город» должна включать в свой состав агент взаимодействия с ПОКВ, обеспечивающий обмен данными с ПОКВ. Агент взаимодействия с ПОКВ в составе ПППР должен функционировать в составе АПК «Безопасный город» в соответствии с соответствующим протоколом информационно-технического взаимодействия.

1.3 Требования к категориям и содержанию информации, передаваемой из действующих автоматизированных информационно-управляющих систем в системы АПК «Безопасный город»

1.3.1 Определение перечня категорий передаваемой информации

Информация, циркулирующая в рамках единого информационного пространства АПК «Безопасный город» подразделяется на следующие категории:

- оперативную;
- плановую;

- нормативно-справочную;
- учетную.

К оперативной информации относятся сведения о прогнозируемых и (или) возникших чрезвычайных ситуациях и происшествиях, сведения о силах и средствах постоянной готовности, привлекаемых для предупреждения и ликвидации чрезвычайных ситуаций и происшествий, а также об их деятельности, направленной на предупреждение и ликвидацию чрезвычайных ситуаций, сведения о динамических параметрах процессов (превышение критических параметров систем обеспечения жизнедеятельности населения, информация о чрезвычайных ситуациях и происшествиях).

К плановой информации относятся сведения о текущих и перспективных планах экономического или социально-экономического развития административно-территориальных образований, для заблаговременного планирования мероприятий по предупреждению и ликвидации чрезвычайных ситуаций и происшествий, включая обеспечение соответствующими ресурсами в необходимом объеме.

К нормативно-справочной информации относится совокупность нормативных документов и справочных материалов, хранящихся в базах данных органов исполнительной власти федерального, регионального и муниципального уровней, предназначенных для информационного обеспечения решения задач по предупреждению и ликвидации чрезвычайных ситуаций и происшествий, выполняемых органами повседневного управления, силами и средствами территориальных и функциональных подсистем.

К учетной информации относятся сведения об имевших место в прошлом чрезвычайных ситуациях, происшествиях и их последствиях, историческая информация о силах и средствах постоянной готовности, а также статистическая информация о результатах их деятельности, направленной на предупреждение и ликвидацию чрезвычайных ситуаций и происшествий, сведения о динамических параметрах процессов развития чрезвычайных ситуаций и происшествий за определенный исторический период времени. В учетную информацию в

обязательном порядке включаются данные об административно-территориальных образованиях, об организациях и их деятельности, о численности и составе населения административно-территориальных образований, а также данные о численности работников организаций.

1.3.2 Определение требований к содержанию информации, передаваемой от действующих АС в АПК «Безопасный город»

1.3.2.1 Требования к содержанию входной информации от действующих АС, относящейся к категории оперативной.

а) Информация от систем видеомониторинга и видеоанализа в целях общественной безопасности должна содержать:

- видеоизображения с мест установки видеокамер на критически важных, потенциально опасных и социально значимых объектах (в том числе дошкольные образовательные учреждения, образовательные учреждения и другие);
- информацию об идентификации и распознавании лиц и сопоставление их с данными о лицах находящихся в розыске.
- информацию об обнаружении скопления людей, в том числе в несанкционированных местах;
- данные об оценке плотности потока людей на значимых для муниципального образования объектах;
- факты обнаружения движения человека против направления потока;
- факты обнаружения движения человека с высокой скоростью (бегущий человек);
- факты обнаружения оставленных предметов;
- факты обнаружения повышенной активности людей в контролируемой зоне;
- факты обнаружения исчезнувших предметов;

- факты обнаружения появления человека или автомобиля в зоне наблюдения (улицы, площади, перекрестки, парки);

- технологическая информация о состоянии систем видеомониторинга и видеоанализа.

б) Информация от систем видеомониторинга и видеоанализа в интересах обеспечения правопорядка, профилактики правонарушений на дорогах должна содержать:

- данные фиксации в автоматическом режиме правонарушений в области дорожного движения и передачу полученной информации в центры автоматизированной фиксации нарушений правил дорожного движения;

- данные фиксации проходящих транспортных средств;

- данные выявления потенциально опасных событий на дорогах и объектах транспортной инфраструктуры железнодорожного, водного, воздушного и автомобильного транспорта, метрополитена и дорожного хозяйства в режиме реального времени;

- данные анализа информации о дорожной ситуации в режиме реального времени;

- данные результатов проверки транспортных средств на предмет имеющихся правонарушений, угона и прочих.

в) Информация от систем мониторинга в интересах защиты от чрезвычайных ситуаций природного и техногенного характера и пожаров должна содержать:

- информацию от систем: пожарной сигнализации; метеорологических датчиков; гидропостов и гидродатчиков; химических датчиков расположенных на территории муниципального образования;

- информацию мониторинга доступа на охраняемые государственные объекты а именно событий несанкционированного проникновения в охраняемую зону (нарушение периметра);

- информацию мониторинга природных пожаров как от локальных систем, так и федеральных информационных систем;

- информацию акустического мониторинга (крики, удары, хлопки, выстрелы, бой стекла).

в) Информация от систем мониторинга коммунальной инфраструктуры должна содержать:

- информацию об аварийных и нештатных ситуациях в сфере коммунальной инфраструктуры;

- данные об объемах потребляемой электрической энергии, расчеты за которую осуществляются с использованием приборов учета (в части многоквартирных домов - с использованием коллективных (общедомовых);

- данные об объемах потребляемой тепловой энергии, расчеты за которую осуществляются с использованием приборов учета (в части многоквартирных домов - с использованием коллективных (общедомовых) приборов учета);

- данные об объемах потребляемой воды, расчеты за которую осуществляются с использованием приборов учета (в части многоквартирных домов - с использованием коллективных приборов учета);

- данные об объемах потребляемого природного газа, расчеты за который осуществляются с использованием приборов учета (в части многоквартирных домов - с использованием индивидуальных и общих (для коммунальной квартиры) приборов учета);

- данные о величинах давления в трубопроводах;

- данные о величинах теплоносителя в трубопроводах.

г) Информация от систем мониторинга обеспечения безопасности имущественного комплекса МО должна содержать:

- данные санитарно-эпидемиологического контроля, в том числе мониторинга заболеваемости населения, инфекционных, паразитарных болезней и отравлений людей, особо опасных болезней сельскохозяйственных животных и рыб, карантинных и особо опасных болезней;

- данные из реестра объектов капитального строительства с указанием расположения внутренних инженерных коммуникаций;

- данные из реестра технических условий по различным видам инженерного обеспечения объектов капитального строительства и земельных участков;
- данные реестровой и пространственной информации об объектах электроснабжения и электросетях;
- данные реестра ремонтных работ на объектах энергетической инфраструктуры;
- данные реестра и пространственной информации об объектах водоснабжения;
- паспортные данные объектов водоснабжения;
- данные гидравлического расчета сетей водоснабжения;
- данные реестровой и пространственной информации об объектах теплоснабжения;
- паспортные данные объектов теплоснабжения;
- данные теплогидравлического расчета сетей теплоснабжения;
- данные реестра ремонтных работ объектов теплоснабжения;
- реестровую и пространственную информацию об объектах транспортной инфраструктуры;
- паспортные данные объектов транспортной инфраструктуры;
- данные из реестра ремонтных работ транспортной инфраструктуры;
- реестровую и пространственную информацию об объектах телекоммуникации;
- паспорта объектов телекоммуникации;
- реестры ремонтных и строительных работ объектов телекоммуникации;
- данные реестровой и пространственной информации об объектах социальной сферы, а именно детских дошкольных учреждениях, школах, лечебно-профилактических учреждениях, спортивных учреждениях, базах отдыха;

- данные из базы данных персонала, аккредитованного к работе на объектах социальной сферы;
- данные из базы данных демографических и социальных характеристик населения;
- данные реестров мест обработки и утилизации отходов;
- данные реестров природоохранных и рекреационных зон и паркового хозяйства в составе:
 - данные об особо охраняемых территориях, зеленых насаждениях, парках и рекреационных зонах;
 - данные из базы данных о промышленных предприятиях и их влиянии на экологию;
 - оперативные данные от государственных информационных систем, приведенных в таблице 1.

Таблица 1

Информационная система	Ответственный ФОИВ	Поставляемые данные
1 Информационно-аналитическая система	Минздрав России	<ul style="list-style-type: none"> - Данные мониторинга реализации государственного задания по оказанию высокотехнологичной медицинской помощи за счет средств федерального бюджета; - Данные Федерального регистра медицинского персонала; - Данные Федерального регистра стационарного больного с острым нарушением мозгового кровообращения; - Данные подсистемы мониторинга санаторно-курортного лечения; - Данные подсистемы мониторинга проведения диспансеризации детей-сирот и детей, находящихся в трудной жизненной ситуации; - Подсистема ведения счетов за оказанные услуги по талонам на оказание ВТМП на

Информационная система	Ответственный ФОИВ	Поставляемые данные
		<p>основании государственного задания;</p> <ul style="list-style-type: none"> - Данные федерального регистра больных социально-значимыми заболеваниями
2 Комплекс программных средств по ведению паспортов медицинских учреждений	Минздрав России	Данные паспортов медицинских учреждений
3 ЕМИСС	Минкомсвязь России	Данные официальной статистической информации, включая метаданные, формируемые в соответствии с федеральным планом статистических работ.
4 ИОД	Минкомсвязь России	Данные о программно-технических средствах и информационных ресурсах инфраструктуры общественного доступа к информации о деятельности органов государственной власти и органов местного самоуправления и к их услугам, предоставляемым с помощью сети Интернет. Информация о конфигурации и состоянии программно-аппаратных компонентов центров общественного доступа на базе инфоматов
5 ЕПГУ	Минкомсвязь России	Данные мониторинга хода предоставления государственных услуг или исполнения государственных функций.
6 ЕСИА	Минкомсвязь России	Протоколы идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.
7 СМЭВ	Минкомсвязь России	Протоколы Системы межведомственного электронного взаимодействия
8 ГИС ЖКХ	Минкомсвязь России, Минстрой России	Данные государственной информационной системы жилищно-коммунального хозяйства о жилищном фонде и работах по

Информационная система	Ответственный ФОИВ	Поставляемые данные
		содержанию и ремонту общего имущества в многоквартирных домах.
9 ИС Россвязи	Минкомсвязь России, Россвязь	Данные реестра сетей связи. Данные реестра почтовых индексов. Данные реестра российской системы и плана нумерации.
10 ИС АКНД ОУ	Минобрнауки России, Рособрнадзор	Данные электронных досье образовательных учреждений.
11 СООИ Минприроды России	Минприроды России	Данные оперативной информации о состоянии природных ресурсов и окружающей среды, включая данные о чрезвычайных ситуациях и их последствиях. Данные о состоянии природных ресурсов и окружающей среды. Результаты прогнозирования развития ситуаций и событий на основе пространственного моделирования по комплексу разнородных данных.
12 АИС ГВР	Минприроды России, Росводресурсы	Сведения о водных объектах, о водопользователях и инфраструктуре на водных объектах. Ретроспективная документированная информация о водных объектах, о водопользователях.
13 ИС ОД	Минприроды России, Росводресурсы	Информация о чрезвычайных ситуациях и происшествиях в сфере деятельности Росводресурсов.
14 ГИС Росводресурсов	Минприроды России, Росводресурсы	<p>Пространственные данные, необходимые по водным ресурсам, включая данные о противопаводковых мероприятиях, мероприятиях по проектированию и установлению водоохранных зон водных объектов и их прибрежных защитных полос, мероприятиях по предотвращению и ликвидации вредного воздействия вод.</p> <p>Тематические подборки картографических материалов для информационной поддержки стратегического управления водными ресурсами. Данные результатов моделирования и прогнозирования последствий аварий.</p> <p>Данные результатов моделирования зон затопления и подтопления при строительстве гидротехнических сооружений, при разрушении</p>

Информационная система	Ответственный ФОИВ	Поставляемые данные
		гидротехнических сооружений и в паводковых ситуациях. Данные результатов моделирования распространения опасных загрязнений в водных объектах и при угрозе попадания в водные объекты.
15 ИАС 2-тп (водхоз)	Минприроды России, Росводресурсы	Данные официальной статистической информации об использовании вод в Российской Федерации по уровням и группировкам, определенным Федеральным планом статистических работ и в соответствии с водохозяйственным районированием Российской Федерации. Данные по изменению показателей водопотребления и водоотведения, в том числе сброса загрязняющих веществ, по годам.
16 АИС ГМВО	Минприроды России, Росводресурсы	Данные о водном объекте, об общей оценке и результатам прогнозирования изменения состояния водных объектов, дна, берегов водных объектов, их морфометрических особенностей, водоохраных зон водных объектов, данные о количественных и качественных показателях состояния водных ресурсов, состояния водохозяйственных систем, в том числе гидротехнических сооружений.
17 ЕСИМО	Минприроды России, Росгидромет	Данные о состоянии морской среды и морской деятельности, полученной в результате наблюдений.
18 АС ПГУ МЭВ Росгидромета	Минприроды России, Росгидромет	Информация о состоянии атмосферного воздуха и его загрязнений. Информация о состоянии поверхностных водных объектов и их загрязнении
19 ИСДМ - Рослесхоз	Минприроды России, Рослесхоз	Данные наземных, авиационных и космических наблюдений (топоосновы, ДЗЗ и атрибутивных данных). Данные по динамике изменений лесного фонда, не связанной с воздействием лесных пожаров.

Информационная система	Ответственный ФОИВ	Поставляемые данные
20 ИС "Учет и баланс подземных вод"	Минприроды России, Роснедра	Данные результатов учета, оценки состояния и степени использования ресурсной базы подземных вод Российской Федерации в системе управления их воспроизводством и рациональным использованием. Данные государственного кадастра месторождений подземных вод, государственного учета и баланса их запасов, планирования использования ресурсов и запасов подземных вод
21 ПТК Госконтроль	Минприроды России, Росприроднадзор	Данные реестра объектов, оказывающих негативное воздействие на окружающую среду и вредное воздействие на атмосферный воздух. Информация о нормах воздействия на окружающую среду. Данные отчетности природопользователей об образовании, использовании, обезвреживании, о размещении отходов субъектами малого и среднего предпринимательства. Данные сводных отчетов по негативному воздействию на окружающую среду.
22 АИС РФС АПК	Минсельхоз России	Сведения о подведомственных Минсельхозу России организациях, о переданном им федеральном имуществе. Данные реестра федеральной собственности агропромышленного комплекса, включая геопространственные данные о дислокации контуров земельных участков.
23 СДМЗ	Минсельхоз России	Информация о состоянии земель сельскохозяйственного назначения и растительности на этих землях. Данные результатов тематической обработки данных дистанционного зондирования земель; Данные оценки состояния растительности и площади, занятой культурами в разрезе пяти циклов съемки на уровне федерального округа, субъекта РФ, района, хозяйства и отдельного поля;

Информационная система	Ответственный ФОИВ	Поставляемые данные
		Данные влияния чрезвычайных ситуаций на сельскохозяйственные угодья и оценка ущерба, нанесенного чрезвычайными ситуациями сельскохозяйственным угодьям.
24 АИС НСИ	Минсельхоз России	Данные реестров, регистров, справочников, классификаторов объектов контролируемых Минсельхозом России
25 АИС РФС АПК	Минсельхоз России	Сведения о подведомственных Минсельхозу России организациях, о переданном им федеральном имуществе. Данные реестра федеральной собственности агропромышленного комплекса, включая геопространственные данные о дислокации контуров земельных участков.
26 СДМЗ	Минсельхоз России	Информация о состоянии земель сельскохозяйственного назначения и растительности на этих землях. Данные результатов тематической обработки данных дистанционного зондирования земель; Данные оценки состояния растительности и площади, занятой культурами в разрезе пяти циклов съемки на уровне федерального округа, субъекта РФ, района, хозяйства и отдельного поля; Данные влияния чрезвычайных ситуаций на сельскохозяйственные угодья и оценка ущерба, нанесенного чрезвычайными ситуациями сельскохозяйственным угодьям.
27 ГИС "Деметра"	Минсельхоз России, Россельхознадзор	Информация о состоянии земель сельскохозяйственного назначения фитосанитарных и ветеринарных карантинных зонах и объектах
28 СС-ТМК	Минтранс России	Сведения поступающие из инженерно-технических средств обеспечения транспортной безопасности и иных автоматизированных систем технического мониторинга и контроля,

Информационная система	Ответственный ФОИВ	Поставляемые данные
		используемых на объектах транспортной инфраструктуры
29 ЕГИС ОТБ	Минтранс России	Сведения об опасных объектах транспортной инфраструктуры и транспортных средствах; Сведения об аварийных ситуациях и действиях диспетчерских, аварийных и технических служб объектов; Результаты расчетов прогнозов развития чрезвычайных ситуаций Информация об объектах транспортной инфраструктуры и транспортных средствах (паспорта объектов); Данные о категорировании транспортной инфраструктуры и транспортных средств; Сведения мониторинга состояния защищенности объектов транспортной инфраструктуры
30 АБДД Дорога	Минтранс России, Росавтодор	Данные автоматизированного банка дорожных данных об автомобильных дорогах, искусственных сооружениях, движении автотранспортных средств, ДТП, объектах сервиса и др. Данные диагностики технического состояния автомобильных дорог общего пользования Российской Федерации, о наличии аварийных участков и потребности в дорожных работах.
31 ЕАВИИАС МСЭ	Минтруд России	Данные статистической и аналитической отчетности
32 АИС ЕСУИ	Минтруд России	Данные единой системы учета инвалидов в Российской Федерации
33 АИС "Миграпотоки"	Минтруд России	Данные о количественных показателях трудовых миграционных потоков граждан, осуществляющих трудовую деятельность вне места постоянного проживания

Информационная система	Ответственный ФОИВ	Поставляемые данные
34 ФГИС ТП	Минэкономразвития России	Данные (слои) единой информационной системы территориального планирования Российской Федерации, информация о состоянии, использовании и планируемом развитии территорий.
35 ПК ПВД	Минэконом-развития России, Росреестр	Данные информационных систем государственного кадастра недвижимости и государственной регистрации прав для нужд Росреестра
36 АИС "Электронный инспектор"	МЧС России	Данные состояния пожарной безопасности объектов защиты и результатов надзорной деятельности на объектах защиты
37 ИАС-ДТП	МЧС России	<p>Данные о реагировании пожарно-спасательных подразделений на ДТП. Результаты расчета компьютерных моделей типовых сценариев дорожно-транспортных происшествий при перевозках опасных грузов. Доступ к электронной библиотеке работ, выполненных МЧС России в рамках ФЦП «Повышение безопасности дорожного движения в 2006-2012 годах».</p> <p>Доступ к Банку данных объектов инфраструктуры, связанных с оказанием помощи лицам, пострадавшим в ДТП, вдоль автомобильных дорог.</p> <p>Данные мониторинга реализации региональных целевых программ в области безопасности дорожного движения.</p>
38 ФБД "ПОЖАРЫ"	МЧС России	Данные единой государственной системы статистического учета пожаров и последствий от них в Российской Федерации
39 ИВС Росстата	Росстат	<p>Данные каталога статистических показателей (КСП).</p> <p>Данные Объединенной системы регистров (ОСР), включая информацию БД "Индивидуальные предприниматели"; БД "Юридические лица".</p>

Информационная система	Ответственный ФОИВ	Поставляемые данные
		Данные центральной базы статистических данных (ЦБСД). Данные БД "Показатели муниципальных образований". Данные региональной базы статистических данных (РБСД). Данные отраслевой базы статистических данных.

1.3.2.2 Входная информация от действующих АС, относящаяся к категории нормативно-справочной.

Для обеспечения деятельности АПК «Безопасный город» в едином информационном пространстве РСЧС необходима постоянная поддержка информационного обеспечения АПК «Безопасный город» в актуальном состоянии.

Информационное обеспечение - это совокупность форм документов, классификаторов, нормативной базы (компоненты информационного обеспечения) и реализованных решений по объемам, размещению и формам существования информации, применяемой при функционировании АПК «Безопасный город».

Информационное единство АПК «Безопасный город» в системе РСЧС должно обеспечиваться использованием общей системы кодирования и классификации информации.

Единая система кодирования и классификации информации должна обеспечивать:

централизованное ведение словарей и классификаторов, использующихся в информационном взаимодействии;

выполнение необходимых технологических функций, в том числе предоставление возможности обмена данными с внешними по отношению к АПК «Безопасный город».

В состав информационного обеспечения АПК «Безопасный город» входят:

- информационная база (ИБ), представляющая собой совокупность баз данных (БД) и массивов (массивов документов) с оперативной информацией (ОИ) и условно-постоянной информацией (УПИ);

- документация с решениями по объемам, размещению и формам существования ОИ и УПИ.

Условно-постоянная информация. К УПИ относятся:

- системные классификаторы;
- унифицированные формы документов (УФД), формируемые в соответствии с установленным регламентом;
- нормативная информация;
- нормативно-справочная информация (НСИ);
- цифровая информация о местности (ЦИМ);
- библиотеки электронных условных знаков обстановки.

В интересах поддержания нормативно-справочной информации АПК «Безопасный город» в актуальном состоянии АПК должен получать из внешних систем следующие данные:

а) Данные общероссийских классификаторов (периодическая загрузка), перечень которых должен включать следующие классификаторы:

- объектов административно-территориального деления (ОКАТО)
- видов экономической деятельности (ОКВЭД)
- основных фондов (ОКОФ)
- продукции (ОКП)
- стран мира (ОКСМ)
- управленческой документации (ОКУД)
- услуг населению (ОКУН)
- единиц измерения (ОКЕИ)
- специальностей по образованию (ОКСО)
- видов экономической деятельности, продукции и услуг (ОКДП)
- форм собственности (ОКФС)
- территорий муниципальных образований (ОКТМО)

- информации о населении (ОКИН)

б) Данные от государственных информационных систем, состав информации которых определяется назначением данных систем.

1.4 Алгоритм информационного обмена действующих автоматизированных систем с АПК «Безопасный город»

1.4.1 Техническая основа информационного обмена

Информационно-телекоммуникационная инфраструктура АПК «Безопасный город» является технической основой информационного обмена. Для обеспечения информационного обмена могут использоваться сети электросвязи следующих категорий:

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

Информационное взаимодействие систем в составе АПК «Безопасный город» осуществляется посредством передачи данных между соответствующей АС и интеграционной шиной в составе АПК «Безопасный город».

Для передачи данных между системами и интеграционной шиной должны использоваться web-сервисы, которые будут обмениваться между собой XML-сообщениями по протоколу SOAP. Для этого на каждом из серверов сопрягаемых систем и интеграционной шины должны быть размещены WSDL-описание web-сервисов.

Все web-сервисы, которые предназначены для передачи данных от взаимодействующих систем и обратно, реализуются на стороне интеграционной шины.

При этом на стороне каждой из взаимодействующих систем может быть реализован один единственный сервис, который будет вызываться сервером доступа сопрягаемой системы и который обеспечивает прием соответствующей системой асинхронной квитанции событийного оповещения. В том случае, если для взаимодействующей системы по каким-либо причинам не удастся реализовать программный интерфейс сетевого взаимодействия, на ее стороне должен быть организован клиентский сокет, в который интеграционная шина будет выдавать необходимую информацию.

1.4.2 Алгоритм информационного обмена

Предлагается В АПК «Безопасный город» использовать следующий алгоритм информационного обмена.

1) Взаимодействующая система передает в интеграционную шину АПК «Безопасный город» требуемые данные путем вызова соответствующего метода web-сервиса, реализованного на стороне интеграционной шины.

2) При появлении в базе данных интеграционной шины, которые необходимо передать во взаимодействующую систему, интеграционная шина вызывает метод web-сервиса или выдает в клиентский сокет в адрес соответствующей системы, в который передает информацию о появлении в БД информационного ресурса, интересующего систему. При этом передается идентификатор этого информационного ресурса.

3) После того, как взаимодействующая система получила оповещение о появлении интересующего информационного ресурса, она вызывает соответствующий метод web-сервиса, который возвращает запрашиваемую структуру данных.

4) В случае, если система сама знает данные, которые ей необходимо запросить из интеграционной шины, она может вызывать соответствующий метод web-сервиса, который возвращает запрашиваемую структуру данных. При

этом в качестве параметра передается идентификатор запрашиваемых данных в контексте хранилища интеграционной шины.

1.5 Требования к организации обмена данными между действующими АС различной ведомственной принадлежности на муниципальном и региональном уровне и системами в составе АПК «Безопасный город».

Обмен данными между действующими АС и АПК «Безопасный город» можно классифицировать следующим образом:

- организационные;
- технические;
- безопасности данных.

К организационным требованиям относится наличие согласованного протокола информационно-технического взаимодействия, который должен освещать следующие аспекты информационно-технического взаимодействия:

-назначение протокола и на основании каких документов он разработан, кем разработан, в каких целях и порядок его уточнения и изменения (при необходимости);

- порядок информационного взаимодействия;
- способ адресования передаваемых данных;
- состав, структуры и форматы представления передаваемых данных;
- чем достигается информационная совместимость взаимодействующих систем;

-чем достигается организационная совместимость взаимодействующих систем;

- перечень КСА взаимодействующих систем, между которыми обеспечивается обмен информацией и их оснащения средствами автоматизации и связи;

- перечень сообщений взаимообмена между взаимодействующими системами, требования к их информационному содержанию;

- регламент информационного обмена;
- чем достигается информационно - лингвистическая совместимость взаимодействующих систем;
- правила конвертирования информационных объектов;
- порядок изменения протокола;
- обеспечение защиты информации;
- чем достигается телекоммуникационной совместимость.

К техническим требованиям относится наличие инфраструктуры взаимодействия систем и программных средств обеспечения взаимодействия.

К требованиям обеспечения безопасности данных при взаимообмене относится необходимость предъявления и дальнейшей реализации, как в средствах сопряжения, так и во взаимодействующих системах требований защиты информации от НСД, определенных в следующих руководящих документах:

- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (РД АС) – определяет требования безопасности, в целом, предъявляемые к взаимодействующим изделиям. В части касающейся, указанный документ определяет требования по обеспечению идентификации, аутентификации и контролю потоков информации по уровням ЭМВОС.

- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (РД СВТ) – определяет функциональные требования безопасности (в том числе требования идентификации, аутентификации, регистрации, политики разграничения доступа, целостности) и требования доверия к программному обеспечению, реализующему защищенную обработку и алгоритмы передачи информации между взаимодействующими изделиями.

- «Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (РД НДВ) – определяет требования в части контроля недеklarированных возможностей программного обеспечения средств информационно-технического взаимодействия.

- «Средства вычислительной техники. Межсетевые экраны. Защиты от НСД к информации. Показатели защищенности от НСД к информации» (РД МЭ) – определяет функциональные требования (в том числе, требования по фильтрации потоков по уровням ЭМВОС) и требования доверия к специализированным устройствам защиты межсетевого взаимодействия (межсетевым экранам и фильтрующим маршрутизаторам).

- Руководящий документ Гостехкомиссии РФ «Концепция защиты информации в средствах вычислительной техники и автоматизированных системах» – определяет стандартную классификацию возможностей нарушителя, в рамках которых реализуются угрозы несанкционированного доступа и технические каналы утечки информации при взаимодействии сопрягаемых изделий.

- Руководящий документ Гостехкомиссии РФ «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам» (СТР–97) – определяет требования и рекомендации по технической защите информации и защите от НСД (в том числе, требования по сопряжению локальных сетей).

- ГОСТ ИСО/МЭК 7498–2–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть II. Архитектура защиты информации – определяет номенклатуру механизмов и функций безопасности при сетевом взаимодействии распределенных систем. В данном документе содержится рекомендуемое распределение механизмов защиты по уровням ЭМВОС. При этом содержание указанных рекомендаций определяет возможное пространство решений по защите информации для произвольной

конфигурации угроз, но не специфицирует требования конкретных систем и не дает классификацию и оценку уровня защищенности тех или иных решений.

- ГОСТ Р 51275–99. Защита информации. Объект автоматизации. Факторы, воздействующие на информацию. Общие положения – определяет структуру угроз, компрометирующих информацию при обработке, передаче и хранении в распределенных компьютерных системах.

В рамках информационного обмена необходимо обеспечить:

- Целостность и конфиденциальность информации при передаче по открытым каналам и сетям передачи данных;

- Защиту информации от НСД и разграничение прав доступа при передаче между взаимодействующими системами, в том числе, за счет нарушения принятых правил адресования и маршрутизации;

- Контроль потоков информации по меткам конфиденциальности в процессе передачи из системы отправителя в систему получатель через телекоммуникационную инфраструктуру;

- Защиту локально обрабатываемой в сопрягаемых системах информации от несанкционированной передачи за пределы сетевого периметра взаимодействующих систем;

- Защиту программной среды КСА взаимодействующих систем от внедрения деструктивных программных воздействий (вирусов);

- Целостность аппаратно-программных средств, в том числе, контроль правильности начальной загрузки КСА из состава взаимодействующих изделий;

- Управление и контроль безопасности функционирования КСА взаимодействующих систем, обнаружение и анализ инцидентов безопасности, оперативное реагирование на возникающие угрозы;

- Защиту обрабатываемой и передаваемой информации от технических каналов утечки информации (каналов ПЭМИН) в комплексах аппаратных средств.

В рамках защиты информации от НСД применительно к организации информационного взаимодействия должна быть разработана модель нарушителя

и модель защиты, которые должны идентифицировать возможные угрозы, возможности по их использованию, меры безопасности и обоснование их достаточности.

С целью взаимоувязанного анализа и описания указанных вопросов в рамках обеспечения комплексной системы защиты информации целесообразно воспользоваться методологией и подходами, предложенными ГОСТ ИСО/МЭК 15408–2002 для спецификации профилей (пакетов) защиты и заданий по безопасности.

В рамках подходов ГОСТ Р ИСО/МЭК 15408–2002 модель нарушителя строится исходя из взаимоувязанного и непротиворечивого описания предположений безопасности, структуры угроз и политики безопасности.

Предположения безопасности устанавливают основные допущения о среде функционирования взаимодействующих изделий, влияющие на безопасность информации. В число предположений безопасности целесообразно включать выполнение требований нормативных документов по режиму и безопасности, которые не зависят от особенностей применяемых информационных технологий (организационные меры режима секретности на объектах, меры защиты от ИТР, защита и аттестация аппаратных для работы по закрытым каналам связи).

Угрозы – определяются уязвимостями, используемыми нарушителем для компрометации информационных ресурсов (активов), или выполнения НСД. Угрозы безопасности информации классифицируются следующим образом:

- угрозы конфиденциальности (несанкционированное чтение), целостности (навязывание и имитация) и доступности (нарушение работы системы и уничтожение информации);

- угрозы, обусловленные действиями пользователей, службы эксплуатации и поставщиков (производителей) технических средств и программного обеспечения;

- угрозы, обусловленные умышленными и неумышленными (при наличии явной мотивации) действиями должностных лиц.

Политика безопасности – определяет критерии безопасности взаимодействия, выраженные в форме функциональных правил и условий, которые должны быть реализованы в средствах (комплексах) защиты взаимодействия. Применительно к рассматриваемой задаче политика безопасности определяет правила идентификации, аутентификации взаимодействующих объектов, таблицу разграничения доступа, а также мандатные параметры, управляющие передачей потоков классифицированной информацией между взаимодействующими изделиями.

