УТВЕРЖДАЮ

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

В.А. Пучков

«29» 12 2014 г.

14-7-5552 от 29.12.2014

Временные единые требования к техническим параметрам сегментов аппаратно-программного комплекса «Безопасный город»

(Одобрены на заседании Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств «Безопасный город» под руководством Заместителя Председателя Правительства Российской Федерации Д.О. Рогозина 23.12.2014)

Содержание

Перечень принятых сокращений

АПК	–	Аппаратно-программный комплекс
АРМ	–	Автоматизированное рабочее место
АС	–	Автоматизированная система
АСУ	–	Автоматизированная система управления
АСУТП	–	Автоматизированная система управления технологическими процессами
АХОВ	–	Аварийно-химически опасные вещества
АЭС	–	Атомная электростанция
BI приложение	–	Бизнес-аналитика, программное обеспечение, созданное для помощи в анализе информации
БГ	–	Безопасный город
БНСТ	–	Бортовое навигационно-связное оборудование
ВОЛС	–	Выделенная оптоволоконная сеть
ГИС	–	Геоинформационная система
ДДС	–	Дежурная диспетчерская служба
ЕЦОР	–	Единый центр оперативного реагирования
ЕТС	–	Единая телекоммуникационная система
ЕДДС	–	Единая диспетчерская служба
ЖКХ	–	Жилищно-коммунальное хозяйство
ИАС	–	Интегрированная автоматизированная система
ИВК	–	Информационно-вычислительный комплекс
ИКТ	–	Информационно-коммуникационные технологии
КВО	–	Критически важные объекты
КСА	–	Комплекс средств автоматизации
КСА АС	–	Комплекс средств автоматизации автоматизированной системы
КСОБЖ	–	Комплексная система обеспечения безопасности жизнедеятельности
ЛВС	–	Локальная вычислительная сеть
МВК	–	Межведомственная комиссия
МЦС	–	Мультисервисная цифровая сеть
МО	–	Муниципальное образование
НПА	–	Нормативно-правовой акт
ОБДП	–	Обобщённая база данных происшествия
ОГВ	–	Органы государственной власти
ОУУ	–	Общедомовой узел учета

ОМС	–	Органы местного самоуправления
ОИВ	–	Органы исполнительной власти
ОС	–	Операционная система
ОЗУ	–	Оперативно запоминающее устройство
ПАМ	–	Пост атмосферного мониторинга
ПАК	–	Программно-аппаратный комплекс
ПО	–	Программное обеспечение
ПВР	–	Персональный аудио- видео регистратор
РСЧС	–	Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций
РФ	–	Российская Федерация
СОИБ	–	Система обеспечения информационной безопасности
СОП	–	Система обеспечения правопорядка и профилактики правонарушений на территории города
СИТС	–	Система идентификации транспортных средств
СПИД	–	Синдром приобретенного иммунодефицита
СППР	–	Система поддержки принятия решений
СС ТМК	–	Система сбора результатов технического мониторинга и контроля объектов транспортной инфраструктуры
ССЦ	–	Система ситуационных центров органов государственной и муниципальной власти
СЦ	–	Ситуационный центр
СУБД	–	Система управления базами данных
СХД	–	Сеть хранения данных
ТЗ	–	Техническое задание
ТИ	–	Телекоммуникационная инфраструктура
УСПД	–	Устройство сбора и передачи данных
ТС	–	Транспортное средство
УК	–	Управляющая компания
ФГИС ТП	–	Федеральная государственная информационная система территориального планирования
ФЗ	–	Федеральный закон
ФОИВ	–	Федеральный орган исполнительной власти
ФЦП	–	Федеральная целевая программа
ЦАФАП	–	Центр автоматизированной фиксации административных правонарушений
ЦОД	–	Центр обработки данных
ЦУКС	–	Центр управления в кризисных ситуациях

ЧС	–	Чрезвычайная ситуация
API	–	Набор готовых процедур, функций, классов и пр., предоставляемых приложением (сервисом) для использования во внешних программных продуктах
TLS	–	Криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети

Введение

Настоящий документ определяет единые технические требования к сегментам АПК «Безопасный город», детализирующие положения Концепции построения и развития АПК «Безопасный город» (утверждена Распоряжением Правительства Российской Федерации №2446-р от 3 декабря 2014 года) в части ее технической реализации.

Единые технические требования к сегментам АПК «Безопасный город» определяют типовой набор функциональных и технических требований к информационно-коммуникационной инфраструктуре и КСА сегментов АПК «Безопасный город» муниципального образования и являются основой для технических требований к сегментам АПК «Безопасный город», разрабатываемых муниципальными образованиями, с учетом своих социально-экономических особенностей, уровня развития городской, инженерной, транспортной и социальной инфраструктуры, информационно-коммуникационных технологий.

Под АПК «Безопасный город» понимается совокупность сопряженных между собой сегментов, объединяющих сгруппированные в соответствие с целевой областью применения КСА федеральных, региональных и муниципальных органов управления и организаций, на местном уровне решающих задачи обеспечения общественной безопасности, правопорядка и безопасности среды обитания.

В рамках реализуемых сегментов АПК «Безопасный город» предусматривается взаимодействие с КСА федеральных, региональных и муниципальных органов управления, а также организаций, в том числе коммерческих, в функции которых не входит непосредственное обеспечение общественной безопасности, правопорядка и безопасности среды обитания, однако информация КСА которых, может быть использована в целях эффективной реализации задач, предусмотренных Концепцией построения и развития АПК «Безопасный город».

Реализуемые в муниципальных образованиях сегменты АПК «Безопасный город» закладывают основу для решения задачи создания интегрированных региональных автоматизированных систем – комплексных систем обеспечения безопасности жизнедеятельности населения субъектов Российской Федерации.

Единые технические требования подлежат корректировке в соответствии с результатами опытной эксплуатации АПК «Безопасный город» в пилотных регионах.

1. Общие сведения

1.1 Полное наименование и условное обозначение

Аппаратно-программный комплекс технических средств «Безопасный город» (далее по тексту – АПК «Безопасный город»).

Краткое наименование: АПК БГ.

1.2 Перечень документов, на основании которых создается АПК «Безопасный город»

Концепция построения и развития аппаратно-программного комплекса «Безопасный город», утвержденная распоряжением Правительства Российской Федерации №2446-р от 03 декабря 2014 года;

Постановление Правительства РФ от 08.09.2010 N 697 (ред. от 19.03.2014) «О единой системе межведомственного электронного взаимодействия»;

Постановление Правительства Российской Федерации от 25 августа 2008 года № 641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS»;

Указ Президента Российской Федерации от 28 декабря 2010 года № 1632 «О совершенствовании системы обеспечения вызова экстренных оперативных служб на территории Российской Федерации»;

ГОСТ Р 51558-2008. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний;

ГОСТ Р 54830-2011. «Системы охранные телевизионные. Компрессия оцифрованных видеоданных. Общие технические требования и методы оценки алгоритмов»;

ГОСТ 12.1.006-84 «Система стандартов безопасности труда. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля»;

ГОСТ 12.1.003-83 «Система стандартов безопасности труда. Шум. Общие требования безопасности»;

ГОСТ Р ИСО 13849-1-2003 «Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования»;

ГОСТ 34.003-90 «Автоматизированные системы. Термины и определения»;

ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы»;

Федеральный закон от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»;

Федеральный закон от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности»;

Федеральный закон от 10.07.2012 № 117-ФЗ «О внесении изменений в Технический регламент о требованиях пожарной безопасности»;

СП 5.13130.2009. «Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования»;

РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств»;

Распоряжения Правительства №2299-р от 17 декабря 2010 года «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения (2011-2015 годы)»;

Федеральный закон Российской Федерации от 21 июля 2014 г. N 209-ФЗ "О государственной информационной системе жилищно-коммунального хозяйства"

Научно-исследовательская работа «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»);

Научно-исследовательская работа «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;

Постановление Правительства Российской Федерации от 20 января 2014 г. № 39 «О Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств «Безопасный город»».

2. Назначение и цели создания АПК «Безопасный город»

2.1 Назначение АПК «Безопасный город»

АПК «Безопасный город» предназначен для решения комплексных задач обеспечения общественной безопасности, правопорядка и безопасности среды обитания на муниципальном, региональном и федеральном уровнях.

2.2 Цели и задачи АПК «Безопасный город»

Целью построения и развития АПК «Безопасный город» является повышение общего уровня общественной безопасности, правопорядка и безопасности среды обитания за счет существенного улучшения координации деятельности сил и служб, ответственных за решение этих задач, путем внедрения на базе муниципальных образований (в соответствии с едиными функциональными и технологическими стандартами) комплексной информационной системы, обеспечивающей мониторинг, прогнозирование, предупреждение и ликвидацию возможных угроз, а также контроль устранения последствий чрезвычайных ситуаций и правонарушений с интеграцией под ее управлением действий информационно-управляющих подсистем дежурных, диспетчерских, муниципальных служб для их оперативного взаимодействия в интересах муниципального образования.

Основными задачами построения и развития АПК «Безопасный город» являются:

1) формирование информационно-коммуникационной платформы для органов местного самоуправления с целью устранения рисков обеспечения безопасности среды обитания, общественной безопасности и правопорядка на базе межведомственного взаимодействия;

2) разработка единых функциональных и технических требований к аппаратно-программным средствам, ориентированным на идентификацию потенциальных точек уязвимости, прогнозирование, реагирование и предупреждение угроз обеспечения безопасности муниципального образования;

3) обеспечение информационного обмена между участниками всех действующих программ соответствующих федеральных органов исполнительной власти в области обеспечения безопасности через единое

информационное пространство с учетом разграничения прав доступа к информации разного характера;

4) обеспечение информационного обмена на федеральном, региональном и муниципальном уровне через единое информационное пространство с учетом разграничения прав доступа к информации разного характера;

5) создание дополнительных инструментов на базе муниципальных образований для оптимизации работы существующей системы мониторинга состояния общественной безопасности;

6) построение и развитие систем ситуационного анализа причин дестабилизации обстановки и прогнозирования существующих и потенциальных угроз для обеспечения безопасности населения муниципального образования.

3. Общие требования к сегментам АПК «Безопасный город»

3.1 Требования к структуре и функционированию

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

АПК «Безопасный город» строится по модульному принципу, с использованием, как уже функционирующих, так и перспективных КСА и существующей инфраструктуры, с учетом положений настоящих Единых технических требований к сегментам АПК «Безопасный город».

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

Базовым уровнем построения и развития комплекса «Безопасный город» является муниципальное образование, которое является центром сбора и обработки информации с целью принятия оперативных решений по всем вопросам обеспечения общественной безопасности и безопасности среды обитания в рамках муниципального образования или межмуниципального объединения.

Построение АПК «Безопасный город» на муниципальном уровне осуществляется на интеграционной платформе, обеспечивающей сопряжение между всеми КСА АПК «Безопасный город» (существующими и перспективными) на базе Единого стека открытых протоколов, общие требования к которому приведены в Приложение 1 «Требования к Единому стеку открытых протоколов информационного взаимодействия КСА АПК «Безопасный город».

Муниципальная интеграционная платформа обеспечивает возможность сквозной передачи и обработки информации, целостность и согласованность потоков информации и процедур в рамках межведомственного взаимодействия с учетом ограничений прав доступа согласно регламентирующим документам соответствующих ведомств.

