ГОСУДАРСТВЕННАЯ КОМПАНИЯ «РОССИЙСКИЕ АВТОМОБИЛЬНЫЕ ДОРОГИ»
(ГОСУДАРСТВЕННАЯ КОМПАНИЯ «АВТОДОР»)

П Р И К А З

28 декабря 2017г. Москва № 382

Об утверждении и введении в действие стандарта Государственной компании «Российские автомобильные дороги» СТО АВТОДОР 8.8-2017 «Требования к подсистеме ИТС «Видеонаблюдение» на автомобильных дорогах Государственной компании «Российский автомобильные дороги»

В соответствии со статьей 4 Федерального закона от 17 июля 2009 г. № 145-ФЗ «О Государственной компании «Российские автомобильные дороги» и о внесении изменений в отдельные законодательные акты Российской Федерации», ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с даты утверждения настоящего приказа стандарт организации Государственной компании «Российские автомобильные дороги» СТО АВТОДОР 8.8-2017 «Требования к подсистеме ИТС «Видеонаблюдение» на автомобильных дорогах Государственной компании «Российский автомобильные дороги» (Приложение № 1 к настоящему приказу).
2. Утвердить План мероприятий по внедрению стандарта организации СТО АВТОДОР 8.8-2017 «Требования к подсистеме ИТС «Видеонаблюдение» на автомобильных дорогах Государственной компании «Российский автомобильные дороги» (Приложение № 2 к настоящему приказу).
3. Руководителям структурных подразделений Государственной компании «Российские автомобильные дороги» обеспечить реализацию Плана мероприятий, указанного в п. 2 настоящего приказа.
4. Контроль за исполнением настоящего приказа возложить на заместителя председателя правления по технической политике И.Ю. Зубарева.

Председатель правления С.В. Кельбах

Евстигнеев Игорь Анатольевич
Тел. 30-46

ПРИЛОЖЕНИЕ № 1
к приказу Государственной компании
«Российские автомобильные дороги»
от «28» декабря 2017 г. № 382

Стандарт Государственной компании «Автодор»

СТО АВТОДОР 8.8-2017

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ,
ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ

ТРЕБОВАНИЯ К ПОДСИСТЕМЕ ИТС «ВИДЕОНАБЛЮДЕНИЕ» НА АВТОМОБИЛЬНЫХ ДОРОГАХ ГОСУДАРСТВЕННОЙ КОМПАНИИ «РОССИЙСКИЕ АВТОМОБИЛЬНЫЕ ДОРОГИ»

Москва 2017

Предисловие

1 РАЗРАБОТАН: Обществом с ограниченной ответственностью «АРМО-Системы» (ООО «АРМО-Системы») совместно с Департаментом информационных технологий и интеллектуальных транспортных систем Государственной компании «Российские автомобильные дороги».

2 ВНЕСЕН: Департаментом информационных технологий и интеллектуальных транспортных систем Государственной компании «Российские автомобильные дороги».

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ: Приказом Государственной компании «Российские автомобильные дороги» от «28» декабря 2017 г. № 382 _____.

4 ВВЕДЕН ВПЕРВЫЕ.

Оглавление

Стандарт Государственной компании «Автодор»

ТРЕБОВАНИЯ К ПОДСИСТЕМЕ ИТС «ВИДЕОНАБЛЮДЕНИЕ» НА АВТОМОБИЛЬНЫХ ДОРОГАХ ГОСУДАРСТВЕННОЙ КОМПАНИИ «РОССИЙСКИЕ АВТОМОБИЛЬНЫЕ ДОРОГИ»

Requirements for ITS subsystem to «Video observation» on highways of the «Russian Highways» State company

1 Область применения

1.1 Настоящий стандарт устанавливает унифицированные требования к созданию подсистемы ИТС «Видеонаблюдение» (далее – подсистема «Видеонаблюдение») на автомобильных дорогах Государственной компании «Российские автомобильные дороги» (далее – Государственная компания) в части:

- назначение и цели создания подсистемы;
- технико-экономических показателей;
- объекта автоматизации;
- условий эксплуатации;
- требований к подсистеме в целом;
- требований к видам ее обеспечения.

1.2 Настоящий стандарт предназначен для применения структурными подразделениями, филиалами, территориальными управлениями, дочерними и зависимыми обществами, а так же контрагентами Государственной компании.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие нормативные документы:

ГОСТ 12.1.030-81 Система стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление

ГОСТ 12.2.007.0-75 Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности

ГОСТ 14254-2015 (IEC 60529:2013) Степени защиты, обеспечиваемые оболочками (Код IP)

ГОСТ 15150-69 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды

ГОСТ 21958-76 Система «Человек-Машина». Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования

ГОСТ 23118-2012 Конструкции стальные строительные. Общие технические условия

ГОСТ 24.501-82 Автоматизированные системы управления дорожным движением. Общие требования

ГОСТ 24.701-86 Единая система стандартов автоматизированных систем управления

ГОСТ 30.001-83 Система стандартов эргономики и технической эстетики. Основные положения

ГОСТ 12.1.019-2009 Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты

ГОСТ 2.601-2013 Единая система конструкторской документации (ЕСКД). Эксплуатационные документы (с Поправкой)

ГОСТ Р 50839-2000 Совместимость технических средств электромагнитная. Устойчивость средств вычислительной техники и информатики к электромагнитным помехам. Требования и методы испытаний

ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство

ГОСТ 6.10.4-84 Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения

ГОСТ Р 52919-2008 (ЕН 1047-2:1999) Информационная технология (ИТ). Методы и средства физической защиты. Классификация и методы испытаний на огнестойкость. Комнаты и контейнеры данных

ГОСТ Р ИСО 14813-1-2011 Интеллектуальные транспортные системы. Схема построения архитектуры интеллектуальных транспортных систем. Часть 1. Сервисные домены в области интеллектуальных транспортных систем, сервисные группы и сервисы

ГОСТ Р 56294-2014 Интеллектуальные транспортные системы. Требования к функциональной и физической архитектурам интеллектуальных транспортных систем

ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

ГОСТ Р 51558-2014 Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний

СТО АВТОДОР 8.2-2013 Элементы интеллектуальной транспортной системы на автомобильных дорогах Государственной компании

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов (сводов правил и/или классификаторов) в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по опубликованным в текущем году выпускам ежемесячно издаваемого информационного указателя «Национальные стандарты». Если заменен ссылочный стандарт (документ), на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта (документа) с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт (документ), на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта (документа) с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт (документ), на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт (документ) отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 Термины и определения

3.1.1 **внешние информационные системы:** любые внешние самостоятельные организованные системы сбора, хранения и передачи информации.

3.1.2 **видеокамера**: Устройство, предназначенное для телевизионного анализа передаваемой сцены при помощи оптоэлектронного преобразования и передачи телевизионного сигнала. ГОСТ Р 51558-2014 [5]

3.1.3 **видеокомплекс:** Видеокамера, конструктивно и функционально объединенная с устройством, позволяющим осуществлять передачу видеоданных по компьютерной сети или по беспроводным каналам связи, а также комплект воспроизводящей и записывающей видеоаппаратуры.

3.1.4 **дайджест-аутентификация доступа:** Метод, используемый веб-сервером для обработки учетных данных пользователя веб-браузера. Этот метод использует шифрование для отправки пароля через сеть, что является более защищенным способом, чем обычная проверка подлинности доступа, при которой данные посылаются открытым текстом.

3.1.5 **интеллектуальная транспортная система (ИТС)**: Система, интегрирующая современные информационные, коммуникационные и телематические технологии, технологии управления и предназначенная для автоматизированного поиска и принятия к реализации максимально эффективных сценариев управления транспортной системой дороги, конкретным транспортным средством или группой транспортных средств, с целью обеспечения заданной мобильности населения, максимизации показателей использования дорожной сети, повышения безопасности и эффективности

транспортного процесса, комфортности для водителей и пользователей транспорта. ГОСТ Р 56294-2014 [6]

3.1.6 **мобильная (передвижная) видеокамера:** Видеокамера, устанавливаемая на трейлерах, на специальных тележках, на служебном транспорте или специальных машинах.

3.1.7 **пользователь ИТС**: Лицо, группа лиц или организация, пользующееся услугами информационной системы для получения информации или решения других задач.

3.1.8 **технические средства ИТС:** Совокупность технических средств телематики в рамках решений одной или нескольких прикладных задач.

3.1.9 **центр управления (ЦУ):** Орган управления производственными и технологическими процессами ИТС (АСУДД), обслуживающий автомобильные дороги Государственной компании.

3.1.10 **центральная система верхнего уровня ИТС:** Центр ситуационного управления Государственной компании.

