АППАРАТ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

"29" июня 2017 г.
№ П4-34362
МОСКВА

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

Направляется для использования в рамках деятельности Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств "Безопасный город", единые требования к техническим параметрам сегментов аппаратно-программного комплекса "Безопасный город".

Приложение: вх. 4516п-П4 от 28.06.2017 на 214 л.

Заместитель директора
Административного департамента
Правительства Российской Федерации А.Смирнов

Мостовюк М.А. 985-54-44

МЧС России
ОТДЕЛ ДОКУМЕНТАЦИОННОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ И ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
(Москва, Театральный проезд, 3)
Вх. № 01-31452
«30» 06 2017 г.

УТВЕРЖДАЮ
Председатель Межведомственной
комиссии по вопросам, связанным
с внедрением и развитием систем
аппаратно-программного
комплекса технических средств
"Безопасный город"

№6

Д.Рогозин

28 июня 2017 г.
№ 4516п-П4

ЕДИНЫЕ ТРЕБОВАНИЯ

к техническим параметрам сегментов аппаратно-программного комплекса "Безопасный город"

27060354.doc

Содержание

Перечень принятых сокращений

Введение

1. Общие сведения

1.1. Полное наименование и условное обозначение

1.2. Перечень нормативных документов

2. Назначение и цели создания единых требований к техническим параметрам сегментов АПК "Безопасный город"

2.1. Назначение единых требований к техническим параметрам сегментов АПК "Безопасный город"

2.2. Цели и задачи единых требований к техническим параметрам сегментов АПК "Безопасный город"

2.3. Схемы построения АПК "Безопасный город"

3. Требования к архитектуре АПК "Безопасный город"

3.1. Общие требования к архитектуре АПК "Безопасный город"

3.2. Требования к архитектуре АПК "Безопасный город" муниципального уровня

3.3. Требования к архитектуре АПК "Безопасный город" регионального уровня

3.4. Требования к архитектуре АПК "Безопасный город" федерального уровня

4. Требования к КСА функционального блока "Координация работ служб и ведомств"

4.1. Состав КСА функционального блока "Координация работы служб и ведомств"

4.1.1. Централизованная схема построения

4.1.2. Децентрализованная схема построения

4.1.3. Гибридная схема построения

4.2. Требования к КСА "Региональная платформа"

4.2.1. Состав КСА "Региональная платформа"

4.2.2. Назначение и функциональность КСА "Региональная платформа"

4.2.3. Требования к внешнему и внутреннему взаимодействию КСА "Региональная платформа"

4.2.4. Требования к техническому обеспечению КСА "Региональная платформа"

4.2.5. Требования к системному программному обеспечению КСА "Региональная платформа"

4.2.6. Требования к информационному обеспечению КСА "Региональная платформа"

4.3. Требования к КСА Единый центр оперативного реагирования функционального блока "Координация работы служб и ведомств"

4.3.1. Состав КСА Единый центр оперативного реагирования функционального блока "Координация работы служб и ведомств"

4.3.2. Назначение и функциональность КСА ЕЦОР

4.3.3. Требования к внутреннему и внешнему взаимодействию КСА ЕЦОР функционального блока "Координация работы служб и ведомств"

4.3.4. Требования к техническому обеспечению КСА ЕЦОР функционального блока "Координация работы служб и ведомств"

4.3.5. Требования к системному программному обеспечению КСА ЕЦОР функционального блока "Координация работы служб и ведомств"

4.3.6. Требования к информационному обеспечению КСА ЕЦОР функционального блока "Координация работы служб и ведомств"

4.4. Требования к "Сервисной платформе"

4.4.1. Состав КСА "Сервисная платформа"

4.4.2. Назначение и функциональность Сервисной платформы

4.4.3. Требования к внутреннему и внешнему взаимодействию Сервисной платформы

4.4.4. Требования к техническому обеспечению Сервисной платформы правоохранительного сегмента

4.4.5. Требования к системному программному обеспечению Сервисной платформы правоохранительного сегмента

4.4.6. Требования к информационному обеспечению Сервисной платформы

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

5.1. Состав КСА функционального блока "Безопасность населения и муниципальной (коммунальной) инфраструктуры"

5.2. Назначение и функциональность КСА функционального блока "Безопасность населения и муниципальной (коммунальной) инфраструктуры"

5.2.1. Назначение и функциональность системы обеспечения правопорядка и профилактики правонарушений

5.2.2. Назначение и функциональность системы обеспечения защиты территории от чрезвычайных ситуаций природного и техногенного характера и пожаров

5.2.3. Назначение и функциональность системы обеспечения безопасности инфраструктуры жилищно-коммунального комплекса

5.2.4. Назначение и функциональность системы управления дежурным планом города

5.2.5. Назначение и функциональность системы информирования и оповещения

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

5.3.1. Требования к внутреннему и внешнему взаимодействию Системы обеспечения правопорядка и профилактики правонарушений

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

5.3.3. Требования к внутреннему и внешнему взаимодействию Системы обеспечения безопасности инфраструктуры жилищно-коммунального комплекса

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

5.5. Требования к системному программному обеспечению КСА функционального блока "Безопасность населения и муниципальной (коммунальной) инфраструктуры"

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

6. Требования к КСА "Безопасность на транспорте"

6.1. Состав КСА "Безопасность на транспорте"

6.2. Назначение и функциональность КСА функционального блока "Безопасность на транспорте"

6.2.1. Назначение и функциональность Системы обеспечения правопорядка, профилактики правонарушений на дорогах

6.2.2. Назначение и функциональность Системы обеспечения безопасности дорожного движения

6.2.3. Назначение и функциональность Системы обеспечения безопасности на транспорте

6.3. Требования к внутреннему и внешнему взаимодействию КСА функционального блока "Безопасность на транспорте"

6.4. Требования к техническому обеспечению КСА функционального блока "Безопасность на транспорте"

6.5. Требования к системному программному обеспечению КСА функционального блока "Безопасность на транспорте"

6.6. Требования к информационному обеспечению КСА функционального блока "Безопасность на транспорте"

7. Требования к КСА функционального блока "Экологическая безопасность"

7.1. Состав КСА функционального блока "Экологическая безопасность"

7.2. Назначение и функциональность КСА функционального блока "Экологическая безопасность"

7.2.1. Назначение и функциональность системы мониторинга состояния окружающей среды

7.2.2. Назначение и функциональность системы управления рисками окружающей среды

7.3. Требования к внутреннему и внешнему взаимодействию КСА функционального блока "Экологическая безопасность"

7.4. Требования к техническому обеспечению КСА функционального блока "Экологическая безопасность"

7.5. Требования к программному обеспечению КСА функционального блока "Экологическая безопасность"

7.6. Требования к информационному обеспечению КСА функционального блока "Экологическая безопасность"

8. Общие требования к системам АПК "Безопасный город"

8.1. Требования к надежности

8.1.1. Состав и количественные значения показателей надежности

8.1.2. Требования к надежности технических средств и программного обеспечения

8.2. Требования безопасности

8.3. Требования к эргономике и технической эстетике

8.4. Требования к эксплуатации, техническому обслуживанию и ремонту

8.5. Требования по сохранности информации при авариях

8.6. Требования к защите от влияния внешних воздействий

8.7. Требования к патентной чистоте

8.8. Требования по стандартизации и унификации

Приложение 1. Схемы построения АПК "Безопасный город"

Приложение 2. Требования к вычислительной инфраструктуре и обеспечивающим прикладным подсистемам КСА "Региональная платформа"

Приложение 3. Требования к общему программному обеспечению КСА "Региональная платформа" функционального блока "Координация работы служб и ведомств"

Приложение 4. Требования к специальному программному обеспечению КСА "Региональная платформа" функционального блока "Координация работы служб и ведомств"

Приложение 5. Требования к информационной совместимости КСА "Региональная платформа" со смежными КСА

Приложение 6. Требования по применению систем управления базами данных АПК "Безопасный город"

Приложение 7. Требования к структуре процесса сбора, обработки, передачи данных в АПК "Безопасный город"

Приложение 8. Требования к защите данных от разрушений при авариях и сбоях в электропитании систем АПК "Безопасный город"

Приложение 9. Требования к контролю, хранению, обновлению и восстановлению данных АПК "Безопасный город"

Приложение 10. Требования к процедуре придания юридической силы документам, продуцируемым техническими средствами АПК "Безопасный город"

Приложение 11. Требования к обеспечивающим подсистемам КСА ЕЦОР

Приложение 12. Требования к вычислительной инфраструктуре КСА ЕЦОР

Приложение 13. Требования к специальному программному обеспечению КСА ЕЦОР функционального блока "Координация работы служб и ведомств"

Приложение 14. Требования к информационной совместимости КСА ЕЦОР со смежными КСА

Приложение 15. Требования к подсистеме контроля и управления работой газовых котлов и оборудованием тепловых сетей

Приложение 16. Требования к телекоммуникационной инфраструктуре

Приложение 17. Технические требования к системе видеонаблюдения

Приложение 18. Требования к системам фотовидеофиксации нарушений правил дорожного движения

Приложение 19. Требования к абонентским терминалам ГЛОНАСС-GPS/GSM и датчикам спутниковой навигации

Приложение 20. Требования к техническому обеспечению к систем функционального блока "Экологическая безопасность"

Приложение 21. Назначение КСА мониторинга социальных медиа

Приложение 22. Требования к подсистеме радиационного мониторинга и аварийного реагирования на ЧС с радиационным фактором в крупных городах (ПРМиАР)

Приложение 23. Требования к Единому стеку открытых протоколов (ЕСОП) информационного взаимодействия АПК "Безопасный город"

Приложение 24. Технические требования к правоохранительному сегменту АПК "Безопасный город"

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 дежурно-диспетчерская служба
ЖКХ	-	Жилищно-коммунальное хозяйство
ИАС	-	Интегрированная автоматизированная система
ИВК	-	Информационно-вычислительный комплекс
ИКТ	-	Информационно-коммуникационные технологии
ИСПДн	-	Информационная система персональных данных
КВО		Критически важные объекты
КСА	-	Комплекс средств автоматизации
КСА АС	-	Комплекс средств автоматизации автоматизированной системы
КСОБЖ	-	Комплексная система обеспечения безопасности жизнедеятельности
КСП	-	Кризисные ситуации и происшествия
ЛВС	-	Локальная вычислительная сеть

МВК	-	Межведомственная комиссия
МИП	-	Муниципальная интеграционная платформа
МО	-	Муниципальное образование
МЦС	-	Мультисервисная цифровая сеть
НПА	-	Нормативный правовой акт
ОБДП	-	Обобщенная база данных происшествия
ОГВ	-	Органы государственной власти
ОУУ	-	Общедомовой узел учета
ОС	-	Операционная система
ОЗУ	-	Оперативное запоминающее устройство
ПАМ	-	Пост атмосферного мониторинга
ПАК	-	Программно-аппаратный комплекс
ПО	-	Программное обеспечение
ПВР	-	Персональный аудио-видео регистратор
ПУСК	-	Подсистема управления справочниками и классификаторами
ПС	-	Правоохранительный сегмент АПК "Безопасный город" - совокупность ведомственных систем органов внутренних дел
РП	-	Региональная платформа
РСЧС	-	Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций
РФ	-	Российская Федерация
СГК	-	Рабочая группа (Совет главных конструкторов АПК "Безопасный город") для обеспечения методической деятельности Межведомственной комиссии по вопросам, связанным с внедрением и развитием аппаратно-программного комплекса технических средств "Безопасный город"
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 защищенную передачу данных между узлами в сети

Введение

Настоящий документ определяет единые технические требования к сегментам аппаратно-программного комплекса "Безопасный город" и детализирует положения Концепции построения и развития аппаратно-программного комплекса "Безопасный город" (далее - Концепция), утвержденной распоряжением Правительством Российской Федерации от 3 декабря 2014 года №2446-р, в части ее технической реализации.

АПК "Безопасный город" - это аппаратно-программный комплекс, включающий в себя системы автоматизации деятельности единой дежурно-диспетчерской службы (далее - ЕДДС), муниципальных служб различных направлений, системы приема и обработки сообщений, системы обеспечения вызова экстренных и других муниципальных служб различных направлений деятельности, системы мониторинга, прогнозирования, оповещения и управления всеми видами рисков и угроз, свойственных данному муниципальному образованию.

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.

Реализуемые в муниципальных образованиях сегменты аппаратно-программного комплекса "Безопасный город" закладывают основу для создания интегрированных в единое информационное пространство автоматизированных систем обеспечения общественной безопасности, правопорядка и безопасности среды обитания субъектов Российской Федерации.

1. Общие сведения

1.1. Полное наименование и условное обозначение

Аппаратно-программный комплекс "Безопасный город" (далее по тексту - АПК "Безопасный город").

Краткое наименование: АПК БГ.

1.2. Перечень нормативных документов

Распоряжение Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р об утверждении Концепции построения и развития аппаратно-программного комплекса "Безопасный город";

Постановление Правительства Российской Федерации от 8 сентября 2010 г. № 697 "О единой системе межведомственного электронного взаимодействия";

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

Указ Президента Российской Федерации от 28 декабря 2010 г. № 1632 "О совершенствовании системы обеспечения вызова экстренных оперативных служб на территории Российской Федерации";

Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 "Об утверждении перечня сведений, отнесенных к государственной тайне";

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";

ГОСТ 28806-90 "Качество программных средств. Термины и определения";

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 июля 2012 г. № 117-ФЗ "О внесении изменений в Технический регламент о требованиях пожарной безопасности";

Федеральный закон от 9 января 1996 г. № 3-ФЗ "О радиационной безопасности населения";

Федеральный закон от 30 марта 1999 г. № 52-ФЗ "О санитарно-эпидемиологическом благополучии населения";

Федеральный закон от 4 мая 2011 г. № 99-ФЗ "О лицензировании отдельных видов деятельности";

Закон Российской Федерации от 21 июля 1993 г. № 5485-1 "О государственной тайне";

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";

Распоряжение Правительства Российской Федерации № 2299-р от 17 декабря 2010 г. 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. № 209-ФЗ "О государственной информационной системе жилищно-коммунального хозяйства";

Постановление Правительства Российской Федерации от 8 июня 2011 г. № 451 "Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых

для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме";

Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме"";

Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а так же с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны";

Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности";

Распоряжение Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, утверждающее стратегию развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года;

Распоряжение Правительства Российской Федерации от 30 июля 2010 г. № 1285-р о комплексной программе обеспечения безопасности населения на транспорте;

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"";

Приказ Минэкономразвития России от 17 марта 2008 г. № 01 "Об утверждении перечня сведений, подлежащих засекречиванию, Министерства экономического развития и торговли Российской Федерации".

2. Назначение и цели создания единых требований к техническим параметрам сегментов АПК "Безопасный город"

2.1. Назначение единых требований к техническим параметрам сегментов АПК "Безопасный город"

АПК "Безопасный город" предназначен для обеспечения системного комплексного подхода к решению задач в области защиты населения от угроз общественной безопасности, правопорядка и безопасности среды обитания.

Комплексный подход при решении задач обеспечения безопасности предусматривает логически завершенный цикл обработки кризисных ситуаций и происшествий, а также вовлечение в единое информационное пространство участников межведомственного и межуровневого взаимодействия в рамках АПК "Безопасный город", посредством информатизации основных процессов предупреждения и реагирования на КСП.

Единые требования к техническим параметрам сегментов АПК "Безопасный город" (ЕТТ) предназначены для определения типового набора функциональных и технических требований к системам АПК "Безопасный город" на муниципальном, региональном и федеральном уровнях.

Требования, приведенные в настоящем документе, являются основой для формирования технических требований к системам АПК "Безопасный город", разрабатываемых органами исполнительной власти субъектов Российской Федерации и органов местного самоуправления, с учетом своих социально-экономических особенностей, рисков, уровня развития городской, инженерной, транспортной и социальной инфраструктуры, информационно-коммуникационной инфраструктуры.

2.2. Цели и задачи единых требований к техническим параметрам сегментов АПК "Безопасный город"

ЕТТ определены с целью формирования единого подхода к построению и развитию АПК "Безопасный город", в том числе для решения следующих основных задач:

1) создания единого информационного пространства для органов местного самоуправления, органов исполнительной власти субъектов Российской Федерации, федеральных органов исполнительной власти и

организаций любых форм собственности при решении задач обеспечения общественной безопасности, правопорядка, безопасности среды обитания посредством организации доступа, с учетом разграничения прав участников, к данным и функциям автоматизированных систем в контуре информационного обмена АПК "Безопасный город";

2) создания инструментов управления и поддержки принятия решений, для служб и организаций муниципального и регионального уровней, включая развитие систем управления и координации силами и средствами, ситуационного анализа и прогнозирования, позволяющих за счет средств автоматизации оптимизировать их деятельность в рамках решения задач обеспечения общественной безопасности, правопорядка, безопасности среды обитания;

3) обеспечения контроля всех угроз на территории муниципальных образований за счет развития систем мониторинга, предупреждения угроз природного и техногенного характера, включая мониторинг опасных природных явлений, потенциально-опасных объектов, параметров работы городских систем жизнеобеспечения, угроз экологической безопасности, а также систем профилактики правонарушений, предупреждения явлений криминального характера и террористической деятельности;

4) обеспечения возможности многоцелевого использования данных и функций систем АПК "Безопасный город" в интересах всех участников информационного взаимодействия АПК "Безопасный город";

5) повышения качества информационного взаимодействия населения, служб и организаций любых форм собственности, должностных лиц органов местного самоуправления, органов исполнительной власти субъектов Российской Федерации и федеральных органов исполнительной власти при решении задач обеспечения общественной безопасности, правопорядка, безопасности среды обитания.

2.3. Схемы построения АПК "Безопасный город"

При создании КСА функциональных блоков АПК "Безопасный город" на территории субъекта Российской Федерации могут использоваться централизованная, децентрализованная и гибридная схемы построения, определяющие техническую и системную архитектуру КСА функциональных блоков АПК "Безопасный город".

Выбор схемы построения АПК "Безопасный город" и соответствующей функциональной и технической архитектуры АПК "Безопасный город" определяется совокупностью социально-

экономических, природно-географических характеристик, а также характеристик информационно-телекоммуникационной инфраструктуры муниципальных образований и субъектов Российской Федерации.

1) Централизованная схема построения АПК "Безопасный город" предполагает консолидацию вычислительных и программных ресурсов, процессов управления и межсистемного взаимодействия на одной логической площадке (физически возможно распределение вычислительных мощностей по облачному принципу).

2) Децентрализованная схема построения АПК "Безопасный город" предполагает автономное размещение вычислительных мощностей, процессов управления и межсистемного взаимодействия для каждого муниципального образования с агрегированием информации на базе региональной интеграционной платформы на уровне субъекта Российской Федерации.

3) Гибридная схема построения АПК "Безопасный город" предполагает совмещение централизованной и децентрализованной архитектур построения АПК "Безопасный город", допуская:

- автономное размещение вычислительных и программных ресурсов для логических площадок на территории отдельных муниципальных образований;

- создание узловой централизованной логической площадки, обеспечивающей предоставление функций и данных систем АПК "Безопасный город" в муниципальные образования без развертывания в них автономных вычислительных ресурсов.

Примеры схем построения АПК "Безопасный город" приведены в Приложении 1 настоящих ЕТТ.

Выбор общей схемы построения АПК "Безопасный город" на территории определяется архитектурой КСА функционального блока "Координации работы служб и ведомств", при этом элементы систем других функциональных блоков могут быть реализованы распределенно.

Рекомендации по выбору архитектуры КСА функционального блока "Координации работы служб и ведомств" приведены в разделе 4.1.

3. Требования к архитектуре АПК "Безопасный город"

3.1. Общие требования к архитектуре АПК "Безопасный город"

Принципиальная функциональная и техническая архитектура АПК "Безопасный город" на уровне муниципальных образований обеспечивает

формирование единого информационного пространства АПК "Безопасный город", которое объединяет все доступные источники информации об угрозах на территории муниципального образования и формирует платформу для межведомственного и межсистемного взаимодействия всех участников АПК "Безопасный город".

Основой для построения АПК "Безопасный город" служит единая информационно-телекоммуникационная инфраструктура, объединяющая компоненты автоматизированных систем обеспечения общественной безопасности, правопорядка и безопасности среды обитания, реализуемых на объектовом, муниципальном (городские округа и муниципальные районы), региональном (уровень субъекта Российской Федерации), федеральном уровнях.

Единая информационно-коммуникационная инфраструктура АПК "Безопасный город" строится по модульному принципу, на открытых протоколах обмена данных и обеспечивает возможность включения в единый контур информационного АПК "Безопасный город" обмена как новых, так и уже существующих автоматизированных систем объектового, муниципального, регионального и федерального уровней.

Возможность включения в единый контур информационного взаимодействия АПК "Безопасный город" компонентов автоматизированных систем обеспечивается посредством открытых протоколов информационного обмена.

Состав базовой информационно-телекоммуникационной инфраструктуры АПК "Безопасный город" включает:

1) Единую сеть передачи данных - совокупность программно-аппаратных средств, формирующих телекоммуникационную инфраструктуру, предназначенную для обеспечения процессов передачи информации между территориально распределенными компонентами комплекса "Безопасный город";

2) Информационно-вычислительную инфраструктуру комплекса "Безопасный город", обеспечивающих работу функциональных блоков АПК "Безопасный город".

3.2. Требования к архитектуре АПК "Безопасный город" муниципального уровня

Основой для построения единого информационного пространства АПК "Безопасный город" в рамках муниципального образования является

муниципальный уровень единой информационно-телекоммуникационной инфраструктуры АПК "Безопасный город".

Состав единой информационно-телекоммуникационной инфраструктуры АПК "Безопасный город" муниципального уровня формируется с помощью распределенной сети программно-аппаратных комплексов, обеспечивающих мониторинг и контроль угроз населению и территории муниципального образования, а также всех обеспечивающих и автоматизированных информационно-аналитические систем АПК "Безопасный город", объединенных единой сетью передачи данных.

Состав базовой информационно-коммуникационной инфраструктуры АПК "Безопасный город" включает:

1) Единую сеть передачи;

2) Информационно-вычислительную инфраструктуру АПК "Безопасный город" муниципального уровня, обеспечивающую работу следующих функциональных блоков АПК "Безопасный город":

координации работы служб и ведомств;

безопасности населения и муниципальной (коммунальной) инфраструктуры;

безопасности на транспорте;

экологической безопасности.

Состав информационно-вычислительной инфраструктуры АПК "Безопасный город" муниципального уровня включает следующие виды программно-технических средств:

1) сети контроля и мониторинга угроз, как совокупности комплексов периферийных устройств, включающей оконечные устройства, аппаратное и программное обеспечение, телекоммуникационное оборудование, обеспечивающие возможность приема и передачи данных об угрозах населению и территории;

2) интеграционную платформу управления данными, которая в соответствии с определенными правилами и алгоритмами обеспечивает передачу и обработку данных между компонентами АПК "Безопасный город" и внешними сопрягаемыми автоматизированными системами муниципального, регионального и федерального уровней;

3) интеграционную платформу управления видеопотоками, обеспечивающую обработку, управление и первичную аналитику видеопотоков;

4) геоинформационную интеграционную платформу, обеспечивающую пространственное отражение данных из различных компонентов комплекса "Безопасный город";

5) единую систему электронного документооборота и контроля поручений в рамках АПК "Безопасный город", обеспечивающую информационных обмен участников межведомственного взаимодействия на муниципальном уровне;

6) систему обработки и хранения данных с поддержкой распределенного хранения данных;

7) прикладные функциональные системы, предназначенные для обеспечения эффективного решения управленческих задач пользователей АПК "Безопасный город";

8) пользовательские прикладные информационные решения, обеспечивающие взаимодействие органов местного самоуправления, органов исполнительной власти субъекта Российской Федерации, федеральных органов исполнительной власти и населения, включая информационно-справочные интранет и интернет-порталы и мобильные приложения;

9) комплекс информационной безопасности в составе аппаратных и программных средств защиты информации, мониторинга качества каналов и услуг связи;

10) инженерную инфраструктуру, предназначенную для обеспечения устойчивого функционирования компонентов АПК "Безопасный город", в составе систем кондиционирования, пожаротушения, энергоснабжения, резервного электропитания, контроля и управления доступом.

3.3. Требования к архитектуре АПК "Безопасный город" регионального уровня

Основой для построения единого информационного пространства АПК "Безопасный город" в рамках субъекта Российской Федерации является региональный уровень единой информационно-телекоммуникационной инфраструктуры АПК "Безопасный город", обеспечивающий консолидацию данных муниципального уровня информационно-телекоммуникационной инфраструктуры АПК "Безопасный город" и информационное взаимодействие с автоматизированных систем регионального и муниципального уровней.

Состав единой информационно-телекоммуникационной инфраструктуры АПК "Безопасный город" регионального уровня

формируется с помощью распределенной сети программно-аппаратных комплексов, обеспечивающих мониторинг и контроль угроз населению и территории субъекта Российской Федерации, а также всех обеспечивающих и автоматизированных информационно-аналитических систем АПК "Безопасный город" регионального уровня, объединенных единой сетью передачи данных.

Состав базовой информационно-коммуникационной инфраструктуры АПК "Безопасный город" включает:

1) Единую сеть передачи;

2) Информационно-вычислительную инфраструктуру АПК "Безопасный город" регионального уровня, обеспечивающую работу следующих функциональных блоков АПК "Безопасный город":

координации работы служб и ведомств;

безопасности населения и муниципальной (коммунальной) инфраструктуры;

безопасности на транспорте;

экологической безопасности.

Состав информационно-вычислительной инфраструктуры АПК "Безопасный город" регионального уровня включает следующие виды программно-технических средств:

1) сети контроля и мониторинга угроз, как совокупности комплексов периферийных устройств, включающей оконечные устройства, аппаратное и программное обеспечение, телекоммуникационное оборудование, обеспечивающие возможность приема и передачи данных об угрозах населению и территории, в том числе технических средств систем интеллектуального видеонаблюдения, систем фиксации нарушений правил дорожного движения, систем экологического и природного мониторинга, систем мониторинга состояния объектов коммунальной инфраструктуры, систем информирования и оповещения населения, систем мониторинга пожарной безопасности, систем технического мониторинга инженерных конструкций и сооружений, иных технических средств систем мониторинга и контроля угроз, реализуемых на уровне субъекта Российской Федерации;

2) интеграционную платформу обмена данными, обеспечивающую передачу и обработку данных между компонентами АПК "Безопасный город" в соответствии с определенными правилами и алгоритмами и внешними сопрягаемыми автоматизированными системами муниципального, регионального и федерального уровней, в том числе

автоматизированными системами федеральных органов исполнительной власти, включая автоматизированные системы Центра управления в кризисных ситуациях Главного управления МЧС России по субъекту Российской Федерации, систему обеспечения вызова экстренных оперативных служб по единому номеру "112", региональную навигационно-информационную систему "НИС ГЛОНАСС", систему сбора результатов технического мониторинга и контроля объектов транспортной инфраструктуры "СС ТМК" и др.

3) интеграционную платформу управления видеопотоками, обеспечивающую консолидацию, централизованную обработку, управление и первичную аналитику видеопотоков, получаемых с контролируемых объектов на территории муниципальных образований;

4) геоинформационную интеграционную платформу регионального уровня, обеспечивающую консолидацию данных муниципального уровня единой информационно-телекоммуникационной инфраструктуры АПК "Безопасный город" и пространственное отражение информации из различных компонентов АПК "Безопасный город", как в разрезе отдельного муниципального образования, так и консолидировано - на уровне субъекта Российской Федерации;

5) единую систему электронного документооборота и контроля поручений в рамках АПК "Безопасный город", обеспечивающую информационный обмен участников межведомственного взаимодействия на муниципальном, межмуниципальном и региональном уровнях;

6) систему обработки и хранения данных с поддержкой распределенного хранения данных;

7) прикладные функциональные системы уровня субъекта Российской Федерации, предназначенные для обеспечения эффективного решения управленческих задач пользователей АПК "Безопасный город" на уровне субъекта Российской Федерации;

8) сервисную платформу (устанавливается по согласованию с руководителями субъектов Российской Федерации и СГК), предназначенную для стандартизированного сбора данных АПК "Безопасный город" и предоставления их потребителям правоохранительного сегмента в соответствие с требованиями к стандартизированным сервисам протокола ЕСОП (Приложение № 23);

9) пользовательские прикладные информационные решения, обеспечивающие взаимодействие органов местного самоуправления, органов исполнительной власти субъекта Российской Федерации,

федеральных органов исполнительной власти и населения, включая информационно-справочные интранет- и интернет-порталы, мобильные приложения;

10) комплекс информационной безопасности в составе аппаратных и программных средств защиты информации, мониторинга качества каналов и услуг связи;

11) инженерную инфраструктуру, предназначенную для обеспечения устойчивого функционирования компонентов АПК "Безопасный город" на уровне субъекта Российской Федерации.

3.4. Требования к архитектуре АПК "Безопасный город" федерального уровня

Формирование единого контура взаимодействия государственных информационных систем и единого информационного пространства АПК "Безопасный город" обеспечивается как средствами создаваемой единой информационно-телекоммуникационной инфраструктуры АПК "Безопасный город", так и средствами государственных информационных систем.