На региональном уровне информация из муниципальных образований консолидируется на базе региональной информационно-коммуникационной платформы, обеспечивающей органам исполнительной власти субъектов Российской Федерации контроль над оперативной

обстановкой в регионе, координацию межведомственного взаимодействия на региональном уровне, оперативное управления службами и ведомствами в случае региональных чрезвычайных ситуаций и в критических ситуациях.

На федеральном уровне соответствующие федеральные органы исполнительной власти имеют полный доступ ко всей информации, находящейся в общей информационной среде АПК «Безопасный город», и имеют возможность пользоваться ею в полном объеме соответственно правам доступа, установленным соответствующими регламентами.

Построение АПК «Безопасный город» осуществляется с учетом уже выполняемых и финансируемых федеральных программ, направленных на создание и развитие информационной инфраструктуры в части обеспечения безопасности, взаимодействие с КСА которой обеспечивается в рамках единой информационной среды на базе единого стека открытых протоколов взаимодействия КСА АПК «Безопасный город».

В состав сегментов АПК «Безопасный город» должны входить следующие КСА (структурная схема АПК «Безопасный город» приведена в Приложении 2):

На муниципальном уровне

КСА ЕЦОР (с муниципальной интеграционной платформой в его составе);

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

КСА взаимодействующих с АПК «Безопасный город» территориальных органов ФОИВ;

КСА АС региональных органов исполнительной власти в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

КСА взаимодействующих с АПК «Безопасный город» региональных органов исполнительной власти;

КСА органов местного самоуправления в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

КСА взаимодействующих с АПК «Безопасный город» АС органов местного самоуправления;

КСА взаимодействующих с АПК «Безопасный город» коммерческих организаций, в том числе обеспечивающих безопасность критически важных, потенциально опасных и социально значимых объектов.

На региональном уровне

— КСА «Региональная интеграционная платформа».

3.2 Требования к надежности

Надежность АПК «Безопасный город» определяется надежностью сегментов АПК «Безопасный город». Надежность сегментов АПК «Безопасный город» определяется надежностью КСА АПК «Безопасный город».

3.2.1 Состав и количественные значения показателей надежности

Для всех КСА, входящих в состав АПК «Безопасный город» должны быть обеспечены следующие уровни надежности:

— уровень сохранения работоспособности;

— уровень сохранности информации.

Показатели надежности должны обеспечивать возможность выполнения функциональных задач комплексами средств автоматизации АПК «Безопасный город».

Показатели надежности включают:

— среднее время между выходом из строя отдельных компонентов КСА, входящих в состав АПК «Безопасный город»;

— среднее время на обслуживание, ремонт или замену вышедшего из строя компонента;

— среднее время на восстановление работоспособности КСА АПК «Безопасный город».

Показатели надежности КСА АПК «Безопасный город» должны достигаться комплексом организационно-технических мер обеспечивающих доступность ресурсов, их управляемость и обслуживаемость.

Технические меры по обеспечению надежности должны предусматривать:

— резервирование критически важных компонентов КСА АПК «Безопасный город» и данных, а также отсутствие единой точки отказа;

— использование технических средств с избыточными компонентами и возможностью их горячей замены;

— конфигурирование используемых средств и применение специализированного программного обеспечения, обеспечивающего высокую доступность.

Организационные меры по обеспечению надежности должны быть направлены на минимизацию в работе КСА АПК «Безопасный город», а также персонала службы эксплуатации при проведении работ по обслуживанию комплекса технических средств КСА АПК «Безопасный город», минимизацию времени ремонта или замены вышедших из строя компонентов за счет:

— регламентации проведения работ и процедур по обслуживанию и восстановлению системы;

— своевременного оповещения должностных лиц о случаях нештатной работы компонентов КСА АПК «Безопасный город»;

— своевременной диагностики неисправностей;

— наличия договоров на сервисное обслуживание и поддержку компонентов комплекса технических средств КСА АПК «Безопасный город».

Должны быть обеспечены следующие значения показателей надежности:

— КСА АПК «Безопасный город» должны быть рассчитаны на круглосуточную работу;

— срок службы КСА АПК «Безопасный город» в целом должен составлять не менее 3 лет;

— наработка КСА АПК «Безопасный город» на отказ должна составлять не менее 5000 часов;

— наработка КСА АПК «Безопасный город» на сбой должна составлять не менее 2500 часов.

Иные количественные значения показателей надежности должны быть учтены в процессе проектирования для каждого компонента КСА АПК «Безопасный город».

Сохранение работоспособности должно обеспечиваться при возникновении локальных отказов компонентов КСА АПК «Безопасный город»:

— отказ оборудования;

— сбой серверной, клиентской операционных систем;

— сбой СУБД в процессе выполнения пользовательских задач;

— отказ каналов связи;

— импульсные помехи, сбои или прекращение электропитания.

При нарушении или выходе из строя внешних каналов связи КСА АПК «Безопасный город» должны переходить на резервный канал, а в случае его отсутствия работать в автономном режиме, подразумевающим выполнение тех функций, которые предусматривают использование периодического обмена информацией.

Сбои или выход из строя одного накопителя на жестком магнитном диске не должны приводить к приостановке работы, т.к. в КСА АПК «Безопасный город» должно быть предусмотрено резервирование дисков.

Должна быть обеспечена возможность «горячей» замены сбойного или вышедшего из строя накопителя на жестком магнитном диске без остановки функционирования КСА АПК «Безопасный город».

Импульсные помехи, сбои или прекращение электропитания не должны приводить к выходу из строя технических средств и/или нарушению целостности данных.

Прекращение электропитания на короткое время не должно приводить к прекращению функционирования КСА АПК «Безопасный город».

Должны быть предусмотрены средства оповещения должностных лиц о нештатной работе КСА АПК «Безопасный город».

3.2.2 Требования к надежности технических средств и программного обеспечения

Надежность сегментов АПК «Безопасный город» в части технического обеспечения должна обеспечиваться:

— наличием в КСА АПК «Безопасный город» технических средств повышенной отказоустойчивости и их структурным резервированием;

— защитой технических средств по электропитанию путем использования источников бесперебойного питания;

— выбором топологии локальной сети, обеспечивающей вариантность маршрутизации потоков информации;

— реализацией, в составе инженерных систем, средств автоматического обнаружения и локализации неисправных блоков и технических средств на безагентной основе;

— должны использоваться средства мониторинга и оповещения об аварийных ситуациях.

— автоматическим оповещением администраторов системы по нештатным ситуациям, как по средствам электронной почты, так и посредством SMS-информирования.

3.3 Требования безопасности

Программное обеспечение КСА АПК «Безопасный город» должно быть проверено на отсутствие известных уязвимостей к атакам на отказ и на несанкционированный доступ.

Требования к межсетевым экранам должны соответствовать Руководящему документу Государственной технической комиссии при Президенте Российской Федерации «Межсетевые экраны. Защита от несанкционированного доступа к информации. Классификация межсетевых экранов и требования по защите информации».

КСА АПК «Безопасный город» должны быть обеспечены средствами антивирусной защиты для обеспечения надежного контроля над потенциальными источниками проникновения компьютерных вирусов.

КСА, входящие в состав АПК «Безопасный город» должны обладать подсистемой информационной безопасности от несанкционированного доступа (далее НСД), которая должна удовлетворять Руководящим Документам ФСТЭК России, а также ГОСТ Р50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования». КСА АПК «Безопасный город» должны соответствовать требованиям класса защищенности «1Г» и выше в зависимости от обрабатываемых данных и решаемых задач.

В ходе проектирования КСА АПК «Безопасный город» должен быть определен состав информации и методов ее обработки, подлежащий защите, а также разработана модель угроз и модель нарушителя.

Техническое задание на создание подсистемы информационной безопасности от НСД для каждого КСА, входящего в состав АПК «Безопасный город» должно предусматривать:

— требования по защите от несанкционированного доступа;

— требования к средствам криптографической защиты;

— требования к средствам обнаружения и предупреждения атак, а также к средствам межсетевого экранирования и шлюзам;

— требования к средствам антивирусной защиты;

— требования по защите персональной информации;

— требования порядку аттестации АПК «Безопасный город».

Технические средства должны быть надежно заземлены в соответствии с действующими правилами и требованиями фирм-изготовителей оборудования.

Все программное и аппаратное обеспечение, реализующее функционал защиты информации, должно быть сертифицировано в системе сертификации ФСТЭК России.

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

Электропитание технических средств должно соответствовать III категории «Правил устройств электроустановок».

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

Требования и нормы проектирования охранно-тревожной сигнализации должны соответствовать документу РД 78.36.003-2002.

Требования и нормы проектирования и установки пожарной сигнализации должны соответствовать документу РД СП 5.13130.2009.

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

3.4 Требования к эргономике и технической эстетике

Графический интерфейс КСА АПК «Безопасный город» должен отвечать следующим требованиям:

— отображение на экране преимущественно необходимой для решения текущей прикладной задачи информации;

— максимальная унификация процедур реализации аналогичных функций в различных компонентах КСА АПК «Безопасный город»;

— использование функциональных и «горячих» клавиш, при этом на экране должна находиться подсказка о назначении таких клавиш;

— отображение на экране хода длительных процессов обработки.

Процедуры ввода данных должны отвечать следующим требованиям:

— пользователь должен иметь возможность гибко контролировать ввод данных: просматривать введенные данные на мониторе, производить их корректировку или отказаться от ввода;

— при вводе должны использоваться справочники для контроля вводимых данных и списки допустимых значений;

— обеспечение возможности ввода значений по умолчанию.

Интерфейс должен обеспечивать корректную обработку ситуаций, вызванных неверными действиями, неверным форматом или недопустимыми значениями входных данных. В указанных случаях должны выдаваться соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

3.5 Требования к эксплуатации, техническому обслуживанию и ремонту

Эксплуатация КСА АПК «Безопасный город» должна производиться в соответствии с эксплуатационной документацией и Регламентом технического обслуживания. Регламент технического обслуживания должен быть определен в составе эксплуатационной документации.

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

Технические средства и персонал должны размещаться в существующих помещениях объектов автоматизации, которые по климатическим условиям должны соответствовать ГОСТ 15150-69. Размещение технических средств и организация автоматизированных рабочих мест должно быть выполнено в соответствии с требованиями (СНиП) ГОСТ 21958-76.

3.6 Требования по сохранности информации при авариях

Сохранность информации в КСА, входящих в состав АПК «Безопасный город» должна обеспечиваться при следующих аварийных ситуациях:

— импульсные помехи, сбои и перерывы в электропитании;
— нарушение или выход из строя каналов связи;
— сбой общего программного обеспечения;
— сбой специального программного обеспечения;
— выход из строя аппаратных средств системы (серверы и АРМ);
— ошибки в работе персонала.

Эксплуатация КСА АПК «Безопасный город» должна производиться в соответствии с эксплуатационной документацией и Регламентом технического обслуживания.

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

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

Должно быть предусмотрено текущее ежедневное техническое обслуживание КСА АПК «Безопасный город». При возникновении неисправностей, должно осуществляться оперативное техническое обслуживание, временные регламенты которого не должны превышать указанных значений времени восстановления.

Регламент технического обслуживания должен быть определен в составе эксплуатационной документации.

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

3.7 Требования к защите от влияния внешних воздействий

Технические средства КСА АПК «Безопасный город» должны отвечать требованиям ГОСТ 19542-83, ГОСТ 29339-92, ГОСТ Р50628-2000, требованиям Госкомсвязи России «Автоматизированные системы управления аппаратурой электросвязи» 1998г. по электромагнитной совместимости и помехозащищенности.