3.2 Сокращения

АРМ	Автоматизированное рабочее место
АСУДД	Автоматизированная система управления дорожным движением
БД	База данных
БПЛА	Беспилотный летательный аппарат
ВОЛС	Волоконно-оптическая линия связи
ДИТ	Дорожное информационное табло
ДКШ	Дорожный коммутационный шкаф
ДТП	Дорожно-транспортное происшествие
ЗИП	Запасные части и принадлежности
ИБП	Источник бесперебойного питания
ИТС	Интеллектуальная транспортная система

НСД	Несанкционированный доступ
ПВП	Пункт взимания платы
ПУЭ	Правила устройства электроустановок
СВП	Система взимания платы
СМИ	Средства массовой информации
СУБД	Система управления базами данных
СХД	Система хранения данных
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦУ	Центр управления
API	Application Programming Interface - набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах
Ethernet	Семейство технологий пакетной передачи данных для компьютерных сетей
GIF	Graphics Interchange Format - формат для обмена графическими изображениями
H.264	Лицензируемый стандарт сжатия видео, предназначенный для достижения высокой степени сжатия видеопотока при сохранении высокого качества
HDTV	High Definition Television - стандарт для цифрового телевидения с высокой четкостью изображения
HTTP	Hyper Text Transfer Protocol - протокол прикладного уровня передачи данных
HTTPS	Hyper Text Transfer Protocol Secure -расширение протокола HTTP для поддержки шифрования в целях повышения безопасности

IP	Internet Protocol - межсетевой протокол, маршрутизируемый протокол сетевого уровня стека TCP/IP
JPG (JPEG)	Joint Photographic Experts Group - графический формат, обеспечивающий наилучшее сжатие при наименьшей потере качества изображения
MJPEG	Motion JPEG - покадровый метод видеосжатия, основной особенностью которого является сжатие каждого отдельного кадра видеопотока с помощью алгоритма сжатия изображений JPEG
MM	Многомодовое оптическое волокно
MOV	Формат мультимедийных типов файлов, который работает с плеерами Apple и QuickTime.
MP4	MPEG-4 Part 14 формат медиаконтейнера, являющийся частью стандарта MPEG-4. Используется для упаковки цифровых видео - и аудиопотоков, субтитров, афиш и метаданных
ONVIF	Open Network Video Interface Forum - отраслевая международная организация, которая занимается разработкой стандартизованных протоколов для взаимодействия различного оборудования и программных средств, входящих в состав систем безопасности (видеокамер, IP-кодеров, видеорегистраторов, контроллеров доступа и т.п.). В рамках спецификаций описания совокупности определенных функций по прикладному назначению объединяется в профили. В частности, разработаны Profile S (для видеоисточников), Profile G (для устройств записи видео)
PTZ	Pan-tilt-zoom - панорамирование, наклон, зум (изменение масштаба)
RAID	Redundant array of independent/inexpensive disks – отказоустойчивый массив независимых дисков

RAW	Формат цифровых файлов изображения, содержащий необработанные данные об электрических сигналах с фотоматрицы цифрового фотоаппарата, цифровой кинокамеры, а также сканеров неподвижных изображений или киноплёнки
RTP	Real-time Transport Protocol – протокол прикладного уровня, используется при передаче трафика в реальном времени
RTSP	Real time streaming protocol - прикладной протокол, предназначенный для использования в системах, работающих с мультимедийными данными (мультимедийным содержимым, медиасодержимым), и позволяющий удалённо управлять потоком данных с сервера, предоставляя возможность выполнения команд, таких как запуск (старт), приостановку (пауза) и остановку (стоп) вещания (проигрывания) мультимедийного содержимого, а также доступа по времени к файлам, расположенным на сервере
RTCP	Real-Time Transport Control Protocol - протокол управления передачей в реальном времени
SM	Одномодовое оптическое волокно
SSL/TLS	Secure Sockets Layer/Transport Layer Security - защищенный протокол, обеспечивающим аутентификацию и защиту от нарушения конфиденциальности и искажения данных (нарушения целостности)
TCP/IP	Transmission Control Protocol/Internet Protocol – протокол управления передачей/межсетевой протокол. Набор сетевых протоколов для передачи данных
TIFF	Tagged Image File Format - формат хранения растровых графических изображений. TIFF стал популярным форматом для хранения изображений с большой глубиной цвета

UDP	User Datagram Protocol - протокол пользовательских датаграмм, один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета
WDR	Wide Dynamic Range – широкий динамический диапазон, технология, позволяющая получать высокое качество изображений при любом перепаде уровней освещённости

4 Назначение и цели создания подсистемы

4.1 Назначение подсистемы

Подсистема «Видеонаблюдение» является инструментальной подсистемой ИТС Государственной компании.

Подсистема предназначена для сбора, контроля, обработки, анализа, хранения и передачи актуальной видеоинформации, необходимой для обеспечения функционирования других подсистем (сервисов) ИТС, содержания автомобильных дорог и предоставления потребителям необходимых видеоданных.

Получение актуальной видеоинформации должно обеспечиваться с целью оценки:

- транспортной обстановки на маршруте для визуального определения дорожной ситуации с целью своевременного вызова спецтехники, аварийно-спасательных служб, а также для контроля уборки автодороги;
- функционирования СВП в зоне непосредственных подъездов (выездов) к ПВП;
- метеорологической обстановки на маршруте;
- заторов, ДТП, наличия свободных парковочных мест и т.д.;
- состояния элементов дорожной инфраструктуры.

4.2 Функции подсистемы

Основными функциями подсистемы являются:

– формирование фото и видеоинформации о складывающейся дорожно-транспортной ситуации;

– видеозапись и архивирование информации;

– ручное управление (поворот, масштабирование изображения) поворотными видеокамерами;

– автоматическое управление поворотными видеокамерами: возможность организации предварительно заданной схемы настроек положения видеокамер (предустановок) и ручной и/или автоматический переход камер на данную схему при определенных условиях;

– возможность автоматического обхода предустановок (патрулирование) поворотными видеокамерами;

– разграничение полномочий пользователей подсистемы;

– возможность установки настроек записи видеопотоков от камер по событиям подсистемы, в т.ч. от камер видеонаблюдения и/или модулей видеоанализа;

– обработка (сжатие) и передача информации в ЦУ и центральный аппаратно-программный комплекс системы;

– вывод изображения с видеокамер на автоматизированные рабочие места системы и коллективные средства отображения информации (видеостены, мониторы, и т.д.);

– возможность предоставления покадрового и потокового видеоизображения;

– программирование последовательностей просмотра изображений с видеокамер;

– обеспечение управления из ЦУ режимами омывания и очистки стекол термокожухов видеокамер;

– выдача сигналов тревоги при пропадании видеосигнала из-за

технической неисправности или вандализма;

– возможность предоставления видеоизображения с видеокамер наблюдения по запросам пользователей;

– обеспечение санкционированной передачи видеоинформации другим подсистемам ИТС, службам экстренного реагирования, дорожным службам, правоохранительным органам, в интернет-сайты и другие СМИ;

– реакция на события видеоанализа (вывод на АРМ видеоизображения по тревогам/событиям/срабатыванию датчиков и видеоаналитики);

– возможности экспорта видеоданных в стандартные форматы;

– взаимодействие со смежными и внешними информационными системами.

4.3 Цели создания подсистемы

Основными целями создания подсистемы являются:

– повышение уровня безопасности и качества управления обстановкой на автомобильных дорогах в повседневной жизни и во время чрезвычайных ситуаций;

– обеспечение информированности пользователей ИТС, прежде всего операторов ЦУ, эксплуатирующих служб и водителей об условиях движения.

Поставленные цели достигаются за счет своевременного получения видеоинформации об оперативной обстановке на дорогах, обеспечения возможности восстановления хода событий на основе анализа архивов информации, сокращения времени реагирования на происшествия и чрезвычайные ситуации.

4.4 Общие показатели эффективности подсистемы

Общая эффективность подсистемы характеризуется следующими показателями:

– качество предоставляемой информации (соответствие стандартам HDTV и соответствующее решаемой задаче разрешение видеокамеры);

– полнота охвата видеонаблюдением контролируемого участка автомобильной дороги;

– степень интеграции подсистемы видеонаблюдения и ресурсов служб управления движением; служб обеспечения безопасности и экстренного вызова; эксплуатационных служб; органов надзора и контроля за транспортной деятельностью;

– полнота и качество аналитической обработки поступающей видеоинформации;

– индексирование видеоинформации и формирование метаданных для последующей обработки различными аналитическими модулями;

– своевременность доведения необходимой видеоинформации.

5 Характеристика объекта автоматизации

5.1 Сведения об объекте автоматизации

5.1.1. Объектом автоматизации является видеонаблюдение за движением транспортных потоков на автомобильных дорогах Государственной компании.

5.1.2. Видеонаблюдение на участках дорог выполняется в рамках локальной ИТС, развернутой на этих участках.

5.1.3. Мониторинг работоспособности видеонаблюдения на всех автомобильных дорогах Государственной компании выполняется в Центре ситуационного управления.

5.2 Сведения о составе объекта автоматизации

В состав комплекса технических средств подсистемы входят:

– Локальные ЦУ ИТС, Центр ситуационного управления, включая сервер (серверы) управления подсистемой;

– сервер (серверы) записи, серверы приложений, серверы БД, СХД, АРМ (АРМы) оператора;

– периферийные технические средства, устанавливаемые на

автомобильных дорогах – поворотные и стационарные видеокамеры, а также мобильные (передвижные) видеокамеры;

– беспилотные летательные аппараты (БПЛА), при необходимости.

5.3 Требования к эксплуатации объекта автоматизации

5.3.1. Комплекс технических средств подсистемы должен функционировать круглосуточно.

5.3.2. Серверы подсистемы видеонаблюдения должны эксплуатироваться в сухих отапливаемых помещениях с обеспечением необходимого микроклимата и соответствовать исполнению по ГОСТ 15150.

5.3.3. Периферийные технические средства подсистемы должны функционировать в уличных условиях (вне помещений) под воздействием климатических и погодных факторов, а также различных агрессивных факторов окружающей среды.

5.3.4. Периферийное оборудование должно быть защищено от вандализма и несанкционированного доступа в соответствии ГОСТ Р 51558-2014. При этом защита не должна создавать проблемы для доступа обслуживающего персонала при проведении технического обслуживания и ремонта.