Единая информационно-телекоммуникационной инфраструктура АПК "Безопасный город" федерального уровня включает:

1) единую сеть передачи данных - совокупность программно-аппаратных средств, формирующих телекоммуникационную инфраструктуру, предназначенную для обеспечения процессов передачи информации между территориально распределенными компонентами АПК "Безопасный город" и государственными информационными системами, участвующими в информационном обмене в рамках АПК "Безопасный город";

2) интеграционную платформу обмена данными, обеспечивающую возможность информационного обмена данными между компонентами АПК "Безопасный город" регионального уровня и государственными информационными системами, включая автоматизированную систему Центра управления в кризисных ситуациях Главного управления Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий по субъекту Российской Федерации, систему обеспечения вызова экстренных оперативных служб по единому номеру "112", региональную навигационно-информационную систему "НИС ГЛОНАСС", систему

сбора результатов технического мониторинга и контроля объектов транспортной инфраструктуры "СС ТМК" и др.

3) элементы программно-аппаратных комплексов государственных информационных систем, обеспечивающих участникам информационного взаимодействия в рамках АПК "Безопасный город" возможность доступа к данным и функциям государственных информационных систем, включая:

единую систему нормативной справочной информации;

систему межведомственного электронного взаимодействия;

единую систему идентификации и аутентификации;

государственную информационную систему жилищно-коммунального хозяйства,

иные государственные информационные системы, информация которых может быть использована в рамках АПК "Безопасный город" в целях обеспечения общественной безопасности, правопорядка и безопасности среды обитания.

4. Требования к КСА функционального блока "Координация работ служб и ведомств"

4.1. Состав КСА функционального блока "Координация работы служб и ведомств"

Состав функционального блока "Координация работы служб и ведомств" формируют подсистемы КСА "Региональная платформа", КСА ЕЦОР и КСА "Сервисной платформы".

В зависимости от выбора схемы построения КСА функционального блока "Координации работы служб и ведомств" и специфики территории субъекта Российской Федерации компонентный набор решений может быть различным.

Для малых, средних и больших городов с численностью населения до 250 тыс. человек возможна реализация КСА функционального блока "Координация работы служб и ведомств" с подключением по централизованной схеме к КСА "Региональная платформа", либо автономная реализация на базе КСА ЕЦОР с подключением к КСА "Региональная платформа" по гибридной схеме построение АПК "Безопасный город".

Для городов крупных городов с численностью населения свыше 250 тыс. человек рекомендуется автономная реализация КСА

функционального блока "Координация работы служб и ведомств" на базе КСА ЕЦОР.

Для региональных центров возможна реализация КСА функционального блока "Координация работы служб и ведомств" по централизованной или децентрализованной схемам построения.

4.1.1. Централизованная схема построения

При централизованной схеме построения состав КСА функционального блока "Координация работы служб и ведомств" АПК "Безопасный город" формируется следующим набором КСА:

1) КСА "Региональная платформа":

подсистема интеграции данных;

геоинформационная подсистема;

подсистема информационно-аналитического сопровождения;

подсистема приема и обработки сообщений;

подсистема поддержки принятия решений;

подсистема комплексного мониторинга;

подсистема электронного взаимодействия с муниципальными службами и населением;

подсистема комплексного информирования и оповещения;

подсистема управления справочниками и классификаторами.

2) КСА Сервисная платформа (опционально на региональном уровне, по согласованию с субъектом Российской Федерации и СГК).

Централизованная схема построения рекомендуется для субъектов Российской Федерации с концентрацией населения более 50% в региональном центре, а также в случаях, когда численность населения подключаемых по КСА "Региональная платформа" муниципальных образований составляет менее 250 тыс. человек.

4.1.2. Децентрализованная схема построения

При децентрализованной схеме построения состав КСА функционального блока "Координация работы служб и ведомств" АПК "Безопасный город" формируется следующим набором КСА:

1) КСА подсистем "Региональной платформы":

подсистема интеграции данных;

геоинформационная подсистема;

подсистема электронного взаимодействия с должностными лицами;

подсистема управления справочниками и классификаторами.

2) КСА подсистем КСА ЕЦОР:

подсистема приема и обработки сообщений;

подсистема поддержки принятия решений;

подсистема комплексного мониторинга;

геоинформационная подсистема;

подсистема электронного взаимодействия с муниципальными службами и населением;

подсистема комплексного информирования и оповещения;

подсистема интеграции данных;

подсистема управления справочниками и классификаторами.

3) КСА Сервисная платформа (опционально, на региональном уровне, по согласованию с субъектом Российской Федерации и СГК).

Децентрализованная схема построения (автономная) рекомендуется для муниципальных образований с населением свыше 250 тыс. человек либо в случаях, когда подключение по централизованной схеме к КСА "Региональной платформы" технически не позволяет обеспечить требования по надежности работы КСА функционального блока "Координация работы служб и ведомств".

4.1.3. Гибридная схема построения

При гибридной схеме построения КСА функционального блока "Координация работы служб и ведомств" АПК "Безопасный город" компоненты функционального блока "Координации работы служб и ведомств" на муниципальном уровне реализуются по централизованной схеме и децентрализованной схеме с консолидацией информации на региональном уровне посредством возможностей КСА "Региональная платформа".

Состав АПК "Безопасный город" муниципальных образований, в которых создаются автономные вычислительные площадки (децентрализованная схема построения) формируется следующим набором подсистем КСА ЕЦОР:

подсистема приема и обработки сообщений;

подсистема поддержки принятия решений;

подсистема комплексного мониторинга;

геоинформационная подсистема;

подсистема электронного взаимодействия с муниципальными службами и населением;

подсистема комплексного информирования и оповещения;

подсистема интеграции данных;

подсистема управления справочниками и классификаторами.

Состав АПК "Безопасный город" муниципальных образований, в которых не создаются автономные вычислительные площадки (централизованная схема построения) и которым предоставляются функции и данные удаленным образом, формируется следующим набором КСА:

1) КСА "Региональная платформа":

подсистема интеграции данных;

геоинформационная подсистема;

подсистема электронного взаимодействия с должностными лицами;

подсистема управления справочниками и классификаторами.

2) подсистемы КСА ЕЦОР:

подсистема приема и обработки сообщений;

подсистема поддержки принятия решений;

подсистема комплексного мониторинга;

подсистема электронного взаимодействия с муниципальными службами и населением;

подсистема комплексного информирования и оповещения.

3) КСА Сервисная платформа (опционально, по согласованию с субъектом Российской Федерации и СГК).

Гибридная схема построения может быть применима к любому субъекту Российской Федерации, в котором планируется создание как минимум одного децентрализованного КСА ЕЦОР.

4.2. Требования к КСА "Региональная платформа"

4.2.1. Состав КСА "Региональная платформа"

Вне зависимости от выбранной схемы построения АПК "Безопасный город" состав КСА "Региональная платформа" формируют следующие подсистемы:

подсистема интеграции данных;

геоинформационная подсистема;

подсистема информационно-аналитического сопровождения;

подсистема управления справочниками и классификаторами.

Базовый состав функциональных систем обеспечивает возможность консолидации данных муниципального уровня, их аналитического

представления для обеспечения поддержки принятия решений, а также организации информационного обмена в рамках АПК "Безопасный город" на региональном уровне.

4.2.2. Назначение и функциональность КСА "Региональная платформа"

КСА "Региональная платформа" предназначен для обеспечения территориальных органов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации оперативной и достоверной информации о ситуации на территориях муниципальных образований соответствующего субъекта Российской Федерации, координации межведомственного взаимодействия на региональном уровне, обеспечения оперативной информационной поддержки служб и ведомств в случае возникновения кризисных ситуаций и происшествий.

КСА "Региональная платформа" должен обеспечивать возможности интеграции на региональном уровне ведомственных вертикально-интегрированных информационных систем, имеющих в своем составе компоненты регионального и муниципального уровней.

Реализуемые в муниципальных образованиях муниципальные интеграционные платформы на региональном уровне должны объединяться региональной интеграционной платформой, формирующей единое информационное пространство для участников информационного взаимодействия АПК "Безопасный город".

Допускается реализация и поддержка обмена данными на региональном уровне для эффективного межведомственного информационного обмена между системами муниципального и регионального уровней с целью обеспечения доступности требуемых данных во всех муниципальных образованиях субъекта Российской Федерации.

Основными функциями КСА "Региональная платформа" являются:

1) агрегация информации от всех КСА ЕЦОР, развернутых на территории муниципальных образований субъекта Российской Федерации;

2) агрегация информации от КСА федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания, а также КСА федеральных органов исполнительной власти и органов исполнительной власти

субъектов Российской Федерации, взаимодействующих с АПК "Безопасный город" на региональном уровне;

3) сопряжение систем АПК "Безопасный город", развернутых на территории всех муниципальных образований, входящих в соответствующий субъект Российской Федерации, с КСА федеральных органов исполнительной власти и органов исполнительной власти субъекта Российской Федерации в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания, а также КСА федеральных органов исполнительной власти и органов исполнительной власти субъекта Российской Федерации, взаимодействующих с АПК "Безопасный город" на региональном уровне;

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

5) обеспечение доступа для федеральных и региональных КСА к необходимым информационным ресурсам АПК "Безопасный город" заданного муниципального образования, в соответствии с регламентами взаимодействия и предоставления информации.

6) предоставление отчетно-аналитической информации по решаемым задачам обеспечения общественной безопасности, правопорядка и безопасности среды обитания в соответствии с принадлежностью региональным органам исполнительной власти, федеральным органам исполнительной, службам и организациям любых форм собственности, участвующих на основании регламентов и соглашений в реагировании на КСП.

Подсистема интеграции данных является базовым компонентом информационно-коммуникационной инфраструктуры АПК "Безопасный город", обеспечивающей работу множества параллельно работающих процессов, связанных с приемом, обработкой и анализом данных, поступающих в систему шин (интеграционную платформу).

Интеграционная платформа должна обеспечивать сбалансированную работу системы в целом за счет встроенных механизмов управления данными, таких как маршрутизации, управлении очередями запросов, управлении заданиями на обработку данных, из которой она может быть получена другими пользователями или вычислительными ресурсами.

Подсистема интеграции данных должна обеспечивать следующие функции:

1) обеспечение информационного обмена между КСА федерального и регионального уровня;

2) обеспечение информационного обмена между КСА регионального уровня и КСА ЕЦОР, развернутых на территории муниципальных образований соответствующего субъекта Российской Федерации;

3) ведение, хранение и резервное копирование информации о КСА федерального и регионального уровня, участвующих в информационном обмене;

4) обеспечение целостности данных;

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

6) ведение журнала операций информационного обмена;

7) организацию маршрутизации, ведение очередей и гарантированную доставку информации, передаваемой между КСА федеральных и региональных органов исполнительной власти и КСА ЕЦОР в рамках АПК "Безопасный город", развернутого на территории муниципальных образований соответствующего субъекта Российской Федерации;

8) агрегацию структурированной и обработанной информации, полученной от КСА ЕЦОР АПК "Безопасный город", развернутого на территории муниципальных образований соответствующего субъекта Российской Федерации;

9) агрегацию информации, полученной от КСА федерального и регионального уровня;

10) обеспечение предоставления единого унифицированного программного интерфейса информационного взаимодействия сопрягаемых автоматизированных систем;

11) обеспечение подключения адаптеров, конвертирующих выходные события к виду, требуемому для выходной системы и обеспечение передачи по требуемому информационной системы протоколу;

12) обеспечение механизма очередей событий в рамках их обработки и передачи во внешние информационные системы с учетом приоритетов, очередности получения, временем хранения и обработки;

13) обеспечение масштабируемости при добавлении вычислительных мощностей;

14) обеспечение балансировки рабочей нагрузки;

15) обеспечение параллельной обработки запросов на выборку данных;

16) обеспечение репликации данных;

17) обеспечение разграничения доступа пользователей к данным;

18) обеспечение систематизированного хранения разнородных данных, в том числе геопространственных данных;

19) обеспечение формирования единой модели данных, позволяющей универсально описать разнородные данные, циркулирующие между сопрягаемыми автоматизированными системами;

20) обеспечение централизованного, в рамках масштабируемого отказоустойчивого кластера, хранения данных, которые используются в информационном обмене;

21) обеспечение возможности по созданию и удалению пользователей подсистемы интеграции данных;

22) обеспечение возможности создания, удаления, редактирования групп и ролей пользователей подсистемы интеграции данных;

23) обеспечение возможности назначения прав пользователей и групп пользователей на добавление, обновление, удаление данных в базе данных подсистемы интеграции данных;

24) обеспечение возможности авторизации пользователей подсистемы интеграции данных;

25) обеспечение возможности динамически (в процессе эксплуатации) создавать и модифицировать структуры данных в базе данных подсистемы интеграции данных посредством графического интерфейса подсистемы интеграции данных;

26) обеспечение централизованного хранения структурированной справочной информации (служебные справочники, классификаторы);

27) обеспечение возможности производить поиск необходимых данных по заданным атрибутам, в том числе при помощи пространственных (геопространственных) запросов, формирование которых должен обеспечивать графический интерфейс подсистемы интеграции данных (возможность формирования запросов при помощи манипулятора типа "мышь");

28) предоставление механизмов асинхронного взаимодействия с сопрягаемыми автоматизированными системами на основе гарантированного их оповещения;

29) защита данных в базе данных подсистемы интеграции данных от случайного изменения путем запрещения выполнения прямых SQL-запросов сопрягаемых систем к базе данных;

30) предоставление механизмов гарантированного доведения информации до адресатов (в подсистеме интеграции данных должен быть реализован механизм гарантированной доставки служебных сообщений);

31) предоставление возможности подписки интегрируемых автоматизированных систем на заданные события и гарантированное доведение соответствующих уведомляющих квитанций о них до подписантов (субъектов взаимодействия с подсистемы интеграции данных);

32) предоставление возможности формирования нестационарных контуров (сценариев) взаимодействия с сопрягаемыми автоматизированными системами путем настройки порядка обработки информационных ресурсов;

33) обеспечение автономной работы без участия операторов системы;

34) обеспечение автоматического контроля доступности элементов системы, изменение конфигурации системы в случае отказа одного из серверов;

35) обеспечение подключения адаптеров, обеспечивающих конвертацию событий, получаемых с использованием других протоколов взаимодействия в стандартный протокол системы.

Подсистема интеграции данных включает в свой состав приложение администратора интеграционной платформы, предоставляющее следующие возможности:

1) управление (создание, изменение, удаление) данных, хранящихся в базе данных подсистемы интеграции данных, в том числе посредством графического интерфейса подсистемы;

2) настройка прав доступа к информационным ресурсам; настройки правил (сценариев) взаимодействия интегрируемых систем, в том числе посредством графического интерфейса подсистемы;

3) настройка жизненных циклов информационных ресурсов, в том числе посредством графического интерфейса подсистемы;

4) отображение и заполнение вложенных (иерархических) формуляров информационных ресурсов (с произвольной глубиной детализации), в том числе посредством графического интерфейса подсистемы;

5) послойное отображение на электронной карте объектов, имеющих координатную информацию (объектов, которые имеют информации о месте расположении), с возможностью отображения детализированных данных по выбранному объекту (при этом должна быть обеспечена возможность перехода от менее детальной к более детальной информации по объектам путем последовательного отображения вложенных формуляров взаимосвязанных объектов с произвольной глубиной детализации);

6) динамическое формирование геоинформационных слоев на основе формирования запросов к встроенной базе данных посредством графического интерфейса (на основе системы фильтров ко всем семантическим данным, хранящихся в базе данных подсистемы) с возможностью отображения на электронной карте подсистемы интеграции данных.

Модуль управления базами данных, в составе подсистемы интеграции данных обеспечивает выполнение следующих требований:

1) поддержку реляционной или объектно-реляционной модели базы данных;

2) совместимость с операционными системами семейства UNIX;

3) поддержку сетевых протоколов TCP/IP;

4) поддержку целостности данных и управление транзакциями;

5) наличие средств оптимизации выполнения запросов и применения индексов;

6) возможность автоматического восстановления базы данных;

7) контроль и управление доступом к данным;

8) многоязыковую поддержку;

9) обеспечение безопасности данных;

10) поддержку кластеризации системы управления базами данных, в том числе: балансировку нагрузки; репликацию, объединение соединений, параллельные запросы.

Подсистема управления справочниками и классификаторами (далее ПУСК) является неотъемлемым компонентом информационно-коммуникационной инфраструктуры АПК "Безопасный город", обеспечивающим управление всей справочной информации.

Функции подсистемы управления справочниками и классификаторами представлены в разделе Подсистема управления справочниками и классификаторами раздела 4.3.1 "Состав КСА Единый

центр оперативного реагирования функционального блока "Координация работы служб и ведомств".

Геоинформационная подсистема предназначена для отображения на электронной карте совокупной информации (об объектах, периферийных устройствах, событиях), связанной с обеспечением общественной безопасности, правопорядка и безопасности среды обитания на территории субъекта Российской Федерации;

Геоинформационная подсистема должна предоставлять следующие функциональные возможности:

1) отображение информации из взаимодействующих КСА федерального и регионального уровня, а также из КСА ЕЦОР, развернутых на территории муниципальных образований субъекта Российской Федерации, в виде семантических слоев, отражающих природно-географические, социально-демографические, экономические характеристики территории;

2) отображение объектов инженерной, транспортной и социальной инфраструктуры муниципальных образований на территории соответствующего субъекта Российской Федерации;

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

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

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

6) атрибутивный поиск на карте объектов классифицированных типов;

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

8) регулярное обновление электронных карт подсистемы для обеспечения актуальности картографической информации.

Подсистема информационно-аналитического сопровождения в составе КСА "Региональная платформа" должна обеспечивать информационное освещение оперативной обстановки на территории региона, предоставлять возможность взаимодействия АПК "Безопасный

город" с должностными лицами региональных государственных организаций по вопросам обеспечения общественной безопасности, правопорядка и безопасности среды обитания.

Региональные государственные организации - организации, подчиненные территориальным органам федеральных органов исполнительной власти, органам исполнительной власти субъекта Российской Федерации.

Подсистема электронного взаимодействия должна предоставлять пользователям следующие возможности:

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

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

3) осуществлять сбор текстовой информации в социальных медиа, напрямую или косвенно связанной с обеспечением безопасности жизнедеятельности, производить анализ ее содержания, удаление дублей, аннотирование, тематическую классификацию и ранжирование информации (см. приложение 21);

4) выявлять значимые события, обсуждаемые в социальных сетях ("информационные всплески"), и предоставлять инструменты для оценки их достоверности (см. приложение 21);

5) предоставлять пользователям сети Интернет актуализированной информации о событиях, связанных с безопасностью жизнедеятельности на территории региона;

6) предоставлять информацию о статусах исполнения обращений граждан с отображением на электронной карте города;

7) обеспечивать фильтрацию зарегистрированных событий, отображаемых на электронной карте подсистемы;

8) предоставлять по принадлежности в соответствие с регламентами и соглашениями органам региональной исполнительной власти, службам и организациям отчетно-аналитическую информацию по происшествиям и чрезвычайным ситуациям.

4.2.3. Требования к внешнему и внутреннему взаимодействию КСА "Региональная платформа"

Внешнее взаимодействие КСА "Региональная платформа" должно предусматривать информационное взаимодействие со следующими КСА:

1) КСА взаимодействующих региональных АС территориальных органов федеральных органов исполнительной власти;

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

3) КСА АС органов исполнительной власти субъекта Российской Федерации в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

4) КСА взаимодействующих АС органов исполнительной власти субъекта Российской Федерации;

5) КСА ЕЦОР на базе ЕДДС муниципальных образований на территории соответствующего субъекта Российской Федерации.

Внутреннее взаимодействие КСА "Региональная платформа" подчиняется следующим принципам:

1) подсистема интеграции данных обеспечивает сопряжение внешних КСА и подсистем, входящих в состав КСА "Региональная платформа";

2) информация, поступающая от сопрягаемых КСА, отображается на электронной карте геоинформационной системы в составе КСА "Региональная платформа" в соответствии с разграничением прав доступа.

Внешнее и внутреннее взаимодействие КСА "Региональная платформа" выполняется на основе стандартизованных протоколов.

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

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

1) узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;

2) базовый протокол обмена сообщениями - XML/SOAP.

4.2.4. Требования к техническому обеспечению КСА "Региональная платформа"

Телекоммуникационная инфраструктура КСА "Региональная платформа" должна обеспечить надежный и безопасный обмен информацией между всеми КСА ЕЦОР, функционирующих на базе ЕДДС, входящих в состав субъекта Российской Федерации.

В основу построения телекоммуникационной инфраструктуры должны быть заложены следующие принципы:

комплексность, унификация и совместимость реализуемых проектных, технических и технологических решений;

открытость архитектуры построения;

обеспечение стандартных интерфейсов и протоколов;

резервирование каналов передачи информации;

обеспечение централизованного сетевого мониторинга и администрирования;

обеспечение возможности организации круглосуточного сервисного обслуживания оборудования;

возможность поэтапного создания и ввода в эксплуатацию без нарушения функционирования существующих элементов;

возможность приоритетного использования существующих сетей передачи данных.

Телекоммуникационная инфраструктура должна обеспечивать:

поддержку стека сетевых протоколов TCP/IP;

поддержку протоколов приоритетной обработки очередей обслуживания;

поддержку транспортных протоколов реального времени;

обеспечение передачи различных видов трафика (данные, аудио- и видео-потоки, управление) и обеспечение динамического распределения полосы пропускания;

использование резервных каналов связи в режиме балансирования нагрузки;

оперативную локализацию сбоев в сетевом оборудовании и каналах связи;

высокий уровень отказоустойчивости, позволяющий осуществлять быстрое автоматическое восстановление работоспособности в случае единичного выхода из строя резервируемых критичных компонент активного сетевого оборудования или основных физических каналов связи в телекоммуникационной инфраструктуре.

Подробные требования к техническому обеспечению КСА "Региональная платформа" представлены в приложении 2.

4.2.5. Требования к системному программному обеспечению КСА "Региональная платформа"

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

Программное обеспечение КСА "Региональная платформа" построено на открытой, компонентной (модульной) архитектуре, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в состав перспективных систем АПК "Безопасный город".

Технология разработки программного обеспечения (включая нормативно-техническую документацию) должно обеспечивать возможность согласованной разработки унифицированного (типового) программного обеспечения силами нескольких разработчиков.

Требования к общему программному обеспечению КСА "Региональная платформа" представлены в приложении 3.

Требования к специальному обеспечению КСА "Региональная платформа" представлены в приложении 4.

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

4.2.6. Требования к информационному обеспечению КСА "Региональная платформа"

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 "Региональная платформа".

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

Единая система кодирования и классификации информации обеспечивает:

централизованное ведение словарей и классификаторов, использующихся в информационном взаимодействии;

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

Для общероссийских классификаторов должен обеспечиваться импорт обновлений из файлов, полученных от организаций и ведомств, ответственных за ведение этого классификатора.

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

Приложение 5 - "Требования к информационной совместимости КСА "Региональная платформа" со смежными КСА";

Приложение 6 - "Требования по применению систем управления базами данных АПК "Безопасный город";

Приложение 7 - "Требования к структуре процесса сбора, обработки, передачи данных в АПК "Безопасный город";

Приложение 8 - "Требования к защите данных от разрушений при авариях и сбоях в электропитании систем АПК "Безопасный город";

Приложение 9 - "Требования к контролю, хранению, обновлению и восстановлению данных АПК "Безопасный город";

Приложение 10 - "Требования к процедуре придания юридической силы документам, продуцируемым техническими средствами АПК "Безопасный город".

Программное обеспечение должно быть сертифицировано по требованиям информационной безопасности.

4.3. Требования к КСА Единый центр оперативного реагирования функционального блока "Координация работы служб и ведомств"

4.3.1. Состав КСА Единый центр оперативного реагирования функционального блока "Координация работы служб и ведомств"

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

Функциональные:

подсистема приема и обработки сообщений;

подсистема поддержки принятия решений;

подсистема комплексного мониторинга;

геоинформационная подсистема;

подсистема электронного взаимодействия с муниципальными службами и населением;

подсистема комплексного информирования и оповещения;

подсистема интеграции данных;

подсистема управления справочниками и классификаторами (ПУСК).

Обеспечивающие:

подсистема обеспечения информационной безопасности;

подсистема резервирования;

подсистема административного управления;

система хранения данных.

4.3.2. Назначение и функциональность КСА ЕЦОР

КСА ЕЦОР предназначен для обеспечения решения задач оперативного предупреждения и 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 обеспечивают:

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

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

комплексный мониторинг угроз общественной безопасности, правопорядка и безопасности среды обитания посредством агрегации данных, полученных от систем АПК "Безопасный город", а также информации о КСП из сопрягаемых внешних систем, в том числе объектовых;

возможность подключения и управления периферийными устройствами систем, включенных в контур информационного взаимодействия АПК "Безопасный город", в соответствие с

определенными с владельцем такого оборудования регламентами доступа и соглашениями;

2) поддержку принятия решений, а именно:

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

автоматическое предоставление сценария реагирования в соответствии с установленными регламентами взаимодействия;

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

оценку сложившейся обстановки и динамическую актуализацию результатов моделирования с учетом поступающих данных с КСА систем мониторинга АПК "Безопасный город";

3) управление и координацию взаимодействия, а именно:

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

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

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

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

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

управление поручениями и контроль исполнения поручений;

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

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

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;

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 АПК "Безопасный город", а именно:

интеграции и информационного взаимодействия между системами "Безопасный город" посредством муниципальной и региональной интеграционных платформ, в том числе посредством предоставления интерфейсов программирования, разработки стандартизированных протоколов и правил информационного обмена, интеграции на уровне баз данных, обмена файлами и иных способов информационного обмена, обеспечивающих возможность включения в контур информационного взаимодействия новых систем;

организация единого информационного-справочного пространства АПК "Безопасный город";

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

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

формирование отчетов для муниципальных органов власти, бизнеса с гибким механизмом настройки и расширения возможностей, позволяющим формировать отчеты за любой период времени;

обеспечение возможности формирования сводных отчетов по нескольким критериям;

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

Подсистема приема и обработки сообщений КСА ЕЦОР предназначена для приема и обработки сообщений о происшествиях на территории муниципального образования, контроля исполнения поручений по связанным с зарегистрированными событиями сценариям реагирования, хранения полученной информации в категорированном виде и виде голосовых записей.

Система приема и обработки сообщений КСА ЕЦОР должна позволять:

1) обеспечить маршрутизацию вызовов в зависимости от выбранной схемы маршрутизации:

централизованной - вызовы приходят на единый центр обработки вызовов и маршрутизируются в ЕДДС в соответствии с географическим признаком территории, с которой звонит абонент (AreaID);

децентрализованной - вызовы приходят непосредственно на ЕДДС.

2) поддерживать настройку различных алгоритмов резервирования вызовов: с возможностью маршрутизации вызова, не принятого ЕДДС, другими ЕДДС, центром обработки вызовов или резервным центром обработки вызовов.

3) осуществлять прием и обработку голосовых вызовов с возможностью заполнения электронной регистрационной карточки, включая: автоматическое определение номера абонента, координат местоположения абонента (при наличии соответствующей возможности у оператора связи), а также дополнительную информацию о происшествии, получаемую из других подсистем КСА ЕЦОР, включая информацию о месте происшествия (объектах), предварительный расчет зоны поражения, ущерба и пострадавших, а также рекомендаций по силам и средствам, которые рекомендуется привлекать к реагированию.

4) осуществлять прием, регистрацию, документирование сообщений поступающих посредством обращений через подсистему электронного взаимодействия с муниципальными службами и населением, в том числе получаемых в виде СМС-сообщений на короткий номер, сообщений по

электронной почте, сообщений на специализированном интернет-портале с автоматическим заполнением информации, указанной в обращении, в том числе с определением местоположения абонента по IP-адресу устройства, с которого направлено сообщение, при наличии соответствующей возможности у оператора связи;

5) осуществлять двусторонний обмен сообщениями о происшествиях (карточками информационного обмена), поступающих из включенных в контур информационного обмена АПК "Безопасный город" автоматизированных систем диспетчерского управления;

6) осуществлять прием, регистрацию, документирование сообщений о происшествиях, поступающих из включенных в контур информационного обмена АПК "Безопасный город" систем мониторинга и контроля угроз на территории муниципального образования, в том числе объектовых, включая уведомления о критических сбоях в работе систем, превышениях критических показателей по контролируемым показателям;

7) обеспечивать позиционирование местоположения события на электронной карте геоинформационной подсистемы в автоматическом режиме при наличии соответствующей технической и организационной возможности у оператора связи, либо в ручном режиме по адресу или метке на геоинформационной интеграционной подсистеме;

8) поддерживать возможность многопользовательского режима при работе с регистрационной карточкой события, обеспечивающего возможность внесения изменений и дополнений в регистрационную карточку привлекаемыми к реагированию службами;

9) обеспечивать двухсторонний обмен изменениями в информации, вносимыми в регистрационную карточку события КСА ЕЦОР и в формируемых на ее основе карточках события в сопрягаемых с КСА ЕЦОР автоматизированных системах оперативного диспетчерского управления;

10) осуществлять выбор состава оповещаемых служб в зависимости от типа происшествия в автоматическом или полуавтоматическом режиме, с возможностью редактирования (добавления или удаления) состава оповещаемых в рамках конкретного происшествия служб;

11) обеспечивать доведение задач по предупреждению и ликвидации КСП до привлекаемых сил и средств, контроль их исполнения и оперативную координацию подчиненными силами и средствами (в том числе, с использованием информационно-навигационных систем на основе ГЛОНАСС);

12) осуществлять контроль хода исполнения поручения с возможностью информирования диспетчера ЕДДС при угрозе срыва срока исполнения поручения, привлекаемыми службами;

13) обеспечивать возможность записи и хранения вызовов, в том числе записи голосовых сообщений на автоответчик с фиксацией номера звонившего абонента, а также определением его местоположения при наличии технической и организационной возможности у оператора связи.

