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»

(Приложения)

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

Приложение А
Сравнение интеграционных решений.

Таблица А.1– Краткие характеристики интеграционных решений

Продукт/ Решение	Разработчик поставщик	Источник информации - сайт	КРИТЕРИИ ОЦЕНКИ									
			Функциональность, технологичность и	Устойчивость к "Санкциям" и пр.	Информационная	Масштабность и сложность Проектов.	Простота представления, изложения и понимания	Сертификация	Доработка, ее доступность, гибкость	Наличие Исх.кодов и документации	Наличие адаптеров взаимодействия с	Примечание
IBM WebSphere ESB	IBM	http://www.ibm.com/	+	–	–	+	+/–	+/–	+/–	–	–	
Oracle Service Bus	Oracle	http://www.jetinfo.ru/stati/integratsionnye-resheniya-oracle-obzor-vazhnejshikh-napravlenij	+	–	–	+	+/–	+/–	+/–	–	–	
SAP NetWeaver	SAP	http://www.aris-portal.ru/docs/SAP_Netweaver.pdf	+	–	–	+	++	+/–	+/–	–	–	
Azure BizTalk Server Service Bus Dynamics AX	Microsoft	https://azure.microsoft.com/ru-ru/solutions/integration/	+	–	–	+	+/–	+/–	+/–	–	–	
Sonic Software	@Astera "Эксклюзивные бизнес-технологии"	http://www.astera.ru/pr/17050/	+	+	–	+/–	+/–	+/–	+	–	–	
SAS	SAS	http://www.sas.com/ru_ru/news/press-releases/2015/april/SAS_Data_Loader_for_Hadoop.html	–	–	–	+/–	–	+/–	+/–	–	–	
Кобальт	Ланит	http://lanit.ru/business	–	+	–	+/–	+/–	+/–	+	–	–	
Mule ESB	OpenSource	http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Mule_ESB	+	+	–	+/–	+	+	+	–	–	
Jboss EJB	OpenSource	http://ejb3.jboss.org/	+/–	+	–	+/–	+/–	+/–	+	–	–	
Apache ServiceMix	OpenSource	http://servicemix.apache.org/index.html	+	+	–	+/–	+/–	+/–	+	–	–	

Продукт/ Решение	Разработчик поставщик	Источник информации - сайт	КРИТЕРИИ ОЦЕНКИ									
			Функциональность, технологичность и	Устойчивость к "Санкциям" и пр.	Информационная	Масштабность и сложность Проектов.	Простота представления, изложения и понимания	Сертификация	Доработка, ее доступность, гибкость	Наличие Исх.кодов и документации	Наличие адаптеров взаимодействия с	Примечание
Mediator ESB	компании «ДаСистемс»	http://www.dasystems.ru/esb.html	+/–	+/–	–	–	+	+/–	+	–	–	
Software AG	Software AG	http://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Software_AG	+	–	–	+	+/–	+/–	+	–	–	
Open ESB	Sun Microsystems	см. Oracle	+	–	–	+	+/–	+/–	+/–	–	–	
OW2 Petals	Sun Microsystems	см. Oracle	+	–	–	+	+/–	+/–	+/–	–	–	
ORACLE and BEA AquaLogic	BEA Systems	http://www.oracle.com/us/corporate/acquisitions/bea/index.html	+	–	–	+	+/–	+/–	+/–	–	–	
TS Bus	ТехносервАС		+	+	+	+/–	+	+	+	+	+(*)	
*–Имеет адаптеры взаимодействия с подсистемами АПК «БГ» в т.ч. подсистемами мониторинга и оповещения												

Приложение Б
Требования к функциональным блокам АПК «Безопасный город»

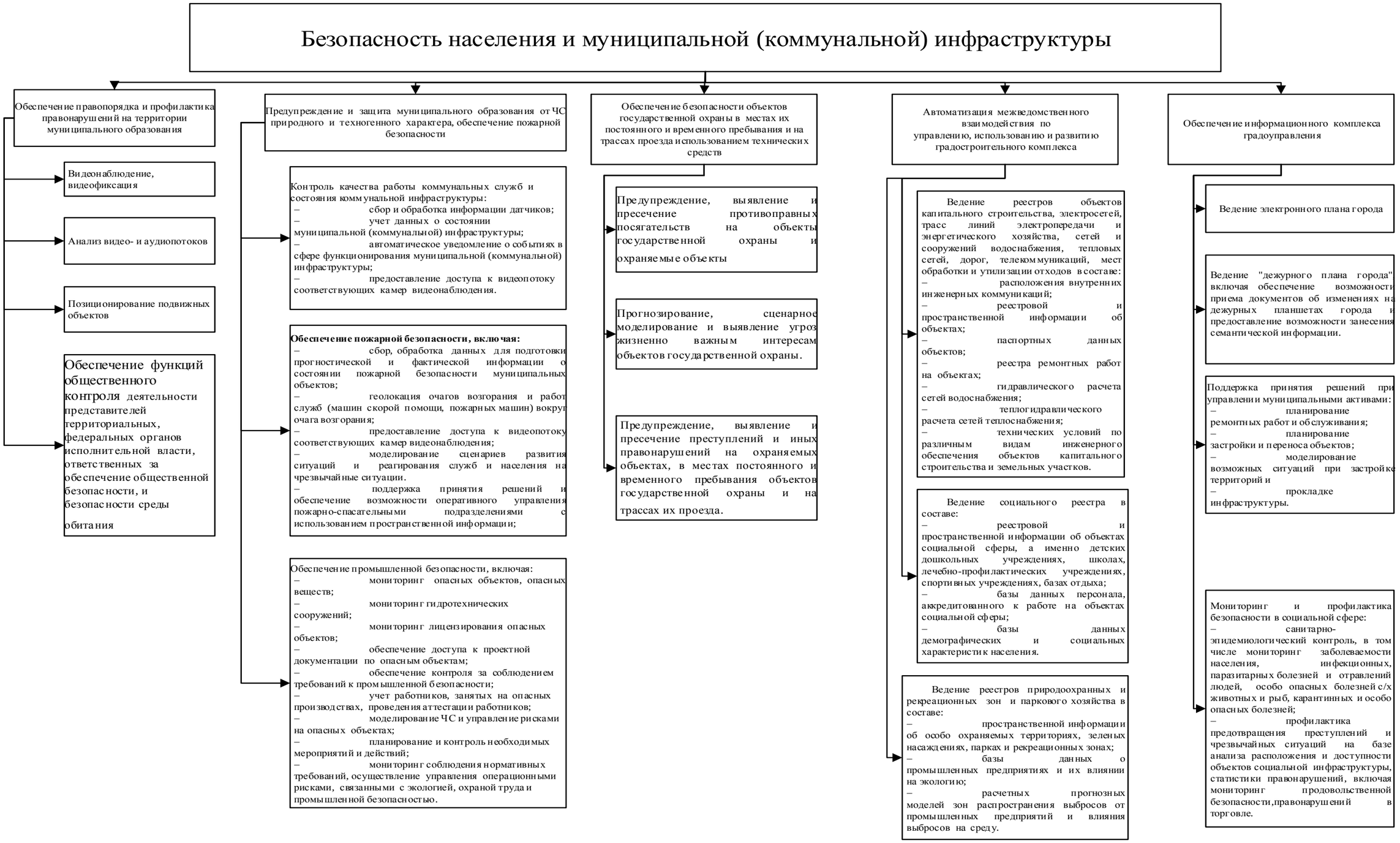


Рисунок Б.1 – Детализация требований к функциональным блокам АПК «Безопасный город»

Транспортная безопасность

Обеспечение правопорядка и профилактика правонарушений на дорогах, объектах транспортной нфраструктуры

Видеонаблюдение и видеофиксация:
– фактов нарушения правил дорожного движения;
– правонарушений в области дорожного движения и передачу полученной информации в центры.

Видеоанализ:
– выявление потенциально опасных событий на дорогах и объектах транспортной инфраструктуры елезнодорожного, водного, воздушного и автомобильного транспорта, метрополитена и дорожного хозяйства;
– восстановление хронологии происшествий;
– отслеживание маршрутов транспортных средств.

Обеспечение функций общественного контроля над работой представителей правоохранительных структур на местах

Моделирование транспортных потоков на основе анализа прогнозируемой ситуации

Обеспечение безопасности дорожного движения

Управление логистикой общественного и личного транспорта

Организация и управление муниципальным парковочным пространством

Динамическое прогнозирование дорожной ситуации на базе поступающих в режиме реального времени данных с видеокамер, датчиков движения

Геолокация и фиксация событий (инцидентов) на дорогах с визуализацией на карте города

Контроль маршрутов движения общественного транспорта

Мониторинг маршрутов воздушных судов, водных судов и железнодорожного транспорта

контроль результатов технического мониторинга объектов транспортной инфраструктуры

контроль технического состояния транспортных средств

Обеспечение безопасности на транспорте

Экстренная связь на транспортных средствах, включая автоматическое оповещение служб экстренного реагирования при авариях и других чрезвычайных ситуациях.

Экстренная связь на объектах транспортной инфраструктуры, объектах систем связи, навигации и управления движением транспортных средств, а также на иных обеспечивающих транспортный комплекс зданиях, сооружениях, устройствах и оборудовании), включая автоматическое оповещение служб экстренного реагирования при авариях и других чрезвычайных ситуациях, геолокация точки вызова.

Информирование о чрезвычайных ситуациях на транспортных средствах и объектах транспортной инфраструктуры:
– идентификацию событий на основе поступающей информации с датчиков, установленных на транспортных средствах с визуализацией на электронной карте города;
– идентификацию событий на основе поступающей информации с датчиков, установленных на объектах транспортной инфраструктуры с визуализацией на электронной карте города;
– обеспечение доступа к видеопотоку с транспортных средств и
– объектов транспортной инфраструктуры;

Обеспечение автоматизированной проверки и учета данных в рамках процедуры лицензирования перевозчиков, контроль лицензиатов на предмет выполнения условий лицензирования.

Экологическая безопасность

Мониторинг предельно допустимых выбросов загрязняющих веществ

Обеспечение взаимодействия природопользователей и контролирующих органов: информационное обеспечение деятельности органов государственной власти в сфере охраны окружающей среды; предоставление доступа к единой нормативной и отчетной базе природопользователей; организацию возможности удаленной подачи отчетности и оплаты штрафов за нарушения требований природоохранного законодательства.

Контроль в области обращения с отходами: контроль процессов сбора, транспортировки, переработки и утилизации отходов; ониторинг состояния окружающей среды в районах размещения отходов и мониторинг экологической обстановки территорий городов в целях предотвращения и выявления несанкционированных мест размещения и захоронения отходов.

Комплексный мониторинг природных явлений и прогнозирование: загрязнения окружающей среды; состояния суши; водных ресурсов; невозобновляемых природных ископаемых; контроль состояния почв; сейсмической активности и обеспечение сейсмической безопасности; гидрологической обстановки и обеспечение безопасности при наводнениях;гидрометеорологической обстановки; лесопожарной опасности;прогнозирование сценариев развития и последствий природных и техногенных инцидентов с учетом погодных условий;мониторинг экологической обстановки на особо охраняемых природных территориях местного значения.

Организация межведомственного взаимодействия предусматривает:
– автоматическое архивирование и обеспечение хранения видео- информации и отчетной информации об инцидентах и всей сопутствующей информации;
– формирование отчетных форм для муниципальных органов власти, бизнеса, населения с гибким механизмом настройки и расширениявозможностей, позволяющим формировать шаблон отчетных форм за любой период времени; сводных отчетов по нескольким аналитическим измерениям; обеспечение качественного обмена информацией о результатах непрерывного мониторинга услуг связи.