5.3.5. Эксплуатация БПЛА осуществляется по мере необходимости для осуществления мониторинга дорожно-транспортной обстановки в режиме реального времени. Технические средства должны обеспечивать бесперебойную работу БПЛА в любое время суток с возможностью корректировки и настройки каналов управления и видеонаблюдения.

6 Требования к подсистеме

6.1 Требования к подсистеме в целом

6.1.1 Требования к структуре и функционированию подсистемы

Подсистема должна отвечать технологическим и техническим требованиям, нормам и правилам, действующим на территории Российской

Федерации, обеспечивать безопасность для жизни и здоровья людей при эксплуатации объекта.

Подсистема должна иметь открытую архитектуру, которая допускает дальнейшее наращивание функциональных возможностей и интеграцию с оборудованием различных производителей (иметь открытые протоколы информационного обмена между периферийными техническими средствами и другими подсистемами ИТС).

Подсистема должна обладать следующими качествами:

– переносимость (возможность эксплуатации на различных аппаратных и программных платформах);

– интероперабельность (способность к взаимодействию с имеющими другую архитектуру системами);

– масштабируемость (возможность наращивания без модернизации программного обеспечения);

– возможность обновляться и расширяться через телекоммуникационную сеть.

Комплекс технических средств подсистемы должен обеспечивать выполнение всех основных функций, указанных в п.4.2 «Функции подсистемы».

6.1.2 Требования к периферийным техническим средствам

6.1.2.1 Требования, предъявляемые к видеокамерам на автомобильных дорогах.

Все видеокамеры подсистемы ИТС «Видеонаблюдение» должны соответствовать следующим требованиям:

– оборудование должно быть официальной продуктовой линейкой производителя, предназначенной для использования в режиме 24/7/365;

– оборудование должно использовать открытые и опубликованные протоколы;

– оборудование должно обеспечивать видео с частотой кадров не менее 25 кадр/с, соотношение сторон кадра должно соответствовать условию, при котором ширина кадра составляет не менее 1.6 высоты кадра;

– оборудование должно поддерживать как минимум один открытый международный стандартизированный протокол взаимодействия оборудования и программных средств, входящих в состав систем безопасности, и соответствовать следующим аспектам взаимодействия видеокамеры с системами управления или видеозаписи посредством данного протокола: конфигурирование сетевого интерфейса, обнаружение устройств в сети, управление профилями работы оборудования, настройка потоковой передачи медиа-данных, управление приводом PTZ в случае его наличия, обработка событий от встроенной в оборудование и загружаемой на его платформу аналитики, защита (управление доступом, шифрование), локальное хранение, поиск и извлечение данных. Поддержка данного протокола используемым оборудованием должна подтверждаться публикацией на открытых ресурсах организации, отвечающей за разработку этого стандарта для систем безопасности;

– оборудование должно сжимать изображение, в соответствии со стандартами H.264, MJPEG или иными, устанавливающими не менее жесткие требования;

– оборудование должно обладать функционалом интеллектуального сжатия видеопотока. Все методы сжатия видеопотока должны быть интегрированы в видеокамеру;

– оборудование должно поддерживать настраиваемую функцию счетчика пикселей, определяющую размер объекта интереса в пикселях;

– оборудование должно поддерживать фильтрацию IP-адресов (не менее 100 уникальных адресов) и обеспечивать, по меньшей мере, три разных уровня защиты паролем;

– оборудование должно иметь возможность добавления второго (резервного) пользователя с правами администратора с уникальным именем и паролем;

– оборудование должно поддерживать установку пароля длиной до 64 символов с использованием строчных и прописных букв, цифрами и специальными знаками;

– оборудование должно поддерживать, как минимум, дайджест-аутентификацию доступа и/или другие, более защищенные протоколы аутентификации;

– дополнительные программные компоненты, загружаемые с видеоустройства для конкретных задач, должны иметь цифровую подпись организации, предоставляющей услуги сервиса сертификации;

– оборудование должно обеспечивать выдачу не менее 4 независимо сконфигурированных видеопотоков;

– оборудование должно обеспечивать регистрацию событий в файле журнала, содержащем информацию как минимум о 250 последних соединениях и попытках доступа с момента последнего перезапуска устройства.

– оборудование должно контролироваться функцией Watchdog (сторожевой таймер), которая автоматически перезапускает процессы или перезапускает устройство, в случае обнаружения неисправности;

– оборудование должно полностью поддерживаться открытым и опубликованным API, который должен содержать всю необходимую информацию для интеграции функционала камеры в сторонние приложения;

– оборудование должно поддерживать загрузку программных приложений на платформу видеокамеры, в том числе стороннего производства;

– оборудование должно поддерживать возможность работы со следующими протоколами: HTTP, HTTPS, SSL/TLS, RTSP, RTP, UDP, RTCP, а также отраслевым стандартом ONVIF, при этом настройка и обслуживание

оборудования должны осуществляться с использованием стека протоколов TCP/IP;

– необходимо, чтобы в устройстве была возможность отключения неиспользуемых протоколов и точной настройки используемых протоколов для обеспечения защиты информации;

– оборудование не должно быть зависимым от облачных сервисов сторонних производителей;

– все компоненты оборудования, предоставленные производителем, должны иметь гарантию в течение как минимум трех (3) лет.

Требования для поворотных видеокамер (минимальные технические характеристики):

– поворотные видеокамеры должны быть полнофункциональными, то есть обеспечивать: дистанционное вращение в вертикальной и горизонтальной плоскостях, масштабирование (приближение и удаление участков и объектов видеонаблюдения) и фокусирование;

– разрешающая способность видеокамеры должна быть не менее 2Мп;

– обязательно наличие зум-объектива с кратностью масштабирования не менее 30х с автоматической фокусировкой;

– скорость поворота и фокусировки видеокамеры должна соответствовать диапазону: мин. 0,05°/с - макс. 120°/с (по горизонтали) и мин. 0,05°/с - макс. 60°/с (по вертикали);

– точность позиционирования не более 0,05°;

– обязательно наличие электронной системы стабилизации изображения;

– оборудование должно обладать чувствительностью, достаточной для наблюдения движущихся объектов (автомобили, пешеходы) в условиях слабого

ночного уличного освещения. Как минимум соответствие значениям минимальной освещенности - в цветном режиме 0,2 лк (при 30 IRE F1.6), в черно-белом 0,01лк (при 30 IRE F1.6);

– оборудование должно обладать широким динамическим диапазоном для работы в условиях сложного освещения (встречная засветка, пересвеченные или затемненные области кадра и т.п.) со значением WDR не менее 120dB;

– наличие функционала автоматического переключения между режимами День/Ночь с использованием физического инфракрасного фильтра;

– отображение текущего азимута и угла наклона на экране;

– возможность подключения устройства омывания и очистки смотрового стекла камеры в случае необходимости (емкость бака с омывающей жидкостью – не менее 5 литров) с последующим управлением данным функционалом из интерфейса камеры и программного обеспечения верхнего уровня;

– всепогодное исполнение в термокожухе с соответствием классу IP66, диапазон рабочих температур -50…+55°С при относительной влажности до 100% (с выпадением конденсата);

– режим безопасного запуска камеры (холодный старт) при температурах от -40°С;

– сохранение работоспособности функционала PTZ при ветровых нагрузках до 30 м/с, без защитного козырька до 40 м/с.

Требования для стационарных фиксированных видеокамер (минимальные технические характеристики):

– разрешающая способность видеокамеры не менее 2Мп;

– возможность установки варифокального объектива;

– поддержка функционала регулировки заднего фокуса (тонкая подстройка фокуса за счёт движения матрицы относительно объектива);

– чувствительность, достаточная для наблюдения движущихся объектов (автомобили, пешеходы) в условиях слабого ночного уличного освещения. Как минимум, соответствие значениям минимальной освещенности - в цветном режиме 0,11лк (при 50 IRE F1.3), в черно-белом 0,01лк (при 50 IRE F1.3);

– широкий динамический диапазон для работы в условиях сложного освещения (встречная засветка, пересвеченные или затемненные области кадра и т.п.) со значением WDR не менее 120 dB;

– возможность автоматического переключения между режимами день/ночь с использованием физического инфракрасного фильтра;

– возможность подключения устройства омывания и очистки смотрового стекла камеры в случае необходимости (емкость бака с омывающей жидкостью – не менее 5 литров) с последующим управлением данным функционалом из интерфейса камеры и программного обеспечения верхнего уровня;

– всепогодное исполнение в термокожухе с соответствием классу IP66, диапазон рабочих температур - 40…+50°С;

– режим безопасного запуска камеры (холодный старт) при температурах от -40°С;

– сохранение работоспособности функционала PTZ при ветровых нагрузках до 30 м/с, без защитного козырька до 40 м/с.

Типы (модели) видеокамер определяются проектом на основании:

– необходимости решения конкретной задачи в определенном проектом месте дислокации оборудования;

– удобства и простоты настройки и установки;

– показателей надежности;

– унификации с уже установленными на автомобильных дорогах Государственной компании типами видеокамер.

6.1.2.2 Требования, предъявляемые к видеокамерам на БПЛА (минимальные технические характеристики):

– наличие гиростабилизированного подвеса;

– разрешающая способность матрицы видеокамеры не менее 12Мп;

– разрешение видео – не ниже FullHD (1920 x 1080);

– видео с частотой кадров не менее 25 кадр/с;

– максимальное разрешение фото: 4000x3000;

– поддержка форматов JPEG, RAW для фото сьемки и MP4, MOV для видеосъемки.