Подсистема поддержки принятия решений предназначена для информационно-аналитического сопровождения деятельности ЕДДС, ДДС, а также служб и организаций, привлекаемых к реагированию на КСП.

Подсистема поддержки принятия решений на основании категории события должна формировать набор семантически связанных рекомендаций по реагированию на КСП, включая формирование плана реагирования, сценариев реагирования на КСП для каждой из служб, задействованных в реагировании на КСП, а также обеспечивать формирование справочной и расчет прогностической информации о зоне потенциального поражения, ущербе, количестве сил и средств рекомендуемых для привлечения к реагированию КСП.

В состав подсистемы поддержки принятия решений входят следующие модули:

Модуль управления диалогами;

Модуль анализа и прогнозирования КСП;

Модуль управления планами реагирования и сценариями реагирования;

Модуль контроля исполнения поручений;

Отчетно-аналитический модуль.

1) Модуль управления диалогами должен обеспечивать возможность ведения детерминированных диалогов на основании заложенных в систему диалоговых ветвей, привязанных к атрибутам КСП, в том числе категории и месту КСП, характеристикам объекта КСП и иным признакам.

2) Модуль анализа и прогнозирования кризисных ситуаций и происшествий должен обеспечивать выполнение следующих функциональных возможностей:

моделирования развития КСП в зависимости от ассоциируемых с территорией рисков, включая риски паводков, лесных пожаров, техногенных пожаров, взрывов на потенциально-опасных объектах,

выбросов АХОВ, радиационного заражения, розлива нефтепродуктов, землетрясений, оползней и иных КСП;

автоматической или полуавтоматической (с возможностью ручного ввода параметров) корректировки расчетов моделей с учетом гидрометеорологической информации: температуры, атмосферных осадкой, скорости ветра;

автоматической корректировки расчетов с учетом семантических связей с характеристиками территории в расчетной зоне поражения из геоинформационной интеграционной подсистемы КСА ЕЦОР, включая наличие природных и техногенных барьеров для распространения КСП, характеристик объектов в зоне поражения, включая информацию по количеству и категориям населения, проживающему в расчетной зоне поражения, хранимым опасным веществам, наличию трубопроводов, продуктоводов и газопроводов, систем жизнеобеспечения и иной информации, содержащейся в паспортах территорий.

автоматического расчета зоны информирования и оповещения.

3) Модуль управления планами реагирования и сценариями реагирования должен обеспечивать выполнение следующих функциональных возможностей:

формирование сценариев реагирования для всех привлекаемых реагированию на КСП служб, в том числе с учетом определенных категорией КСП семантических связей с характеристиками территории, объектов и иной информации их подсистем КСА ЕЦОР;

предоставление рекомендаций по привлечению сил и средств для каждой из служб в зависимости от категории КСП,

формирование инструкций диспетчеру ЕДДС по обработке зарегистрированного события на основе утвержденных регламентов при ликвидации КСП;

формирование на основании сценариев реагирования совокупного плана реагирования по КСП с возможностью контроля диспетчером ЕДДС исполнения выданных на его основании поручений службам и организациям, привлекаемым к реагированию.

4) Модуль контроля исполнения поручений должен обеспечивать выполнение следующих функциональных возможностей:

автоматическое формирование поручений на основании сценариев реагирования и совокупного плана реагирования для всех, привлекаемых к реагированию на КСП служб и организаций;

ведение временных и качественных лимитов исполнения поручений и контроль своевременного выполнения выданных службам и организациям поручений;

автоматическое информирование диспетчеров ЕДДС и привлекаемых к реагированию служб и организаций о нарушении сроков исполнения поручений, угрозе переквалификации события в ЧС и иных случаях, предусмотренных системой лимитов.

информационно-аналитическое обеспечение работы координационного и постоянно действующего органа управления РСЧС муниципального образования;

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

5) Отчетно-аналитический модуль должен обеспечивать выполнение следующих функциональных возможностей:

формирование графиков и отчетов по работе ЕДДС и ДДС на основе имеющейся (накапливаемой) в КСА ЕЦОР информации;

автоматизация информационного обмена отчетно-аналитической информацией ЕДДС и ДДС в рамках регламентных процедур взаимодействия с органами государственной власти;

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

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

---

* Примечание: В соответствие с Положением о единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций, утвержденном постановлением Правительства Российской Федерации 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.

подсистему приема и обработки сообщений, в виде описания и количественных показателей;

подсистему "Интеграционная географическая информационная система", в виде слоев предполагаемых зон поражения, а также необходимой и достаточной зоны информирования и оповещения населения;

подсистему электронного взаимодействия с муниципальными службами и населением, в виде информационного сообщения и инструкции действий для населения;

подсистему комплексного информирования и оповещения, в виде списка средств оповещения, попадающих в расчетную зону оповещения населения.

Подсистема комплексного мониторинга предназначена для сбора и анализа параметров контролируемых объектов, формирования тревожных сообщений о превышении контрольных значений и инициирования запросов на формирование регистрационной карточке и соответствующей ей сценариев реагирования.

Подсистема комплексного мониторинга должна обеспечивать следующие функциональные возможности:

1) сбор и хранение информации о параметрах контролируемых объектов на основании данных, получаемых из сопрягаемых КСА;

2) автоматическую группировку событий по местоположению и категории КСП или иным атрибутам;

3) автоматическое формирование тревожных сообщений в случае превышения контрольных значений по контролируемому объекту;

4) автоматическое формирование сценария реагирования в случае превышения контрольных значений по контролируемому объекту;

5) осуществление мониторинга технического состояния оконечных устройств сопрягаемых КСА.

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

подсистему приема и обработки сообщений, в части формирования запросов на формирование регистрационной карточки происшествия в случае нарушения контрольных параметров по контролируемым объектам, а также предоставления информации для автозаполнения регистрационной карточки с указанием координат оконечных устройств и характера нарушений контрольных параметров по контролируемому объекту;

подсистему поддержки принятия решений, в части предоставления информации, необходимой для анализа изменений контролируемых параметров, формирования запросов на запуск расчетных задач по моделированию и прогнозированию развития КСП, а также формирования статистики и отчетности по ним;

геоинформационную подсистему для следующих целей специальной маркировки (на электронной карте) условного знака первоисточника информации, зафиксировавшего критическое значение, или по которому обнаружен технический сбой.

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

В подсистеме предусматривается механизм регулярного обновления электронных карт подсистемы для обеспечения актуальности картографической информации.

Интеграционная геоинформационная подсистема предоставляет следующие функциональные возможности:

1) ведения пространственной информации следующих семантических слоев:

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

б) набор слоев органов экстренного оперативного реагирования, визуализирующий места расположения ЕДДС, взаимодействующих ДДС, подразделений служб экстренного реагирования и других принимающих в реагировании служб и организаций;

в) места расположения потенциально опасных и критически важных объектов;

г) места расположения социально значимых объектов, объектов с массовым пребыванием людей;

д) места расположения мобильных подразделений, привлекаемых к предупреждению и ликвидации кризисных ситуаций и происшествий.

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

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

4) атрибутивного поиска на карте объектов классифицированных типов;

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

6) отображения задействованных в реагировании мобильных средств (транспортных) в привязке к конкретному КСП (регистрационной карточке).

Пользовательский интерфейс подсистемы должен предоставлять следующие функциональные возможности:

атрибутивный поиск на карте объектов классифицированных типов;

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

прокладку маршрутов движения между заданными объектами.

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

Функциональные возможности подсистемы электронного взаимодействия с ДДС, муниципальными службами и населением предоставляются с использованием сети Интернет и не требуют установки дополнительного специализированного программного обеспечения на АРМы пользователей.

Подсистема электронного взаимодействия с муниципальными службами и населением предоставляет следующие возможности:

1) получение актуальной информации о событиях, напрямую или косвенно связанных с обеспечением безопасности жизнедеятельности, а так же о допустимых к общему доступу инцидентах и заявках с обозначением их статуса и с привязкой к местности (обозначением на электронной карте города);

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

3) предоставление населению необходимой актуализированной информации о событиях, связанных с безопасностью жизнедеятельности;

4) предоставление населению информации о статусах исполнения обращений граждан с отображением на электронной карте города;

5) присоединение к формируемому пользователем обращению мультимедийной информации о событии;

6) автоматическое определение устройства обратившегося пользователя с автоматическим предоставлением соответствующей версии веб-интерфейса (для мобильных устройств - мобильную версию);

7) фильтрация зарегистрированных событий, отображаемых на электронной карте веб-интерфейса подсистемы электронного взаимодействия по следующим критериям: завершенные события, обрабатываемые события, категории событий, события по заданному периоду времени;

8) предоставление отдельного непубличного функционального контура для должностных лиц муниципального образования, реализуемого посредством личного кабинета, обеспечивающего в дополнении к функциям публичного контура, доступного населению, следующие функциональные возможности:

обеспечение информационного взаимодействия с органами повседневного управления РСЧС на муниципальном уровне посредством электронных сообщений;

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

предоставление дополнительной информации по КСП, необходимой должностному лицу для принятия решений по реагированию на КСП;

оперативное предоставления плана реагирования на КСП;

формирование уведомления о поступлении нового задания;

ведение журнала приема и обработки заданий;

отображение совокупной информации на электронной карте города с учетом разграничения прав доступа;

отображение совокупной статистической информации об основных показателях функционирования АПК "Безопасный город" с

использованием графиков и цветовой маркировки критических показателей, отслеживаемых в режиме реального времени.

Подсистема комплексного информирования и оповещения предназначена для информирования населения о событиях, связанных с угрозами безопасности жизнедеятельности и среды обитания.

Подсистема комплексного информирования и оповещения обеспечивает оповещение и информирование граждан по заранее подготовленным шаблонам и сценариям, посредством направления информационных сообщений, через подсистему интеграции данных, существующим и перспективным КСА, предназначенным для оповещения и информирования населения об угрозах общественной безопасности, правопорядка и безопасности среды обитания.

Подсистема комплексного информирования и оповещения обеспечивает следующие функциональные возможности:

1) оповещение муниципальных органов управления РСЧС и подчиненных сил и средств о переводе в высшие степени готовности (режимы повышенной готовности и чрезвычайной ситуации) автоматизированных систем, систем связи и оповещения;

2) запуск сигналов оповещения на локальные средства оповещения (цифровые) существующих на территории муниципального образования систем оповещения и информирования населения;

3) выбор способа оповещения и применяемой для оповещения конфигурации средств оповещения, в том числе:

с задействованием всех средств оповещения, включая СМС-информирование, теле-радиоперехват, терминальных комплексов информирования, сирен и иных ЛСО;

с применением пользовательской конфигурации средств оповещения, включая возможность запуска сигналов оповещения только в расчетной зоне оповещения или на отдельных устройствах оповещения (при наличии соответствующей технической возможности производителя оборудования ЛСО).

формирование и передача речевых и голосовых сообщений по телефону;

формирование и передача тестовых сообщений (СМС) на мобильные устройства для различных групп абонентов в зависимости от категорий событий.

Подсистема интеграции данных - основной компонент при построении АПК "Безопасный город" на муниципальном уровне,

являющийся совокупностью интеграционных шин (интеграционной платформой), обеспечивающей на муниципальном уровне сопряжение между автоматизированными системами в контуре информационного взаимодействия АПК "Безопасный город" муниципального уровня и объединение их в единое информационное пространство.

Подсистема интеграции данных может быть использована отдельно от других подсистем КСА ЕЦОР в составе других функциональных блоков, в качестве базовой платформы обеспечения электронного обмена информацией.

Основными задачами подсистемы интеграции данных являются:

интеграция подсистем и КСА с целью организации комплексного информационного взаимодействия и обеспечения целостного процесса обработки информации;

обеспечение функционирования сопрягаемых подсистем и КСА в едином информационном пространстве и в единой понятийной среде.

Для объединения КСА, участвующих в информационном обмене в рамках построения и развития АПК "Безопасный город", в единое информационного пространства, используются следующие источники информации:

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

системы мониторинга сил и средств постоянной готовности, действующих на территории муниципального образования;

системы видеонаблюдения в местах массового скопления людей и проведения массовых мероприятий, на транспорте и объектах транспортной инфраструктуры, местах отдыха, развлекательных и торговых центрах;

автоматизированные системы управления муниципальным хозяйством;

федеральные государственные информационные системы и системы мониторинга;

региональные государственные системы мониторинга угроз и информационные системы.

Подсистема интеграции данных КСА ЕЦОР должна обеспечивать следующие функции:

1) обеспечение информационного обмена между КСА федерального, регионального и муниципального уровней;

2) ведение, хранения и резервного копирования информации о КСА сопрягаемых систем муниципального уровня, участвующих в информационном обмене;

3) ведение журнала операций информационного обмена;

4) ведение нормативно-справочной информации;

5) организация маршрутизации, ведение очередей и гарантированную доставку информации, передаваемой между КСА федеральных и региональных органов исполнительной власти, КСА "Региональная платформа" и КСА ЕЦОР муниципальных образований соответствующего субъекта Российской Федерации;

6) агрегация структурированной и обработанной информации, полученной от КСА ЕЦОР муниципальных образований соответствующего субъекта Российской Федерации;

7) агрегация информации, полученной от КСА федерального и регионального уровней, а также КСА ЕЦОР муниципальных образований соответствующего субъекта Российской Федерации;

8) предоставление единого унифицированного программного интерфейса информационного взаимодействия сопрягаемых автоматизированных систем;

9) подключение адаптеров, конвертирующих выходные события к виду, требуемому для выходной системы и обеспечение передачи по требуемому информационной системы протоколу;

10) обеспечение механизма очередей событий в рамках их обработки и передачи во внешние информационные системы с учетом приоритетов, очередности получения, временем хранения и обработки;

11) масштабируемость при добавлении вычислительных мощностей;

12) обеспечение балансировки рабочей нагрузки;

13) обеспечение параллельной обработки запросов на выборку данных;

14) обеспечение репликации данных;

15) обеспечение разграничения доступа пользователей к данным;

16) обеспечение систематизированного хранения разнородных данных, в том числе геопространственных данных;

17) формирование единой модели данных, позволяющей универсально описать разнородные данные, циркулирующие между сопрягаемыми автоматизированными системами;

18) обеспечение централизованного хранения, в рамках масштабируемого отказоустойчивого кластера, данных, которые используются в информационном обмене;

19) возможность создания, удаления пользователей подсистемы интеграции данных;

20) возможность создавать, удалять, редактировать группы, роли пользователей подсистемы интеграции данных;

21) возможность назначать права пользователям и группам пользователей на добавление, обновление, удаление данных в базе данных подсистемы интеграции данных;

22) возможность авторизовать пользователей подсистемы интеграции данных;

23) возможность динамически (в процессе эксплуатации) создавать и модифицировать структуры данных в базе данных подсистемы интеграции данных посредством графического интерфейса подсистемы интеграции данных;

24) обеспечение централизованного хранение структурированной справочной информации (служебные справочники, классификаторы);

25) возможность производить поиск необходимых данных по заданным атрибутам, в том числе при помощи пространственных (геопространственных) запросов, формирование которых должен обеспечивать графический интерфейс подсистемы интеграции данных (возможность формирования запросов при помощи манипулятора типа "мышь");

26) предоставление механизмов асинхронного взаимодействия с сопрягаемыми автоматизированными системами на основе гарантированного их оповещения;

27) защита данные в базе данных подсистемы интеграции данных от случайного изменения путем запрещения выполнения прямых SQL-запросов сопрягаемых систем к базе данных;

28) предоставление механизмов гарантированного доведения информации до адресатов (в подсистеме интеграции данных должен быть реализован механизм гарантированной доставки служебных сообщений);

29) предоставление возможности подписки интегрируемых автоматизированных систем на заданные события и гарантированное доведение соответствующих уведомляющих квитанций о них до подписантов (субъектов взаимодействия с подсистемой интеграции данных).

30) предоставление возможности формирования нестационарных контуров (сценариев) взаимодействия с сопрягаемыми автоматизированными системами путем настройки порядка обработки информационных ресурсов;

31) обеспечение автономной работы без участия операторов системы;

32) обеспечение автоматического контроля доступности элементов системы, изменение конфигурации системы в случае отказа одного из серверов;

33) обеспечение подключения адаптеров, обеспечивающих конвертацию событий, получаемых с использованием других протоколов взаимодействия в стандартный протокол системы;

Система управления базами данных, в составе подсистемы интеграции данных должна обеспечивать выполнение следующих требований:

1) поддержку реляционной или объектно-реляционной модели базы данных;

2) совместимость с операционными системами семейства UNIX;

3) поддержку сетевых протоколов TCP/IP;

4) поддержку целостности данных и управление транзакциями;

5) наличие средств оптимизации выполнения запросов и применения индексов;

6) возможность автоматического восстановления базы данных;

7) контроль и управление доступом к данным;

8) многоязыковую поддержку;

9) обеспечение безопасности данных;

10) поддержку кластеризации системы управления базами данных, в том числе: балансировку нагрузки; репликацию, объединение соединений, параллельные запросы.

Подсистема управления справочниками и классификаторами (ПУСК) является неотъемлемым компонентом информационно-коммуникационной инфраструктуры АПК "Безопасный город", обеспечивающим управление всей справочной информации.

ПУСК должна обеспечивать следующие функции:

1) обеспечение централизованного хранения и управления структурированной справочной информации:

служебные справочники и классификаторы;

общероссийские классификаторы;

2) обеспечение ведения общей системы кодирования и классификации информации;

3) обеспечение формирования единой модели основных данных, позволяющей универсально описать разнородную справочную информацию, циркулирующую между сопрягаемыми автоматизированными системами;

4) динамическое (в процессе эксплуатации) создание и модификация структуры данных в базе данных ПУСК посредством графического интерфейса подсистемы интеграции данных;

5) обеспечение управления иерархическими классификаторами, в том числе:

создание и изменение структуры иерархических классификаторов, атрибутов, ограничений на значение атрибутов;

управление наследованием атрибутивного состава на каждом уровне иерархии классификатора;

задание правил кодирования на каждом уровне иерархии классификатора;

построение справочников с фасетной и иерархической системой классификации;

6) обеспечение управления связями между справочниками и классификаторами, в том числе:

поддержка различных типов связей (один-к-одному, многие-ко-многим и т.д.) между объектами, включая возможность задания дополнительных атрибутов для экземпляра связи между объектами;

использование разветвленной ссылочной структуры для формирования дополнительных связей между данными;

формирование ассоциативных связей-ссылок между близкими по свойствам объектами, функциональными эквивалентами, а также взаимозаменяемыми и аналогичными материалами и т.п.;

7) обеспечение управления качеством справочных данных, в том числе:

создание правил качества на основе функций очистки и нормализации данных;

возможность настраивать область применимости в зависимости от происхождения данных (систем источников);

управление наследованием правил качества данных по уровням иерархии классификатора;

управление правилами идентификации дубликатов;

управление правилами слияния дубликатов в ручном и автоматических режимах, с возможностью указания уровня доверия конкретным источникам данных на по-атрибутной основе.

8) обеспечение взаимодействия с внешними сервисами, таким как ЕГРЮЛ, ЕГРИП, ЕГРН, КЛАДР, ФИАС и т.п., для исправления и обогащения справочных данных;

9) обеспечение историчности данных и поддержки различных версий, в том числе:

поддержка концепции периодов актуальности записи с возможностью одновременного существования нескольких активных периодов, включая прошлое и будущее;

хранение истории модификации записи как целиком, так и в отдельности для каждого периода актуальности;

возможность возврата к определенной исторической версии записи;

возможность сравнения исторических версий записей справочника.

10) консолидация структурированной и обработанной справочной информации, полученной всех систем АПК "Безопасный город", развернутых на территории муниципальных образований соответствующего субъекта Российской Федерации;

11) консолидация справочной информации, полученной от КСА федерального и регионального уровня;

12) возможность производить поиск справочных данных и классификаторов, в том числе:

многокритериальный поиск по заданным атрибутам, в том числе с возможностью формирования сложных условий;

полнотекстовый поиск с учетом русской морфологии;

поиск по связям между справочниками;

фасетный поиск на основе классификационных групп.

13) обеспечение управления регламентами изменения данных справочников и классификаторов (управление заявками), в том числе:

возможность настройки собственных сценариев обработки заявок пользователей в зависимости от справочника и значения атрибутов записей;

возможность настройки исполнителей на каждом шаге жизненного цикла заявки с детализацией до роли, конкретного пользователя;

возможность настройки формирования шаблонов уведомлений пользователям;

возможность визуального конструирования шаблонов жизненного цикла заявки (последовательные/параллельные шаги, цикличность, возврат заявки на доработку и др.);

возможность настройки состава полей формы заявки и доступа к ним (чтение, редактирование, обязательность заполнения) на каждом шаге жизненного цикла заявки.

14) обеспечение протоколирования событий подсистемы, в том числе:

протоколирование всех действий пользователя с фиксацией (логина, ФИО, даты совершения операции, затронутых данных), включая доступ к данным в режиме просмотра, а также входа и выхода из подсистемы;

протоколирование всех системных действий с фиксацией, включая автоматический запуск пакетных операций;

предоставление возможности анализа журнала действий пользователя и системных событий с фильтрации и сортировкой информации по всем видам зафиксированных атрибутов;

предоставление возможности доступа к журналу действий пользователя и системных событий через программные интерфейсы (API).

15) обеспечение предоставления единого унифицированного программного интерфейса информационного взаимодействия для доступа и модификации основных данных;

16) обеспечение централизованного хранения, в рамках масштабируемого отказоустойчивого кластера, данных, которые используются в информационном обмене;

17) предоставление механизмов синхронного и асинхронного взаимодействия с подсистемой интеграции данных;

18) защита данных в базе данных ПУСК от случайного изменения путем запрещения выполнения прямых SQL-запросов сопрягаемых систем к базе данных;

19) обеспечение автономной работы без участия операторов системы;

20) обеспечение разграничения прав доступа, в том числе:

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

обеспечение разграничения доступа пользователей к данным;

возможность создавать, удалять пользователей ПУСК;

возможность создавать, удалять, редактировать группы, роли пользователей ПУСК;

возможность назначать права пользователям и группам пользователей на добавление, обновление, удаление данных в базе данных ПУСК;

возможность настройки прав доступа на уровне действия (согласование, добавление, изменение, удаление, импорту/экспорту данных, печать);

обеспечение ведения журнала операций изменения и доступа к данным;

обеспечение возможности использования механизмов разграничения доступа из подсистемы интеграции данных.

21) обеспечение возможности управления базами данных, в том числе:

обеспечение поддержки реляционной или объектно-реляционной модели базы данных;

обеспечение совместимости с операционными системами семейства UNIX;

обеспечение поддержки сетевых протоколов TCP/IP;

обеспечение поддержки целостности данных и управление транзакциями;

предоставление средств оптимизации выполнения запросов и применения индексов;

предоставление возможности автоматического восстановления базы данных;

предоставление возможности контроля и управления доступом к данным;

обеспечение поддержки кластеризации системы управления базами данных, в том числе: балансировку нагрузки; репликацию, объединение соединений, параллельные запросы.

ПУСК предоставляет следующие администраторские возможности:

1) возможность просмотра, создания, редактирования, логического и физического удаления записей, включая просмотр истории записи/источников данных записи, с учетом периодов актуальности;

2) возможность физического удаления записей;

3) возможность восстановления логически удаленных записей;

4) возможность создания черновиков данных;

5) возможность импорта сложных объектов (связанные объекты, иерархии и др.) из файлов (*.xls, *xlsx, *.csv и др.);

6) возможность экспорта сложных объектов (связанные объекты, иерархии и др.) из файлов (*.xls, *xlsx, *.csv и др.);

7) возможность массового изменения одного или нескольких атрибутов справочника, а также его связей;

8) возможность сохранять поисковые шаблоны для последующего быстрого использования;

9) возможность давать доступ к сохраненным шаблонам между разными пользователями;

10) возможность настраивать способ поисковой выдачи (список, табличное представление, картинки, и т.д.);

11) возможность сохранять настроенные способы поисковой выдачи для каждого справочника и поискового шаблона для каждого пользователя;

12) возможность формирования перечня пользовательских заявок с возможностью выборки по всем штатным свойствам заявок, таким как: календарный период, организация, тип заявки, пользователь, статус, справочник и т.д.;

13) возможность формирования отчета по процессам тиражирования изменений справочников в прикладные системы;

14) возможность формирования отчета в процентном и количественном соотношении о работе пользователей (добавление, изменение, удаление, закрытие, перенос позиций);

15) возможность формирования отчета в процентном и количественном соотношении о качестве данных с разбивкой по справочникам, группам ошибок, уровне критичности и т.д. за отчетный период;

16) возможность формирования отчета в процентном и количественном соотношении о дубликатах и загруженных данных с разбивкой по справочникам за отчетный период;

17) возможность вывода всех форм отчетов в табличном виде (*.xls, *xlsx, *.csv и др.), либо в формате *.pdf;

18) возможность специализации пользовательского интерфейса для отображения данных и быстрого перехода в смежные информационные системы.

Кроме того, ПУСК включает следующие возможности:

1) возможность управления (создания, изменения, удаления) данными, хранящихся в базе данных ПУСК, в том числе посредством графического интерфейса подсистемы;

2) возможность настройки прав доступа к информационным ресурсам; настройки правил (сценариев) взаимодействия интегрируемых систем, в том числе посредством графического интерфейса подсистемы;

3) возможность настройки жизненных циклов информационных ресурсов, в том числе посредством графического интерфейса подсистемы;

4) возможность отображения и заполнения вложенных (иерархических) формуляров информационных ресурсов (с произвольной глубиной детализации), в том числе посредством графического интерфейса подсистемы.

Требования к обеспечивающим системам представлены в Приложении 11.

4.3.3. Требования к внутреннему и внешнему взаимодействию КСА ЕЦОР функционального блока "Координация работы служб и ведомств"

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

1) КСА взаимодействующих муниципальных АС территориальных органов федеральных органов исполнительной власти;

2) КСА муниципальных АС территориальных органов федеральных органов исполнительной власти в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

3) КСА АС органов местного самоуправления и муниципальных организаций в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

4) КСА критически важных, потенциально опасных и социально значимых объектов;

5) КСА взаимодействующих муниципальных АС органов исполнительной власти субъекта РФ в сфере обеспечения общественной безопасности, правопорядка и безопасности среды обитания;

6) КСА взаимодействующих муниципальных АС органов исполнительной власти субъекта РФ;

7) КСА взаимодействующих АС органов местного самоуправления;

8) КСА "Региональная платформа" соответствующего субъекта Российской Федерации.

Внутреннее взаимодействие КСА ЕЦОР должно выполняться по следующему принципу. Подсистема интеграции данных должна обеспечивать сопряжение внешних КСА и подсистем, входящих в состав КСА ЕЦОР. Информация, поступающая от сопрягаемых КСА должна

отображаться на электронной карте геоинформационной подсистемы в составе КСА ЕЦОР в соответствии с разграничением прав доступа.

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

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

1) узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;

2) базовый протокол обмена сообщениями - XML/SOAP.

4.3.4. Требования к техническому обеспечению КСА ЕЦОР функционального блока "Координация работы служб и ведомств"

Средства вычислительной техники должны быть максимально приспособлены для последующей модернизации.

Для серверных и сетевых компонент, а также 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 систем 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 в режиме 24/7 (ежедневно и круглосуточно). Для участков сети, требующих повышенную надежность, необходимо предусмотреть резервные каналы связи.

Для линий связи проходящих через общедоступные помещения и линий связи соединения с сетью Интернет должны использоваться средства шифрования трафика, при передаче по таким линиям связи информации, к которой предъявляются требования по обеспечению конфиденциальности.

Подробные требования к техническому обеспечению КСА ЕЦОР представлены в приложении 12.

4.3.5. Требования к системному программному обеспечению КСА ЕЦОР функционального блока "Координация работы служб и ведомств"

Системное программное обеспечение КСА ЕЦОР функционального блока "Координация работы служб и ведомств" представляет совокупность общего программного обеспечения и специального программного обеспечения.

Программное обеспечение КСА ЕЦОР функционального блока "Координация работы служб и ведомств" должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития.

Требования к общему программному обеспечению КСА ЕЦОР функционального блока "Координации работы служб и ведомств" представлены в Приложении 3.

Требования к специальному обеспечению КСА ЕЦОР функционального блока "Координация работы служб и ведомств" представлены в Приложении 13.

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

4.3.6. Требования к информационному обеспечению КСА ЕЦОР функционального блока "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 ЕЦОР функционального блока "Координация работы служб и ведомств".

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

Единая система кодирования и классификации информации должна обеспечивать:

централизованное ведение словарей и классификаторов, использующихся в информационном взаимодействии;

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

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

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

Приложение 14 - Требования к информационной совместимости КСА ЕЦОР со смежными КСА;

Приложение 6 - Требования по применению систем управления базами данных АПК "Безопасный город";

Приложение 7 - Требования к структуре процесса сбора, обработки, передачи данных в АПК "Безопасный город";

Приложение 8 - Требования к защите данных от разрушений при авариях и сбоях в электропитании систем АПК "Безопасный город";

Приложение 9 - Требования к контролю, хранению, обновлению и восстановлению данных АПК "Безопасный город";

Приложение 10 - Требования к процедуре придания юридической силы документам, продуцируемым техническими средствами АПК "Безопасный город".