В рамках структуры профилей и заданий по безопасности ГОСТ Р ИСО/МЭК 15408–2002 модель защиты предполагает установление следующих отношений:

- отношение между структурой угроз и политикой безопасности с одной стороны и целями безопасностями (для средств защиты взаимодействия и среды их применения) при заданных предположениях безопасности с другой стороны;

- отношение между целями и требованиями безопасности (для средств защиты взаимодействия и среды их применения) для установленной политики и угрозами безопасности.

Полнота моделей защиты согласно ГОСТ ИСО/МЭК 15408-2002 обеспечивается исходя из выполнения следующих условий:

- каждая из угроз и каждое из правил политики безопасности отображается, по крайней мере, на одну цель безопасности (для средств защиты взаимодействия или среды их применения);

- для каждой цели безопасности указывается, по крайней мере, одно требование безопасности, выполнение которого позволяет достигнуть указанной цели.

Для формирования каталога функциональных требований безопасности и требований доверия безопасности предлагается использовать:

- руководящие и нормативные документы по защите информации-данные источники требований применяются для достижения базовых целей безопасности функционирования;

- механизмы и функции защиты, необходимость применения которых вытекает из анализа отдельных аспектов взаимодействия, не покрываемых либо не подлежащих интерпретации в рамках требований нормативных документов по защите информации от НСД;

- механизмы и функции защиты информации, предлагаемые к реализации в системно-образующих компонентах АПК «Безопасный город».

2 ПРЕДЛОЖЕНИЯ ПО ПРИМЕНЕНИЮ ДЕЙСТВУЮЩИХ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ УПРАВЛЯЮЩИХ И ДРУГИХ СИСТЕМ ДЛЯ ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ И ПРОИСШЕСТВИЙ, ОБЕСПЕЧЕНИЯ ПРАВОПОРЯДКА В СОСТАВЕ АПК «БЕЗОПАСНЫЙ ГОРОД»

2.1 Анализ действующих и перспективных автоматизированных информационно-управляющих систем различной ведомственной принадлежности на муниципальном и региональном уровне на предмет соответствия их функциональных характеристик требованиям, указанным в Концепции построения и развития АПК «Безопасный город»

2.1.1 Исходные данные анализа

Предложения по применению действующих систем базировались на результатах анализа технических заданий на создание АПК «Безопасный город» муниципальных образований.

В ходе выполнения данной работы всего было проанализировано более 150 технических заданий, включающих более 200 пилотных муниципальных образований. Распределение обследованных пилотных муниципальных образований по регионам России показано на карте (рисунок 2.1).

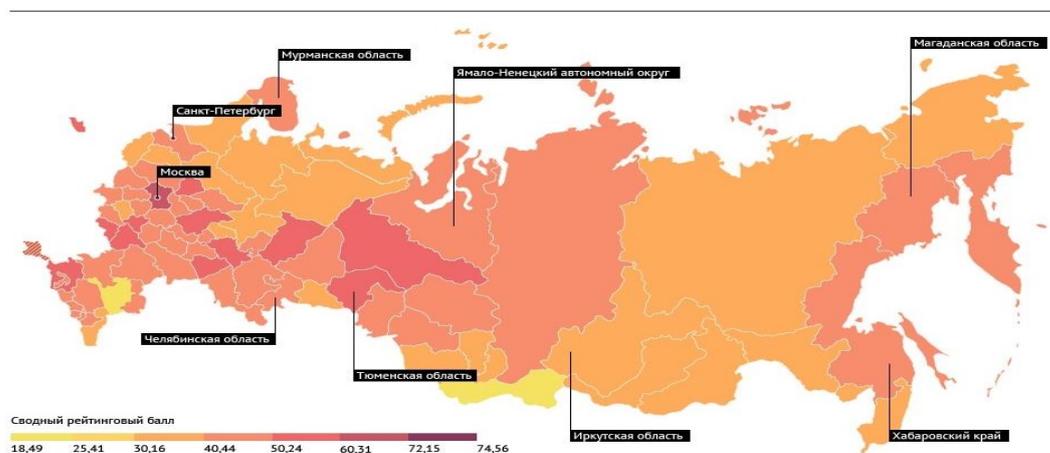


Рисунок 2.1 — Распределение обследованных муниципальных образований.

Из рисунка видно, что в целом, обследования проведены относительно равномерно по все территории России. В тоже время можно отметить наиболее высокую плотность представленных технических заданий из Центрального региона и наименьшую плотность Красноярского края и Тюменской области.

Обследования ИТ инфраструктуры дежурных, диспетчерских и экстренных служб МО и анализ разделов ТЗ с описанием действующих АС выявили следующее. Различные ДДС МО используют АС различных уровней и различной ведомственной принадлежности.

Общее соотношение обследованных МО Сведения по численности обследовав различных ФО показано на рисунке 3.2.



Рисунок 2.2 – Соотношение обследованных МО в различных ФО

На диаграмме видно, что наибольшее число МО представлено в Центральном и Южном ФО, а наименьшее в Уральском и Приволжском. В тоже время статистическая проверка подтвердила гипотезы о статистической однородности выборок.

Таким образом, объем, состав и качество выборочных данных по обследованиям ИТ инфраструктуры дежурных, диспетчерских и экстренных служб муниципальных образований является достаточным и в дальнейшем позволяет результаты, полученные по данным выборочным обследованиям, распространять на всю совокупность МО России. результаты анализа и других

исследований могут быть распространены на всю совокупность МО, охватываемых проектом АПК «Безопасный город».

2.1.2 Функциональные подсистемы АПК "Безопасный город"

2.1.2.1 Функциональные задачи комплекса "Безопасный город" сгруппированы по следующим блокам:

- безопасность населения и муниципальной (коммунальной) инфраструктуры;
- безопасность на транспорте;
- экологическая безопасность;
- координация работы служб и ведомств и их взаимодействие.

Детализация требований к функциональным блокам АПК «Безопасный город» представлена в «Приложении Б».

Анализ соответствия функций действующих АС требованиям к АПК «Безопасный город» приведен в таблице 2.

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
1 Информационно-аналитическая система Министерства здравоохранения Российской Федерации Минздрав России	<ul style="list-style-type: none"> - Данные мониторинга реализации государственного задания по оказанию высокотехнологичной медицинской помощи за счет средств федерального бюджета; - Данные Федерального регистра медицинского персонала; - Данные Федерального регистра стационарного больного с острым нарушением мозгового кровообращения; - Данные подсистемы мониторинга санаторно-курортного лечения; - Данные подсистемы мониторинга проведения диспансеризации детей-сирот и детей, находящихся в трудной жизненной ситуации; - Подсистема ведения счетов за оказанные услуги по талонам на оказание ВТМП на основании государственного задания; - Данные федерального регистра больных социально-значимыми заболеваниями 	+			+	XML; DOC; RTF; PDF; JPEG Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
2 Комплекс программных средств по ведению паспортов медицинских учреждений Минздрав России	Данные паспортов медицинских учреждений	+			+	XML; DOC; RTF; PDF; JPEG Интеграционная платформа (интеграционная шина)
3 ЕМИСС Минкомсвязь России	Данные официальной статистической информации, включая метаданные, формируемые в соответствии с федеральным планом статистических работ.				+	XML Интеграционная платформа (интеграционная шина)
4 ИОД Минкомсвязь России	Данные о программно-технических средствах и информационных ресурсах инфраструктуры общественного доступа к информации о деятельности органов государственной власти и органов местного самоуправления и к их услугам, предоставляемым с помощью сети Интернет. Информация о конфигурации и состоянии программно-аппаратных компонентов центров общественного доступа на базе инфоматов				+	XML; DOC; RTF; PDF Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
5 ЕПГУ Минкомсвязь России	Данные мониторинга хода предоставления государственных услуг или исполнения государственных функций.				+	XML; DOC; RTF; PDF Интеграционная платформа
6 ЕСИА Минкомсвязь России	Протоколы идентификации и аутентификации в инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.	+			+	XML; DOC; RTF Интеграционная платформа (интеграционная шина)
7 СМЭВ Минкомсвязь России	Протоколы Системы межведомственного электронного взаимодействия				+	XLS; HTML; DOC; DOCX; RTF; GIF; JPEG; PNG; PDF; XML; XLSX
8 ГИС ЖКХ Минкомсвязь России, Минстрой России	Данные государственной информационной системы жилищно-коммунального хозяйства о жилищном фонде и работах по содержанию и ремонту общего имущества в многоквартирных домах.	+			+	HTML; XLS; ZIP; TIF; DOC; DOCX; RTF; PDF; JPEG; JPEG 2000; JPG; XLSM; XLSB; dbf; XML

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
9 ИС Росвязи Минкомсвязь России, Росвязь	Данные реестра сетей связи. Данные реестра почтовых индексов. Данные реестра российской системы и плана нумерации.	+			+	DOC; RTF; TIFF
10 ИС АКНД ОУ Минобрнауки России, Рособнадзор	Данные электронных досье образовательных учреждений.	+			+	XLS; HTML; DOC; DOCX; RTF; GIF; JPEG; PNG; PDF; XML; XLSX
11 СООИ Минприроды России Минприроды России	Данные оперативной информации о состоянии природных ресурсов и окружающей среды, включая данные о чрезвычайных ситуациях и их последствиях. Данные о состоянии природных ресурсов и окружающей среды. Результаты прогнозирования развития ситуаций и событий на основе пространственного моделирования по комплексу разнородных данных.	+			+	HTML; XLS; ZIP; TIF; DOC; DOCX; RTF; PDF; JPEG; JPEG 2000; JPG; XLSM; XLSB; dbf; XML

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
12 АИС ГВР Минприроды России, Росводресурсы	Сведения о водных объектах, о водопользователях и инфраструктуре на водных объектах. Ретроспективная документированная информация о водных объектах, о водопользователях.					DOC; RTF; TIFF
13 ИС ОД Минприроды России, Росводресурсы	Информация о чрезвычайных ситуациях и происшествиях в сфере деятельности Росводресурсов.					DOC; RTF; TIFF
14 ГИС Росводресурсов Минприроды России, Росводресурсы	Пространственные данные, необходимые по водным ресурсам, включая данные о противопаводковых мероприятиях, мероприятиях по проектированию и установлению водоохранных зон водных объектов и их прибрежных защитных полос, мероприятиях по предотвращению и ликвидации вредного воздействия вод. Тематические подборки картографических материалов для информационной поддержки стратегического управления водными ресурсами. Данные результатов моделирования и прогнозирования последствий аварий. Данные результатов моделирования зон затопления и подтопления при строительстве гидротехнических сооружений, при разрушении гидротехнических сооружений и в паводковых ситуациях. Данные результатов моделирования распространения опасных загрязнений в водных	+		+	+	ArcGIS Server 9.2; 7zip, Ccleaner, Python 2.5, LogMeIn Hamachi Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	объектах и при угрозе попадания в водные объекты.					
15 ИАС 2-тп (водхоз) Минприроды России, Росводресурсы	Данные официальной статистической информации об использовании вод в Российской Федерации по уровням и группировкам, определенным Федеральным планом статистических работ и в соответствии с водохозяйственным районированием Российской Федерации. Данные по изменению показателей водопотребления и водоотведения, в том числе сброса загрязняющих веществ, по годам.	+		+	+	Внутренний формат данных ИС
16 АИС ГМВО Минприроды России, Росводресурсы	Данные о водном объекте, об общей оценке и результатам прогнозирования изменения состояния водных объектов, дна, берегов водных объектов, их морфометрических особенностей, водоохранных зон водных объектов, данные о количественных и качественных показателях состояния водных ресурсов, состояния водохозяйственных систем, в том числе гидротехнических сооружений.	+		+	+	HTML; BMP; ZIP; DOC; DOCX; PDF; GIF; JPEG; PNG; TIFF Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
17 ЕСИМО Минприроды России, Росгидромет	Данные о состоянии морской среды и морской деятельности, полученной в результате наблюдений.	+		+	+	XLS; BMP; HTML; ZIP; DOC; PDF; JPEG; JPEG 2000; PCX; PNG; TIFF; SHP
18 АС ПГУ МЭВ Росгидромета Минприроды России, Росгидромет	Информация о состоянии атмосферного воздуха и его загрязнений. Информация о состоянии поверхностных водных объектов и их загрязнении	+		+	+	Интеграционная платформа (
19 ИСДМ - Рослесхоз Минприроды России, Рослесхоз	Данные наземных, авиационных и космических наблюдений (топоосновы, ДЗЗ и атрибутивных данных). Данные по динамике изменений лесного фонда, не связанной с воздействием лесных пожаров.	+		+	+	XML; DOC; RTF Интеграционная платформа
20 ИС "Учет и баланс подземных вод" Минприроды России, Роснедра	Данные результатов учета, оценки состояния и степени использования ресурсной базы подземных вод Российской Федерации в системе управления их воспроизводством и рациональным использованием. Данные государственного кадастра месторождений подземных вод, государственного учета и баланса их запасов, планирования использования ресурсов и запасов подземных вод	+		+	+	XLS; BMP; HTML; ZIP; DOC; PDF; JPEG; JPEG 2000; PCX; PNG; TIFF; SHP Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
21 ПТК Госконтроль Минприроды России, Росприроднадзор	<p>Данные реестра объектов, оказывающих негативное воздействие на окружающую среду и вредное воздействие на атмосферный воздух.</p> <p>Информация о нормах воздействия на окружающую среду.</p> <p>Данные отчетности природопользователей об образовании, использовании, обезвреживании, о размещении отходов субъектами малого и среднего предпринимательства.</p> <p>Данные сводных отчетов по негативному воздействию на окружающую среду.</p>	+		+	+	XML; DOC; RTF Интеграционная платформа (интеграционная шина)
22 АИС РФС АПК Минсельхоз России	Сведения о подведомственных Минсельхозу России организациях, о переданном им федеральном имуществе. Данные реестра федеральной собственности агропромышленного комплекса, включая геопространственные данные о дислокации контуров земельных участков.	+		+	+	XML; DOC; RTF Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
23 СДМЗ Минсельхоз России	Информация о состоянии земель сельскохозяйственного назначения и растительности на этих землях. Данные результатов тематической обработки данных дистанционного зондирования земель; Данные оценки состояния растительности и площади, занятой культурами в разрезе пяти циклов съемки на уровне федерального округа, субъекта РФ, района, хозяйства и отдельного поля; Данные влияния чрезвычайных ситуаций на сельскохозяйственные угодья и оценка ущерба, нанесенного чрезвычайными ситуациями сельскохозяйственным угодьям.	+		+	+	GeoTIFF; GDB; XML Интеграционная платформа
24 АИС НСИ Минсельхоз России	Данные реестров, регистров, справочников, классификаторов объектов контролируемых Минсельхозом России				+	GeoTIFF; GDB; XML Интеграционная платформа
25 ГИС "Деметра" Минсельхоз России, Россельхознадзор	Информация о состоянии земель сельскохозяйственного назначения фитосанитарных и ветеринарных карантинных зонах и объектах	+		+	+	GeoTIFF; GDB; XML Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
26 СС-ТМК Минтранс России	Сведения поступающие из инженерно-технических средств обеспечения транспортной безопасности и иных автоматизированных систем технического мониторинга и контроля, используемых на объектах транспортной инфраструктуры	+	+		+	XML; DOC; RTF Интеграционная платформа
27 ЕГИС ОТБ Минтранс России	Сведения об опасных объектах транспортной инфраструктуры и транспортных средствах; Сведения об аварийных ситуациях и действиях диспетчерских, аварийных и технических служб объектов; Результаты расчетов прогнозов развития чрезвычайных ситуаций Информация об объектах транспортной инфраструктуры и транспортных средствах (паспорта объектов); Данные о категорировании транспортной инфраструктуры и транспортных средств; Сведения мониторинга состояния защищенности объектов транспортной инфраструктуры	+	+		+	XML; DOC; RTF Интеграционная платформа (интеграционная шина)
28 АБДД Дорога Минтранс России, Росавтодор	Данные автоматизированного банка дорожных данных об автомобильных дорогах, искусственных сооружениях, движении автотранспортных средств, ДТП, объектах сервиса и др. Данные диагностики	+	+		+	GDB; XML, DOC; RTF Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	технического состояния автомобильных дорог общего пользования Российской Федерации, о наличии аварийных участков и потребности в дорожных работах.					
29 ЕАВИИАС МСЭ Минтруд России	Данные статистической и аналитической отчетности				+	DOC; RTF
30 АИС ЕСУИ Минтруд России	Данные единой системы учета инвалидов в Российской Федерации	+			+	DOC; RTF Интеграционная платформа)
31 АИС "Миграпотоки" Минтруд России	Данные о количественных показателях трудовых миграционных потоков граждан, осуществляющих трудовую деятельность вне места постоянного проживания	+			+	DOC; RTF
32 ФГИС ТП Минэкономразвития России	Данные (слои) единой информационной системы территориального планирования Российской Федерации, информация о состоянии, использовании и планируемом развитии территорий.	+			+	TIFF; SHP;DOC; RTF Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
33 ПК ПВД Минэконом-развития России, Росреестр	Данные информационных систем государственного кадастра недвижимости и государственной регистрации прав для нужд Росреестра				+	DOC; RTF Интеграционная платформа (интеграционная шина)
34 АИС "Электронный инспектор" МЧС России	Данные состояния пожарной безопасности объектов защиты и результатов надзорной деятельности на объектах защиты	+			+	DOC; RTF Интеграционная платформа
35 ИАС-ДТП МЧС России	Данные о реагировании пожарно-спасательных подразделений на ДТП. Результаты расчета компьютерных моделей типовых сценариев дорожно-транспортных происшествий при перевозках опасных грузов. Доступ к электронной библиотеке работ, выполненных МЧС России в рамках ФЦП «Повышение безопасности дорожного движения в 2006-2012 годах». Доступ к Банку данных объектов инфраструктуры, связанных с оказанием помощи лицам, пострадавшим в ДТП, вдоль автомобильных дорог. Данные мониторинга реализации региональных целевых программ в области безопасности дорожного движения.	+	+		+	DOC; RTF Интеграционная платформа

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
36 ФБД "ПОЖАРЫ" МЧС России	Данные единой государственной системы статистического учета пожаров и последствий от них в Российской Федерации	+	+		+	DOC; RTF Интеграционная платформа
37 ИВС Росстата Росстат	Данные каталога статистических показателей (КСП). Данные Объединенной системы регистров (ОСР), включая информацию БД "Индивидуальные предприниматели"; БД "Юридические лица". Данные центральной базы статистических данных (ЦБСД). Данные БД "Показатели муниципальных образований". Данные региональной базы статистических данных (РБСД). Данные отраслевой базы статистических данных.				+	DOC; RTF Интеграционная платформа
38 Стрелец-Мониторинг (Аргус Спектр)	данные о параметрах возгорания, угрозах и рисках развития крупных пожаров в сложных зданиях и сооружениях, в высотных зданиях, а также на объектах с массовым пребыванием людей	+			+	XML Интеграционная платформа (
39 Система «БРИЗ» (МЧС России)	БРИЗ предназначена для создания систем, обеспечивающих мониторинг ситуаций в различных сферах деятельности, информационного обеспечения органов управления в различных режимах функционирования, а также выработки	+			+	XML Интеграционная платформа

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	<p>предложений (на основе типовых решений) для оперативного принятия решений по возникшим ситуациям. На базе платформы БРИЗ создаются территориально-распределенные системы, которые обеспечивают возможность работы в едином информационном пространстве органов управления и подчинённых организаций различного уровня иерархии.</p> <p>Обмен информацией между органами управления и организациями осуществляется как по вертикали (между органами управления и организациями разного уровня иерархии), так и по горизонтали (между органами управления и организациями одного уровня иерархии).</p> <p>База данных системы формируется нижестоящими органами управления и организациями, а также по информации, поступающей из внешних систем. База данных вышестоящих органов управления и организаций формируется как консолидированная база данных нижестоящих органов управления и организаций с возможностью изменения информации (с автоматической репликацией изменений в нижестоящие органы по настраиваемым регламентам).</p>					

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
40 КСМ-3Н (Комплексная система мониторинга защиты населения)	<ul style="list-style-type: none"> - данные непрерывного автоматизированного контроля радиационной обстановки и метеопараметров; - представление оперативных данных с использованием геоинформационных технологий; - данные оценки и прогноза радиационной обстановки, оценки доз облучения населения и выработки рекомендаций по мерам защиты населения в случаях ЧС с радиационным фактором. 	+		+	+	XML Интеграционная платформа (интеграционная шина)
41 Автоматизированная система расчета времени достижения фронтом пожара населенных пунктов (КосмоМониторинг)	<ul style="list-style-type: none"> - результаты расчета потенциальных угроз населенным пунктам по данным космического мониторинга (термоточкам); - результаты прогноза развития пожароопасной обстановки; - результаты расчета времени достижения пожара до населенного пункта. 	+		+	+	XML;TIFF; SHP;DOC; RTF Интеграционная платформа (интеграционная шина)
42 Система поиска и отображения космоснимков «Космоплан»	- космоснимки различного масштаба.	+	+	+		TIFF; SHP
43 БСЧС – автоматизированная система информационного обеспечения СМПЧС и НЦУКС.	<ul style="list-style-type: none"> - Предоставление данных по параметрам биолого-социальных источников ЧС; - предоставление информации о различных заболеваниях животных, человека и растений. 	+		+	+	DOC; RTF

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
44 ГЛОНАСС	- Глобальная оперативная навигация приземных подвижных объектов: наземных (сухопутных, морских, воздушных) и низкоорбитальных космических.	+	+	+	+	Протокол транспортного уровня Интеграционная платформа (интеграционная шина)
45 СЗИОНТ - система защиты, информирования и оповещения населения на транспорте.	- повышение защищенности пассажиров и персонала на транспорте от актов незаконного вмешательства, в том числе террористической направленности, а также от чрезвычайных ситуаций природного и техногенного характера; - подготовка населения в области гражданской обороны, защиты от ЧС; - обеспечения пожарной безопасности и охраны общественного порядка; - своевременное оповещение и оперативное информирование граждан о ЧС и угрозе террористических актов; - мониторинг обстановки и состояния правопорядка в местах массового пребывания людей на территории транспортных узлов.	+	+		+	XML Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
46 ИС ЕДДС - информационная система Единой дежурно-диспетчерской службы(ЗАО «НПП ТЕЛДА»)	<ul style="list-style-type: none"> - 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 (систем мониторинга) 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 ОСОДУ; - 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); 	+	+	+	+	XML Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	<ul style="list-style-type: none"> - 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. 					
47 ОКСИОН	<ul style="list-style-type: none"> - подготовка населения в области гражданской обороны, защиты от чрезвычайных ситуаций; - обеспечения пожарной безопасности и охраны общественного порядка; - своевременное оповещение и оперативное информирование граждан о чрезвычайных ситуациях и угрозе террористических акций; - мониторинг обстановки и состояния правопорядка в местах массового пребывания 	+	+	+	+	XML Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	людей на основе использования современных технических средств и технологий.					
48 Система мониторинга «Навигатор-С» («ЕНДС-Астрахань»)	- Обеспечение эффективности использования автотранспорта; - обеспечение защиты и безопасности. Достигается это применением технологий глобального позиционирования ГЛОНАСС/GPS, мобильной связи и оригинального программного обеспечения.		+		+	XML Интеграционная платформа (интеграционная шина)
49 СМИС (ООО «Базис»)	- Снижение людских и материальных потерь в случае развития аварийной ситуации, пожара; - автоматизированный мониторинг в режиме реального времени критически важных для безопасности персонала, населения и окружающей среды состояний технологических систем, систем жизнеобеспечения, систем безопасности, систем противопожарной защиты и систем связи; - информирование в режиме реального времени ЕДДС (ЕСОДУ) муниципального образования о предаварийном, аварийном состоянии технологических систем, систем жизнеобеспечения, систем безопасности, систем противопожарной защиты, систем связи, террористических проявлениях; - обеспечение через ЕДДС (ЕСОДУ) муниципального образования соответствующих служб и подразделений (экстренного вызова, дежурно-диспетчерских, оперативно-дежурных, аварийно-спасательных) информацией,	+			+	XML; TIFF; SHP;DOC; RTF Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	необходимой для проведения аварийно-спасательных работ и ликвидации последствий аварий, пожаров, ЧС.					
50 КТСО-Р – комплекс технических средств оповещения населения по радиоканалам (МЧС России)	Предназначен для создания региональных (субъектов Российской Федерации), местных (муниципальных образований) и локальных автоматизированных систем централизованного оповещения (АСЦО) в районах со слаборазвитой инфраструктурой связи с целью обеспечения доведения сигналов и информации оповещения до населения с использованием сетей проводного вещания и телевидения, выходных акустических устройств (П-166 ВАУ), электросирен и радиовещательных приемников оповещения, а также до должностных лиц с использованием стационарных и носимых приемников персонального радиовызова (пейджеров).	+			+	XML; Интеграционная платформа (интеграционная шина)
51 КСЭОН - Комплексная система экстренного оповещения населения	КСЭОН предназначена для своевременного и гарантированного оповещения населения в зонах экстренного оповещения с использованием современных информационно-коммутационных технологий и программно-технических комплексов (технических средств и оконечных средств), тип и вид которых определяется в зависимости от характеристики (паспорта) зоны экстренного оповещения, присущих данной территории опасных природных и техногенных процессов, а также	+			+	XML; Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	групп населения, которые могут находиться в данной зоне.					
52 Система -112	- ускорение реагирования и улучшения взаимодействия экстренных оперативных служб при вызовах населения; - организация удобного вызова экстренных оперативных служб по принципу «одного окна»; - уменьшение социально-экономического ущерба вследствие происшествий и чрезвычайных ситуаций; - гармонизация способа вызова экстренных оперативных служб с законодательством Европейского союза.	+	+	+	+	XML; Интеграционная платформа (интеграционная шина)
53 РАСЦО - Региональная автоматизированная система централизованного оповещения населения	Предназначена для обеспечения своевременного доведения информации и сигналов оповещения до органов управления, сил и средств гражданской обороны, территориальных подсистем единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций и населения об опасностях, возникающих при ведении военных действий, а также угрозе возникновения или возникновении чрезвычайных ситуаций природного и техногенного характера.	+			+	XML; Интеграционная платформа (интеграционная шина)
54 Федеральная информационная адресная система (ФИАС)	Федеральная информационная адресная система (ФИАС) содержит достоверную единообразную и структурированную адресную информацию по территории Российской Федерации, доступную				+	XML; Интеграционная платформа

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	для использования органами государственной власти, органами местного самоуправления, физическими и юридическими лицами. Система разработана в соответствии с Распоряжением Правительства Российской Федерации от 10.06.2011 № 1011-р. Сведения из ФИАС представляются на основе административно-территориального деления субъектов Российской Федерации и на основе муниципального деления. Адресная информация, содержащаяся в ФИАС, является открытой и предоставляется на бесплатной основе.					(интеграционная шина)
55 Автоматизированная информационная система "Государственный водный реестр"	Сбор, хранение и анализ документированных сведений о водных объектах, о водопользователях и инфраструктуре на водных объектах.; Ретроспективное хранение документированной информации о водных объектах, о водопользователях	+			+	DOC; RTF
56 Информационная система дистанционного мониторинга Федерального агентства лесного хозяйства	Упрощение процедуры идентификации и аутентификации в ИСДМ-Рослесхоз; Сопоставление данных наземных, авиационных и космических наблюдений, включающее обратную связь с регионами; Интеграция в одном ГИС-интерфейсе комплексной информации (топоосновы, ДЗЗ и атрибутивных данных); Поддержка управленческих решений в области мониторинга лесопожарной ситуации;	+		+	+	XML; TIFF; SHP; DOC; RTF Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	Контроль за переданными субъектам полномочиями и оценка эффективности использования субвенций; Формирование данных по динамике изменений лесного фонда, не связанной с воздействием лесных пожаров					
57 Программный комплекс для автоматизации мониторинга подготовки теплогенерирующих объектов к осенне-зимнему периоду "Энергосистема-Зима"	Осуществление контроля должностными лицами органов надзора за подготовкой электротеплоснабжающих организаций субъектов Российской Федерации к осенне-зимнему периоду.; Анализ и мониторинг состояния готовности субъектов к осенне-зимнему периоду в территориальных управлениях Ростехнадзора; Анализ и мониторинг состояния готовности субъектов к осенне-зимнему периоду в центральном аппарате Ростехнадзора	+			+	DOC; RTF Интеграционная платформа (интеграционная шина)
58 Автоматизированная информационно-аналитическая система "Поиск" (ИАС-Поиск) Единой Системы авиационно-космического поиска и спасания	Информационная поддержка и обеспечение решения аналитических задач и задач организации авиационно-космического поиска и спасания, поддержка проведения поисково-спасательных операций (работ); мониторинг состояния обстановки и состояния дежурных поисково-спасательных сил и средств.; Сбор формализованных данных по каналам связи с систем "Поиск", установленных в региональных и местных подразделениях авиационно-космического поиска и спасания; Хранение и ведение архивов графических схем и карт, подготовленных для анализа мероприятий	+			+	XML; TIFF; SHP;DOC; RTF Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	в области авиационно-космического поиска и спасания; Проведение расчетов для анализа обеспеченности территории РФ средствами авиационно-космического поиска и спасания					
59 Автоматизированная система «По учету транспортных происшествий на морском и речном транспорте и выработке мер по их предупреждению в соответствии с функциями, возложенными на Ространснадзор, в связи с введением в обязательную силу Международного кодекса стандартов и рекомендуемой практики расследования аварий и инцидентов на море (приказ Минтранса России от 14.05.2009 №75).; Автоматизация процесса сбора, обобщения и анализа данных об авариях и инцидентах на морском и речном транспорте; Обеспечение возможности ввода информации и доступа к данным для территориальных подразделений Ространснадзора; Оперативное формирование отчетности о транспортных происшествиях на морском и речном транспорте Российской Федерации; Повышение качества расследования аварий и инцидентов; Повышение оперативности принятия управленческих решений по вопросам предотвращения аварий и инцидентов	Учет транспортных происшествий на морском и речном транспорте и выработка мер по их предупреждению в соответствии с функциями, возложенными на Ространснадзор, в связи с введением в обязательную силу Международного кодекса стандартов и рекомендуемой практики расследования аварий и инцидентов на море (приказ Минтранса России от 14.05.2009 №75).; Автоматизация процесса сбора, обобщения и анализа данных об авариях и инцидентах на морском и речном транспорте; Обеспечение возможности ввода информации и доступа к данным для территориальных подразделений Ространснадзора; Оперативное формирование отчетности о транспортных происшествиях на морском и речном транспорте Российской Федерации; Повышение качества расследования аварий и инцидентов; Повышение оперативности принятия управленческих решений по вопросам предотвращения аварий и инцидентов				+	DOC; RTF
60 Федеральное агентство водных ресурсов Информационная система	позволяет получать оперативную информацию с территории России для своевременного принятия мер по				+	DOC; RTF