6.1.2.3 Требования к функции видеозаписи в составе подсистемы

– непрерывная запись видеоинформации, поступающей от всех видеокамер на автомобильной дороге (участке дороги), ее архивирование для последующего анализа выявления причин осложнения дорожно-транспортной обстановки;

– запись всех входных видеосигналов в оперативный архив должна производиться в постоянном непрерывном режиме;

– запись на карту памяти MicroSD объемом не менее 64 Гб, находящейся во встроенном слоте камеры, в случае потери связи сервера записи с камерой, с последующим встраиванием данного отрезка в основной архив записи при восстановлении связи;

– доступ в видеоархив должен осуществляться с выделенных АРМ, доступ в видеоархив сторонних пользователей должен быть исключен;

– видеосигналы должны преобразовываться, записываться, храниться и передаваться в систему видеозаписи в цифровом формате со следующими параметрами:

- разрешающая способность - не ниже FullHD (1920 x 1080);
- требуемая полоса пропускания канала связи не более 12 Мбит/с на канал видео.

– дополнительно может быть обеспечена поддержка записи видеосигналов в оперативный архив в старт-стопном режиме по командам со стороны ПО ЦУ;

– носители информации для хранения видеозаписей должны предусматривать «горячую замену» (замену вышедшего из строя носителя без остановки работы базового блока в целом и автоматическую подготовку вновь установленных носителей для работы в составе базового блока);

– реализация поддержки записи видеосигналов в оперативный архив. Длительность хранения информации, если в поле обзора видеокамеры попал дорожный инцидент или ДТП, должна составлять не менее 1 года, в остальных случаях 10 суток. Аппаратно-программные средства должны обеспечивать автоматическое удаление информации при превышении длительности их хранения;

– служебная информация для каждого видеофрагмента должна включать, как минимум:

- номер видеокамеры (канала);
- дату и время записи.

– видеозапись должна обеспечивать поиск массивов видеоинформации по отдельным критериям и их комбинациям, как минимум:

- по номеру камеры (канала);
- по дате и времени.

– модуль видеозаписи должен обеспечить реализацию запросов на поиск и выдачу в сеть видеоинформации не менее чем от 2 клиентов одновременно, без снижения качества записи по всем видеоканалам;

– для выбранного канала должны поддерживаться следующие

минимальные режимы воспроизведения: вперед и назад с заданной скоростью (нормальное, ускоренное или замедленное), стоп-кадр;

– обеспечивать, как минимум, возможность вывода изображения стоп-кадра в графический файл стандартного формата (JPG, GIF, TIFF и др.) с последующей его печатью на принтере;

– необходимо реализовать поддержку сохранения видеофрагментов в файлы стандартного формата хранения видеозаписей;

– дальнейшее развитие функции видеозаписи должно проводиться с учетом существующих систем видеозаписи Государственной компании «Российские автомобильные дороги», путем их частичной модернизации.

6.1.3 Общие рекомендации по определению мест дислокации периферийного оборудования подсистемы.

Определение мест установки средств видеонаблюдения желательно проводить с использованием программ имитационного моделирования.

Оценка определения мест установки должна осуществляться путем сравнения внешних интегральных индикаторов эффективности на этапе создания базовой модели и на этапе внедрения и функционирования моделей систем.

Видеокамеры размещаются вдоль автомобильной дороги сбоку от проезжей части на отдельных опорах, а также на опорах стационарного электрического освещения и искусственных дорожных сооружениях.

Частота установки видеокамер определяется решаемой этими видеокамерами задачами и требованием к разрешающей способности оборудования на данном участке. Данные требования могут формироваться исходя из характеристик аналитических модулей в случае их наличия.

Видеокамеры устанавливают на участках дорог:

– аварийно-опасных;

– характеризующихся высоким трафиком и повторяющимися

заторовыми ситуациями (длина очереди превышает 1 км);

– на поворотах, развязках и местах слияния и разделения транспортных потоков с уменьшением полос движения;

– на которых периодически возникают неблагоприятные погодные условия, такие как сильные поперечные ветры, снежные заносы и гололед;

– в пределах и на подходах к мостам, путепроводам и тоннелям;

– на площадках отдыха;

– в районе светофорных объектов;

– перед въездами на пункты взимания платы и на выездах с них.

На остальных участках дорог видеокамеры следует располагать на основе технико-экономического обоснования в соответствии с данными Таблицы 1.

Таблица 1 - Установка видеокамер на основном направлении движения автомобильных дорог

Категория автомобильной дороги	**Общее количество полос**	**Наличие искусственного освещения**	**Частота установки видеокамер**
IA	4 и более	Присутствует	Обеспечение возможности 100% видеопокрытием проезжей части
		Отсутствует	
IБ и IВ	4 и более	Присутствует	Обеспечение возможности 100% видеопокрытием проезжей части
		Отсутствует	3-5 км.
II	4	Присутствует	Обеспечение возможности 100% видеопокрытием проезжей части
		Отсутствует	3-5 км.
	2- 3	Присутствует	3-5 км.
		Отсутствует	5-10 км.

Категория автомобильной дороги	Общее количество полос	Наличие искусственного освещения	Частота установки видеокамер
III (альтернативные дороги)	2 - 3	Присутствует	5-10 км.
		Отсутствует	

Новые видеокамеры должны устанавливаться с учетом существующей подсистемы видеонаблюдения Государственной компании, путем ее частичной модернизации.

Мобильные видеокамеры следует использовать при отсутствии постоянно действующей системы видеонаблюдения на данном участке автомобильной дороги или сбоя в их работе для периодического кратковременного сбора видеоданных.

Мобильные видеокамеры стационарно устанавливаются на трейлерах, на специальных тележках, на служебном транспорте или специальных машинах.

6.1.4 Общие требования к монтажу оборудования

– должен быть надежно закреплен каждый элемент подсистемы;

– в случае использования магистральных сетей Ethernet на открытом воздухе подключать их через соответствующие устройства грозозащиты;

– монтаж оборудования выполнять в соответствии с рекомендациями изготовителя;

– соблюдать требования, предъявляемые к соединительным кабелям и их прокладке;

– заземляющие проводники всех использованных устройств надежно соединять в одной точке заземления или на шине заземления в соответствии с требованиями нормативных документов.

6.1.5 Особенности выбора и установки видеокамер. Требования.

6.1.5.1. Требования к местам установки и ориентации видеокамеры

– при установке видеокамеры следует обеспечить максимальное соответствие зоны обзора видеокамеры, определенной ее техническими характеристиками, местными условиями и особенностями объекта. Это означает отсутствие в поле зрения камеры видеонаблюдения посторонних предметов, ограничивающих обзор;

– наружная установка камеры должна учитывать наличие таких строительных конструкций как козырьки, пилястры и пр.;

– обзор объекта видеонаблюдения не должен перекрываться (даже частично) оптически непрозрачными препятствиями, как-то: ветки деревьев и кустарников, листвой, различными трубами, столбами и пр. объектами, мешающими обзору и фокусировке видеокамеры;

– установка подсистемы видеонаблюдения должна осуществляться с учетом характеристик, назначения объекта, где планируется монтаж системы (см. Приложение А);

– расположение видеокамеры и выбор фокусного расстояния (угла обзора) определяется исходя из того, что изображение объекта должно занимать не менее 50 процентов общего объёма изображения;

Рассчитать размер сцены видеокамеры и максимально допустимое расстояние от видеокамеры до объекта с учетом фокусного расстояния объектива и размера матрицы рекомендуется с учетом данных Таблицы 2 (для матрицы 1/3) или специальными программными утилитами, предоставляемыми производителем оборудования.

Таблица 2 – Расчёт размера сцены для видеокамеры с учетом фокусного расстояния объектива и размера матрицы (гор. х верт.)

Дистанция / f (мм)	2,5	2,8	2,9	3,6	3,7	4,3	6,0	8,0	12,0	16,0
3 м	6x4,5	5,1x3,8	5x3,75	4x3	3,95x2,96	3,8x2,85	2,4x1,8	1,8x1,35	1,2x0,9	0,9x0,67
5 м	10x7,5	8,25x6,2	8,4x6,8	6,6x4,5	6,5x4,9	6x4,5	4x3	3x2,25	2x1,5	1,5x1,12
10 м	20x15	13x9,7	17x12,8	13x10	13x9,8	12x9	8x6	6x4,5	4x3	3x2,2
20 м	40x30	34x25,5	34x25	26x20	28x19	22x16,5	16x12	12x9	8x6	6x4,5
30 м	60x45	51x38	50x37	40x30	39x29	36x16,5	24x18	18x13,5	12x9	9x6,7
40 м	80x60	69x52	65x49	53x40	52x39	48x36	34x2,5	24x18	16x12	12x9
50 м					65x49	95x71	40x30	30x22	20x15	15x11,2
80 м							64x48	48x36	32x24	24x18
100 м								60x44	40x30	30x22
150 м									60x45	45x34

– в случае наличия на автодороге более одного объекта наблюдения размещение видеокамеры должно обеспечивать общий (панорамный) обзор определенной зоны автодороги. При необходимости, на площадке может быть установлено несколько видеокамер, исходя из потребностей видеомониторинга;

– места размещения видеокамер должны обеспечиваться согласно категории надежности электроснабжения объектов инфраструктуры;

– необходимо, чтобы настройка видеокамеры на объекте не нарушала права граждан на неприкосновенность частной жизни, не делая достоянием общественности подробности их быта в соответствии с Гражданским кодексом РФ [4]. Видеокамеры должны иметь функцию маскирования фрагментов кадра;

– при определении места установки следует учитывать конструктивные особенности, технические характеристики камер видеонаблюдения;

– необходимо проанализировать условия освещенности контролируемой зоны: наличие, количество, параметры источников освещения и их расположение относительно зоны наблюдения. При этом надо учесть, как первичные источники (естественные и искусственные), так и вторичные;

– при возможности использовать дополнительные источники освещения, преимущественно ИК и обязательно с учетом возможных изменений освещенности в процессе эксплуатации в течение суток и в разное время года.