Координация работы служб и ведомств

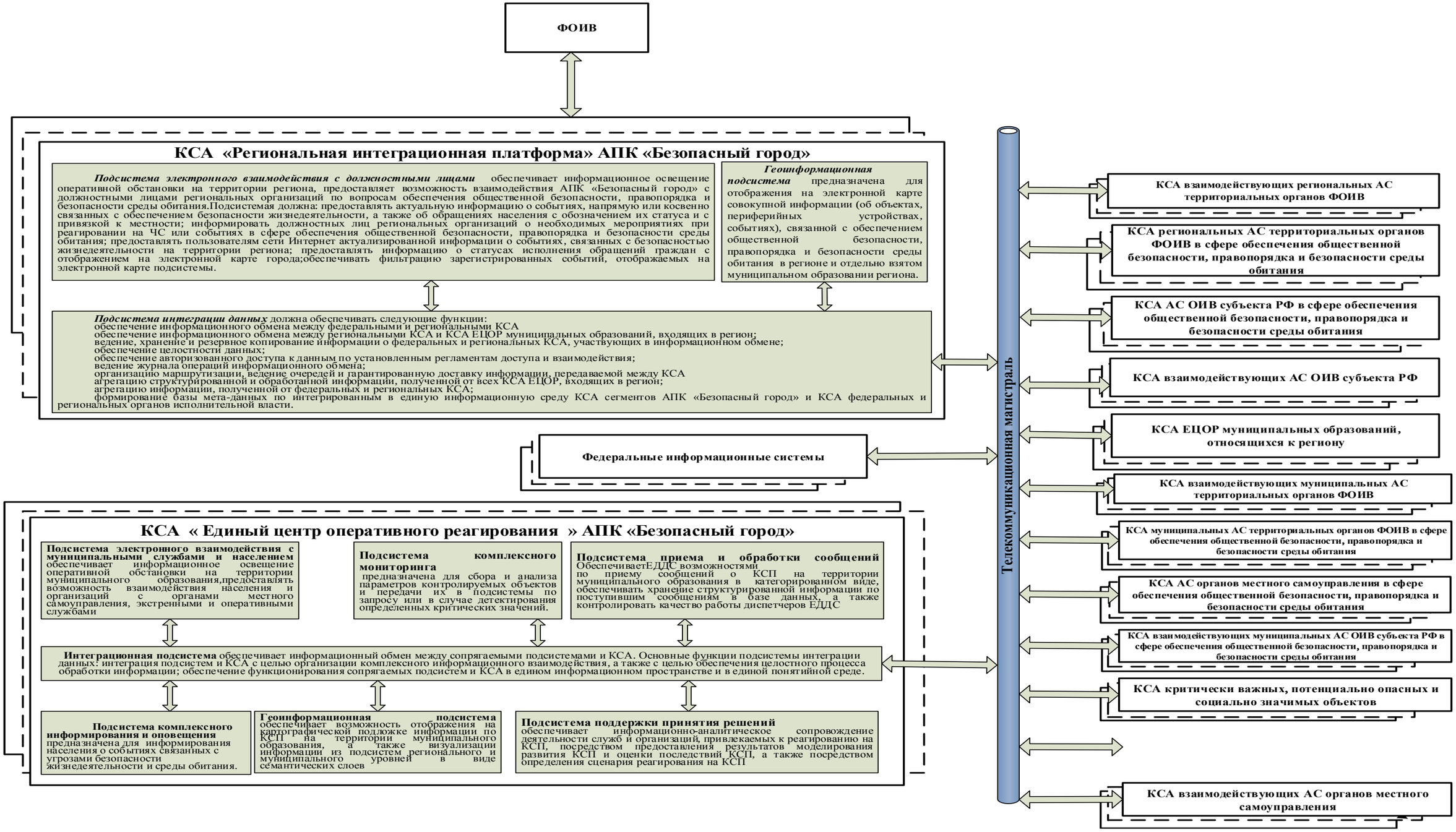
Обеспечение возможностей оперативного реагирования с учетом разграничения прав доступа предусматривает: прием и обработку обращений; автоматическую регистрацию всех входящих и исходящих звонков, электронных писем. хранение информации об обращениях и об инициаторе обращения; статическую и интеллектуальную маршрутизацию обращения (организацию очереди и маршрутизацию по номеру абонента); геолокацию и визуализацию на рабочей станции оператора информации о поступившем звонке и карточке клиента; контроль качества работы операторов; планирование расписания рабочих смен операторов; контроль обработки и исполнения заявки со стороны федеральных, региональных и муниципальных служб; оперативное предоставление всем службам доступа к оперативной и архивной информации, касающейся инцидента в соответствии с правами доступа; контроль качества исполнения заявки муниципальными службами (организация обратной связи о качестве работы всех служб и ведомств); геофиксацию событий на электронной карте с возможностью фильтрации по типу событий, а также с возможностью детализации информации по любым запросам разной тематической направленности.

Организация межведомственного взаимодействия предусматривает:
– создание единого информационного пространства, в котором любой инцидент оперативно доводится до всех служб оперативного реагирования и муниципальных служб, отвечающих за проведение работы над инцидентом;
– организацию межведомственного взаимодействия на уровне служб оперативного реагирования и муниципальных служб; формирование поручений на основе заранее подготовленных шаблонов и сценариев реагирования; контроль хода исполнения поручения; обеспечение сценариев информирования при угрозе срыва срока исполнения поручения;
– обеспечение доступа к информационной базе градоуправления и архитектуры, включая: получение оперативной информации о воздействии события на муниципальную инфраструктуру с отображением на электронной карте; организацию и координацию совместной работы различных муниципальных служб и служб оперативного реагирования;
– обеспечение безопасного хранения и обработки данных, включая: обеспечение защищенного доступа к информации с использованием средств криптографической защиты информации.
– сводных отчетов по
– нескольким аналитическим измерениям;
– обеспечение качественного обмена информацией.
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.
– а к оперативной и архивной информации, касающейся инцидента в соответствии с правами доступа;
– контроль качества исполнения заявки муниципальными службами (организация обратной связи о качестве работы всех служб и ведомств);
– в) геофиксацию событий на электронной карте с возможностью фильтрации по типу событий, а также с возможностью детализации информации по любым запросам разной тематической направленности.

Рисунок Б2 - Детализация требований к функциональным блокам АПК «Безопасный город»

Приложение 1

Структурная схема АПК «Безопасный город»



Приложении 2
Требования к Единому стеку открытых протоколов информационного взаимодействия КСА 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 1. 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 1.22.

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 глоссарий общих тем извещений, таких как

1 Обязательный The Real-time Pull-Point Notification Interface в соответствии с ONVIF Core Specification требует постоянного опроса источников событий требуется постоянное поддержание пропорционального количества TCP-соединений, что приводит к избыточной нагрузке на участников обмена и сетевые узлы и плохо работает в условиях «слабого» канала связи с источником (например, GSM-модема). В то же время механизм Base Notification позволяет реализовать асинхронную передачу извещений по факту возникновения соответствующих событий.

2 В то время, как Message хорошо подходит для передачи информации о системных событиях, таких как «изменение конфигурации модуля видеоанализа», alert непосредственно предназначен для передачи сведений о событиях безопасности жизнедеятельности, чрезвычайного оповещения и др.

«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 глоссариев. 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 общий глоссарий 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, разоборудование 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

Приложении 3

Перечень федеральных государственных информационных систем и систем мониторинга

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
1 Информационно-аналитическая система Министерства здравоохранения Российской Федерации Минздрав России	– 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; HTML; XLSX; DOC;

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
2 Комплекс программных средств по ведению паспортов медицинских учреждений **Минздрав России**	Данные паспортов медицинских учреждений	Данные паспортов медицинских учреждений	Данные паспортов медицинских учреждений	DOC; DOCX; XML; XLSX
3 ЕМИСС **Минкомсвязь России**	Данные официальной статистической информации, включая метаданные, формируемые в соответствии с федеральным планом статистических работ.			Внутренний формат; XML; HTML; XLS
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
5 ЕПГУ **Минкомсвязь России**	Данные мониторинга хода предоставления государственных услуг или исполнения государственных функций.			HTML; XML

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
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			HTML; PDF; XML
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
9 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

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
10 ИС Россвязи **Минкомсвязь России, Россвязь**	Данные реестра сетей связи. Данные реестра почтовых индексов. Данные реестра российской системы и плана нумерации.			DOC; RTF; TIFF
11 ИС АКНД ОУ **Минобрнауки России, Рособрнадзор**	Данные электронных досье образовательных учреждений.			XLS; HTML; DOC; DOCX; RTF; GIF; JPEG; PNG; PDF; XML; XLSX
12 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; BMP; HTML; ZIP; XLSX; DOC; DOCX; TXT; PDF; GIF; ICO; JPEG; JPEG 2000; PNG; mdb; SHP; MDF; CSV; dbf; XML
13 АИС ГВР **Минприроды России, Росводресурсы**	Сведения о водных объектах, о водопользователях и инфраструктуре на водных объектах. Ретроспективная документированная информация о водных объектах, о водопользователях.			XML; DOC; RTF; PDF; JPEG

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
14 ИС ОД Минприроды России, Росводресурсы	Информация о чрезвычайных ситуациях и происшествиях в сфере деятельности Росводресурсов.			XLS; HTML; RAR; ZIP; DOC; TXT; RTF; BMP; ICO; JPEG; PNG; PDF; WAV; mdb; dbf; XML
15 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 объектах и при угрозе попадания в водные объекты.			ArcGIS Server 9.2; 7zip, Ccleaner, Python 2.5, LogMeIn Hamachi

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
16 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
17 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
18 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

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
19 АС ПГУ МЭВ Росгидромета Минприроды России, Росгидромет	Информация о состоянии атмосферного воздуха и его загрязнений. Информация о состоянии поверхностных водных объектов и их загрязнении			XML
20 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; HTML
21 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			HTML; MDF
22 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			XML;XLS; DOC; DOCX

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
	размещении отходов субъектами малого и среднего предпринимательства. Данные сводных отчетов по негативному воздействию на окружающую среду.			
23 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
24 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

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
25 АИС НСИ **Минсельхоз России**	Данные реестров, регистров, справочников, классификаторов объектов контролируемых Минсельхозом России			Внутренний формат; XML; HTML; XLS; XLSX; PDF; CSV; dbf
26 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
27 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,			XML; GeoTIFF; GDB; XML

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
	нанесенного чрезвычайными ситуациями сельскохозяйственным угодьям.			
28 ГИС "Деметра" Минсельхоз России, Россельхознадзор	Информация о состоянии земель сельскохозяйственного назначения фитосанитарных и ветеринарных карантинных зонах и объектах			XML; HTML ZIP; DOC; RTF; JPEG; TIFF; PDF; XML
29 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; HTML; DOC; RTF; TXT
30 ЕГИС ОТБ Минтранс России	Сведения об опасных объектах транспортной инфрастурктуры и транспортных средствах; Сведения об аварийных ситуациях и действиях диспетчерских, аварийных и технических служб объектов; Результаты расчетов прогнозов развития чрезвычайных ситуаций			XML; HTML; DOC; GIF; JPEG; PDF; XML

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
	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			
31 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.			
32 ЕАВИИАС МСЭ Минтруд России	Данные статистической и аналитической отчетности			XML; HTML; XLSX; DOCX; JPEG; PNG; TIFF; PDF

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
33 АИС ЕСУИ Минтруд России	Данные единой системы учета инвалидов в Российской Федерации			XML
34 АИС "Миграпотоки" Минтруд России	Данные о количественных показателях трудовых миграционных потоков граждан, осуществляющих трудовую деятельность вне места постоянного проживания			XLS; HTML; RAR; ZIP; AVI; mp4; DOC; DOCX; TXT; RTF; PDF; BMP; GIF; JPEG; TIFF; MP3; WMA; CSV;
35 ФГИС ТП Минэкономразвития России	Данные (слои) единой информационной системы территориального планирования Российской Федерации, информация о состоянии, использовании и планируемом развитии территорий.			XLS; DWG; MIFF/MID; GeoTIFF; MrSID; DOC; DOCX; TXT; RTF; JPEG; PNG; TIFF; PDF; SHP; GML; SXF; ODF; RSW
36 ПК ПВД Минэконом-развития России, Росреестр	Данные информационных систем государственного кадастра недвижимости и государственной регистрации прав для нужд Росреестра			Внутренний формат; ZIP; XML

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
37 АИС "Электронный инспектор" МЧС России	Данные состояния пожарной безопасности объектов защиты и результатов надзорной деятельности на объектах защиты			XLS; HTML; DOC; DOCX; TXT; RTF; PDF; JPEG; ppt; pptx; XML
38 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.			HTML; ZIP; DOC; JPEG; JPG
39 ФБД "ПОЖАРЫ" МЧС России	Данные единой государственной системы статистического учета пожаров и последствий от них в Российской Федерации			dbf

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
40 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.			XLS; HTML; RAR; ZIP; XLSX; DOC; DOCX; RTF; TIFF; PDF; CSV; dbf; XML
41 Стрелец-Мониторинг (Аргус Спектр)	Предназначена для обработки и передачи данных 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	Передача сигнала «Пожар» от систем автоматической пожарной сигнализации, смонтированных на объектах защиты	нет	
42 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 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. Обмен информацией между органами управления и организациями осуществляется как по вертикали (между органами управления и	– реестр организаций, обеспечивающих выполнение мероприятий, включая данные по количественному составу специальной техники по типам и запасам расходных материалов	– по оперативным событиям (ЧС, угрозы ЧС, происшествия) – по прогнозам неблагоприятных и опасных явлений – по органам управления,	По запросу взаимодействующей системы в соответствии с протоколом информационно-технического взаимодействия.

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	**Входящая информация (получает из АПК БГ)**	**Формат взаимодействия**
	организациями разного уровня иерархии), так и по горизонтали (между органами управления и организациями одного уровня иерархии). 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).	– реестр спецоборудования – уровень рисков по объектам базы данных – сводные данные по рискам на объектах по различным критериям,	силам и средствам РСЧС, – по потенциально-опасным объектам, – по объектам транспортной инфраструктуры; – по социально-важным объектам и объектам с массовым пребыванием людей; – по объектам мониторинга;	
43 КСМ-ЗН (Комплексная система мониторинга защиты населения)	– Осуществление непрерывного автоматизированного контроля радиационной обстановки и метеопараметров; – обработка, хранение и представление оперативных данных с использованием геоинформационных технологий; – оценка и прогноз радиационной обстановки, оценка доз облучения населения и выработка рекомендаций по мерам защиты населения в случаях ЧС с радиационным фактором.			