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
"Оперативный дежурный"	предупреждению или минимизации неблагоприятных ситуаций, ликвидации последствий чрезвычайных ситуаций, для своевременного информирования руководства Росводресурсов.; Оперативное информирование ОД центрального аппарата Росводресурсов о поступлении доклада о чрезвычайной ситуации или возможности чрезвычайной ситуации; Обобщение и наглядное представление поступившей информации для анализа текущей обстановки и представление ее руководству Росводресурсов					
61 Информационно-аналитическая система контроля и надзора за пожарной безопасностью при эксплуатации воздушных, морских судов, судов внутреннего водного и смешанного (река-море) плавания, иных плавучих объектов, железнодорожного подвижного состава Информационно-аналитическая система контроля и надзора за пожарной безопасностью при эксплуатации воздушных, морских судов, судов внутреннего водного и смешанного (река-море)	Функциональный блок «Учет пожаров и их последствий» предназначен для информационного обеспечения и автоматизации деятельности сотрудников федеральной службы и ее территориальных органов по учету пожаров на транспорте и их последствий, контролю расследования обстоятельств и причин произошедших пожаров. Функциональный блок «Ведомственный надзор за пожарной безопасностью» предназначен для информационного обеспечения и автоматизации деятельности сотрудников федеральной службы и ее территориальных органов по планированию и проведению контрольных мероприятий по соблюдению требований пожарной безопасности при эксплуатации транспорта субъектами транспорта. Функциональный блок				+	DOC; RTF

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
плавания, иных плавучих объектов, железнодорожного подвижного состава	«Реестры субъектов и объектов надзора» предназначен для информационного обеспечения и автоматизации деятельности сотрудников федеральной службы и ее территориальных органов по ведению реестров поднадзорных объектов и субъектов в сфере пожарной безопасности на транспорте. Функциональный блок «Анализ и формирование отчетности» предназначен для обеспечения автоматизированного мониторинга уровня пожарной безопасности при эксплуатации транспортных средств и соблюдения требований, установленных законодательством, мониторинга основных показателей контрольно-надзорной деятельности Федеральной службы по надзору в сфере транспорта и принимаемых ею мер по нарушениям в этой сфере с целью обеспечения информационной поддержки принятия управленческих решений руководящим составом службы. Функциональный блок «НСИ и обмен данными» предназначен для управления ведомственными информационными ресурсами; ведения нормативно-справочной информации, необходимой для функционирования системы; обмена необходимыми данными с ФМ «Монитор» и внешними по отношению к ФМ «Пожарная безопасность на транспорте» системами, входящими в состав ЕИАС РОСТРАНСНАДЗОРА, обработки и передачи их					

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	в другие функциональные блоки ФМ для дальнейшего использования. ; Сбор, хранение, аналитическая обработка информации о пожарах на транспортных средствах, а также о проверках в части обеспечения пожарной безопасности на транспорте; Формирование регламентированной отчетности; Подготовка аналитических отчетов					
62 Государственная информационная система жилищно-коммунального хозяйства	Государственная информационная система жилищно-коммунального хозяйства - единая федеральная централизованная информационная система, функционирующая на основе программных, технических средств и информационных технологий, обеспечивающих сбор, обработку, хранение, предоставление, размещение и использование информации о жилищном фонде, стоимости и перечне услуг по управлению общим имуществом в многоквартирных домах, работах по содержанию и ремонту общего имущества в многоквартирных домах, предоставлении коммунальных услуг и поставках ресурсов, необходимых для предоставления коммунальных услуг, размере платы за жилое помещение и коммунальные услуги, задолженности по указанной плате, об объектах коммунальной и инженерной инфраструктур, а также иной информации, связанной с жилищно-коммунальным хозяйством.; Сбор, обработка, хранение, предоставление, размещение и	+			+	XML; Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	использование информации о жилищном фонде, стоимости и перечне услуг по управлению общим имуществом в многоквартирных домах; Сбор, обработка, хранение, предоставление, размещение и использование информации о работах по содержанию и ремонту общего имущества в многоквартирных домах, предоставлении коммунальных услуг и поставках ресурсов, необходимых для предоставления коммунальных услуг; Сбор, обработка, хранение, предоставление, размещение и использование информации о размере платы за жилое помещение и коммунальные услуги, задолженности по указанной плате, об объектах коммунальной и инженерной инфраструктур					
63 АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДИСТАНЦИОННОГО МОНИТОРИНГА (АСД-ЛИДАР)	система, предназначенная для дистанционного обнаружения аварий на химически опасных объектах, пожаров, взрывов и т.п.; разведки зоны аварии для обеспечения действий аварийно-спасательных формирований; прогноза зон поражения для принятия решений по защите и эвакуации населения. А.с.д.м. состоит из стационарного поста и мобильного лидарного комплекса. Стационарный пост включает в себя лидар кругового обзора, панорамную телевизионную систему и сканирующую тепловизионную систему, позволяющие проводить обнаружение	+		+	+	XML; Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	<p>аэрозольных выбросов в атмосферу и очагов возгорания над значительной территорией. Главной частью стационарного поста является лидар кругового обзора, результат работы которого отображается на мониторе. Панорамная телевизионная система позволяет оператору визуально контролировать состояние атмосферы и в случае обнаружения чрезвычайных ситуаций проводить лидар-ные измерения в заданном секторе. Использование тепловизионной системы повышает достоверность обнаружения чрезвычайных ситуаций, которые вызывают локальное изменение температуры (пожар, выбросы некоторых химических веществ). Оператор также имеет возможность наблюдать любой из ракурсов в ИК-диапазоне, используя сканирующую тепловизионную систему, что существенно повышает достоверность обнаружения чрезвычайных ситуаций. Мобильный лидарный комплекс (лаборатория) размещён на автомобильном шасси и представляет собой сложную оптоэлектронную систему, в состав которой входят инфракрасный гетеродинный лидар и импульсный лидар вакуумного ультрафиолетового (ВУФ) диапазона. Гетеродинный лидар позволяет получать информацию об относительном распределении аэрозоля, векторе скорости ветра, интенсивности турбулентности атмосферы, а</p>					

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	также о распределении в атмосфере таких газов, как аммиак, хлор, акролеин и др. Импульсный лидар ВУФ-диапазона позволяет в режиме DIAL контролировать аномальные выбросы в атмосферу города таких газов, как аммиак, хлор, а также озон, окислы азота и др					
64 АВТОМАТИЗИРОВАННАЯ СИСТЕМА КОНСУЛЬТАЦИОННОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ	подсистема в составе автоматизированной информационно-управляющей системы РСЧС, предназначенная для оказания информационных услуг населению и организациям по вопросам обеспечения безопасности в чрезвычайных ситуациях на основе: интеграции информационных ресурсов; формирования единого информационного пространства между структурными подразделениями центрального аппарата, организациями и учреждениями МЧС России, региональными центрами ГОЧС и главными управлениями МЧС России по субъектам РФ, органами управления ГОЧС субъектов РФ и муниципальных образований; информатизации и автоматизации функционирования перечисленных органов управления в части работы с населением на федеральном, региональном, территориальном и местном уровнях.	+	+	+	+	XML; Интеграционная платформа (интеграционная шина)
65 Ками - Система моделирования/прогнозирования распространения ЧС	прогнозы для следующих типов ЧС: 1. Наводнение, паводок	+	+	+	+	XML;

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	2. Взрыв 3. Пожар 4. Выброс АХОВ 5. Лесной пожар Прогнозирование запускается в следующих вариантах: 1. Запуск расчетной задачи в автоматическом режиме на основании сигнала, поступившего от датчика 2. Запуск расчетной задачи на повторное прогнозирование по таймауту (уточнение прогноза) 3. Запуск расчетной задачи на повторное прогнозирование по запросу (уточнение прогноза)					Интеграционная платформа (интеграционная шина)
66 Система видеонаблюдения и видеоанализа	—оценка плотности потока людей на значимых для города объектах; - выявление движения человека против потока; - остановка человека в контролируемой зоне (с заданием времени остановки); - автоматическое наведение поворотных камер на обнаруженные цели (человек, ТС, группа людей) с оптическим увеличением и	+	+		+	XML; Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	<p>сопровождением по видеоизображению с обзорной камеры;</p> <ul style="list-style-type: none"> - резкое ускорение движения человека; - хаотичное движение человека (праздношатание); - индексирование событий в условиях дорожного движения (плотность потока, заторы, массовое скопление автотранспорта), в том числе в парковочных зонах; - детектор оставленных предметов; - детектор фактов пересечения запрещенной зоны (проезд, проход); - детектор исчезнувших предметов; - реагирование на проход людей в заданном направлении (входы, выходы, переходы, коридоры и т.п.); - появление человека или автомобиля в зоне наблюдения (улицы, площади, перекрестки, парки). - обнаружение скопления людей, в том числе в несанкционированных местах; - расфокусировка видеокамеры; - загрязнение объектива видеокамеры; 					

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	<ul style="list-style-type: none"> - изменение фона; - сдвиг камеры - заслонение объектива камеры. - потеря сигнала от камеры 					
67 Лесохранитель	- это система лесопожарного мониторинга, которая работает по следующему принципу: камеры, установленные на вышках сотовой связи на территории Свердловской области, передают видеопоток на сервер Уральской базы охраны лесов, где соответствующая видеоаналитика определяет факт лесного возгорания и его координаты.	+		+	+	XML; JPEG; JPEG 2000; Интеграционная платформа (интеграционная шина)
68 Грифон	Обмен событиями, оповещение населения	+	+	+	+	XML; Интеграционная платформа
69 Эмерсит (метеодатчики)	<p>Датчики погоды, предоставляют данные:</p> <ol style="list-style-type: none"> 1. Показания поста 2. Статус поста <p>Перечень статусов:</p> <ol style="list-style-type: none"> 1. Норма 	+			+	XML; Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	2. На обслуживании 3. Неисправен 4. Потеря поста					
70 Пилотный участок подсистемы оповещения в составе программно-аппаратного комплекса «Единый центр оперативного реагирования» в составе АПК «Безопасный город». ЗАО НПО «Сенсор»	<p>Основные задачи системы, реализуемые в рамках пилотного участка:</p> <ul style="list-style-type: none"> - своевременное и гарантированное доведение до населения достоверной информации об угрозе или о возникновении чрезвычайной ситуации, правилах поведения и способах защиты в таких ситуациях; - передача в автоматическом и (или) автоматизированном режимах необходимой информации и сигналов оповещения для адекватного восприятия населением при угрозе возникновения или при возникновении ЧС; - возможность сопряжения технических устройств, осуществляющих приём, обработку и передачу аудио- и (или) аудиовизуальных, а также иных сообщений об угрозе или о возникновении чрезвычайной ситуации, правилах поведения и способах защиты в таких ситуациях; - возможность сопряжения системы с локальными системами оповещения потенциально опасных объектов; 	+	+	+	+	XML; Интеграционная платформа (интеграционная шина)

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	<ul style="list-style-type: none"> - использование современных информационных технологий для своевременного и гарантированного информирования населения об угрозе возникновения или о возникновении чрезвычайных ситуаций, правилах поведения и способах защиты в таких ситуациях; -своевременная передача информации до органов управления РСЧС соответствующего уровня в целях принятия необходимых мер по защите населения; - управление оконечными средствами оповещения и информирования с пунктов управления органов повседневного управления РСЧС соответствующего уровня; -передача информации в заданных режимах (индивидуальный, избирательный,циркулярный, по группам по заранее установленным программам); - защита информации от несанкционированного доступа и сохранность информации при авариях в системе; -повышение оперативности реагирование сил и средств РСЧС в целях защиты населения; - снижениелюдских потерь и материального ущерба при возникновении ЧС;- повышение 					

Таблица 2 - Результаты анализа действующих автоматизированных систем различной ведомственной принадлежности, применяемых в настоящее время на федеральном, региональном и муниципальном уровне

Наименование системы и производитель	Поставляемые в АПК БГ данные	Функциональные подсистемы АПК БГ				Способ взаимодействия
		Безопасность населения и муниципальной (коммунальной) инфраструктуры	Безопасность на транспорте	Экологическая безопасность	Координация работы служб и ведомств и их взаимодействие.	
	эффективности принимаемых мер по предупреждению и ликвидации ЧС.					
71 «АДИС» (далее ПК «АДИС»).	Программный комплекс автоматизированной системы диспетчерской службы скорой медицинской помощи ПК «АДИС» предназначен для поддержания в полном объеме всего процесса обработки вызовов на станциях скорой медицинской помощи, начиная от приема вызова диспетчером «03» до статистической обработки вызовов, накопленных в результате их обслуживания.	+			+	XML; Интеграционная платформа
72 ГИС ЖКХ.	Имеет сервисы: управления приборами учета и передачей показаний работы с планами проверок и проверками сервис управления экспортом лицензий и дисквалифицированных лиц Сервис получения и импорта данных НСИ	+			+	XML; Интеграционная платформа
73 Система мониторинга карет скорой помощи (КБ Навигатор)	Данные мониторинга	+			+	XML; Интеграционная платформа
74 Система мониторинга школьных автобусов	Данные мониторинга	+			+	XML; Интеграционная платформа

Действующие АС различной ведомственной принадлежности, применяемые в настоящее время на региональном и муниципальном уровне, при условии интеграции в состав АПК «Безопасный город» обеспечивают решение вышеперечисленных блоков функциональных требований.

2.1.3 Функциональная схема АПК «Безопасный город».

АПК «Безопасный город» должен строиться по распределенной архитектуре, обеспечивающей возможность распределения вычислительных ресурсов, функций управления входящими в состав его сегментов КСА и взаимодействия узлов АПК «Безопасный город».

АПК «Безопасный город» должен строиться по модульному принципу, с использованием, как уже функционирующих, так и перспективных КСА и существующей инфраструктуры). При построении АПК «Безопасный город» приоритет отдается уже функционирующим КСА и существующей инфраструктуре, которые по своим функциональным техническим и прочим характеристикам удовлетворяют требованиям к сегментам АПК «Безопасный город».

Совокупность КСА сегментов АПК «Безопасный город» должны формировать единую информационную среду, обеспечивающую эффективное взаимодействие органов государственной, организаций и населения в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания.

Построение АПК «Безопасный город» на муниципальном уровне осуществляется с использованием интеграционной платформы, обеспечивающей сопряжение между всеми КСА, входящими в состав АПК «Безопасный город».

Интеграционная платформа на муниципальном уровне должна обеспечивать возможность сквозной передачи и обработки информации, целостность и согласованность потоков информации и процедур в рамках

межведомственного взаимодействия с учетом ограничений прав доступа согласно регламентирующим документам соответствующих ведомств.

На региональном уровне информация из муниципальных образований должна консолидироваться на базе региональной информационно-коммуникационной платформы, обеспечивающей органам исполнительной власти субъектов Российской Федерации контроль над оперативной обстановкой в регионе, координацию межведомственного взаимодействия на региональном уровне, обеспечение оперативного управления службами и ведомствами в случае региональных кризисных ситуаций и происшествий.

На федеральном уровне соответствующие органы исполнительной власти должны иметь доступ к информации, находящейся в информационной среде АПК «Безопасный город» и пользоваться ею в соответствии с правами доступа, установленными соответствующими регламентами.

Структурная схема АПК «Безопасный город» приведена на рисунке 2.3 и в «Приложении 1».

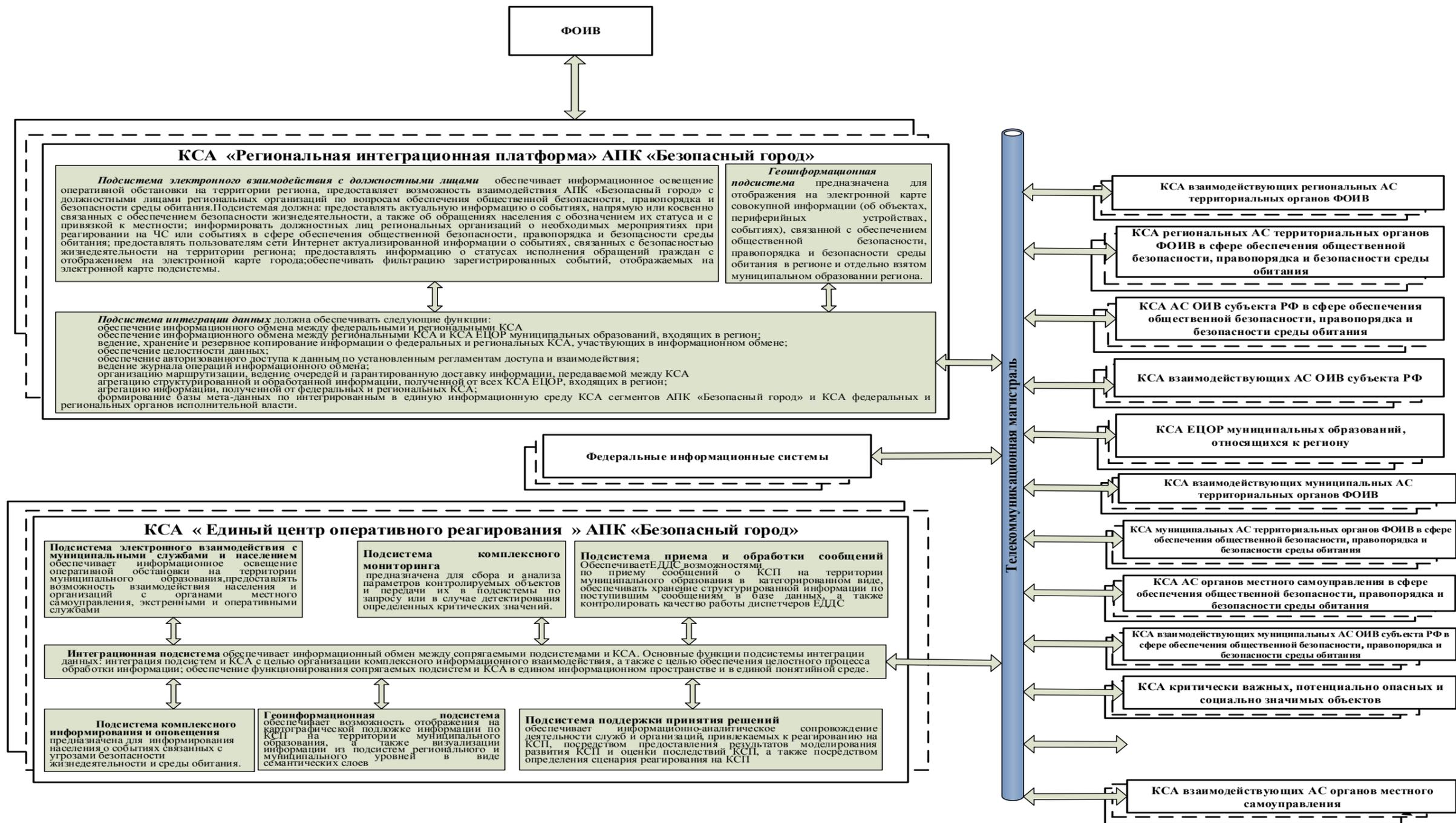


Рисунок 2.3. Структурная схема АПК «Безопасный город»

2.1.4 Функциональные задачи организаций, задействованных в информационном обмене в АПК «Безопасный город»

Основные функциональные задачи организаций, задействованных в информационном обмене в АПК «Безопасный город» заключаются в том, чтобы:

- осуществлять информационный обмен и обеспечить выполнение других функций, связанных с обеспечением информационного взаимодействия в рамках построения и развития АПК «Безопасный город» и определенных регламентом взаимодействия (протоколом информационно-технического взаимодействия);
- обеспечивать достоверность и актуальность информации;
- обеспечивать работоспособность баз данных и программно-технических средств в области их ответственности, задействованных автоматическом информационном обмене в режиме 24/7/365;
- принимать необходимые меры по защите информации и выполнять требования по информационной безопасности на основе регламента взаимодействия.

2.2 Анализ возможности и условий сопряжения действующих автоматизированных информационно-управляющих систем различной ведомственной принадлежности на муниципальном и региональном уровне с системами АПК «Безопасный город»

2.2.1 Общие положения

Для обеспечения возможности сопряжения действующих автоматизированных информационно-управляющих системам различной ведомственной принадлежности на муниципальном и региональном уровне с

системами АПК «Безопасный город» необходимо выполнение следующих условий:

- наличие протоколов информационно-технического взаимодействия (регламента взаимодействия) систем различной ведомственной принадлежности на муниципальном и региональном уровне с системами АПК «Безопасный город»;

- наличие единого стека открытых протоколов информационного взаимодействия АПК «Безопасный город»;

- реализация программной и технической поддержки взаимодействующими системами регламентов взаимодействия (протоколов ИТВ);

- реализация программной и технической поддержки взаимодействующими системами стека открытых протоколов информационного взаимодействия АПК «Безопасный город»;

2.2.2 Требования к Единому стеку открытых протоколов информационного взаимодействия АПК «Безопасный город»

Назначением Единого стека открытых протоколов взаимодействия (далее ЕСОП) является формализация форматов, правил и регламентов взаимодействия между всеми участниками информационного обмена в рамках АПК «Безопасный город».

ЕСОП должен содержать семантические модели данных, участвующих в информационном взаимодействии КСА и представлять собой средство представления структуры предметной области АПК «Безопасный город».

ЕСОП должен определять регламенты доступа к данным для всех участников информационного взаимодействия в рамках АПК «Безопасный город».

Семантические модели данных ЕСОП должны отвечать следующим требованиям:

- обеспечить представление о предметной области АПК «Безопасный город»;
- семантические модели должны быть понятны как специалисту предметной области, так и специалистам в области разработки программного обеспечения;
- модели должны содержать информацию, достаточную для проектирования и реализации АПК «Безопасный город».

ЕСОП должен содержать протоколы информационного взаимодействия между всеми участниками информационного взаимодействия единой информационной среды АПК «Безопасный город» по следующей схеме:

- КСА муниципального уровня должны взаимодействовать с КСА ЕЦОР;
- КСА регионального уровня должны взаимодействовать с КСА ЕЦОР через муниципальную составляющую интеграционной платформы;
- КСА ЕЦОР должен взаимодействовать с региональным уровнем через региональную составляющую интеграционной платформы.

Ниже приведены типовые требования к протоколам в составе ЕСОП.

Все протоколы информационного взаимодействия в составе ЕСОП должны быть независимы от технических и программных средств реализации КСА и любых других участников информационного обмена.

При разработке протоколов ЕСОП следует руководствоваться и использовать существующие российские и международные отраслевые стандарты и спецификации, такие как ONVIF, WS-BaseNotification, WS-Security, WS-I Basic Profile и др. Допускается ограничивать требования таких стандартов и спецификаций до объёма, необходимого для решения задач АПК «Безопасный город».

Прямые вызовы к КСА (например, запрос сведений или отправка управляющей команды) должны преимущественно осуществляться в рамках стека технологий веб-сервисов с применением протоколов XML / SOAP / HTTP. Интерфейсы соответствующих веб-сервисов в таком случае должны быть

описаны в форме документов на языках WSDL версии 1.1 и XML Schema. Взаимодействие с такими сервисами должно отвечать требованиям WS-I Basic Profile 1.2.

В ЕСОП должны быть определены общие требования по защите информационного взаимодействия, основанные на применении общепринятых средств защиты. Так, безопасность взаимодействия в рамках стека технологий веб-сервисов следует обеспечивать посредством использования российских алгоритмов шифрования в протоколе TLS, содержащий как ранее существовавшие наборы параметров шифрования, так и новые, основанные на новых российских криптографических стандартах ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012.

В части взаимодействия с КСА видеомониторинга, видеообнаружения, видеоидентификации, видеораспознавания и других КСА, занимающихся обработкой медиаданных (видео-, аудио- и фотоданных) протокол должен быть основан на спецификациях отраслевого стандарта ONVIF версии не ниже 2.2. Кроме того, протокол дополнительно должен определять спецификации веб-сервисов и соответствующие требования по доступу к ним в рамках протоколов XML / SOAP / HTTP в части:

получения сведений о медиаисточниках (видеокамерах, аудио-, фотоисточниках), в том числе об их географическом местоположении и областях обзора видеокамер;

импорта медиазаписей в КСА в форме файлов, в том числе с привязкой к географическим координатам места записи данных — как постоянных (для стационарных источников), так и изменяющихся во времени (гео-треки, для мобильных источников);

ограничения доступа к медиаисточникам с разбивкой по типу взаимодействия — получения «живых» / «архивных» медиаданных, управления PTZ, фокусировкой видеокамер и др.;

управления заданиями на выполнение длительных операций, таких как, например, отслеживания транспортного средства (поиска на фото / видеоизображениях транспортного средства по регистрационному номеру).

В части передачи событийной информации ЕСОП должен определять протокол, не зависящий от классов систем и типов угроз безопасности населения и среды обитания. Управление процессом передачи и непосредственная передача извещений о событиях, зафиксированных КСА и другими участниками информационного обмена, должны осуществляться в рамках протоколов XML / SOAP / HTTP в соответствии со схемами XML, определяемыми спецификациями сервиса ONVIF Event Service и WS-BaseNotification версии 1.3. Поддержка интерфейса Base Notification в соответствии с ONVIF Core Specification (раздел 9.1) версии не ниже 2.4 является обязательной. Для передачи информации о событиях в пакете Notify в рамках интерфейса Base Notification следует использовать либо структуру данных Message, определённую в ONVIF Core Specification (раздел 9.5.2), либо структуру данных alert, определённую в Common Alerting Protocol версии 1.2.

Протокол в части передачи извещений должен определять машинный язык, который позволяет описывать коды в форме нескольких тем извещений в соответствии с WS-Topics (применяется в WS-BaseNotification и ONVIF Event Service для описания кодов событий). ЕСОП должен определять классификатор общих тем извещений, таких как «Тревога», «Норма», «Неисправность» и др. Специализированные глоссарии, определяющие новые темы извещений, могут быть как разработаны и внедрены на уровне КСА, так и включены позднее в ЕСОП. В каждом извещении должен передаваться код, состоящий из нескольких тем извещений из любых классификаторов. В коде каждого извещения должна присутствовать хотя бы одна тема из единого классификатора. Такой подход обеспечит возможность на машинном уровне идентифицировать тип события, по которому сформировано извещение, даже если часть тем системе-потребителю неизвестна.

В единый классификатор также должны быть включены темы извещений, определённые в отраслевом стандарте ONVIF. Кроме того, в единый классификатор должны быть включены темы извещений в соответствии со следующими типами угроз безопасности населения и среды обитания:

- природные угрозы;
- техногенные угрозы;
- биолого-социальные угрозы;
- экологические угрозы;
- угрозы транспортной безопасности;
- конфликтные угрозы;
- угрозы информационной безопасности;
- управленческие (операционных) риски.

В области природных угроз единый классификатор должен определять темы извещений и требования к данным извещения по следующим зафиксированным событиям:

- подтопления территории города;
- сейсмическая опасность, появление деформации земной поверхности в виде провалов и неравномерных оседаний земли;
- появление оползней;
- возникновение ураганов, штормового ветра, обильных снегопадов и затяжных дождей, обледенения дорог и токонесущих проводов;
- падение крупных небесных тел (метеоритов, болидов);
- задымление вследствие массовых торфяных и лесных пожаров.

В области техногенных угроз единый классификатор должен определять темы извещений и требования к данным извещения по следующим зафиксированным событиям:

- транспортные аварии, включая дорожно-транспортные происшествия, крушения поездов, железнодорожные аварии и авиационные катастрофы;
- пожары на промышленных объектах, транспорте и в жилых зданиях;

- обрушения элементов транспортных коммуникаций, производственных и непроизводственных зданий и сооружений;
- аварии на магистральных трубопроводах;
- аварии на подземных сооружениях;
- прорывы гидротехнических сооружений, являющихся гидродинамически опасными объектами (плотин, запруд, дамб, шлюзов, перемычек и др.) с образованием волн прорыва и катастрофических затоплений;
- аварии с выбросом химически опасных веществ и образованием зон химического заражения;
- аварии с выбросом радиоактивных веществ с образованием обширных зон загрязнения;
- аварии с разливом нефтепродуктов;
- аварии на электростанциях и сетях с долговременным перерывом электроснабжения основных потребителей;
- аварии на системах жизнеобеспечения и очистных сооружениях;
- прорывы в сетях тепло- и водоснабжения;
- старение жилого фонда, инженерной инфраструктуры;
- снижение надежности и устойчивости энергоснабжения;
- перегруженность магистральных инженерных сетей канализации и полей фильтрации;
- дефицит источников теплоснабжения;
- медленное внедрение новых технологий очистки питьевой воды;
- несвоевременная и некачественная уборка улиц;
- нарушение порядка утилизации производственных и бытовых отходов;
- воздействие внешних факторов на качество питьевой воды;
- несоответствие дорожного покрытия требованиям безопасности автомобильных перевозок.

В области биолого-социальных угроз единый классификатор должен определять темы извещений и требования к данным извещения по следующим зафиксированным событиям:

- инфекционные, паразитарные болезни и отравления людей;
- особо опасные болезни сельскохозяйственных животных и рыб;
- карантинные и особо опасные болезни.

В области экологических угроз единый классификатор должен определять темы извещений и требования к данным извещения по следующим зафиксированным событиям:

- просадки, оползни, обвалы земной поверхности из-за выработки недр при добыче полезных ископаемых и другой деятельности человека;
- наличие тяжелых металлов (в том числе радионуклидов) и других вредных веществ в почве (грунте) сверх предельно допустимых концентраций;
- интенсивная деградация почв, опустынивание на обширных территориях из-за эрозии, засоления, заболачивания почв и так далее;
- ситуации, связанные с истощением невозобновляемых природных ископаемых;
- ситуации, вызванные переполнением хранилищ (свалок) промышленными и бытовыми отходами, загрязнением ими окружающей среды;
- резкие изменения погоды или климата в результате антропогенной деятельности;
- превышение предельно допустимой концентрации вредных примесей в атмосфере;
- температурные инверсии над городами;
- «кислородный» голод в городах;
- значительное превышение предельно допустимого уровня городского шума;
- образование обширной зоны кислотных осадков;
- разрушение озонового слоя атмосферы;
- значительные изменения прозрачности атмосферы;

- недостаток питьевой воды вследствие истощения водных источников или их загрязнения;

- истощение водных ресурсов, необходимых для организации хозяйственно-бытового водоснабжения и обеспечения технологических процессов;

- нарушение хозяйственной деятельности и экологического равновесия вследствие загрязнения зон внутренних морей и мирового океана.

В области угроз транспортной безопасности единый классификатор должен определять темы извещений и требования к данным извещения по следующим зафиксированным событиям:

- террористические и диверсионные акции (угон или захват воздушных, морских, речных судов, железнодорожного подвижного состава, автотранспорта, взрывы на железнодорожных вокзалах, на транспорте, диверсии против гидротехнических сооружений и прочее);

- иные случаи незаконного вмешательства в функционирование транспорта, (наложение посторонних предметов на рельсы, разборудование устройств железнодорожных путей, «телефонный терроризм», противоправное блокирование аэропортов и основных транспортных магистралей), угрожающие жизни и здоровью пассажиров, несущие прямой ущерб транспортной сфере и порождающие в обществе негативные социально-политические, экономические и психологические последствия;

- криминальные действия против пассажиров;

- криминальные действия против грузов;

- чрезвычайные происшествия (аварии), обусловленные состоянием транспортных технических систем (их изношенностью, аварийностью и несовершенством), нарушением правил эксплуатации технических систем, в том числе нормативных требований по экологической безопасности при перевозках, а также природными факторами, создающими аварийную обстановку и влекущими за собой материальные потери и человеческие жертвы.