Приложение 23 - Требования к единому стеку открытых протоколов (ЕСОП) информационного взаимодействия АПК "Безопасный город"

Специальное программное обеспечение должно быть сертифицировано по требованиям информационной безопасности.

4.4. Требования к "Сервисной платформе"

4.4.1. Состав КСА "Сервисная платформа"

КСА "Сервисная платформа" создается по согласованию с субъектом Российской Федерации и СГК для обеспечения стандартизированного информационного взаимодействия с потребителями информации от АПК "Безопасный город" в правоохранительном сегменте по сервисной модели (МВД России, ФСБ России и другими ведомствами).

В состав КСА "Сервисная платформа" (далее Сервисная платформа), входят следующие КСА:

модуль управления правами доступа и авторизации пользователей;

модуль сервисов видеонаблюдения;
модуль сервисов фотовидеофиксации;
модуль сервисов событий и тревог;
модуль управления хранением данных и материалов;
муниципальный компонент КСА "Сервисная платформа".

4.4.2. Назначение и функциональность Сервисной платформы

Сервисная платформа должна поддерживать единую точку авторизации, предоставляющую доступ к консолидированным ресурсам АПК "Безопасный город" на региональном уровне пользователям в соответствии с правами доступа. При этом должен быть обеспечен анонимный доступ пользователей правоохранительного сегмента к консолидированным ресурсам АПК "Безопасный город".

Сервисная платформа может поддерживать следующие базовые функции:

предоставление информации для систем-потребителей правоохранительного сегмента;

формирование материалов, связанных с событиями, информация о которых поступает с систем интеллектуального видеонаблюдения, фотовидеофиксации правонарушений ПДД;

управление хранением материалов;

обеспечение анонимности доступа пользователей из правоохранительного сегмента к ресурсам АПК "Безопасный город";

ведение реестра источников данных, систем-потребителей и пользователей АПК "Безопасный город";

ведение журнала учета запросов и извещений, регистрирующий все извещения от систем-источников, а также запросы пользователей на доступ к ресурсам АПК "Безопасный город", на формирование и выдачу материалов.

Функции КСА сервисной платформы включают:

1) В части систем видеонаблюдения:

автоматическое получение информации о составе сервисов прикладной системы, их возможностях и параметрах, верификации факта синхронизации времени и получения информации о конкретных сетевых адресах прикладных сервисов;

автоматическое получение информации о списке видеоисточников в составе системы видеонаблюдения, их данных, местоположения, области

обзора камер и параметрах доступа к ним (сетевые адреса, параметры авторизации и др.);

определение порядка доступа к "живым" потокам аудио и видеоданных с камер системы видеонаблюдения;

определение порядка доступа к архивным записям медиа данных с камер системы видеонаблюдения;

управление устройствами видеонаблюдения: поворотом, наклоном и приближением (Pan-Tilt-Zoom) камер системы видеонаблюдения;

управление фокусировкой камер системы видеонаблюдения;

управление разграничением доступа к видеоисточникам в системе видеонаблюдения, обеспечивая возможность через сервисную платформу АПК БГ ограничить доступ операторов системы видеонаблюдения к "живым" и архивным медиа данным, управлению PTZ и фокусировкой с выбранных камер за указанное время;

обеспечение конфиденциальности запросов для определенных групп пользователей (в соответствие с определенными нормативными документами и регламентами правами);

2) В части систем фотовидеофиксации нарушений правил дорожного движения:

автоматическое получение информации о составе сервисов прикладной системы, их возможностях и параметрах, верификации факта синхронизации времени и получения информации о поддерживаемых сервисах;

получения информации о списке фото источников в составе системы видеонаблюдения, их данных, местоположения и области обзора;

поиска и предоставление фотоматериалов в системе фотовидеофиксации по времени и географической области;

поиска и предоставление фотоматериалов по параметрам: номеру транспортного средства (фрагмент номера), время, географическая область или перечень рубежей;

доступа к карточкам фактов фотовидеофиксации;

фильтрация фотоматериалов по признакам наличия/отсутствия нарушения ПДД, типу нарушения ПДД;

возможность одновременной выдачи потока фотоматериалов разным потребителям;

мониторинг системы контроля доступа к узлам вычислительных модулей рубежей фотовидеофиксации;

предоставление доступа к живому видео с рубежей, оборудованных камерами видеонаблюдения;

обеспечение конфиденциальности запросов для определенных групп пользователей (в соответствие с определенными нормативными документами и регламентами правами);

3) В части работы с источниками голосовых (медиа) сообщений:

возможность системам регистрации медиа данных выполнять загрузку записей поддерживаемого формата в сервисную платформу с указанием всей необходимой сопроводительной информации (дата и времени, географического местоположения и так далее);

обеспечение конфиденциальности запросов для определенных групп пользователей (в соответствие с определенными нормативными документами и регламентами правами).

4.4.3. Требования к внутреннему и внешнему взаимодействию Сервисной платформы

Сервисная платформа обеспечивает работу с сопрягаемыми системами правоохранительного сегмента и выполнение требований информационной безопасности за счет отделения систем-источников от прикладных автоматизируемых систем.

Таким образом, обеспечивается:

возможность независимого развития систем-источников и систем-потребителей;

возможность использования данных от различных типов систем-источников в общих сценариях независимо реализуемых различными прикладными системами-потребителями;

централизованное управление доступом к ресурсам с возможностью обеспечения анонимного и монопольного доступа к ресурсам АПК "Безопасный город" со стороны правоохранителей в оговоренных регламентами случаях;

возможность выполнения ведомственных требований по защите информации при взаимодействии со смежными системами.

На базе Сервисной платформы обеспечивается информационный обмен со следующими типами автоматизированных систем-источников в области обеспечения общественной безопасности и правопорядка:

системами видеонаблюдения и интеллектуального видеонаблюдения;

системами биометрического анализа;

терминалами экстренной связи;
системами фото-видеофиксации;

4.4.4. Требования к техническому обеспечению Сервисной платформы правоохранительного сегмента

КСА Сервисной платформы базируется на формируемой в рамках АПК "Безопасный город" телекоммуникационной инфраструктуре.

4.4.5. Требования к системному программному обеспечению Сервисной платформы правоохранительного сегмента

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

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

Общее программное обеспечение КСА Сервисной платформы должно удовлетворять требованиям к общему программному обеспечению КСА "Региональная платформа" функционального блока "Координации работы служб и ведомств", представленном в Приложении 3.

Требования к специальному обеспечению КСА Сервисной платформы определяются набором КСА сопрягаемых систем, в том числе составом функциональных возможностей и назначением.

4.4.6. Требования к информационному обеспечению Сервисной платформы

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 Сервисной платформы.

Функции Сервисной платформы обеспечиваются использованием общей системы кодирования и классификации информации.

Единая система кодирования и классификации информации, обеспечиваемая средствами Сервисной платформы, должна обеспечивать:

централизованное ведение словарей и классификаторов, использующихся в информационном взаимодействии;

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

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 систем:

1) Система обеспечения общественной безопасности, правопорядка и профилактики правонарушений на территории муниципального образования в составе КСА следующих подсистем:

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

подсистема экстренной связи;

подсистема обеспечения безопасности охраняемых объектов;

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

подсистема мониторинга объектов инженерной инфраструктуры;

подсистема мониторинга критически-важных и потенциально опасных объектов;

подсистема мониторинга социально значимых объектов;

подсистема мониторинга пожарной безопасности объектов;

подсистема раннего обнаружения лесных пожаров;

подсистема радиационного мониторинга и аварийного реагирования на ЧС с радиационным фактором в населенных пунктах, имеющих радиационно-опасные объекты;

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

подсистема мониторинга состояния сети водоснабжения;

подсистема мониторинга состояния сети водоотведения;

подсистема мониторинга состояния сети газоснабжения;

подсистема мониторинга состояния сети теплоснабжения;

подсистема мониторинга состояния сети электроснабжения;

подсистема мониторинга состояния сети уличного освещения;

4) Система мониторинга дежурного плана города в составе КСА следующих подсистем:

подсистема управления земельным муниципальным реестром;

подсистема управления реестром электросетей;

подсистема управления реестром сетей и сооружений водоснабжения;

подсистема управления реестром тепловых сетей

подсистема управления реестром дорог;

подсистема управления реестром телекоммуникационных сетей;

подсистема управления социальным реестром;

подсистема управления реестром мест обработки и утилизации отходов;

подсистема управления реестром природоохранных и рекреационных зон и паркового хозяйства;

подсистема управления реестром природных ресурсов;

подсистема управления реестром территорий;

5) Система информирования и оповещения населения.

5.2. Назначение и функциональность КСА функционального блока "Безопасность населения и муниципальной (коммунальной) инфраструктуры"

5.2.1. Назначение и функциональность системы обеспечения правопорядка и профилактики правонарушений

Система "Обеспечения правопорядка и профилактики правонарушений на территории муниципального образования" предназначена для решения комплекса задач обеспечения общественной безопасности и правопорядка посредством своевременной идентификации и реагирования на потенциальные угрозы общественной безопасности и нарушений правопорядка.

Система "Обеспечения правопорядка и профилактики правонарушений на территории муниципального образования" создается с учетом требований правоохранительных органов Российской Федерации, в

том числе результатов научно-исследовательских работ МВД России: "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 г.), "Выработка научно-технического и финансового обоснования для принятия решений по созданию системы обеспечения безопасности транспортной инфраструктуры с учетом существующих федеральных программ" (шифр "БТИ"), а также методических рекомендаций по вопросам построения, развития и использования сегментов аппаратно-программного комплекса "Безопасный город".

Основной задачей системы "Обеспечения правопорядка и профилактики правонарушений на территории муниципального образования" является обеспечение возможности предоставления сведений в АПК "Безопасный город"(в том числе и в системы правоохранительного сегмента АПК "Безопасный город") из следующих источников информации:

камеры видеонаблюдения и систем фотовидеофиксации, расположенных в субъекте Российской Федерации;

системы безопасности объектов, включая объекты транспортной инфраструктуры, о происшествиях и тревожных событиях.

Подробные требования к правоохранительному сегменту АПК "Безопасный город" представлены в приложении 24.

Подсистема интеллектуального видеонаблюдения в составе Системы "Обеспечения правопорядка и профилактики правонарушений на территории муниципального образования" должна обеспечивать выполнение следующих функций:

получение видеоизображения с мест установки видеокамер на критически важных, потенциально опасных и социально значимых объектах (в том числе дошкольных образовательных учреждениях, образовательных учреждениях и других);

отображение получаемого с камер видеонаблюдения видеоизображения в режиме реального времени в КСА ЕЦОР (с учетом потребностей ФСБ России и ФСО России);

возможность управления поворотными камерами видеонаблюдения из КСА ЕЦОР и интерфейса АРМ должностных лиц (права доступа и регламент управления согласовывается с ФСБ России и ФСО России);

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 КСА ЕЦОР;

идентификации и распознавания лиц, а также сопоставление их с данными о лицах, находящихся в розыске при наличии информационного обмена;

обнаружение скопления людей;

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 (хаотичных движений большого числа 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, полученных от различных видеокамер, из видеопотока которых был идентифицирован государственный номер транспортного средства.

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

Подсистема экстренной связи в составе системы "Обеспечения правопорядка и профилактики правонарушений на территории муниципального образования" должна обеспечивать выполнение следующих функций:

возможности экстренной связи населения с экстренными оперативными службами посредством специализированных терминалов "гражданин-полиция", тревожных кнопок, иных устройств, устанавливаемых в местах массового скопления людей, социально-

значимых объектах, объектах транспортной инфраструктуры и других объектах;

передачи информации в КСА ЕЦОР о местах установки оконечных, сопрягаемых с подсистемой экстренной связи, терминальных устройств экстренной связи с возможностью индикации активных устройств экстренной связи;

обеспечения голосовой связи и видеосвязи с ДДС территориального органа МВД России или иной уполномоченной службой при поддержке терминальным комплексом данных видов связи;

возможности приема и обработки голосового вызова и видеопотока на специализированное рабочее место КСА ЕЦОР.

Места размещения экстренной связи с полицией должны согласовываться с территориальными органами МВД России на этапах разработки технического задания и рабочей конструкторской документации правоохранительного сегмента АПК "Безопасный город".

5.2.2. Назначение и функциональность системы обеспечения защиты территории от чрезвычайных ситуаций природного и техногенного характера и пожаров

Система "Обеспечения защиты от чрезвычайных ситуаций природного и техногенного характера и пожаров" предназначена 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.

Система "Обеспечения защиты от чрезвычайных ситуаций природного и техногенного характера и пожаров" во взаимодействии с КСА функционального блока "Координация работы служб и ведомств" обеспечивает выполнение следующих функций:

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;

обработка и передача информации в КСА ЕЦОР для решения задач моделирования и прогнозирования развития возможных негативных последствий пожаров, аварий, катастроф и стихийных бедствий, оценки сложившейся и возможной обстановки.

1) подсистема мониторинга объектов инженерной инфраструктуры предназначена для выполнения следующих функций:

мониторинг технического состояния сложных конструкционных сооружений на территории муниципального образования с использованием оконечных устройств: датчиков и контроллеров линейных отклонений, вибраций, иных устройств, обеспечивающих контроль целостности конструкций;

передача информации в КСА ЕЦОР для обработки и анализа статистических данных на предмет возможных отклонений от ключевых значений.

2) подсистема мониторинга критически-важных и потенциально опасных объектов обеспечивает выполнение следующих функций:

непрерывный автоматизированный мониторинг подсистем жизнеобеспечения и безопасности объектов, а также инженерно-технических конструкций потенциально-опасных объектов, включая сбор и обработку оперативной информации о состоянии технологических систем и изменении состояния инженерно-технических конструкций объекта;

автоматизированный мониторинг работы ключевых технологических узлов потенциального опасного объекта на предмет критических отклонений от ключевых параметров работы, грозящих возникновением ЧС;

передача информации в КСА ЕЦОР для обработки и анализа статистических данных на предмет возможных отклонений конструкционных сооружений, а также работы технологических узлов и потенциально-опасного объекта от ключевых значений.

3) подсистема мониторинга критически-важных и потенциально опасных объектов обеспечивает выполнение следующих функций:

интеллектуальное видеонаблюдение за объектом с применением средств видеоанализа и биометрических систем;

обеспечение автоматизированного контроля доступа в охраняемые помещения объекта;

мониторинг состояния работы объектовых систем жизнеобеспечения;

мониторинг состояния пожарной безопасности на объекте охраны;

сбор и передача информации в КСА ЕЦОР для обработки на предмет критических отклонений контролируемых показателей работы систем жизнеобеспечения, пожарной опасности, а также выявленных автоматизированной системой контроля доступа, средствами видеоанализа и биометрического контроля нарушений в режиме доступа на охраняемый объект.

4) подсистема обеспечения пожарной охраны обеспечивает непрерывный мониторинг состояния пожарной безопасности на объекте мониторинга и передачу в КСА ЕЦОР и сопрягаемую АСОДУ дежурной пожарной части случаев срабатывания датчиков систем пожарной охраны с информацией о местоположении датчика.

5) подсистема раннего обнаружения лесных пожаров обеспечивает выполнение следующих функций:

фиксация угроз лесных пожаров с использованием интегрированных средств видеонаблюдения и видеоаналитики, тепловизоров и иных устройств, обеспечивающих раннее обнаружение лесных пожаров;

передача информации о детектированном возгорании в КСА ЕЦОР и АСОДУ дежурной пожарной части с указанием местоположения устройств зафиксировавших возгорание, а также расчетного местоположения возгорания.

6) подсистема радиационного мониторинга и аварийного реагирования на ЧС с радиационным фактором в населенных пунктах, имеющих радиационно-опасные объекты, обеспечивает выполнение следующих функций:

осуществление непрерывного автоматизированного контроля радиационной обстановки на территории населенного пункта;

осуществление непрерывного автоматизированного контроля отдельных параметров метеорологической обстановки;

сбор и оперативная передача информации в КСА ЕЦОР для обработки на предмет превышения контролируемых параметров радиационной обстановки установленных пороговых значений;

оценка и прогнозирование радиационной обстановки и радиологических последствий в зоне загрязнения на территории населенного пункта, а также выработка консолидированных рекомендаций по эффективным мерам реагирования на ЧС с радиационным фактором.

Требования к подсистеме радиационного мониторинга и аварийного реагирования на ЧС с радиационным фактором представлены в Приложении 22.

5.2.3. Назначение и функциональность системы обеспечения безопасности инфраструктуры жилищно-коммунального комплекса

Система обеспечения безопасности инфраструктуры жилищно-коммунального комплекса предназначена для мониторинга потенциальных угроз системам жизнеобеспечения муниципального образования, в том числе контроля технического состояния и работы муниципальной коммунальной инфраструктуры, а также координации работ по предупреждению и ликвидации последствий происшествий, вызванных сбоями в работе муниципальной коммунальной инфраструктуры.

В состав системы обеспечения безопасности инфраструктуры жилищно-коммунального комплекса входят следующие функциональные подсистемы:

подсистема мониторинга состояния сети водоснабжения;

подсистема мониторинга состояния сети водоотведения;

подсистема мониторинга работе состояния сети газоснабжения;

подсистема мониторинга состояния сети теплоснабжения;

подсистема мониторинга состояния сети электроснабжения;

подсистема мониторинга состояния сети уличного освещения;

подсистема диспетчеризации поддержки принятия решений по предупреждению и ликвидации кризисных ситуаций и происшествий в сфере ЖКХ.

1) подсистема мониторинга состояния сетей водоснабжения обеспечивает выполнение следующих функций:

сбор и обработку информации с систем АСУТП, счетчиков, датчиков и телеконтроллеров о параметрах работы элементов сети водоснабжения, включая показатели давления, расхода и температуры воды, показатели давления и технические параметры работы скважного и поверхностного водозабора, насосных станций (НС) 1..3 подъемов, водонапорных башен (ВНБ) и резервуаров чистой воды (РЧВ), иных сооружений водопроводной системы;

мониторинг и анализ технико-экономических параметров работы системы на основе информации счетчиков расхода воды, датчиков давления и температуры, контроллеров и сопрягаемых АСКУЭ о фактических объемах поставленной воды, фактических расходах

потребленной воды (собственные нужды и отдельно по потребителям), потребленной оборудованием электроэнергии (насосные агрегаты, отопление, освещение);

формирование уведомлений для ДДС и ЕДДС о критических нарушениях в работе оборудования скважного и поверхностного водозабора, насосных станций 1..3 подъемов, водонапорных башен и резервуаров чистой воды, иных сооружений водопроводной системы, фиксируемых счетчиками, датчиками и телеконтроллерами, а также срабатывании пожарной и охранной сигнализации, отключения фидеров электроснабжения, датчиков затопления и перелива;

отображение местоположения на картографической подоснове элементов сети водоснабжения, скважного и поверхностного водозабора, насосных станций 1..3 подъемов, водонапорных башен и резервуаров чистой воды, колодцев, гидрантов, камер, запорной-регулирующей арматуры, иных сооружений водопроводной системы с выводом информации о параметрах их работы, фиксируемых установленными счетчиками, датчиками и телеконтроллерами;

ведение паспортов элементов сети водоснабжения;

осуществление гидравлического расчета и моделирования водопроводных сетей произвольной размерности, с несколькими источниками, работающими на общую сеть, в том числе с учетом графиков суточной неравномерности;

моделирование переключений запорно-регулирующей арматуры, скважных водозаборов, насосных агрегатов, водонапорных башен и резервуаров чистой воды;

создание и администрирование модельных баз для многовариантных расчетов;

построение пьезометрических графиков, в том числе сравнительных;

анализ режимов работы скважного и поверхностного водозабора, насосных станций 1..3 подъемов, водонапорных башен и резервуаров чистой воды, иных сооружений водопроводной системы.

2) подсистема мониторинга состояния сети водоотведения обеспечивает выполнение следующих функций:

сбор и обработку информации с систем АСУТП, электросчетчиков и счетчиков сточных вод, датчиков давления и уровня, контроллеров о параметрах работы элементов сети водоотведения, включая индикацию протечек и подтоплений, засоров, показатели давления и технические

параметры работы канализационных насосных станций (КНС), очистных сооружений, резервуаров и иных сооружений системы водоотведения;

формирование уведомлений для ДДС и ЕДД о критических нарушениях в работе системы водоотведения, фиксируемых счетчиками, измерительными датчиками и контроллерами, датчиками охранной и пожарной сигнализации;

отображение местоположения на картографической подоснове канализационных насосных станций, очистных сооружений, резервуаров, элементов запорно-регулирующей арматуры, колодцев, камер, коллекторов и иных сооружений системы водоотведения, с выводом информации о параметрах работы ее технологических узлов, фиксируемых установленными датчиками, контроллерами и счетчиками;

мониторинг и анализ технико-экономических параметров работы системы на основе информации счетчиков, датчиков, контроллеров и сопрягаемых АСКУЭ о фактических объемах стоков, затраченной электроэнергии, отработанного ресурса насосных агрегатов, объема потребленной холодной воды на собственные нужды;

ведение паспортов элементов сети водоотведения с детализацией оборудования узлов (внутреннее оборудование колодцев и камер, коллекторов, канализационных насосных станций и иных сооружений системы водоотведения);

ведение детализированных схем водоотведения (указанием элементов запорно-регулирующей арматуры, насосных агрегатов) с привязкой объектов (зданий и сооружений) к узлам системы водоотведения (насосным станциям);

автоматическое определение дерева стоков (зоны канализования) для произвольного узла сети водоотведения, в том числе для точки засора, с формированием графического выделения и отчета по сформированной зоне канализования;

анализ режимов работы канализационных насосных станций и очистных сооружений.

3) подсистема мониторинга состояния сети газоснабжения обеспечивает выполнение следующих функций:

сбор и обработку информации с систем АСУТП, газовых счетчиков, датчиков и контроллеров о параметрах работы элементов газораспределительной сети, включая индикацию утечек (с использованием газоанализаторов и иного оборудования), показатели давления и температуры, технические параметры работы

газорегуляторных пунктов (ГРП и ГРПШ), газорегуляторных установок (ГРУ), станций катодной защиты (СКЗ) и иных сооружений газораспределительной системы;

формирование уведомлений для ДДС и ЕДД о критических нарушениях в работе газовой системы, срабатывания отсечного и сбросного клапана, возможных утечках газа, фиксируемых датчиками и контроллерами, а также срабатывании пожарной сигнализации и охранных систем;

мониторинг и анализ технико-экономических параметров работы системы на основе информации счетчиков, датчиков, контроллеров и сопрягаемых АСКУЭ о фактических объемах поставленного газа и фактических расходах потребленного газа;

отображение местоположения на картографической подоснове газорегуляторных пунктов, газорегуляторных установок, станций катодной защиты, диктующих точек и других элементов газораспределительной сети на картографической подложке с указанием актуальных параметров их работы (давлении и температуре, энергопотреблении, состоянии запорной аппаратуры, охранной и пожарной сигнализации, технических характеристиках, режимах работы);

ведение информационной паспортизации объектов;

гидравлический расчет разветвленных и кольцевых газораспределительных и газотранспортных сетей высокого, среднего и низкого давления произвольной размерности, с несколькими источниками, работающими на общую газовую сеть;

моделирование переключений запорно-регулирующей арматуры;

создание и администрирование модельных баз для многовариантных расчетов;

построение пьезометрических графиков (профилей давления), в том числе сравнительных;

групповые изменения характеристик нагрузок по заданным критериям;

групповые изменения характеристик участков по заданным критериям (калибровочный инструментарий);

выдача рекомендаций по закрытию запорной арматуры в узлах сети с целью полной или частичной (от источников) локализации аварийного участка газораспределительной сети, с учетом критериев доступности и исправности арматуры, с генерацией отчетов о локализуемой области и отключаемых нагрузках.

4) подсистема мониторинга состояния сети теплоснабжения обеспечивает выполнение следующих функций:

сбор и обработку информации с систем АСУТП, датчиков расхода, температуры и давления, телеконтроллеров о параметрах работы элементов тепловой сети, включая индикацию протечек на трубопроводной сети и падения температуры на трубопроводе, утечек газа на газовых котельных, процент остатка резервного топлива котельной, показатели давления в котлах и трубопроводной сети, технические параметры работы котельных, центральных и индивидуальных тепловых пунктов, иных сооружений системы теплоснабжения;

формирование уведомлений для ДДС и ЕДД о критических нарушениях в работе системы теплоснабжения, возможных утечках газа на газовых котельных, остановке работы котлов и насосов, пропадании напряжения электропитания на любом из фидеров, утечках теплоносителя, фиксируемых различными датчиками и телеконтроллерами, а также срабатывании пожарной и охранной сигнализации;

мониторинг и анализ технико-экономических параметров работы системы на основе информации датчиков, телеконтроллеров и сопрягаемых АСКУЭ о фактических объемах поставленного ресурса и фактических расходах на затрачиваемые ресурсы, объема потребленного топлива котельной, фактического объема утечек теплоносителя, учет ресурсной наработки котлов и электрооборудования, определение коэффициента полезного действия теплового пункта, оценка эффективности работы котельной с учетом температуры отходящих газов котлов, оценка коэффициента удельной теплоты сгорания топлива;

отображение местоположения на картографической подоснове элементов тепловой сети, котельных, центральных и индивидуальных тепловых пунктов, диктующих точек, тепловых камер на картографической подложке с указанием актуальных параметров их работы (давлении и температуры, энергопотреблении котельных, технических характеристиках, режимах работы);

ведение информационной паспортизации объектов;

теплотехнический расчет многокольцевых тепловых сетей произвольной размерности, с несколькими источниками, работающими на общую сеть;

моделирование переключений запорно-регулирующей арматуры, котлов и насосных агрегатов;

создание и администрирование модельных баз для многовариантных расчетов;

построение пьезометрических графиков, в том числе сравнительных;

анализ режимов работы котельных, центральных и индивидуальных тепловых пунктов в ручном, автоматическом (по погодозависимому и годовому графику теплоснабжения);

анализ гидравлической разбалансировки тепловой сети после центрального теплового пункта на вводах многоквартирных домов;

расчет нормативных и фактических тепловых потерь через изоляцию в соответствии с Порядком расчета и обоснования нормативов технологических потерь при передаче тепловой энергии", утвержденного приказом Минпромэнерго России от 4 октября 2005 г. № 265;

расчет численных показателей надежности теплоснабжения потребителей тепла в соответствии с методическими рекомендациями по разработке схем теплоснабжения", утвержденными приказом Минэнерго России и Минрегиона России от 29 декабря 2012 г. № 565/667.

Требования к подсистеме контроля и управления работой газовых котлов и оборудованием тепловых сетей указаны в Приложении 15.

5) подсистема мониторинга состояния сети электроснабжения обеспечивает выполнение следующих функций:

сбор и обработка информации с систем АСУТП, электросчетчиков, датчиков и контроллеров, микропроцессорных блоков релейной защиты и автоматики о параметрах работы элементов электросети, включая технические параметры работы подстанций и распределительных пунктов;

отображение местоположения на картографической подоснове элементов электросети, подстанций и распределительных пунктов на картографической подложке с указанием актуальных параметров их работы (напряжении и тока, технических характеристиках, режимах работы);

мониторинг и анализ технико-экономических параметров работы системы на основе информации с датчиков и контроллеров, сопрягаемых АСКУЭ о фактических объемах поставленной электроэнергии, фактических расходах потребленной электроэнергии (собственные нужды, лифтовое хозяйство, отдельно по потребителям);

формирование уведомлений для ДДС и ЕДД о критических нарушениях в работе энергосистемы, перекосах фаз, обрывах нейтрали, отключениях абонентов, срабатывания автоматического ввода резерва (АВР) и аппаратуры автоматического повторного включения (АПВ),

фиксируемых датчиками и контроллерами, а также срабатывании пожарной сигнализации и охранных систем на подстанциях и распределительных пунктах;

ведение паспортов оборудования узлов (внутреннее оборудование подстанций и распределительных пунктов, категория энергоснабжения), опор и линий электропередач;

расчет потерь электроэнергии в элементах сети, баланса активной и реактивной мощности;

расчет и анализ установившихся токов и падений напряжения, токов короткого замыкания в сетях, подстанциях и распределительных пунктах;

расчет и анализ степени нагруженности и резерва пропускной способности линий электропередач, построение профилей падения напряжения, в том числе сравнительных для различных режимов нагруженности;

моделирование переключений коммутирующего оборудования на подстанциях и распределительных пунктах;

создание и администрирование модельных баз для многовариантных расчетов.

б) подсистема мониторинга состояния сети уличного освещения обеспечивает выполнение следующих функций:

сбор и обработка информации от систем АСУТП, шкафов управления, непосредственно со светильников о параметрах работы элементов сети городского освещения с использованием существующих силовых линий и беспроводных каналов связи;

формирование уведомлений для ДДС и ЕДД о критических нарушениях в работе системы, отключениях освещения, местах обрывов линий электропитания, фиксируемых контроллерами шкафов управления;

мониторинг и анализ технико-экономических параметров работы системы на основе информации со счетчиков электроэнергии, контроллеров и сопрягаемых АСКУЭ о фактических объемах потребляемой электроэнергии, учет процента негорения ламп и их ресурса, прогнозирование момента выхода светильника из работы;

отображение местоположения на картографической подоснове трансформаторных подстанций, шкафов управления, осветительных приборов и элементов иллюминации на картографической подложке с указанием актуальных параметров их работы (энергопотреблении, технических характеристиках, режимах работы);

ведение информационной паспортизации объектов;

расчет оптимальных режимов работы городской осветительной сети с возможностью управление уровнем освещенности (диммирование) в соответствии с СП 52.13330.2011 "Естественное и искусственное освещение";

адресное управление работой светильниками и элементами иллюминации в ручном, дистанционном и автоматическом режиме (по заданному графику или командам с передающих устройств, подключенных к фотореле).