6.1.5.2. Требования к углам обзора

– угол обзора каждой видеокамеры должен определяться на этапе проектирования системы видеонаблюдения. В системах видеонаблюдения используются объективы с фиксированным и переменным фокусным расстоянием - вариофокальные объективы (вариообъективы);

– в уличных видеокамерах использовать вариофокальные объективы. В этом случае в технических характеристиках видеокамеры указывается не фиксированный угол обзора, а диапазон возможных углов поля зрения. При необходимости, угол обзора может быть скорректирован;

– применять видеокамеры с возможностью удаленного управления настройками, чтобы при необходимости настраивать фокус и угол обзора, удаленно из ЦУ;

– разработчик подсистемы обязан предоставить схему дислокации с секторами обзора видеокамер.

6.1.6 Архитектура подсистемы

В соответствии с ГОСТ Р ИСО 14813-1 и ГОСТ Р 56294 структурно подсистема входит в состав нескольких сервисных доменов:

1) «Информирование участников дорожного движения», который в свою очередь состоит из сервисных групп:

– дотранспортное (предварительное) информирование:

- о транспортной ситуации на автомобильной дороге;
- о состоянии функционирования дорожных объектов;
- о наличии свободных парковочных мест в районе места назначения.

– информирование в процессе движения:

- о местах дислокации придорожных объектов;

- о загруженности автомобильной дороги по предполагаемому маршруту движения;
- о наличии свободных мест на парковках в месте назначения.

2) «Управление дорожным движением», который в свою очередь состоит из сервисных групп:

– организация и управление дорожным движением:

- мониторинг дорожного движения;
- координация между управлением уличным движением и управлением движением на скоростных автомагистралях.

– управление инцидентами, связанными с транспортом:

- мониторинг и подтверждение происшествия;
- организация помощи участникам происшествия на месте;
- координация действий на месте и освобождение транспортных путей;

3) «Персональная безопасность, связанная с дорожным движением», на основе сервисной группы:

– меры безопасности пешеходов.

4) «Погодные условия (дорожная метеообстановка)», на основе сервисной группы:

– прогнозирование погоды на дорогах.

5) «Катастрофы и Чрезвычайные ситуации (управление и координация), на основе следующих сервисных групп:

– управление информацией о катастрофах и ЧС:

- сбор и передача данных;
- совместное использование данных.

– управление при катастрофах и ЧС:

- планирование действий в дорожной сети при ЧС.

6) «Управление данными ИТС», на основе следующих сервисных групп:

– ПО для ИТС:

- приобретение (разработка) ПО для нужд ИТС;
- ответственное хранение и доработка ПО под текущие и перспективные нужды.

– справочники данных:

- разработка, регистрация, ответственное хранение различных сценариев работы ИТС;

– данные центров управления:

- регистрация, хранение и обмен дорожной информацией, которая может быть востребована другими центрами управления, ведомствами, организациями, службами, а также различными федеральными, областными, городскими и частными автоматизированными управляющими или информационными системами;
- хранение и обмен данными для использования в рамках одного центра или между различными ЦУ движением, дорожными операторами, государственными службами и ведомствами, оперативными службами для обеспечения контроля соблюдения законодательства Российской Федерации в дорожной сфере.

Структура подсистемы в части реализации функций управления, контроля, сбора и обработки видеоданных должна являться централизованной и иметь три уровня иерархии (три компонента):

– Центр ситуационного управления Государственной компании - верхний уровень;

– Локальные проекты ИТС - средний уровень;

– Периферийные комплексы технических средств на автомобильных дорогах - нижний уровень.

6.1.7 Требования к способам и средствам связи для информационного обмена между компонентами подсистемы.

6.1.7.1 В связи с требованиями по пропускной способности каналов передачи данных, в целях повышения устойчивости к электромагнитным помехам и усиления защиты от несанкционированного доступа в качестве основной среды передачи данных между центральным оборудованием функциональных подсистем в ЦУ, а также периферийным оборудованием рекомендуется использовать ВОЛС.

6.1.7.2 Выбор способа передачи видеоданных в сервер управления подсистемой должен осуществляться с учетом обеспечения его стабильности, а также необходимой пропускной способности в соответствии с указанными требованиями по передаче видеоданных.

6.1.7.3 Для организации резервных (аварийных) каналов связи, а также при технической невозможности или экономической нецелесообразности применения ВОЛС предусмотреть организацию беспроводных способов передачи данных.

6.1.7.4 Протокол цифровой обработки видеоданных – H.264 и/или MJPEG. Передача видеоинформации должна осуществляться с разрешением не хуже 1920x1080.

6.1.7.5 Протоколы обмена данными между элементами подсистемы – стек TCP/IP.

6.1.7.6 Каналы связи между блоками периферийного оборудования, центрального оборудования - Ethernet 10/100/1000 (витая пара) - при расстоянии между блоками до 100 метров, и волоконно-оптический кабель - при расстоянии между блоками свыше 100 метров (MM – для прокладки внутри помещений и зданий, SM – для магистральных линий).

6.1.7.7 Номенклатура используемого оборудования определяется максимально с учетом унификации принятых решений по другим, ранее

выпущенным проектам в части систем связи и передачи данных на автомобильных дорогах, находящихся в доверительном управлении Государственной компании и обеспечения интеграции. Проектные решения по оборудованию должны соответствовать требованиям нормативных документов.

6.1.7.8 Допускается реализация двух типов видеонаблюдения:

– непрерывное, обеспечивающее передачу цветного видеоизображения с частотой не менее 25 кадров в секунду, реализуемого управляемыми видеокамерами;

– дискретное, обеспечивающее передачу цветного либо черно-белого изображения с частотой 1 кадра в 5-15 секунд, реализуемого стационарными или управляемыми видеокамерами с использованием беспроводной связи.

6.1.7.9 Сжатие (компрессирование) видеоизображения должно осуществляться непосредственно видеокамерой.

6.1.7.10 Оборудование видеонаблюдения должно поддерживать возможность сжатия изображения кодеком H.264 и/или MJPEG с поддержкой динамически изменяющегося коэффициента компрессии в областях изображения без движения в кадре и динамическое изменение частоты опорных кадров в случае отсутствия движения в кадре.

6.1.7.11 Функциональные элементы подсистемы должны обмениваться информацией через совместно используемую базу данных.

6.1.7.12 Информационное и программное обеспечение подсистемы следует реализовать в рамках модели «клиент / сервер»:

– на клиентах (рабочих местах диспетчеров и другого персонала системы) должны размещаться средства организации интерфейса пользователя и некоторая часть ПО, реализующего технологические алгоритмы анализа и представления информации;

– основная часть ПО, реализующего технологические алгоритмы (в

том числе все алгоритмы управления), должна размещаться на серверах приложений;

– база данных системы должна располагаться на серверах базы данных.

6.1.8 Требования по диагностированию подсистемы

6.1.8.1 Режим автодиагностики Подсистемы должен функционировать параллельно с основным (штатным) режимом работы (необходимо предусматривать диагностику работоспособности компонентов подсистемы, хранение структурных и заданных режимов работы и параметров пакетом программ, установленных на сервере управления видеопотоками).

6.1.8.2 Диагностирование подсистемы должно осуществляться на уровнях функциональных подсистем, программных и технических комплексов, средств передачи данных и отдельных технических средств.

6.1.8.3 Диагностика компонентов подсистемы должна производиться автоматически программными средствами на основе обработки и анализа информации, поступающей в ЦУ.

6.1.8.4 Должно быть обеспечено визуальное отображение информации о неисправности периферийного оборудования на АРМ технолога Центра управления.

6.1.8.5 Информация о неисправностях должна быть дифференцированной с указанием возможных причин неисправности с учетом возможностей встроенного самотестирования, осуществляемого на уровне периферийного устройства.

6.1.8.6. Результаты диагностики должны быть документированы.

6.1.9 Требования к численности и квалификации персонала подсистемы

Требования к численности и квалификации персонала подсистемы устанавливаются в организационно-распорядительных документах

Государственной компании с учетом круглосуточного поддержания подсистемы в рабочем состоянии, анализа поступающей информации, совершенствования алгоритмов управления на основе полученной статистической и динамической видеоинформации.

6.1.10 Показатели назначения

6.1.10.1 Параметры, характеризующие степень соответствия подсистемы ее назначению

Степень соответствия системы ее назначению должна оцениваться одним или несколькими параметрами из следующего перечня:

– динамика снижения числа ДТП как результат улучшения качества содержания дорог;

– динамика снижения числа ДТП как результат более эффективного информационного обеспечения пользователей дорог;

– динамика повышения скорости оказания технической и медицинской помощи пострадавшим при авариях;

– динамика снижения заторовых ситуаций;

– улучшение планирования работ контрагентами.

6.1.10.2 Вероятностно-временные характеристики сохранения целевого назначения подсистемы

Эффективность функционирования подсистемы не должна понижаться в случаях:

– неоптимального управления из-за неполной или недостоверной информации на некоторой части периферийных комплексов технических средств;

– отказов в выполнении основной функции подсистемы и в том числе отказов оборудования на некоторой части автомобильной дороги.