Технические средства должны удовлетворять требованиям по электромагнитной совместимости, определенным в ГОСТ 22505-97 и ГОСТ Р51275-2006.

3.8 Требования к патентной чистоте

Проектные решения КСА АПК «Безопасный город» должны отвечать требованиям по патентной чистоте согласно действующему законодательству Российской Федерации.

При поставке КСА АПК «Безопасный город» должны быть выполнены требования Федерального закона Российской Федерации от 23.09.92 г. № 3523-I «О правовой охране программ для электронных вычислительных машин и баз данных».

3.9 Требования по стандартизации и унификации

Программная реализация необходимого протокола или протоколов Единого стека открытых протоколов в КСА АПК «Безопасный город», планируемых к внедрению, должны проходить проверку на соответствие требованиям наиболее поздней версии Единого стека открытых протоколов (см. Приложение 1) по методике, утвержденной федеральным органом исполнительной власти – координатором АПК «Безопасный город».

Программная документация на КСА АПК «Безопасный город», планируемых к внедрению, должна проходить проверку на соответствие настоящим требованиям по методике, утвержденной федеральным органом исполнительной власти – координатором АПК «Безопасный город».

Процесс разработки КСА АПК «Безопасный город» должен соответствовать требованиям к созданию АС, регламентированных стандартами:

— ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

— ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

— ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

КСА АПК «Безопасный город» должны быть разработаны в соответствии с требованиями национальных стандартов (ГОСТ), Единой системы конструкторской документации, Единой системы программной документации, а также требованиями нормативно-методических и руководящих документов ФСТЭК России и ФСБ России.

Разработка программных средств должна учитывать требования к реализации программного обеспечения на основе отечественных и (или) открытых технологий, с учетом требований Распоряжения Правительства №2299-р от 17 декабря 2010 года «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения (2011-2015 годы)».

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

4. Требования к КСА функционального блока «Координация работы служб и ведомств»

4.1 Состав КСА функционального блока «Координация работы служб и ведомств»

Функциональный блок «Координация работы служб и ведомств» состоит из следующих КСА:

1) Единого центра оперативного реагирования (ЕЦОР), в составе следующих подсистем:

а) подсистемы приема и обработки обращений.

б) подсистемы поддержки принятия решений.

в) подсистемы комплексного мониторинга.

г) интернет – портала.

д) подсистемы обеспечения координации и взаимодействия.

е) подсистемы комплексного информирования и оповещения.

ж) подсистемы интеграции данных.

2) «Региональная интеграционная платформа», в составе:

а) модуля ведения реестра КСА (федеральных и региональных КСА в сфере обеспечения общественной безопасности, правопорядка и безопасности среды, взаимодействующих с ними федеральными и региональными КСА и КСА ЕЦОР всех муниципальных образований, входящих в состав региона);

б) модуля управления данными.

4.2 Назначение и функциональность КСА функционального блока «Координация работы служб и ведомств»

4.2.1 Назначение и функциональность КСА ЕЦОР

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

Функции КСА ЕЦОР должны обеспечивать:

1) централизованный мониторинг угроз общественной безопасности, правопорядка и безопасности среды обитания, а именно:

а) прием и регистрацию сообщений об угрозах, общественной безопасности, правопорядка и безопасности среды обитания по доступным в муниципальном образовании каналам связи, включая телефонную связь, интернет, средства экстренной связи;

б) комплексный мониторинг угроз общественной безопасности, правопорядка и безопасности среды обитания посредством агрегации данных, полученных от всех КСА АПК «Безопасный город» (существующих и перспективных) по Единому стеку открытых протоколов;

в) возможность подключения и управления периферийными устройствами КСА сегментов АПК «Безопасный город» посредством единого стека отрытых протоколов в соответствие с определенными регламентами доступа;

2) поддержку принятия решений, а именно:

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

б) автоматическое предоставление вариантов сценария реагирования по заранее подготовленным шаблонам в соответствии с установленными регламентами взаимодействия;

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

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

3) управление и координацию взаимодействия, а именно:

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

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

в) обеспечение оперативного информирования о статусе события и поручения служб оперативного реагирования и муниципальных служб, отвечающих за проведение работы над инцидентом

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

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

е) управление поручениями и контроль исполнения поручений;

ж) обеспечение отображения на электронной карте полной информации о событии, включая просмотр изменения статусов события и выданных поручений.

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

а) комплексное оповещение населения муниципального образования об угрозах безопасности, правопорядка и безопасности среды обитания с использованием средств информирования и связи, интегрированным с КСА ЕЦОР в том числе: громкоговорителей, информационных табло, смс-рассылок, мобильных приложений, электронной почты, радио и телевидения, интернет-портала и иных средств информирования;

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

5) формирование единого информационного пространства, а именно:

а) обеспечение интеграции и информационного взаимодействия между КСА сегментов «Безопасный город» на базе муниципальной и региональной интеграционных платформ,

б) организация единого информационного-справочного пространства АПК «Безопасный город»

в) обеспечение защищенного доступа к информации с использованием средств криптографической защиты информации;

г) автоматическое архивирование и обеспечение хранения видео-информации и отчетной информации о событиях и всей сопутствующей информации;

д) формирование отчетных форм для муниципальных органов власти, бизнеса с гибким механизмом настройки и расширения возможностей, позволяющим формировать шаблон отчетных форм и отчеты за любой период времени;

е) обеспечение возможности формирования сводных отчетов по нескольким аналитическим измерениям;

ж) обеспечение качественного обмена информацией о результатах непрерывного мониторинга услуг связи и измерения эксплуатационных показателей сети, оперативное уведомление о нарушениях связи между объектами инфраструктуры или об отклонении ее качества от требуемого уровня.

Подробные требования к КСА ЕЦОР представлены в Приложении 3 и Приложении 4.

4.2.2 Назначение и функциональность КСА «Региональная интеграционная платформа»

КСА «Региональная интеграционная платформа» предназначен для обеспечения органов исполнительной власти субъектов Российской Федерации оперативной и достоверной информации о ситуации в регионе, координации межведомственного взаимодействия на региональном уровне, обеспечения оперативной информационной поддержки служб и ведомств в случае возникновения региональных чрезвычайных ситуаций и в критических ситуациях.

Основными функциями КСА «Региональная интеграционная платформа» являются:

1) агрегация информации от всех КСА ЕЦОР, муниципальные образования которых, входят в регион;

2) агрегация информации от КСА федеральных и региональных органов исполнительной власти в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания, а также КСА федеральных и региональных органов исполнительной власти, взаимодействующих с АПК «Безопасный город» на региональном уровне;

3) сопряжение КСА АПК «Безопасный город» (через КСА ЕЦОР) всех муниципальных образований, входящих в регион с КСА федеральных и региональных органов исполнительной власти в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания, а также КСА федеральных и региональных органов исполнительной власти, взаимодействующих с АПК «Безопасный город» на региональном уровне;

4) предоставление органам исполнительной власти субъекта Российской Федерации отчетно-аналитического инструмента мониторинга в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания в регионе в целом и отдельно взятом муниципальном образовании в частности;

5) предоставление различных аналитических срезов информации по муниципальным образованиям (совокупно или по отдельности в рамках аналитического среза) на основе объединенных в рамках единого информационного пространства данных о регионе;

6) обеспечение доступа для федеральных и региональных КСА к необходимым информационным ресурсам КСА сегментов АПК

«Безопасный город» заданного муниципального образования, в соответствии с регламентами взаимодействия и предоставления информации;

Модуль ведения реестра внешних КСА АПК «Безопасный город» КСА «Региональная интеграционная платформа» должен обеспечивать следующие функции:

1) ведение, хранение и резервное копирование информации о федеральных и региональных КСА;

2) ведение, хранение и резервное копирование информации о всех КСА ЕЦОР, входящих в регион;

3) обеспечение целостности данных;

4) обеспечение авторизованного доступа к данным по установленным регламентам доступа и взаимодействия;

5) ведение журнала операций информационного обмена.

Модуль управления данными КСА «Региональная интеграционная платформа» должен обеспечивать:

1) организацию маршрутизации, ведение очередей и гарантированную доставку информации, передаваемой между КСА федеральных и региональных органов исполнительной власти и КСА ЕЦОР всех АПК «Безопасный город», входящих в регион.

2) агрегацию структурированной и обработанной информации, полученной от всех КСА ЕЦОР, входящих в регион;

3) агрегацию информации, полученной от федеральных и региональных КСА;

4) формирование базы мета-данных по интегрированным в единую информационную среду КСА сегментов АПК «Безопасный город» и КСА федеральных и региональных органов исполнительной власти.

4.3 Требования к внутреннему и внешнему взаимодействию КСА функционального блока «Координация работы служб и ведомств»

Смежными КСА по отношению к АПК «Безопасный город» должны являться региональные и федеральные КСА, за исключением КСА «Региональная интеграционная платформа».

Информационное сопряжение КСА АПК «Безопасный город» со смежными КСА должно осуществляться через КСА «Региональная

интеграционная платформа» по правилам Единого стека открытых протоколов.

КСА «Региональная интеграционная платформа» должен обеспечивать информационное сопряжение КСА АПК «Безопасный город» через КСА ЕЦОР всех муниципальных образований, входящих в состав региона и федеральными и региональными КСА, по Единому стеку открытых протоколов.

КСА «Региональная интеграционная платформа» должен обеспечивать возможность информационного взаимодействия со смежными КСА по распространенным технологиям, таких как RPC или SOAP.

Внутреннее информационное взаимодействие (сопряжение) КСА АПК «Безопасный город» должно быть реализовано через КСА ЕЦОР.

В рамках КСА ЕЦОР должна быть реализована поддержка всех протоколов Единого стека открытых протоколов. В остальных КСА АПК «Безопасный город» должна быть реализована поддержка соответствующих им протоколов Единого стека открытых протоколов.

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

4.4.1 Общие технические требования к техническому обеспечению КСА функционального блока «Координация работы служб и ведомств»

Техническое обеспечение КСА функционального блока «Координации работы служб и ведомств» должно отвечать следующим требованиям:

— базироваться на сертифицированных образцах средств вычислительной техники, средств коммуникационной техники, средств организационной техники;

— обладать информационной, программной и технической совместимостью, адаптируемостью к условиям функционирования, возможностью расширения с целью подключения новых устройств;

— обеспечивать устойчивую управляемость, надежное хранение информации, оперативность ее обработки, а также резервное копирование и восстановление информации;

— электронно-вычислительная техника должна соответствовать или превышать требования технических спецификаций по производительности.

Выбор технических средств КСА функционального блока «Координация работы служб и ведомств» должен строиться на основе ориентации на отечественный рынок, использования совокупности научно обоснованных оценочных критериев, состав которых предопределен функциональностью и структурой КСА функционального блока «Координация работы служб и ведомств».

Исходными данными для выбора технических средств являются:

— характеристики функциональных задач КСА ЕЦОР;

— характеристики функциональных задач КСА «Региональная интеграционная платформа»;

— характеристики задач обеспечения информационной безопасности КСА функционального блока «Координация работы служб и ведомств»;

— заявленные производителем технические характеристики оборудования.

4.4.2 Требования к техническому обеспечению КСА ЕЦОР

Средства вычислительной техники должны быть максимально приспособлены для последующей модернизации.

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

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

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

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

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

Подробные требования к техническому обеспечению КСА ЕЦОР представлены в Приложении 3 (Требования к вычислительной инфраструктуре КСА ЕЦОР) и Приложении 4 (Требования к подсистемам КСА ЕЦОР).