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
44 Автоматизированная система расчета времени достижения фронтом пожара населенных пунктов (КосмоМониторинг)	– - Расчет потенциальных угроз населенным пунктам по данным космического мониторинга (термоточкам); – - прогноз развития пожароопасной обстановки; – - расчет времени достижения пожара до населенного пункта.			
45 **Система поиска и отображения космоснимков «Космоплан»**	- Получение космоснимков, карт различного масштаба.			
46 **БСЧС – автоматизированная система информационного обеспечения СМПЧС и НЦУКС.**	- Предоставление данных по параметрам биолого-социальных источников ЧС; - предоставление информации о различных заболеваниях животных, человека и растений.			
47 **ГЛОНАСС**	- Глобальная оперативная навигация приземных подвижных объектов: наземных (сухопутных, морских, воздушных) и низкоорбитальных космических.			
48 **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.			

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
49 **ИС ЕДДС - информационная система Единой дежурно-диспетчерской службы(ЗАО «НПП ТЕЛДА»)**	- 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); - 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;			

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	**Входящая информация (получает из АПК БГ)**	**Формат взаимодействия**
	- обобщение информации о произошедших ЧС (за сутки дежурства), ходе работ по их ликвидации и представление соответствующих докладов по подчиненности.			
50 **ОКСИОН**	- 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 людей на основе использования современных технических средств и технологий.	Видеоинформация с камер наблюдения.		
51 **Систему 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.			
52 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			

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
	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, необходимой для проведения аварийно-спасательных работ и ликвидации последствий аварий, пожаров, ЧС.			
53 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).			
54 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 групп населения, которые могут находиться в данной зоне.			
55 **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.			
56 **РАСЦО - Региональная автоматизированная**	Предназначена для обеспечения своевременного доведения информации и сигналов оповещения до органов управления, сил и средств гражданской обороны, территориальных подсистем единой государственной системы			

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
система централизованного оповещения населения	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.			
57 Федеральная информационная адресная система (ФИАС)	Федеральная информационная адресная система (ФИАС) содержит достоверную единообразную и структурированную адресную информацию по территории Российской Федерации, доступную 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.			ФИАС является систематизированным сводом актуальных адресных сведений, истории их изменения. Адресные сведения в ФИАС представлены: классификатором адресообразующих элементов (далее - КЛАДЭ); сведениями об элементах адреса, идентифицирующих адресуемые объекты - земельные участки и объекты капитального строительства (дома, владения, домовладения, корпуса, строения, сооружения),

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
				дополнительная информация, уточняющая (при необходимости) местоположение этих объектов относительно ориентиров на местности. Предоставляет выгрузки из БД в формате XML.
58 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			
59 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; Контроль за переданными субъектам полномочиями и оценка эффективности использования субвенций; Формирование данных по динамике изменений лесного фонда, не связанной с воздействием лесных пожаров			
60 Программный комплекс для автоматизации мониторинга подготовки теплогенерирующих	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-			

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
объектов к осенне-зимнему периоду "Энергосистема-Зима"	зимнему периоду в территориальных управлениях Ростехнадзора; Анализ и мониторинг состояния готовности субъектов к осенне-зимнему периоду в центральном аппарате Ростехнадзора			
61 Автоматизированная информационно-аналитическая система "Поиск" (ИАС-Поиск) Единой Системы авиационно-космического поиска и спасания	нформационная 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 в области авиационно-космического поиска и спасания; Проведение расчетов для анализа обеспеченности территории РФ средствами авиационно-космического поиска и спасания			
62 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 международных стандартов и рекомендуемой практики расследования аварий и инцидентов на море	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 международных 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			

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
(приказ Минтранса России от 14.05.2009 № 75)	принятия управленческих решений по вопросам предотвращения аварий и инцидентов			
63 Федеральное агентство водных ресурсов Информационная система "Оперативный дежурный"	позволяет получать оперативную информацию с территории России для своевременного принятия мер по 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			
64 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) плавания, иных плавучих	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 «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			

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
объектов, железнодорожного подвижного состава	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 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			
65 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			

Наименование системы и производитель	Назначение системы	Предложения по взаимодействию с АПК «БГ»		
		Исходящая информация (передает в АПК)	Входящая информация (получает из АПК БГ)	Формат взаимодействия
	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 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			

Приложение 4
Требования к вычислительной инфраструктуре и обеспечивающим прикладным подсистемам КСА «Региональная платформа»

Технические требования к подсистеме хранения данных:

—отсутствие единой точки отказа;

—обеспечение файлового доступа к данным по протоколам NFS и CIFS(SMB);

—поддержка пулов хранения данных;

—поддержка 10GBE или GBE (зависит от объема поступающей и хранимой информации) на каждом интерфейсном узле;

—возможность расширения системы без остановки обслуживания;

—поддержка жестких дисков 300ГБ, 2ТБ, 3ТБ, 4ТБ;

—поддержка SSD накопителей;

—использование уровней RAID6 и RAID60;

—использование центрально-распределённой топологии сети хранения данных;

—подсистема хранения данных должна поддерживать использование дисковых полок высокой плотности.

Требования к подсистеме резервного копирования:

—должна быть реализована поддержка резервного копирования и восстановления;

—должна быть обеспечена возможность подключения к продуктивным системам по сети 10GBE или GBE (зависит от нагрузки) и к устройству хранения резервных копий и архиву по интерфейсу FC 8Gb\s. Требования к подсистеме резервного копирования:

—должна быть реализована поддержка резервного копирования и восстановления;

—должна быть обеспечена возможность подключения к продуктивным системам по сети 10GBE или GBE (в зависимости от нагрузки) и к устройству хранения резервных копий, а также к архиву данных.

При построении вычислительной инфраструктуры допускается использование средств виртуализации и кластеризации.

Приложение 5
Требования к общему программному обеспечению КСА «Региональная платформа»

Общее программное обеспечение должно представлять собой совокупность программных средств со стандартными интерфейсами Российской Федерацией, предназначенных для организации и реализации информационно-вычислительных процессов в функциональном блоке «Региональная платформа». Состав общего программного обеспечения формируется при проектировании конфигурации программной технической документации интегрируемых информационных систем.

Общее программное обеспечение должно обеспечить:

—выполнение информационно-вычислительных процессов совместно с другими видами обеспечения;

—управление вычислительным процессом и вычислительными ресурсами с учетом приоритетов пользователей;

—коллективное использование технических, информационных и программных ресурсов;

—обмен неформализованной и формализованной информацией между информационными подсистемами, а также между КСА и пользователями КСА с протоколами информационно-логического взаимодействия;

—ведение учета и регистрации передаваемой и принимаемой информации;

—автоматизированный контроль и диагностику функционирования технических и программных средств, а также тестирование технических средств;

—создание и ведение баз данных с обеспечением контроля, целостности, сохранности, реорганизации, модификации и защиты данных от несанкционированного доступа;

—создание и ведение словарей, справочников, классификаторов и унифицированных форм документов, параллельный доступ пользователей к ним;

—поиск по запросам информации в диалоговом режиме и представление ее в виде документов;

—выполнение распределенных запросов к данным;

—синхронизацию корректировки данных и контроль за изменением документов в базах документов;

—разработку, отладку и выполнение программ, формирующих распределенные запросы к данным;

—формирование и ведение личных архивов пользователей;

—организацию решения функциональных задач специального программного обеспечения;

—наращивание состава общего программного, а также специального программного, информационного и лингвистического обеспечения;

—работу с электронными таблицами;

—многопользовательскую работу с цифровыми (электронными) картами;

—обработку (формирование, контроль, просмотр, распознавание, редактирование, выдачу на средства отображения и печати) текстовой, табличной, пространственной и мультимедийной информации;

—разграничение доступа пользователей к информации, защиту информации от несанкционированных действий пользователей, регистрацию и сигнализацию о несанкционированных действиях пользователей;

—реализацию системы приоритетов;

—восстановление работоспособности программного обеспечения и баз документов после сбоев и отказов технических и программных средств.

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

Общее программное обеспечение должно включать следующие основные компоненты:

—графические 32 (64 и более) - разрядные многозадачные (многопроцессорные) операционные системы;

—сетевые операционные системы;

—системы управления базами данных;

—телекоммуникационные программные средства, включая средства электронной почты;

—средства архивирования файлов;

—инструментальные средства для создания и ведения текстовых и графических документов, электронных таблиц и т.д.;

—средства поддержки Internet и Intranet -технологий;

—программные средства защиты от несанкционированного доступа к информационным и программным ресурсам;

—средства антивирусной защиты;

—средства управления выводом данных на устройства отображения информации группового и коллективного пользования;

—технологические программные средства.

Должно быть обеспечено ведение депозитария для всего программного обеспечения, а также создание дистрибутивов для любого компонента КСА функционального блока «Региональная платформа».

Поставляемое программное обеспечение, должно быть сертифицировано (в том числе по требованиям безопасности информации) или иметь соответствующие лицензии. Вопросы его использования и тиражирования должны регулироваться соответствующими соглашениями или сублицензионными договорами.

Приложение 6
Требования к специальному обеспечению КСА «Региональная платформа»

Разработка специального программного обеспечения должна быть в первую очередь направлена на реализацию функциональных подсистем КСА функционального блока «Региональная платформа».

При разработке задач специальное программное обеспечение должно быть обеспечено использование всех возможностей, предоставляемых средствами общего программного обеспечения (системными сервисами) по обработке данных.

Задачи специального программного обеспечения должны позволять проводить их оперативную адаптацию при изменении российского законодательства и их совершенствование при появлении новых требований пользователей в процессе эксплуатации.

Для обеспечения возможности наращивания функциональности специального программного обеспечения должна быть разработана нормативно-техническая документация, содержащая описания принятых в АПК «Безопасный город» протоколов и интерфейсов, выполнение которых позволит КСА функционального блока «Региональная платформа» нормально функционировать в операционной и информационной среде АПК «Безопасный город».

Для обеспечения принципов сохранения ранее вложенных инвестиций и соблюдения преемственности функциональной наполненности программно-технических комплексов КСА АПК «Безопасный город» создаваемое специальное программное обеспечение должно по возможности функционировать в среде текущего состояния общего программного обеспечения.

Специальное программное обеспечение должно быть спроектировано и реализовано таким образом, чтобы обеспечивались:

—кроссплатформенность - возможность работы как в среде операционных систем семейства Windows, так и операционных систем семейства LINUX;

—функциональная полнота - реализация всех функций КСА функционального блока «Координация работы служб и ведомств»;

—возможность адаптации и настройки программных средств с учетом специфики каждого объекта автоматизации;

—эргономичность - обеспечение удобства и унификации пользовательского интерфейса;

—защита от ошибочных действий оператора (пользователя);

—контроль и защита от некорректных исходных данных

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

Информационная совместимость КСА функционального блока «Региональная платформа» со смежными КСА должна обеспечиваться возможностью использования в них одних и тех же форматов данных и протоколов обмена данными между КСА.

Информационная совместимость КСА функционального блока «Региональная платформа» со смежными КСА реализуется в ходе электронного информационного взаимодействия (передачи данных) - неоднородных КСА функционального блока «Региональная платформа» между собой, между КСА АПК «Безопасный город», а также между КСА функционального блока «Региональная платформа» и региональными, федеральными КСА. Неоднородность может проявляться в использовании КСА различных стеков протоколов (специальных стандартов электронного взаимодействия - SPX/IPX, TCP/IP, ISO).

Регламентация КСА при электронном информационном

взаимодействии (передаче данных) со смежными разнородными информационными системами должна определяться:

—специальными стандартами - протоколами взаимодействия входящими в состав Единого стека открытых протоколов («Приложение Г»);

—типовым синтаксисом сообщений, именами элементов данных, операции управления и состояния;

—типовыми пользовательскими сервисами и межсистемными интерфейсами электронного информационного взаимодействия;

—типовыми процедурами электронного взаимодействия.

Протоколы взаимодействия должны представлять собой специальные стандарты, которые должны содержать наборы правил

взаимодействия функциональных блоков смежных систем на основе сетевой модели взаимодействия открытых систем.

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

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

Межсистемные интерфейсы должны реализовываться на базе международных стандартов на электронные документы, включая: стандарты UN/EDIFACT, разработанные Европейской Экономической Комиссией ООН (ЕЭК ООН) и принятые в качестве международных стандартов; стандарты ISO серии 8613 «Обработка информации. Текстовые и учрежденческие системы. Архитектура, ориентированная на обработку учрежденческих документов (ODA), и формат обмена»; стандарты ISO серии 10021 «Информационная технология. Передача текстов. Системы обмена текстами в режиме сообщений (MOTIS)»; стандарты SWIFT; стандарты TCP/IP, SGML и др. определения пути и IP; физической адресации; кабеля, сигналов, бинарной передачи.

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

Процедуры запрос-ответ должны быть реализованы на основе использования клиент-серверной архитектуры КСА функционального блока «Координация работы служб и ведомств».

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

Процедуры авторизации должны представлять собой процесс, а также результат процесса проверки установленных параметров пользователя (логин, пароль и другие) и предоставление ему или группе пользователей

определенных полномочий на выполнение действий, связанных с доступом к ресурсам КСА функционального блока «Региональная платформа». Должно обеспечиваться ведение журнала пользователя.