путем сбора и обработки статистических данных о надежности элементов подсистемы.

6.1.11.3.2 Контроль достигнутых значений надежности должен производиться периодически в процессе функционирования подсистемы.

6.1.12 Требования к электробезопасности

6.1.12.1 Технические средства должны обеспечивать защиту обслуживающего персонала от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.007.0 по классу I, что означает наличие рабочей изоляции и элемента для заземления. В случае, если изделие имеет провод для присоединения к источнику питания, этот провод должен иметь заземляющую жилу и вилку с заземляющим контактом.

6.1.12.2 Все внешние элементы технических средств, находящихся под напряжением, согласно ГОСТ 12.1.019, должны иметь защиту от случайного прикосновения, а сами технические средства должны иметь защитное заземление в соответствии с ГОСТ 12.1.030. Шкафы, пульты и корпуса должны иметь зажимы или сетевые вилки с контактом для подключения защитного заземления.

6.1.12.3 Периферийное оборудование должно иметь изоляцию между цепями питания и корпусом в соответствии с ПУЭ [8].

6.1.12.4 Монтаж, наладка, эксплуатация, обслуживание и ремонт технических средств подсистемы должны производиться согласно инструкциям по эксплуатации на эти устройства, где есть соответствующие разделы по обеспечению безопасности. Все виды работ по монтажу и демонтажу должны выполняться при отключенном напряжении питания.

6.1.13 Требования к эргономике и технической эстетике

6.1.13.1 Компоновка технических средств на рабочих местах диспетчерского персонала должна отвечать условиям удобства обслуживания и

работы с ними и соответствовать общим эргономическим требованиям по ГОСТ 23000.

6.1.13.2 Поверхности пультов управления должны обладать покрытием, исключающим появление бликов в поле зрения оператора.

6.1.13.3 Взаимное расположение рабочих мест диспетчерского персонала должно отвечать требованиям ГОСТ 21958.

6.1.13.4 Внешнее оформление технических средств должно отвечать требованиям технической эстетики по ГОСТ 30.001.

6.1.14 Требования к условиям и режимам эксплуатации технических средств

6.1.14.1 Периферийные технические средства являются стационарными и мобильными (передвижными) и должны функционировать круглосуточно в течение всего срока службы.

6.1.14.2 Технические средства сервера центра (-ов) управления являются стационарными, должны размещаться в закрытом отапливаемом помещении с кондиционированием и функционировать круглосуточно в течение всего срока службы.

6.1.15 Требования к параметрам сетей энергоснабжения

6.1.15.1 Блоки питания оборудования должны быть рассчитаны на питание от сети переменного тока напряжением 220 В, частотой 50 Гц и должны сохранять работоспособность при отклонении напряжения питающей сети от плюс 15% до минус 15% от номинального значения, частоты ±1 Гц.

6.1.15.2 В тех местах, где отсутствует возможность обеспечения подключения к стационарным сетям электроснабжения, возможно обеспечение энергоснабжения за счет применения альтернативных источников питания (солнечные батареи, ветрогенераторы и др.).

6.1.15.3 Электроснабжение периферийного оборудования подсистемы обеспечить по III категории надежности.

Для электроснабжения оборудования на опорах и мачтах предусмотреть установку щита распределительного из полимерного материала антивандального исполнения степенью защиты IP не менее 66.

В электрической схеме щита предусмотреть:

– возможность подключения переносного электрогенератора для производства работ в случае отсутствия напряжения внешней сети,

– установку устройства защиты от импульсных перенапряжений.

Секцию гарантированного питания вывести:

– на опорах (в распределительном щите);

– на мачтах (в шкафу ДКШ).

В качестве естественного молниеприемника предусматривать опоры и мачты АСУДД.

6.1.15.4 Заземление выполнить в соответствии с ГОСТ Р 50571.5.54-2011.

6.1.15.5 Нормы качества электрической энергии по ГОСТ 13109.

6.1.15.6 Отключение электропитания не должно приводить к повреждению периферийного оборудования.

6.1.15.7 Энергоснабжение сервера управления подсистемы должно быть организовано по первой категории. Энергоснабжение периферийного оборудования должно быть организовано по третьей категории. Категория энергоснабжения должна соответствовать ПУЭ [9] и СН 512 [7].

6.1.16 Требования к металлоконструкциям для монтажа периферийного оборудования.

6.1.16.1 В качестве несущих конструкций предусмотреть максимально возможное применение уже существующих опор, стоящих на балансе Государственной компании.

6.1.16.2 Все несущие конструкции должны иметь оцинкованные поверхности (ГОСТ 23118, СП 28.13330.2017 [10]), за исключением отдельных случаев, оговоренных действующими нормативными документами.

6.1.16.3 Несущие конструкции, крепежные элементы и фундаменты должны рассчитываться с учетом ветровой нагрузки, безопасности в эксплуатации и безопасности для участников дорожного движения (СП 42.13330 [9]). В случае использования типовых конструкций, крепежных элементов и фундаментов предоставить ссылочные материалы на соответствующую документацию. При использовании нетиповых конструкций, крепежных элементов и фундаментов предоставить рабочие чертежи данных конструкций и расчет на нагрузки в составе строительной части проекта.

6.1.17 Требования к составу, размещению и хранению комплекта ЗИП

6.1.17.1 Номенклатура ЗИП, необходимых для эксплуатации и ремонта технических средств, определяется ЗИП соответствующих изделий, входящих в состав комплекса средств автоматизации.

6.1.17.2 В соответствии с ГОСТ 2.601 должна быть составлена ведомость ЗИП, в которой для каждого элемента указывается его обозначение, код и наименование, место укладки, применяемость, количество в изделии и в комплекте.

6.1.17.3 К каждому комплекту ЗИП должна прилагаться инструкция по его использованию, содержащая перечень входящих в ЗИП составных частей с ограниченными сроками хранения, указания о правилах хранения и консервации комплекта ЗИП, а также о нормах расхода материалов, необходимых для этих работ.

6.1.18 Требования к регламенту обслуживания

Регламент обслуживания технических средств подсистемы или допустимость работы без обслуживания должны соответствовать требованиям

эксплуатационной документации на соответствующие технические средства подсистемы.

6.1.19 Требования к защите информации от несанкционированного доступа

6.1.19.1 В подсистеме не предполагается обрабатывать информацию, содержащую сведения, отнесенные к государственной или служебной тайне. Циркулирующая в ней информация не имеет грифа «для служебного пользования» и должна быть отнесена к информации с ограниченным доступом.

6.1.19.2 Подсистема должна удовлетворять, как минимум, требованиям руководящего документа ФСТЭК [11]. В случае необходимости должны учитываться специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) ФСТЭК от 02.03.2001 г. и ГОСТ Р 51583.

6.1.19.3 Система защиты сервера управления и информации подсистемы должна предусматривать, в качестве основных мер:

– разграничение доступа к сетевым устройствам, серверам управления и программным средствам, как со стороны персонала, так и со стороны пользователей внешних систем;

– исключение доступа к информации, к сетевым устройствам, к серверам управления и базам данных сторонних лиц;

– физическую сохранность сетевых устройств, серверов и носителей информации.

6.1.19.4 Для защиты от НСД к конфигурационным средствам сетевых устройств, серверам, базам данных и программному обеспечению должны обеспечиваться идентификация, проверка подлинности и контроль доступа. Для каждого пользователя должен быть предусмотрен индивидуальный пароль, обеспечивающий доступ к подсистеме с соответствующими полномочиями и

приоритетами разных уровней. При этом нужно обеспечить такое положение, при котором отдельные классы операторов имеют права только на запрос информации, но не имеют прав на активное управление.

Сведения об операторе и пароле следует хранить в закодированном виде. Не допускается возможность доступа к управлению объектами без соответствующего допуска, а также фальсификации данных, переданных уполномоченным оператором.

6.1.19.5 Защита от НСД должна предусматривать защиту на канальном и сетевом уровне, а также на уровне приложений.

6.1.19.6 Защита информации на канальном уровне может быть обеспечена организацией системы связи с помощью выделенных ВОЛС.

6.1.19.7 Для защиты от НСД при передаче данных между периферийным оборудованием и сервером управления подсистемы следует использовать непосредственно ВОЛС Государственной компании, но при невозможности подключения или экономической нецелесообразности допускается использование ведомственных сетей. Для передачи информации сторонним абонентам могут использоваться выделенные волоконно-оптические каналы связи, либо виртуальные выделенные каналы общегородских или ведомственных мультисервисных сетей.

6.1.19.8 На сервере управления подсистемой должны использоваться операционные системы, включающие средства разграничения доступа к файлам.

6.1.19.9 Для хранения всех конфигураций, журналов действий, оповещений о событиях, поступающих из подсистемы, должна использоваться система управления базами данных, основанная на модели клиент/сервер и поддерживающая средства регистрации (аудита) и разграничение доступа к объектам базы данных на основе прав, привилегий, ролей, хранимых процедур и т.п.

6.1.19.10 В подсистеме должны осуществляться регистрация и учет:

– носителей информации;

– входа/выхода субъектов доступа в/из подсистемы;

– попыток несанкционированного доступа, включая попытки подбора кода доступа;

– выдачи печатных документов.

6.1.19.11 Защита от компьютерных вирусов должна быть организована в соответствии с ГОСТ Р 51188.

6.1.19.12 В технических средствах, устанавливаемых на периферийных объектах, должны быть предусмотрены меры по защите от несанкционированного, неквалифицированного вмешательства посторонних лиц.