7) подсистема диспетчеризации и поддержки принятия решений по предупреждению и ликвидации кризисных ситуаций и происшествий в сфере ЖКХ обеспечивает выполнение следующих функций:

прием, обработка и регистрация вызовов населения по коммунально-бытовым вопросам;

формирование регистрационных карточек события и ремонтных заявок;

ведение диспетчерских журналов заявок на плановые и аварийные ремонтно-восстановительные работы;

контроль текущего состояния заявок по этапам их жизненного цикла;

привязка заявок к графическому представлению сетей на плане местности в семантической связи с паспортами объектов;

ведение журнала повреждений с привязкой к заявкам;

ведение журналов использования бригад, материалов, машин и механизмов;

статистическая обработка и анализ журналов;

графическая визуализация мест повреждений и дефектов по данным архива заявок и повреждений;

обработка и консолидация информации по паспортам элементов системы ЖКХ муниципального образования, данных поступающих из систем АСУТП, а также датчиков и контроллеров о параметрах работы систем ЖКХ;

отображение местоположения контрольных устройств систем мониторинга инфраструктуры ЖКХ на картографической подложке с указанием актуальных параметров их работы, статистики, технических характеристиках, режимах работы;

предоставление отчетно-аналитической информации по работе систем ЖКХ на территории города.

5.2.4. Назначение и функциональность системы управления дежурным планом города

Подсистема управления дежурным планом города обеспечивает выполнение следующих функций:

1) ведение совокупного электронного плана города с учетом семантических связей с существующими геоинформационными ресурсами, используемыми городскими службами, при условии наличия унифицированных форматов обмена данными между системами, единой картографической подосновы, единой системы координат;

2) прием электронных документов (по согласованному шаблону) об изменениях на дежурных планшетах города с предоставлением возможности занесения семантической информации;

3) автоматизация процессов по предоставлению выписок из генерального плана территории структур, осуществляющих строительную деятельность;

4) обеспечение поддержки принятия решений при управлении муниципальными активами, включая планирование ремонтных работ и обслуживания, планирование застройки и переноса объектов, моделирование возможных ситуаций при застройке территорий и прокладке инфраструктуры;

5) мониторинг и профилактика безопасности в социальной сфере, на основе специализированных информационных слоев, обеспечивающих визуализацию статистической информации в разрезе правоохранительного сегмента, сегмента защиты населения и территорий от ЧС природного и техногенного характера, здравоохранения, экологической обстановки, экономической деятельности (ремонтных и капитальных расходов в привязке к целевым объектам), иных информационно-аналитических слоев;

6) ведение реестров объектов капитального строительства с указанием расположения внутренних инженерных коммуникаций, технических условий по различным видам инженерного обеспечения объектов капитального строительства и земельных участков;

7) ведение реестров и паспортов элементов электросетей, трасс линий электропередачи и энергетического хозяйства;

8) ведение реестров и паспортов сетей и сооружений водоснабжения;

9) ведение реестров и паспортов элементов тепловых сетей;

10) ведение реестров и паспортов элементов дорожной сети;

11) ведение реестров телекоммуникационной сети;

12) ведение социального реестра и паспортов объектов социальной сферы, включая детские дошкольные учреждения, школы, лечебно-профилактические учреждения, спортивные учреждения, базы отдыха.

13) ведение реестров мест обработки и утилизации отходов;

14) ведение реестров природоохранных и рекреационных зон и паркового хозяйства в составе пространственной и паспортной информации об особо охраняемых территориях, зеленых насаждениях, парках и рекреационных зонах.

5.2.5. Назначение и функциональность системы информирования и оповещения

Подсистема информирования и оповещения обеспечивает выполнение следующих функций:

1) прием, обработка и воспроизведение сигналов оповещения, передаваемых из КСА ЕЦОР;

2) прием, обработка и воспроизведение сигналов оповещения, передаваемых КСЭОН;

3) отображение на картографической подложке установленных средств оповещения и вывод информации о техническом состоянии;

4) передача голосовых и речевых трансляций при помощи громкоговорящих устройств оповещения;

5) воспроизведение текстовых сообщений в виде речевых трансляций посредством громкоговорящих устройств оповещения;

6) активация всех оконечных средств информирования и оповещения населения;

7) воспроизведение текстовых и мультимедийных трансляций на устройствах, передающих графическое изображение (бегущие строки, дисплеи, и терминалы);

8) воспроизведение голосовых сообщений с использованием домофонов;

9) воспроизведение голосовых сообщений с использованием телефонной связи.

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

Внутреннее и внешнее взаимодействие подсистемы функционального блока "Безопасность населения и муниципальной

(коммунальной) инфраструктуры" обеспечивается средствами подсистемы интеграции данных, входящей в состав КСА ЕЦОР, на базе которой выстраивается информационное взаимодействие всех элементов АПК "Безопасный город". При этом подсистема интеграции данных может быть использована отдельно от других подсистем КСА ЕЦОР в составе других функциональных блоков, в качестве базовой платформы обеспечения электронного обмена информацией.

Взаимодействие КСА подсистем функционального блока "Безопасность населения и муниципальной (коммунальной) инфраструктуры" осуществляется на основе стандартов на архитектуру построения системных сервисов (служб) и взаимно-совместимых приложений (стандарты типа ONVIF, 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 системами смежных функциональных блоков должно осуществляться на основе стандартизированных открытых протоколов;

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

все сетевые видеокамеры или кодеры (преобразователи аналогового сигнала в цифровой) должны поддерживать отраслевой стандарт, определяющий протоколы взаимодействия - ONVIF версии 1.02 и 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 Системы обеспечения правопорядка и профилактики правонарушений

Система 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 и стандартизированными протоколами.

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

КСА автоматизированных систем, входящих в систему 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 системы 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 платформы должно также обеспечиваться информационно-программное сопряжение системы 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 г. № 195, распоряжение Правительства Российской Федерации от 4 августа 2011 г. № 1391-р);

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

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

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

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

государственной автоматизированной информационной системы "ЭРА-ГЛОНАСС" (Федеральный закон от 28 декабря 2013 г. № 395-ФЗ, распоряжение Правительства РФ от 9 августа 2014 г. № 1498-р).

5.3.3. Требования к внутреннему и внешнему взаимодействию Системы 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 получения с использованием стандартизированных протоколов информационного обмена данными о критичных нарушениях в работе систем жизнеобеспечения и коммунальных систем, а также статистической информации о работе систем жилищно-коммунального комплекса.

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

Размещенные на территории муниципального образования средства мониторинга и контроля угроз, интегрируемые в контур информационного обмена АПК "Безопасный город", должны поддерживать стандартизованные протоколы электронного информационного обмена.

Средства вычислительной техники должны быть максимально приспособлены для последующей модернизации.

Активное сетевое оборудование должно обеспечивать достаточную пропускную способность для функционирования систем 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 в режиме 24/7 (ежедневно и круглосуточно). Для участков сети, требующих повышенную надежность, необходимо предусмотреть резервные каналы связи.

Для линий связи проходящих через общедоступные помещения и линий связи соединения с сетью Интернет должны использоваться средства шифрования трафика при передаче по таким линиям связи информации, к которой предъявляются требования по обеспечению конфиденциальности.

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 АПК "Безопасный город" не должно существовать ни одного территориально компактного элемента, отказ или разрушение которого выводил бы из строя все системы комплекса.

Устройства обеспечения электронной связи и приема сигналов тревоги от граждан на транспорте должны соответствовать требованиям приказа Минтранса России от 31 июля 2012 г. № 285 "Об утверждении требований к средствам навигации, функционирующим с использованием навигационных сигналов системы ГЛОНАСС или ГЛОНАСС/GPS и предназначенным для обязательного оснащения транспортных средств категории M, используемых для коммерческих перевозок пассажиров, и категории N, используемых для перевозки опасных грузов" и подключены к системе экстренной связи на транспортных средствах.

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 (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 том числе купольного исполнения.

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

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

Системы 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 системы 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 16.

Технические требования к системе видеонаблюдения представлены в Приложении 17.

5.5. Требования к системному программному обеспечению КСА функционального блока "Безопасность населения и муниципальной (коммунальной) инфраструктуры"

Системы функционального блока "Безопасность населения и муниципальной (коммунальной) инфраструктуры" представляет собой совокупность общего программного обеспечения и специального программного обеспечения.

Система функционального блока "Безопасности населения и муниципальной (коммунальной) инфраструктуры" строится на открытой, компонентной (модульной) архитектуре, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в состав систем "Безопасности населения и муниципальной (коммунальной) инфраструктуры" перспективных КСА.

Программное обеспечение должно быть сертифицировано по требованиям безопасности информации.

Требования к общему программному обеспечению систем функционального блока "Безопасности населения и муниципальной (коммунальной) инфраструктуры" должны соответствовать требованиям к общему программному обеспечению, представленным в приложении 3.

Требования к специальному обеспечению подсистем систем функционального блока "Безопасность населения и муниципальной (коммунальной) инфраструктуры" должно быть аналогичны требованиям к специальному программному обеспечению КСА "Региональная платформа" функционального блока "Координации работы служб и ведомств", представленных в приложении 4.

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

Требования к информационному обеспечению КСА "Безопасность населения и муниципальной (коммунальной) инфраструктуры" должны быть аналогичны требованиям к информационному обеспечению КСА "Региональная платформа" функционального блока "Координация работы служб и ведомств" представленных в разделе 4.2.6 "Требования к информационному обеспечению КСА "Региональная платформа" функционального блока "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 систем АПК "Безопасный город":

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

подсистема фотовидеофиксации событий (правонарушений) на дорогах (ФВФ);

подсистема весогабаритного контроля (ВГК);

подсистема контроля и управление мобильным персоналом ДДС.

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

интеллектуальная транспортная система (ИТС);

автоматизированная система управлением дорожным движением (АСУДД):

автоматизированная система управления техническими средствами регулирования и организации дорожного движения (АСУТСР и ОДД);

автоматизированная система информирования участников дорожного движения (АСИУДД);

автоматизированная система мониторинга параметров транспортных потоков (АСМПТП);

автоматизированная система наружного освещения (АСУНО);

подсистема учета технические средства регулирования дорожного движения (ТСРДД) и технические средства организации дорожного движения (ТСОДД).

система телеобзора (СТ);

система парковочного пространства (АСКПП);

система экстренной связи (ЭС).

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

подсистема мониторинга объектов транспортной инфраструктуры (СМОТИ);

подсистема дорожного метеорологического обеспечения (СДМО);

подсистема мониторинга и позиционирования общественного транспорта (СМПОТ);

подсистема управления движением общественного транспорта (СУДОТ);

подсистема информирования населения на транспортных средствах и объектах транспортной инфраструктуры.

6.2. Назначение и функциональность КСА функционального блока "Безопасность на транспорте"

6.2.1. Назначение и функциональность системы обеспечения правопорядка, профилактики правонарушений на дорогах

Система обеспечения правопорядка, профилактики правонарушений на дорогах предназначена 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 состав системы обеспечения правопорядка, профилактики правонарушений на дорогах входят следующие функциональные подсистемы:

1) фото-видеофиксация (ФВФ) нарушений ПДД, предназначенная для решения следующих задач:

снижения совершаемых участниками дорожного движения нарушений правил дорожного движения;

общего снижение аварийности;

сведения к минимуму роли "человеческого фактора", имеющего место при общении сотрудников ГИБДД с участниками дорожного движения;

повышения эффективности в ходе проведения подразделениями МВД России, специальными службами и другими силовыми структурами специальных мероприятий.

Аппаратно-программные средства ФВФ должны обеспечивать:

автоматическое выявление нарушений правил дорожного движения и передачу данных в центр обработки данных, при этом допускается использование облачных технологий для предобработки и хранения данных;

автоматический контроль соблюдения специального пропускного режима (контроль за движением грузового и специального транспорта);

мониторинг транспортных потоков, автоматическое формирование и передача данных в систему мониторинга параметров транспортных потоков;

автоматическая проверка транспортных средств по существующим информационным базам;

осуществление оперативно-розыскных мероприятий;

удаленная диагностика оборудования;

создание и ведение базы данных нарушений правил дорожного движения.

Технические требования к источникам фото-видеофиксации приведены в Приложении 18.

2) весогабаритный контроль (ВГК), предназначенный для реализации функций весового и габаритного контроля посредством специализированного оборудования и программного обеспечения пунктов весогабаритного контроля транспортных средств (ТС), которые обеспечивают мониторинг и контроль ТС, как в динамическом режиме

(измерение осуществляется без снижения скорости транспортного средства), так и в статическом.

Подсистема весогабаритного контроля (ВГК) предназначена для решения следующих задач:

обеспечения сохранности автомобильных дорог и повышения транспортной безопасности на автомобильном транспорте;

выявления нарушений действующего законодательства РФ в сфере дорожного движения, нарушений перевозок крупногабаритных и/или тяжеловесных грузов на автомобильном транспорте.

Аппаратно-программные средства ВГК должны обеспечивать:

сбор данных о соблюдении установленных действующим законодательством Российской Федерации ограничениях в области перевозки крупногабаритных и (или) тяжеловесных грузов;

автоматическое выявление нарушений в области перевозки крупногабаритных и (или) тяжеловесных грузов, и передачу данных в центр обработки данных, контрольно-надзорные органы, в том числе ГИБДД и Минтранс России, при этом допускается использование облачных технологий для предобработки и хранения данных;

удаленная диагностика оборудования;

создание и ведение базы данных нарушений перевозок крупногабаритных и/или тяжеловесных грузов на автомобильном транспорте.

Подсистема ВГК должен быть интегрирован с системами Росавтодора "Выдача специальных разрешений на автомобильную перевозку крупногабаритных и (или) тяжеловесных грузов" с целью выявления наличия специального разрешения на перевозку конкретным транспортным средством крупногабаритного и (или) тяжеловесного груза.

3) контроль и управление мобильным персоналом, подсистема предназначена для автоматизации процессов подготовки и планирования дежурного мобильного персонала и ТС и повышения эффективности использования сил и средств при выполнении своих должностных и функциональных обязанностей с целью сокращения времени реагирования на КСП.

Аппаратно-программные средства подсистемы контроля и управления мобильным персоналом должны обеспечивать:

планирование работы мобильного персонала служб, ДДС и транспорта;

управление нарядами (дежурными ремонтными бригадами и иными дежурными службами);

контроль сил и средств;

сбор и отображение на карте оперативной обстановки по местоположению персонала и ТС с использованием средств ГЛОНАСС/GPS;

регистрацию происшествий с использованием систем ЭРА-ГЛОНАСС или аналогичных систем экстренного реагирования на аварии;

передачу информации о происшествиях с персоналом контролируемыми транспортными средствами в профильные ДДС и КСА ЕЦОР для реагирования на происшествия;

составление отчетности, сопровождающей процессы планирования.

6.2.2. Назначение и функциональность Системы обеспечения безопасности дорожного движения

Система обеспечения безопасности дорожного движения предназначена для решения задач управления транспортными потоками и обеспечения эффективного взаимодействия различных служб и организаций муниципального образования в сфере организации и обеспечения безопасности дорожного движения.

В состав системы обеспечения безопасности дорожного движения входят следующие функциональные подсистемы:

1) Интеллектуальная транспортная система (ИТС), предназначенная для решения следующих задач:

эффективное управление транспортными потоками;

обеспечения оперативного реагирования и взаимодействия специальных (МВД России, МЧС России, Минздрав России) и коммунальных городских служб при возникновении чрезвычайных ситуаций на улично-дорожной сети (УДС);

оптимизации движения общественного транспорта и повышения качества пассажирских перевозок;

обеспечения информированности участников движения о складывающейся дорожно-транспортной ситуации и вариантах оптимального маршрута движения;

предоставления должностным лицам, органам государственной власти, местного самоуправления необходимой информации, касающейся транспортного обслуживания и дорожного движения.

Основными функциями ИТС являются:

мониторинг дорожного движения (сбор сведений о параметрах транспортных потоков, телеобзор с функцией автоматического выявления инцидентов, метеорологический контроль, сбор сведений о наличии парковочных мест);

навигационно-информационный сервис на основе системы позиционирования (контроль движения пассажирского и специального транспорта, автотранспорта служб городского хозяйства, передача информации на абонентские мобильные электронные устройства, функционирование географического информационного ресурса);

автоматизированное управление транспортными потоками (координированное управление светофорными объектами на магистралях, координированное управление светофорными объектами на отдельных участках УДС, введение оперативных изменений в организацию движения на отдельных участках УДС с помощью управляемых дорожных знаков):

информирование участников дорожного движения (вывод текстовой и графической информации о складывающейся дорожно-транспортной обстановке на различные информационные табло, устанавливаемые на УДС и на периферийное (пользовательское) оборудование системы позиционирования, вывод информации о наличии свободных парковочных мест, функционирование call-центра, передача информации с помощью интернет-сайтов и средств массовой информации);

диспетчеризация (реализация полномочий и функций ГИБДД по регулированию движения транспорта в городе, единый общегородской диспетчерский центр управления наземным пассажирским транспортом, управление движением специального транспорта, управление движением транспорта служб городского хозяйства, управление мобильными нарядами и экипажами специальных служб, диспетчерские службы по управлению движением).

информационное обеспечение оперативного реагирования и взаимодействия специальных служб (ГИБДД МВД России, МЧС России, служб скорой помощи), а также коммунальных городских служб при возникновении чрезвычайных ситуаций на УДС;

предоставление руководителям всех уровней необходимой информации, касающейся транспортного обслуживания и дорожного движения, для принятия оперативных и стратегических решений в сфере транспорта.

2) Автоматизированная система управлением дорожным движением (АСУДД), предназначенная для решения следующих задач:

автоматическое управление движением транспортных потоков на улично-дорожных сетях городов, муниципальных образований, транспортных магистралях;

автоматическое управление движением транспорта на улично-дорожной сети города в штатных ситуациях;

оперативное диспетчерское управление движением транспорта при возникновении инцидентов и в других нештатных ситуациях;

автоматическое определение нештатных ситуаций по заданным параметрам;

построение алгоритмов движения транспорта;

организация маршрутов движения транспортных средств;

организация маршрутов движения специализированных и специальных транспортных средств (включая маршруты объезда и подвода специализированной техники для ликвидации последствий КСП).

Основными функциями АСУДД являются:

минимизация общих потерь, возникающих при движении транспортных средств на УДС города;

организация и управление движением при возникновении чрезвычайных ситуаций;

повышение безопасности участников дорожного движения;

снижение эксплуатационных расходов на перевозку грузов и пассажиров, в т.ч. расхода горюче-смазочных материалов;

снижение экологически вредоносного воздействия на окружающую среду;

уменьшение общей эмоциональной и психофизической нагрузки водителей и повышение комфортабельности поездок;

получение информации о дорожно-транспортной ситуации на УДС;

сокращение времени поездки общественным, личным и грузовым транспортом;

максимизация пропускной способности УДС;

организация и управление движением при возникновении КСП;

повышение безопасности участников дорожного движения;

сдерживание объемов выбросов загрязняющих веществ от автотранспорта.

Состав функциональных модулей АСУДД формируется следующими подсистемами:

1) автоматизированное управление техническими средствами регулирования и организации дорожного движения, обеспечивающее:

диспетчерское управление с измененными параметрами планов координации (ПК);

выбор ПК диспетчером;

автоматический выбор ПК по календарному расписанию;

включение участков "зеленых улиц".

автоматический выбор ПК по измеренным параметрам транспортных потоков;

автоматический выбор ПК по прогнозу развития транспортной ситуации (прогноз должен строиться соответствующим алгоритмом автоматизированной системы мониторинга параметров транспортных потоков).

2) оповещение участников дорожного движения, в том числе с применением следующих функций:

информирование участников дорожного движения об оперативной обстановке на дороге, о состоянии движения - заторах, пробках, плохих дорожных условиях и т.д. с использованием табло и управляемых дорожных знаков;

обеспечение участников дорожного движения оперативной информацией экстренного характера о происходящих КСП;

вывод оперативной информации (текстовой информации, предупреждающих и запрещающих знаков);

самодиагностика работоспособности комплексов.

3) мониторинг параметров транспортных потоков, обеспечивающий выполнение следующих функций:

получение информации о состоянии транспортных потоков, как в текущий момент, так и о периодически повторяющихся проблемах на основе анализа статистических данных;

прогнозирование заторов в случае планируемого закрытия определенных улиц, проведения мероприятий с целью предоставления рекомендаций по оптимальному распределению движения транспортных потоков;

верификация и оценка распределения транспортных потоков по альтернативным маршрутам;

выработка маршрутов и ограничений движения для определенных типов транспортных средств;

обнаружение транспортных средств в зоне контроля по каждой полосе движения (при технической возможности периферийного оборудования);

измерение общего количества транспортных средств, прошедших по каждой полосе за заданный период времени (при технической возможности периферийного оборудования);

измерение средней скорости движения транспортного потока по полосе за определенный период (при технической возможности периферийного оборудования);

определение усредненного значения занятости в зонах контроля по полосам за определенный период (при технической возможности периферийного оборудования);

классификация транспортных средств;

автоматическое определение нештатных ситуаций (ДТП, предзатор, затор и т.д.);

прогнозирование развития транспортной ситуации;

расчет времени проезда по заданному маршруту.

4) управление наружным освещением, обеспечивающее выполнение следующих функций:

обеспечение оперативного автоматизированного централизованного управления наружным освещением населенных пунктов, промышленных объектов и автомагистралей;

обеспечение контроля наружным освещением населенных пунктов, промышленных объектов и автомагистралей;

возможность включения - отключения освещения в автоматическом, дистанционном и ручном режимах;

измерение, учет и контроль потребления электрической энергии по каждому шкафу управления;

контроль основных параметров электрической сети;

сбор и обработка информации о состоянии оборудования наружного освещения;

обнаружение и своевременная сигнализация и регистрация аварийных ситуаций в сети;

регулирование энергопотребления системы;

интеграция с городскими системами диспетчеризации и учет энергоресурсов.

5) учет технических средств регулирования дорожного движения (ТСРДД) и технических средств организации дорожного движения (ТСОДД), обеспечивающий выполнение следующих функций:

обеспечение автоматического мониторинга актуального (текущего) состояния технических средств организации и регулирования дорожного движения на УДС;

создание схем дислокации технических средств организации и регулирования дорожного движения на электронной карте.

6) телеобзор, обеспечивающий выполнение следующих функций:

визуальный контроль оператором транспортной ситуации в наиболее напряженных узлах улично-дорожной сети;

автоматическое выявление инцидентов (остановившееся ТС, образование заторов и т.д.);

выявление мест и причин возникновения предзаторовых и заторовых ситуаций;

визуальная обратная связь по принятым решениям при диспетчерском управлении техническими средствами регулирования движения;

наблюдение за оперативной обстановкой при проведении специальных мероприятий;

анализ ДТП, КСП и прочих изменений условий движения транспорта;

контроль работы сотрудников специальных и других служб.

7) управление парковочным пространством, предназначенное для мониторинга, обработки, хранение и передачи данных о наличии парковочных мест, необходимых для обеспечения функционирования системы управления техническими средствами регулирования и организации дорожного движения, системы информирования участников дорожного движения и единой диспетчерской службы.

Основными функциями АСКПП являются:

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

повышение безопасности хранения транспортных средств;

обеспечение фото-видеофиксации нарушений правил парковки;

профилактика нарушений правил парковки, включая перемещение транспортных средств, мешающих нормальному дорожному движению;

обеспечение расчетов за пользование парковкой;

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

сбор данных по уличной парковке;

сбор данных по внутридворовой парковке;

ввод данных по гаражам;

ввод данных по автостоянкам;

учет объектов единого парковочного пространства;

контроль свободных мест на организованных уличных парковках и автостоянках.

8) экстренная связь, предназначенная для обращения граждан через устройство экстренной связи (терминалы) в мониторинговый центр и приема от населения сообщений о фактах криминального характера, нарушений общественного порядка и т.п.

Элементы объектового оборудования системы (терминалы) ЭС устанавливаются на УДС и автомобильных дорогах общего пользования, на площадках кратковременного отдыха и осуществляют прямые соединения, сопровождаемые передачей данных по аудиоканалу и/или видеоканалу.

Подсистема экстренной связи должна обеспечивать следующие функциональные возможности:

функции визуального и акустического контроля оперативной обстановки, а также регистрацию поступающей аудио и видео-информации, интеграцию с комплексной системой видеонаблюдения;

предоставление гражданам круглосуточной оперативной экстренной голосовой и видеосвязи с операторами в режиме реального времени;

вызов как со стороны гражданина, так и со стороны оператора, с автоматической записью разговора;

переадресация поступающих вызовов в иные центры управления и экстренные службы;

ручное и автоматическое управление видеокамерами, подключенными к терминалам;

автоматическая регистрация и хранение видеоизображения на серверных мощностях.

6.2.3. Назначение и функциональность Системы обеспечения безопасности на транспорте

Система обеспечения безопасности на транспорте предназначена для решения комплекса задач повышения безопасности на транспорте и объектах транспортной инфраструктуры, в том числе предоставления 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.

Систему обеспечения безопасности на транспорте формируют следующие функциональные подсистемы:

1) мониторинг объектов транспортной инфраструктуры, обеспечивающий выполнение следующих функций:

автоматизация технического учета объектов дорожно-транспортной инфраструктуры;

классификация и технический учет объектов дорожно-транспортной инфраструктуры (ДТИ);

предоставление агрегированных и детальных данных руководству и населению города об объектах ДТИ;

многомерный анализ данных об объектах ДТИ в целях определения возможной корреляции между состоянием объектов и изменениями дорожного трафика;

обеспечение пользователей Системы информацией в целях перспективного планирования, модернизации и развития ДТИ;

классификация и учет выполняемых изменений дорожного хозяйства (проекты капитального строительства, реконструкции, развития, модернизации инфраструктуры);

предоставление актуальной информации об объектах ДТИ и обеспечивающей инфраструктуры всем заинтересованным и подключаемым в процессе эксплуатации СМОТИ ведомствам и пользователям;

повышение качества оперативного диспетчерского управления движением транспорта;

регулярная актуализация информации об объектах ДТИ в целях обеспечения пользователей максимально достоверными сведениями о них.

2) сигнализация, контроль доступа, видеонаблюдение, аудио- и видеозаписи на объектах транспортной инфраструктуры, обеспечивающие выполнение следующих функций на объектах транспортной инфраструктуры:

обеспечение охранной сигнализации;

обеспечение контроля доступа;

обеспечение аудио- видеозаписи.

Технические средства сигнализации, контроля доступа, видеонаблюдения, аудио- и видеозаписи, используемые на объектах транспортной инфраструктуры, должны соответствовать требованиям,

определенным постановлением Правительства Российской Федерации от 29 сентября 2016 г. №969 "Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности".

Сертификация указанных технических средств должна проводиться МВД России в обязательном порядке на основании протоколов сертификационных испытаний испытательных лабораторий, аккредитованных в соответствии с законодательством Российской Федерации.

3) мониторинг и позиционирование общественного транспорта (СМПОТ), обеспечивающие выполнение следующих функций:

повышение безопасности подвижного состава наземного пассажирского транспорта на линии;

минимизация финансовых расходов на эксплуатацию подвижного состава наземного пассажирского транспорта.

создание единой автоматизированной навигационной системы обеспечения безопасности перевозки пассажиров наземным пассажирским транспортом и повышения антитеррористической защищенности транспортных средств;

сокращение времени реагирования на возникающие нештатные ситуации и обеспечения информационного взаимодействия с оперативными службами;

поддержка единой распределенной информационно-телекоммуникационной среды, объединяющей органы управления и предприятия-перевозчики и обеспечивающей информационный обмен между ними;

предоставление соответствующим должностным лицам необходимой информации, касающейся транспортного обслуживания;

интеграция с существующими системами управления движением общественного транспорта для обеспечения управления наземным пассажирским транспортом в обычной обстановке и в критических ситуациях.

4) Система дорожного метеорологического обеспечения (СДМО), обеспечивающая выполнение следующих функций:

сбор (в т.ч. от системы Росгидромета), обработка, хранение и передача информации о метеорологической и экологической обстановке на УДС в подсистемы ИТС.

обеспечение функционирования системы управления техническими средствами регулирования и организации дорожного движения, системы

информирования участников дорожного движения и единой диспетчерской службы, для оперативного информирования заинтересованных служб, участников дорожного движения о состоянии УДС, чтобы, в том числе, исключить аварийные ситуации вследствие гололеда или мокрой дороги.

контроль метеорологических параметров и состояния дорожного покрытия: температура воздуха, относительная влажность воздуха, температура точки росы, скорость и направление ветра, атмосферное давление, наличие, интенсивность и количество осадков, метеорологическая дальность видимости,

состояние дорожного покрытия (сухое, влажное, лед, снег, иней), толщина отложений на покрытии, температура дорожного покрытия и дорожной конструкции, наличие на дорожном покрытии количества и концентрации противогололедных реагентов.

передача информации с пунктов дорожного метеоконтроля в органы управления дорожным хозяйством и в дорожные подрядные организации в автоматическом режиме.