Процедуры индикации должны представлять собой процессы отображения результатов мониторинга управления обмена информацией в КСА функционального блока «Координация работы служб и ведомств» с применением обеспечивающих эти процессы программных и технических устройств отображения.

Приложении 8
Требования по применению систем управления базами данных КСА АПК «Безопасный город»

Используемые в КСА АПК «Безопасный город» система управления базами данными (СУБД) должна быть промышленного изготовления с необходимыми лицензиями.

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

СУБД в общем должна обеспечивать контроль, обновление (ввод и корректировку) и восстановление данных.

Общими требованиями к СУБД являются:

—поддержка реляционной или объектно-реляционной модели базы данных;

—поддержка международного стандарта ANSI SQL-92 и выше;

—наличие средств создания индексов и кластеров данных;

—автоматическое восстановление базы данных;

—совместимость серверов БД с различными операционными системами (семейства Windows и семейства LINUX);

—поддержка сетевых протоколов TCP/IP;

—возможность контроля доступа к данным;

—централизованное управление учетными записями пользователей; —оптимизация запросов.

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

Требования к структуре процесса сбора, обработки, передачи данных в КСА АПК «Безопасный город» и предоставлению данных должны быть реализованы в операциях:

—однократного ввода данных в КСА и многократного их использования при решении задач АПК «Безопасный город»;

—формирования, ведения, применения баз данных КСА АПК «Безопасный город»;

—настройки программного обеспечения;

—хранения, обновления информации о событиях;

—репликации информации по компонентам КСА АПК «Безопасный город»;

—обмена информацией в режиме импорта-экспорта в соответствии с регламентами информационного обмена, реализуемого прикладным программным обеспечением;

—обеспечения информационной совместимости КСА АПК «Безопасный город» с федеральными и региональными КСА.

Процессы сбора, обработки и передачи данных в КСА АПК «Безопасный город» должны определяться ведомственными нормативно - техническими документами и быть отражены в должностных инструкциях сотрудников подразделений - пользователей АПК «Безопасный город».

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

В КСА АПК «Безопасный город» должна быть обеспечена сохранность информации при авариях и сбоях в системе электропитания, отказов в работе серверного оборудования и сетевого оборудования.

В КСА АПК «Безопасный город» должны быть предусмотрены средства для резервного копирования информации. В состав эксплуатационной документации должен входить регламент, определяющий процедуры резервного копирования, восстановления данных и программного обеспечения.

КСА АПК «Безопасный город» должны включать следующие средства обеспечения сохранности информации:

—средства создания резервной копии базы данных;

—средства восстановления базы данных из резервной копии при возникновении событий, приведших к повреждению базы данных;

—резервные серверы (функционально дублирующие серверы);

—резервные АРМ управления;

—резервные коммутаторы;

—источники бесперебойного питания.

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

Обеспечение надежности хранения и восстановления данных должно осуществляться на основе:

—быстрого сброса cache памяти в случае отказа внешнего электропитания;

—использования глобальных дисков горячей замены;

—упреждающего резервирования дисков;

—изоляции диска в случае его сбоя;

—постоянной проверки целостности персональных данных о пассажирах в фоновом режиме;

—возможности переноса данных внутри системы без остановки приложений;

—использования технологии RAID, обеспечивающей защиту от одновременного выхода из строя двух дисков.

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

Данные КСА АПК «Безопасный город» должны храниться на дисках системы хранения данных (далее СХД).

СХД должна содержать следующие подсистемы и компоненты:

—устройства хранения (дисковые массивы);

—инфраструктуру доступа к устройствам хранения;

—подсистему резервного копирования и архивирования данных;

—программное обеспечение управления хранением;

—систему управления и мониторинга.

Имеющиеся в системе диски могут быть разбиты на группы и объединены в RAID.

Требования к системе хранения:

—управление СХД осуществляется через web-интерфейс и/или командную строку;

—должна иметь функции мониторинга и несколько вариантов оповещения администратора о неполадках;

—в СХД должно быть предусмотрено (по возможности) полное резервирование всех компонент - блоков питания, путей доступа, процессорных модулей, дисков, кэша и т.д.;

—должна обеспечивать доступность данных. (использование технологии RAID, создание полных и мгновенных копий данных внутри дисковой стойки, реплицирование данных на удаленную СХД и т.д.);

—должна предусматривать возможностью добавления (обновления) аппаратуры и программного обеспечения в горячем режиме без остановки комплекса;

—должна обеспечивать достаточную производительность для работы КСА АПК «Безопасный город»;

—должна обеспечивать масштабируемость;

—не должна иметь единой точки отказа;

—обеспечение файлового доступа к данным по протоколам NFS и CIFS(SMB);

—поддержка пулов хранения данных.

Возможность наращивания числа жёстких дисков, объёма кэш¬памяти, аппаратной модернизации и расширения функционала с помощью

специального программного обеспечения. Все перечисленные операции должны производиться без значительного переконфигурирования и потерь функциональности.

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

Требования к приданию юридической силы документам, продуцируемым техническими средствами КСА АПК «Безопасный город», должны соответствовать ГОСТ 6.10.4, в том числе:

—требованиям к составу и содержанию реквизитов, придающих юридическую силу документам на машинном носителе и машинограмме, создаваемой КСА АПК «Безопасный город»;

—требованиям к подлинникам, дубликатам, копиям документов на машинном носителе и машинограммам, полученным программными средствами КСА АПК «Безопасный город»;

—порядку внесения изменений в документ на машинном носителе и машинограмму.

При осуществлении информационного обмена документами на машинном носителе и машинограммами, юридическая сила документам должна обеспечиваться в соответствии с ГОСТ 6.10.4-84, только при наличии соответствующих решений ведомств участвующих в подобном информационном обмене (п. 1.3 ГОСТ 6.10.4-84).

Приложении 13
Требования к обеспечивающим системам

В состав функциональных подсистем КСА ЕЦОР должны входить следующие обеспечивающие подсистемы:

1. Подсистема обеспечения информационной безопасности.
2. Подсистема архивирования.
3. Подсистема резервирования.
4. Подсистема административного управления.
5. Подсистема хранения данных.
6. Подсистема электронного документооборота.
7. Требования к подсистеме обеспечения информационной безопасности

Подсистема обеспечения информационной безопасности реализуется организационными мерами, а также программно-техническими средствами и должна обеспечивать:

—управление доступом к информационным ресурсам КСА ЕЦОР;

—обеспечение безопасности передачи данных при межсетевом взаимодействии;

—регистрацию и учет работы пользователей;

—обеспечения целостности информации;

—антивирусную защиту;

—обнаружения вторжений;

—криптографическую защиту при передаче и хранении данных. Подсистема обеспечения информационной безопасности должна обеспечивать требуемый уровень защиты информации от внешних и внутренних угроз.

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

К объектам защиты КСА ЕЦОР относятся:

—технические средства;

—программные средства;

—информация (в любой форме ее представления), содержащая охраняемые сведения, в том числе регламенты и процедуры работы;

—помещения, предназначенные для обработки и хранения информации.

В КСА ЕЦОР должен обеспечивать возможность обработки конфиденциальной информации, относящейся к следующим типам:

—персональные данные;

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

—сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

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

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

присутствуют в составе локальной сети, не должны иметь доступ к компонентам ПОИБ.

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

Для организации информационного обмена с использованием каналов связи, выходящих за пределы контролируемой зоны, требуется использовать средства криптографической защиты информации, которые в установленном порядке прошли процедуру оценки соответствия требованиям безопасности информации ФСБ России. Криптографическая защита информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны, должна обеспечиваться с использованием криптографического алгоритма ГОСТ 28147-89. Используемые средства криптографической защиты информации должны обеспечивать криптографическую защиту по уровню не ниже КС2 (Приложение № 1 «Требования к средствам электронной подписи» к приказу ФСБ России от 27 декабря 2011 г. № 796).

В соответствии с Приказом ФСТЭК России от 28.02.2013 года №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах» для обеспечения безопасности персональных данных при их обработке в информационной системе (далее по тексту - ИСПДн) требуется использовать мероприятия по обеспечению безопасности персональных данных (далее по тексту - ПДн). Для реализации данных мероприятий необходимо создание, как минимум, следующих функциональных модулей:

—управления доступом;

—регистрации и учета;

—обеспечения целостности;

—обеспечения безопасного межсетевого взаимодействия;

—анализа защищенности;

—обнаружения вторжений;

—антивирусной защиты.

Функциональный модуль управления доступом Модуль управления доступом должен осуществлять идентификацию и проверку подлинности субъектов доступа при входе в КСА ЕЦОР по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

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

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

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

Функциональный модуль регистрации и учета

Должна осуществляться регистрация входа (выхода) субъектов доступа в КСА ЕЦОР (из КСА ЕЦОР).

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

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

—идентификатор субъекта доступа;

—спецификация защищаемого файла.

Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа:

терминалам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

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

Должен проводиться учет всех защищаемых носителей информации

с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

Учет защищаемых носителей должен проводиться в журнале

(картотеке) с регистрацией их выдачи (приема).

Функциональный модуль обеспечения целостности

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

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

Целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств

модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

Должна осуществляться физическая охрана технических средств (устройств и носителей информации), предусматривающая контроль

доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации, особенно в нерабочее время.

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

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

Функциональный модуль обеспечения безопасного межсетевого взаимодействия

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

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

России. Функциональный модуль обнаружения вторжений Данный модуль должен быть реализован путем использования в составе ИСПДн сертифицированных программных или программно¬аппаратных средств (систем) обнаружения вторжений.

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

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

II. Требования к подсистеме архивирования

Подсистема архивирования предназначена для консервации и восстановления информационных массивов КСА ЕЦОР и должна обеспечивать:

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

III. Требования к подсистеме резервирования

Подсистема резервирования должна обеспечивать дублирование критически важных элементов КСА ЕЦОР, выход из строя которых может привести к отказу КСА ЕЦОР.

IV. Требования к подсистеме административного управления Подсистема административного управления предназначена для

управления программно-техническим комплексом и информационным обеспечением КСА ЕЦОР и должна обеспечивать:

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

V. Требования к системе хранения данных

Данные КСА ЕЦОР должны храниться на дисках системы хранения данных (далее СХД).

СХД должна содержать следующие компоненты:

—устройства хранения (дисковые массивы);

—инфраструктуру доступа к устройствам хранения;

—подсистему резервного копирования и архивирования данных;

—программное обеспечение управления хранением;

—систему управления и мониторинга.

Имеющиеся в системе диски можно разбивать на группы и объединять в RAID.

Требования к системе хранения:

—управление СХД осуществляется через web-интерфейс и/или командную строку;

—должна иметь функции мониторинга и несколько вариантов оповещения администратора о неполадках;

—в СХД должно быть предусмотрено (по возможности) полное резервирование всех компонент - блоков питания, процессорных модулей, дисков и так далее;

—должна обеспечивать доступность данных (использование технологии RAID, реплицирование данных на удаленную СХД);

—должна предусматривать возможностью добавления (обновления) аппаратуры и программного обеспечения в горячем режиме без остановки комплекса;

—должна обеспечивать достаточную производительность для работы КСА ЕЦОР;

—должна обеспечивать масштабируемость;

—не должна иметь единой точки отказа;

—обеспечение файлового доступа к данным по протоколам NFS и CIFS(SMB);

—поддержка пулов хранения данных.

Возможность увеличения объема дискового массива без приостановки работы СХД, аппаратной модернизации и расширения функционала с помощью специального программного обеспечения. Все перечисленные операции должны производиться без значительного переконфигурирования и потерь функциональности.

VI. Требования к подсистеме электронного документооборота

Подсистема электронного документооборота предназначена для организации хранения электронных документов, а также работы с ними.

Подсистема электронного документооборота не должен иметь технических ограничений на число одновременно работающих пользователей.

Подсистема электронного документооборота должна основываться на отечественных разработках.

Подсистема электронного документооборота должна обладать следующими возможностями:

—обмен документами между подразделениями;

—отслеживание хода исполнения документов;

—добавление замечаний в документ и возврат документа на доработку;

—выдача заданий и сквозной контроль исполнения заданий;

—формирование консолидированных отчетов от подразделений;

—поиск документов;

—наличие мандатного и дискреционного принципов разграничения доступа для должностных лиц, с учетом штатного расписания;

—встроенные средства защиты от НСД, обеспечивающие возможность обработки информации, содержащей сведения, составляющие государственную тайну.

—гарантированное доведение и обработку документов и поручений; — идентификация и проверка подлинности субъекта доступа при входе в систему по паролю условно-постоянного действия;

—доступ к информации в соответствии с правами пользователя, назначаемыми администратором при регистрации пользователя в системе;

—аппаратного и программного масштабирования по мере увеличения нагрузки;

—функционального поэтапного расширения в рамках единой программно-аппаратной платформы;

—гибкой и эффективной системой настройки, позволяющей без корректировки исходных кодов программ осуществлять настройку параметров функциональных модулей при изменении управленческих, деловых процессов или организационной структуры и подразделений;

—регистрация всех действий субъектов доступа в подсистеме.