В области конфликтных угроз единый классификатор должен определять темы извещений и требования к данным извещения по следующим зафиксированным событиям:

- нападения на объекты и их захват;
- взрывы;
- похищения людей;
- применение отравляющих биологически активных и радиоактивных веществ;
- преступления (правонарушения), совершаемые на улицах, объектах транспорта и иных общественных местах;
- действия организованной преступности;
- несанкционированные публичные мероприятия, массовые беспорядки.

В области угроз информационной безопасности единый классификатор должен определять темы извещений и требования к данным извещения по следующим зафиксированным событиям:

- нарушение информационного обеспечения деятельности органов государственной власти, муниципальных предприятий и служб;
- перехват трансляций телерадиовещания, систем оповещения и информирования населения;
- несанкционированный доступ к информации деятельности органов государственной власти, муниципальных предприятий и служб;
- несанкционированный доступ к управлению информационными ресурсами;
- оказание целенаправленного негативного информационного воздействия на население через средства массовой информации и информационно-телекоммуникационную сеть «Интернет»;
- неполная реализация прав граждан в области получения и обмена достоверной информацией, в том числе манипулирование массовым сознанием с использованием информационно-психологического воздействия;

- провоцирование социальной, межнациональной и религиозной напряженности через деятельность отдельных (в том числе электронных) средств массовой информации;

- распространение злоупотреблений в кредитно-финансовой сфере, связанных с проникновением в компьютерные системы и сети.

В области управленческих (операционных) рисков единый классификатор должен определять темы извещений и требования к данным извещения по следующим зафиксированным событиям:

- риски возникновения потенциально опасных техногенных угроз при работе с объектами муниципальной инфраструктуры;

- нарушение нормальных условий жизнедеятельности населения в силу несвоевременного устранения последствий происшествий, аварий и чрезвычайных ситуаций;

- риски причинения ущерба среде обитания и здоровью людей, а также дополнительных материальных расходов на устранение последствий чрезвычайных ситуаций и происшествий в силу низкой эффективности систем прогнозирования и поддержки решений.

2.2.3 Требования к протоколу информационно-технического взаимодействия АПК «Безопасный город»

Протокол информационно-технического взаимодействия должен определять:

- назначение, на основании каких документов он разработан, кем разработан, в каких целях и порядок его уточнения и изменения (при необходимости);

- регламент информационного взаимодействия;

- способ адресования передаваемых данных;

- состав, структуры и форматы представления передаваемых данных;

- чем достигается информационная совместимость взаимодействующих систем;
- чем достигается организационная совместимость взаимодействующих систем;
- перечень КСА взаимодействующих систем, между которыми обеспечивается обмен информацией и их оснащения средствами автоматизации и связи;
- перечень сообщений взаимообмена между взаимодействующими системами, требования к их информационному содержанию;
- требования к информационно - лингвистической совместимости взаимодействующих систем;
- правила конвертирования информационных объектов;
- порядок изменения протокола;
- требования к защите и сохранности информации;
- требования телекоммуникационной инфраструктуре.

2.2.4 Требования к программным средствам поддержки информационно взаимодействия (интеграционной шине)

Интеграционная подсистема (интеграционная шина) должна предоставлять взаимодействующим системам набор сервисов, представленный на рисунке 2.4.

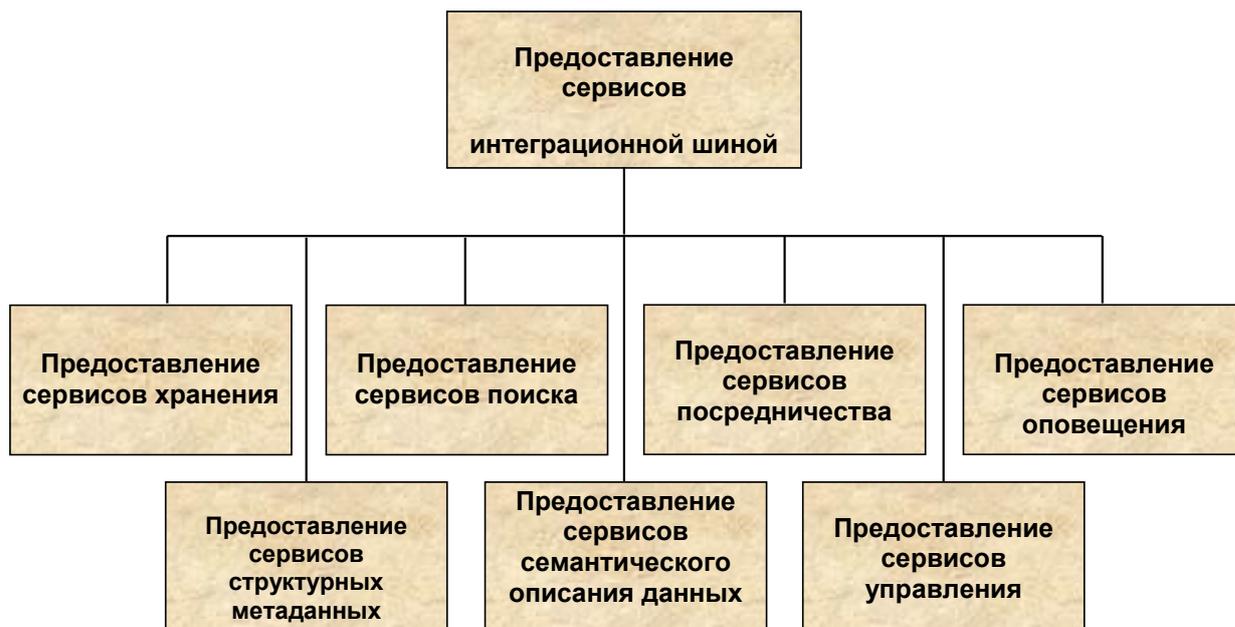


Рисунок 2.4 – Сервисы интеграционной шины

На рисунке 2.4. показан состав сервисов интеграционной шины. В данном случае в состав включены сервисы:

- Хранения;
- Поиска;
- Посредничества;
- Оповещения;
- Структурных метаданных;
- Семантического описания данных;
- Управления.

Сервисы хранения обеспечивают возможности работы с хранилищем данных. Они предоставляют Сервисы размещения, поиска, чтения ИО, а также управления хранилищем данных.

Сервисы хранения обеспечивают процессы управления размещением данных и метаданных (рисунок 2.5).



Рисунок 2.5 – Декомпозиция сервисов хранения

На рисунке 2.5 показана детализация состава сервиса хранения.

Сервисы поиска обеспечивают динамическую публикацию и поиск данных.

Сервисы поиска позволяют:

- осуществлять поиск ИО и/или «частей данных» по их атрибутам;
- прозрачно размещать, выдавать и публиковать данные;
- обеспечивать предоставления интегрированных сервисов.

Сервисы поиска обеспечивают возможности:

- предоставления релевантной информации в нужное время;
- повторного использования размещенных ИО;
- унификации понимания метаданных, что улучшит возможности взаимодействия;
- формирования таких поисковых метаданных, которые соответствуют возможным запросам на поиск.

На рисунке 2.6 изображена декомпозиция сервисов поиска.

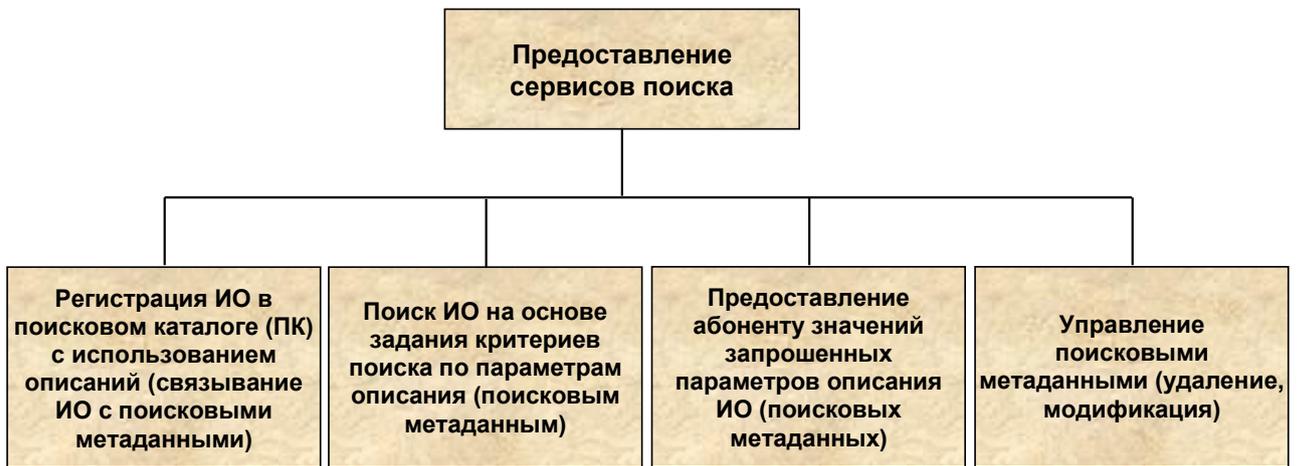


Рисунок 2.6 – Декомпозиция сервисов поиска

На рисунке 2.7 представлена спецификация сервисов посредничества. Они обеспечивают преобразование форматов и сложное агрегирование данных в соответствии с потребностями процессов управления.

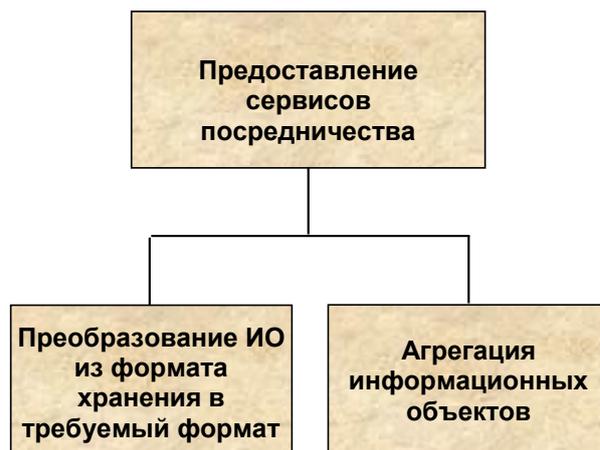


Рисунок 2.7 – Декомпозиция сервисов посредничества

Спецификация сервисов оповещения представлена на рисунке 2.8. Они позволяют извещать потребителя об определенном событии: это может быть добавление, изменение или удаление ИО, а также размещение нового ИО, удовлетворяющего определенному набору критериев.



Рисунок 2.8 – Декомпозиция сервисов оповещения

Предоставление этого сервиса осуществляется по подписке, т.е. потребитель должен явно указать, о каких событиях он должен быть оповещен. Для доставки оповещения используются сервисы, которые гарантируют точечную и групповую приоритетную доставку оповещений с контролем времени жизни, а также обеспечивают отложенную доставку оповещений потребителям, отключенным на момент события. Возможной реакцией на оповещение может быть появление окна, сигнализирующего о событии, запуск автоматического чтения ИО или запуск некоторого приложения.

Структурные метаданные используются для описания данных. Сервисы метаданных позволяют искать и использовать (публиковать, делать видимыми и получать доступ) различные артефакты метаданных. Сервисы метаданных предоставляют инструменты и ресурсы, необходимые для формирования, публикации, доступа, управления метаданными и продвижению возможностей взаимодействия. Сервисы метаданных стандартизируют извлечение информации. Спецификация сервисов структурных метаданных изображена на рисунке 2.9.

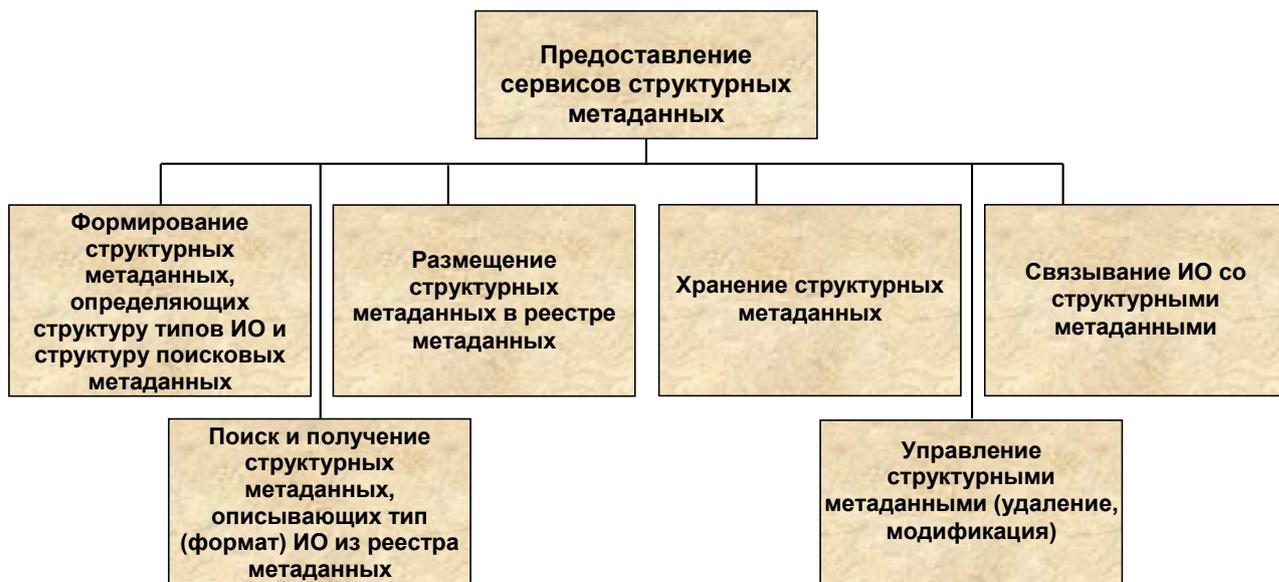


Рисунок 2.9 – Сервисы структурных метаданных

Спецификация сервисов семантического описания данных представлена на рисунке 2.10.

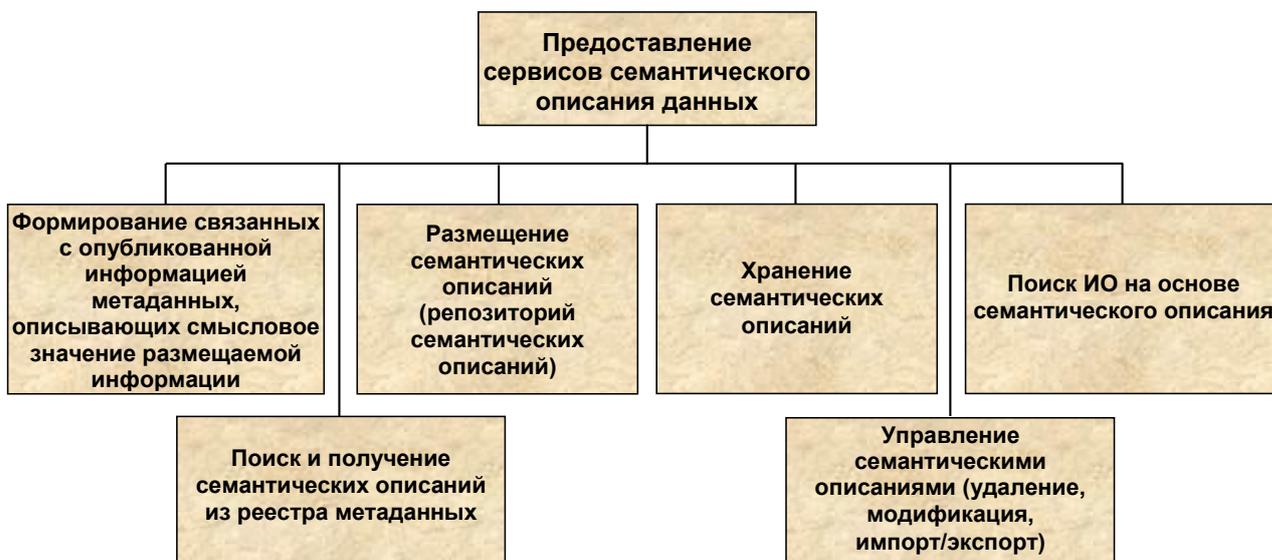


Рисунок 2.10 – Сервисы семантического описания данных

Семантическая информация является основой обеспечения понятности данных и несет основную нагрузку при создании, ведении модели предметной области.

На рисунке 2.11 приведена обобщенная структура и описание групп элементов метаданных, связанных с информационным объектом.

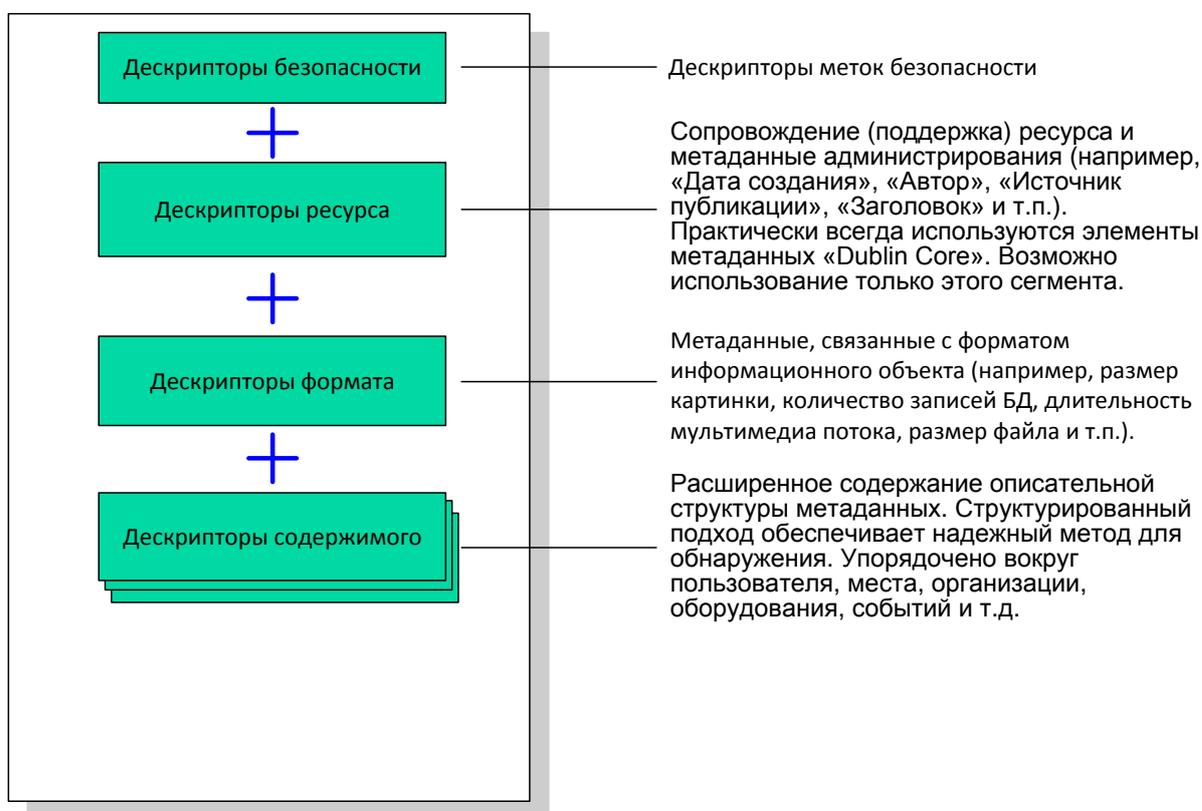


Рисунок 2.11 – Структура метаданных информационного объекта

Поисковый каталог и реестр метаданных могут прямо или косвенно использовать наборы элементов метаописания.

Использование при описании информационного объекта некоторых значений из онтологий (присваивается элементу метаданных) позволяет вовлекать объект в целую систему взаимосвязей, определяемых этими онтологиями. Если в онтологии формализованы богатые знания, то это обеспечивает принципиально более качественные возможности для программных агентов и других сервисов, использующих «интеллектуальную» обработку данных.

Под информационным ресурсом в хранилище данных интеграционной шины понимается любой элемент, который описывает или определяет некоторые

данные (или наборы данных), заключенные/закодированные в строго предписанной форме. Например, документ XML-схемы, также как и элемент XML, определяет формат XML для некоторого набора данных.

Преобразование XML описывает отображение между одним форматом XML и другим; в случае если используется преобразование XSLT (eXtensible Stylesheet Language Transformations – расширяемый язык таблицы стилей), то это формально определенные операции для выполнения отображения. Необходимо отметить, что текстовые файлы, документы Microsoft Word, а также документы, описывающие данные или наборы данных, тоже считаются информационными ресурсами.

Каждый информационный ресурс характеризуется определенным состоянием, которое указывает, на каком этапе жизненного (технологического) цикла он находится. На рисунке 2.12 проиллюстрированы структурные типы метаданных в соответствии с понятием информационного ресурса.

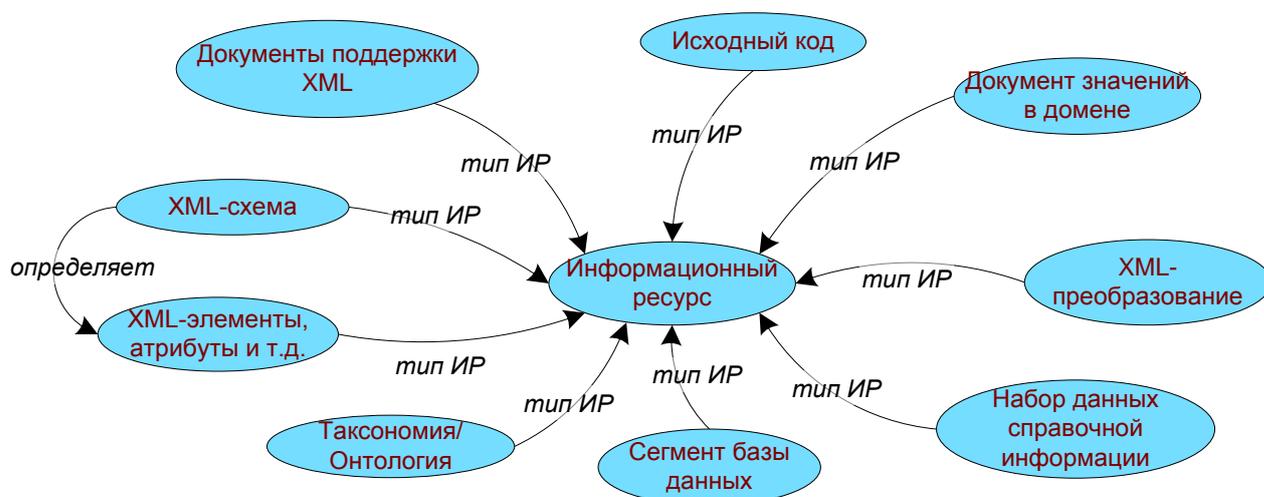


Рисунок 2.12 – Типы информационных ресурсов

Информационные ресурсы могут быть сгруппированы по различным критериям:

- тип метаданных;
- предмет;
- наборы элементов управления конфигурацией;

- состояние элементов управления конфигурацией в их жизненном (технологическом) цикле;
- определенными отношениями среди артефактов.

Критерии классификации метаданных могут все время развиваться, поскольку пользователи публикуют новые информационные ресурсы. Они контролируют их и управляют ими через пространства имен (ПИ).

Таблица 3 – Описание типов информационных ресурсов

Наименование типа ИР	Описание
Документ XML-схема	Документ-схема такой как DTD, который описывает структуру документа. Следующие типы схем могут поддерживаться реестром: DTD; RDFS; SOX; XDR; DCD; DML; BIZ; XSD; and OSC
XML-элемент	Элемент XML, либо сложного, либо терминального типа (содержит элементы или данные)
XML-атрибут	XML-атрибут, который может быть связан с одним или более XML-элементами. Атрибуты обеспечивают дополнительную информацию об элементах
Документы поддержки XML	Текстовый документ форматов «Word», «PDF» или «ASCII», которые могут быть связаны с одним или более информационными ресурсами
Исходный код	Один или более файлов (возможно и zip-файл), который показывает, как проводить разбор или использовать типовой документ XML
Документ значений в домене	Документ, содержащий допустимые значения для XML-элемента или XML-атрибута в домене. Этот документ также является XML-файлом, присоединенным к файлу «registry_domain_values.dtd»
XML-преобразование	Таблица стилей XSL определяет представление класса документов XML, описывая, как экземпляр класса преобразован в документ XML, который использует словарь форматирования

Наименование типа ИР	Описание
Набор данных справочной информации	Справочные данные системы
Сегмент базы данных	Часть или полноценная база данных
Узел таксономии	Узел информационного ресурса для каждого класса, описанного в формате OWL
Онтология	Информационный ресурс формата OWL, описывающий таксономию и метаданные

2.3 Модель взаимодействия действующих информационно-управляющих систем и систем в составе АПК «Безопасный город».

2.3.1 Общие положения по взаимодействию

Обмен информацией в рамках единого информационного пространства АПК «Безопасный город» осуществляется в автоматическом, автоматизированном:

- обмен информацией в автоматическом режиме реализуется без привлечения человеческих ресурсов средствами автоматизации при наличии сопряжения с функциональными системами участников межведомственного взаимодействия в рамках построения и развития АПК «Безопасный город»;
- обмен информацией в автоматизированном режиме реализуется средствами автоматизации с участием человеческих ресурсов в случаях, когда по техническим или экономическим причинам использование автоматического режима нецелесообразно.

Информация должна представляться своевременно, в четких формулировках, точная и достоверная, оптимальная с точки зрения систематизации и непрерывности сбора и обработки сведений.

Участники межведомственного взаимодействия обеспечивают возможность передачи информации в АПК «Безопасный город» с учетом разграничения прав доступа.

За счет реализации взаимодействия достигается повышение эффективности действующих АС обеспечивающих мониторинг в интересах общественной безопасности населения. Предпосылками для повышения эффективности при функционировании действующих АС в едином информационном пространстве служат следующие факторы:

- объектами мониторинга являются многокомпонентные системы, в которых не исключено взаимовлияние различных факторов подвергающихся мониторингу. В широком смысле, под мониторингом понимают идентификацию отклонений характеристик объекта мониторинга от штатного режима функционирования, либо выявления тенденции изменения характеристик на основе систематического сбора и анализа информации об объекте. Задача мониторинга характерна для тех видов деятельности, где изучаемый объект представляет сложную многокомпонентную систему, о состоянии которой можно судить по изменению свойств системы в целом или совокупности составляющих её объектов. В связи с вышеизложенным при комплексной оценке данных мониторинга, которая возможна только в результате интеграции систем, будет обеспечен более достоверный анализ ситуации и ее прогнозирование;

- повышение качества оценки обстановки за счет получения данных от различных источников;

- сокращение времени на оценку обстановки, принятие решения и реагирования на КСП за счет формирования компонент мониторинга, оценки обстановки, принятия решения и контроля исполнения в едином информационном пространстве.

На рисунке 2.13. показана общая (упрощенная) схема взаимодействия через интеграционную шину.

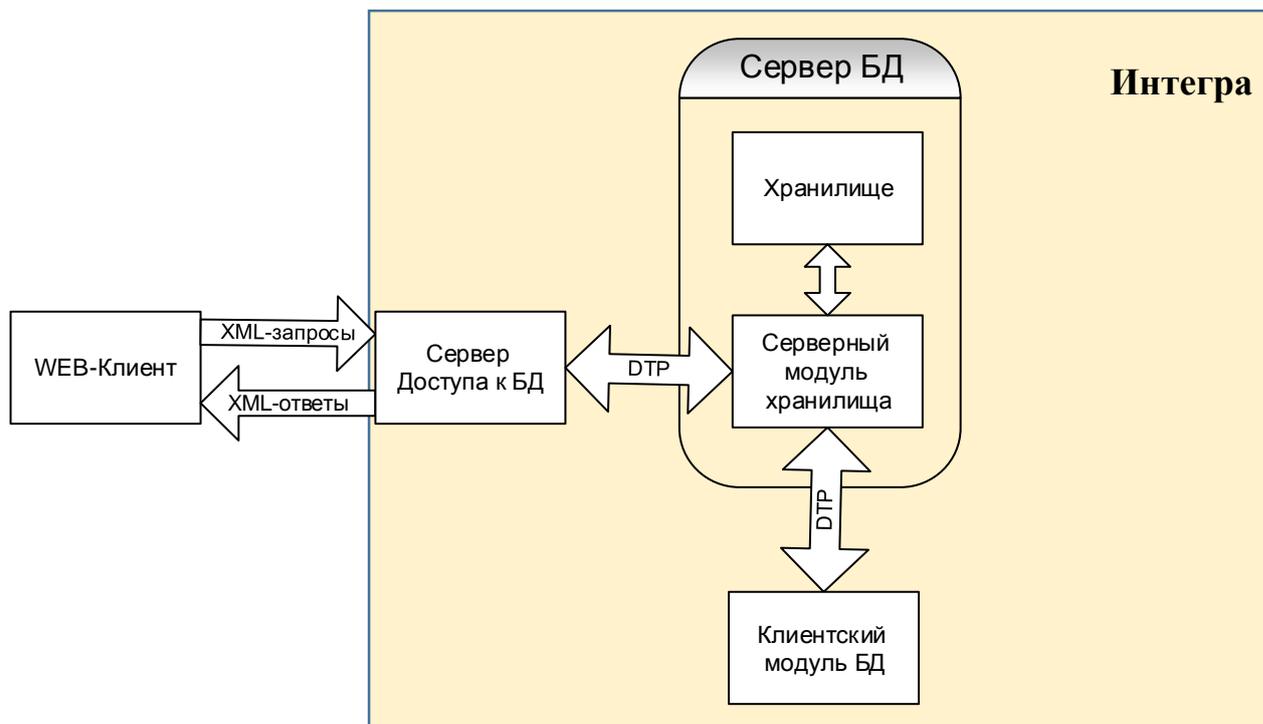


Рисунок 2.13 Общая схема взаимодействия при интеграции

Интеграционная шина должна обеспечить:

предоставление единого программного интерфейса информационного взаимодействия автоматизированных систем в АПК «Безопасный город»;

сквозное управление бизнес-процессами взаимодействующих систем, средствами унифицированного событийно-ориентированного механизма взаимодействия;

организацию структурированных, разделяемых данных («мастер»-справочников);

ведение нормативно-справочной информации;

разграничение доступа пользователей взаимодействующих систем к циркулирующим данным;

систематизированное хранение данных.

Интеграционная шина должна выполнять следующие функции:

создавать, удалять пользователей хранилища данных;

создавать, удалять, редактировать группы, роли пользователей;

назначать права пользователям и группам пользователей на добавление,

обновление, удаление данных в БД;

авторизовать пользователей в программе;

создавать структуры данных;

организовывать хранение структурированной нормативно-справочной информации.