4.4.3 Требования к техническому обеспечению КСА «Региональная интеграционная платформа»

Телекоммуникационная инфраструктура (далее – ТИ) должна обеспечить надежный и безопасный обмен информацией между всеми КСА ЕЦОР Субъекта.

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.

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;

— 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.

Подробные требования к техническому обеспечению КСА «Региональная платформа» представлены в Приложении 5 (Требования к вычислительной инфраструктуре и обеспечивающим прикладным подсистемам КСА «Региональная интеграционная платформа»).

4.5 Требования к программному обеспечению КСА функционального блока «Координация работы служб и ведомств»

Программное обеспечение КСА функционального блока «Координация работы служб и ведомств» представляет совокупность

общего программного обеспечения и специального программного обеспечения.

Программное обеспечение КСА функционального блока «Координация работы служб и ведомств» должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в состав перспективных КСА АПК «Безопасный город».

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

Требования к общему программному обеспечению КСА функционального блока «Координации работы служб и ведомств» представлены в Приложении 6 (Требования к общему программному обеспечению функционального блока «Координация работы служб и ведомств»).

Требования к специальному обеспечению КСА функционального блока «Координация работы служб и ведомств» представлены в Приложении 7 (Требования к специальному программному обеспечению КСА «Координация работы служб и ведомств»).

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

4.6 Требования к информационному обеспечению КСА «Координация работы служб и ведомств»

Информационное обеспечение - это совокупность форм документов, классификаторов, нормативной базы (компоненты информационного обеспечения) и реализованных решений по объемам, размещению и формам существования информации, применяемой при функционировании КСА функционального блока «Координация работы служб и ведомств».

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

Единая система кодирования и классификации информации должна обеспечивать:

– централизованное ведение словарей и классификаторов, использующихся в информационном взаимодействии;

– выполнение необходимых технологических функций, в том числе предоставление возможности обмена данными со смежными по отношению к КСА функционального блока «Координация и взаимодействие служб и ведомств».

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

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

Приложение 8 - Требования к информационной совместимости КСА функционального блока «Координация работы служб и ведомств» со смежными КСА;

Приложение 9 - Требования по применению систем управления базами данных КСА АПК «Безопасный город»;

Приложение 10 - Требования к структуре процесса сбора, обработки, передачи данных в АПК «Безопасный город»;

Приложение 11 - Требования к защите данных от разрушений при авариях и сбоях в электропитании КСА АПК «Безопасный город»;

Приложение 12 - Требования к контролю, хранению, обновлению и восстановлению данных КСА АПК «Безопасный город»;

Приложение 13 - Требования к процедуре придания юридической силы документам, продуцируемым техническими средствами КСА АПК «Безопасный город».

Программное обеспечение должно быть сертифицировано по требованиям информационной безопасности.

5. Требования к КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»

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

КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры» состоит из следующих сегментов:

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

а) управления видеопотоками;

б) мониторинг и видеоанализ предупреждения и профилактики правонарушений;

в) оценки качества деятельности представителей территориальных органов федеральных органов исполнительной власти, ответственных за обеспечение общественной безопасности, правопорядка и безопасности среды обитания;

г) позиционирования и управление мобильным персоналом.

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

а) мониторинга критически важных, потенциально опасных и социально значимых объектов;

б) позиционирования и управления мобильными подразделениями сил РСЧС, привлекаемыми к ликвидации ЧС и пожаров, в том числе, пожарно-спасательными и пожарными подразделениями;

в) поддержки принятия решений по предупреждению и ликвидации ЧС природного и техногенного характера, снижению рисков возникновения ЧС и пожаров;

г) информирования и оповещения населения.

3. Сегмента обеспечения безопасности инфраструктуры жилищно-коммунального комплекса в составе КСА следующих подсистем:

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

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

в) предупреждения и ликвидации чрезвычайных ситуаций, возникающих при нарушении правил пожарной безопасности;

г) обеспечения безопасности охраняемых объектов, придомовых территорий и объектов социального назначения;

д) обеспечения экстренной связи;

е) информирования и оповещения населения;

ж) моделирования предпосылок и оценка последствий чрезвычайных ситуаций.

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

а) ведения дежурного плана города;

б) поддержки принятия решений при управлении муниципальными активами;

в) обеспечения социальной безопасности;

г) земельный муниципальный реестр;

д) реестр электросетей;

е) реестр сетей и сооружений водоснабжения;

ж) реестр тепловых сетей;

з) реестр дорог;

и) реестр телекоммуникаций;

к) социальный реестр;

л) реестр мест обработки и утилизации отходов;

м) реестр природоохранных и рекреационных зон и паркового хозяйства.

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

5.2.1 Назначение и функциональность сегмента «Обеспечения правопорядка и профилактики правонарушений»

Сегмент «Обеспечения правопорядка и профилактики правонарушений на территории муниципального образования» предназначен для решения комплекса задач обеспечения общественной безопасности и правопорядка посредством своевременной идентификации и реагирования на потенциальные угрозы общественной безопасности и нарушений правопорядка.

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

1) осуществление видеонаблюдения и видеоанализа, в том числе:

— получение видеоизображения с мест установки видеокамер на критически важных, потенциально опасных и социально значимых объектах (в том числе дошкольные образовательные учреждения, образовательные учреждения и другие);

— отображение, получаемого с камер видеонаблюдения, видеоизображения в режиме реального времени на АРМ должностных лиц;

— возможность управления поворотными камерами видеонаблюдения из интерфейса АРМ должностных лиц;

— запись видеопотоков, получаемых с камер видеонаблюдения;

— хранение записанных видеоданных с возможностью быстрого поиска по заданному интервалу времени всех видеоданных связанных с зафиксированным правонарушением;

— отображение мнемоник видеокамер на электронной карте с возможностью просмотра получаемого видеопотока путем выбора видеокамеры из интерфейса АРМ;

— идентификации и распознавания лиц и сопоставление их с данными о лицах находящихся в розыске.

— обнаружение скопления людей, в том числе в несанкционированных местах;

— оценка плотности потока людей на значимых для муниципального образования объектах;

— выявление фактов движения человека против направления потока;

— выявление фактов движения человека с высокой скоростью (бегущий человек);

— выявление фактов оставленных предметов;

— выявление фактов повышенной активности людей в контролируемой зоне;

— выявление исчезнувших предметов;

— появление человека или автомобиля в зоне наблюдения (улицы, площади, перекрестки, парки);

— построение предполагаемых маршрутов движения транспортного средства на основе видеоданных данных полученных от различных видеокамер, на видеопотока которых был идентифицирован государственный номер транспортного средства.

— обеспечение распределенной структуры видеосерверов, объединяющих камеры видеонаблюдения в группы;

— обеспечения доступа к видеоданным по событиям зафиксированным средствами видеообнаружения, видеоидентификации и видеораспознавания.

2) позиционирование подвижных объектов, в том числе:

— построение оптимальных маршрутов передвижения с учетом данных о фактической загруженности дорог и отображением на электронной карте;

3) обеспечение функций информирования и получения отзывов от населения о работе представителей территориальных органов федеральных органов исполнительной власти, ответственных за обеспечение общественной безопасности, правопорядка и безопасности среды обитания, в том числе:

— накапливать статистическую информацию об обращениях населения, связанных с угрозами общественной безопасности, правопорядка и безопасности среды обитания на территории муниципального образования, в том числе поступающих через КСА ЕЦОР, а также о статусах их исполнения;

— предоставлять населению возможность оценивать качество деятельности представителей территориальных органов федеральных органов исполнительной власти, ответственных за обеспечение общественной безопасности, правопорядка и безопасности среды обитания

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

— подготавливать сводные аналитические отчеты на основе накопленных статистических данных;

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

— информировать население, посредством Интернет портала, а также посредством мобильных приложений о качестве деятельности представителей территориальных органов федеральных органов исполнительной власти, ответственных за обеспечение общественной безопасности, правопорядка и безопасности среды обитания;

— обеспечивать выявление фактов целенаправленного негативного информационного воздействия на население через средства массовой информации и Интернет (Приложение 20);

— обеспечивать выявление фактов провоцирования социальной, межнациональной, религиозной напряженности через деятельность отдельных (в том числе электронных) средств массовой информации (СМИ) (Приложение 20).

5.2.2 Назначение и функциональность сегмента «Обеспечения защиты от чрезвычайных ситуаций природного и техногенного характера и пожаров»

Сегмент «Обеспечения защиты от чрезвычайных ситуаций природного и техногенного характера и пожаров» предназначен для пожарного и аварийного мониторинга критически важных, потенциально опасных и социально значимых объектов, мониторинга возможных угроз на потенциально опасных территориях окружающей природной среды, оценки сложившейся или прогнозируемой обстановки, поддержки принятия решений по предупреждению и ликвидации ЧС, управлению рисками возникновения пожаров, техногенных аварий, катастроф и стихийных бедствий, а также доведения принятых решений до органов управления, сил РСЧС и населения.

Сегмент «Обеспечения защиты от чрезвычайных ситуаций природного и техногенного характера и пожаров» во взаимодействии с КСА функционального блока «Координация работы служб и ведомств» должен обеспечить выполнение следующих функций:

1) сбор, обработка и анализ информации об угрозах и фактах пожаров, техногенных аварий и катастроф, стихийных бедствий от населения и организаций, систем мониторинга, подчиненных сил и средств, а также от взаимодействующих и вышестоящих органов повседневного управления РСЧС;

2) прогнозирование развития возможных негативных последствий пожаров, аварий, катастроф и стихийных бедствий, оценка сложившейся и возможной обстановки (в том числе, оценка достаточности муниципальных сил, средств и ресурсов для предупреждения или ликвидации ЧС и необходимости оказания помощи со стороны вышестоящих региональных и федеральных органов исполнительной власти), принятие управленческих решений по экстренному реагированию;

3) подготовка и представление по подчиненности постоянно действующему и координационному органам управления РСЧС муниципального образования[*)] докладов (донесений) об угрозе или возникновении ЧС, сложившейся обстановке, возможных сценариях развития ЧС, вариантах возможных решений и планов их реализации, принятых мерах по ликвидации ЧС, а также необходимых информационных документов - взаимодействующим органам управления РСЧС, и организационно-распорядительных документов - подчинённым подразделениям;

4) доведение задач по предупреждению и ликвидации ЧС, тушению пожаров до привлекаемых сил и средств РСЧС, контроль их исполнения и оперативное управление подчиненными силами и средствами (в том числе, с использованием информационно-навигационных систем на основе ГЛОНАСС);

5) оповещение муниципальных органов управления РСЧС и подчинённых сил и средств о переводе в высшие степени готовности (режимы повышенной готовности и чрезвычайной ситуации), обеспечение

[*)] Примечание: В соответствие с «Положением о единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций», утвержденном постановлением Правительства РФ от 30 декабря 2003 г. № 794, координационным органом управления РСЧС в муниципальном образовании является комиссия по предупреждению и ликвидации ЧС и обеспечению пожарной безопасности органа местного самоуправления, а постоянно действующим органом - орган, специально уполномоченный на решение задач в области защиты населения и территорий от чрезвычайных ситуаций и (или) гражданской обороны.