5) управление движением общественного транспорта (СУДОТ), обеспечивающее выполнение следующих функций:

поддержка единой распределенной ИТС, объединяющей органы управления и предприятия-перевозчики, а также обеспечивающей информационный обмен между ними;

предоставление должностным лица и руководителям транспортного комплекса необходимой информации, касающейся транспортного обслуживания;

обеспечение электронного документооборота для повышения оперативности принятия решений;

организация системы обмена данными между предприятиями-перевозчиками, административными органами управления и другими службами города, информационный обмен с которыми необходим;

обеспечение безопасности и целостности данных по планированию, регулированию и учету работы пассажирского городского наземного транспорта;

интеграция создаваемых автоматизированных систем для обеспечения управления движением с существующими и проектируемыми информационными системами и информационными ресурсами предприятий-перевозчиков, административных органов управления в рамках создаваемой ИТС;

объединение в единую систему управления существующих и планируемых к внедрению локальных систем автоматизации технологических процессов на городском пассажирском транспорте, в частности: систем автоматизации составления маршрутных расписаний, систем автоматизированного изучения пассажиропотоков, систем автоматизированного ведения паспортов маршрутов, систем оперативного контроля и диспетчерского управления пассажирскими транспортными средствами, внедренных у некоторых предприятий - перевозчиков, систем обеспечения безопасности перевозок пассажиров, систем автоматизированного информирования пассажиров, систем автоматизированного контроля оплаты за проезд.

создание единой, автоматизированной на базе технологий спутниковой навигации ГЛОНАСС/GPS, системы оперативного диспетчерского управления наземным пассажирским транспортом;

автоматизация процессов формирования городского заказа на пассажирские перевозки и контроля за его выполнением;

автоматизация процессов оперативного диспетчерского управления движением наземного городского пассажирского транспорта;

автоматизированный сбор и обработка информации о состоянии процессов перевозок, о местоположении и движении транспортных средств;

создание единой автоматизированной навигационной системы обеспечения безопасности перевозки пассажиров наземным городским пассажирским транспортом и повышения антитеррористической защищенности транспортных средств;

создание единой автоматизированной системы информирования пассажиров наземного городского пассажирского транспорта.

6) Система информирования населения на транспортных средствах и объектах транспортной инфраструктуры, обеспечивающая выполнение следующих функций:

сбор информации о складывающейся на объектах транспортной инфраструктуры обстановке на основании: видеоинформации с камер наблюдения, с датчиков радиационного и химического контроля, об охранно-пожарной безопасности серверного оборудования и терминалов информирования и оповещения, а также информации по интенсивности пассажиропотока посредством датчиков и/или камер,.

мониторинг обстановки на объекте транспортной инфраструктуры посредством установленных камер видеонаблюдения;

архивирование информации с камер видеонаблюдения в оперативном архиве сегмента СЗИОНТ на объекте транспортной инфраструктуры;

передача в режиме реального времени информации с видеокамер на АРМ дежурного по объекту, в центр управления сегментами СЗИОНТ в ЦУКС МЧС России, в ЕДДС соответствующего муниципального образования;

передача по запросу операторов информации из оперативного архива на АРМ дежурного по объекту, а так же в центр управления сегментами СЗИОНТ в ЦУКС для просмотра и долгосрочного хранения при необходимости.

определение пассажиропотока на входах и выходах здания объектов транспортной инфраструктуры;

архивирование данных в сегменте СЗИОНТ объекта транспортной инфраструктуры о пассажиропотоке на входах и выходах здания объекта;

передача в режиме реального времени данных о пассажиропотоке на АРМ дежурного по объекту, а так же в центр управления сегментами СЗИОНТ в ЦУКС;

передача по запросу операторов данных из архива о пассажиропотоке на входах и выходах здания объекта транспортной инфраструктуры на АРМ дежурного, а так же в центр управления сегментами СЗИОНТ в ЦУКС.

предотвращение попадания на территорию объекта транспортной инфраструктуры запрещенных к проносу радиоактивных и химических веществ, в том числе предотвращение действий направленных на совершение террористических актов.

фиксирование попыток несанкционированного доступа и угроз возникновения пожара в шкафах с управляющим оборудованием и внутри терминалов информирования и оповещения.

отображение плана помещений (3D-модель) объекта транспортной инфраструктуры с нанесенными на него элементами сегмента СЗИОНТ на объекте;

отображение цветом тревожных событий с датчиков ОПС, экстренных вызовов через ПЭС и др.;

просмотр значений контролируемых параметров интересующего оборудования;

экстренное оповещение пассажиров, находящихся на объекте транспортной инфраструктуры путем активации режима сценариев модуля видео информирования ПМИ.

обеспечение оповещения и информирования населения, а также экстренной связи на транспортных средствах (автомобильном, железнодорожном, водном и воздушном транспорте), включая автоматическое оповещение служб экстренного реагирования при авариях и других чрезвычайных ситуациях, автоматическое позиционирование точки вызова и регистрацию события, информирование населения по вопросам гражданской обороны;

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 автоматическое оповещение служб экстренного реагирования при авариях и других чрезвычайных ситуациях, автоматическое позиционирование точки вызова и регистрацию события, информирование населения по вопросам гражданской обороны;

информирование о чрезвычайных ситуациях на транспортных средствах и объектах транспортной инфраструктуры, включая идентификацию событий на основе поступающей информации с датчиков и средств видеонаблюдения, установленных на транспортных средствах, объектах транспортной инфраструктуры с визуализацией на электронной карте города.

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.

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 при помощи стандартизированных протоколов;

КСА "Безопасность на транспорте" должны проектироваться на основе мультисервисной цифровой сети передачи данных;

узлы мультисервисной цифровой сети должны быть объединены сетевым протоколом IP;

все сетевые видеокамеры или кодеры (преобразователи аналогового сигнала в цифровой) должны поддерживать отраслевой стандарт, определяющий протоколы взаимодействия - ONVIF версии 1.02 и 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 и 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 и 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 КСА "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 КСА "Безопасность на транспорте" для серверных и сетевых компонентов, а также 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 систем 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 фото-видеофиксации определяется из расчета: одна камера - одна и более полоса движения.

Данные о фактах фиксации передвижения транспортных средств, полученные путем распознавания государственных регистрационных знаков (ГРЗ) при передвижении транспортных средств через контролируемые зоны, формируются с использованием систем идентификации транспортных средств (далее - СИТС). Данные от установленных СИТС должны передаваться через узлы сбора данных с использованием стандартизированных протоколов обмена данными.

Технические требования к источникам фото-видеофиксации приведены в приложении 18.

Требования к абонентским терминалам ГЛОНАСС-GPS/GSM, датчикам спутниковой навигации, бортовому навигационному оборудованию приведены в приложении 19.

Должны быть соблюдены требования к телекоммуникационной инфраструктуре, представленные в приложении 16.

Технические требования к системе видеонаблюдения представлены в приложении 17.

6.5. Требования к системному программному обеспечению КСА функционального блока "Безопасность на транспорте"

Программное обеспечение КСА функционального блока "Безопасность на транспорте" представляет собой совокупность общего программного обеспечения и специального программного обеспечения.

Программное обеспечение КСА функционального блока "Безопасность на транспорте" должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития, в том числе с учетом включения в состав КСА 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 КСА "Региональная платформа" функционального блока "Координации работы служб и ведомств", представленных в приложении 3.

Требования к специальному обеспечению КСА функционального блока "Безопасность на транспорте" должны быть аналогичны требованиям к специальному программному обеспечению КСА "Региональная платформа" функционального блока "Координация работы служб и ведомств", представленных в приложении 4.

6.6. Требования к информационному обеспечению КСА функционального блока "Безопасность на транспорте"

Требования к информационному обеспечению КСА функционального блока "Безопасность на транспорте" должны быть аналогичны требованиям к информационному обеспечению КСА "Региональная платформа" функционального блока "Координация работы служб и ведомств", представленных в разделе 4.2.6. "Требования к информационному обеспечению КСА "Региональная платформа" 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 систем АПК "Безопасный город":

системы мониторинга состояния окружающей среды;

системы управления рисками окружающей среды.

7.2. Назначение и функциональность КСА функционального блока "Экологическая безопасность"

7.2.1. Назначение и функциональность системы мониторинга состояния окружающей среды

Система мониторинга состояния окружающей среды обеспечивает радиационный экологический контроль, непрерывный мониторинг ключевых показателей окружающей среды, включая гидрометеорологическую информацию, уровень загрязнения и состав воздуха, почвы, предельно допустимых выбросов, предельно допустимой

концентрации (ПДК) и предельно допустимого сброса (ПДС) вредных веществ в атмосфере, почве, воде.

В состав системы мониторинга состояния окружающей среды должны входить следующие функциональные подсистемы:

мониторинг гидрометеорологической обстановки;

мониторинг состояния почв;

мониторинг водных ресурсов;

мониторинг сейсмической активности;

мониторинг пожарной опасности;

наружный и внутренний мониторинг вредных химических веществ;

мониторинг радиационной обстановки.

1) Подсистема мониторинга гидрометеорологической обстановки в составе гидрометеорологических комплексов, осуществляющих измерение температуры воздуха, давления, силы и направления ветра, влажности, количества осадков, высоты снежного покрова, измерение уровня зеркала воды, предоставляет следующие функциональные возможности:

сбор и обработка данных с гидрометеорологических комплексов;

сбор и обработка данных со специализированных ресурсов гидрометеорологических служб;

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

идентификация угроз с формированием тревожного события в случае превышения измеряемыми показателями критических значений;

отображение на картографической подоснове мест размещения гидрометеорологических комплексов, включая комплексы в составе сопрягаемых автоматизированных систем мониторинга гидрометеорологических служб, статистики измерений и технических параметров работы комплексов.

2) Подсистема мониторинга состояния почв в составе гидрометеорологических комплексов, лабораторных систем измерения химического состава почвы, устройств изменения линейных отклонений и вибраций, комплексов радиационного контроля, предоставляет следующие функциональные возможности:

сбор и обработка данных с гидрометеорологических комплексов в части контроля уровня осадков, влажности почвы, температуры почвы;

сбор и учет данных о химическом составе почвы;

сбор и обработка данных с датчиков линейных отклонений массива почвы для определения угрозы оползней и обвалов;

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

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

идентификация угроз с формированием тревожного события в случае превышения измеряемыми показателями критических значений;

отображение на картографической подоснове мест размещения оконечных устройств мониторинга состояния почв, статистики осуществляемых измерений и технических параметров работы комплексов.

3) Подсистема мониторинга водных ресурсов в составе телеметрических комплексов лабораторного контроля качества воды предоставляет следующие функциональные возможности:

сбор и обработка данных о химическом составе с автоматизированных комплексов лабораторного контроля качества воды;

идентификация угроз с формированием тревожного события в случае превышения измеряемыми показателями критических значений;

отображение на картографической подоснове мест размещения оконечных устройств мониторинга водных ресурсов, статистики осуществляемых измерений и технических параметров работы комплексов.

4) Подсистема мониторинга сейсмической активности в составе телеметрических комплексов мониторинга сейсмической активности, вибраций, линейных отклонений почвы и конструкций, предоставляет следующие функциональные возможности:

сбор и обработка данных с оконечных устройств о сейсмической активности, сдвигах почвы, вибрациях;

идентификация угроз с формированием тревожного события в случае превышения измеряемыми показателями критических значений;

отображение на картографической подоснове мест размещения оконечных устройств мониторинга сейсмической активности, статистики осуществляемых измерений и технических параметров работы комплексов.

5) Подсистема мониторинга пожарной опасности в составе телеметрических комплексов химического контроля качества воздуха, интеллектуальных систем видеонаблюдения, систем дистанционного

зондирования Земли, предоставляет следующие функциональные возможности:

сбор и обработка данных с оконечных устройств контроля качества воздуха о превышении содержания угарного газа;

сбор и обработка информации о регистрируемых очагах возгорания системами раннего обнаружения природных пожаров;

сбор и обработка информации о термоточках из систем дистанционного зондирования земли;

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

идентификация угроз с формированием тревожного события в случае превышения измеряемыми показателями критических значений;

отображение на картографической подоснове мест размещения оконечных устройств мониторинга пожарной опасности, статистики осуществляемых измерений и технических параметров работы комплексов.

6) Подсистема наружного и внутреннего мониторинга вредных химических веществ (ВХВ) в составе телеметрических комплексов химического контроля качества воздуха, предоставляет следующие функциональные возможности:

сбор и обработка данных с оконечных устройств контроля качества воздуха, включая содержание кислорода, превышении содержания примесей водорода, CO2, соединений углеводородной группы, метана, сернистого газа, азотных соединений, изобутанов, толуола, этанола, аммиака и других опасных веществ;

сбор и обработка данных с оконечных устройств контроля ПДС/ПДК ВХВ в воде на соответствие экологическим нормативам установленных для конкретного выпуска сточных вод действующего предприятия - водопользователя;

сбор и обработку данных с оконечных устройств контроля ПДС/ПДК ВХВ в почве и грунтах на соответствие экологическим нормативам, установленным для кларков почв селитебных ландшафтов;

идентификация угроз с формированием тревожного события в случае превышения измеряемыми показателями критических значений;

отображение на картографической подоснове мест размещения оконечных устройств мониторинга химической опасности, статистики осуществляемых измерений и технических параметров работы комплексов.

7) Подсистема радиационного экологического мониторинга в составе комплексов радиоэкологического мониторинга предоставляет следующие функциональные возможности:

сбор и обработка данных с устройств радиоэкологического мониторинга;

идентификация угроз с формированием тревожного события в случае превышения измеряемыми показателями критических значений;

отображение на картографической подоснове мест размещения оконечных устройств радиоэкологического мониторинга, статистики осуществляемых измерений и технических параметров работы комплексов.

7.2.2. Назначение и функциональность системы управления рисками окружающей среды

Система управления рисками окружающей среды должна обеспечивать анализ информации, принимаемой из подсистем мониторинга состояния окружающей среды, обеспечивать непрерывное моделирование угроз на основании поступающей динамической информации, предоставлять прогностическую и отчетную информации об угрозах, обеспечивать поддержку принятия решений при осуществлении планирования территориального развития.

В состав системы управления рисками окружающей среды должны входить следующие функциональные подсистемы:

1) подсистема идентификации и оценки экологических рисков, с набором следующих функциональных возможностей:

идентификация угроз экологических рисков с автоматическим формированием тревожного сообщения;

динамическое моделирование событий на основе поступающей статистики с целью заблаговременного предупреждения развития КСП;

отображение результатов расчетов и моделирования на картографической подоснове;

расчеты источников загрязнения с учетом гидрометеорологической информации, данных комплексов мониторинга экологической обстановки.

2) подсистема управления процессами планирования и осуществления муниципального экологического контроля с набором следующих функциональных возможностей:

ведение паспортов объектов воздействия на окружающую среду, содержащих информацию о параметрах опасных хранимых опасных веществ, характере загрязнения, нормативов ПДС и ПДК;

регистрация объектов вредного воздействия на окружающую среду с возможностью автоматического расчета платы за негативное воздействие на окружающую среду исходя из фактических данных, предоставляемых объектом посредством интеграции с системами контроля ПДС и ПДК, файлообменных ресурсов;

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

дистанционный мониторинг транспортных средств, осуществляющих вывоз промышленных и бытовых отходов;

мониторинг состояния окружающей среды в районах размещения отходов и мониторинг экологической обстановки территорий городов для предотвращения и выявления несанкционированных захоронений отходов с использованием средств дистанционного зондирования Земли (анализ космоснимков);

планирования муниципального развития с учетом норм экологической безопасности с использованием геоинформационных систем.

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.

Взаимодействие компонентов программного обеспечения в КСА систем 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 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 стандартизированных протоколов;

КСА функционального блока "Экологическая безопасность" должны проектироваться на основе мультисервисной цифровой сети передачи

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

все сетевые видеокамеры или кодеры (преобразователи аналогового сигнала в цифровой) должны поддерживать отраслевой стандарт, определяющий протоколы взаимодействия - ONVIF версии 1.02 и 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 и 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 и 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 в режиме 24/7 (ежедневно и круглосуточно). Для участков сети, требующих повышенной надежности, необходимо предусмотреть резервные каналы связи.

Для обеспечения высокой доступности сервисов КСА подсистем функционального блока "Экологическая безопасность" для серверных и сетевых компонент, а также 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 систем АПК "Безопасный город" в соответствии с настоящими требованиями.

Должны быть обеспечены требования к техническому обеспечению КСА функционального блока "Экологическая безопасность" в соответствии с приложением 20 "Требования к техническому обеспечению КСА функционального блока "Экологическая безопасность".

Должны быть соблюдены требования к телекоммуникационной инфраструктуре, представленные в приложении 16.

Технические требования к системе видеонаблюдения представлены в приложении 17.

7.5. Требования к программному обеспечению КСА функционального блока "Экологическая безопасность"

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

Программное обеспечение КСА функционального блока "Экологическая безопасность" должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в состав КСА "Экологическая безопасность" перспективных КСА.

Программное обеспечение должно быть сертифицировано по требованиям безопасности информации.

Требования к общему программному обеспечению функционального блока "Экологическая безопасность" должны быть аналогичны требованиям к общему программному обеспечению в приложении 3.

Требования к специальному обеспечению КСА функционального блока "Экологическая безопасность" должны быть аналогичны требованиям к специальному программному обеспечению КСА "Региональная платформа" функционального блока "Координация работы служб и ведомств", представленных в приложении 4.

7.6. Требования к информационному обеспечению КСА функционального блока "Экологическая безопасность"

Требования к информационному обеспечению КСА функционального блока "Экологическая безопасность" должны быть аналогичны требованиям к информационному обеспечению КСА "Региональная платформа" функционального блока "Координация работы служб и ведомств", представленных в разделе 4.2.6. "Требования к информационному обеспечению КСА Региональная платформа".

8. Общие требования к системам АПК "Безопасный город"

8.1. Требования к надежности

Надежность АПК "Безопасный город" определяется надежностью систем АПК "Безопасный город".

8.1.1. Состав и количественные значения показателей надежности

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

уровень сохранения работоспособности;

уровень сохранности информации.

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

Показатели надежности включают:

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

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

среднее время на восстановление работоспособности систем АПК "Безопасный город".

Показатели надежности систем 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 систем 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 потерь в работе систем АПК "Безопасный город" и временных затрат эксплуатирующего персонала при проведении работ по обслуживанию систем АПК "Безопасный город", а также на 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 систем АПК "Безопасный город";

своевременной диагностики неисправностей;

наличия договоров на сервисное обслуживание и поддержку компонентов комплекса технических средств АПК "Безопасный город".

Должны быть обеспечены следующие значения показателей надежности:

Системы АПК "Безопасный город" должны быть рассчитаны на круглосуточную работу;

срок службы систем АПК "Безопасный город" в целом должен составлять не менее 3 лет;

наработка систем АПК "Безопасный город" на отказ должна составлять не менее 5000 часов;

наработка систем 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 систем АПК "Безопасный город".

Сохранение работоспособности должно обеспечиваться при возникновении локальных отказов компонентов систем 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 системы 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, так как в системах АПК "Безопасный город" должно быть предусмотрено резервирование дисков.

Кроме того, должна быть обеспечена возможность "горячей" замены сбойного или вышедшего из строя накопителя на жестком магнитном диске без остановки функционирования систем 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 систем АПК "Безопасный город".

Должны быть предусмотрены средства оповещения должностных лиц о нештатной работе систем АПК "Безопасный город".

8.1.2. Требования к надежности технических средств и программного обеспечения

Надежность систем АПК "Безопасный город" в части технического обеспечения должна обеспечиваться:

наличием в 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;

автоматическим оповещением администраторов системы по нештатным ситуациям посредством электронной почты.

При выявлении внештатной ситуации в работе систем должны использоваться средства мониторинга и оповещения об аварийных ситуациях.

8.2. Требования безопасности

Программное обеспечение 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".

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

Системы, входящие в состав АПК "Безопасный город" должны обладать подсистемой информационной безопасности от несанкционированного доступа (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". Системы АПК

"Безопасный город" должны соответствовать требованиям класса защищенности "1Г" и выше, в зависимости от обрабатываемых данных и решаемых задач.

В техническом задании на создание подсистемы информационной безопасности должен быть определен состав информации, передача, обработка и хранение которой предполагается программно-техническими средствами АПК "Безопасный город", в том числе в такой состав должна быть включена информация, которая относится к защищаемым государством сведениям, утрата или распространение которых может нанести ущерб безопасности Российской Федерации, в том числе сведений, составляющих государственную тайну.

К таким сведениям в соответствии с действующим законодательством Российской Федерации[1] могут быть отнесены:

сведения о силах или средствах гражданской обороны;

сведения о степени обеспечения безопасности населения;

сведения, раскрывающие схемы водоснабжения городов с населением более 200 тыс. человек или железнодорожных узлов, расположение головных сооружений водопровода или водовода, их питающих;

геопространственные сведения по территории Российской Федерации и другим районам Земли, раскрывающим результаты топографической, геодезической, картографической деятельности, имеющие важное оборонное или экономическое значение;

сведения об объектах гидрографии, гидротехнических сооружениях, содержащиеся на топографических картах, топографических планах, фотокартах, фотопланах, ортофотокартах, ортофотопланах масштаба 1:50 000 и крупнее в государственных системах координат, местных системах координат территории Российской Федерации в графической, цифровой (электронной) или иных формах представления информации о местности.

Проведение анализа возможных каналов утечки защищаемых государством сведений должно быть осуществлено исполнителем на этапе технического проектирования с учетом возможных демаскирующих признаков, раскрывающих сведения в отношении информации, которая может циркулировать в АПК "Безопасный город". Такими

---

[1] Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 "Об утверждении перечня сведений, отнесенных к государственной тайне", Приказ Минэкономразвития России от 17 марта 2008 г. № 01 "Об утверждении перечня сведений, подлежащих засекречиванию, Министерства экономического развития и торговли Российской Федерации" и пр.

демаскирующими признаками могут быть: побочные электромагнитные излучения и наводки, создаваемые техническими средствами АПК "Безопасный город"; визуально-оптическая информация, составляющая государственную тайну, выводимая на устройства отображения, входящие в состав АПК "Безопасный город"; акустические и вибрационные сигналы, создаваемые в процессе обсуждения вопросов, содержащих охраняемые сведения на объектах автоматизации.

Режимные меры по предотвращению утечки защищаемых государством сведений на всех этапах работы должны быть включены в единый план мероприятий исполнителя по сохранению режима секретности. Контроль и оценку достаточности и эффективности принимаемых мер обеспечения секретности осуществляют режимно-секретные органы исполнителя. Ответственность за организацию выполнения требований по обеспечению сохранения государственной тайны при выполнении работ возлагается на исполнителя, а ответственность за непосредственный допуск исполнителя к выполнению работ, связанных с сохранением сведений содержащих государственную тайну - на заказчика работ.

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется на основании лицензий на право выполнения работ со сведениями соответствующей степени секретности, получаемых в порядке, устанавливаемом Правительством Российской Федерации,

Органами, уполномоченными на ведение лицензионной деятельности, являются[2]:

на право проведения работ, связанных с созданием средств защиты информации - ФСТЭК России и ФСБ России;

на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны - ФСБ России и ее территориальные органы, ФСТЭК России.

---

[2] Постановление Правительства Российской Федерации от 15 апреля 1995 г. №333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а так же с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны".

Техническое задание на создание подсистемы информационной безопасности для каждого комплекса средств автоматизации, входящего в состав АПК "Безопасный город" обязательно должно предусматривать:

разработку модели угроз и нарушителя для каждого КСА и определение:

а) требований по защите от несанкционированного доступа;

б) требований к средствам криптографической защиты;

в) требований к средствам обнаружения и предупреждения атак, а также к средствам межсетевого экранирования и шлюзам;

г) требований к средствам антивирусной защиты;

д) требований по защите персональной информации;

е) требований по защите сведений содержащих государственную тайну и противодействию иностранным техническим разведкам (при наличии таких соответствующих сведений в составе информации);

разработку технических решений по нейтрализации выявленных угроз и действий нарушителя и обеспечивающих выполнение требований по безопасности;

проведение аттестации КСА.

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

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

В ходе проектирования систем АПК "Безопасный город" должен быть уточнен состав информации и методов ее обработки, подлежащий защите, а также разработана модель угроз и модель нарушителя.

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 ПУЭ.

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 систем АПК "Безопасный город", не должны превышать действующих норм (СанПиН 2.2.2./2.4.1340-03 от 03 июня 2003 г.).

8.3. Требования к эргономике и технической эстетике

Графический интерфейс систем 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 систем 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 пользователя:

возможность гибко контролировать ввод данных, просматривать введенные данные на мониторе, производить их корректировку или отказаться от ввода;

при вводе иметь возможность использовать справочники для контроля вводимых данных и списки допустимых значений;

возможность обеспечения 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 исходное рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

8.4. Требования к эксплуатации, техническому обслуживанию и ремонту

Эксплуатация систем 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.

8.5. Требования по сохранности информации при авариях

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

импульсные помехи, сбои и перерывы в электропитании;

нарушение или выход из строя каналов связи;

сбой общего программного обеспечения;

сбой специального программного обеспечения;

выход из строя аппаратных средств (серверы, системы хранения данных, АРМ и другие);

ошибки в работе персонала.

Эксплуатация систем 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 систем 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".

8.6. Требования к защите от влияния внешних воздействий

Технические средства 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.

8.7. Требования к патентной чистоте

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

При поставке систем АПК "Безопасный город" должны быть выполнены требования Федерального закона Российской Федерации от 23 сентября 1992 г. № 3523-I "О правовой охране программ для электронных вычислительных машин и баз данных".

8.8. Требования по стандартизации и унификации

Программная документация на системы АПК "Безопасный город", планируемые к внедрению, должна проходить проверку на соответствие настоящим требованиям по методике, утвержденной СГК.

Процесс разработки систем 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".

Системы 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 Российской Федерации от 17 декабря 2010 г. № 2299-р о плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения (2011 - 2015 годы).

В системах 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.

Выполнение работ по созданию (развитию), внедрению и дальнейшей эксплуатации систем АПК "Безопасный город" должно осуществляться с учетом требований и положений действующей системы законодательства в области лицензирования отдельных видов деятельности.

ПРИЛОЖЕНИЕ № 1

Схемы построения АПК "Безопасный город"

Рисунок 1. Схемы построения АПК "Безопасный город"

27060355.doc

Рисунок 2. Состав систем функционального блока координации и взаимодействия служб и ведомств в зависимости от выбора схемы построения АПК "Безопасный город"

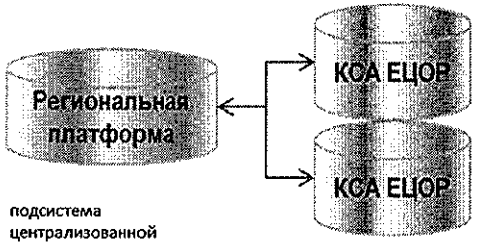
Централизованная

- Функции системы предоставляются из регионального центра

- подсистема приема и обработки обращений.
- региональная подсистема интеграции данных
- региональная интеграционная геоинформационная подсистема
- подсистема электронного взаимодействия
- подсистема поддержки принятия решений.
- подсистема комплексного мониторинга
- подсистема обеспечения координации и взаимодействия
- подсистема комплексного информирования и оповещения

Децентрализованная

- Функции системы предоставляются с площадок на базе ЕДДС МО

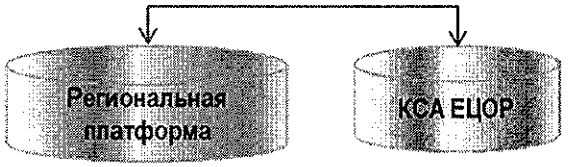


- подсистема централизованной обработки вызовов
- подсистема интеграции данных
- интеграционная геоинформационная подсистема
- подсистема электронного взаимодействия;

- подсистема приема и обработки обращений.
- муниципальная подсистема интеграции данных
- муниципальная интеграционная географическая подсистема
- подсистема поддержки принятия решений.
- подсистема комплексного мониторинга МО
- подсистема обеспечения взаимодействия городских служб и населения.
- подсистема обеспечения координации и взаимодействия.
- подсистема комплексного информирования и оповещения.

Гибридная

- Функции системы для крупных МО предоставляются с площадок на базе ЕДДС
- Функции системы для малых МО предоставляются из регионального центра



- подсистема приема и обработки обращений
- региональная подсистема интеграции данных
- региональная интеграционная геоинформационная подсистема
- подсистема поддержки принятия решений
- подсистема комплексного мониторинга
- подсистема электронного взаимодействия (региональный портал)
- подсистема обеспечения координации и взаимодействия
- подсистема комплексного информирования и оповещения

- подсистема приема и обработки обращений.
- муниципальная подсистема интеграции данных
- муниципальная интеграционная географическая подсистема
- подсистема поддержки принятия решений.
- подсистема комплексного мониторинга МО
- подсистема обеспечения взаимодействия городских служб и населения.
- подсистема обеспечения координации и взаимодействия.
- подсистема комплексного информирования и оповещения.