организовывать статическую и алгоритмическую маршрутизацию информационных потоков;

производить поиск необходимых данных по атрибутам.

Сервер доступа в составе интеграционной шины предназначен для:

предоставления сопрягаемым системам API (в виде SOAP и REST веб-сервисов) для доступа к данным, содержащимся в базе данных интеграционной шины;

предоставление механизма асинхронного взаимодействия с сопрягаемыми системами на основе их гарантированного оповещения;

передачи специальным образом подготовленных данных из базы данных интеграционной шины в интегрируемые и взаимодействующие системы;

защиты данных в базе данных интеграционной шины от случайного изменения путем запрещения выполнения прямых SQL-запросов сопрягаемых систем к базе данных;

предоставления механизма сессионной работы с базой данных: открытие и поддержание отдельных для каждого пользователя соединений с базой данных, обращение к которым происходит с помощью временных ключей доступа;

предоставление механизма защиты от несанкционированного доступа к интеграционной шине;

предоставления сервисов-обработчиков жизненных циклов информационных объектов в базе данных интеграционной шины.

Информационное взаимодействие автоматизированных систем с АПК

«Безопасный город» осуществляется посредством передачи данных между соответствующей АС и сервером доступа в составе интеграционной шины.

Для передачи данных между системами и сервером доступа интеграционной шины должны использоваться web-сервисы, которые будут обмениваться между собой XML-сообщениями по протоколу SOAP.

Для этого на каждом из серверов сопрягаемых систем и интеграционной шиной должны быть размещены WSDL-описание web-сервисов.

Все web-сервисы, которые предназначены для передачи данных от взаимодействующих систем и обратно, реализуются на стороне сервера доступа интеграционной шины.

При этом, на стороне каждой из взаимодействующих систем может быть реализован один единственный сервис, который будет вызываться сервером доступа интеграционной шины и обеспечивать прием соответствующей системой асинхронной квитанции событийного оповещения. В том случае, если для взаимодействующей системы, по каким-либо причинам, не удастся реализовать программный интерфейс сетевого взаимодействия, на ее стороне должен быть организован клиентский сокет, в который интеграционная шина будет выдавать необходимую информацию.

2.3.2 Модель информационного взаимодействия

Модель информационного взаимодействия включает следующие процедуры:

Взаимодействующая система передает в интеграционную шину АПК «Безопасный город» требуемые данные путем вызова соответствующего метода web-сервиса, реализованного на стороне сервера доступа интеграционной шины.

При появлении в БД интеграционной шины данных, которые необходимо передать во взаимодействующую систему, сервер доступа интеграционной

шины вызывает метод web-сервиса или выдает в клиентский сокет соответствующей системы информацию о появлении в БД информационного ресурса, интересующего систему (квитанцию). При этом передается идентификатор этого информационного ресурса.

После того, как система получила квитанцию о появлении интересующего информационного ресурса, она вызывает соответствующий метод web-сервиса, который возвращает запрашиваемую структуру данных.

В случае, если взаимодействующая система знает данные, которые ей необходимо запросить из интеграционной шины, она может вызывать соответствующий метод web-сервиса, который возвращает запрашиваемую структуру данных. При этом, в качестве параметра, передается идентификатор запрашиваемых данных в контексте хранилища интеграционной шины.

Реализация данной модели взаимодействия позволяет:

Снизить потребность в ресурсах (человеко-часах), а соответственно - уменьшить риски по разработке ОДНОТИПНЫХ сервисов на каждой из сопрягаемых систем.

Позволит реализовать подход, при котором решение когда и в какой момент получать пакет информационного ресурса будет принимать сопрягаемая (заинтересованная) система, что, соответственно, уменьшит нагрузку на вычислительные мощности АПК «Безопасный город», а также повысит отказоустойчивость сопрягаемой системы.

Сервер доступа в составе интеграционной шине должен предоставлять наборы сервисов следующих типов:

асинхронный сервис событийного оповещения;

сервисы, обеспечивающие открытие и закрытие сеансов работы сопрягаемых систем с сервером доступа;

сервисы в составе специализированного программного интерфейса информационного взаимодействия, который позволяет общаться

автоматизированным системам с сервером доступа путем вызова специализированных методов web-сервисов, позволяющих обмениваться заранее описанными структурами данных. Описание структур данных предоставляется разработчиками взаимодействующих систем. Использование данного программного интерфейса является рекомендуемым методом информационного взаимодействия с интеграционной шиной. Данный интерфейс должен быть подробно изложен в протоколе информационного взаимодействия и реализован на этапе программной реализации протокола;

сервисы в составе унифицированного программного интерфейса информационного взаимодействия, основанного на понятии каталога данных (самоописываемого информационного ресурса табличной формы), который позволяет обеспечить получение и передачу в интеграционную шину структур данных, которые по тем или иным причинам не были заранее описаны и для них не создано специализированных методов web-сервисов. Данный программный интерфейс является рекомендуемым при работе с общей нормативно-справочной информацией, которая хранится и ведется в БД интеграционной шины.

сервисы в составе низкоуровневого программного интерфейса информационного взаимодействия.

3. ПРОЕКТ АРХИТЕКТУРЫ РЕШЕНИЙ АПК «БЕЗОПАСНЫЙ ГОРОД»

3.1 Требования к архитектуре АПК «Безопасный город»

Архитектура АПК «Безопасный город» должна обеспечивать:

- совершенствование системы управления муниципального звена РСЧС при решении задач обеспечения природно-техногенной и общественной безопасности, в том числе мониторинга, предупреждения, ликвидации ЧС и происшествий, организации межведомственного взаимодействия, организации оповещения, информирования и жизнеобеспечения населения, а также других задач, возложенных на РСЧС в соответствии с действующими нормативными правовыми актами;
- повышение эффективности анализа текущей обстановки и представления оперативной информации для принятия управленческих решений должностными лицами органов местного самоуправления и органов исполнительной власти субъекта Российской Федерации;
- своевременное получение текущей информации о состоянии объектов жизнеобеспечения, потенциально-опасных и критически важных объектов, а также оперативной информации при угрозе возникновения или возникновении чрезвычайных ситуаций природного и техногенного характера;
- сопряжение действующих информационно-аналитических, управляющих и других систем, обеспечивающих реализацию функций АПК «Безопасный город», на базе ЕДДС муниципального образования;
- организацию всестороннего информационного обеспечения деятельности органов повседневного управления РСЧС на муниципальном уровне в повседневной деятельности, а также при возникновении чрезвычайных ситуаций и происшествий;
- интеграцию АПК «Безопасный город» в комплексную систему обеспечения безопасности жизнедеятельности субъекта Российской Федерации

– инструмента обеспечения реализации задач и функций ЦУКС главных управлений МЧС России по субъектам Российской Федерации.

3.2 Функциональные сегменты, системы и подсистемы (типовой вариант) АПК «Безопасный город», их функции и технические характеристики, предложения по сопряжению.

3.2.1 Архитектура АПК «Безопасный город»

Функциональная структуры АПК «Безопасный город» включает в себя:

На региональном уровне - КСА «Региональная платформа»;

На муниципальном уровне - КСА ЕЦОР, включающий КСА функциональных блоков.

Типовой вариант функциональной структуры АПК «Безопасный город» представлен на рисунке 3.1.

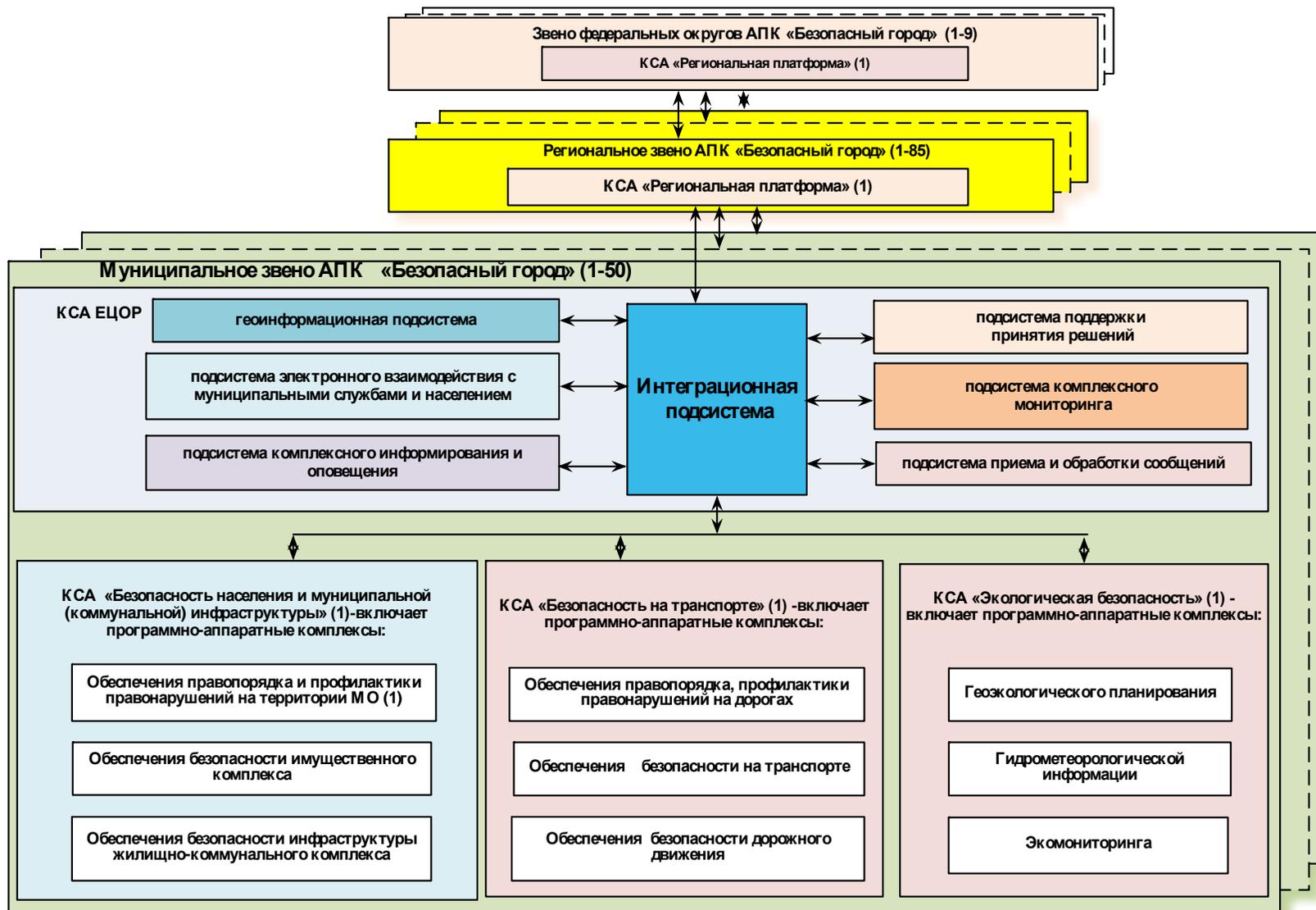


Рисунок 3.1- Типовой вариант функциональной структуры АПК «Безопасный город»

3.2.2 КСА «Региональная платформа»

3.2.2.1 Состав КСА «Региональная платформа»

В состав КСА «Региональная платформа» должны входить следующие подсистемы:

- подсистема интеграции данных;
- геоинформационная подсистема;
- подсистема электронного взаимодействия с должностными лицами.

3.2.2.2 Назначение и функции КСА «Региональная платформа»

КСА «Региональная платформа» предназначен для обеспечения органов исполнительной власти субъектов Российской Федерации оперативной и достоверной информации о ситуации в регионе, координации межведомственного взаимодействия на региональном уровне, обеспечения оперативной информационной экстренных и дежурных служб при угрозе возникновения или возникновении чрезвычайных ситуаций.

Основными функциями КСА «Региональная платформа» являются:

сопряжение с КСА ЕЦОР всех муниципальных образований, входящих в регион;

агрегация информации от всех КСА ЕЦОР муниципальных образований;

агрегация необходимой информации от федеральных и региональных КСА в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

предоставление органам исполнительной власти субъекта Российской Федерации информации о событиях в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания в регионе в целом и отдельно взятом муниципальном образовании в частности;

обеспечение доступа к необходимым информационным ресурсам АПК «Безопасный город» в соответствии с регламентами взаимодействия и предоставления информации.

3.2.2.3 Подсистема интеграции данных КСА «Региональная платформа»

Подсистема интеграции данных КСА «Региональная платформа» должна обеспечивать следующие функции:

- 1) обеспечение информационного обмена между федеральными и региональными КСА (перечень федеральных государственных информационных систем и систем мониторинга представлен в Приложении 3);
- 2) обеспечение информационного обмена между региональными КСА и КСА ЕЦОР муниципальных образований, входящих в регион;
- 3) ведение, хранение и резервное копирование информации о федеральных и региональных КСА, участвующих в информационном обмене;
- 4) обеспечение целостности данных;
- 5) обеспечение авторизованного доступа к данным по установленным регламентам доступа и взаимодействия;
- 6) ведение журнала операций информационного обмена;
- 7) организацию маршрутизации, ведение очередей и гарантированную доставку информации, передаваемой между федеральными и региональными КСА и КСА ЕЦОР муниципальных образований субъекта Российской Федерации;
- 8) агрегацию структурированной и обработанной информации, полученной от всех КСА ЕЦОР, входящих в регион;
- 9) агрегацию информации, полученной от федеральных и региональных КСА;
- 10) формирование базы мета-данных по интегрированным в единую информационную среду КСА, входящих в состав АПК «Безопасный город».

3.2.2.4 Геоинформационная подсистема КСА «Региональная платформа»

Геоинформационная подсистема КСА «Региональная платформа» предназначена для отображения на электронной карте совокупной информации (об объектах, периферийных устройствах, событиях), связанной с обеспечением

общественной безопасности, правопорядка и безопасности среды обитания в регионе и отдельно взятом муниципальном образовании региона.

Геоинформационная подсистема КСА «Региональная платформа» должна обеспечивать следующие функции:

1) отображения информации из сопрягаемых федеральных и региональных КСА, КСА ЕЦОР муниципальных образований в виде семантических слоев, отражающих природно-географические, социально-демографические, экономические характеристики территории;

2) отображения объектов инженерной, транспортной и социальной инфраструктуры муниципальных образований, относящихся к региону;

3) добавления новых слоев, а также добавление атрибутов в существующие тематические слои;

4) привязки к объектам на электронной карте электронных паспортов соответствующих потенциально опасных и критически важных объектов, социально значимых объектов, объектов с массовым пребыванием людей;

5) позиционирования объектов на электронной карте на основе указания адреса или получаемого тревожного события от систем мониторинга;

6) атрибутивного поиска на карте объектов классифицированных типов;

7) указания и уточнения местоположения объектов, связанных с происшествием, как с помощью визуальных графических средств, так и с помощью прямого ввода координат;

8) регулярного обновления электронных карт подсистемы для обеспечения актуальности картографической информации.

3.2.2.5 Подсистема электронного взаимодействия с должностными лицами в составе КСА «Региональная платформа»

Подсистема электронного взаимодействия должна предоставлять пользователям следующие возможности:

1) предоставлять актуальную информацию о событиях, напрямую или косвенно связанных с обеспечением безопасности жизнедеятельности, а также об обращениях населения с обозначением их статуса и с привязкой к местности;

2) информировать должностных лиц о необходимых мероприятиях при реагировании на ЧС или событиях в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

3) предоставлять пользователям сети Интернет актуализированную информацию о событиях, связанных с безопасностью жизнедеятельности на территории региона;

4) предоставлять информацию о статусах исполнения обращений граждан;

5) обеспечивать фильтрацию зарегистрированных событий.

3.2.2.6 Требования к информационному взаимодействию КСА «Региональная платформа»

Внешнее взаимодействие КСА «Региональная платформа» должно предусматривать информационное взаимодействие со следующими КСА:

- КСА территориальных органов ФОИВ в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

- КСА ОИВ субъекта РФ в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

- КСА взаимодействующих ОИВ субъекта РФ;

- КСА ЕЦОР муниципальных образований, относящихся к региону.

Внутреннее взаимодействие КСА «Региональная платформа» должно выполняться по следующему принципу. Подсистема интеграции данных должна обеспечивать сопряжение внешних КСА и подсистем, входящих в состав КСА «Региональная платформа». Информация, поступающая от сопрягаемых КСА должна отображаться на электронной карте геоинформационной системы в составе КСА «Региональная платформа» в соответствии с разграничением прав доступа.

Внешнее и внутреннее взаимодействие КСА «Региональная платформа» должно выполняться на основе Единого стека открытых протоколов (далее ЕСОП), требования к которому приведены в Приложении 2.

Взаимодействие подсистем КСА «Региональная платформа» должно осуществляться на основе принципов построения системных сервисов (служб) и

взаимно-совместимых приложений (стандарты типа CORBA, DCOM, SOAP/XML, RPC, RMI или JSON).

Должны быть обеспечены следующие требования к характеристикам взаимосвязи подсистем КСА «Региональная платформа» между собой, а также с подсистемами смежных КСА:

узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;

базовый протокол обмена сообщениями - XML/SOAP.

3.2.2.7 Требования к техническому обеспечению КСА «Региональная платформа»

Телекоммуникационная инфраструктура КСА «Региональная платформа» должна обеспечить надежный и безопасный обмен информацией между всеми КСА ЕЦОР субъекта Российской Федерации.

В основу построения телекоммуникационной инфраструктуры должны быть заложены следующие принципы:

- комплексность, унификация и совместимость реализуемых проектных, технических и технологических решений;
- открытость архитектуры построения;
- обеспечение стандартных интерфейсов и протоколов;
- резервирование каналов передачи информации;
- обеспечение централизованного сетевого мониторинга и администрирования;
- обеспечение возможности организации круглосуточного сервисного обслуживания оборудования;
- возможность поэтапного создания и ввода в эксплуатацию без нарушения функционирования существующих элементов;
- возможность приоритетного использования существующих сетей передачи данных.

Телекоммуникационная инфраструктура должна обеспечивать:

- поддержку стека сетевых протоколов TCP/IP;

- поддержку протоколов приоритетной обработки очередей обслуживания;
- поддержку транспортных протоколов реального времени;
- обеспечение передачи различных видов трафика (данные, аудио- и видео-потoki, управление) и обеспечение динамического распределения полосы пропускания;
- использование резервных каналов связи в режиме балансирования нагрузки;
- оперативную локализацию сбоев в сетевом оборудовании и каналах связи;
- высокий уровень отказоустойчивости, позволяющий осуществлять быстрое автоматическое восстановление работоспособности в случае единичного выхода из строя резервируемых критичных компонент активного сетевого оборудования или основных физических каналов связи в телекоммуникационной инфраструктуре.

Подробные требования к техническому обеспечению КСА «Региональная платформа» представлены в Приложении 4 (Требования к вычислительной инфраструктуре и обеспечивающим прикладным подсистемам КСА «Региональная платформа»).

3.2.3.8 Требования к системному программному обеспечению КСА «Региональная платформа»

Программное обеспечение КСА «Региональная платформа» представляет совокупность общего программного обеспечения и специального программного обеспечения.

Программное обеспечение КСА «Региональная платформа» должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в ее состав перспективных КСА.

Программное обеспечение, технология (включая нормативно-техническую документацию) его разработки должны обеспечивать возможность

согласованной разработки унифицированного (типового) программного обеспечения силами нескольких разработчиков.

Требования к общему программному обеспечению КСА «Региональная платформа» представлены в Приложении 5 (Требования к общему программному обеспечению).

Требования к специальному программному обеспечению КСА «Региональная платформа» представлены в Приложении 6 (Требования к специальному программному обеспечению КСА «Региональная платформа»).

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

3.2.2.9 Требования к информационному обеспечению КСА «Региональная платформа»

Информационное единство комплексов средств автоматизации КСА «Региональная платформа» должно обеспечиваться использованием общей системы кодирования и классификации информации.

Единая система кодирования и классификации информации должна обеспечивать:

централизованное ведение словарей и классификаторов, использующихся в информационном взаимодействии;

выполнение необходимых технологических функций, в том числе предоставление возможности обмена данными со смежными по отношению к КСА «Региональная платформа».

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

Дополнительные требования к информационному обеспечению КСА «Региональная платформа» представлены в приложениях:

Приложение 7 - Требования к информационной совместимости КСА «Региональная платформа» со смежными КСА;

Приложение 8 - Требования по применению систем управления базами данных КСА АПК «Безопасный город»;

Приложение 9 - Требования к структуре процесса сбора, обработки, передачи данных в АПК «Безопасный город»;

Приложение 10 - Требования к защите данных от разрушений при авариях и сбоях в электропитании АПК «Безопасный город»;

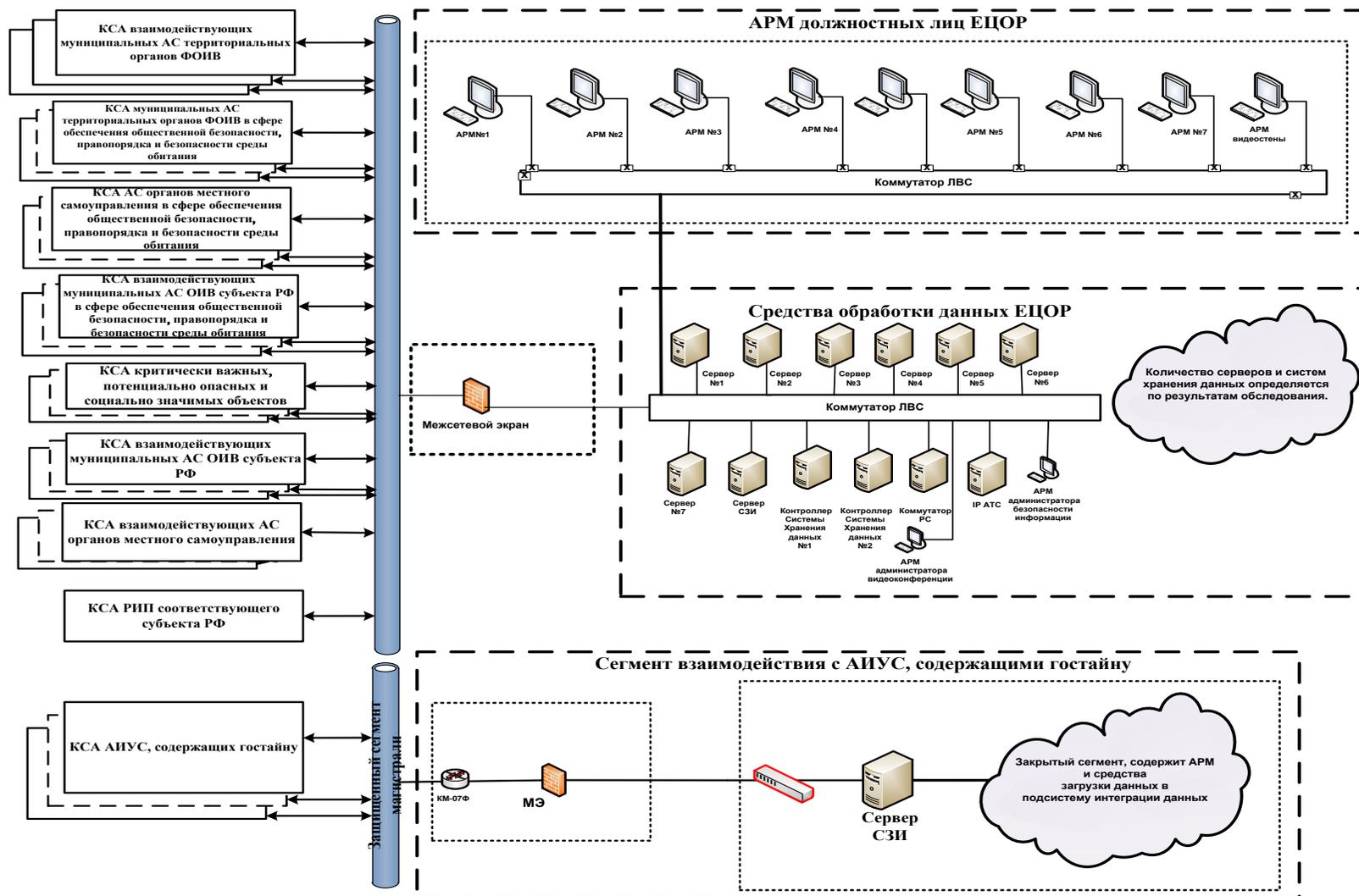
Приложение 11 - Требования к контролю, хранению, обновлению и восстановлению данных АПК «Безопасный город»;

Приложение 12 - Требования к процедуре придания юридической силы документам, продуцируемым техническими средствами АПК «Безопасный город».

Программное обеспечение должно быть сертифицировано по требованиям информационной безопасности.

3.2.4 КСА Единый центр оперативного реагирования

Структурная схема КСА ЕЦОР АПК «Безопасный город» приведена на рисунке 3.2



Примечание-количество серверов, систем хранения данных, АРМ и их комплектация определяется в ходе обследования объекта размещения

Рисунок 3.2. Структурная схема КСА ЕЦОР АПК «Безопасный город»

3.2.4.1 Состав КСА Единый центр оперативного реагирования

КСА Единый центр оперативного реагирования функционального блока «Координация работы служб и ведомств» включает в свой состав следующие подсистемы:

а) Функциональные

- подсистема приема и обработки сообщений;
- подсистема поддержки принятия решений;
- подсистема комплексного мониторинга;
- геоинформационная подсистема;
- подсистема электронного взаимодействия с муниципальными службами и населением;
- интеграционная подсистема;
- подсистема комплексного информирования и оповещения;

б) Обеспечивающие

- подсистема обеспечения информационной безопасности;
- подсистема резервирования;
- подсистема административного управления;
- система хранения данных.

3.2.4.2 Назначение и функциональность КСА ЕЦОР

КСА ЕЦОР предназначен для обеспечения решения задач оперативного реагирования на угрозы общественной безопасности, правопорядка и безопасности среды обитания, а также обеспечения эффективного взаимодействия и координации органов повседневного управления, служб экстренного реагирования и муниципальных служб.

КСА ЕЦОР должен обеспечивать:

- 1) централизованный мониторинг угроз общественной безопасности, правопорядка и безопасности среды обитания, включая:
 - прием и регистрацию сообщений об угрозах, общественной безопасности, правопорядка и безопасности среды обитания по доступным в

муниципальном образовании каналам связи, включая телефонную связь, интернет, средства экстренной связи;

- комплексный мониторинг угроз общественной безопасности, правопорядка и безопасности среды обитания посредством агрегации данных, полученных от средств мониторинга;

- возможность подключения и управления периферийными устройствами КСА сегментов АПК «Безопасный город» в соответствии с определенными регламентами доступа;

2) поддержку принятия решений, включая:

- категоризацию событий и соответствующих им правил реагирования для экстренных оперативных и муниципальных служб, определенных регламентами, нормативными и правовыми документами;

- автоматическое предоставление сценария реагирования в соответствии с установленными регламентами взаимодействия;

- моделирование различных сценариев возникновения потенциальных угроз безопасности среды обитания и общественной безопасности муниципального образования, включая построение прогнозов их развития и отображение на электронной карте результатов моделирования;

- оценку сложившейся обстановки и динамическую актуализацию результатов моделирования с учетом поступающих данных с КСА сегментов АПК «Безопасный город»;

3) управление и координацию взаимодействия, включая:

- обеспечение доступа к единой информационной среде, включая доступ содержащейся в нем реестровой, справочной и пространственной информации об объектах инженерной, транспортной и социальной инфраструктуры;

- формирование в автоматическом или полуавтоматическом режиме поручений службам оперативного реагирования и муниципальных служб по определенным сценариям реагирования в соответствии с категориями событий;

- обеспечение оперативного информирования о статусе события и поручения служб оперативного реагирования и муниципальных служб, отвечающих за выполнение работ;

- координацию и обеспечение информационной поддержки при реагировании соответствующим органам повседневного управления, службам экстренного реагирования и муниципальных служб, включая предоставление необходимой реестровой, справочной, пространственной информации из КСА сегментов АПК «Безопасный город»;

- оперативное доведение информации и задач до органов повседневного управления, служб экстренного реагирования и муниципальных служб, в соответствии с определенными регламентами взаимодействия;

- управление поручениями и контроль исполнения поручений;

- обеспечение отображения на электронной карте полной информации о событии, включая информацию об объектах инженерной, транспортной и социальной инфраструктуры муниципального образования, а также просмотр изменения статусов события и выданных поручений.

4) информирование и оповещение населения муниципального образования, а именно:

- визуализацию функционирования системы оповещения населения муниципального образования;

- информирование населения муниципального образования посредством информационных интернет-ресурсов, мобильных приложений и иных информационных каналов о результатах реагирования органов повседневного управления, служб экстренного реагирования и муниципальных служб на угрозы общественной безопасности, правопорядка и безопасности среды обитания.

5) формирование единого информационного пространства, а именно:

- обеспечение интеграции и информационного взаимодействия между КСА сегментов «Безопасный город» посредством муниципальной и региональной интеграционных платформ;

- организация единого информационного-справочного пространства АПК «Безопасный город»;
- обеспечение защищенного доступа к информации с использованием средств криптографической защиты информации;
- автоматическое архивирование и обеспечение хранения видео-информации и отчетной информации о событиях и всей сопутствующей информации;
- формирование отчетов для муниципальных органов власти, бизнеса с гибким механизмом настройки и расширения возможностей, позволяющим формировать отчеты за любой период времени;
- обеспечение возможности формирования сводных отчетов по нескольким критериям;
- обеспечение качественного обмена информацией о результатах непрерывного мониторинга услуг связи и измерения эксплуатационных показателей сети, оперативное уведомление о нарушениях связи между объектами инфраструктуры или об отклонении ее качества от требуемого уровня.

3.2.4.3 Подсистема приема и обработки сообщений КСА ЕЦОР

Подсистема приема и обработки сообщений КСА ЕЦОР предназначена для обработки сообщений о происшествиях, с возможностью привязки происшествия к местности на электронной карте и должна обеспечивать ЕДДС возможностями по приему сообщений о КСП на территории муниципального образования в категорированном виде, обеспечивать хранение структурированной информации по поступившим сообщениям в базе данных, а также контролировать качество работы диспетчеров.

подсистема приема и обработки сообщений КСА ЕЦОР должна обеспечивать:

- прием и обработку вызовов с возможностью заполнения электронной регистрационной карточки;

- прием, регистрацию, документирование сообщений поступающих посредством обращений через подсистему электронного взаимодействия с муниципальными службами и населением с автоматическим заполнением информации, указанной в обращении;
- прием и обработку событий поступающих от подсистемы комплексного мониторинга (время события, местоположение события, тип события и возможные последствия);
- позиционирование местоположения события на электронной карте геоинформационной подсистемы;
- возможность обновления информации в карточке происшествия;
- выбор состава оповещаемых служб в зависимости от типа происшествия;
- контроль хода исполнения поручения с возможностью информирования диспетчера ЕДДС при угрозе срыва срока исполнения поручения.