Встроенные средства защиты информации в подсистемы электронного документооборота должны обеспечивать:

—целостность (предотвращение возможности несанкционированных изменений электронных документов);

—конфиденциальность (разграничение прав доступа к электронным документам);

—аутентичность (подтверждение авторства электронных документов);

—юридическая значимость.

Юридическая значимость документов обеспечивается использованием сертифицированных средств криптографической защиты информации - электронной подписи.

Приложении 14
Требования к вычислительной инфраструктуре КСА ЕЦОР

Технические требования к подсистеме хранения данных:

—отсутствие единой точки отказа;

—обеспечение файлового доступа к данным по протоколам NFS и CIFS(SMB);

—поддержка пулов хранения данных;

—поддержка 10GBE или GBE (зависит от объема поступающей и хранимой информации) на каждом интерфейсном узле;

—возможность расширения системы без остановки обслуживания;

—поддержка жестких дисков 300ГБ, 2ТБ, 3ТБ, 4ТБ;

—поддержка SSD накопителей;

—использование уровней RAID6 и RAID60;

—использование центрально-распределённой топологии сети хранения данных;

—подсистема хранения данных должна поддерживать использование дисковых полок высокой плотности.

Требования к подсистеме резервного копирования:

—должна быть реализована поддержка резервного копирования и восстановления;

—должна быть обеспечена возможность подключения к продуктивным системам по сети 10GBE или GBE (зависит от нагрузки) и к устройству хранения резервных копий и архиву по интерфейсу FC 8Gb\s. Требования к подсистеме резервного копирования:

—должна быть реализована поддержка резервного копирования и восстановления;

—должна быть обеспечена возможность подключения к продуктивным системам по сети 10GBE или GBE (в зависимости от нагрузки) и к устройству хранения резервных копий, а также к архиву данных.

При построении вычислительной инфраструктуры допускается использование средств виртуализации и кластеризации.

Приложение 15
Требования к подсистемам КСА ЕЦОР

КСА ЕЦОР включает в себя следующие функциональные подсистемы:

1. Подсистема приема и обработки обращений.
2. Подсистема поддержки принятия решений.
3. Подсистема комплексного мониторинга.
4. Интернет - портал.
5. Подсистема обеспечения координации и взаимодействия.
6. Подсистема комплексного информирования и оповещения.
7. Подсистема интеграции данных.

1. Подсистема приема и обработки обращений

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

Подсистема должна обеспечивать следующие функции:

1) приём и обработка (регистрация и документирование) вызовов на единый телефонный номер, поступающих через операторов фиксированной и мобильной связи, в том числе:

а) автоматическое заполнение электронной карточки вызова данными, получаемыми от оператора связи (АОН, др. данные);

б) ручное (диспетчером, оператором) заполнение соответствующих полей электронной карточки;

2) дополнительный прием, регистрация, документирование вызовов поступающих посредством электронной почты, SMS, факс-сообщений, обращений через Интернет - портал, мобильных приложений, средств экстренной связи.

2. Подсистема поддержки принятия решений

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

Подсистема поддержки принятия решений должна обеспечивать выполнение следующих функций:

—моделирование распространения поражающих факторов аварий, природных катастроф и прогнозирование их воздействия на население и городскую инфраструктуру с динамической актуализацией результатов моделирования в зависимости от поступающих данных от КСА сегментов АПК БГ;

—автоматизация процесса принятия решений, в том числе использование типовых сценариев реагирования на основе утвержденных ведомственных регламентов при ликвидации кризисных ситуаций и происшествий;

—построение произвольных аналитических и статистических отчетов, в том числе:

а) сбор, обработку и представление информации о кризисных ситуациях и происшествиях, зарегистрированных в КСА ЕЦОР, в различной форме, в том числе и с применением средств деловой графики, и в различных разрезах (временном, территориальном);

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

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

г) отчеты по кризисным ситуациям и происшествиям (превышение пороговых значений, устанавливаемых в настройках подсистемы и т.п.);

д) сбор и хранение статистической информации.

3. Подсистема комплексного мониторинга

Подсистема комплексного мониторинга предназначена для сбора и обработки данных, поступающих от всех КСА входящих в состав АПК «Безопасный город» с целью предупреждения возникновения угроз (природного, техногенного, биолого-социального, экологического и другого характера) для всей среды обитания населения (жилых, общественных и административных зданий, объектов промышленного и сельскохозяйственного производства, транспорта, связи, радиовещания, телевидения, технических сооружений и систем коммунального хозяйства (водо-, газо-, тепло-, электроснабжения и др.), систем водоотведения, природных ресурсов и др.

Подсистема комплексного мониторинга должна предоставлять должностным лицам совокупную и полную информацию на основе данных, связанных с природными, техногенными угрозами и экологическими угрозами, полученных от существующих и перспективных КСА, входящих в состав, а также от взаимодействующих с АПК «Безопасный город».

Подсистема комплексного мониторинга должна иметь возможность представления информации, а также возможность автоматического информирования должностных лиц при получении данных о следующих КСП или ЧС:

—подтопления территории города;

—сейсмическая опасность, появление деформации земной поверхности в виде провалов и неравномерных оседаний земли;

—появление оползней;

—вероятность возникновения ураганов, штормового ветра, обильных снегопадов и затяжных дождей, обледенения дорог и токонесущих проводов;

—задымление вследствие массовых торфяных и лесных пожаров;

—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;

—просадки, оползни, обвалы земной поверхности из-за выработки недр при добыче полезных ископаемых и другой деятельности человека.

Подсистема комплексного мониторинга должна иметь возможность отображения информации о КСП или ЧС на электронной карте со следующими возможностями:

—место возникновения КСП или ЧС;

—отображение зон ответственности ДДС;

—для каждого ДДС отображение объектов учета и мониторинга, входящих в зону ответственности данного ДДС;

—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.

—отображение мест расположения источников первичной информации (оконечных устройств);

—расположение потенциально опасных и критически важных объектов, относящихся к зоне возможного влияния КСП или ЧС, с возможностью получения детализированной информации;

—информации о текущем местонахождении и перемещении сил и средств реагирования;

—характеристики территории;

— отображение картографических слоев многослойного цифрового плана города (здания, границы кварталов, зеленые массивы, водные объекты, железные дороги, мосты, улицы и т.д.) в произвольном масштабе с возможностью настройки параметров отображения (порядок отображения слоев, цвета и стили линий и заливок, шрифты надписей, использование условных знаков и т.д.);

—выполнение пространственных измерений;

—вычисление прямоугольных или географических координат объекта по его почтовому адресу и наоборот (поддержка геокодирования); —поиск объекта по его почтовому адресу, телефону, наименованию.

4. Интернет - портал

Интернет-портал предназначен для обеспечения информационного обмена с населением города и должен являться эффективным средством коммуникации в задачах предупреждения, устранения инцидентов и чрезвычайных ситуаций и минимизации их последствий.

Интернет портал должен предоставлять пользователям глобальной вычислительной сети Интернет следующие возможности:

—предоставлять актуальную информацию о событиях, напрямую или косвенно связанных с обеспечением безопасности жизнедеятельности и среды обитания, а так же о допустимых к общему доступу событиях и заявках с обозначением их статуса и с привязкой к местности (обозначением на электронной карте города);

—предоставлять пользователям глобальной вычислительной сети Интернет возможность информировать должностных лиц о событиях, связанных с обеспечением безопасности жизнедеятельности и среды обитания, с возможность присоединения мультимедийной информации.

—предоставлять пользователям глобальной вычислительной сети Интернет актуальную информацию о статусах исполнения обращений граждан с отображением на электронной карте города.

5. Подсистема обеспечения координации и взаимодействия Подсистема обеспечения координации и взаимодействия должна обеспечивать оперативное доведение информации и задач, в соответствии с регламентами взаимодействия, до органов повседневного управления. Подсистема обеспечения координации и взаимодействия должна, также обеспечивать контроль исполнения задач.

Взаимодействие между всеми КСА, участвующих в информационном обмене должно выполняться по правилам Единого стека открытых протоколов, требования к которому представлены в Приложении 1.

Подсистема обеспечения координации и взаимодействия должна обеспечивать следующее:

—организация межведомственного взаимодействия в работе служб оперативного/экстренного реагирования при реагировании на чрезвычайные ситуации;

—обеспечение возможности управления статусами событий 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.

6. Подсистема комплексного информирования и оповещения Подсистема комплексного информирования и оповещения

предназначена для информирования населения о событиях связанных с угрозами безопасности жизнедеятельности и среды обитания.

Подсистема комплексного информирования и оповещения должна обеспечивать оповещение и информирование граждан, по заранее подготовленным шаблонам и сценариям, посредством направления информационных сообщений, через Подсистему интеграции данных (по правилам Единого стека открытых протоколов), существующим и перспективным КСА, предназначенным для оповещения и информирования населения об угрозах общественной безопасности, правопорядка и безопасности среды обитания.

7. Подсистема интеграции данных

Подсистема интеграции данных КСА ЕЦОР должна обеспечивать надежный защищенный информационный обмен между КСА АПК «Безопасный город» по правилам Единого стека открытых протоколов взаимодействия (требования к Единому стеку протоколов представлены в Приложении 1).

Основными задачами подсистемы интеграции данных являются:

- интеграция разнородных КСА АПК «Безопасный город» с целью организации комплексного информационного взаимодействия, а также с целью обеспечения целостного процесса обработки информации;
- обеспечение информационного взаимодействия КСА ЕЦОР с КСА «Региональная интеграционная платформа»;
- обеспечение доступа для КСА АПК «Безопасный город» к необходимым ресурсам в соответствии с регламентами взаимодействия и предоставления информации.

С целью решения задачи интеграции разнородных КСА, в подсистему интеграции данных должны входить следующие модули:

—модуль ведения реестра КСА АПК «Безопасный город»;

—модуль маршрутизации.

Модуль ведения реестра КСА АПК «Безопасный город» должен обеспечивать следующие функции:

—ведение, хранение и резервное копирование информации о всех КСА, входящих в состав АПК «Безопасный город»;

—обеспечение целостности данных;

—обеспечение авторизованного доступа к данным;

—ведение журнала операций информационного обмена.

Модуль маршрутизации должен обеспечивать организацию

маршрутизации, ведение очередей и гарантированную доставку информации, передаваемой между всеми КСА АПК «Безопасный город», а также между КСА ЕЦОР и КСА «Региональная интеграционная платформа».

Приложение 16
Назначение КСА мониторинга общественного мнения

КСА мониторинга общественного мнения должен обеспечивать выполнение следующих возможностей:

—производить постоянный мониторинг общественного мнения, складывающегося на основании медийных событий, в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания, на основе публикаций пользователей в социальных сетях или стихийной активности рядовых интернет пользователей;

—производить анализ медиаполя в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания, с целью выявления фактов оказания целенаправленного негативного информационного воздействия на население через средства массовой информации и Интернет, а также уровня и характера социальной напряженности;

—выявлять негативные информационные сообщения, возникающие в медийном пространстве, с целью своевременного выявления и реагирования на угрозы общественной безопасности, правопорядка и безопасности среды обитания, в том числе провоцирование социальной, межнациональной, религиозной напряженности;

—производить сбор информации, появляющейся во всех значимых открытых источниках, и многоаспектную лингвистическую и статистическую обработку с целью выявления сообщений и событий, связанных с угрозами общественной безопасности, правопорядка и безопасностью среды обитания;

—осуществлять обработку собранной информации и максимально быстрое предоставление должностным лицам в удобной для анализа форме. В том числе в виде информационной новостной ленты, оперативных, регулярных и итоговых отчетов.

Для обеспечения возможности анализа медиаполя в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания, выявления сообщений об угрозах общественной безопасности, правопорядка и безопасности среды обитания, КСА должен обеспечивать многоаспектный статистический анализ и классификацию информационных сообщений по семантически значимым критериям, в том числе информационным объектам и характеру упоминания.

КСА должен обеспечивать возможность поиска и выявления первопричин и/или последствий событий, обнаруженных в социальных медиа, и информационных «волн» путем полнотекстового поиска по встроенному электронному архиву материалов СМИ и социальных сетей.

Приложение 17
Требования к подсистеме контроля и управления работой газовых котлов и оборудованием тепловых сетей

В основу работы подсистемы должен быть положен принцип локализации повреждений теплоцентрали за счет контроля увлажнения изоляции посредством модернизируемой системы оперативного дистанционного контроля. Для повышения эффективности и оперативности процесса сбора и обработки данных о повреждениях теплоцентралей терминалы должны быть оснащены сенсорными модулями с датчиками сопротивления. Модули должны устанавливаться в местах замыкания шлейфа для контрольных измерений для передачи информации о сопротивлении проводников.

Для проведения контроля и оповещения должностных лиц КСА ЕЦОР о неудовлетворительном техническом состоянии инженерного оборудования, сосредоточенного на объектах тепловых сетей, котельных, оборудование должно позволять дистанционно контролировать такие параметры как:

—несанкционированное открытие дверей котельных;

—загазованность котельных;

—остановка котлов;

—остановка сетевых насосов;

—отсутствие электропитания;

—давление теплоносителя на подаче и обрате;

—температура теплоносителя на подаче и обрате;

—расход теплоносителя.