перевода в режим повышенной готовности или чрезвычайной ситуации муниципальных органов управления РСЧС, а также имеющихся автоматизированных систем, систем связи и оповещения;

6) оповещение населения об угрозе или возникновении ЧС и его информирование о рекомендуемых мерах защиты от поражающих факторов ЧС;

7) доведение задач, поставленных вышестоящими координационными органами управления РСЧС, до привлеченных к ликвидации ЧС муниципальных органов управления РСЧС, контроль их выполнения;

8) постоянное информационное взаимодействие с органами повседневного управления РСЧС на муниципальном уровне;

9) информационно-аналитическое обеспечение работы координационного и постоянно действующего органов управления РСЧС муниципального образования;

10) контроль и поддержание в готовности к переводу в высшие режимы функционирования муниципальных органов повседневного управления;

11) сбор и обработка сведений от подчинённых сил и средств РСЧС о заступившем на дежурство личном составе и состоянии имеющейся техники, оценка их готовности к выполнению возложенных задач;

12) обобщение информации о произошедших пожарах и ЧС, ходе работ по ликвидации их последствий и представление соответствующих докладов по подчиненности;

13) обеспечение проведения учений и тренировок муниципальных органов управления РСЧС;

14) моделирование возможных пожаров, аварий, катастроф и стихийных бедствий на территории муниципального образования, а также мероприятий по их предотвращению и смягчению последствий в целях прогнозирования возникновения и предупреждения чрезвычайных ситуаций природного и техногенного характера, управления рисками ЧС;

15) формирование и ведение в специализированных базах данных, геоинформационных системах, каталогах и архивах нормативно-справочной информации о пожарах и ЧС, рисках их возникновения, объектах проведения аварийно-спасательных работ, муниципальных силах, средствах и ресурсах РСЧС, планах действий и взаимодействия по предупреждению и ликвидации ЧС, а также другой необходимой информации;

16) обеспечение доступа к имеющейся нормативно-справочной и оперативной информации муниципального звена РСЧС для всех вышестоящих органов повседневного управления РСЧС (до Национального центра управления в кризисных ситуациях включительно).

5.2.3 Назначение и функциональность сегмента «Обеспечения безопасности инфраструктуры жилищно-коммунального комплекса»

Сегмент «Обеспечения безопасности инфраструктуры жилищно-коммунального комплекса» предназначен для мониторинга всех потенциальных рисков безопасности среды обитания, в том числе мониторинга муниципальной (коммунальной) инфраструктуры, социальной сферы и координации работы по предупреждению и ликвидации последствий происшествий, вызванных сбоями в работе коммунальной инфраструктуры.

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

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

а) сбор и обработку информации с датчиков;

б) контроль и управление работой газовых котлов и оборудованием тепловых сетей (Приложение 14);

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

— информацию об аварийных и нештатных ситуациях;

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

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

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

— объемы природного газа, расчеты за который осуществляются с

использованием приборов учета (в части многоквартирных домов - с использованием индивидуальных и общих (для коммунальной квартиры) приборов учета);

— измерение давления в трубопроводах;

— измерение температуры теплоносителя в трубопроводах.

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

д) предоставление доступа к видеопотоку соответствующих камер видеонаблюдения;

2) обеспечение промышленной безопасности, включая:

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

б) мониторинг гидротехнических сооружений;

в) мониторинг соблюдения условий лицензирования опасных производственных объектов;

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

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

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

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

з) планирование и контроль необходимых мероприятий и действий;

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

3) мониторинг доступа на охраняемые государственные объекты, включая:

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

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

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

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

4) обеспечение экстренной связи, включая:

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

б) геолокацию точки вызова экстренной службы;

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

5.2.4 Назначение и функциональность сегмента «Обеспечение безопасности имущественного комплекса»

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

КСА «Обеспечение безопасности имущественного комплекса» должен обеспечивать выполнение следующих функций:

1) ведение электронного плана города;

2) ведение «дежурного плана города», включая:

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

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

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

а) планирование ремонтных работ и обслуживания;

б) планирование застройки и переноса объектов;

в) моделирование возможных ситуаций при застройке территорий и прокладке инфраструктуры;

4) мониторинг и профилактику безопасности в социальной сфере, включая:

а) санитарно-эпидемиологический контроль, в том числе мониторинг заболеваемости населения, мониторинг инфекционных, паразитарных болезней и отравлений людей, мониторинг особо опасных болезней сельскохозяйственных животных и рыб, мониторинг карантинных и особо опасных болезней;

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

5) ведение реестров объектов капитального строительства в составе:

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

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

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

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

б) реестра ремонтных работ на объектах энергетической инфраструктуры;

7) ведение реестров сетей и сооружений водоснабжения в составе:

а) реестровой и пространственной информации об объектах водоснабжения;

б) паспортных данных объектов водоснабжения;

в) данных гидравлического расчета сетей водоснабжения;

г) реестра ремонтных работ;

8) ведение реестров тепловых сетей в составе:

а) реестровой и пространственной информации об объектах теплоснабжения;

б) паспортных данных объектов теплоснабжения;

в) данных теплогидравлического расчета сетей теплоснабжения;

г) реестра ремонтных работ;

9) ведение реестров дорог в составе:

а) реестровой и пространственной информации об объектах транспортной инфраструктуры;

б) паспортных данных объектов транспортной инфраструктуры;

в) реестра ремонтных работ;

10) ведение реестров телекоммуникаций в составе:

а) реестровой и пространственной информации об объектах телекоммуникации;

б) паспортов объектов;

в) реестров ремонтных и строительных работ;

11) ведение социального реестра в составе:

а) реестровой и пространственной информации об объектах социальной сферы, а именно детских дошкольных учреждениях, школах, лечебно-профилактических учреждениях, спортивных учреждениях, базах отдыха;

б) базы данных персонала, аккредитованного к работе на объектах социальной сферы;

в) базы данных демографических и социальных характеристик населения;

12) ведение реестров мест обработки и утилизации отходов;

13) ведение реестров природоохранных и рекреационных зон и паркового хозяйства в составе:

а) пространственной информации об особо охраняемых территориях, зеленых насаждениях, парках и рекреационных зонах;

б) базы данных о промышленных предприятиях и их влиянии на экологию;

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

5.3 Требования к внутреннему и внешнему взаимодействию КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры»

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

Для информационного взаимодействия, непредусмотренного протоколами Единого стека открытых протоколов, допускается взаимодействие подсистем КСА, входящих в состав функционального

блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры» напрямую.

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

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

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

— КСА функционального блока «Безопасность населения и муниципальной (коммунальной) инфраструктуры» должны проектироваться на основе мультисервисной цифровой сети передачи данных. Узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;

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

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

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

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

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

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

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

применение закрытых или проприетарных протоколов обмена и интерфейсов взаимодействия недопустимо.

5.3.1 Требования к внутреннему и внешнему взаимодействию КСА сегмента обеспечения правопорядка и профилактики правонарушений

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

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

5.3.2 Требования к внутреннему и внешнему взаимодействию КСА сегмента обеспечения защиты от чрезвычайных ситуаций природного и техногенного характера и пожаров

КСА автоматизированных систем, входящих в сегмент обеспечения защиты от чрезвычайных ситуаций природного и техногенного характера и пожаров, должны взаимодействовать друг с другом, а также с внешними автоматизированными системами через КСА ЕЦОР.

В состав сегмента должны войти взаимодействующие КСА существующих и перспективных муниципальных и объектовых автоматизированных систем органов управления РСЧС соответствующего уровня, в том числе:

диспетчерских и информационно-навигационных систем для

оперативного управления муниципальными и объектовыми силами и средствами РСЧС;

систем поддержки принятия решений по предупреждению и ликвидации ЧС;

систем информирования и оповещения населения при угрозах и возникновении ЧС;

систем мониторинга аварий на потенциально опасных объектах;

систем охранно-пожарной сигнализации, видеонаблюдения и локального оповещения на критически важных, потенциально опасных и социально значимых объектах;

структурированных систем мониторинга и управления инженерными системами зданий и сооружений и др.

С использованием региональной интеграционной платформы должно также обеспечиваться информационно-программное сопряжение этого сегмента с КСА взаимодействующих региональных АС, в том числе, создаваемых во исполнение ранее принятых федеральных нормативных правовых актов:

автоматизированной системы ЦУКС ГУ МЧС России по субъекту РФ (Указ Президента Российской Федерации от 15 февраля 2011 года № 195, распоряжение Правительства Российской Федерации от 4 августа 2011 года № 1391-р);

системы защиты, информирования и оповещения в ЧС населения на транспорте (Указ Президента Российской Федерации от 31 марта 2010 года № 403, распоряжение Правительства Российской Федерации от 30 июля 2010 года №1285-р);

системы обеспечения вызовов экстренных оперативных служб по единому номеру «112» (Указ Президента Российской Федерации от 28 декабря 2010 года № 1632, постановления Правительства Российской Федерации от 21 ноября 2011 года № 958 и от 16 марта 2013 года № 223);

комплексной системы экстренного оповещения населения об угрозе возникновения или о возникновении чрезвычайных ситуаций (Указ Президента Российской Федерации от 13 ноября 2012 года № 1522);

региональной навигационно-информационной системы (постановление Правительства Российской Федерации от 21 декабря 2012 года № 1367, распоряжение Правительства Российской Федерации от 18 ноября 2013 № 2127-р);

государственной автоматизированной информационной системы "ЭРА-ГЛОНАСС" (федеральный закон от 28 декабря 2013 года № 395-ФЗ, распоряжение Правительства РФ от 09 августа 2014 года № 1498-р).

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

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

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

5.3.4 Требования к внутреннему и внешнему взаимодействию КСА сегмента обеспечения безопасности имущественного комплекса

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

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

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

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

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

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

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

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

Помимо крупных терминальных комплексов ОКСИОН городская система оповещения должна быть оснащена сетью малогабаритных пунктов локального информирования и оповещения населения (далее - ПЛИОН), использующих каналы эфирного телерадиовещания, ПЛИОН данного типа должны обеспечивать:

— прием федерального мультиплекса, транслируемого городским радиотелевизионным центром в формате цифрового телевещания DVB-T2 с включенными (инкапсулированными) в состав этого мультиплекса служебными данными;

— извлечение (декапсуляцию) служебных данных из принимаемого мультиплекса, контроль их подлинности и целостности;

— воспроизведение принятых служебных данных в виде предупредительных звуковых и световых сигналов, речевых и/или текстовых сообщений.

В сети ПЛИОН должна быть предусмотрена адресация получателей с целью передачи служебных данных конкретному пункту (подъезд дома), группе пунктов (дом, микрорайон) или всем пунктам оповещения города.

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

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

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

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

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

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

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

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

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

Должны быть соблюдены требования к телекоммуникационной инфраструктуре представленные в Приложении 15.

Технические требования к системе видеонаблюдения представлены в Приложении 16.

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

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

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

Программное обеспечение должно быть сертифицировано по требованиям безопасности информации.

Требования к общему программному обеспечению сегмента «Безопасности населения и муниципальной (коммунальной) инфраструктуры» должны быть аналогичны требованиям к общему программному обеспечению подсистем функционального блока «Координации работы служб и ведомств», представленных в Приложении 6 (Требования к общему программному обеспечению функционального блока «Координация работы служб и ведомств»).

Требования к специальному обеспечению подсистем сегмента «Безопасность населения и муниципальной (коммунальной) инфраструктуры» должно быть аналогичны требованиям к специальному программному обеспечению КСА функционального блока «Координации работы служб и ведомств», представленных в Приложении 7 (Требования к специальному программному обеспечению КСА «Координация работы служб и ведомств»).