ПРИЛОЖЕНИЕ № 2

ТРЕБОВАНИЯ

к вычислительной инфраструктуре и обеспечивающим прикладным подсистемам КСА "Региональная платформа"

Технические требования к подсистеме хранения данных:

- отсутствие единой точки отказа;
- обеспечение файлового доступа к данным по протоколам NFS и CIFS(SMB) или блочного доступа к данным по протоколам iSCSI и FCP;
- поддержка пулов хранения данных;
- поддержка протоколов высокоскоростной передачи данных в интерфейсных узлах сети;
- возможность расширения системы без остановки обслуживания;
- поддержка жестких дисков 2ТБ, 3ТБ, 4ТБ, 6ТБ;
- поддержка SSD накопителей;
- поддержка использования уровней RAID-0,1,10,5,6;
- 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 с поддержкой протоколов высокоскоростной передачи данных в интерфейсных узлах и к устройству хранения резервных копий, а также к архиву данных.

При построении вычислительной инфраструктуры допускается использование средств виртуализации и кластеризации.

При построении вычислительной инфраструктуры КСА "Региональная платформа" приоритет должен отдаваться техническим решениям отечественного производства.

Для построения обеспечивающих прикладных подсистем должны использоваться решения отечественного производства, в том числе на базе свободного программного обеспечения с открытыми исходными кодами.

ПРИЛОЖЕНИЕ № 3

ТРЕБОВАНИЯ

к общему программному обеспечению КСА "Региональная платформа" 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. 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 Интернет и Интранет -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.

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.

Должно использоваться общее программное обеспечение отечественного производства, в том числе на базе свободного программного обеспечения с открытыми исходными кодами. Использование общего программного обеспечения не отечественного производства допускается только при отсутствии соответствующего общего программного обеспечения отечественного производства.

ПРИЛОЖЕНИЕ № 4

ТРЕБОВАНИЯ

к специальному программному обеспечению КСА "Региональная платформа" функционального блока "Координация работы служб и ведомств"

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

При разработке специального программного обеспечения должны быть использованы все возможности, предоставляемые 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 "Региональная платформа" нормально функционировать в операционной и информационной среде АПК "Безопасный город".

Для обеспечения принципов сохранения ранее вложенных инвестиций и соблюдения преемственности функциональной наполненности систем 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 "Региональная платформа";

- 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.

Специальное программное обеспечение должно быть отечественного производства, в том числе на базе свободного программного обеспечения с открытыми исходными кодами.

ПРИЛОЖЕНИЕ № 5

ТРЕБОВАНИЯ

к информационной совместимости КСА "Региональная платформа" со смежными КСА

Информационная совместимость КСА "Региональная платформа" со смежными КСА должна обеспечиваться возможностью использования одних и тех же форматов данных и протоколов обмена данными между КСА.

Информационная совместимость КСА "Региональная платформа" со смежными КСА реализуется в ходе электронного информационного взаимодействия (передачи данных) - КСА функционального блока "Координация работ служб и ведомств" между собой, между АПК "Безопасный город" и федеральными и региональными КСА.

Регламентация КСА при электронном информационном взаимодействии (передаче данных) со смежными разнородными информационными системами должна определяться:

- специальными стандартами - стандартизированными протоколами взаимодействия;
- типовым синтаксисом сообщений, именами элементов данных, операциями 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 другие 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 № 6

ТРЕБОВАНИЯ

по применению систем управления базами данных АПК "Безопасный город"

Используемые в АПК "Безопасный город" системы управления базами данными (СУБД) должны быть промышленного изготовления, с использованием необходимых лицензий.

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 № 7

ТРЕБОВАНИЯ

к структуре процесса сбора, обработки, передачи данных в АПК "Безопасный город"

Требования к структуре процесса сбора, обработки, передачи данных в системах 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 систем АПК "Безопасный город";
- настройки программного обеспечения;
- хранения, обновления информации о событиях;
- репликации информации по компонентам систем АПК "Безопасный город";
- обмена информацией в режиме импорта-экспорта в соответствии с регламентами информационного обмена, реализуемого прикладным программным обеспечением;
- обеспечения информационной совместимости системами АПК "Безопасный город" с федеральными и региональными системами.

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

ПРИЛОЖЕНИЕ № 8

ТРЕБОВАНИЯ

к защите данных от разрушений при авариях и сбоях в электропитании систем АПК "Безопасный город"

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

В 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.

Системы 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 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 систем АПК "Безопасный город".

Обеспечение надежности хранения и восстановления данных должно осуществляться на основе:

- быстрого сброса кэш-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 гражданах в фоновом режиме;

- возможности переноса данных внутри системы без остановки приложений;

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

ПРИЛОЖЕНИЕ № 9

ТРЕБОВАНИЯ

к контролю, хранению, обновлению и восстановлению данных АПК "Безопасный город"

Данные систем АПК "Безопасный город" должны храниться на дисках системы хранения данных (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, возможность реплицирования 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 систем АПК "Безопасный город";
- должна обеспечивать масштабируемость;
- не должна иметь единой точки отказа;

- обеспечение файлового доступа к данным по протоколам NFS и CIFS(SMB) или блочного доступа к данным по протоколам iSCSI и FCP;

- поддержка пулов хранения данных.

Возможность наращивания числа жестких дисков, объема кэш-памяти, аппаратной модернизации и расширения функционала с помощью специального программного обеспечения. Все перечисленные операции должны производиться без значительного переконфигурирования и потерь функциональности.

ПРИЛОЖЕНИЕ № 10

ТРЕБОВАНИЯ

к процедуре придания юридической силы документам, продуцируемым техническими средствами АПК "Безопасный город"

Требования к приданию юридической силы документам, продуцируемым техническими средствами 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 в АПК "Безопасный город";

- требованиям к подлинникам, дубликатам, копиям документов на машинном носителе и машинограммам, полученным программными средствами 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 № 11

ТРЕБОВАНИЯ
к обеспечивающим подсистемам КСА ЕЦОР

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;
- обеспечение целостности информации;
- антивирусную защиту;
- обнаружение 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 должна быть обеспечена возможность обработки конфиденциальной информации, относящейся к следующим типам:

- персональные данные;

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с законодательством Российской Федерации;

- 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 (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.

Для организации информационного обмена с использованием каналов связи, выходящих за пределы контролируемой зоны, при передаче по таким каналам связи информации, к которой предъявляются требования по обеспечению конфиденциальности, 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 криптографических алгоритмов, утвержденных в качестве национальных стандартов Российской Федерации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" для обеспечения безопасности информации ограниченного доступа при ее обработке в государственной информационной системе требуется использовать мероприятия по

обеспечению безопасности информации. 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 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 Системы к сетям связи общего пользования данный функциональный модуль должен быть реализован

путем использования средств межсетевого экранирования, соответствующих классу защищенности (в соответствии с руководящим документом ФСТЭК России "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"), который должен быть определен после согласования модели угроз и модели нарушителя. 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 АПК "Безопасный город", 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 Системы на рабочих станциях и серверах должны применяться сертифицированные средства антивирусной защиты в целях защиты обрабатываемой информации и программно-технических средств от воздействия вредоносного программного обеспечения.

Для программных средств, используемых при защите информации в Системе, 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.

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.

Требования к подсистеме резервирования

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

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.

Требования к системе хранения данных

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

СХД должна удовлетворять следующим параметрам:

- отсутствие единой точки отказа;

- обеспечение файлового доступа к данным по протоколам NFS и CIFS(SMB) или блочного доступа к данным по протоколам iSCSI и FCP;

- поддержка пулов хранения данных;

- поддержка протоколов высокоскоростной передачи данных в интерфейсных узлах сети;

- возможность расширения системы без остановки обслуживания;

- поддержка жестких дисков 2ТБ, 3ТБ, 4ТБ, 6ТБ;

- поддержка SSD накопителей;

- поддержка использования уровней RAID-0,1,10,5,6, 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 с поддержкой протоколов высокоскоростной передачи данных в интерфейсных узлах и к устройству хранения резервных копий, а также к архиву 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.

ПРИЛОЖЕНИЕ № 12

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 протоколов высокоскоростной передачи данных в интерфейсных узлах сети;
- возможность расширения системы без остановки обслуживания;
- поддержка жестких дисков 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 с поддержкой протоколов высокоскоростной передачи данных в интерфейсных узлах и к устройству хранения резервных копий, а также к архиву данных.

При построении вычислительной инфраструктуры должны использоваться средства виртуализации и кластеризации.

При построении вычислительной инфраструктуры КСА ЕЦОР должны быть предусмотрены, в интересах ФСБ России и ФСО России, разделы для решения специальных задач (далее - Специальные разделы вычислительной инфраструктуры). Количество специальных разделов, а также их вычислительные характеристики зависят от объема обрабатываемых и хранимых данных в КСА ЕЦОР и должны быть определены на этапе проектирования КСА ЕЦОР.

ПРИЛОЖЕНИЕ № 13

ТРЕБОВАНИЯ

к специальному программному обеспечению КСА ЕЦОР функционального блока "Координация работы служб и ведомств"

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

При реализации задач специального программного обеспечения могут быть использованы любые возможности, предоставляемые 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 ЕЦОР 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 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 ЕЦОР;

- 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;

- возможность передачи данных о камерах видеонаблюдения, устанавливаемых в рамках реализации КСА ЕЦОР, в Специальные разделы вычислительной инфраструктуры, а именно:

- данные о месте расположения камеры видеонаблюдения;

- наименование марки, модели и производителя камеры видеонаблюдения;

- параметры доступа к видеокамере (параметры доступа к видеопотоку);

- записи видеоархива.

ПРИЛОЖЕНИЕ № 14

ТРЕБОВАНИЯ

к информационной совместимости КСА ЕЦОР со смежными КСА

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

Регламентация КСА ЕЦОР при электронном информационном взаимодействии (передаче данных) со смежными разнородными информационными системами должна определяться:

- специальными стандартами - стандартизированными протоколами информационного взаимодействия;
- 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, другие 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.

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 ЕЦОР. Должно обеспечиваться ведение журнала пользователя.

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

ПРИЛОЖЕНИЕ № 15

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 № 16

ТРЕБОВАНИЯ
к телекоммуникационной инфраструктуре

Телекоммуникационная инфраструктура должна обеспечить надежный и безопасный обмен информацией между основными территориально разнесенными информационными системами АПК "Безопасный город".

Телекоммуникационная инфраструктура 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.

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

В основу построения телекоммуникационной инфраструктуры должны быть заложены следующие принципы:

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

- возможность приоритетного использования существующих сетей передачи данных в целях обеспечения бюджетной экономии и сокращения сроков развертывания систем АПК "Безопасный город".

Телекоммуникационная инфраструктура должна обеспечивать:

- поддержку стека сетевых протоколов TCP/IP;

- поддержку протоколов приоритетной обработки очередей обслуживания;

- поддержку транспортных протоколов реального времени;

- обеспечение передачи различных видов трафика (данные, аудио- и видео-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 телекоммуникационной инфраструктуры должны быть определены на этапе проектирования исходя из расчетов пропускной способности каналов, географии расположения коммутационных узлов и конечного оборудования.

Требование к производительности телекоммуникационной инфраструктуры: архитектура телекоммуникационной инфраструктуры, используемые модели и компоненты активного сетевого оборудования должны соответствовать объемам передаваемого трафика сетевых приложений и сервисов АПК "Безопасный город".

При проектировании необходимо произвести расчет инфраструктуры компьютерной сети с параметрами качества, приведенными в таблице 2. Значения параметров в таблице 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	4Мбит/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.

Сервер 1 - сервера, принимающие/передающие большие потоки информации (видеосервер, сервер обработки заявок).

Сервер 2 - 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 "Безопасный город" должна состоять из следующих функциональных подсистем:

подсистемы защиты каналов связи внутри АПК "Безопасный город";

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

Телекоммуникационная инфраструктура 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 телекоммуникационной инфраструктуре.

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 № 17

Технические требования к системе видеонаблюдения

Система видеонаблюдения должна строиться с учетом результатов научно-исследовательских работ МВД России: "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 г.), "Выработка научно-технического и финансового обоснования для принятия решений по созданию системы обеспечения безопасности транспортной инфраструктуры с учетом существующих федеральных программ" (шифр "БТИ").

Места размещения систем видеонаблюдения должны согласовываться с территориальными органами ФСБ России и МВД России на этапах разработки технического задания и рабочей конструкторской документации правоохранительного сегмента АПК "Безопасный город".

Определения:

видеоидентификация (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 (СВН)

Архитектура СВН должна обеспечивать:

- взаимодействие подсистем и элементов на основе единого и открытого стандарта интерфейсов;
- возможность защищенного подключения внешних пользователей из подразделений МЧС России, ФСБ России, МВД России, ФСО России и других заинтересованных федеральных органов исполнительной власти;
- возможность передачи данных (мультимедийных и, при наличии, канала телеуправления/телесигнализации) с видеокамер в специальные разделы вычислительной инфраструктуры (выполнение данного требования допускает дублирование на телекоммуникационном оборудовании);
- 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

В состав СВН могут входить следующие подсистемы:

- видеоидентификации;
- видеоаналитики;
- обзорное видеонаблюдение;
- система хранения (система архивирования);
- система взаимодействия с внешними информационными системами;
- телекоммуникационная система;

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

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

1) В состав подсистемы видеоидентификации входят:

- видеокамеры;
- серверное оборудование;

- СПО.

Требования к видеокамерам.

Видеокамеры подсистемы видеоидентификации предназначены для регистрации лиц людей, движущихся в поле зрения видеокамер.

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

Таблица 1

Требования к видеоизображению, регистрируемому подсистемой видеоидентификации

№	Параметр	Значение
1	Разрешение регистрируемого изображения	от 1.2 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.
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 подсистемы видеоидентификации, с помощью устанавливаемого на него СПО и подразделяется на:

- серверы вычислений;
- серверы базы данных.

Количество и технические характеристики вычислительных мощностей 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.

Требования к СПО

СПО предназначено для детектирования и идентификации лиц людей в видеопотоке, зарегистрированном камерами из состава подсистемы видеоидентификации. СПО может быть установлено на серверном оборудовании или включено в программную прошивку видеокамеры.

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 подсистемы видеоидентификации.

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 в базу данных.

Интерфейс пользователя должен обеспечивать выполнение следующих функций:

- настройка и конфигурирование СПО;
- выборочный просмотр видеопотока, регистрируемого камерами из состава подсистемы видеоидентификации 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 (буфера данных);
- просмотр и редактирование видеоархива;
- поиск лица в архиве видеозаписей по заданию оператора;
- актуализация 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 подсистемы видеоидентификации определяется на этапе проектирования системы.

СПО должно обладать следующими эксплуатационными характеристиками:

- вероятность детектирования лица в видеопотоке - не менее 95%;
- вероятность истинноположительной идентификации человека - не менее 85%, при вероятности ложноположительной идентификации не более 1%;

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 более 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 подсистемы видеоидентификации могут входить другие дополнительные технические средства, обеспечивающие размещение и функционирование подсистемы видеоидентификации.

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

Требования к построению архитектуры системы

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

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

Архитектурой подсистемы видеоидентификации 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).

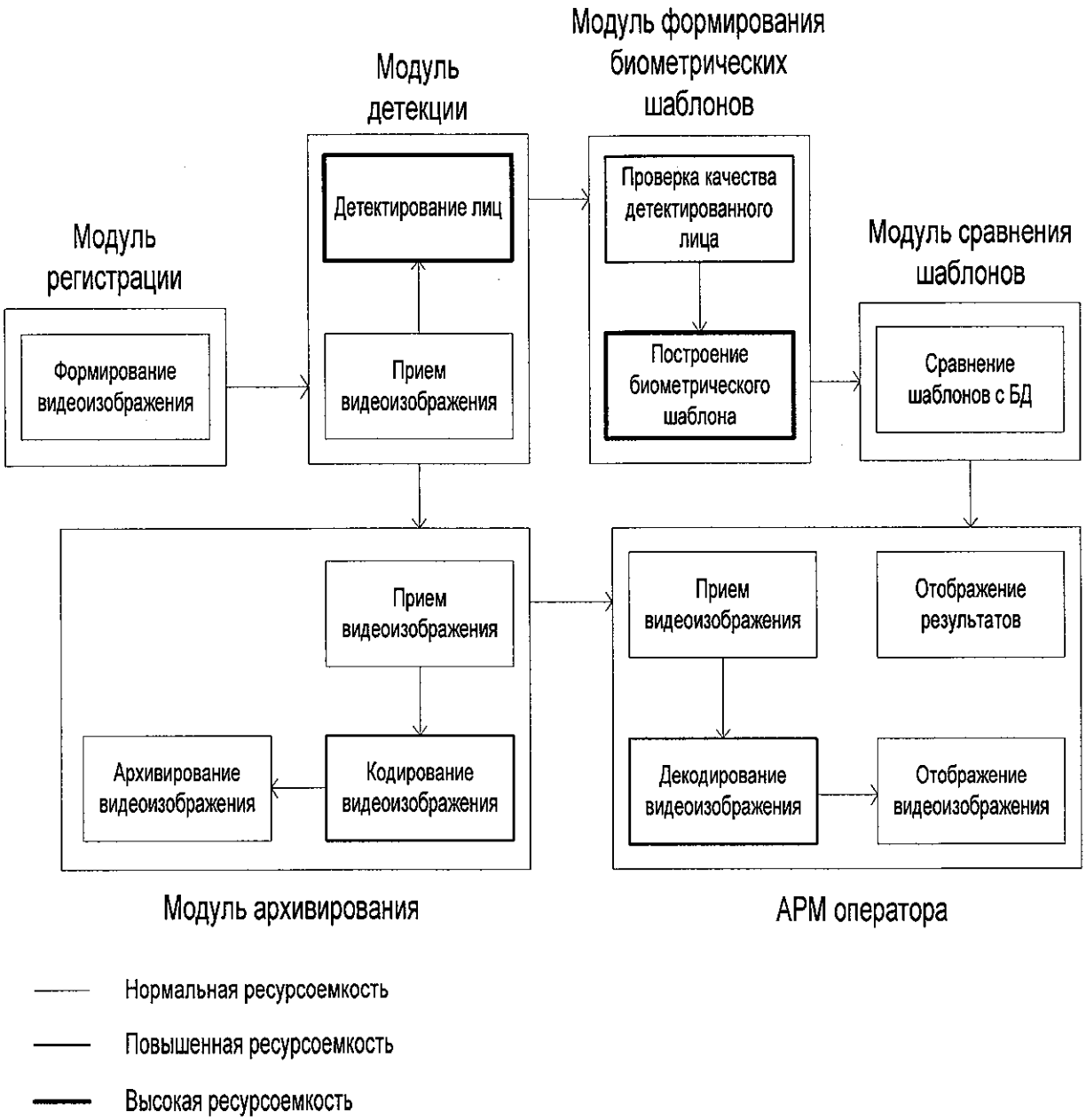


Рисунок 1 - Пример построения архитектуры системы идентификации

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

Требования к базе данных

База данных в составе подсистемы видеоидентификации предназначена для хранения изображений лиц, относительно которых

производится идентификация, их биометрических шаблонов и установочных данных.

Объем информации, хранимой в базе данных:

- 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 подсистемы видеоидентификации:

а) сжатого видеопотока от каждой из камер в составе подсистемы видеоидентификации:

- 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, *.JPEG;

- 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, *.JPEG;

- 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).

В состав подсистемы видеоидентификации должны входить:
- видеокамеры;
- серверное оборудование;
- СПО видеоаналитики.

2) 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 видеоаналитики

№	Параметр	Значение
1.	Разрешение регистрируемого изображения	от 1.3 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:

- 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 подсистемы видеоаналитики.

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 90%;

- доля истинно положительных срабатываний от общего числа срабатываний - не менее 90%.

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 видеоаналитики.

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

Требования к построению архитектуры системы

Подсистема видеоаналитики 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 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 видеоаналитики:

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.

В состав подсистемы видеонаблюдения 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

3) Требования к качеству видеоизображения, регистрируемого камерами из состава подсистемы видеонаблюдения

№	Параметр	Значение
1.	Разрешение регистрируемого изображения	от 1.2 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 подсистемы видеонаблюдения, 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 подсистемы видеонаблюдения и его отображения с использованием интерфейса пользователя.

Интерфейс пользователя должен обеспечивать выполнение следующих функций:

- настройку и конфигурирование СПО подсистемы видеонаблюдения;

- выборочный просмотр видеопотока, регистрируемого камерами из состава подсистемы видеонаблюдения 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 подсистемы видеонаблюдения:

- 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 видеонаблюдения могут входить другие дополнительные технические средства, обеспечивающие размещение и её функционирование. Точный состав, конфигурация и технические характеристики оборудования в составе подсистемы видеонаблюдения, не определенные настоящими требованиями, уточняются на этапе проектирования системы в зависимости от условий эксплуатации на конкретном объекте.

4) Подсистема хранения данных должна обеспечивать запись хранение и выдачу результатов работы составных частей СВН и 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.

Подсистема хранения данных 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 подсистемы хранения данных определяются на этапе проектирования системы.

5) 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 базы данных 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.

6) Взаимодействие систем в составе СВН должно осуществляться на основе открытых стандартов сетевого видео.

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 (SMPTE 292M).

7) 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), не менее
Кодирование основного видеопотока	H.264	H.264
Частота кадров основного видеопотока	24 кадра в секунду	24 кадра в секунду, не менее
Разрешение для записи событий	1080p(1920×1080 пикселей)	1080p(1920×1080 пикселей), не менее
Кодирование для записи событий	MotionJPEG	MotionJPEG
Количество событий в минуту	10	10, не менее
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 150 м.	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 125 м.	Разрешение не менее 1,2 - 2 мегапикселей, выбирается с учетом удаленности и расположения зоны наблюдения; частота кадров не менее 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 15 м	Разрешение не менее 1,3 мегапикселей, выбирается с учетом удаленности 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 8 м.	от 1,2 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 не менее 24 кадров/с; алгоритм сжатия H.264, MJPEG

ПРИЛОЖЕНИЕ № 18

ТРЕБОВАНИЯ

к системам фотовидеофиксации нарушений правил дорожного движения

Системы идентификации транспортных средств (СИТС) предназначены для автоматической регистрации фактов нарушения ПДД и автоматизации процессов выявления нарушений ПДД, формирования, временного хранения, передачи доказательных материалов об административных правонарушениях. Масштабирование СИТС должно осуществляться путем подключения новых рубежей фиксации нарушений ПДД с соответствующим наращиванием мощностей центра обработки данных и сохранении его функциональных возможностей.

Требования к СИТС

СИТС должны обеспечивать автоматическую фиксацию нарушений ПДД с качеством, обеспечивающим достаточную доказательную базу.

Данные от СИТС должны передаваться в центр обработки данных для исполнения действий, предусмотренных Кодексом Российской Федерации об административных правонарушениях (КоАП).

Минимальный перечень нарушений, фиксируемых СИТС, указан в Таблице 1.

Таблица 1

Превышение установленного порога скорости (статья 12.9 КоАП);
Проезд на запрещающий сигнал светофора (статья 12.12.1 КоАП);
Выезд на сторону проезжей части дороги, предназначенную для встречного движения (статьи 12.15.3, 12.15.4 КоАП);
Невыполнение требования ПДД об остановке перед стоп-линией (статья 12.12.2 КоАП);
Невыполнение требования ПДД уступить дорогу пешеходу (статья 12.18 КоАП);
Несоблюдение требований предписанных дорожными знаками или разметкой проезжей части (ч. 3 статьи 12.16 КоАП);
Поворот из несоответствующего крайнего положения на перекрестке, (статья 12.14.1.1 КоАП).

Для каждого транспортного средства - нарушителя, двигающегося в поле обзора, должно быть обеспечено автоматическое формирование изображения общего плана и укрупненного изображения транспортного средства. Укрупненное изображение транспортного средства должно использоваться для оформления постановлений об административных правонарушениях владельцев транспортных средств - нарушителей правил дорожного движения.

В служебном поле фотографии должны быть указаны: зафиксированное нарушение, направление движения, дата и время нарушения, значение максимально допустимой скорости на данном участке дороги (если нарушен скоростной режим), географические координаты места нарушения, серийный номер комплекса.

Сохраняемые данные о нарушении должны заключать в себя цифровую фотографию транспортного средства нарушителя, номер государственного регистрационного знака (ГРЗ), тип нарушения, зафиксированную скорость транспортного средства (если нарушен скоростной режим), направление движения, дату и время нарушения, значение максимально допустимой скорости на данном участке дороги, место нарушения, серийный номер комплекса.

Данные о нарушении должны храниться в отдельных файлах общепринятых форматов.

Класс защиты по погодным условиям для оборудования, устанавливаемого на рубежах контроля, должен быть не ниже IP65 и обеспечивать круглогодичное функционирование в погодных условиях региона.

СИТС должны иметь действующее свидетельство федерального агентства по техническому регулированию и метрологии о внесении комплекса в государственный реестр средств измерений (сертификат об утверждении типа средств измерений), сертификат соответствия, паспорт.

Оборудование СИТС должны соответствовать следующим характеристикам:

- измерение скорости транспортного средства с помощью радарного и безрадарного метода;

- механизм автокалибровки и автоматической оптимизации программных настроек;

- ГЛОНАСС - приемник в наличии;

- диапазон измерения скорости ТС - от 0 до 255 км/ч.;

- пределы допускаемой погрешности измерений расстояния от комплекса до ТС - не более +/- 1 м.;

- минимальная рабочая температура окружающей среды - -45 °С;

- максимальная рабочая температура окружающей среды - +55 °С;

- распознавание номеров транспортного средства (ТС) в латинской и кириллической кодировке;

- возможность дистанционного мониторинга состояния оборудования комплекса, настройки оборудования комплекса;

- обеспечивать распознавание передних и задних ГРЗ;

- обеспечивать распознавание регистрационных знаков в диапазоне от 5 до 160 метров;

- возможность настройки контролируемых направлений движения - приближающиеся или удаляющиеся ТС;

- межповерочный интервал оборудования должен составлять не менее одного года;

- оборудование должно позволять проводить метрологическую поверку без снятия его с места установки;

срок службы не менее 5 лет.

ПРИЛОЖЕНИЕ № 19

ТРЕБОВАНИЯ

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

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

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

- двигатель - заведен/заглушён;
- данные от датчика уровня топлива в баке;
- данные от дополнительных датчиков.

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 № 20

ТРЕБОВАНИЯ

к техническому обеспечению к систем функционального блока "Экологическая безопасность"

К системам 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 также нефтепродуктами, металлической ртутью и ее соединениями);
- оценка показателей 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 систем функционального блока "Экологическая безопасность" должен включать в свой состав следующие компоненты:

пост атмосферного мониторинга;

передвижная экологическая лаборатория контроля состояния атмосферного воздуха, воды и почвы;

автоматизированный стационарный пост сейсмологического контроля;

подсистема автоматического контроля промышленных выбросов;

подсистема контроля утилизации отходов;

автоматизированный гидрологический пост.

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.

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.

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.

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.

Система контроля утилизации отходов

Должна предусматривать оборудование мусоровозов датчиками спутникового слежения ГЛОНАСС/GPS и оборудование камерами видеонаблюдения въездов на городские свалки и/или мусороперерабатывающие предприятия.

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 № 21

НАЗНАЧЕНИЕ

КСА мониторинга социальных медиа

КСА мониторинга социальных медиа должен обеспечивать выполнение следующих возможностей:

сбор в социальных медиа сообщений, содержащих признаки угроз возникновения КСП, их фильтрация для устранения социального шума, а также передача информации в автоматизированные системы органов повседневного управления РСЧС;

обнаружение значимых событий связанных с угрозой КСП или происшествиями, находящиеся в ранней стадии своего развития в социальных сетях, и предоставление инструментов для оценки их достоверности;

предоставление инструментов для мониторинга 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;

предоставление инструментов для анализа 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 сеть Интернет, в том числе провоцирование социальной, межнациональной, религиозной напряженности;

предоставление инструментов для поиска и выявления первопричин и/или последствий событий, обнаруженных в социальных медиа;

осуществление обработки собранной информации и максимально быстрое предоставление должностным лицам в удобной для анализа форме.

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.

Допускается реализация КСА мониторинга общественного мнения на региональном уровне.

ПРИЛОЖЕНИЕ № 22

ТРЕБОВАНИЯ

к подсистеме радиационного мониторинга и аварийного реагирования на ЧС с радиационным фактором в крупных городах (ПРМиАР)

Чрезвычайные ситуации с радиационным фактором, в том числе и террористические акты, могут нанести гораздо более значительный ущерб крупным городам, чем другим селитебным территориям. Среди основных факторов, способствующих этому можно выделить социально-демографические и инфраструктурные особенности городов и характер формирования радиоактивного загрязнения.

Социально-демографические и инфраструктурные особенности крупных городов:

высокая плотность населения;

значительная концентрация социально-бытовых и культурных объектов;

наличие особо опасных промышленных объектов разного типа, включая ядерно и радиационно опасные;

наличие критически важных объектов инфраструктуры, систем жизнеобеспечения, включая разветвленную транспортную систему;

Характер формирования радиоактивного загрязнения:

высокая неоднородность радиоактивного загрязнения;

формирование локальных участков с высоким уровнем загрязнения (водостоки, обочины дороги т.д.);

наличие вертикальной и высотной составляющей радиоактивного загрязнения (фасады и крыши строений);

значимый антропогенный перенос загрязнения с транспортом и пешеходами;

ветровой подъем и распространение радиоактивного загрязнения за счет локальных ветровых потоков на застроенной территории.

Наличие вышеуказанных особенностей, относящихся к крупным городам, требует создания подсистемы радиационного мониторинга и аварийного реагирования включающей в себя разветвленную городскую сеть стационарных автоматизированных постов радиационного контроля, а также передвижные радиометрические лаборатории, оснащенные современным измерительным, компьютерным и коммуникационным оборудованием.