Приложение 18
Требования к телекоммуникационной инфраструктуре

Телекоммуникационная инфраструктура (далее - ТИ) должна обеспечить надежный и безопасный обмен информацией между основными территориально разнесенными информационными системами АПК БГ и его сегментов.

ТИ должна развиваться и строиться в соответствии с действующим законодательством Российской Федерации, международными стандартами и соответствовать требованиям безопасности и надежности. Телекоммуникационное оборудование должно быть сертифицировано по требованиям безопасности и, предпочтительно, производиться на территории Российской Федерации.

Логическая схема и топология, а также технология построения каналов связи должны быть определены на этапе проектирования исходя из расчетов пропускной способности каналов, географии расположения коммутационных узлов и конечного оборудования.

ТИ должна обеспечивать поддержку возможности одновременной передачи данных, голоса и видеоданных.

В основу построения ТИ 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 системы в эксплуатацию без нарушения функционирования существующих элементов;

—возможность приоритетного использования существующих сетей передачи данных в целях обеспечения бюджетной экономии и сокращения сроков развертывания сегментов АПК БГ.

ТИ 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-потоки, управление и т.д.) и обеспечение динамического распределения полосы пропускания;

—использование резервных каналов связи в режиме балансирования нагрузки;

—оперативную локализацию сбоев в сетевом оборудовании и каналах связи.

Требования к производительности сети

Узлы сети (коммутаторы, маршрутизаторы и пр.) должны обеспечивать достаточную пропускную способность для обслуживания оконечных устройств сети.

Логическая схема и топология, а также технология построения магистральных каналов связи ТИ должны быть определены на этапе проектирования исходя из расчетов пропускной способности каналов, географии расположения коммутационных узлов и конечного оборудования.

Требование к производительности ТИ: архитектура ТИ,

используемые модели и компоненты активного сетевого оборудования должны соответствовать объемам передаваемого трафика сетевых приложений и сервисов АПК БГ.

При проектировании необходимо произвести расчет инфраструктуры компьютерной сети с параметрами качества, приведенными в таблице 2. Значения параметров в таблице 2 приводятся для примера и могут отличаться в разных муниципальных образованиях.

Таблица Ц.1 – Параметры качества телекоммуникационной инфраструктуры

Параметр	**Сервер1**	**Сервер2**	**Класс 0**	**Класс 1**	**Класс 2**
Пропускная способность	10Гбит/с	1Гбит/с	100Мбит/с Fast Ethernet	100Мбит/с Fast Ethernet	24/1,4 Мбит/с ADSL
Скорость передачи трафика	7Гбит/с	0,9Гбит/с	12 Мбит/с	4 Мбит/с	512 кбит/с
Задержка не более	25 мс	100мс	100 мс	100 мс	400 мс
Вариация задержки не более			50 мс	50 мс	-
Процент потерянных пакетов не более	0,0001	0,0001	0,001	0,001	0,001

класс 0 - применяется для работы пользователей, использующих насыщенные веб-интерфейсы с мультимедиа-компонентами, подготовку сложных отчетных форм, работу с пакетным экспортом/импортом файлов, потоковое видео H.264;

класс 1 - применяется для работы основной группы пользователей, без использования мультимедиа-компонент и сложных отчетных форм. Для данного класса гарантируется выполнение основных параметров быстродействия и времени отклика информационных систем;

класс 2 - применяется в резервном варианте, в случае технической невозможности организовать телекоммуникационный канал необходимого

качества. Соблюдение параметров быстродействия и времени отклика от информационных систем для данного класса не гарантируется.

сервер1 - сервера принимающих/передающих большие потоки информации (видеосервер, сервер обработки заявок).

сервер2 - сервера не требующие широкой полосы пропускания

Требования к надежности и безопасности Узлы сети должны обеспечивать высокую готовность (24/7). Для критически важных участков сети, требующих повышенной надежности, необходимо предусмотреть резервные каналы связи.

Для линий связи проходящих через общедоступные помещения и линий связи соединения с глобальной общедоступной сетью (Интернет) необходимо использовать системы шифрования трафика.

Подсистема защиты каналов передачи данных АПК БГ должна состоять из следующих функциональных подсистем:

—подсистемы защиты каналов связи внутри КСА АПК БГ;

—подсистемы криптографической защиты внешних каналов связи; — подсистемы централизованного управления средствами криптографической защиты внешних каналов связи.

Требование к расширяемости и масштабируемости Расширяемость

Сеть должна обеспечивать возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений, служб), наращивания длины сегментов сети и замены существующей аппаратуры более мощной. При этом принципиально

важно, что легкость расширения системы иногда может обеспечиваться в весьма ограниченных пределах.

Масштабируемость

Сеть должна позволять наращивать количество узлов и

протяженность линий связей, при этом производительность сети не должна ухудшаться. Для обеспечения масштабируемости сети должно

применяться дополнительное коммуникационное оборудование. Необходимо специальным образом структурировать сеть, чтобы иметь возможность включать большое количество оконечных устройств и при этом обеспечивать каждому пользователю сети необходимое качество обслуживания.

Требования к управляемости

Средства управления сетями должны осуществлять наблюдение, контроль и управление каждым элементом сети — от простейших до самых сложных устройств, при этом такая система рассматривает сеть как единое целое, а не как разрозненный набор отдельных устройств. Система должна обеспечивать возможность централизованно контролировать состояние основных элементов сети, выявлять и решать проблемы, возникающие при работе сети, выполнять анализ производительности и планировать развитие сети.

Требования к совместимости

Сеть может включать в себя разнообразное программное и аппаратное обеспечение, в ней могут сосуществовать различные операционные системы, поддерживающие разные коммуникационные протоколы, и работать аппаратные средства и приложения от разных производителей. Поэтому создание сети необходимо выполнять в соответствии с открытыми стандартами и спецификациями.

Требования к отказоустойчивости

ТИ должна обеспечивать 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 ТИ.

Требования к качеству обслуживания

Узлы сети должны поддерживать технологию QoS. Поскольку данные, которыми обмениваются два конечных узла, проходят через некоторое количество промежуточных сетевых устройств, таких как

концентраторы, коммутаторы и маршрутизаторы, то поддержка QoS требуется для всех сетевых элементов на пути следования трафика.

Приложение 19
Технические требования к системе видеонаблюдения

Система видеонаблюдения должна строиться с учетом результатов научно-исследовательских работ: «Выработка научно-технического и финансового обоснования для принятия решений по созданию информационной системы в интересах обеспечения охраны общественного порядка с учетом существующих федеральных программ» (шифр «Безопасный город», ГОСУДАРСТВЕННЫЙ КОНТРАКТ № 124- 2013/ИСОД от 23 октября 2013), «Выработка научно-технического и финансового обоснования для принятия решений по созданию системы обеспечения безопасности транспортной инфраструктуры с учетом существующих федеральных программ» (шифр «БТИ») проводимых в МВД России.

Определения:

Видеоидентификация (далее ВИ) - идентификация физических лиц и/или транспортных средств, являющихся объектами видеонаблюдения, на основании данных видеонаблюдения при их перемещении через заданные контрольные зоны.

Видеораспознавание - обнаружение и распознавание характера событий, связанных с объектами видеонаблюдения, на основании данных видеонаблюдения и их обнаружение в произвольном месте зоны видеонаблюдения и в произвольное время;

Видеообнаружение - обнаружение физических лиц и транспортных средств, являющихся объектами видеонаблюдения на основании данных видеонаблюдения, в произвольном месте зоны видеонаблюдения и в произвольное время;

Видеомониторинг - обнаружение физических лиц и транспортных средств, являющихся объектами видеонаблюдения, в заданном месте зоны видеонаблюдения и в заданное время.

Требования к архитектуре системы видеонаблюдения (далее СВН)

Архитектура СВН должна обеспечивать:

- взаимодействие подсистем и элементов на основе единого и открытого стандарта интерфейсов;
- возможность защищенного подключения внешних пользователей из подразделений ведомств МЧС России, ФСБ России, МВД России, ФСО России и других заинтересованных ведомств;
- масштабируемость по количеству оборудования, функциональности, объему хранимых данных;
- возможность модернизации отдельных компонентов СВН независимо от других;
- единую отчетность (журналирование событий в системе);
- централизованное администрирование и управление политикой разграничения доступа пользователей к информационным ресурсам СВН;
- централизованный мониторинг и управление состоянием системы.

Требования к составу и характеристикам СВН

1) В состав СВН могут входить следующие системы:

—видеоидентификация (далее ВИ);

—видеоаналитика (далее ВА);

—обзорное видеонаблюдение (ВН);

—система хранения (система архивирования);

—система взаимодействия с внешними информационными системами;

—телекоммуникационная система;

—АРМ операторов.

В состав СВН могут входить другие системы, обеспечивающие их функционирование.

Окончательный состав СВН определяется в соответствии с перечнем задач, решаемых СВН.

2) Требования к ВИ

В состав ВИ должны входить:

—видеокамеры;

—серверное оборудование;

—СПО.

Требования к видеокамерам

Видеокамеры в составе ВИ предназначены для регистрации лиц людей, движущихся в поле зрения видеокамер.

Технические характеристики видеокамер и объективов из состава ВИ определяются на этапе проектирования системы, исходя из условий регистрации и требований к качеству регистрируемого видеоизображения (Таблица Ш.1).

Таблица Ш.1 - Требования к видеоизображению, регистрируемому ВИ

	Параметр	Значение
	Разрешение регистрируемого	от 1.2 до 4 мегапикселей

Требования к серверному оборудованию

Серверное оборудование предназначено для приема и обработки видеопотока, регистрируемого видеокамерами из состава ВИ, с помощью устанавливаемого на него СПО и подразделяется на:

- серверы вычислений;
- серверы базы данных.

Количество и технические характеристики серверов вычислений определяются, исходя из следующих требований к производительности системы:

	Параметр	Значение
1	изображения	Выбирается таким образом, чтобы на изображении лица, расположенном фронтально относительно оптической оси камеры, зарегистрированном на рабочем расстоянии камеры, расстояние между центрами глаз составляло не менее 60 пикселей.
2	Глубина резко отображаемого пространства в зоне регистрации	1 м, не менее
3	Динамический диапазон интенсивности изображения в области лица	8 бит, не менее
4	Дисторсия	5 %, не более
5	Частота кадров при максимальном разрешении	16 кадров/с, не менее
6	Цветность	черно-белое

- загрузка процессоров не более 60% при одновременном выполнении всех функций системы;

- время, затрачиваемое системой на идентификацию лица, т. е. с момента обнаружения лица в кадре до отображения на АРМ оператора положительного результата идентификации, не должно превышать 3 секунд.

Количество и технические характеристики серверов баз данных определяются исходя из требований к базе данных (п. 3.2.5 настоящих требований).

Требования к СПО

СПО предназначено для детектирования и идентификации лиц людей в видеопотоке, зарегистрированном камерами из состава ВИ.

СПО должно иметь модульную архитектуру и включать в состав следующие программные модули:

- программный модуль детектирования лиц;

- программный модуль вычисления биометрических шаблонов;
- программный модуль сравнения шаблонов с эталонами, хранящимися в базе данных;
- интерфейс пользователя.

Программный модуль детектирования лиц предназначен для обнаружения и выделения изображений лиц людей в видеопотоке, регистрируемом камерами из состава ВИ.

Для каждой камеры модуль должен обеспечивать одновременное выделение не менее 4-х лиц в случае их нахождения в зоне регистрации.

Программный модуль вычисления биометрических шаблонов предназначен для формирования векторов признаков изображений лиц, выделенных модулем детектирования лиц.

Модуль вычисления биометрических шаблонов должен обеспечивать обработку данных, поступающих от модулей детектирования лиц.

Модуль вычисления биометрических шаблонов предназначен для формирования векторов признаков изображений лиц, выделенных модулем детектирования лиц.

Модуль сравнения шаблонов с эталонами, хранящимися в базе данных, должен обеспечивать сравнение векторов признаков изображений лиц, поступающих от модулей вычисления биометрических шаблонов, с векторами признаков изображений эталонных лиц, занесенных БД.

Интерфейс пользователя должен обеспечивать выполнение следующих функций с использованием АРМ:

- настройку и конфигурирование СПО;
- выборочный просмотр видеопотока, регистрируемого камерами из состава ВИ в режиме реального времени;
- вывод результатов работы СПО с отображением текущих результатов идентификации;

- вывод сигнальной информации оператору в случае положительного результата идентификации;
- просмотр и редактирование архива выделенных и идентифицированных лиц;
- просмотр и редактирование видеоархива;
- поиск лица в архиве видеозаписей по заданию оператора;
- актуализацию базы данных.

СПО должно предусматривать разграничение прав доступа к функциям системы для различных групп пользователей.

В СПО должна быть предусмотрена возможность изменения ранга идентификации (определение в соответствии с ГОСТ Р ИСО/МЭК 19795-1).

В состав СПО могут входить другие дополнительные модули, обеспечивающие функционирование ВИ.

Окончательный состав и конфигурация СПО ВИ определяется на этапе проектирования системы.