3.2.4.4 Подсистема поддержки принятия решений КСА ЕЦОР

Подсистема поддержки принятия решений должна обеспечивать информационно-аналитическое сопровождение деятельности служб и организаций, привлекаемых к реагированию на КСП, посредством предоставления результатов моделирования развития КСП и оценки последствий КСП, а также посредством определения сценария реагирования на КСП.

Подсистема поддержки принятия решений должна обеспечивать выполнение следующих функциональных возможностей:

- опрос абонента по заранее определенным сценариям (наличие системы детерминированных диалогов);
- формирование совокупного плана реагирования по КСП, а также сценариев реагирования и инструкций диспетчеру ЕДДС по обработке зарегистрированного события на основе утвержденных регламентов при ликвидации КСП и происшествий;

- моделирования развития КСП и расчет предполагаемых потерь и ущерба;
- формирование графиков и отчетов на основе имеющейся (накапливаемой) в Системе информации.
- организация межведомственного взаимодействия в работе служб экстренного реагирования при реагировании на КСП;
- обеспечение возможности управления статусами инцидентов в многопользовательском режиме;
- автоматизированное формирование поручений на основе заранее подготовленных шаблонов и сценариев реагирования;
- контроль хода исполнения поручения и автоматический запуск сценариев информирования при угрозе срыва срока исполнения поручения.

Подсистема должна обеспечивать результатами расчета предполагаемых потерь и ущерба, посредством Подсистемы интеграции данных, следующие подсистемы:

- подсистема приема и обработки сообщений, в виде описания и количественных показателей;
- подсистема «Интеграционная географическая информационная система», в виде слоев предполагаемых зон поражения (затопления), а также необходимой и достаточной зоны информирования и оповещения населения;
- подсистема электронного взаимодействия с муниципальными службами и населением, в виде информационного сообщения и инструкции действий для населения;
- подсистема комплексного информирования и оповещения, в виде списка средств оповещения, попадающих в расчетную зону оповещения населения.

3.2.4.5 Подсистема комплексного мониторинга

Подсистема комплексного мониторинга предназначена для сбора и анализа параметров контролируемых объектов и передачи их в подсистемы по запросу или в случае детектирования определенных критических значений.

Подсистема должна обеспечивать необходимой информацией, посредством Подсистемы интеграции данных, следующие подсистемы:

а) подсистему приема и обработки сообщений, с целью автоматического формирования и заполнения информационной карточки происшествия;

б) подсистему поддержки принятия решений, для следующих целей:

- автоматического запуска расчетных задач по моделированию и прогнозированию развития КСП;

- анализа динамики изменений контролируемых параметров, а также формирования статистики и отчетности по ним;

в) геоинформационную подсистему для следующих целей:

- специальной маркировки (на электронной карте) условного знака первоисточника информации, зафиксировавшего критическое значение;

- предоставление информации о текущих показателях контролируемого объекта по запросу пользователя;

- специальной маркировки (на электронной карте) условного знака первоисточника информации, по которому обнаружен технический сбой.

3.2.4.6 Геоинформационная подсистема

Геоинформационная подсистема должна обеспечивать возможность отображения на карте информации по КСП на территории муниципального образования, а также визуализации информации из подсистем регионального и муниципального уровней в виде семантических слоев, отражающих природно-географические, социально-демографические, экономические характеристики территории.

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

Геоинформационная подсистема должна предоставлять следующие функциональные возможности:

а) ведения пространственной информации следующих семантических слоев:

- набор слоев инфраструктуры систем мониторинга, сопрягаемых с КСА ЕЦОР, включая характеристики, фиксируемых ими параметров;

- набор слоев органов экстренного оперативного реагирования, визуализирующий места расположения ЕДДС, взаимодействующих ДДС и подразделений служб экстренного реагирования;

- места расположения потенциально опасных и критически важных объектов;

- места расположения социально значимых объектов, объектов с массовым пребыванием людей;

- места расположения мобильных подразделений, привлекаемых к предупреждению и ликвидации кризисных ситуаций и происшествий

б) возможность привязки к объектам на электронной карте электронных паспортов соответствующих потенциально опасных и критически важных объектов, социально значимых объектов, объектов с массовым пребыванием людей;

в) позиционирования объектов на электронной карте на основе указания адреса и/или получаемого тревожного события от систем мониторинга;

г) атрибутивного поиска на карте объектов классифицированных типов;

д) указания и уточнения местоположения объектов, связанных с происшествием, как с помощью визуальных графических средств, так и с помощью прямого ввода координат.

Пользовательский интерфейс подсистемы должен предоставлять следующие функциональные возможности:

- атрибутивный поиск на карте объектов классифицированных типов;

- указание и уточнение местоположения объектов, связанных с происшествием, как с помощью визуальных графических средств, так и с помощью прямого ввода координат;

- прокладка маршрутов движения между заданными объектами.

3.2.4.7 Подсистема электронного взаимодействия с муниципальными службами и населением

Подсистема электронного взаимодействия с муниципальными службами и населением КСА ЕЦОР должна обеспечивать информационное освещение оперативной обстановки на территории муниципального образования, предоставлять возможность взаимодействия населения и организаций с органами местного самоуправления, экстренными и оперативными службами по комплексу вопросов, связанных с обеспечением общественной безопасности, правопорядка и безопасности среды обитания.

Подсистема электронного взаимодействия с муниципальными службами и населением должна представлять собой вэб-портал предназначенный для организации взаимодействия ЕДДС, муниципальных служб и населения с использованием веб-интерфейса.

Подсистема электронного взаимодействия с муниципальными службами и населением должна предоставлять пользователям сети Интернет следующие возможности:

а) предоставлять актуальную информацию о событиях, напрямую или косвенно связанных с обеспечением безопасности жизнедеятельности, а так же о допустимых к общему доступу инцидентах и заявках с обозначением их статуса;

б) информировать оператора КСА ЕЦОР о зарегистрированных, посредством подсистемы электронного взаимодействия, событиях с автоматической регистрацией и постановкой заявки на контроль исполнения;

в) предоставление пользователям сети Интернет необходимой актуализированной информации о событиях, связанных с безопасностью жизнедеятельности;

г) предоставление информации о статусах исполнения обращений граждан;

д) присоединения мультимедийной информации к сообщению о событии;

е) определение устройства пользователя, обращающегося с использованием подсистемы электронного взаимодействия с автоматическим предоставлением соответствующей версии веб-интерфейса (для мобильных устройств – мобильную версию);

ж) фильтрацию зарегистрированных событий, отображаемых на электронной карте веб-интерфейса подсистемы электронного взаимодействия по следующим критериям:

- завершенные события;
- обрабатываемые события;
- категории событий;
- события по заданному периоду времени.

Подсистема электронного взаимодействия с муниципальными службами и населением должна предоставлять должностным лицам муниципального образования следующие возможности:

- предоставления необходимой и достаточной информации по КСП;
- оперативного предоставления плана реагирования на КСП;
- формирование уведомления о поступлении нового задания;
- ведение журнала приема и обработки заданий;
- обработка заданий;
- отображение совокупной информации на электронной карте города с учетом разграничения прав доступа.

- отображение совокупной статистической информации об основных показателях функционирования АПК «Безопасный город» с использованием графиков и цветовой маркировки критических показателей, отслеживаемых в режиме реального времени.

3.2.4.8 Подсистема комплексного информирования и оповещения

Подсистема комплексного оповещения и информирования должна обеспечить:

в части систем оповещения:

мониторинг работоспособности системы оповещения на территории муниципального образования;

визуализация выполнения системой оповещения сценариев (регламентов) по предназначению на территории муниципального образования.

в части системы информирования:

мониторинг и контроль системы информирования.

Требования к функциям данной подсистемы должны касаться контроля функционального состояния комплексной системы информирования и оповещения населения при угрозе и возникновении чрезвычайных ситуаций.

Подсистема комплексного информирования и оповещения взаимодействует, через Подсистему интеграции данных (по правилам Единого стека открытых протоколов).

3.2.4.9 Подсистема интеграции данных

Подсистема интеграции данных должна обеспечивать информационный обмен между сопрягаемыми подсистемами и КСА ЕЦОР.

Основными функциями подсистемы интеграции данных должны являться:

- интеграция подсистем и КСА с целью организации комплексного информационного взаимодействия, а также с целью обеспечения целостного процесса обработки информации;
- обеспечение функционирования сопрягаемых подсистем и КСА в едином информационном пространстве и в единой понятийной среде.

Для формирования единого информационного пространства для КСА, участвующих в информационном обмене в рамках построения и развития АПК «Безопасный город» должны использоваться следующие источники информации:

- системы мониторинга и видеонаблюдения объектов промышленного и сельскохозяйственного производства, критически важных и потенциально опасных объектов, транспорта, связи, технических сооружений и сетей коммунального хозяйства (водо-, газо-, тепло-, электроснабжения);

- системы мониторинга сил и средств постоянной готовности, действующих на территории муниципального образования;
- системы видеонаблюдения в местах массового скопления людей и проведения массовых мероприятий, на транспорте и объектах транспортной инфраструктуры, местах отдыха, развлекательных и торговых центрах;
- автоматизированные системы управления муниципальным хозяйством;
- федеральные государственные информационные системы и системы мониторинга (перечень представлен в и 3);
- региональные государственные системы мониторинга угроз и информационные системы.

Требования к обеспечивающим системам представлены в Приложении 13.

Требования к вычислительной инфраструктуре КСА ЕЦОР представлены в Приложении 14.

3.2.4.10 Требования к информационному взаимодействию КСА ЕЦОР

Внешнее взаимодействие КСА ЕЦОР должно предусматривать информационное взаимодействие со следующими КСА:

- 1) КСА муниципальных территориальных органов ФОИВ в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;
- 2) КСА органов местного самоуправления в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;
- 3) КСА критически важных, потенциально опасных и социально значимых объектов;
- 5) КСА взаимодействующих муниципальных ОИВ субъекта РФ в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;
- 6) КСА взаимодействующих муниципальных ОИВ субъекта РФ;
- 7) КСА взаимодействующих органов местного самоуправления;
- 8) КСА «Региональная платформа» соответствующего субъекта РФ;

Внутреннее взаимодействие КСА ЕЦОР должно выполняться по следующему принципу. Подсистема интеграции данных должна обеспечивать сопряжение внешних КСА и подсистем, входящих в состав КСА ЕЦОР. Информация, поступающая от сопрягаемых КСА должна отображаться на электронной карте геоинформационной подсистемы в составе КСА ЕЦОР в соответствии с разграничением прав доступа.

Внешнее и внутреннее взаимодействие КСА ЕЦОР должно выполняться на основе Единого стека открытых протоколов, требования к которому приведены в Приложении 2.

Взаимодействие подсистем КСА ЕЦОР должно осуществляться на основе принципов построения системных сервисов (служб) и взаимно-совместимых приложений (стандарты типа CORBA, DCOM, SOAP/XML, RPC, RMI или JSON).

Должны быть обеспечены следующие требования к характеристикам взаимосвязи подсистем КСА «Региональная платформа» между собой, а также с подсистемами смежных КСА:

- узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;
- базовый протокол обмена сообщениями - XML/SOAP.

3.2.4.11 Требования к техническому обеспечению КСА ЕЦОР функционального блока «Координация работы служб и ведомств»

Средства вычислительной техники должны быть максимально приспособлены для последующей модернизации.

Для серверных и сетевых компонент, а так же для оборудования, выход которого из строя приводит к недоступности сервисов КСА ЕЦОР, время восстановления не должно превышать 2 часа. Время восстановления для остальной техники 24 часа.

Активное сетевое оборудование должно обеспечивать достаточную пропускную способность для функционирования сегментов АПК «Безопасный город» в соответствии с настоящими требованиями.

Используемые модели и компоненты активного сетевого оборудования должны соответствовать объемам передаваемого трафика в рамках АПК «Безопасный город».

Узлы сети должны обеспечивать высокую готовность (24/7). Для участков сети, требующих повышенную надежность, необходимо предусмотреть резервные каналы связи.

Для линий связи проходящих через общедоступные помещения и линий связи соединения с глобальной вычислительной сетью Интернет должны использоваться средства шифрования трафика.

Подробные требования к техническому обеспечению КСА ЕЦОР представлены в Приложении 14 (Требования к вычислительной инфраструктуре КСА ЕЦОР) и Приложении 15 (Требования к подсистемам КСА ЕЦОР).

3.2.4.12 Требования к системному программному обеспечению КСА ЕЦОР функционального блока «Координация работы служб и ведомств»

Системное программное обеспечение КСА ЕЦОР представляет совокупность общего программного обеспечения и специального программного обеспечения.

Программное обеспечение КСА ЕЦОР должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития.

Требования к общему программному обеспечению КСА ЕЦОР представлены в Приложении 5 (Требования к общему программному обеспечению).

Требования к специальному обеспечению КСА ЕЦОР представлены в Приложении 15 (Требования к специальному программному обеспечению КСА ЕЦОР).

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

3.2.4.13 Требования к информационному обеспечению КСА ЕЦОР функционального блока «Координация работы служб и ведомств»

Информационное единство КСА ЕЦОР функционального блока «Координация работы служб и ведомств» должно обеспечиваться использованием общей системы кодирования и классификации информации.

Единая система кодирования и классификации информации должна обеспечивать:

централизованное ведение словарей и классификаторов, использующихся в информационном взаимодействии;

выполнение необходимых технологических функций, в том числе предоставление возможности обмена данными со смежными КСА по отношению к КСА ЕЦОР.

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

Дополнительные требования к информационному обеспечению КСА ЕЦОР функционального блока «Координация работы служб и ведомств» представлены в приложениях:

Приложение 2 - Требования к Единому стеку открытых протоколов информационного взаимодействия АПК «Безопасный город»;

Приложение 8 - Требования по применению систем управления базами данных АПК «Безопасный город»;

Приложение 9 - Требования к структуре процесса сбора, обработки, передачи данных в АПК «Безопасный город»;

Приложение 10 - Требования к защите данных от разрушений при авариях и сбоях в электропитании АПК «Безопасный город»;

Приложение 11 - Требования к контролю, хранению, обновлению и восстановлению данных АПК «Безопасный город»;

Приложение 12 - Требования к процедуре придания юридической силы документам, продуцируемым техническими средствами АПК «Безопасный город».

Программное обеспечение должно быть сертифицировано по требованиям информационной безопасности.

3.2.5 КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»

3.2.5.1 Состав КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»

КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры» состоит из следующих программно-аппаратных комплексов:

1) обеспечения правопорядка и профилактики правонарушений на территории муниципального образования в составе следующих подсистем:

- подсистема интеллектуального видеонаблюдения, обеспечивающая автоматическое детектирование (видеообнаружения, видеоидентификации и видеораспознавания) определенных событий с целью мониторинга, предупреждения и профилактики правонарушений;

- подсистема оценки качества деятельности представителей территориальных органов федеральных органов исполнительной власти, ответственных за обеспечение правопорядка и профилактики правонарушений на территории муниципального образования;

- подсистема позиционирования мобильным персоналом органов исполнительной власти, ответственных за правопорядка и профилактики правонарушений на территории муниципального образования;

- подсистема обеспечения экстренной связи;

- подсистема управления мобильным персоналом органов исполнительной власти, ответственных за правопорядка и профилактики правонарушений на территории муниципального образования;

- подсистема управления территориальными органами федеральных органов исполнительной власти, ответственных за обеспечение правопорядка и профилактики правонарушений на территории муниципального образования;

- подсистема управления видеонаблюдением и видеопотоками.

2) обеспечения безопасности инфраструктуры жилищно-коммунального комплекса в составе КСА следующих подсистем:

- мониторинга и управление работой по предупреждению и ликвидации чрезвычайных ситуаций, вызванных сбоями в работе коммунальной инфраструктуры;

- подсистема мониторинга сбоев в работе сети водоснабжения;

- подсистема мониторинга сбоев в работе сети газоснабжения;

- подсистема мониторинга сбоев в работе сети теплоснабжения;

- подсистема мониторинга сбоев в работе сети электроснабжения;

- подсистема мониторинга, предупреждения и ликвидации чрезвычайных ситуаций, возникающих при нарушении правил пожарной безопасности;

- обеспечения безопасности охраняемых объектов, придомовых территорий и объектов социального назначения;

- обеспечения экстренной связи;

- управления ремонтными работами на объектах муниципальной (коммунальной) инфраструктуры;

- подсистема управления технического обеспечения и ремонтного обслуживания сети водоснабжения;

- подсистема управления технического обеспечения и ремонтного обслуживания сети газоснабжения;

- подсистема управления технического обеспечения и ремонтного обслуживания сети теплоснабжения;

- подсистема управления технического обеспечения и ремонтного обслуживания сети электроснабжения;
- подсистема информирования и оповещения населения;
- подсистема моделирования предпосылок и оценка последствий чрезвычайных ситуаций.

3) обеспечения безопасности имущественного комплекса, в составе следующих подсистем:

- подсистема управления дежурного плана города;
- подсистема поддержки принятия решений при управлении муниципальными активами;
- подсистема обеспечения социальной безопасности;
- подсистема управления земельным муниципальным реестром;
- подсистема управления реестром электросетей;
- подсистема управления реестром сетей и сооружений водоснабжения;
- подсистема управления реестром тепловых сетей;
- подсистема управления реестром дорог;
- подсистема управления реестром телекоммуникаций;
- подсистема управления социальным реестром;
- подсистема управления реестром мест обработки и утилизации отходов;
- подсистема управления реестром природоохранных и рекреационных зон и паркового хозяйства.

3.2.5.2 Назначение и функциональность КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»

3.2.5.2.1 Назначение и функциональность программно-аппаратных комплексов «Обеспечения правопорядка и профилактики правонарушений»

Программно-аппаратные комплексы «Обеспечения правопорядка и профилактики правонарушений на территории муниципального образования» КСА функционального блока «Безопасность населения и муниципальной

(коммунальной) инфраструктуры» предназначены для решения комплекса задач обеспечения общественной безопасности и правопорядка посредством своевременной идентификации и реагирования на потенциальные угрозы общественной безопасности и нарушений правопорядка.

Сегмент «Обеспечения правопорядка и профилактики правонарушений на территории муниципального образования» должен обеспечивать выполнение следующих функций:

- 1) осуществление видеонаблюдения и видеоанализа, в том числе:
 - получение видеоизображения с мест установки видеокамер на критически важных, потенциально опасных и социально значимых объектах (в том числе дошкольные образовательные учреждения, образовательные учреждения и другие);
 - отображение, получаемого с камер видеонаблюдения, видеоизображения в режиме реального времени на АРМ должностных лиц;
 - возможность управления поворотными камерами видеонаблюдения из интерфейса АРМ должностных лиц;
 - запись видеопотоков, получаемых с камер видеонаблюдения;
 - хранение записанных видеоданных с возможностью быстрого поиска по заданному интервалу времени всех видеоданных связанных с зафиксированным правонарушением;
 - отображение мнемоник видеокамер на электронной карте с возможностью просмотра получаемого видеопотока путем выбора видеокамеры из интерфейса АРМ;
 - идентификации и распознавания лиц и сопоставление их с данными о лицах находящихся в розыске.
 - обнаружение скопления людей, в том числе в несанкционированных местах;
 - оценка плотности потока людей на значимых для муниципального образования объектах;
 - выявление фактов движения человека против направления потока;

- выявление фактов движения человека с высокой скоростью (бегущий человек);
 - выявление фактов оставленных предметов;
 - выявление фактов повышенной активности людей в контролируемой зоне;
 - выявление исчезнувших предметов;
 - появление человека или автомобиля в зоне наблюдения (улицы, площади, перекрестки, парки);
 - построение предполагаемых маршрутов движения транспортного средства на основе видеоданных данных полученных от различных видеокамер, на видеопотока которых был идентифицирован государственный номер транспортного средства.
 - обеспечение распределенной структуры видеосерверов, объединяющих камеры видеонаблюдения в группы;
 - обеспечения доступа к видеоданным по событиям зафиксированным средствами видеообнаружения, видеоидентификации и видеораспознавания.
- 2) позиционирование подвижных объектов, в том числе:
- построение оптимальных маршрутов передвижения с учетом данных о фактической загруженности дорог и отображением на электронной карте;
- 3) обеспечение функций информирования и получения отзывов от населения о работе представителей территориальных органов федеральных органов исполнительной власти, ответственных за обеспечение общественной безопасности, правопорядка и безопасности среды обитания, в том числе:
- накапливать статистическую информацию об обращениях населения, связанных с угрозами общественной безопасности, правопорядка и безопасности среды обитания на территории муниципального образования, в том числе поступающих через КСА ЕЦОР, а также о статусах их исполнения;
 - предоставлять населению возможность оценивать качество деятельности представителей территориальных органов федеральных органов исполнительной власти, ответственных за обеспечение общественной

безопасности, правопорядка и безопасности среды обитания по отношению к конкретному событию, посредством, размещенных на Интернет портале, унифицированных анкетных форм, содержащих поля для выставления оценок качества по категориям событий (имеющих разные коэффициенты);

- подготавливать сводные аналитические отчеты на основе накопленных статистических данных;

- обеспечивать сопоставление плановых и фактических ключевых показателей деятельности территориальных органов ФОИВ, ответственных за обеспечение общественной безопасности, правопорядка и безопасности среды обитания;

- информировать население, посредством подсистемы электронного взаимодействия с муниципальными службами и населением, а также посредством мобильных приложений о качестве деятельности представителей территориальных органов федеральных органов исполнительной власти, ответственных за обеспечение общественной безопасности, правопорядка и безопасности среды обитания;

- обеспечивать выявление фактов целенаправленного негативного информационного воздействия на население через средства массовой информации и Интернет;

- обеспечивать выявление фактов провоцирования социальной, межнациональной, религиозной напряженности через деятельность отдельных (в том числе электронных) средств массовой информации (СМИ).

3.2.5.2.3 Назначение и функциональность программно-аппаратных комплексов «Обеспечения безопасности инфраструктуры жилищно-коммунального комплекса»

Программно-аппаратные комплексы «Обеспечения безопасности инфраструктуры жилищно-коммунального комплекса» предназначены для мониторинга всех потенциальных рисков безопасности среды обитания, в том числе мониторинга муниципальной (коммунальной) инфраструктуры, социальной сферы и координации работы по предупреждению и ликвидации

последствий происшествий, вызванных сбоями в работе коммунальной инфраструктуры.

Сегмент «Обеспечения безопасности инфраструктуры жилищно-коммунального комплекса» должен обеспечивать выполнение следующих функций:

1) контроль качества работы коммунальных служб и состояния коммунальной инфраструктуры, включая:

а) сбор и обработку информации с датчиков;

б) контроль и управление работой газовых котлов и оборудованием тепловых сетей;

в) учет актуальных данных о состоянии муниципальной (коммунальной) инфраструктуры, в том числе:

- информацию об аварийных и нештатных ситуациях;

- объемы электрической энергии, расчеты за которую осуществляются с использованием приборов учета (в части многоквартирных домов - с использованием коллективных (общедомовых));

- объемы тепловой энергии, расчеты за которую осуществляются с использованием приборов учета (в части многоквартирных домов - с использованием коллективных (общедомовых) приборов учета);

- объемы воды, расчеты за которую осуществляются с использованием приборов учета (в части многоквартирных домов - с использованием коллективных приборов учета);

- объемы природного газа, расчеты за который осуществляются с использованием приборов учета (в части многоквартирных домов - с использованием индивидуальных и общих (для коммунальной квартиры) приборов учета);

- измерение давления в трубопроводах;

- измерение температуры теплоносителя в трубопроводах.

г) автоматическое уведомление о событиях в сфере функционирования муниципальной (коммунальной) инфраструктуры;

д) предоставление доступа к видеопотоку соответствующих камер видеонаблюдения;

2) обеспечение промышленной безопасности, включая:

а) оперативный мониторинг состояния опасных производственных объектов, а также используемых, производимых, перерабатываемых, хранимых и транспортируемых радиоактивных, пожаровзрывоопасных, опасных химических и биологических веществ;

б) мониторинг гидротехнических сооружений;

в) мониторинг соблюдения условий лицензирования опасных производственных объектов;

г) обеспечение доступа к проектной документации по опасным производственным объектам;

д) обеспечение производственного контроля за соблюдением требований к обеспечению промышленной безопасности;

е) учет работников, занятых на опасных производствах, учет проведения аттестации работников;

ж) моделирование чрезвычайных ситуаций и управление рисками на опасных производственных объектах;

з) планирование и контроль необходимых мероприятий и действий;

и) мониторинг соблюдения нормативных требований, осуществление комплексного управления операционными рисками, связанными с экологией, охраной труда и промышленной безопасностью;

3) мониторинг доступа на охраняемые государственные объекты, включая:

а) организацию доступа к видеопотоку с камер, принадлежащих государственным объектам;

б) фиксацию событий несанкционированного проникновения в охраняемую зону (нарушение периметра) и уведомление о нем соответствующих служб;

в) геолокацию в режиме реального времени экстренных ситуаций несанкционированного доступа на объекты;

г) акустический мониторинг (крики, удары, хлопки, выстрелы, бой стекла);

4) обеспечение экстренной связи, включая:

а) обеспечение возможности предоставления прямой, экстренной связи со службами экстренного реагирования посредством специальных устройств (типа «гражданин - полиция»), расположенных на территории муниципального образования, в том числе в местах частого скопления людей и потенциально опасных местах;

в) отслеживание ситуации через доступ к видеопотоку в режиме реального времени.

3.2.5.2.4 Назначение и функциональность программно-аппаратных комплексов «Обеспечение безопасности имущественного комплекса»

Программно-аппаратные комплексы «Обеспечение безопасности имущественного комплекса» предназначены для комплексной автоматизации задач управления активами и ресурсами муниципального образования, управления градостроительной политикой и обеспечения эффективного взаимодействия органов местного самоуправления, организаций и населения в сфере градостроения и имущественных отношений.

Программно-аппаратные комплексы «Обеспечение безопасности имущественного комплекса» должны обеспечивать выполнение следующих функций:

1) ведение электронного плана города;

2) ведение «дежурного плана города», включая:

а) обеспечение возможности приема документов об изменениях на дежурных планшетах города и предоставление возможности занесения семантической информации;

б) обеспечение выписками из генерального плана территории всех структур, осуществляющих строительную деятельность;

3) поддержку принятия решений при управлении муниципальными активами, включая:

а) планирование ремонтных работ и обслуживания;

б) планирование застройки и переноса объектов;
в) моделирование возможных ситуаций при застройке территорий и прокладке инфраструктуры;

4) мониторинг и профилактику безопасности в социальной сфере, включая:
а) санитарно-эпидемиологический контроль, в том числе мониторинг заболеваемости населения, мониторинг инфекционных, паразитарных болезней и отравлений людей, мониторинг особо опасных болезней сельскохозяйственных животных и рыб, мониторинг карантинных и особо опасных болезней;

б) профилактику предотвращения преступлений и чрезвычайных ситуаций на базе анализа расположения и доступности объектов социальной инфраструктуры, статистики правонарушений, включая мониторинг продовольственной безопасности, мониторинг правонарушений в торговле, включая случаи выявления просроченных товаров, контрафактной продукции, нарушений в области лицензирования и правил торговли.

5) ведение реестров объектов капитального строительства в составе:

а) реестров объектов капитального строительства с указанием расположения внутренних инженерных коммуникаций;

б) реестров технических условий по различным видам инженерного обеспечения объектов капитального строительства и земельных участков;

б) ведение реестров электросетей, трасс линий электропередачи и энергетического хозяйства в составе:

а) реестровой и пространственной информации об объектах электроснабжения и электросетях;

б) реестра ремонтных работ на объектах энергетической инфраструктуры;

7) ведение реестров сетей и сооружений водоснабжения в составе:

а) реестровой и пространственной информации об объектах водоснабжения;

б) паспортных данных объектов водоснабжения;

в) данных гидравлического расчета сетей водоснабжения;

- г) реестра ремонтных работ;
- 8) ведение реестров тепловых сетей в составе:
 - а) реестровой и пространственной информации об объектах теплоснабжения;
 - б) паспортных данных объектов теплоснабжения;
 - в) данных теплогидравлического расчета сетей теплоснабжения;
 - г) реестра ремонтных работ;
- 9) ведение реестров дорог в составе:
 - а) реестровой и пространственной информации об объектах транспортной инфраструктуры;
 - б) паспортных данных объектов транспортной инфраструктуры;
 - в) реестра ремонтных работ;
- 10) ведение реестров телекоммуникаций в составе:
 - а) реестровой и пространственной информации об объектах телекоммуникации;
 - б) паспортов объектов;
 - в) реестров ремонтных и строительных работ;
- 11) ведение социального реестра в составе:
 - а) реестровой и пространственной информации об объектах социальной сферы, а именно детских дошкольных учреждениях, школах, лечебно-профилактических учреждениях, спортивных учреждениях, базах отдыха;
 - б) базы данных персонала, аккредитованного к работе на объектах социальной сферы;
 - в) базы данных демографических и социальных характеристик населения;
- 12) ведение реестров мест обработки и утилизации отходов;
- 13) ведение реестров природоохранных и рекреационных зон и паркового хозяйства в составе:
 - а) пространственной информации об особо охраняемых территориях, зеленых насаждениях, парках и рекреационных зонах;
 - б) базы данных о промышленных предприятиях и их влиянии на экологию;

в) расчетных прогнозных моделей зон распространения выбросов от промышленных предприятий и влияния выбросов на среду жизнедеятельности населения.

3.2.5.3 Требования к внутреннему и внешнему взаимодействию

КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»

КСА сегментов «Безопасность населения и муниципальной (коммунальной) инфраструктуры» должны взаимодействовать между собой, со смежными КСА, входящими в состав АПК «Безопасный город» через КСА ЕЦОР.

Для информационного взаимодействия, непредусмотренного протоколами Единого стека открытых протоколов, допускается взаимодействие подсистем КСА, входящих в состав функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры» напрямую.

Взаимодействие КСА подсистем функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры» должно осуществляться на основе стандартов на архитектуру построения системных сервисов (служб) и взаимно-совместимых приложений (стандарты типа CORBA, DCOM, SOAP/XML, RPC, RMI или JSON).

Должны быть обеспечены следующие требования к характеристикам взаимосвязи КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры» между собой и подсистемами смежных КСА:

- внутреннее взаимодействие подсистем функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры» и взаимодействие с сегментами смежных функциональных блоков должно осуществляться на основе открытых протоколов Единого стандарта открытых протоколов;

- КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры» должны проектироваться на

основе мультисервисной цифровой сети передачи данных. Узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;

- все сетевые видеокамеры или кодеры (преобразователи аналогового сигнала в цифровой) должны поддерживать отраслевой стандарт, определяющий протоколы взаимодействия - ONVIF версии 1.02 или выше;

- все передатчики сетевого видео, включая камеры и видеосервера, должны поддерживать компрессию H.264 Main Profile, MJPG для передачи потокового видео и JPEG для передачи отдельных кадров;

- видеоаналитические сервера, подключаемые к сетевым камерам, должны на выходе поддерживать ONVIF версии 2.2 или выше, тип устройства аналитика сетевого видео (NVA) для передачи видео и результатов работы видеоаналитики от сервера к другим компонентам подсистемы;

- сжатое видео должно передаваться по протоколу RTP/RTSP с компрессией H.264 (Main Profile или High Profile) и компрессией MJPG;

- тревожные кадры или фрагменты тревожных кадров должны передаваться в формате JPEG;

- тревожные сообщения, формируемые видеоаналитическими серверами, должны передаваться по протоколу XML/SOAP в соответствии со схемами XML, определяемыми спецификациями сервиса ONVIF Event Service;

- метаданные видеоаналитики, включая координаты объектов и их признаки, должны передаваться в соответствии со спецификациями ONVIF версии 2.2 или выше;

- применение закрытых или проприетарных протоколов обмена и интерфейсов взаимодействия недопустимо.