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

Требования к информационному обеспечению КСА «Безопасность населения и муниципальной (коммунальной) инфраструктуры» должны быть аналогичны требованиям к информационному обеспечению КСА «Координация работы служб и ведомств» представленных в разделе 4.6 «Требования к информационному обеспечению комплексов средств автоматизации КСА «Координация работы служб и ведомств».

6. Требования к КСА «Безопасность на транспорте»

6.1 Состав КСА «Безопасность на транспорте»

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

1) КСА обеспечения правопорядка, профилактики правонарушений на дорогах в составе следующих подсистем:

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

б) управления видеопотоками и видеоанализа происшествий;

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

2) КСА обеспечения безопасности дорожного движения, в составе следующих подсистем:

а) интеллектуального управления светофорами;

б) планирования дорожной сети;

в) геоинформационной системы мониторинга дорожной обстановки;

г) геоинформационной системы муниципального парковочного оператора;

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

е) управления видеопотоками и видеоанализа событий на дорогах;

ж) анализа и прогнозирования дорожной ситуации;

з) сценарного моделирования транспортных потоков;

и) информирования о дорожной ситуации

к) информационной поддержки парковочного оператора;

л) оплаты услуг парковочного оператора;

м) иные информационные системы.

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

а) диспетчеризации и управления дорожной ситуацией;

б) обеспечения защиты от чрезвычайных ситуаций природного и техногенного характера на объектах транспортной инфраструктуры железнодорожного, водного, воздушного и автомобильного транспорта, метрополитена и дорожного хозяйства;

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

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

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

е) управления общественным транспортом;

ж) диспетчеризации грузового транспорта

з) контроля технического состояния транспортных средств;

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

к) контроля деятельности перевозчиков.

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

6.2.1 Назначение и функциональность сегмента «Обеспечение правопорядка, профилактики правонарушений на дорогах»

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

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

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

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

б) фиксация проходящих транспортных средств;

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

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

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

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

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

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

6.2.2 Назначение и функциональность сегмента «Обеспечения безопасности дорожного движения»

Сегмент «Обеспечения безопасности дорожного движения» предназначен для решения задач управления транспортными потоками и обеспечения эффективного взаимодействия различных служб и организаций муниципального образования в сфере организации и обеспечения безопасности дорожного движения.

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

1) управление логистикой общественного и личного транспорта, включая:

а) расчет расписаний и маршрутов общественного транспорта по результатам сценарного моделирования с учетом данных по пассажиропотокам и перспективным планам развития территорий муниципального образования;

б) расчет оптимальных маршрутов для транспортных средств служб оперативного реагирования;

в) расчет оптимальных маршрутов (коридоров) и графиков проезда для грузового транспорта;

г) расчет маршрутов и расписаний работы городских коммунальных служб;

д) планирование графиков ремонтных работ;

е) планирование зон, ограничивающих движение по типам транспортных средств, и графиков доступа в зоны с ограниченным движением для различных типов транспортных средств.

2) организация и управление муниципальным парковочным пространством, включая:

а) расчет зональности парковочных зон по временному и ценовому признакам для различных категорий транспортных средств;

б) повышение безопасности хранения транспортных средств;

в) обеспечение фото-видеофиксации нарушений правил парковки;

г) профилактику нарушений правил парковки, включая перемещение транспортных средств, мешающих нормальному дорожному движению;

д) обеспечение расчетов за пользование парковкой;

е) подготовка комплекта документов по нарушениям правил парковки и формирование платежных документов для местной расчетной системы;

3) моделирование транспортных потоков, включая:

а) сбор, хранение и анализ информации о дорожной ситуации с установленных датчиков и контроллеров, средств видеонаблюдения;

б) сценарное моделирование дорожной ситуации с использованием методов исторической симуляции, Монте-Карло и других применимых математических моделей;

4) динамическое прогнозирование дорожной ситуации на базе поступающих в режиме реального времени данных с видеокамер, датчиков и контроллеров дорожного движения, включая:

а) отображение на электронной карте текущей и прогнозируемой дорожной ситуации;

б) адаптивное управление дорожной ситуацией в автоматическом и полуавтоматическом режиме (организация «зеленой волны»);

в) расчет сценариев работы периферийных КСА управления дорожным движением (светофоров);

г) прогнозирование последствий дорожного происшествия (события) с учетом данных о текущей дорожной ситуации и исторических данных;

5) автоматическая геолокация и фиксацию событий (инцидентов) на дорогах с визуализацией на карте города, включая:

а) автоматическое распознавание типа события и его фиксацию на карте города;

б) передачу информации о событии в КСА ЕЦОР.

6) обеспечение функций общественного контроля над работой правоохранительных структур на местах.

6.2.3 Назначение и функциональность сегмента «Обеспечения безопасности на транспорте»

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

Основными функциями сегмента «Обеспечения безопасности на транспорте» являются:

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

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

б) автоматическое позиционирование точки вызова и регистрацию события;

в) информирование населения по вопросам гражданской обороны;

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

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

б) автоматическое позиционирование точки вызова и регистрацию события;

в) информирование населения по вопросам гражданской обороны;

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

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

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

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

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

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

б) контроль времени прохождения пути, средней скорости;

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

г) осуществление весового контроля;

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

е) ведение исторической базы перевозок;

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

а) фиксацию отклонений от заданных маршрутов;

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

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

г) предоставление требуемого количества транспортных средств для перевозки;

д) ведение исторической базы перевозок;

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

а) мониторинг графика расписаний воздушных судов, водных судов и железнодорожного транспорта;

б) информирование об отклонениях в расписании воздушных судов, водных судов и железнодорожного транспорта.

6) контроль результатов технического мониторинга объектов транспортной инфраструктуры, включая:

а) автоматизированный сбор данных технических средств мониторинга и контроля транспортной инфраструктуры в целях последующей аналитической обработки;

б) информационно-аналитическое обеспечение деятельности уполномоченных органов исполнительной власти в сфере транспортной безопасности;

7) контроль технического состояния транспортных средств, включая:

а) получение и обработку информации о состоянии транспортных средств;

б) автоматическое отслеживание необходимости планового технического обслуживания;

в) ведение единой базы учета технического состояния транспортных средств (по видам транспортных средств);

8) обеспечение автоматизированной проверки и учета данных в рамках процедуры лицензирования перевозчиков, контроль лицензиатов на предмет выполнения условий лицензирования, включая:

а) сбор и анализ информации с тахографов;

б) учет карточек водителей,

в) осуществление проверки на предмет соблюдения условий договоров об осуществлении пассажирских перевозок;

10) организацию системы информирования населения о работе общественного транспорта и дорожной ситуации, включая:

а) предоставление информации о маршрутах и об актуальном расписании движения общественного транспорта;

б) информирование о фактической дорожной ситуации и ее динамике.

6.3 Требования к внутреннему и внешнему взаимодействию КСА функционального блока «Безопасность на транспорте»

КСА функционального блока «Безопасность на транспорте» должны взаимодействовать между собой и со смежными КСА, входящими в состав АПК «Безопасный город» через КСА ЕЦОР.

Для информационного взаимодействия, непредусмотренного протоколами Единого стека открытых протоколов, допускается прямое взаимодействие подсистем КСА, входящих в состав сегмента «Безопасность на транспорте».

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

Должны быть обеспечены следующие требования к характеристикам взаимосвязи подсистем КСА «Безопасность на транспорте» между собой, с подсистемами смежных КСА:

— взаимодействие КСА подсистем между собой и с подсистемами смежных КСА должно осуществляться на основе открытых протоколов Единого стандарта открытых протоколов;

— сегменты КСА «Безопасность на транспорте» должны проектироваться на основе мультисервисной цифровой сети передачи данных;

— узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;

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

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

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

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

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

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

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

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

6.4 Требования к техническому обеспечению КСА функционального блока «Безопасность на транспорте»

Техническое обеспечение функционального блока «Безопасность на транспорте» должно отвечать следующим общим требованиям:

— образцы средств вычислительной техники и средств коммуникационной техники должны быть сертифицированы;

— обладать расширяемостью;

— обеспечивать устойчивую управляемость;

— электронно-вычислительная техника должна соответствовать или превышать требования технических спецификаций по производительности.

— при выборе технических средств сегмента «Безопасность на транспорте» предпочтение должно отдаваться продукции отечественного производства;

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

Для обеспечения высокой доступности сервисов сегмента «Безопасность на транспорте» для серверных и сетевых компонент, а так же для оборудования, выход которого из строя приводит к недоступности сервиса, время восстановления не должно превышать 2 часа (без учета времени перемещения до места сбоя). Время восстановления для остальной техники 24 часа.

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

Должны применяться видеокамеры, которые позволяют получать цветное видеоизображение в дневное время суток и черно-белое в ночное время. Количество камер видеофиксации определяется из расчета 1 камера на 1 и более полос движения.

Данные о фактах фиксации передвижения транспортных средств, полученные путем распознавания государственных регистрационных знаков (ГРЗ) при передвижении транспортных средств (далее – ТС) через контролируемые зоны формируются с использованием систем идентификации транспортных средств (далее - СИТС). Данные, от уже установленых СИТС, должны передаваться через узлы сбора данных с использованием ЕСОП.

Технические требования к источникам фото-видеофиксации приведены в Приложении 19.

Требования к абонентским терминалам ГЛОНАСС-GPS/GSM, датчикам спутниковой навигации, бортовому навигационному оборудованию приведены в Приложении 17.

Должны быть соблюдены требования к телекоммуникационной инфраструктуре представленные в Приложении 15.

Технические требования к системе видеонаблюдения представлены в Приложении 16.

6.5 Требования к программному обеспечению КСА функционального блока «Безопасность на транспорте»

Программное обеспечение КСА сегментов функционального блока «Безопасность на транспорте» должно представлять собой совокупность общего программного обеспечения и специального программного обеспечения.

Программное обеспечение КСА сегментов функционального блока «Безопасность на транспорте» должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в состав сегментов функционального блока «Безопасность на транспорте» перспективных КСА.

Программное обеспечение должно быть сертифицировано по требованиям безопасности информации.

Функциональные требования к специальному программному обеспечению базовых станций:

— контроль качества данных от каждой станции сети;

— контроль состояния и целостности всей сети;

— возможность ведения мониторинга сети;

— возможность моделирования ионосферных, тропосферных поправок и учет многолучевости для каждого пользователя;

— передача пользователям информации об используемой системе координат;

— реализация технологии VRS в реальном времени и в постобработке;

— учет информации, предоставляемой пользователям, и реализация мощной биллинговой системы.

Требования к общему программному обеспечению КСА «Безопасность на транспорте» должны быть аналогичны требованиям к общему программному обеспечению функционального блока «Координации работы служб и ведомств» представленных в Приложении 6 (Требования к общему программному обеспечению функционального блока «Координация работы служб и ведомств»).

Требования к специальному обеспечению КСА сегментов функционального блока «Безопасность на транспорте» должно быть аналогичны требованиям к специальному программному обеспечению

КСА сегментов функционального блока «Координация работы служб и ведомств» представленных в Приложении 7 (Требования к специальному программному обеспечению КСА функционального блока «Координация работы служб и ведомств»).

6.6 Требования к информационному обеспечению КСА функционального блока «Безопасность на транспорте»

Требования к информационному обеспечению КСА сегментов функционального блока «Безопасность на транспорте» должны быть аналогичны требованиям к информационному обеспечению КСА функционального блока «Координация работы служб и ведомств» представленных в разделе 4.6 «Требования к информационному обеспечению КСА функционального блока «Координация работы служб и ведомств»».