СПО должно обладать следующими эксплуатационными характеристиками:

- вероятность детектирования лица в видеопотоке - не менее 95%;
- вероятность истинно положительной идентификации человека - не менее 85% при вероятности ложноположительной идентификации не более 0,5%;

Указанные характеристики должны обеспечиваться при следующих условиях:

- стабильной освещенности области лица в зоне регистрации от 150 до 1000 лк;
- неравномерности освещенности области лица не более 50%;
- скорости движения людей до 5 км/ч;
- плотности потока людей не менее 1 чел./м2;

- ракурсах лица относительно фронтального: наклон и отклонение - не более 15°, поворот - не более 20°;

- объеме базы данных не менее 1000 лиц условно фронтального типа (в соответствии с ГОСТ Р ИСО/МЭК 19794-5).

В состав ВИ могут входить другие дополнительные технические средства, обеспечивающие размещение и функционирование ВИ.

Точный состав, конфигурация и технические характеристики оборудования в составе ВИ, не определенные настоящими требованиями, уточняются на этапе проектирования системы в зависимости от условий эксплуатации на конкретном объекте.

Требования к построению архитектуры системы

ВИ должна обладать открытой сетевой архитектурой с возможностью замены используемых программных и аппаратных модулей аналогичными по выполняемым функциям.

Архитектура ВИ должна быть масштабируемой по количеству камер регистрации, серверного оборудования, АРМ и используемых модулей СПО.

Архитектурой ВИ должно предусматриваться распределение вычислительных функций системы с выделением наиболее ресурсоемких операций в отдельные модули и централизация функций поиска лиц по базам данных учета и управления (рисунок Ш.1).

Рисунок Ш.1 - Пример построения архитектуры системы идентификации

Эффективное использование ресурсов ВИ должно быть обеспечено за счет равномерного распределения нагрузки между модулями, выполняющими одинаковые функции.

Требования к БД

БД в составе ВИ предназначена для хранения изображений лиц, относительно которых производится идентификация, их биометрических шаблонов и установочных данных.

Объем информации, хранимой в БД:

- объем изображения лица - не более 150 кб;

- объем биометрического шаблона - определяется в соответствии с характеристиками СПО;
- объем установочных данных - не более 10 кб;
- максимальное количество записей в БД - не менее 500 000.

Должно быть предусмотрено разделение лиц в БД по категориям. Должна быть обеспечена возможность удаленной актуализации БД. Требования к системе хранения

Должно быть обеспечено архивирование следующих результатов работы ВИ:

а) сжатого видеопотока от каждой из камер в составе ВИ:

- алгоритм сжатия - MJPEG, H.264;
- степень сжатия - не более 30%;
- частота - не менее 12 кадров/с;
- разрешение - не менее 1.2 мегапикселей;
- глубина архива - не менее 30 суток.

б) выделенных изображений лиц (с исходным разрешением, без потери качества):

- формат - *.png, *.jpg;
- объем - не более 150 кб;
- разрядность - 8 бит/пиксель;
- метаданные - дата, время, номер камеры, метка для поиска соответствующего видеофрагмента в архиве.
- максимальное количество записей - не менее 400 000;
- глубина архива - не менее 30 суток.

Примечание - допускается хранение более одного выделенного изображения лица каждого прошедшего человека.

в) изображений полных видеокадров, содержащих лицо, по которому была произведена идентификация (с исходным разрешением, без потери качества):

- формат - *.png, *.jpg;
- объем - не более 1200 кб;
- разрядность - 8 бит/пиксель;
- глубина архива - не менее 30 суток.

г) данных о результатах идентификации:

- дата, время, номер камеры;
- ссылка на изображения лиц в архиве;
- метка для поиска соответствующего видеофрагмента в архиве;
- идентификаторы записей в базе данных, относительно которых было принято решение об идентичности обнаруженного лица, и значения степени схожести (количество идентификаторов определяется значением ранга).

3) Требования к ВА

В состав ВА должны входить:

- видеокамеры;
- серверное оборудование;
- СПО видеоаналитики.

Требования к видеокамерам

Технические характеристики видеокамер и объективов из состава подсистемы определяются на этапе проектирования системы, исходя из условий регистрации и требований к качеству регистрируемого видеоизображения (Таблица Ш.2).

Таблица Ш.2 – Требования к качеству видеоизображения, регистрируемого камерами из состава _ подсистемы ВА

Параметр	Значение
Разрешение регистрируемого изображения	от 1.3 до 2 мегапикселей
Динамический диапазон интенсивности изображения	8 бит, не менее
Частота кадров при максимальном разрешении	25 кадров/с, не менее
Цветность изображения	Цветное
Дисторсия	15%, не более

Требования к серверному оборудованию

Серверное оборудование предназначено для приема и обработки видеопотока, регистрируемого видеокамерами, с помощью устанавливаемого на него СПО видеоаналитики.

Количество и технические характеристики серверного оборудования определяются, исходя из требований к производительности системы:

- загрузка процессоров не более 60% при одновременном выполнении всех функций системы;

- время, затрачиваемое системой на обнаружение тревожной ситуации, не должно превышать 5 секунд.

Требования к СПО видеоаналитики

СПО видеоаналитики предназначено для обнаружения и распознавания тревожных ситуаций в видеопотоке, зарегистрированном камерами из состава СВН .

СПО видеаналитики должно иметь модульную архитектуру.

СПО должно обеспечивать возможность конфигурирования задач видеоаналитики для каждой камеры или групп камер.

СПО видеоаналитики должно включать в состав следующие программные модули:

- программный модуль видеоаналитики;
- интерфейс пользователя.

Программный модуль видеоаналитики предназначен для обработки видеопотока и решения в режиме реального времени следующих задач видеоаналитики:

- обнаружение объекта (человека) в запрещенной зоне;
- обнаружение оставленного предмета и его владельца;
- выявление несанкционированного скопления людей;
- обнаружение драк, потасовок;
- обнаружение запрещенного или нетипичного движения (в том числе в пассажиропотоке);
- сервисный мониторинг и оценка работоспособности системы видеонаблюдения.

К задачам сервисного мониторинга относятся:

- потеря видеосигнала;
- затемнение изображения (в том числе отключение освещения);
- засветка изображения (в том числе поломка автоматической регулировки диафрагмы объектива);
- потеря контрастности (в том числе загрязнение объектива);
- изменение ориентации камеры (в том числе поворот камеры).

Интерфейс пользователя должен обеспечивать выполнение следующих функций с использованием АРМ:

- настройку и конфигурирование СПО видеоаналитики;
- выборочный просмотр видеопотока, регистрируемого камерами из состава СВН в режиме реального времени;
- вывод результатов работы СПО с отображением текущих результатов видеоанализа;

- вывод сигнальной информации оператору в случае обнаружения тревожной ситуации;
- просмотр и редактирование архива тревожных ситуаций;
- просмотр и редактирование видео архива;
- поиск события в архиве видеозаписей по заданию оператора: по дате и времени, типу тревожной ситуации.

СПО должно предусматривать разграничение прав доступа к функциям системы для различных групп пользователей.

В состав СПО видеоаналитики могут входить другие дополнительные модули, обеспечивающие функционирование ВА.

Окончательный состав и конфигурация СПО определяется на этапе проектирования системы.

СПО видеоаналитики должно обеспечивать следующие эксплуатационные характеристики:

- доля истинно положительных срабатываний от общего числа событий, которые требовалось обнаружить, - не менее 98%;
- доля истинно положительных срабатываний от общего числа срабатываний - не менее 98%.

Указанные характеристики должны обеспечиваться при следующих условиях регистрации:

- освещенность в зоне регистрации от 100 до 1000 лк;
- дистанция съемки от 5 до 30 м;
- плотность потока людей не более 1 чел/м .
- скорость движения людей не более 5 км/ч;
- объем оставленного предмета от 0,001 м .

В состав подсистемы могут входить другие дополнительные технические средства, обеспечивающие размещение и функционирование подсистемы ВА.

Точный состав, конфигурация и технические характеристики оборудования в составе подсистемы ВА, не определенные настоящими требованиями, уточняются на этапе проектирования системы в зависимости от условий эксплуатации на конкретном объекте.

Требования к построению архитектуры системы

Подсистема ВА должна обладать открытой сетевой архитектурой с возможностью замены используемых программных и аппаратных модулей аналогичными по выполняемым функциям.

Архитектура должна быть масштабируемой по количеству камер регистрации, серверного оборудования, АРМ и используемых модулей СПО.

Архитектурой должно предусматриваться распределение вычислительных функций системы и централизация функций управления.

Эффективное использование ресурсов должно быть обеспечено за счет равномерного распределения нагрузки между модулями, выполняющими одинаковые функции.

Требования к системе хранения

Должно быть обеспечено архивирование следующих результатов работы подсистемы ВА:

а) сжатого видепотока от каждой из камер:

- алгоритм сжатия - MJPEG, H.264;
- степень сжатия - не более 30%;
- частота - не менее 12 кадров/с;
- разрешение - не менее 1.2 мегапикселей;
- глубина архива - не менее 30 суток.

б) метаданные - дата, время, номер камеры, тип ситуации, метка для поиска соответствующего видеофрагмента в архиве.

4) Требования подсистеме ВН

В состав ВН должны входить:

- видеокамеры;
- серверное оборудование;
- СПО.

Требования к видеокамерам

В качестве передающей части должны использоваться цветные сетевые видеокамеры. Характеристики видеокамер определяются, исходя из требований к качеству регистрируемого видеоизображения (Таблица Ш.3):

Таблица Ш.3 –Требования к качеству видеоизображения, регистрируемого камерами из состава подсистемы ВН

№	Параметр	Значение
1.	Разрешение регистрируемого изображения	от 1.2 до 2 мегапикселей
2.	Динамический диапазон интенсивности изображения	8 бит, не менее
3.	Частота кадров при максимальном разрешении	25 кадров/с, не менее

Видеокамеры должны поддерживать открытые стандарты сетевого видео ONVIF версии не ниже 2.2, а также синхронизацию данных даты/времени регистрации с сигналами точного времени.

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

Требования к серверному оборудованию

Серверное оборудование предназначено для приема и обработки видеопотока, регистрируемого видеокамерами из состава ВН, с помощью устанавливаемого на него СПО.

Количество и технические характеристики серверного оборудования определяются, исходя из требований к производительности системы: загрузка

процессоров не более 60% при одновременном выполнении всех функций системы.

Требования к СПО

СПО предназначено для приема и обработки (кодирование, сжатие) видеопотока от камер из состава ВН и его отображения на АРМ оператора с использованием интерфейса пользователя.

Интерфейс пользователя должен обеспечивать выполнение следующих функций:

- настройку и конфигурирование СПО ВН;
- выборочный просмотр видеопотока, регистрируемого камерами из состава ВН в режиме реального времени;
- просмотр и редактирование видео архива;
- поиск события в архиве видеозаписей по заданию оператора: по дате и времени.

СПО должно предусматривать разграничение прав доступа к функциям системы для различных групп пользователей.

Требования к архивированию

Должно быть обеспечено архивирование сжатого видеопотока, регистрируемого видеокамерами из состава подсистемы ВН:

- алгоритм сжатия - MJPEG, H.264;
- степень сжатия - не более 40%;
- частота - не менее 12 кадров/с;
- разрешение - исходное;
- глубина архива - не менее 30 суток.

В состав подсистемы ВН могут входить другие дополнительные технические средства, обеспечивающие размещение и её функционирование. Точный состав, конфигурация и технические характеристики оборудования в составе ВН, не определенные настоящими требованиями, уточняются на этапе

проектирования системы в зависимости от условий эксплуатации на конкретном объекте.

5) Требования к системе хранения

Система хранения данных должна обеспечивать запись хранение и выдачу результатов работы составных частей СВН.

СА должна хранить другие данные о работе СВН, включая:

- сведения о действиях операторов СВН;
- сведения о сбоях работы оборудования и компонентов СВН, вне зависимости от природы сбоев.

СА должна обеспечивать:

- удаленный доступ к материалам архива через открытый интерфейс;
- удаленный поиск по материалам архива через открытый интерфейс по следующим критериям (тип события, интервал времени, место, номер камеры, изображение лица человека).
- экспорт видеоданных;
- мониторинг состояния оборудования и соединения с источниками видеоданных.

Состав и характеристики оборудования СА определяются на этапе проектирования системы.

6) Решения по общесистемному программному обеспечению компонентов СВН

Программное обеспечение серверного оборудования должно иметь возможность выполняться под операционными системами из семейства Windows или LINUX.

Программное обеспечение АРМ операторов должно выполняться под операционной системой Windows версии не ниже 7.

Функционирование БД должно обеспечиваться под управлением операционной системы, совместимой с СПО ВА.

Для обеспечения функционирования СВН могут использоваться дополнительные прикладные программы. При этом все используемое ПО должно быть лицензировано.

7) Требования к интерфейсам взаимодействия компонентов СВН

Взаимодействие систем в составе СВН должно осуществляться на основе открытых стандартов сетевого видео (ONVIF версии не ниже 2.0).

Видеокамеры и компоненты СВН должны взаимодействовать через открытые программные интерфейсы:

- ONVIF версии не ниже 2.2;
- GigE Vision версии не ниже 2.0;
- HD-SDI версии SMPTE 292M.