6.1.19.13 Оборудование сервера управления подсистемой должно размещаться в помещении с физической охраной, предусматривающей контроль доступа в помещения посторонних лиц. Серверное и коммуникационное оборудование должны размещаться в промышленных стойках, оснащенных замками.

6.1.19.14 При обнаружении попыток НСД подсистема должна выдать соответствующие сообщения в ЦУ.

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

6.1.20.1 Для обеспечения сохранности информации при авариях, вызванных отключением электропитания на длительный период, в состав программно-технического комплекса должны быть включены технические средства и программное обеспечение резервного копирования и восстановления информации. Копии должны храниться на энергонезависимых носителях и периодически обновляться по мере поступления новых данных.

6.1.20.2 При перерыве подачи электроэнергии длительностью до 15 минут должно быть обеспечено корректное закрытие приложений на сервере при разряде батарей ИБП до соответствующего порогового значения.

6.1.20.3 При специфицировании сервера подсистемы необходимо предусмотреть установку дополнительного блока питания для автоматического переключения при пропадании напряжения в основном блоке питания (или выходе его из строя).

6.1.21 Требования к защите от влияния внешних воздействий

6.1.21.1 Требования к радиоэлектронной защите средств системы

Устойчивость оборудования к электромагнитным помехам и электромагнитная совместимость должна быть обеспечена согласно критериям качества функционирования "А" ГОСТ Р 50839.

6.1.21.2 Требования по стойкости, устойчивости и прочности к внешним воздействиям

Периферийное оборудование должно иметь корпуса со степенью защиты от проникновения твердых тел и от проникновения воды внутрь изделия не хуже IP66 по ГОСТ 14254.

6.1.22 Требования по стандартизации и унификации

6.1.22.1 При разработке проекта подсистемы должны быть использованы типовые проектные решения по алгоритмическому, математическому и техническому обеспечению.

6.1.22.2 В основу унифицированных проектных и технических решений должен быть положен принцип модульности.

6.1.23 Требования к техническому обеспечению

6.1.23.1 Требования к техническому обеспечению серверного оборудования управления подсистемой.

6.1.23.1.1 Основное оборудование управления подсистемой должно включать в себя:

– серверы;

– системы хранения данных;

– системы бесперебойного гарантированного энергоснабжения.

Все технические решения должны соответствовать современным нормам и требованиям, касающимся надежности, экологичности, безопасности и технологичной развитости всех компонентов подсистемы.

6.1.23.1.2 Технические требования к серверам

Для обеспечения высокой доступности и восстановления после аппаратных сбоев с минимальными простоями для серверов системы (серверы управления/ серверы базы данных/серверы приложений) должно быть использовано решение на базе кластера, состоящего как минимум из двух узлов.

Сервер должен работать под управлением операционной системы, разработанной с учетом ее использования в кластерах и обладающей следующими основными свойствами:

– поддержка сетевых взаимодействий, в т. ч. стека протоколов TCP/IP;

– поддержка многопоточности;

– поддержки автоматического переконфигурирования RAID-массивов в режиме «on-line»;

– обеспечение безопасности (защиты от случаев отказа в выполнении того или иного сервиса, а также от попыток вторгнуться в систему извне);

– возможность выполнения на данной программно-аппаратной платформе целого ряда распространенных программных продуктов для серверов.

6.1.23.1.3 Технические требования к системам хранения данных

СХД, входящая в состав комплекса оборудования управления подсистемой, в целом должна обеспечивать круглосуточный бесперебойный доступ к данным со стороны группировок серверов комплекса и рабочих групп пользователей. СХД должна предоставлять возможность иерархического хранения данных с выделением ресурсов хранения с определенным для данного класса информации и класса приложения типом носителя и обеспечивать функции защиты и менеджмента данных.

6.1.23.1.4 Технические требования к коллективным средствам отображения

Система коллективного средства отображения информации должна обеспечивать аудио - и видео сопровождение различных форм коллективной работы сотрудников ЦУ с помощью современных технологий представления информации и видеоконференцсвязи.

Система коллективного средства отображения должна обеспечивать максимальную информативность и гибкость отображения визуальной информации. В состав системы коллективного отображения информации входят:

– видеостена (жидкокристаллические и плазменные панели, проекционные экраны, мультимедийные проекторы и экраны);

– процессор видеостены.

Основным элементом отображения информации коллективного средства отображения является видеостена.

Размещение видеостены требуется определить, исходя из обеспечения оптимального обзора со всех рабочих мест ЦУ, а также с учётом требований к эстетике помещения. Визуализация видеоинформации должна обеспечивать комфортную коллективную работу и формирование изображения на видеостене и видеомониторах в виде подвижных масштабируемых окон, которые можно в реальном времени передвигать, изменять размер и располагать в любом порядке.

Видеопроцессор должен быть построен на базе промышленного высокопроизводительного компьютера под управлением операционной системы

с открытым исходным кодом и формировать изображение с разрешением, равным суммарному разрешению видеостены. Программное обеспечение, установленное на видеопроцессоре, должно позволять использовать все разрешение видеостены при выводе графической информации.

В качестве источников графической и видеоинформации могут выступать:

– любое из АРМ персонала ИТС;

– эфирное и спутниковое телевидение;

– DVD/CD проигрыватель.

6.2 Требования к видам обеспечения

6.2.1 Требования к математическому обеспечению

6.2.1.1 Требования к составу, области применения и способам использования математических методов и моделей

6.2.1.1.1. Состав и области применения

Группа математических методов и моделей должна обеспечивать статистическую обработку показателей функционирования подсистемы и показателей функционирования элементов комплекса технических средств.

6.2.2 Требования к информационному обеспечению

6.2.2.1 Требования к составу, структуре и способам организации данных.

6.2.2.1.1 Информационное обеспечение подсистемы должно включать в себя:

– базовую информацию, определяющую характер и режим работы объектов (настройки);

– оперативную информацию, дающую представление о реальных процессах видеонаблюдения и состоянии элементов подсистемы в тот или иной момент времени;

– данные, формируемые в виде сводок и отчетных документов.

6.2.2.1.2 Базовая информация должна отражать основные характеристики подсистемы и корректироваться по мере их изменения.

6.2.2.1.3 Оперативная информация должна приниматься от объектов управления и диспетчеров, смежных систем и изменяться в произвольные моменты времени.

6.2.2.1.4 Контрагентам должна передаваться только та видеоинформация, которая необходима для обеспечения их технологического процесса..

6.2.2.2 Требования к информационной совместимости со смежными подсистемами

Подсистема видеонаблюдения должна быть совместима с системой верхнего уровня локальной ИТС. Для обеспечения совместимости требуется использовать согласованные протоколы и алгоритмы взаимного обмена данными.

6.2.2.3 Требования по использованию отраслевых классификаторов и унифицированных документов

Формы документов, используемые в процессе функционирования подсистемы до начала разработки рабочего проекта должны быть согласованы в Государственной Компании. Документы должны соответствовать требованиям унифицированной системы документации, определенной ГОСТами, учитывать структуру документов. Формы документов могут быть модифицированы, исходя из возможностей и параметров технических средств системы.

6.2.2.4 Требования по применению систем управления базами данных

6.2.2.5.1 При разработке подсистемы должна использоваться СУБД, отвечающая следующим основным требованиям:

– соответствие архитектуре «клиент/сервер»;

– открытость, то есть переносимость (наличие поддержки различных аппаратных платформ и операционных систем), интероперабельность

(способность к взаимодействию с системами другой архитектуры).

6.2.2.5.2 В составе СУБД должны иметься следующие средства и механизмы:

– многопоточность сервера БД, необходимая для увеличения числа одновременно обрабатываемых транзакций и более эффективного использования возможностей симметричных многопроцессорных систем;

– средства обеспечения надежности: журналы транзакций, а также средства создания резервных копий и восстановления поврежденных фрагментов БД в режиме on-line без остановки системы;

– средства обеспечения целостности (взаимной согласованности) данных с использованием процедурных (триггеры) и декларативных ограничений целостности;

– механизм блокировки для обеспечения согласованности чтения данных, находящихся в процессе постоянного обновления со стороны множества пользователей, и предотвращения конфликтов. При этом должна иметься возможность блокировки на уровне таблицы, страницы данных и отдельной записи;

– фрагментация и поддержка распределенных БД;

– средства тиражирования (репликации);

– средства обеспечения безопасности, в том числе механизмы привилегий на выполнение определенных операций с БД, разграничения доступа к отдельным объектам (таблицам, формам, отчетам, программам), идентификации пользователей с использованием паролей, аудита, а также поддержки ролей.

6.2.2.5 Требования к структуре технологического процесса, сбора, обработки, передачи и представления данных

6.2.2.6.1. В системе в качестве исходной должна использоваться:

- информация об объектах управления;
- информация об автомобильной дороге;
- нормативно - справочная информация;
- информация смежных подсистем.

6.2.2.6.2. Информация поступает в подсистему в виде различных документов. При поступлении должны осуществляться ее регистрация, ручная обработка и приведение к виду, удобному для ввода в БД.

В информации об объекте управления может быть выделена постоянная и оперативная информация. Постоянная информация должна вводиться однократно при начальном заполнении БД, а затем корректироваться в случае необходимости. Оперативная информация об объектах управления должна поступать в систему по каналам связи автоматически.

Информация о состоянии дорожного движения на автомобильной дороге, и постоянная информация об объекте управления должны вводиться в БД системы в ходе процедуры ведения БД.

6.2.2.6.3 В результате обработки регулярно поступающей оперативной информации об объектах управления должна формироваться выходная информация.