7. Требования к КСА функционального блока «Экологическая безопасность»

7.1 Состав КСА функционального блока «Экологическая безопасность»

Функциональный блок «Экологическая безопасность» состоит из следующих сегментов АПК «Безопасный город»:

1) сегмент геоэкологического планирования в составе следующих КСА подсистем:

а) ведения реестра природопользователей;

б) геоинформационной системы экологического мониторинга;

в) ведения реестра нормативов допустимого воздействия на окружающую среду;

г) автоматизированного документооборота процессов планирования и осуществления муниципального экологического контроля;

д) контроля и мониторинга исполнения предписаний, выданных по результатам муниципального экологического контроля;

е) отчетно-аналитической поддержки природопользователей;

ж) нормативно-справочной базы природопользователей;

з) расчетного обслуживания.

2) сегмент гидрометеорологической информации, включающий следующие компоненты в составе КСА следующих подсистем:

а) модуль предоставления оперативной гидрометеорологической информации;

б) геоинформационная система сейсмической активности;

в) геоинформационная система гидрологии;

3) сегмент экомониторинга, в составе КСА следующих подсистем:

а) геоинформационная система мониторинга экологической обстановки, включая подсистемы мониторинга состояния суши, водных ресурсов, невозобновляемых природных ископаемых, контроль состояния почв;

б) геоинформационная система мониторинга природных явлений;

в) геоинформационная система мест захоронений отходов;

г) система контроля транспортных средств, осуществляющих вывоз и утилизацию отходов.

7.2 Назначение и функциональность КСА функционального блока «Экологическая безопасность»

7.2.1 Назначение и функциональность сегмента «Геоэкологического планирования»

КСА сегмента «Геоэкологического планирования» предназначен для решения задач комплекса задач по обеспечению экологической безопасности, включая аналитическое сопровождение экологических аспектов градостроительной политики, обеспечение эффективной деятельности органов государственной власти в сфере охраны окружающей среды и их взаимодействия природопользователями.

Основными функциями КСА «Геоэкологического планирования» являются:

1) комплексный мониторинг муниципальной застройки и уже существующих объектов с учетом данных по экологической ситуации, в том числе:

а) ведение реестров природопользователей и объектов экологического контроля,

б) ведение реестров нормативных и фактических значений предельно допустимых выбросов и предельно допустимой концентрации веществ;

в) отображение на электронной карте реестровой информации;

г) ежедневный мониторинг предельно допустимого содержимого, предельно допустимых выбросов, предельно допустимой концентрации веществ на предприятиях (близи предприятий), чьи технологические процессы связаны с возможностью вредных выбросов в окружающую среду;

д) сбор и обработку информации с установленных устройств (датчиков) о фактических значениях предельно допустимого содержимого, предельно допустимых выбросов, предельно допустимой концентрации веществ;

е) определение источников загрязнения окружающей среды на базе встроенных аналитических моделей, использующих оперативную фактическую информацию о параметрах загрязнений окружающей среды, исторические статистические данные, гидрометеорологическую информацию;

ж) сценарное моделирование угроз экологической безопасности;

з) прогнозирование развития угроз экологической безопасности с учетом муниципальной застройки и гидрометеорологической обстановки;

2) обеспечение автоматизированного документооборота процессов планирования и осуществления муниципального экологического контроля, включая:

а) автоматизацию сбора и анализ данных от природопользователей о фактических значениях предельно допустимого содержимого, предельно допустимых выбросов, предельно допустимой концентрации веществ, размещение отходов производства и потребления посредством электронного документооборота или импорта отчетных форм;

б) отчетно-аналитическую поддержку природопользователей;

в) ведение нормативно-справочной базы природопользователей;

3) осуществление контроля и мониторинга исполнения предписаний, выданных по результатам муниципального экологического контроля;

а) формирование графиков комплексных проверок объектов муниципального экологического контроля;

б) ведение истории комплексных проверок объектов муниципального экологического контроля;

в) раскрытие информации о результатах комплексных проверок объектов муниципального экологического контроля для природопользователей и населения;

г) автоматизация функций контроля над природопользователями по лицензируемым видам деятельности;

4) обеспечение расчетного обслуживания приропользователей, включая:

а) автоматический расчет платы за предельно допустимое содержимое, предельно допустимые выбросы, предельно допустимую концентрацию веществ, размещение отходов производства и потребления на основании предоставленной природопользователями информации;

б) формирование необходимого пакета платежных документов для природопользователя;

7.2.2 Назначение и функциональность сегмента «Гидрометеорологической информации»

Сегмент «Гидрометеорологической информации» предназначен для информационной поддержки принятия решений по обеспечению экологической безопасности в части сбора, обработки и анализа данных о состоянии атмосферы, водных ресурсов и земной поверхности.

Основными функциями сегмента «Гидрометеорологической информации», являются:

1) предоставление оперативной гидрометеорологической информации, включая:

а) сбор и обработку информации о текущей метеорологической ситуации с установленных периферийных устройств;

б) автоматизированный импорт прогнозной метеорологической информации из внешних источников (специализированных ресурсов);

в) информирование о резких изменениях погоды или климата в том числе угроз ураганов, штормового ветра, обильных снегопадов и затяжных дождей, обледенения дорог и токонесущих проводов;

2) предоставление информации о сейсмической активности;

а) мониторинг сейсмической активности на предмет возникновения просадок, оползней, обвалов земной поверхности;

б) автоматизированный импорт информации о сейсмической активности в регионе из внешних источников (специализированных ресурсов);

3) предоставление гидрологической информации, включая:

а) сбор и обработку данных с периферийных устройств о гидрологической ситуации;

б) мониторинг угроз истощения водных ресурсов, необходимых для организации хозяйственно-бытового водоснабжения и обеспечения технологических процессов;

в) мониторинг паводковой ситуации;

г) мониторинг угроз подтопления населенных пунктов.

7.2.3 Назначение и функциональность сегмента «Экомониторинг»

Сегмент «Экомониторинг» предназначен для решения задач комплексного мониторинга, оперативного реагирования, предупреждения и устранения последствий природных и экологических угроз посредством интеграции данных об экологической обстановке на единой геоинформационной платформе экомониторинга.

Основными функциями сегмента «Экомониторинг», являются:

1) мониторинг загрязнения окружающей среды, включая:

а) консолидацию и отражение на электронной карте данных периферийных устройств в соответствующих реестрах геоинформационной системы в части превышения предельно допустимой концентрации вредных примесей в атмосфере, содержания вредных веществ в воде, наличия вредных примесей в почве;

б) обеспечение представления в геоинформационной системе информации реестров природопользователей в части фактических и допустимых значений предельно допустимого содержимого, предельно допустимых выбросов, предельно допустимой концентрации веществ;

2) контроль состояния суши, включая мониторинг угроз просадок, оползней ни, обвалов земной поверхности из-за выработки недр при добыче полезных ископаемых и другой деятельности человека;

3) мониторинг водных ресурсов, включая

а) контроль загрязнения водных ресурсов;

б) мониторинг угрозы истощения водных ресурсов, необходимых для организации хозяйственно-бытового водоснабжения и обеспечения технологических процессов;

4) мониторинг угроз, связанных с связанных с истощением невозобновляемых природных ископаемых, включая:

а) представление информации о природопользователях и объектах экологического мониторинга;

б) предоставление информации о лицензиях природопользователей и фактических данных по выработки природных ресурсов;

5) контроль состояния почв;

б) мониторинг наличия тяжелых металлов (в том числе радионуклидов) и других вредных веществ в почве (грунте) сверх предельно допустимых концентраций;

в) мониторинг угроз интенсивной деградации почв, опустынивания на обширных территориях из-за эрозии, засоления, заболачивания почв и так далее;

6) мониторинг сейсмической активности в регионе и обеспечение сейсмической безопасности, включая:

а) представление актуальной и исторической информации о сейсмической активности в геоинформационной системе;

б) представление информации о сейсмической устойчивости зданий и объектов городской инфраструктуры;

7) мониторинг гидрологической обстановки и обеспечение безопасности при наводнениях, включая:

а) мониторинг паводковой ситуации, угроз образования ледовых заторов,

б) графическое отображение прогнозов гидрологической обстановки и сопоставление с данными аэрофотосъемки и космоснимков;

8) мониторинг гидрометеорологической обстановки, включая:

а) предоставление актуальной и прогнозной информации по гидрометеорологической обстановке;

б) расчет влияния гидрометеорологической обстановки на развитие потенциальных угроз среде обитания;

9) мониторинг лесопожарной опасности, включая:

а) представление на электронной карте актуальной и исторической информации о лесных пожарах;

б) представление информации о пожароопасных участках;

в) прогнозирование развития угроз лесных пожаров с учетом гидрометеоролической информации;

г) графическое отображение лесопожарной опасности и сопоставление с данными аэрофотосъемки и космоснимков;

10) мониторинг ситуаций, вызванных переполнением хранилищ (свалок) промышленными и бытовыми отходами, загрязнением ими окружающей среды, включая:

а) контроль процессов сбора, транспортировки и переработки отходов, включая формирование и контроль графиков вывоза мусора и отходов;

б) спутниковый контроль транспортных средств, осуществляющих вывоз и утилизацию отходов, включая контроль соблюдения маршрутов и графиков движения, фиксацию остановок транспортных средств .

в) мониторинг состояния окружающей среды в районах размещения отходов и мониторинг экологической обстановки территорий городов для предотвращения и выявления несанкционированных захоронений отходов;

г) ведение базы данных организаций осуществляющих сбор, обработку и утилизацию производственных и бытовых отходов.

7.3 Требования к внутреннему и внешнему взаимодействию КСА функционального блока «Экологическая безопасность»

КСА функционального блока «Экологическая безопасность» должны взаимодействовать между собой и с подсистемами смежных КСА через КСА ЕЦОР.

Для информационного взаимодействия, непредусмотренного протоколами Единого стека открытых протоколов, допускается взаимодействие подсистем КСА функционального блока «Экологическая безопасность» напрямую.

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

Должны быть обеспечены следующие требования к характеристикам взаимосвязи КСА сегментов функционального блока «Экологическая безопасность» между собой и с КСА смежных функциональных блоков:

— взаимодействие КСА и их подсистем между собой и с подсистемами смежных КСА должно осуществляться на основе открытых протоколов Единого стандарта открытых протоколов;

— КСА функционального блока «Экологическая безопасность» должны проектироваться на основе мультисервисной цифровой сети передачи данных. Узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;

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

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

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

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

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

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

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

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

7.4 Требования к техническому обеспечению КСА функционального блока «Экологическая безопасность»

Техническое обеспечение КСА функционального блока «Экологическая безопасность» должно отвечать следующим общим требованиям:

— образцы средств вычислительной техники и средств коммуникационной техники должны быть сертифицированы;

— обладать расширяемостью;

— обеспечивать устойчивую управляемость;

— электронно-вычислительная техника должна соответствовать или превышать требования технических спецификаций по производительности.

— при выборе технических средств КСА подсистем функционального блока «Экологическая безопасность» предпочтение должно отдаваться продукции отечественного производства;

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

Для обеспечения высокой доступности сервисов КСА подсистем функционального блока «Экологическая безопасность» для серверных и сетевых компонент, а так же для оборудования, выход которого из строя приводит к недоступности сервиса, время восстановления не должно превышать 2 часа (без учета времени перемещения до места сбоя). Время восстановления для остальной техники 24 часа.

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

Должны быть обеспечены требования к техническому обеспечению КСА функционального блока «Экологическая безопасность» в соответствие с Приложением 18 (Требования к техническому обеспечению КСА функционального блока «Экологическая безопасность»).