3.2.5.3.1 Требования к внутреннему и внешнему взаимодействию программно-аппаратных комплексов обеспечения правопорядка и профилактики правонарушений

КСА функционального блока обеспечения правопорядка и профилактики правонарушений должны взаимодействовать с подсистемой интеграции данных КСА ЕЦОР.

КСА функционального блока обеспечения правопорядка и профилактики правонарушений должны предоставлять подсистеме комплексного мониторинга КСА ЕЦОР возможность подключения и управления оконечными устройствами в соответствии с определенными регламентами доступа, а также возможность получения необходимых данных, предусмотренных соответствующим протоколом Единого стека открытых протоколов.

3.2.5.3.2 Требования к внутреннему и внешнему взаимодействию КСА сегмента обеспечения безопасности инфраструктуры жилищно-коммунального комплекса

КСА функционального блока обеспечения безопасности инфраструктуры жилищно-коммунального комплекса должны взаимодействовать с подсистемой интеграции данных КСА ЕЦОР.

КСА функционального блока обеспечения безопасности инфраструктуры жилищно-коммунального комплекса должны предоставлять подсистеме комплексного мониторинга КСА ЕЦОР возможность подключения и управления оконечными устройствами в соответствии с определенными регламентами доступа, а также возможность получения необходимых данных, предусмотренных соответствующим протоколом Единого стека открытых протоколов.

3.2.5.3.3 Требования к внутреннему и внешнему взаимодействию сегмента обеспечения безопасности имущественного комплекса

Подсистемы КСА функционального блока обеспечения безопасности имущественного комплекса должны взаимодействовать с подсистемой интеграции данных КСА ЕЦОР.

Подсистемы КСА функционального блока обеспечения безопасности имущественного комплекса должны предоставлять подсистеме комплексного мониторинга КСА ЕЦОР возможность подключения и управления оконечными

устройствами в соответствии с определенными регламентами доступа, а также возможность получения необходимых данных, предусмотренных соответствующим протоколом Единого стека открытых протоколов.

3.2.5.4 Требования к техническому обеспечению КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»

Устройства обеспечения электронной связи и приема сигналов тревоги от граждан на транспорте должны соответствовать требованиям Приказ Минтранса РФ от 31 июля 2012. № 285 и должны быть подключены к системе экстренной связи на транспортных средствах.

Должно быть обеспечено устойчивое функционирование в условиях чрезвычайных ситуаций, когда может происходить возможное постепенное отключение различных элементов.

Устойчивость к поражающим факторам должна достигаться с помощью децентрализованных сетевых решений. В КСА не должно существовать ни одного территориально компактного элемента, отказ или разрушение которого выводил бы из строя весь КСА.

В качестве мест размещения технических средств информирования и оповещения населения могут использоваться:

- основные выезды, въезды в город перед постами ГИБДД, пересечение основных городских магистралей;
- аэропорты и аэровокзалы;
- автовокзалы и железнодорожные вокзалы;
- крупные торговые центры;
- станции метрополитена;
- центральные площади городов;
- городские рынки и стадионы.

Помимо крупных терминальных комплексов ОКСИОН городская система оповещения должна быть оснащена сетью малогабаритных пунктов локального информирования и оповещения населения (далее - ПЛИОН), использующих

каналы эфирного телерадиовещания, ПЛИОН данного типа должны обеспечивать:

- прием федерального мультиплекса, транслируемого городским радиотелевизионным центром в формате цифрового телевидения DVB-T2 с включенными (инкапсулированными) в состав этого мультиплекса служебными данными;
- извлечение (декапсуляцию) служебных данных из принимаемого мультиплекса, контроль их подлинности и целостности;
- воспроизведение принятых служебных данных в виде предупредительных звуковых и световых сигналов, речевых и/или текстовых сообщений.

Для обеспечения требуемой надежности должно обеспечиваться выполнение требований по автоматическому диагностированию подсистем КСА «Безопасность населения и муниципальной (коммунальной) инфраструктуры». Диагностирование должно обеспечиваться штатными средствами (тестирование и протоколирование).

Система хранения данных должна обеспечивать полезный объем необходимый для хранения всей поступающей видеoinформации в формате H.264 в течение 30 дней, в формате MJPG в течение 7 дней. Программное обеспечение КСА должно предусматривать разграничение прав доступа (ролей) к функциям КСА.

Для решения задач обзорного наблюдения и видеоаналитики должны использоваться стационарные и поворотные камеры высокого разрешения, в том числе купольного исполнения.

Для проведения оперативного обзора ситуации должны использоваться поворотные купольные камеры с моторизованным объективом. Для обзора протяженных пространств промышленных зон должны использоваться тепловизионные камеры. Для подъездного наблюдения должны использоваться антивандальные камеры миниатюрного исполнения.

Серверное оборудование должно отвечать требованиям по производительности программного обеспечения и иметь резерв по производительности не менее 40%. Технические характеристики оборудования сегментов функционального блока «Обеспечения правопорядка и профилактики правонарушений на территории муниципального образования» должны определяться исходя из требований к производительности сегментов (количества видеопотоков, разрешение видеоданных и т.п.).

Сегменты функционального блока «Обеспечения правопорядка и профилактики правонарушений на территории муниципального образования» должны функционировать в основном режиме 24 часа в сутки, 7 дней в неделю, 365 дней в году.

В профилактическом режиме должно быть обеспечено: техническое обслуживание, модернизация КСА, устранение аварийных ситуаций. Общее время проведения профилактических работ не должно превышать 2% от общего времени работы сегмента без приостановки в обслуживании и 0,1% с приостановкой.

Дополнительные требования к видеоизображению формируются в зависимости от конкретных решаемых задач.

В зависимости от условий регистрации в конкретных зонах видеокамеры могут поддерживать функции автоэкспозиции и автоматического управления диафрагмой.

Должны быть соблюдены требования к телекоммуникационной инфраструктуре представленные в Приложении 18.

Технические требования к системе видеонаблюдения представлены в Приложении 19.

3.2.5.5 Требования к системному программному обеспечению КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»

КСА сегмента «Безопасность населения и муниципальной (коммунальной) инфраструктуры» представляет собой совокупность общего программного обеспечения и специального программного обеспечения.

Сегмент «Безопасности населения и муниципальной (коммунальной) инфраструктуры» строится на открытой, компонентной (модульной) архитектуре, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в сегмент «Безопасности населения и муниципальной (коммунальной) инфраструктуры» перспективных КСА.

Программное обеспечение должно быть сертифицировано по требованиям безопасности информации.

Требования к общему программному обеспечению сегмента «Безопасности населения и муниципальной (коммунальной) инфраструктуры» должны соответствовать требованиям к общему программному обеспечению, представленным в Приложении 5 (Требования к общему программному обеспечению).

Требования к специальному обеспечению подсистем сегмента «Безопасность населения и муниципальной (коммунальной) инфраструктуры» должно быть аналогичны требованиям к специальному программному обеспечению КСА функционального блока «Координации работы служб и ведомств», представленных в Приложении 6 (Требования к специальному программному обеспечению КСА «Региональная платформа» функционального блока «Координация работы служб и ведомств»).

3.2.5.6 Требования к информационному обеспечению КСА

функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»

Требования к информационному обеспечению КСА «Безопасность населения и муниципальной (коммунальной) инфраструктуры» должны быть аналогичны требованиям к информационному обеспечению КСА «Региональная платформа» функционального блока «Координация работы служб и ведомств» представленных в разделе «Требования к информационному обеспечению КСА

«Региональная платформа» функционального блока «Координация работы служб и ведомств».

3.2.6 КСА функционального блока «Безопасность на транспорте»

3.2.6.1 Состав КСА «Безопасность на транспорте»

КСА «Безопасность на транспорте» состоит из следующих ПАК «Безопасный город»:

1) Программно-аппаратные комплексы обеспечения правопорядка, профилактики правонарушений на дорогах в составе следующих подсистем:

а) подсистема фото-видеофиксации событий (правонарушений) на дорогах;

б) подсистема мониторинга объектов транспортной инфраструктуры;

в) подсистема мониторинга транспортных средств;

г) управления видеопотоками и видеоанализа происшествий;

д) контроля и управление мобильным персоналом (экипажами Госавтоинспекции Министерства внутренних дел Российской Федерации) и др.

2) Программно-аппаратные комплексы обеспечения безопасности дорожного движения, в составе следующих подсистем:

а) подсистема мониторинга дорожной ситуации;

б) фото-видеофиксация нарушений правил дорожного движения в автоматическом режиме;

в) информационной поддержки парковочного оператора;

г) подсистема интеллектуального управления светофорами;

д) подсистема управления и планирования дорожной сети;

е) геоинформационная система муниципального парковочного оператора;

ж) подсистема управления видеонаблюдением и видеоанализа событий на дорогах;

з) подсистема управления и анализа и прогнозирования дорожной ситуации;

и) подсистема сценарного моделирования транспортных потоков;

к) подсистема оплаты услуг парковочного оператора;

л) иные информационно-управляющие системы.

3) КСА обеспечения безопасности на транспорте в составе следующих подсистем:

а) подсистема мониторинга маршрутов транспортных средств (автомобильных, воздушных, водных и железнодорожных);

б) подсистема мониторинга и диспетчеризации грузового транспорта;

в) подсистема мониторинга и диспетчеризации общественного транспорта;

г) подсистема видеонаблюдения и анализа оперативной обстановки на объектах транспортной инфраструктуры железнодорожного, водного, воздушного и автомобильного транспорта, метрополитена и дорожного хозяйства;

д) подсистема диспетчеризации и управления дорожной ситуацией;

е) подсистема обеспечения экстренной связи, информирования и оповещения на транспорте и объектах транспортной инфраструктуры железнодорожного, водного, воздушного и автомобильного транспорта, метрополитена и дорожного хозяйства;

ж) подсистема управления общественным транспортом;

з) подсистема контроля технического состояния транспортных средств;

и) подсистема сбора результатов технического мониторинга и контроль объектов транспортной инфраструктуры;

к) подсистема контроля деятельности перевозчиков.

3.2.6.2 Назначение и функциональность КСА функционального блока «Безопасность на транспорте»

3.2.6.2.1 Назначение и функциональность программно-аппаратных комплексов «Обеспечение правопорядка, профилактики правонарушений на дорогах»

Программно-аппаратные комплексы «Обеспечение правопорядка, профилактики правонарушений на дорогах» предназначены для решения задач профилактики правонарушений в области дорожного движения, сбора и анализа оперативной информации о ситуации на дорогах, повышения уровня безопасности на дорогах и объектах транспортной инфраструктуры, усиления контроля и повышения качества управления мобильным персоналом, в том числе экипажами Госавтоинспекции Министерства внутренних дел Российской Федерации и другими.

Основными функциями сегмента «Обеспечение правопорядка, профилактики правонарушений на дорогах» являются:

1) обеспечение видеонаблюдения за ситуацией на дорогах и фото-видеофиксации правонарушений, а именно:

а) фиксация в автоматическом режиме правонарушений в области дорожного движения и передачу полученной информации в центры автоматизированной фиксации нарушений правил дорожного движения;

б) фиксация проходящих транспортных средств;

2) видеоанализ событий и происшествий на дорогах, а именно:

а) выявление потенциально опасных событий на дорогах и объектах транспортной инфраструктуры железнодорожного, водного, воздушного и автомобильного транспорта, метрополитена и дорожного хозяйства в режиме реального времени;

б) анализ информации о дорожной ситуации в режиме реального времени;

в) обеспечение доступа к хранимой информации и восстановление хронологии происшествий, в том числе посредством обработки данных с нескольких источников;

г) автоматическое отслеживание маршрутов транспортных средств, в том числе отклонений от маршрутов и графиков городского транспорта;

д) автоматическую проверку транспортных средств на предмет имеющихся правонарушений, угона и прочих.

3.2.6.2.2 Назначение и функциональность программно-аппаратных комплексов «Обеспечения безопасности дорожного движения»

Программно-аппаратные комплексы «Обеспечения безопасности дорожного движения» предназначены для решения задач управления транспортными потоками и обеспечения эффективного взаимодействия различных служб и организаций муниципального образования в сфере организации и обеспечения безопасности дорожного движения.

Основными функциями сегмента «Обеспечения безопасности дорожного движения» на дорогах являются:

- 1) управление логистикой общественного и личного транспорта, включая:
 - а) расчет расписаний и маршрутов общественного транспорта по результатам сценарного моделирования с учетом данных по пассажиропотокам и перспективным планам развития территорий муниципального образования;
 - б) расчет оптимальных маршрутов для транспортных средств служб оперативного реагирования;
 - в) расчет оптимальных маршрутов (коридоров) и графиков проезда для грузового транспорта;
 - г) расчет маршрутов и расписаний работы городских коммунальных служб;
 - д) планирование графиков ремонтных работ;
 - е) планирование зон, ограничивающих движение по типам транспортных средств, и графиков доступа в зоны с ограниченным движением для различных типов транспортных средств.
- 2) организация и управление муниципальным парковочным пространством, включая:
 - а) расчет зональности парковочных зон по временному и ценовому признакам для различных категорий транспортных средств;
 - б) повышение безопасности хранения транспортных средств;

- в) обеспечение фото-видеофиксации нарушений правил парковки;
 - г) профилактику нарушений правил парковки, включая перемещение транспортных средств, мешающих нормальному дорожному движению;
 - д) обеспечение расчетов за пользование парковкой;
 - е) подготовка комплекта документов по нарушениям правил парковки и формирование платежных документов для местной расчетной системы;
- 3) моделирование транспортных потоков, включая:
- а) сбор, хранение и анализ информации о дорожной ситуации с установленных датчиков и контроллеров, средств видеонаблюдения;
 - б) сценарное моделирование дорожной ситуации с использованием методов исторической симуляции, Монте-Карло и других применимых математических моделей;
- 4) динамическое прогнозирование дорожной ситуации на базе поступающих в режиме реального времени данных с видеокамер, датчиков и контроллеров дорожного движения, включая:
- а) отображение на электронной карте текущей и прогнозируемой дорожной ситуации;
 - б) адаптивное управление дорожной ситуацией в автоматическом и полуавтоматическом режиме (организация «зеленой волны»);
 - в) расчет сценариев работы периферийных КСА управления дорожным движением (светофоров);
 - г) прогнозирование последствий дорожного происшествия (события) с учетом данных о текущей дорожной ситуации и исторических данных;
- 5) автоматическая геолокация и фиксацию событий (инцидентов) на дорогах с визуализацией на карте города, включая:
- а) автоматическое распознавание типа события и его фиксацию на карте города;
 - б) передачу информации о событии в КСА ЕЦОР.
- 6) обеспечение функций общественного контроля над работой правоохранительных структур на местах.

3.2.6.2.3 Назначение и функциональность программно-аппаратного комплекса «Обеспечения безопасности на транспорте»

Программно-аппаратные комплексы «Обеспечения безопасности на транспорте» предназначены для решения комплекса задач повышения безопасности на транспорте и объектах транспортной инфраструктуры, в том числе обеспечения возможности идентификации и оперативного реагирования на вероятные угрозы общественной безопасности и правопорядка на транспорте и объектах транспортной инфраструктуры, повышения уровня безопасности пассажироперевозок, в том числе коммерческими организациями.

Основными функциями сегмента «Обеспечения безопасности на транспорте» являются:

1) обеспечение экстренной связи на транспортных средствах (автомобильном, железнодорожном, водном и воздушном транспорте), включая:

а) автоматическое оповещение служб экстренного реагирования при авариях и других чрезвычайных ситуациях;

б) автоматическое позиционирование точки вызова и регистрацию события;

в) информирование населения по вопросам гражданской обороны;

2) обеспечение экстренной связи на объектах транспортной инфраструктуры (вокзалах, аэродромах, аэропортах, объектах систем связи, навигации и управления движением транспортных средств, а также на иных обеспечивающих функционирование транспортного комплекса зданиях, сооружениях, устройствах и оборудовании), включая:

а) автоматическое оповещение служб экстренного реагирования при авариях и других чрезвычайных ситуациях;

б) автоматическое позиционирование точки вызова и регистрацию события;

в) информирование населения по вопросам гражданской обороны;

3) информирование о чрезвычайных ситуациях на транспортных средствах и объектах транспортной инфраструктуры, включая:

а) идентификацию событий на основе поступающей информации с датчиков, установленных на транспортных средствах с визуализацией на электронной карте города;

б) идентификацию событий на основе поступающей информации с датчиков, установленных на объектах транспортной инфраструктуры с визуализацией на электронной карте города;

в) обеспечение доступа к видеопотоку с транспортных средств и объектов транспортной инфраструктуры;

4) контроль маршрутов движения общественного и грузового транспорта, включая:

а) фиксацию отклонений от заданных маршрутов (транспортных коридоров);

б) контроль времени прохождения пути, средней скорости;

в) аналитику по различным характеристикам перемещений общественного транспорта (расстояние, маршрут, время прохождения, длительность остановок, расход топлива, длина рабочей смены водителя, число перевезенных пассажиров и прочие);

г) осуществление весового контроля;

д) диспетчеризацию пассажирского и грузового транспорта в рамках оптимизации маршрутов и управления транспортными потоками;

е) ведение исторической базы перевозок;

5) фиксацию на основе видеонаблюдения нарушений условий договоров с частными перевозчиками, осуществляющими пассажирские перевозки, включая:

а) фиксацию отклонений от заданных маршрутов;

б) контроль времени прохождения пути, средней скорости, графика перевозок;

в) аналитику по различным характеристикам перемещений общественного транспорта (расстояние, маршрут, время прохождения, длительность остановок, расход топлива, длина рабочей смены водителя, число перевезенных пассажиров и прочие);

г) предоставление требуемого количества транспортных средств для перевозки;

д) ведение исторической базы перевозок;

б) мониторинг маршрутов воздушных судов, водных судов и железнодорожного транспорта, включая:

а) мониторинг графика расписаний воздушных судов, водных судов и железнодорожного транспорта;

б) информирование об отклонениях в расписании воздушных судов, водных судов и железнодорожного транспорта.

б) контроль результатов технического мониторинга объектов транспортной инфраструктуры, включая:

а) автоматизированный сбор данных технических средств мониторинга и контроля транспортной инфраструктуры в целях последующей аналитической обработки;

б) информационно-аналитическое обеспечение деятельности уполномоченных органов исполнительной власти в сфере транспортной безопасности;

7) контроль технического состояния транспортных средств, включая:

а) получение и обработку информации о состоянии транспортных средств;

б) автоматическое отслеживание необходимости планового технического обслуживания;

в) ведение единой базы учета технического состояния транспортных средств (по видам транспортных средств);

8) обеспечение автоматизированной проверки и учета данных в рамках процедуры лицензирования перевозчиков, контроль лицензиатов на предмет выполнения условий лицензирования, включая:

а) сбор и анализ информации с тахографов;

б) учет карточек водителей,

в) осуществление проверки на предмет соблюдения условий договоров об осуществлении пассажирских перевозок;

10) организацию системы информирования населения о работе общественного транспорта и дорожной ситуации, включая:

а) предоставление информации о маршрутах и об актуальном расписании движения общественного транспорта;

б) информирование о фактической дорожной ситуации и ее динамике.

3.2.6.3 Требования к внутреннему и внешнему взаимодействию КСА функционального блока «Безопасность на транспорте»

КСА функционального блока «Безопасность на транспорте» должны взаимодействовать между собой и со смежными КСА, входящими в состав АПК «Безопасный город» через КСА ЕЦОР.

Для информационного взаимодействия, непредусмотренного протоколами Единого стека открытых протоколов, допускается прямое взаимодействие подсистем КСА, входящих в состав сегмента «Безопасность на транспорте».

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

Должны быть обеспечены следующие требования к характеристикам взаимосвязи подсистем КСА «Безопасность на транспорте» между собой, с подсистемами смежных КСА:

- взаимодействие КСА подсистем между собой и с подсистемами смежных КСА должно осуществляться на основе открытых протоколов Единого стека открытых протоколов;

- сегменты КСА «Безопасность на транспорте» должны проектироваться на основе мультисервисной цифровой сети передачи данных;

- узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;

- все сетевые видеокамеры или кодеры (преобразователи аналогового сигнала в цифровой) должны поддерживать отраслевой стандарт, определяющий протоколы взаимодействия - ONVIF версии 1.02 или выше;
- все передатчики сетевого видео, включая камеры и видеосервера, должны поддерживать компрессию H.264 Main Profile, MJPG для передачи потокового видео и JPEG для передачи отдельных кадров;
- видеоаналитические сервера, подключаемые к сетевым камерам, должны на выходе поддерживать ONVIF версии 2.2 или выше, тип устройства аналитика сетевого видео (NVA) для передачи видео и результатов работы видеоаналитики от сервера к другим компонентам подсистемы;
- сжатое видео должно передаваться по протоколу RTP/RTSP с компрессией H.264 (Main Profile или High Profile) и компрессией MJPG;
- тревожные кадры или фрагменты тревожных кадров должны передаваться в формате JPEG;
- тревожные сообщения, формируемые видеоаналитическими серверами, должны передаваться по протоколу XML/SOAP в соответствии со схемами XML, определяемыми спецификациями сервиса ONVIF Event Service;
- метаданные видеоаналитики, включая координаты объектов и их признаки, должны передаваться в соответствии со спецификациями ONVIF версии 2.2 или выше;
- применение закрытых или проприетарных протоколов обмена и интерфейсов взаимодействия недопустимо.

3.2.6.4 Требования к техническому обеспечению КСА функционального блока «Безопасность на транспорте»

Техническое обеспечение функционального блока «Безопасность на транспорте» должно отвечать следующим общим требованиям:

- образцы средств вычислительной техники и средств коммуникационной техники должны быть сертифицированы;
- обладать расширяемостью;

- обеспечивать устойчивую управляемость;
- электронно-вычислительная техника должна соответствовать или превышать требования технических спецификаций по производительности.

при выборе технических средств сегмента «Безопасность на транспорте» предпочтение должно отдаваться продукции отечественного производства;

узлы сети должны обеспечивать высокую готовность (24/7). Для участков сети, требующих повышенную надежность, необходимо предусмотреть резервные каналы связи.

Для обеспечения высокой доступности сервисов сегмента «Безопасность на транспорте» для серверных и сетевых компонент, а так же для оборудования, выход которого из строя приводит к недоступности сервиса, время восстановления не должно превышать 2 часа (без учета времени перемещения до места сбоя). Время восстановления для остальной техники 24 часа.

Активное сетевое оборудование должно обеспечивать достаточную пропускную способность для функционирования КСА сегментов АПК «Безопасный город» в соответствии с настоящими требованиями.

Должны применяться видеокамеры, которые позволяют получать цветное видеоизображение в дневное время суток и черно-белое в ночное время. Количество камер видеофиксации определяется из расчета 1 камера на 1 и более полос движения.

Данные о фактах фиксации передвижения транспортных средств, полученные путем распознавания государственных регистрационных знаков (ГРЗ) при передвижении транспортных средств (далее – ТС) через контролируемые зоны формируются с использованием систем идентификации транспортных средств (далее - СИТС). Данные, от уже установленных СИТС, должны передаваться через узлы сбора данных с использованием ЕСОП.

Технические требования к источникам фото-видеофиксации приведены в Приложении 20.

Требования к абонентским терминалам ГЛОНАСС-GPS/GSM, датчикам спутниковой навигации, бортовому навигационному оборудованию приведены в Приложении 21.

Должны быть соблюдены требования к телекоммуникационной инфраструктуре представленные в Приложении 18.

Технические требования к системе видеонаблюдения представлены в Приложении 19.

3.2.6.5 Требования к системному программному обеспечению КСА функционального блока «Безопасность на транспорте»

Программное обеспечение КСА сегментов функционального блока «Безопасность на транспорте» должно представлять собой совокупность общего программного обеспечения и специального программного обеспечения.

Программное обеспечение КСА сегментов функционального блока «Безопасность на транспорте» должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в состав сегментов функционального блока «Безопасность на транспорте» перспективных КСА.

Программное обеспечение должно быть сертифицировано по требованиям безопасности информации.

Функциональные требования к специальному программному обеспечению базовых станций:

- контроль качества данных от каждой станции сети;
- контроль состояния и целостности всей сети;
- возможность ведения мониторинга сети;
- возможность моделирования ионосферных, тропосферных поправок и учет многолучевости для каждого пользователя;
- передача пользователям информации об используемой системе координат;
- реализация технологии VRS в реальном времени и в постобработке;

- учет информации, предоставляемой пользователям, и реализация мощной биллинговой системы.

Требования к общему программному обеспечению КСА «Безопасность на транспорте» должны быть аналогичны требованиям к общему программному обеспечению функционального блока «Координации работы служб и ведомств» представленных в Приложении 6 (Требования к общему программному обеспечению функционального блока «Координация работы служб и ведомств»).

Требования к специальному обеспечению КСА сегментов функционального блока «Безопасность на транспорте» должно быть аналогичны требованиям к специальному программному обеспечению КСА сегментов функционального блока «Координация работы служб и ведомств» представленных в Приложении 7 (Требования к специальному программному обеспечению КСА функционального блока «Координация работы служб и ведомств»).

3.2.6.6 Требования к информационному обеспечению КСА функционального блока «Безопасность на транспорте»

Требования к информационному обеспечению КСА сегментов функционального блока «Безопасность на транспорте» должны быть аналогичны требованиям к информационному обеспечению КСА «Региональная платформа» функционального блока «Координация работы служб и ведомств» представленных в разделе «Требования к информационному обеспечению КСА «Региональная платформа» функционального блока «Координация работы служб и ведомств»».

3.2.7 КСА функционального блока «Экологическая безопасность»

3.2.7.1 Состав КСА функционального блока «Экологическая безопасность»

КСА функционального блока «Экологическая безопасность» состоит из следующих программно-аппаратных комплексов:

- 1) геоэкологического планирования в составе следующих подсистем:
 - а) подсистема мониторинга и контроля исполнения предписаний, выданных по результатам муниципального экологического контроля;
 - б) геоинформационной системы экологического мониторинга;
 - в) подсистема управления реестром природопользователей;
 - г) подсистема управления реестром нормативов допустимого воздействия на окружающую среду;
 - д) подсистема управления процессами планирования и осуществления муниципального экологического контроля;
 - е) подсистемы отчетно-аналитической поддержки природопользователей;
 - ж) подсистема управления нормативно-справочной базы природопользователей;
- з) подсистема расчетного обслуживания.
- 2) гидрометеорологической информации, включающий следующие компоненты в составе следующих подсистем:
 - а) подсистема мониторинга оперативной гидрометеорологической обстановки;
 - б) подсистема мониторинга сейсмической активности;
 - в) подсистема управления идентификации и оценки экологических рисков;
 - г) подсистема регистрации объектов воздействия на окружающую среду;
 - д) подсистема реестра природных ресурсов;
 - е) подсистема реестра «загрязненных» территорий;
 - ж) подсистема реестра природоохранных и рекреационных зон и паркового хозяйства;
- 3) экомониторинга, в составе следующих подсистем:

- а) подсистема мониторинга загрязнения окружающей среды;
- б) подсистема мониторинга состояния почв;
- в) подсистема мониторинга водных ресурсов;
- г) подсистема мониторинга сейсмической активности;
- д) подсистема мониторинга гидрологической обстановки;
- е) подсистема мониторинга метеорологической обстановки;
- ж) подсистема мониторинга радиационной обстановки;
- з) геоинформационная система мониторинга экологической обстановки, включая подсистемы мониторинга состояния суши, водных ресурсов, невозобновляемых природных ископаемых, контроль состояния почв;
- и) геоинформационная система природных явлений;
- к) геоинформационная система мест захоронений отходов;
- л) система контроля транспортных средств, осуществляющих вывоз и утилизацию отходов.

4.2.7.2 Назначение и функциональность КСА функционального блока «Экологическая безопасность»

4.2.7.2.1 Назначение и функциональность программно-аппаратных комплексов «Геоэкологического планирования»

Программно-аппаратные комплексы «Геоэкологического планирования» предназначены для решения задач комплекса задач по обеспечению экологической безопасности, включая аналитическое сопровождение экологических аспектов градостроительной политики, обеспечение эффективной деятельности органов государственной власти в сфере охраны окружающей среды и их взаимодействия природопользователями.

Основными функциями программно-аппаратных комплексов «Геоэкологического планирования» являются:

- 1) комплексный мониторинг муниципальной застройки и уже существующих объектов с учетом данных по экологической ситуации, в том числе:

а) ведение реестров природопользователей и объектов экологического контроля,

б) ведение реестров нормативных и фактических значений предельно допустимых выбросов и предельно допустимой концентрации веществ;

в) отображение на электронной карте реестровой информации;

г) ежедневный мониторинг предельно допустимого содержания, предельно допустимых выбросов, предельно допустимой концентрации веществ на предприятиях (близии предприятий), чьи технологические процессы связаны с возможностью вредных выбросов в окружающую среду;

д) сбор и обработку информации с установленных устройств (датчиков) о фактических значениях предельно допустимого содержания, предельно допустимых выбросов, предельно допустимой концентрации веществ;

е) определение источников загрязнения окружающей среды на базе встроенных аналитических моделей, использующих оперативную фактическую информацию о параметрах загрязнений окружающей среды, исторические статистические данные, гидрометеорологическую информацию;

ж) сценарное моделирование угроз экологической безопасности;

з) прогнозирование развития угроз экологической безопасности с учетом муниципальной застройки и гидрометеорологической обстановки;

2) обеспечение автоматизированного документооборота процессов планирования и осуществления муниципального экологического контроля, включая:

а) автоматизацию сбора и анализ данных от природопользователей о фактических значениях предельно допустимого содержания, предельно допустимых выбросов, предельно допустимой концентрации веществ, размещение отходов производства и потребления посредством электронного документооборота или импорта отчетных форм;

б) отчетно-аналитическую поддержку природопользователей;

в) ведение нормативно-справочной базы природопользователей;

3) осуществление контроля и мониторинга исполнения предписаний, выданных по результатам муниципального экологического контроля;

а) формирование графиков комплексных проверок объектов муниципального экологического контроля;

б) ведение истории комплексных проверок объектов муниципального экологического контроля;

в) раскрытие информации о результатах комплексных проверок объектов муниципального экологического контроля для природопользователей и населения;

г) автоматизация функций контроля над природопользователями по лицензируемым видам деятельности;

4) обеспечение расчетного обслуживания природопользователей, включая:

а) автоматический расчет платы за предельно допустимое содержимое, предельно допустимые выбросы, предельно допустимую концентрацию веществ, размещение отходов производства и потребления на основании предоставленной природопользователями информации;

б) формирование необходимого пакета платежных документов для природопользователя;

4.2.7.2.2 Назначение и функциональность программно-аппаратных комплексов «Гидрометеорологической информации»

Программно-аппаратные комплексы «Гидрометеорологической информации» предназначены для информационной поддержки принятия решений по обеспечению экологической безопасности в части сбора, обработки и анализа данных о состоянии атмосферы, водных ресурсов и земной поверхности.