Назначением подсистемы радиационного мониторинга и аварийного реагирования на ЧС с радиационным фактором в крупных городах является инструментальный контроль радиационной обстановки (подтверждение нормальной радиационной обстановки в местах расположения автоматизированных постов контроля радиационной обстановки при повседневной деятельности, раннее предупреждение об изменении радиационной обстановки, обеспечение данными по радиационной обстановке в местах размещения постов контроля в режиме ЧС) и информационная поддержка деятельности территориальных и федеральных органов исполнительной власти по обеспечению радиационной безопасности.

ПРМиАР является источником информации о радиационной обстановке на территории крупного города для органов, осуществляющих контроль радиационной обстановки и обеспечивающих защиту населения при ЧС с радиационным фактором, а также населения и СМИ.

В состав ПРиАР должны входить следующие основные элементы:

1) стационарные автоматизированные посты радиационного контроля;

2) передвижная радиометрическая лаборатория (ПРЛ);

3) центр сбора обработки информации.

Стационарный автоматизированный пост контроля радиационной обстановки должен включать в себя:

1) блок детектирования гамма-излучения, обеспечивающий измерение мощности амбиентного эквивалента дозы гамма-излучения;

2) блок обработки и передачи данных, предназначенный для сбора измерительной информации с блоков детектирования;

3) электронное информационной табло для отображения результатов измерения параметров радиационной обстановки.

Блок детектирования мощности дозы гамма-излучения должен иметь следующие характеристики:

1) диапазон измерения (γ), мкЗв/ч: не более чем от 0,1 не менее чем до 104;

2) диапазон регистрируемых энергий, МэВ: не более чем от 0,06 не менее чем до 1,5;

3) основная относительная погрешность, %: не более 20;

4) диапазон рабочих температур, °С: от - 40 до +60;

5) наличие одного или нескольких стандартных интерфейсов связи (RS-232, RS-485, USB и др.);

6) наличие стандартного открытого протокола обмена данными измерений (ModBusRTU, ModBusTCP и др.).

Блок обработки и передачи данных (БОП) должен обеспечивать автоматический контроль работоспособности внешних устройств, с выдачей информации о статусе их состояния во внешнюю информационную сеть.

Блок обработки и передачи данных должен обладать следующими характеристиками:

1) предварительная обработка данных поступающих от блоков детектирования гамма излучения;

2) наличие стандартных интерфейсов связи (RS-232, RS-485, USB, Ethernet и др.) необходимых и достаточных для подключения блоков детектирования гамма-излучения, электронного информационного табло для вывода результатов измерения, автоматического метеорологического комплекса;

3) обеспечение электропитанием блока детектирования гамма-излучения;

4) наличие возможности передачи данных, как с использованием сетей сотовых операторов, так и проводных локальных вычислительных сетей;

5) наличие возможности автономной работы от встроенного аккумулятора, не менее 10 часов при температуре окружающего воздуха + 20 °С;

6) степень защиты оболочек не менее IP 65 по ГОСТ 14254-96;

7) электропитание: ~220 В, 50 Гц.

Требования к характеристикам электронного информационного табло должны определяться на этапе проектирования подсистемы с учетом конкретных мест установки табло.

Из числа стационарных автоматизированных постов контроля радиационной обстановки выделяются опорные стационарные посты, которые дополнительно оснащаются автоматическим метеорологическим комплексом и автоматизированными спектрометрическими устройствами для определения нуклидного состава радиоактивного загрязнения.

Автоматический метеорологический комплекс, которым оснащаются опорные стационарные посты контроля радиационной обстановки должен обладать характеристиками не хуже чем характеристики, указанные ниже:

1) диапазон измерения температуры воздуха, °С: от - 50 до +60;

2) диапазон измерения скорости ветра, м/с: 0 до 60;

3) диапазон измерения направления ветра, град: от 00 до 3600;

4) диапазон измерения влажности воздуха, % отн.: от 0 до 100;

5) диапазон измерения атмосферного давления, гПа: от 600 до 1100.

Спектрометрическое устройство для определения нуклидного состава радиоактивного загрязнения должно обладать характеристиками не хуже характеристик, приведенных ниже:

1) диапазон регистрируемых энергий, МэВ: не более чем от 0,06 не менее чем до 3;

2) относительное энергетическое разрешение по линии 662 кэВ (137Cs) не более 8;

3) интегральная нелинейность, % не более 1;

4) число каналов накапливаемого спектра не менее 1024;

5) емкость канала накапливаемого спектра не менее 232-1;

6) степень защиты оболочек не менее IP 54 по ГОСТ 14254-96:

- наличие одного или нескольких стандартных интерфейсов связи (RS-232, RS-485, USB и др.);

- наличие стандартного открытого протокола обмена данными измерений (ModBusRTU, ModBusTCP и др.).

Надежность ПРМиАР должна характеризоваться следующими значениями показателей надежности:

- средняя наработка на отказ должна быть не менее 10 000 часов;

- коэффициент готовности должен быть не менее 0,997 при времени восстановления не более 3 часов.

Передвижная радиометрическая лаборатория должна обеспечивать выполнение следующих задач:

- доставка персонала, измерительного и вспомогательного оборудования к местам проведения работ;

- проведение гамма-съемки на местности и одновременной привязкой к координатам измерения и с передачей результатов измерения в центр сбора и обработки информации ПРМиАР в режиме реального времени;

- определение местонахождения источников ионизирующего излучения, и оценка радионуклидного состава источника;

- отбор, транспортировка проб почвы, воды и воздуха.

Все средства измерения, входящие в состав ПРМиАР должны быть внесены в Государственный реестр средств измерения и иметь отметку о метрологической поверке.

Центр сбора и обработки информации должен иметь в своем составе серверное и телекоммуникационное оборудование, а также программное обеспечение обеспечивающее выполнение следующих задач:

- получение в автоматическом режиме данных измерений со стационарных автоматизированных постов контроля радиационной обстановки;

- получение в автоматическом режиме данных гамма-съемки местности с передвижной радиометрической лаборатории;

- хранение и архивирование полученных данных;

- оперативная передача информации в КСА ЕЦОР для обработки на предмет превышения контролируемых параметров радиационной обстановки установленных пороговых значений;

- оценка и прогноз радиационной обстановки и радиологических последствий в зоне загрязнения на территории города.

Оценка и прогноз радиационной обстановки и радиологических последствий в зоне загрязнения должны выполняться с использованием сертифицированного программного обеспечения.

Стационарные автоматизированные посты радиационного контроля должны размещаться на территории города с учетом потенциальных источников радиационной опасности, их характеристик, результатов анализа многолетних наблюдений за метеопараметрами, результатов анализа проектных и запроектных аварий, мест проживания населения, расположения обеспечивающей инфраструктуры.

Число стационарных автоматизированных постов радиационного контроля определяется в зависимости от численности населения в городе, площади населенного пункта, рельефа местности и степени индустриализации, рассредоточенности мест массового скопления населения и в зависимости от численности населения.

Конкретное количество постов определяется с учетом рельефа местности, наличии ядерно радиационно опасных объектов (ЯРОО) всех категорий потенциальной опасности по ОСПОРБ-99/2010 на территории города, наличии ЯРОО 1-й категории опасности по ОСПОРБ-99/2010 на удалении менее 100 км от городской черты и на основании анализа расчетов последствий потенциальных радиационных аварий, полученных с помощью сертифицированных программных комплексов.

ПРИЛОЖЕНИЕ № 23

ТРЕБОВАНИЯ

к Единому стеку открытых протоколов (ЕСОП) информационного взаимодействия АПК "Безопасный город"

Назначением единого стека открытых протоколов информационного взаимодействия (ЕСОП) АПК "Безопасный город", а также взаимодействующих с ним КСА является формализация форматов, правил и регламентов взаимодействия между всеми участниками информационного обмена, в том числе с сервисной платформой правоохранительного сегмента 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 взаимодействия с сервисной платформой правоохранительного сегмента.

Семантические модели данных ЕСОП должны отвечать следующим требованиям:

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

Взаимодействие АПК "Безопасный город" с сервисной платформой правоохранительного сегмента 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-IBasicProfile и др. Допускается ограничивать требования таких стандартов и спецификаций до объема, 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 XMLSchema. Взаимодействие с такими сервисами должно отвечать требованиям WS-IBasicProfile 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 и/или с использованием сертифицированных наложенных средств защиты каналов связи.

В части взаимодействия с КСА видеомониторинга, видеообнаружения, видеоидентификации, видеораспознавания и других КСА, занимающихся обработкой медиаданных (видео-, аудио- и фотоданных) протокол должен быть открыт и взаимодействовать со всеми существующими протоколами обмена с соответствующими системами. 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 BaseNotification в соответствии с ONVIF CoreSpecification (раздел 9.1) версии не ниже 2.4 является обязательной [1]. Для передачи информации о событиях в пакете Notify в рамках интерфейса BaseNotification следует использовать либо структуру данных Message, определенную в ONVIF CoreSpecification (раздел 9.5.2), либо структуру данных alert, определенную в CommonAlertingProtocol версии 1.2 [2].

Протокол в части передачи извещений должен определять машинный язык, который позволяет описывать коды в форме нескольких тем извещений в соответствии с WS-Topics (применяется в WS-BaseNotification и ONVIF Event Service для описания кодов событий). ЕСОП должен определять глоссарий общих тем извещений, таких как "Тревога", "Норма", "Неисправность" и др. Специализированные глоссарии, определяющие новые темы извещений, могут быть как разработаны и внедрены на уровне КСА, так и включены позднее в ЕСОП. В каждом извещении должен передаваться код, состоящий из нескольких тем извещений из любых глоссариев. В коде каждого извещения должна

---

[1] Обязательный The Real-time Pull-Point Notification Interface в соответствии с ONVIF CoreSpecification требует постоянного опроса источников событий и поддержания 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 BaseNotification 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.

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, определенные в отраслевом стандарте ONVIF. Кроме того, в общий глоссарий могут 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 (операционные) риски;
- в области экстренного реагирования (системы 112).

ПРИЛОЖЕНИЕ № 24

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

к правоохранительному сегменту АПК "Безопасный город"

1. Цели и задачи правоохранительного сегмента АПК "Безопасный город"

1.1. Целью создания (развития) правоохранительного сегмента АПК "Безопасный город" (далее - ПС) является повышение уровня общественной безопасности в субъектах Российской Федерации за счет повышения качества информационного сопровождения повседневной и оперативно-служебной деятельности должностных лиц органов внутренних дел Российской Федерации путем развития существующих и внедрения новых технических решений с использованием современных информационных технологий.

1.2. Основными задачами ПС являются:

- получение сведений из информационных систем, входящих в АПК "Безопасный город";
- получение сведений от камер видеонаблюдения и систем фото-видеофиксации, расположенных в субъекте Российской Федерации;
- получение сведений о происшествиях и тревожных событиях от систем безопасности объектов, включая объекты транспортной инфраструктуры.

2. Требования к правоохранительному сегменту АПК "Безопасный город"

2.1. В целях обеспечения работы ПС используются следующие системы и подсистемы АПК "Безопасный город":

- средства видеонаблюдения;
- средства фотовидеофиксации нарушения правил дорожного движения;
- пункты экстренной связи "Гражданин-полиция";
- телекоммуникационная инфраструктура;
- система сбора и хранения данных;
- программное обеспечение;
- система защиты информации;
- эксплуатационная документация.

2.2. Требования к средствам видеонаблюдения в целях обеспечения работы ПС:

2.2.1. Средства видеонаблюдения должны обеспечивать возможность фиксации фактов совершения криминальных действий в соответствии с указанием МВД России от 29.10.2009 №28/НПО-5307 "О требованиях к подсистеме видеонаблюдения АПК "Безопасный город" (Технические требования ЭКЦ МВД России к системам охранным телевизионным (СОТ), используемым на улицах и в других общественных местах для получения изображений, пригодных для проведения идентификационных исследований).

2.2.2. Средства видеонаблюдения должны обеспечивать следующие технические характеристики:

- минимально допустимый размер объекта в кадре должен составлять не менее 240 пикселей по горизонтали, расстояние до объекта и параметры объектива телекамеры (ТК) должны удовлетворять указанному условию;
- при использовании цифровых видеонакопителей прогрессивная строчная развертка, чересстрочная кадровая развертка не допускаются;
- ТК с цифровым видеонакопителем должны на аппаратном уровне обеспечивать получение кадра на выходе не ниже 720 х 576 пикселей;
- для цветного изображения цветовая насыщенность 24-битного изображения должна быть таковой, чтобы при его преобразовании к изображению в градациях серого, динамический диапазон интенсивности кодировался не менее чем 7 битами;
- для черно-белого изображения динамический диапазон интенсивности изображения (разрядность шкалы градаций серого) должен кодироваться не менее чем 8 битами;
- структура дискретизации цифрового сигнала должна составлять 4:2:2;
- режим записи должен быть не менее 25 кадров/сек по каждому каналу;
- видеоинформация должна представляться в виде последовательных статических фотографических картинок с параметрами не хуже вышеуказанных. Применение алгоритмов цифровой обработки (компрессии видеоинформации) с межкадровым сжатием не допускается;
- значение разрешения должно составлять не менее 450 ТВЛ для цветных ТК и не менее 500 ТВЛ для черно-белых;
- светочувствительность ТК должна составлять не менее 0,1 лк;

- разрешающая способность объектива ТК должна быть не хуже 40 lp/mm.

2.2.3. При монтаже и установке средств видеонаблюдения должны обеспечиваться следующие требования:

- средства видеонаблюдения должны быть установлены максимально близко к горизонтальной визирной линии по отношению к фиксируемому объекту наблюдения, отклонение от горизонтальной визирной линии должно составлять ± 15 градусов;

- при установке режимов работы средств видеонаблюдения необходимо учитывать скорости перемещения объектов, находящихся в зоне видимости ТК, с тем, чтобы исключить появление нерезких изображений и "смазов" на записанных видеокадрах;

- не допускается установка средств видеонаблюдения в местах, где не обеспечена достаточная освещенность объекта, наблюдается избыточная освещенность (блики, тени), контровой свет, делающие невозможным выявление на изображении индивидуализирующих объект признаков.

2.2.4. Адреса, места размещения, сроки ввода и вывода из эксплуатации средств видеонаблюдения должны быть согласованы с территориальным органом внутренних дел.

2.2.5. Применяемые средства видеонаблюдения должны пройти оценку соответствия технических характеристик в заинтересованных подразделениях МВД России в установленном порядке.

2.2.6. Изменение технических характеристик средств видеонаблюдения допускается по согласованию с заинтересованными подразделениями МВД России.

2.3. Требования к средствам фотовидеофиксации нарушений правил дорожного движения (СФВФ) в целях обеспечения работы ПС:

2.3.1. СФВФ должны соответствовать требованиям:

- Постановления Правительства Российской Федерации от 29 сентября 2016 г № 969 "Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности";

- ГОСТ Р 57144-2016 "Специальные технические средства, работающие в автоматическом режиме и имеющие функции фото- и

киносъемки, видеозаписи, для обеспечения контроля за дорожным движением. Общие технические требования";

- ГОСТ Р 57145-2016 "Специальные технические средства, работающие в автоматическом режиме и имеющие функции фото- и киносъемки, видеозаписи, для обеспечения контроля за дорожным движением. Правила применения";

- приказа МВД России от 8 ноября 2012 г. № 1014 "Об утверждении перечня измерений, относящихся к сфере государственного регулирования обеспечения единства измерений и обязательных метрологических требований к ним";

2.3.2. СФВФ нарушения правил дорожного движения (ПДД) должны обеспечивать:

- контроль дорожной обстановки и автоматическое детектирование фактов нарушений ПДД, в том числе превышение разрешенного скоростного режима, выезд на встречную полосу, движение задним ходом, проезд на запрещающий сигнал светофора, нарушение пропускного режима и другие нарушения ПДД, определяемые территориальным органом МВД России, исходя из реальных условий организации движения в зонах контроля;

- возможность фотовидеофиксации факта нарушения ПДД не менее чем с двух точек обзора;

- фотовидеофиксацию и считывание номерных знаков транспортных средств (ТС), попавших в зону контроля;

- фотовидеофиксацию распознанного номерного знака ТС, нарушившего ПДД.

2.3.3. СФВФ должны обеспечивать круглосуточный режим работы.

2.3.4. Средства защиты и поворотные устройства СФВФ должны обеспечивать выполнение следующих требований по механическому воздействию и температурному режиму:

- класс защиты - не хуже IP66 в соответствии с ГОСТ 14254-96;

- рабочий диапазон температур не хуже -40/+50 градусов Цельсия.

2.3.5. Поворотные устройства СФВФ должны обеспечивать выполнение следующих требований по ориентации в пространстве:

- максимальный угол поворота по горизонтали - не менее 300 градусов;

- максимальный угол поворота по вертикали - не менее 120 градусов;

- скорость поворота - не менее 30 градусов в секунду;

- точность позиционирования - не хуже 3 градусов;

- интерфейс управления поворотными устройствами: RS422, RS232, RS485.

2.3.6. Адреса, места размещения, сроки ввода и вывода из эксплуатации СФВФ должны согласовываться с территориальными органами МВД России.

2.3.7. Применяемые СФВФ должны пройти оценку соответствия технических характеристик в МВД России в установленном порядке.

2.3.8. Изменение технических характеристик СФВФ допускается по согласованию с заинтересованными подразделениями МВД России.

2.4. Требования к пунктам экстренной связи "Гражданин-полиция" (ПЭС ГП) в целях обеспечения работы ПС:

2.4.1. ПЭС-ГП предназначены для обеспечения круглосуточной оперативной связи граждан с операторами линий "02" подразделений территориального ОВД.

2.4.2. ПЭС-ГП должны обеспечивать решение следующих задач:

- предоставление гражданам круглосуточной оперативной экстренной голосовой связи с операторами линий "02";

- ручное и автоматическое управление видеокамерами наблюдения, подключенными к пункту экстренной связи, с автоматической регистрацией аудио и видео сигнала;

- многоканальную запись аудио и видео переговоров с возможностью их прослушивания и передачи в электронном виде на другие сетевые устройства.

2.4.3. Пункт экстренной связи должен представлять собой оконечное устройство, состоящие из переговорного блока, видеокамеры и датчика вскрытия в полной комплектации, либо только переговорного блока и датчика вскрытия.

2.4.4. Пункт экстренной связи, оборудованный видеокамерой, должен обеспечивать:

- визуальный и акустический контроль оперативной обстановки в зоне его действия;

- двусторонний сеанс видеосвязи между гражданином и операторами линий "02".

2.4.5. Пункт экстренной связи, не оборудованный видеокамерой, должен обеспечивать двусторонний дуплексный сеанс голосовой связи между гражданином и операторами линий "02".

2.4.6. Пункт экстренной связи, должен быть выполнен в антивандальном исполнении и работать в круглосуточном режиме в диапазоне температур от - 30 до +50° С.

2.4.7. Пункт экстренной связи должен строиться на базе стандартов TCP/IP, IP телефонии и обеспечивать передачу видеосигнала и управляющих сигналов по сетям Ethernet, а также содержать интерфейсы (интерфейсные блоки), преобразующие сигналы аудио, видео и сигнализации в формат Ethernet.

2.4.8. Интерфейсные блоки должны поддерживать стандарты связи аудио H.323, G.711 (для "узких" каналов связи - G729), видео MJPEG, MPEG4, H.263 (с возможностью двусторонней видеосвязи).

2.4.9. Полученные сигналы должны иметь возможность переадресации на любые внешние, в том числе телефонные линии связи.

2.4.10. Аппаратура ПЭС-ГП должна обеспечивать выполнение следующих требований МВД России к качеству аудиоинформации и ее пригодности для проведения идентификационных исследований по голосу и речи:

- средний частотный диапазон частот - не менее 100 - 5500 Гц;
- средняя величина отношения сигнал/шум - не менее 15 дБ;
- отсутствие шумовых и тональных помех, а также нелинейных искажений, разрушающих гармоническую структуру звуков;
- стандарт цифровой записи - PCM (импульсно-кодовая модуляция) без сжатия данных;
- режим записи - моно/стерео;
- разрядность - не менее 16 бит;
- частота дискретизации - не менее 11025/116000 Гц;
- неравномерность амплитудно-частотной характеристики - не более 2 дБ;
- соотношение сигнал/шум на микрофонном входе - не менее 75 дБ;
- коэффициент нелинейных искажений - не более 1%;
- двухканальный режим записи с раздельной фиксацией речи дикторов по каналам при документировании телефонных переговоров.

2.4.11. Устройство передачи голосовых сообщений должно иметь заключение МВД России о пригодности устройства для проведения идентификационных исследований по голосу и речи;

2.4.12. Аппаратура регистрации переговоров должна иметь заключение МВД России о пригодности получаемой с его помощью

аудиоинформации для проведения идентификационных исследований по голосу и речи.

2.4.13. Адреса, места размещения, сроки ввода и вывода из эксплуатации ПЭС-ГП должны быть согласованы с территориальным органом внутренних дел.

2.4.14. Применяемые ПЭС-ГП должны пройти оценку соответствия технических характеристик в заинтересованных подразделениях МВД России в установленном порядке.

2.4.15. Изменение технических характеристик ПЭС-ГП допускается по согласованию с заинтересованными подразделениями МВД России.

2.5. Требования к телекоммуникационной инфраструктуре в целях обеспечения работы ПС

2.5.1. Телекоммуникационная инфраструктура ПС должна обеспечивать:

- защищенную передачу информации получаемой от средств видеонаблюдения, СФВФ, ПЭС-ГП, информационных систем АПК "Безопасный город" по классу криптографической защиты КС1;

- защищенную передачу информации из системы хранения данных ПС в интегрированную мультисервисную телекоммуникационную сеть (ИМТС) МВД России по классу криптографической защиты не менее КС3.

2.5.2. Подключение к ИМТС должно осуществляться в соответствии с соглашением об информационном взаимодействии, заключаемым между муниципальным органом власти и территориальным органом МВД России по согласованию с заинтересованными подразделениями МВД России, а также протоколами по информационному и технологическому взаимодействию и обеспечению информационной безопасности, которые являются неотъемлемой частью соглашения об информационном взаимодействии.

2.5.3. В состав телекоммуникационной инфраструктуры могут входить радио и проводные каналы связи, обеспечивающие пропускную способность, достаточную для передачи информации поступающих от указанных в пункте 2.6.1 средств и систем в реальном масштабе времени.

2.6. Требования к системе сбора и хранения данных в целях обеспечения работы ПС

2.6.1. Система сбора и хранения данных должна обеспечивать:

- сбор данных поступающих от средств видеонаблюдения, СФВФ, ПЭС-ГП, информационных систем АПК "Безопасный город";

- хранение собранных данных не менее 30 суток со дня получения;

- предоставление по запросу собранной информации в единую систему информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России).

2.6.2. Серверы, используемые в системе сбора и хранения данных АПК "Безопасный город", должны быть построены на базе многоядерных микропроцессоров, в том числе семейства "Эльбрус".

2.6.3. МВД России и территориальный орган МВД России может иметь возможность осуществлять контроль доступа к оборудованию системы сбора и хранения данных АПК "Безопасный город", а также в помещение, в котором оно расположено.

2.6.4. По согласованию с МВД России и территориальным органом МВД России должен быть разработан регламент осуществления эксплуатации оборудования ПС.

2.7. Требования к программному обеспечению

2.7.1. Программное обеспечение ПС должно обеспечивать выполнение функций, перечисленных в пунктах 2.3 - 2.7.

2.7.2. Программное обеспечение должно быть основано на программном обеспечении с открытым исходным кодом, сертифицировано в системе сертификации ФСТЭК России и быть свободным от лицензионных отчислений в сторону третьих лиц.

2.7.3. Права на программное обеспечение должны принадлежать Российской Федерации.

2.8. Требования к системе защиты информации в целях обеспечения работы ПС

2.8.1. СЗИ должны удовлетворять следующим требованиям:

- максимальный гриф секретности обрабатываемой информации - "несекретно";

- класс защищенности - не ниже К2, в соответствии с порядком классификации, определенным приказом ФСТЭК России № 17 от 11 февраля 2013 г.;

- уровень защищенности персональных данных - не ниже У32, в соответствии с постановлением Правительства Российской Федерации № 1119 от 1 ноября 2012 г.

2.8.2. СЗИ для обработки информации, не содержащей государственную тайну должны соответствовать действующим нормативным правовым актам Российской Федерации и МВД России в области информационной безопасности.

2.8.3. При реализации СЗИ должны использоваться применяемые в МВД России средства защиты информации.

2.8.4. МВД России и территориальному органу МВД России может быть предоставлена возможность для осуществления контроля работы СЗИ ПС и управления доступом к ПС.

2.8.5. Изменение технических характеристик СЗИ допускается по согласованию с заинтересованными подразделениями МВД России.

2.8.6. Требования к вероятностно-временным характеристикам.

2.8.6.1. Среднее время между предъявлением ПС входных данных в виде формализованного запроса объемом не более 5 кбайт с рабочих мест должностных лиц ОВД МВД России и получением соответствующей выходной информации объемом не более 50 кбайт должно составлять не более 10 секунд с вероятностью обслуживания не менее 0,9.

2.8.6.2. Должна быть построена математическая модель с декомпозицией по составляющим элементами и проведено имитационное моделирование работы для оценки качества функционирования и производительности системы.

2.8.7. Изменение технических характеристик СЗИ допускается по согласованию с заинтересованными подразделениями МВД России.

2.9. Требования по живучести и стойкости к внешним воздействиям

2.9.1. Приобретаемые или создаваемые технические средства должны быть стойкими, прочными и устойчивыми к внешним воздействующим факторам в соответствии с требованиями ГОСТ РВ 20.39.304, ГОСТ РВ 20.39.308 назначения и условий эксплуатации.

2.9.2. В ходе выполнения работы должны быть проведены мероприятия по оценке устойчивости оборудования, входящего в состав ПС к воздействиям:

- электростатических разрядов по ГОСТ Р 51317.4.2;

- радиочастотного электромагнитного поля по ГОСТ Р 51317.4.3, ГОСТ Р 51317.4.6;

- наносекундных импульсных помех по ГОСТ Р 51317.4.4;

- микросекундных импульсных помех по ГОСТ Р 51317.4.5;

- динамического изменения напряжения питания по ГОСТ Р 51317.4.11;

- аварийного перенапряжения в электросетях по ГОСТ 13109;

- кондуктивным электромагнитным воздействиям по ГОСТ Р 52863.

2.9.3. Объем проводимых мероприятий уточняется по согласованию с заинтересованными подразделениями МВД России.

2.10. Требования по надежности

2.10.1. Надежность ПС в условиях и режимах эксплуатации, установленных пунктом 2.12, должна характеризоваться следующими значениями показателей надежности:

- коэффициент готовности - не менее 0,95;

- среднее время восстановления на объекте эксплуатации силами и средствами дежурной смены - не более 8 часов;

- полный средний срок службы до списания - не менее 5 лет;

- средний срок сохраняемости в заводской упаковке в отапливаемом помещении - не менее 3 лет.

2.10.2. Предельным состоянием ПС считают превышение годовой суммарной стоимости технического обслуживания и текущих ремонтов над амортизационной стоимостью системы.

2.10.3. Отказом ПС считают:

- неработоспособное состояние системы сбора и хранения данных;

- неработоспособное состояние системы защиты информации;

- неработоспособное состояние оборудования видеонаблюдения, СФВФ, ПЭС-ГП в определенных территориальным органом МВД России местах, обозначенных как критически важные.

2.10.4. В ходе выполнения работы должна быть разработана и согласована с МВД России и территориальным органом МВД России программа обеспечения надежности с учетом ГОСТ В 15.206.

2.10.5. Изменение требований по надежности допускается по согласованию с заинтересованными подразделениями МВД России.

2.11. Требования по эксплуатации, хранению, удобству технического обслуживания и ремонта.

2.11.1. ПС должен работать в непрерывном режиме: 7 дней в неделю, 24 часа в сутки, 365 дней в году.

2.11.2. Эксплуатация, техническое обслуживание и ремонт систем должен осуществляться специалистами, прошедших необходимое обучение в строгом соответствии с эксплуатационной документацией.

2.11.3. Изменение требований допускается по согласованию с заинтересованными подразделениями МВД России.

2.12. Требования к стандартизации, унификации и каталогизации.

2.12.1. Требования к стандартизации и унификации.

2.12.1.1. При создании ПС должны применяться действующие в Российской Федерации нормативно-технические документы (НТД).

2.12.1.2. В процессе проведения работы должны быть осуществлены мероприятия по стандартизации с учетом ГОСТ В 15.207.

2.12.1.3. При выполнении работ максимально должны использоваться ранее разработанные средства и технологии.

2.12.2. Требования к каталогизации.

2.12.3. Должны быть проанализированы используемые каталогизированные средства и даны предложения по отказу от покупных изделий иностранного производства в случае наличия ограничений на их применение.

2.12.4. Изменение требований допускается по согласованию с заинтересованными подразделениями МВД России.

2.13. Требования по технологичности

2.13.1. Должны быть проанализированы используемые в ПС аппаратные и программные средства, протоколы и стандарты и даны предложения по обеспечению технологической независимости ПС от изделий иностранного производства с учетом ГОСТ РВ 15.201.

2.13.2. Изменение требований допускается по согласованию с заинтересованными подразделениями МВД России.