Должны быть соблюдены требования к телекоммуникационной инфраструктуре представленные в Приложении 15.

Технические требования к системе видеонаблюдения представлены в Приложении 16.

7.5 Требования к программному обеспечению КСА функционального блока «Экологическая безопасность»

Программное обеспечение КСА функционального блока «Экологическая безопасность» должно представлять собой совокупность общего программного обеспечения и специального программного обеспечения.

Программное обеспечение КСА функционального блока «Экологическая безопасность» должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного

развития, в частности, с учетом включения в состав КСА «Экологическая безопасность» перспективных КСА.

Программное обеспечение должно быть сертифицировано по требованиям безопасности информации.

Требования к общему программному обеспечению функционального блока «Экологическая безопасность» должны быть аналогичны требованиям к общему программному обеспечению КСА функционального блока «Координации работы служб и ведомств» представленных в Приложении 6 (Требования к общему программному обеспечению функционального блока «Координация работы служб и ведомств»).

Требования к специальному обеспечению КСА функционального блока «Экологическая безопасность» должно быть аналогичны требованиям к специальному программному обеспечению КСА функционального блока «Координация работы служб и ведомств» представленных в Приложении 7 (Требования к специальному программному обеспечению КСА «Координация работы служб и ведомств»).

7.6 Требования к информационному обеспечению КСА функционального блока «Экологическая безопасность»

Требования к информационному обеспечению КСА функционального блока «Экологическая безопасность» должны быть аналогичны требованиям к информационному обеспечению КСА функционального блока «Координация работы служб и ведомств» представленных в разделе 4.6 «Требования к информационному обеспечению КСА функционального блока «Координация работы служб и ведомств»».

ПРИЛОЖЕНИЯ

Приложение 1
Требования к Единому стеку открытых протоколов информационного взаимодействия КСА АПК «Безопасный город»

Назначением Единого стека открытых протоколов взаимодействия (далее ЕСОП) КСА «Безопасный город», а также взаимодействующих с ним КСА 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 КСА «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 «Региональная интеграционная платформа»;

—КСА ЕЦОР должен взаимодействовать с КСА «Региональная интеграционная платформа».

Взаимодействие КСА АПК «Безопасный город» между собой и со смежными КСА должно осуществляться только в рамках ЕСОП.

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 обязательной1. 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 общего глоссария. Такой подход обеспечит возможность на машинном уровне идентифицировать тип события, по которому сформировано извещение, даже если часть тем системе-потребителю неизвестна.

В общий глоссарий 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 общий глоссарий 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 общий глоссарий 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 общий глоссарий 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 общий глоссарий 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 общий глоссарий 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 общий глоссарий 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 общий глоссарий 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.

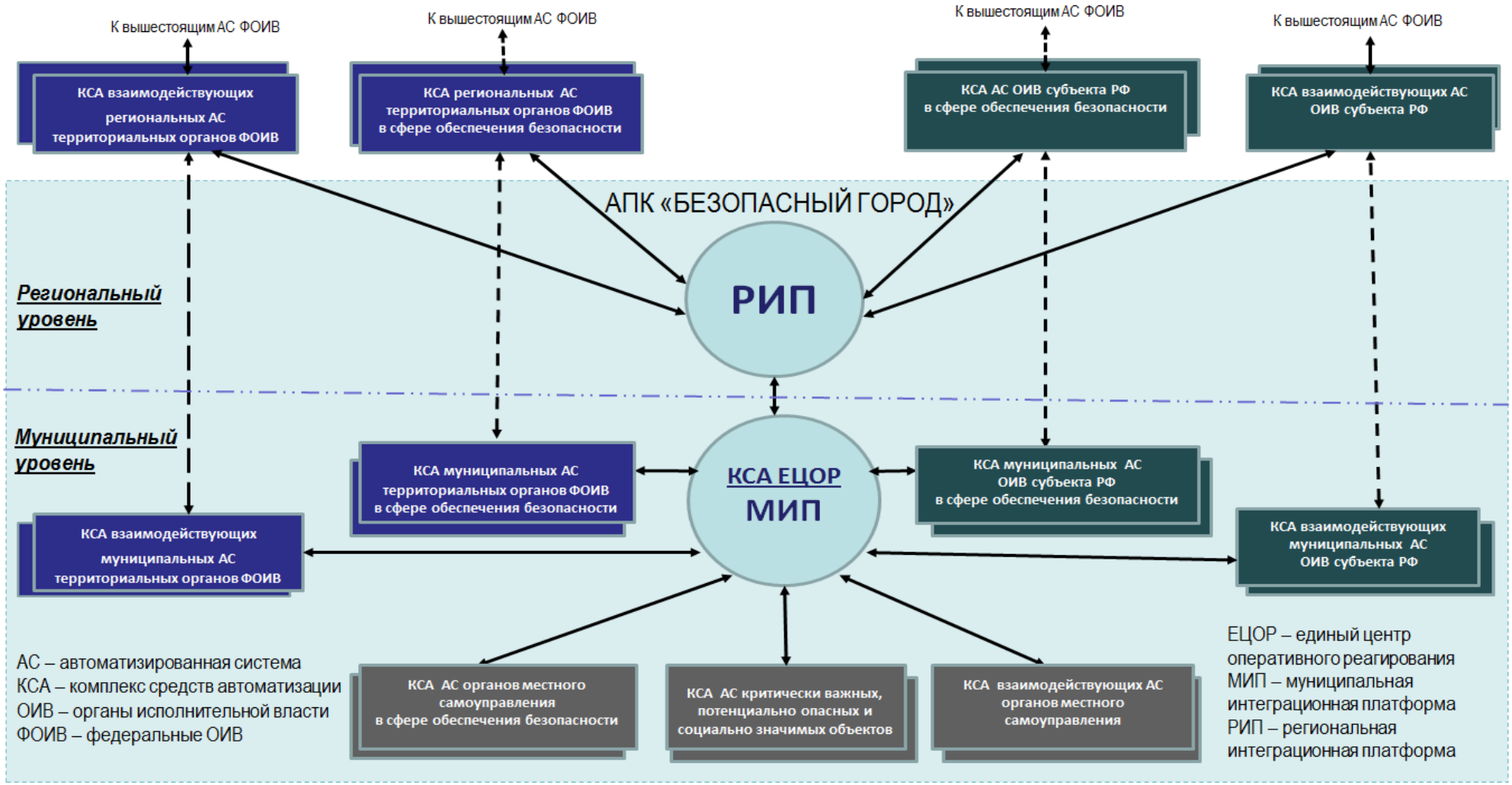
В области управленческих (операционных) рисков общий глоссарий должен определять темы извещений и требования к данным извещения по следующим зафиксированным событиям:

—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.

Приложение 2. Структурная схема АПК «Безопасный город»



Приложение 3
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 4
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».

В состав вышеперечисленных 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.

I. 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.

Приложение 5
Требования к вычислительной инфраструктуре и обеспечивающим прикладным подсистемам КСА «Региональная интеграционная 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 6
Требования к общему программному обеспечению КСА функционального блока «Координация работы служб и ведомств»

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 «Координация работы служб и ведомств». 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 «Координация работы служб и ведомств».

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 7
Требования к специальному программному обеспечению КСА функционального блока «Координация работы служб и ведомств»

Разработка специального программного обеспечения должна быть в первую очередь направлена на реализацию функциональных подсистем КСА функционального блока «Координация работы служб и ведомств».

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 «Координация работы служб и ведомств» 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 8
Требования к информационной совместимости КСА функционального блока «Координация работы служб и ведомств» со смежными КСА

Информационная совместимость КСА функционального блока «Координация работы служб и ведомств» 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 «Координация работы служб и ведомств» со смежными КСА реализуется в ходе электронного информационного взаимодействия (передачи данных) – неоднородных КСА функционального блока «Координация работ служб и ведомств» между собой, между КСА АПК «Безопасный город», а также между КСА функционального блока «Координация работы служб и ведомств» 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 1);

—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 «Координация работы служб и ведомств». 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.

Приложение 9
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 10
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 11
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 12
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 13
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).

Приложение 14
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 15
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: 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 16
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 1).

Таблица 1 – Требования к видеоизображению, регистрируемому ВИ

	Параметр	Значение
	Разрешение регистрируемого	от 1.2 до 4 мегапикселей

	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

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:

– 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./м^2;

– 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 1).

Рисунок 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 2).

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

№	Параметр	Значение
1.	Разрешение регистрируемого изображения	от 1.3 до 2 мегапикселей
2.	Динамический диапазон интенсивности изображения	8 бит, не менее
3.	Частота кадров при максимальном разрешении	25 кадров/с, не менее
4.	Цветность изображения	Цветное
5.	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^2.

– скорость движения людей не более 5 км/ч;

– объем оставленного предмета от 0,001 м^3.

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 3):

Таблица 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: 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
Разрешение для записи событий	1080p(1920×1080 пикселей)	1080p(1920×1080 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.

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 125м.	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); дальность около 15м	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 17
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 18
Требования к техническому обеспечению к сегментам 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 NH3;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.

Приложение 19
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.

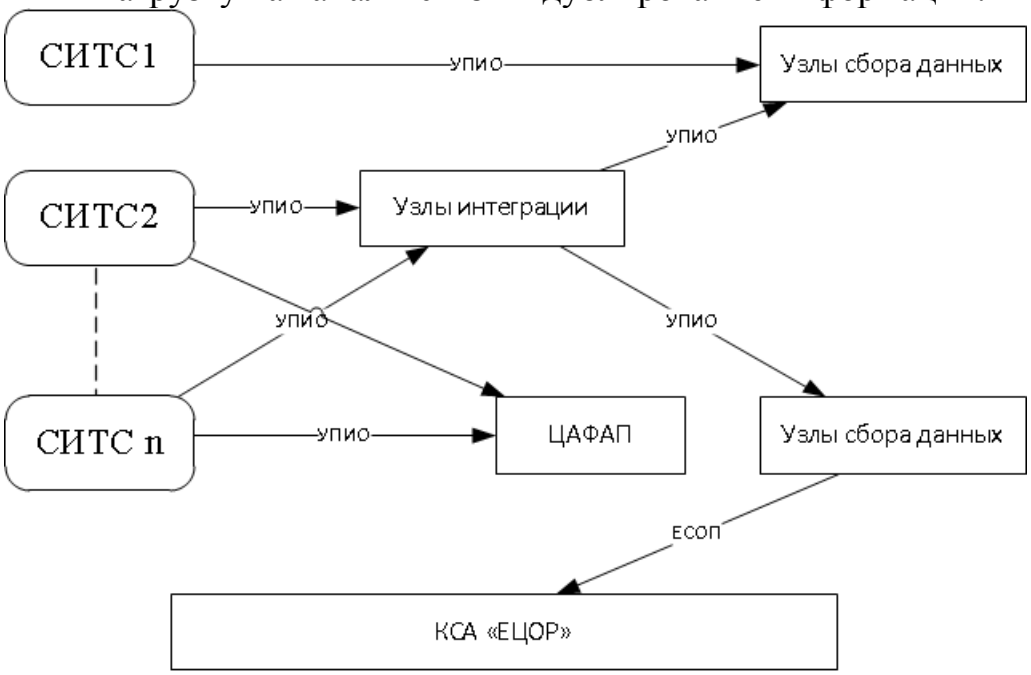


Рисунок 1. Схема передачи данных от СИТС в АПК БГ

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 20
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.