Основными функциями программно-аппаратных комплексов «Гидрометеорологической информации», являются:

1) предоставление оперативной гидрометеорологической информации, включая:

а) сбор и обработку информации о текущей метеорологической ситуации с установленных периферийных устройств;

б) автоматизированный импорт прогнозной метеорологической информации из внешних источников (специализированных ресурсов);

в) информирование о резких изменениях погоды или климата в том числе угроз ураганов, штормового ветра, обильных снегопадов и затяжных дождей, обледенения дорог и токонесущих проводов;

2) предоставление информации о сейсмической активности;

а) мониторинг сейсмической активности на предмет возникновения просадок, оползней, обвалов земной поверхности;

б) автоматизированный импорт информации о сейсмической активности в регионе из внешних источников (специализированных ресурсов);

3) предоставление гидрологической информации, включая:

а) сбор и обработку данных с периферийных устройств о гидрологической ситуации;

б) мониторинг угроз истощения водных ресурсов, необходимых для организации хозяйственно-бытового водоснабжения и обеспечения технологических процессов;

в) мониторинг паводковой ситуации;

г) мониторинг угроз подтопления населенных пунктов.

4.2.7.2.3 Назначение и функциональность программно-аппаратных комплексов «Экомониторинга»

Программно-аппаратные комплексы «Экомониторинга» предназначены для решения задач комплексного мониторинга, оперативного реагирования, предупреждения и устранения последствий природных и экологических угроз посредством интеграции данных об экологической обстановке на единой геоинформационной платформе экомониторинга.

Основными функциями программно-аппаратных комплексов «Экомониторинга», являются:

1) мониторинг загрязнения окружающей среды, включая:

а) консолидацию и отражение на электронной карте данных периферийных устройств в соответствующих реестрах геоинформационной системы в части превышения предельно допустимой концентрации вредных примесей в атмосфере, содержания вредных веществ в воде, наличия вредных примесей в почве;

б) обеспечение представления в геоинформационной системе информации реестров природопользователей в части фактических и допустимых значений предельно допустимого содержания, предельно допустимых выбросов, предельно допустимой концентрации веществ;

2) контроль состояния суши, включая мониторинг угроз просадок, оползней и обвалов земной поверхности из-за выработки недр при добыче полезных ископаемых и другой деятельности человека;

3) мониторинг водных ресурсов, включая

а) контроль загрязнения водных ресурсов;

б) мониторинг угрозы истощения водных ресурсов, необходимых для организации хозяйственно-бытового водоснабжения и обеспечения технологических процессов;

4) мониторинг угроз, связанных с истощением невозобновляемых природных ископаемых, включая:

а) представление информации о природопользователях и объектах экологического мониторинга;

б) предоставление информации о лицензиях природопользователей и фактических данных по выработке природных ресурсов;

5) контроль состояния почв;

б) мониторинг наличия тяжелых металлов (в том числе радионуклидов) и других вредных веществ в почве (грунте) сверх предельно допустимых концентраций;

в) мониторинг угроз интенсивной деградации почв, опустынивания на обширных территориях из-за эрозии, засоления, заболачивания почв и так далее;

б) мониторинг сейсмической активности в регионе и обеспечение сейсмической безопасности, включая:

а) представление актуальной и исторической информации о сейсмической активности в геоинформационной системе;

б) представление информации о сейсмической устойчивости зданий и объектов городской инфраструктуры;

7) мониторинг гидрологической обстановки и обеспечение безопасности при наводнениях, включая:

а) мониторинг паводковой ситуации, угроз образования ледовых заторов,

б) графическое отображение прогнозов гидрологической обстановки и сопоставление с данными аэрофотосъемки и космоснимков;

8) мониторинг гидрометеорологической обстановки, включая:

а) предоставление актуальной и прогнозной информации по гидрометеорологической обстановке;

б) расчет влияния гидрометеорологической обстановки на развитие потенциальных угроз среде обитания;

9) мониторинг лесопожарной опасности, включая:

а) представление на электронной карте актуальной и исторической информации о лесных пожарах;

б) представление информации о пожароопасных участках;

в) прогнозирование развития угроз лесных пожаров с учетом гидрометеорологической информации;

г) графическое отображение лесопожарной опасности и сопоставление с данными аэрофотосъемки и космоснимков;

10) мониторинг ситуаций, вызванных переполнением хранилищ (свалок) промышленными и бытовыми отходами, загрязнением ими окружающей среды, включая:

а) контроль процессов сбора, транспортировки и переработки отходов, включая формирование и контроль графиков вывоза мусора и отходов;

б) спутниковый контроль транспортных средств, осуществляющих вывоз и утилизацию отходов, включая контроль соблюдения маршрутов и графиков движения, фиксацию остановок транспортных средств .

в) мониторинг состояния окружающей среды в районах размещения отходов и мониторинг экологической обстановки территорий городов для предотвращения и выявления несанкционированных захоронений отходов;

г) ведение базы данных организаций осуществляющих сбор, обработку и утилизацию производственных и бытовых отходов.

4.2.7.3 Требования к внутреннему и внешнему взаимодействию

КСА функционального блока «Экологическая безопасность»

КСА функционального блока «Экологическая безопасность» должны взаимодействовать между собой и с подсистемами смежных КСА через КСА ЕЦОР.

Для информационного взаимодействия, непредусмотренного протоколами Единого стека открытых протоколов, допускается взаимодействие подсистем КСА функционального блока «Экологическая безопасность» напрямую.

Взаимодействие компонентов программного обеспечения в КСА сегментов функционального блока «Экологическая безопасность» должно осуществляться на основе стандартов на архитектуру построения системных сервисов (служб) и взаимно-совместимых приложений (стандарты типа CORBA, DCOM, SOAP/XML, RPC, RMI или JSON).

Должны быть обеспечены следующие требования к характеристикам взаимосвязи КСА сегментов функционального блока «Экологическая безопасность» между собой и с КСА смежных функциональных блоков:

- взаимодействие КСА и их подсистем между собой и с подсистемами смежных КСА должно осуществляться на основе открытых протоколов Единого стандарта открытых протоколов;

- КСА функционального блока «Экологическая безопасность» должны проектироваться на основе мультисервисной цифровой сети передачи

данных. Узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;

- все сетевые видеокамеры или кодеры (преобразователи аналогового сигнала в цифровой) должны поддерживать отраслевой стандарт, определяющий протоколы взаимодействия - ONVIF версии 1.02 или выше;

- все передатчики сетевого видео, включая камеры и видеосервера, должны поддерживать компрессию H.264 Main Profile, MJPG для передачи потокового видео и JPEG для передачи отдельных кадров;

- видеоаналитические сервера, подключаемые к сетевым камерам, должны на выходе поддерживать ONVIF версии 2.2 или выше, тип устройства аналитика сетевого видео (NVA) для передачи видео и результатов работы видеоаналитики от сервера к другим компонентам подсистемы;

- сжатое видео должно передаваться по протоколу RTP/RTSP с компрессией H.264 (Main Profile или High Profile) и компрессией MJPG;

- тревожные кадры или фрагменты тревожных кадров должны передаваться в формате JPEG;

- тревожные сообщения, формируемые видеоаналитическими серверами, должны передаваться по протоколу XML/SOAP в соответствии со схемами XML, определяемыми спецификациями сервиса ONVIF Event Service;

- метаданные видеоаналитики, включая координаты объектов и их признаки, должны передаваться в соответствии со спецификациями ONVIF версии 2.2 или выше;

- применение закрытых или проприетарных протоколов обмена и интерфейсов взаимодействия недопустимо.

4.2.7.4 Требования к техническому обеспечению КСА функционального блока «Экологическая безопасность»

Техническое обеспечение КСА функционального блока «Экологическая безопасность» должно отвечать следующим общим требованиям:

- образцы средств вычислительной техники и средств коммуникационной техники должны быть сертифицированы;

- обладать расширяемостью;
- обеспечивать устойчивую управляемость;
- электронно-вычислительная техника должна соответствовать или превышать требования технических спецификаций по производительности.

- при выборе технических средств КСА подсистем функционального блока «Экологическая безопасность» предпочтение должно отдаваться продукции отечественного производства;

- узлы сети должны обеспечивать высокую готовность (24/7). Для участков сети, требующих повышенную надежность, необходимо предусмотреть резервные каналы связи.

Для обеспечения высокой доступности сервисов КСА функционального блока «Экологическая безопасность» для серверных и сетевых компонент, а так же для оборудования, выход которого из строя приводит к недоступности сервиса, время восстановления не должно превышать 2 часа (без учета времени перемещения до места сбоя). Время восстановления для остальной техники 24 часа.

Активное сетевое оборудование должно обеспечивать достаточную пропускную способность для функционирования сегментов АПК «Безопасный город» в соответствии с настоящими требованиями.

Должны быть обеспечены требования к техническому обеспечению КСА функционального блока «Экологическая безопасность» в соответствии с Приложением 22 (Требования к техническому обеспечению КСА функционального блока «Экологическая безопасность»).

Должны быть соблюдены требования к телекоммуникационной инфраструктуре представленные в Приложении 18.

Технические требования к системе видеонаблюдения представлены в Приложении 19.

4.2.7.5 Требования к программному обеспечению КСА функционального блока «Экологическая безопасность»

Программное обеспечение КСА функционального блока «Экологическая безопасность» должно представлять собой совокупность общего программного обеспечения и специального программного обеспечения.

Программное обеспечение КСА функционального блока «Экологическая безопасность» должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в состав КСА «Экологическая безопасность» перспективных КСА.

Программное обеспечение должно быть сертифицировано по требованиям безопасности информации.

Требования к общему программному обеспечению функционального блока «Экологическая безопасность» должны быть аналогичны требованиям к общему программному обеспечению в Приложении 5 (Требования к общему программному обеспечению функционального блока «Координация работы служб и ведомств»).

Требования к специальному обеспечению КСА функционального блока «Экологическая безопасность» должно быть аналогичны требованиям к специальному программному обеспечению КСА «Региональная платформа» функционального блока «Координация работы служб и ведомств» представленных в Приложении 6 (Требования к специальному программному обеспечению КСА «Региональная платформа» функционального блока «Координация работы служб и ведомств»).

4.2.7.6 Требования к информационному обеспечению КСА функционального блока «Экологическая безопасность»

Требования к информационному обеспечению КСА функционального блока «Экологическая безопасность» должны быть аналогичны требованиям к информационному обеспечению КСА «Региональная платформа» функционального блока «Координация работы служб и ведомств» представленных в разделе «Требования к информационному обеспечению КСА функционального блока «Координация работы служб и ведомств»

3.3 Основные технические требования к параметрам оборудования АПК «Безопасный город»

3.3.1 Требования к надежности

3.3.1.1 Состав и количественные значения показателей надежности

Для всех КСА, входящих в состав АПК «Безопасный город» должны быть обеспечены следующие уровни надежности:

- уровень сохранения работоспособности;
- уровень сохранности информации.

Показатели надежности должны обеспечивать возможность выполнения функциональных задач комплексами средств автоматизации АПК «Безопасный город».

Показатели надежности включают:

- среднее время между выходом из строя отдельных компонентов КСА, входящих в состав АПК «Безопасный город»;
- среднее время на обслуживание, ремонт или замену вышедшего из строя компонента;
- среднее время на восстановление работоспособности КСА АПК «Безопасный город».

Показатели надежности КСА АПК «Безопасный город» должны достигаться комплексом организационно-технических мер обеспечивающих доступность ресурсов, их управляемость и обслуживаемость.

Технические меры по обеспечению надежности должны предусматривать:

- резервирование критически важных компонентов КСА АПК «Безопасный город» и данных, а также отсутствие единой точки отказа;
- использование технических средств с избыточными компонентами и возможностью их горячей замены;

- конфигурирование используемых средств и применение специализированного программного обеспечения, обеспечивающего высокую доступность.

Организационные меры по обеспечению надежности должны быть направлены на минимизацию в работе КСА АПК «Безопасный город», а также персонала службы эксплуатации при проведении работ по обслуживанию комплекса технических средств КСА АПК «Безопасный город», минимизацию времени ремонта или замены вышедших из строя компонентов за счет:

- регламентации проведения работ и процедур по обслуживанию и восстановлению системы;
- своевременного оповещения должностных лиц о случаях нештатной работы компонентов КСА АПК «Безопасный город»;
- своевременной диагностики неисправностей;
- наличия договоров на сервисное обслуживание и поддержку компонентов комплекса технических средств КСА АПК «Безопасный город».

Должны быть обеспечены следующие значения показателей надежности:

- КСА АПК «Безопасный город» должны быть рассчитаны на круглосуточную работу;
- срок службы КСА АПК «Безопасный город» в целом должен составлять не менее 3 лет;
- наработка КСА АПК «Безопасный город» на отказ должна составлять не менее 5000 часов;
- наработка КСА АПК «Безопасный город» на сбой должна составлять не менее 2500 часов.

Иные количественные значения показателей надежности должны быть учтены в процессе проектирования для каждого КСА АПК «Безопасный город».

Сохранение работоспособности должно обеспечиваться при возникновении локальных отказов компонентов КСА АПК «Безопасный город»:

- отказ оборудования;
- сбой серверной, клиентской операционных систем;

- сбой СУБД в процессе выполнения пользовательских задач;
- отказ каналов связи;
- импульсные помехи, сбои или прекращение электропитания.

При нарушении или выходе из строя внешних каналов связи КСА АПК «Безопасный город» должны переходить на резервный канал, а в случае его отсутствия работать в автономном режиме, подразумевающим выполнение тех функций, которые предусматривают использование периодического обмена информацией.

Сбои или выход из строя одного накопителя на жестком магнитном диске не должны приводить к приостановке работы, т.к. в КСА АПК «Безопасный город» должно быть предусмотрено резервирование дисков.

Должна быть обеспечена возможность «горячей» замены сбойного или вышедшего из строя накопителя на жестком магнитном диске без остановки функционирования КСА АПК «Безопасный город».

Импульсные помехи, сбои или прекращение электропитания не должны приводить к выходу из строя технических средств и/или нарушению целостности данных.

Прекращение электропитания на короткое время не должно приводить к прекращению функционирования КСА АПК «Безопасный город».

Должны быть предусмотрены средства оповещения должностных лиц о нештатной работе КСА АПК «Безопасный город».

3.3.1.2 Требования к надежности технических средств и программного обеспечения

Надежность КСА АПК «Безопасный город» в части технического обеспечения должна обеспечиваться:

- наличием в КСА АПК «Безопасный город» технических средств повышенной отказоустойчивости и их структурным резервированием;
- защитой технических средств по электропитанию путем использования источников бесперебойного питания;

- выбором топологии локальной сети, обеспечивающей вариантность маршрутизации потоков информации;
- реализацией, в составе инженерных систем, средств автоматического обнаружения и локализации неисправных блоков и технических средств на безагентной основе;
- должны использоваться средства мониторинга и оповещения об аварийных ситуациях.
- автоматическим оповещением администраторов системы по нештатным ситуациям, как по средствам электронной почты, так и посредством SMS-информирования.

3.3.2 Требования безопасности

Программное обеспечение КСА АПК «Безопасный город» должно быть проверено на отсутствие известных уязвимостей к атакам на отказ и на несанкционированный доступ.

Требования к межсетевым экранам должны соответствовать Руководящему документу Государственной технической комиссии при Президенте Российской Федерации «Межсетевые экраны. Защита от несанкционированного доступа к информации. Классификация межсетевых экранов и требования по защите информации».

КСА АПК «Безопасный город» должны быть обеспечены средствами антивирусной защиты для обеспечения надежного контроля над потенциальными источниками проникновения компьютерных вирусов.

КСА, входящие в состав АПК «Безопасный город» должны обладать подсистемой информационной безопасности от несанкционированного доступа (далее НСД), которая должна удовлетворять Руководящим Документам ФСТЭК России, а также ГОСТ Р50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования». КСА АПК «Безопасный город» должны соответствовать

требованиям класса защищенности «1Г» и выше в зависимости от обрабатываемых данных и решаемых задач.

В ходе проектирования КСА АПК «Безопасный город» должен быть определен состав информации и методов ее обработки, подлежащий защите, а также разработана модель угроз и модель нарушителя.

Техническое задание на создание подсистемы информационной безопасности от НСД для каждого КСА, входящего в состав АПК «Безопасный город» должно предусматривать:

- разработку модели угроз и нарушителя для каждого КСА;

- определение:

 - требований по защите от несанкционированного доступа;

 - требований к средствам криптографической защиты;

 - требований к средствам обнаружения и предупреждения атак, а также к средствам межсетевого экранирования и шлюзам;

 - требований к средствам антивирусной защиты;

 - требований по защите персональной информации;

 - разработку технических решений по нейтрализации выявленных угроз и действий нарушителя и обеспечивающих выполнение требований по безопасности;

 - проведение аттестации КСА.

Технические средства должны быть надежно заземлены в соответствии с действующими правилами и требованиями фирм-изготовителей оборудования.

Все программное и аппаратное обеспечение, реализующее функционал защиты информации, должно быть сертифицировано в системе сертификации ФСТЭК России.

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

Электропитание технических средств должно соответствовать III категории «Правил устройств электроустановок».

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

Требования и нормы проектирования охранно-тревожной сигнализации должны соответствовать документу РД 78.36.003-2002.

Требования и нормы проектирования и установки пожарной сигнализации должны соответствовать документу РД СП 5.13130.2009.

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

3.3.3 Требования к эргономике и технической эстетике

Графический интерфейс КСА АПК «Безопасный город» должен отвечать следующим требованиям:

- отображение на экране преимущественно необходимой для решения текущей прикладной задачи информации;
- максимальная унификация процедур реализации аналогичных функций в различных компонентах КСА АПК «Безопасный город»;
- использование функциональных и «горячих» клавиш, при этом на экране должна находиться подсказка о назначении таких клавиш;
- отображение на экране хода длительных процессов обработки.

Процедуры ввода данных должны отвечать следующим требованиям:

- пользователь должен иметь возможность гибко контролировать ввод данных: просматривать введенные данные на мониторе, производить их корректировку или отказаться от ввода;

- при вводе должны использоваться справочники для контроля вводимых данных и списки допустимых значений;
- обеспечение возможности ввода значений по умолчанию.

Интерфейс должен обеспечивать корректную обработку ситуаций, вызванных неверными действиями, неверным форматом или недопустимыми значениями входных данных. В указанных случаях должны выдаваться соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

3.3.4 Требования к эксплуатации, техническому обслуживанию и ремонту

Эксплуатация КСА АПК «Безопасный город» должна производиться в соответствии с эксплуатационной документацией и Регламентом технического обслуживания. Регламент технического обслуживания должен быть определен в составе эксплуатационной документации.

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

Технические средства и персонал должны размещаться в существующих помещениях объектов автоматизации, которые по климатическим условиям должны соответствовать ГОСТ 15150-69. Размещение технических средств и организация автоматизированных рабочих мест должно быть выполнено в соответствии с требованиями (СНиП) ГОСТ 21958-76.

3.3.5 Требования по сохранности информации при авариях

Сохранность информации в КСА, входящих в состав АПК «Безопасный город» должна обеспечиваться при следующих аварийных ситуациях:

- импульсные помехи, сбои и перерывы в электропитании;
- нарушение или выход из строя каналов связи;
- сбой общего программного обеспечения;
- сбой специального программного обеспечения;
- выход из строя аппаратных средств (серверы, системы хранения данных, АРМ и другие);
- ошибки в работе персонала.

Эксплуатация КСА АПК «Безопасный город» должна производиться в соответствии с эксплуатационной документацией и Регламентом технического обслуживания.

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

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

Должно быть предусмотрено текущее ежедневное техническое обслуживание КСА АПК «Безопасный город». При возникновении неисправностей, должно осуществляться оперативное техническое обслуживание, временные регламенты которого не должны превышать указанных значений времени восстановления.

Регламент технического обслуживания должен быть определен в составе эксплуатационной документации.

Размещение технических средств и организация автоматизированных рабочих мест должны быть выполнены в соответствии с требованиями ГОСТ

21958-76 «Система «человек-машина». Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования».

3.3.6 Требования к защите от влияния внешних воздействий

Технические средства КСА АПК «Безопасный город» должны отвечать требованиям ГОСТ 19542-83, ГОСТ 29339-92, ГОСТ Р50628-2000, требованиям Госкомсвязи России «Автоматизированные системы управления аппаратурой электросвязи» 1998г. по электромагнитной совместимости и помехозащищенности.

Технические средства должны удовлетворять требованиям по электромагнитной совместимости, определенным в ГОСТ 22505-97 и ГОСТ Р51275 2006.

3.3.7 Требования к патентной чистоте

Проектные решения КСА АПК «Безопасный город» должны отвечать требованиям по патентной чистоте согласно действующему законодательству Российской Федерации.

При поставке КСА АПК «Безопасный город» должны быть выполнены требования Федерального закона Российской Федерации от 23.09.92 г. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных».

3.3.8 Требования по стандартизации и унификации

Программная реализация необходимого протокола или протоколов Единого стека открытых протоколов в КСА АПК «Безопасный город», планируемых к внедрению, должны проходить проверку на соответствие требованиям наиболее поздней версии Единого стека открытых протоколов (см.

Приложение 2) по методике, утвержденной федеральным органом исполнительной власти – координатором АПК «Безопасный город».

Программная документация на КСА АПК «Безопасный город», планируемых к внедрению, должна проходить проверку на соответствие настоящим требованиям по методике, утвержденной федеральным органом исполнительной власти – координатором АПК «Безопасный город».

Процесс разработки КСА АПК «Безопасный город» должен соответствовать требованиям к созданию АС, регламентированных стандартами:

ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

КСА АПК «Безопасный город» должны быть разработаны в соответствии с требованиями национальных стандартов (ГОСТ), Единой системы конструкторской документации, Единой системы программной документации, а также требованиями нормативно-методических и руководящих документов ФСТЭК России и ФСБ России.

Разработка программных средств должна учитывать требования к реализации программного обеспечения на основе отечественных и (или) открытых технологий, с учетом требований Распоряжения Правительства №2299-р от 17 декабря 2010 года «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения (2011-2015 годы)».

В КСА АПК «Безопасный город» должны использоваться типовые проектные решения; унифицированные формы управленческих документов; общероссийские классификаторы технико-экономических и социальных

показателей и классификаторы других категорий; унифицированные методы реализации функций системы; стандартные технические и программные средства общего назначения, общепринятые (стандарты де-факто) языки и процедуры информационного обмена.

3.4 Предложения по режимам функционирования, диагностирования и работы АПК «Безопасный город».

КСА АПК «Безопасный город» должны функционировать в штатном и автономном режимах.

Штатный режим является основным режимом функционирования КСА АПК «Безопасный город», при котором поддерживается выполнение всех функций КСА и обеспечивается работа всех пользователей.

Автономный режим является вспомогательным режимом функционирования отдельных сегментов КСА АПК «Безопасный город», т.е. все или отдельные функции комплекса становятся недоступными для пользователей. В этом режиме осуществляются техническое обслуживание, реконфигурация, модернизация и совершенствование компонентов КСА АПК «Безопасный город», а также резервное копирование информационного наполнения и конфигурационных файлов.

КСА АПК «Безопасный город» в целом должна обеспечивать выполнение целевых функций в режиме 24x365 (24 часа в день, 365 дней в году) за исключением периодов технического обслуживания, предусмотренных технической документацией.

Оборудование и ПО КСА АПК «Безопасный город» должны проектироваться для круглосуточной работы, позволять осуществлять резервирование и восстановление после сбоев.

Диагностирование должно обеспечиваться штатными средствами (тестирование и протоколирование).

При необходимости, могут быть предусмотрены дополнительные организационно-методические и технические меры по автоматизированному контролю и диагностированию сбоев в работе аппаратно-программных средств структурных компонентов АПК «Безопасный город».

Под организационно-методическими мерами понимаются мероприятия по разработке структуры эксплуатационных подразделений, соответствующей

территориально-распределенному характеру АПК «Безопасный город» и способной производить своевременную диагностику функционирования его сегментов.

В методические меры рекомендуется включать мероприятия по подготовке и обучению персонала, а также разработке необходимых эксплуатационных документов по диагностике функционирования различных сегментов АПК «Безопасный город».

В качестве технических мер могут создаваться инструменты диагностирования основных компонентов АПК «Безопасный город».

Диагностические инструменты должны предоставлять удобный интерфейс для возможности просмотра диагностических событий и мониторинга процессов работоспособности компонентов комплекса.

Диагностирование сегментов АПК «Безопасный город» должно осуществляться посредством анализа различных системных журналов (например, журнала запуска и остановки, журнала возникновения исключительных ситуаций и т.д.) и информационных (log) файлов системы.

Объектами диагностирования могут являться:

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

Диагностирование компонентов АПК «Безопасный город» должно осуществляться во всех режимах его функционирования.

В случае необходимости, для организации работы подразделений, обслуживающих КСА АПК «Безопасный город», может быть разработан комплекс программ для эксплуатационной службы.

ЗАКЛЮЧЕНИЕ

В методическом пособии обследованы и проанализированы дежурные-диспетчерские и экстренные службы в более 200 пилотных муниципальных образованиях в 53 регионах 19 округах Российской Федерации.

При проведении обследования проанализированы риски возникновения ЧС на территории муниципальных образований, исследована ИТ-инфраструктура и действующие автоматизированные системы различных уровней (федерального, регионального, муниципального) и различной ведомственной принадлежности.

Сравнительный анализ современных интеграционных решений, представленных в настоящее время на Российском рынке показал, что по функциональным критериям все решения близки и явного лидера не выделено.

Проведенные исследования позволили оценить возможности интеграции существующих АС различных уровней и различной ведомственной принадлежности в единое информационное пространство с использованием современных интеграционных решений.

В ходе работы подготовлены:

- 1) Предложения по интеграции действующих информационно-аналитических, управляющих и других систем в области обеспечения природно-техногенной и общественной безопасности в АПК «Безопасный город»;
- 2) Предложения по применению действующих информационно-аналитических, управляющих других систем в области обеспечения природно-техногенной и общественной безопасности в АПК «Безопасный город»;
- 3) Проект архитектурных решений АПК «Безопасный город»;
- 4) Презентация результатов работы.

Материалы, приведенные в методическом пособии могут использоваться при формировании единой технической политике по вопросам создания и внедрения АПК «Безопасный город» в муниципальных образованиях.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. В. А. Акимов, В. В. Лесных, Н. Н. Радаев «Основы анализа и управления риском в природной и техногенной сферах. — М.: Деловой экспресс, 2004. — 352 с.
2. Концепция построения и развития аппаратно-программного комплекса "Безопасный город". Утверждена распоряжением Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р.
3. Шапошников А.С. Совершенствование управления рисками чрезвычайных ситуаций в мегаполисе на основе их мониторинга и прогнозирования. Диссертация на соискание ученой степени кандидата технических наук. <http://www.dissercat.com/content/sovershenstvovanie-upravleniya-riskami-chrezvychainykh-situatsii-v-megapolise-na-osnove-ikh->
4. Шабалин Е.К. Оценка последствий и механизм предотвращения чрезвычайных ситуаций в крупном промышленном городе Научная библиотека диссертаций и авторефератов disserCat <http://www.dissercat.com/content/otsenka-posledstviy-i-mekhanizm-predotvrashcheniya-chrezvychainykh-situatsii-v-krupnom-promy#ixzz3sA082gLl>
5. Методические рекомендации АПК «Безопасный город» построение (развитие), внедрение и эксплуатация, утвержденному МЧС России 22.02.2015 № 2-4-87-12-14 .
6. ГОСТ Р 22.0.02-94 Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий.
7. ГОСТ Р 55059-2012 Безопасность в чрезвычайных ситуациях. Менеджмент риска чрезвычайной ситуации. Термины и определения.
8. ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем.

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Федеральный конституционный закон от 30 мая 2001 года № 3-ФКЗ «О чрезвычайном положении».
2. Федеральный закон от 28 декабря 2010 года № 390-ФЗ «О безопасности».
3. Федеральный закон от 21 декабря 1994 года № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера».
4. Федеральный закон от 21 декабря 1994 года № 69-ФЗ «О пожарной безопасности».
5. Федеральный закон от 9 января 1996 года № 3-ФЗ «О радиационной безопасности».
6. Федеральный закон от 21 июля 1997 года № 117-ФЗ «О безопасности гидротехнических сооружений».
7. Федеральный закон от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму».
8. Федеральный закон от 9 февраля 2007 года №16-ФЗ «О транспортной безопасности».
9. Федеральный закон от 7 февраля 2011 года N 3-ФЗ «О полиции».
10. Федеральный закон от 06 октября 2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации».
11. Федеральный закон от 07 июля 2003 года № 126–ФЗ «О связи».
12. Постановление Совета Министров – Правительства Российской Федерации от 1 марта 1993 года № 178 «О создании локальных систем оповещения в районах размещения потенциально опасных объектов».
13. Постановление Правительства Российской Федерации от 30 декабря 2003 года № 794 «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций».

14. Постановление Правительства РФ от 08.09.2010 N 697 (ред. от 19.03.2014) «О единой системе межведомственного электронного взаимодействия».

15. Постановление Правительства Российской Федерации от 25 августа 2008 года № 641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS».

16. Постановление Правительства Российской Федерации от 24 марта 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».

17. Постановление Правительства Российской Федерации от 21 мая 2007 года № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера».

18. Постановление Правительства Российской Федерации от 8 ноября 2013 г. № 1007 «О силах и средствах единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций»

19. «Основы государственной политики в области безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года» от 15.11.2011 года № Пр-3400.

20. Приказ МЧС России от 4 ноября 2004 года № 506 «Об утверждении паспорта безопасности опасного объекта».

21. Постановление Правительства Российской Федерации от 4 сентября 2003 года № 547 «О подготовке населения в области защиты от чрезвычайных ситуаций природного и техногенного характера».

22. Приказ МЧС России от 28 февраля 2003 года № 105 «Об утверждении требований по предупреждению чрезвычайных ситуаций на потенциально опасных объектах и объектах жизнеобеспечения».

23. Концепция построения и развития АПК «Безопасный город» утвержденная распоряжением Правительства российской Федерации от 03.12.2014 № 2446-р.

24. Методические рекомендации АПК «Безопасный город» построение (развитие), внедрение и эксплуатация. Утвержденные МЧС России 22.02.2015 №2-4-87-12-14.

25. Временные единые требования к техническим параметрам сегментов аппаратно-программного комплекса «Безопасный город». Утвержденные МЧС России 29.12.2014 «14-7-5552.