8) Требования к сети передачи данных для СВН

Сеть передачи данных должна обеспечивать пропускную способность (трафик) 10Мбит/с от каждой камеры видеонаблюдения до узла обработки и/или хранения видеоданных. Фактический трафик, который генерирует камера, чаще всего меньше 10Мбит/с и зависит от параметров видеопотока и динамики сцены видеонаблюдения. Например, для видеопотока параметрами, указанными в таблице 2, трафик составит около 9 Мбит/с для станции и 3,7 Мбит/с для школьного двора.

Таблица Ш.4 – Параметры видеопотока для расчета

Параметр	Значение (Станция)	Значение (школьный двор)
Разрешение основного видеопотока	720p(1280*720 пикселей)	720p(1280*720 пикселей)
Кодирование основного видеопотока	H.264	H.264
Частота кадров основного видеопотока	24 кадра в секундц	24 кадра в секундц

Параметр	Значение (Станция)	Значение (школьный двор)
Разрешение для записи событий	1080p(1920x1080 пикселей)	1080p(1920x1080 пикселей)
Кодирование для записи событий	MotionJPEG	MotionJPEG
Количество событий в минуту	10	10
Сжатие	Минимальное	Минимальное
Место наблюдения	«Станция» (высокая динамика)	«школьный двор»

Транспортная сеть должна обеспечивать:

—передачу пакетов данных по протоколу IP с неблокирующей коммутацией пакетов 2-го (Port-based VLAN, port mirroring, Link Aggregation, MSTP/RSTP, Broadcast storm suppression) и 3-го уровней(Protocol-based VLAN, RIPv2, OSPF, IS-IS, BGPv4, Routing policy, DHCP);

—достаточную пропускную способность для полнофункционального информационного обмена;

—групповое вещание: IGMP V1/2/3, IGMP snooping, PIM-DM/PIM- SM, MSDP/MBGP.

Таблица Ш.5 – Технические требования к камерам СВН по группам выполняемых задач.

Группа 1	Общая оценка обстановки. Дальность до 150м.	Разрешение не менее от 2 мегапикселей Частота кадров 15 кадров/с Алгоритм сжатия H.264
Группа 2	Классификация изменений: 1) людей (стоит, бежит, идет и пр.); 2) предметов (лежит, стоит, падает, оставлен); 3) транспорта (стоит, движется). 4) обнаружения объектов неопределенной формы и тревожных ситуаций (сигнальная линия, движение в зоне, остановка/праздношатание); 5) обнаружения скопления людей; 6) обнаружения пожара; 7) обнаружения драки. дальность	Разрешение 1,2-2 мегапикселей выбирается с учетом удаленности и расположения зоны наблюдения Частота кадров 24 кадров/с Алгоритм сжатия H.264
Группа 3	Распознавание: 1) людей (пол, рост, крупные детали одежды); 2) предметов (сумки, чемоданы и пр); 3) транспорта (вид и модель);	Разрешение не менее 1,3 мегапикселей выбирается с учетом удаальности и расположения зоны наблюдения Частота кадров от 24 кадров/с Алгоритм сжатия H.264
Группа 4	видеоидентификация: 1) распознавание лиц, деталей одежды; 2) предметов (сумки, чемоданы и пр); 3) детали, транспорта (вид, модель, детали);дальность около 8м.	от 1,2 до 4 мегапикселей (Выбирается таким образом, чтобы на изображении лица, расположенном фронтально относительно оптической оси камеры, зарегистрированном на рабочем расстоянии камеры, расстояние между центрами глаз составляло не менее 60 пикселей). Частота кадров от 24 кадров/с Алгоритм сжатия H.264, MJPEG

Приложение 20
Требования к источникам фото-видеофиксации

Данные от СИТС (таких как «АвтоУраган», «Поток», «Филин», «Стрелка», «КРИС», «АРЕНА», «КРЕЧЕТ», «КОРДОН» и других) должны передаваться в центр автоматизированной фиксации административных правонарушений (далее - ЦАФАП) для исполнения действий, предусмотренных Кодексом Российской Федерации об административных правонарушениях Российской Федерации, а также в узлы сбора данных. Данные о фактах фиксации формируются на СИТС и передаются потребителям посредством унифицированного протокола информационного обмена. Передача данных от СИТС через узлы интеграции позволяет исключить прямое сетевое взаимодействие с СИТС, что уменьшит нагрузку на каналы связи и дублирование информации.

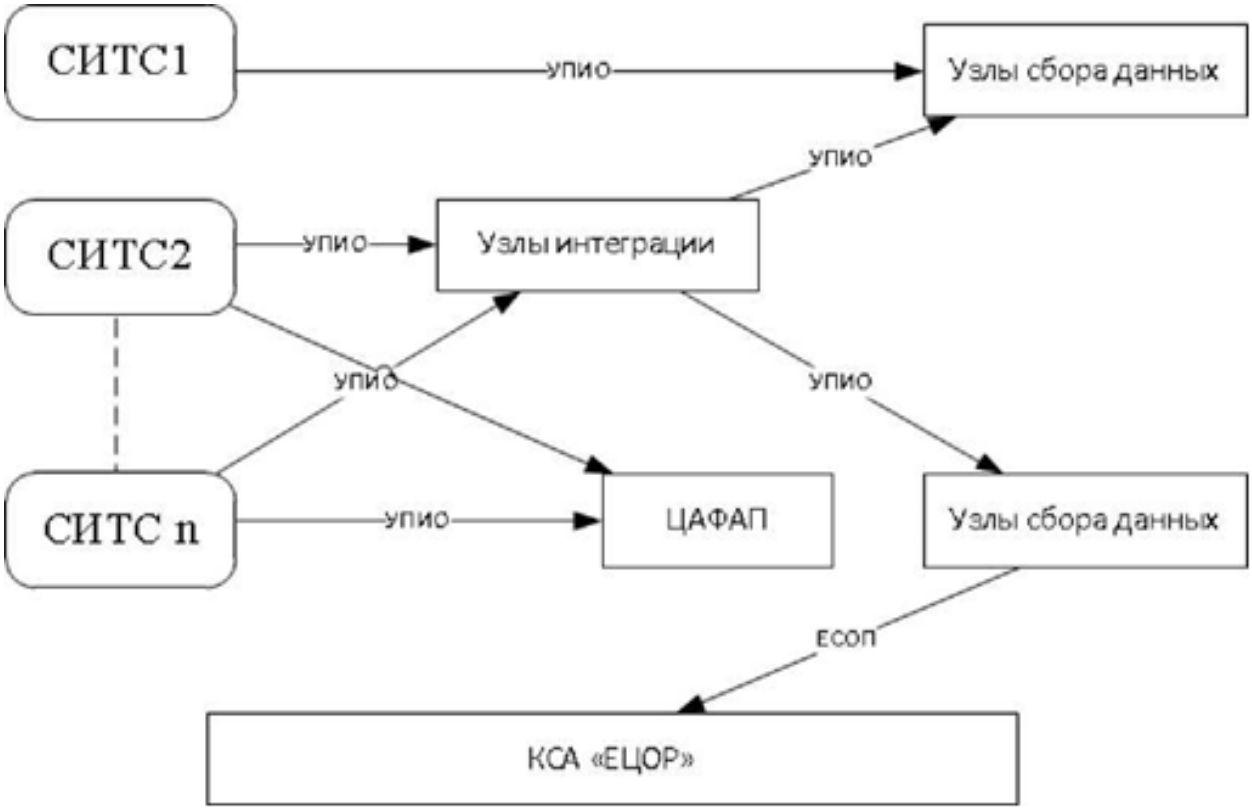


Рисунок 1. Схема передачи данных от СИТС в АПК БГ

При наличии технической возможности в узлы сбора данных передается максимальный объем информации, в частности государственные регистрационные знаки всех ТС, как нарушивших, так и не нарушивших правила дорожного движения, фотографию ТС, тип государственного регистрационного знака, дату и время фиксации.

Узлы сбора данных в свою очередь должны являться источниками данных для КСА ЕЦОР, предоставляя информацию в соответствии с требованиями Приложения 1 «Требования к Единому стеку открытых протоколов информационного взаимодействия КСА АПК «Безопасный город»».

Приложение 21
Требования к абонентским терминалам ГЛОНАСС-GPS/GSM и датчикам спутниковой навигации

Муниципальный легковой и грузовой автотранспорт должен быть оборудован трекерами ГЛОНАСС-GPS/GSM.

Требования к бортовому навигационно-связному оборудованию

Программное обеспечение бортового навигационно-связного оборудования (далее БНСТ) должно обеспечивать возможности обработки данных от внешних датчиков:

—двигатель - заведен/заглушён;

—данные от датчика уровня топлива в баке;

—данные от дополнительных датчиков.

Бортовое навигационно-связное оборудование (БНСТ) должно обеспечивать возможность интерактивного отображения основных параметров эксплуатации автотранспорта:

—общий пробег, пробег до технического осмотра;

—уровень топлива;

—количество моточасов;

—температура охлаждающей жидкости, масла, топлива;

—другие параметры эксплуатации.

Бортовое навигационно-связное оборудование должно состоять из следующих компонентов:

—модуля системы ГЛОНАСС/GPS или GPS с погрешностью определения координат подвижного объекта не более 30 метров;

—модуля GSM;

—антенны ГЛОНАСС/GPS и GSM;

—кабеля бортового блока;

—защитного алюминиевого корпуса;

—датчик вскрытия защитного корпуса;

—резервного аккумулятора;

—встроенного 3-х осевого акселерометра;

—модуля защиты аккумулятора от глубокого разряда.

Приложение 22
Требования к техническому обеспечению сегментов функционального блока «Экологическая безопасность»

К сегментам функционального блока «Экологическая безопасность» безопасности предъявляются следующие требования:

—автоматический сбор и обработка информации с пунктов контроля загрязнений;

—оперативная локализация аварийных ситуаций и инцидентов, связанных с загрязнением объектов (в том числе радиоактивными и химически опасными веществами, а так же нефтепродуктами, металлической ртутью и ее соединениями);

—оценить показатели состояния и функциональной целостности экосистем и среды обитания человека;

—выявление причин изменения показателей;

—оценка последствий изменений показателей;

—автоматизированное ведение архива первичных и обработанных данных;

—автоматизированное формирование отчетности.

КСА сегментов функционального блока «Экологическая безопасность» должен включать в свой состав следующие компоненты:

1. Пост атмосферного мониторинга.
2. Передвижная экологическая лаборатория контроля состояния атмосферного воздуха, воды и почвы.
3. Автоматизированный стационарный пост сейсмологического контроля.
4. Подсистема автоматического контроля промышленных выбросов.
5. Подсистема контроля утилизации отходов.

6. Автоматизированный гидрологический пост.

I. Пост атмосферного мониторинга

Пост атмосферного мониторинга должен обеспечивать выполнение следующих функций:

—определение загрязненности атмосферного воздуха - непрерывный автоматический контроль содержания в атмосферном воздухе загрязняющих веществ, взвешенных частиц (пыли);

—измерение метеорологических параметров: температуры,

относительной влажности, атмосферного давления, скорости и направления ветра, количества осадков и радиационного гамма-фона;

—измерение содержание в атмосферном воздухе веществ: окислов азота NO, NO2, NOx; аммиака КН3;углеводородов SCH, NCH, CH4, оксида углерода CO, диоксида серы SO2, сероводорода H2S, озона O3, диоксида углерода CO2.

II. Передвижная экологическая лаборатория контроля состояния атмосферного воздуха, воды и почвы

В состав передвижной экологической лаборатории контроля состояния атмосферного воздуха, воды и почвы должны входить:

—средства жизнеобеспечения;

—газоаналитический комплекс;

—метеорологический комплекс;

—система сбора, обработки и передачи данных;

—вспомогательное оборудование;

—средства экспресс-анализа воды и почвы;

—автомобиль - носитель;

—средства отбора проб воздуха, воды, донных отложений и почвы.

III. Автоматизированный стационарный пост сейсмологического контроля (АСПСК)

АСПСК должна быть оборудована приемником ГЛОНАСС/GPS. Допустимое расстояние выноса приемника ГЛОНАСС/GPS от станции до 150 м. Точность ведения времени не хуже 50 мкс. Исполнение (пылевлагозащищенность) IP65.

IV. Автоматическая система контроля промышленных выбросов (АСКПВ)

В состав АСКПВ должны входить: устройство пробоподготовки; устройство измерения расхода и температуры отходящих газов; блок измерения параметров; рабочая станция сбора, отображения и передачи данных.

V. Система контроля утилизации отходов (СКУО)

Должна предусматривать оборудование мусоровозов датчиками спутникового слежения ГЛОНАС/GPS, и оборудование камерами видеонаблюдения въезды городских свалок и/или мусороперерабатывающих предприятий.

VI. Требования к автоматизированному гидрологическому посту (АГП)

Применяемые измерительные приборы должны быть метрологически аттестованы на территории Российской Федерации и иметь сертификаты средств измерения и свидетельства о первичной поверки.

Для измерения уровня и температуры воды рекомендуется использовать гидростатический уровнемер со встроенным датчиком температуры, либо прибор, обладающий аналогичными характеристиками