6.2.2.6 Требования к контролю, хранению, обновлению и восстановлению данных

6.2.2.7.1 БД подсистемы должна предусматривать создания резервных копий БД. Копии должны храниться на энергонезависимых носителях и периодически обновляться по мере поступления новых данных и/или через определенные промежутки времени. Целесообразно использование нескольких уровней резервных копий. Восстановление данных должно осуществляться путем выбора последней неиспорченной копии.

6.2.2.7.2 Контроль за созданием резервных копий должен быть возложен на администратора подсистемы.

6.2.2.8 Требования к процедуре придания юридической силы формируемым документам

В соответствии с ГОСТ 6.10.4 для придания юридической силы документам, формируемым подсистемой в ходе ее функционирования, должно оформляться сопроводительное письмо.

Для решения данной задачи допускается применение электронных ключей.

6.2.3 Требования к лингвистическому обеспечению

6.2.3.1 Требования к языковому взаимодействию пользователей с подсистемой и к способам организации диалога

6.2.3.3.1 Оперативное диспетчерское управление движением должно осуществляться в интерактивном режиме.

6.2.3.3.2 Интерфейс пользователя должен быть графическим, многооконным, с поддержкой манипуляторов, в том числе «мыши».

6.2.3.3.3 Сокращения и аббревиатуры должны соответствовать общепринятым, при этом должен преобладать полный текст без сокращений.

6.2.3.3.4 Действия диспетчеров в процессе диалога с системой должны протоколироваться в БД подсистемы для проведения последующего анализа.

6.2.4 Требования к программному обеспечению

Разрабатываемые программные средства должны быть в максимальной степени независимыми от используемых средств вычислительной техники и операционной среды.

6.2.4.1 Требования к качеству программных средств, способам его обеспечения и контроля качества

6.2.4.2.1 Для решения задачи автоматизации оперативного управления программный продукт должен соответствовать следующим общим требованиям:

– возможность гибкого реагирования на изменения бизнес-процессов Государственной компании с точки зрения настройки программного

обеспечения;

– возможность и простота настройки бизнес-процессов;

– наличие генераторов отчетов, экранных и выходных форм;

– возможность гибкой настройки пользовательского интерфейса;

– возможность поддержки распределенных БД;

– наличие русифицированного пользовательского интерфейса;

– наличие инструкций пользователя и программных подсказок на русском языке;

– наличие процедур контроля, сводящие возможные ошибки к минимуму;

– приемлемая стоимость владения программным обеспечением системы с учетом обновления клиентской и серверной части подсистемы.

6.2.4.2.2 Оператор ЦУ должен иметь возможность работы с подсистемой с любого компьютера ИТС, оснащенного набором необходимого ПО, подключенного к локальной или телекоммуникационной сети. Подсистема должна иметь возможность обеспечить зарегистрированным мобильным пользователям оперативный доступ к информации.

На рабочих местах пользователей должно устанавливаться только утвержденное Государственной компанией программное обеспечение.

6.2.4.2.3 ПО должно обеспечивать простой и последовательный контроль и сбор данных в отношении системы видеонаблюдения.

Используя интеграцию всех установленных систем, ПО должно предлагать полноценный эргономичный интерфейс для централизованного контроля дорожного движения и интеграции всех систем.

6.2.5 Требования к сертификации

Сертификация видеокамер должна быть организована и проведена в соответствии с требованиями Федеральных законов, постановлений Правительства РФ и Таможенного союза.

6.2.6 Требования к организационному обеспечению

Порядок взаимодействия диспетчерского персонала и персонала службы технической поддержки должен определяться специально разработанным регламентом.

Порядок взаимодействия персонала сервера управления подсистемой и сотрудников правоохранительных органов, прочих организаций и ведомств должен определяться специально разработанным регламентом.

6.2.7 Требования к защите от ошибочных действий персонала

6.2.7.1.1 Факты обращения персонала к подсистеме через клиентские рабочие места должны автоматически документироваться.

6.2.7.1.2 Ошибочные обращения к подсистеме должны отбраковываться, а на рабочую станцию, с которой поступило обращение, должно выдаваться сообщение об ошибке.

6.2.7.1.3 Для предотвращения и/или снижения числа ошибочных действий со стороны диспетчерского персонала диалог системы с человеком - оператором должен быть организован таким образом, чтобы возможность задания недопустимых параметров была сведена к минимуму. Для этого ввод параметров, которые могут принимать лишь одно из значений из заранее предопределенного набора, должен быть организован с использованием соответствующих элементов графического интерфейса.

Приложение А

(рекомендуемое)

Типовые схемы размещения элементов подсистемы видеонаблюдения

Схема 1

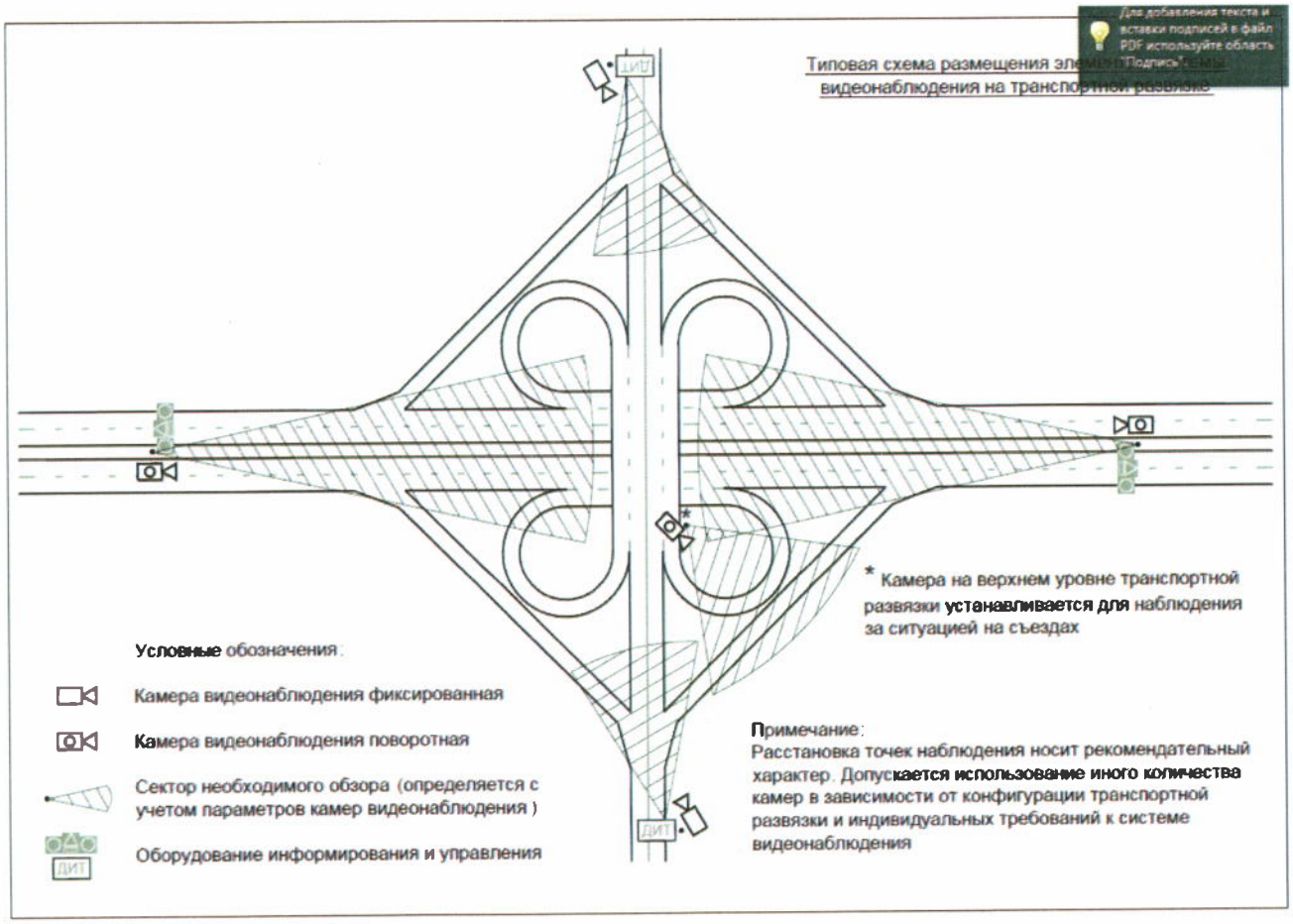
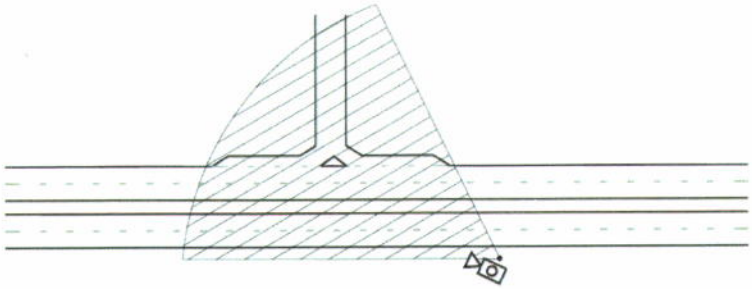


Схема 2

Типовая схема размещения элементов системы видеонаблюдения на примыкании второстепенной автомобильной дороги



Условные обозначения:

Камера видеонаблюдения поворотная

Сектор необходимого обзора (определяется с учетом параметров камер видеонаблюдения)

Примечание:
Расстановка точек наблюдения носит рекомендательный характер. Допускается использование иного количества камер в зависимости от индивидуальных требований к системе видеонаблюдения

Схема 3

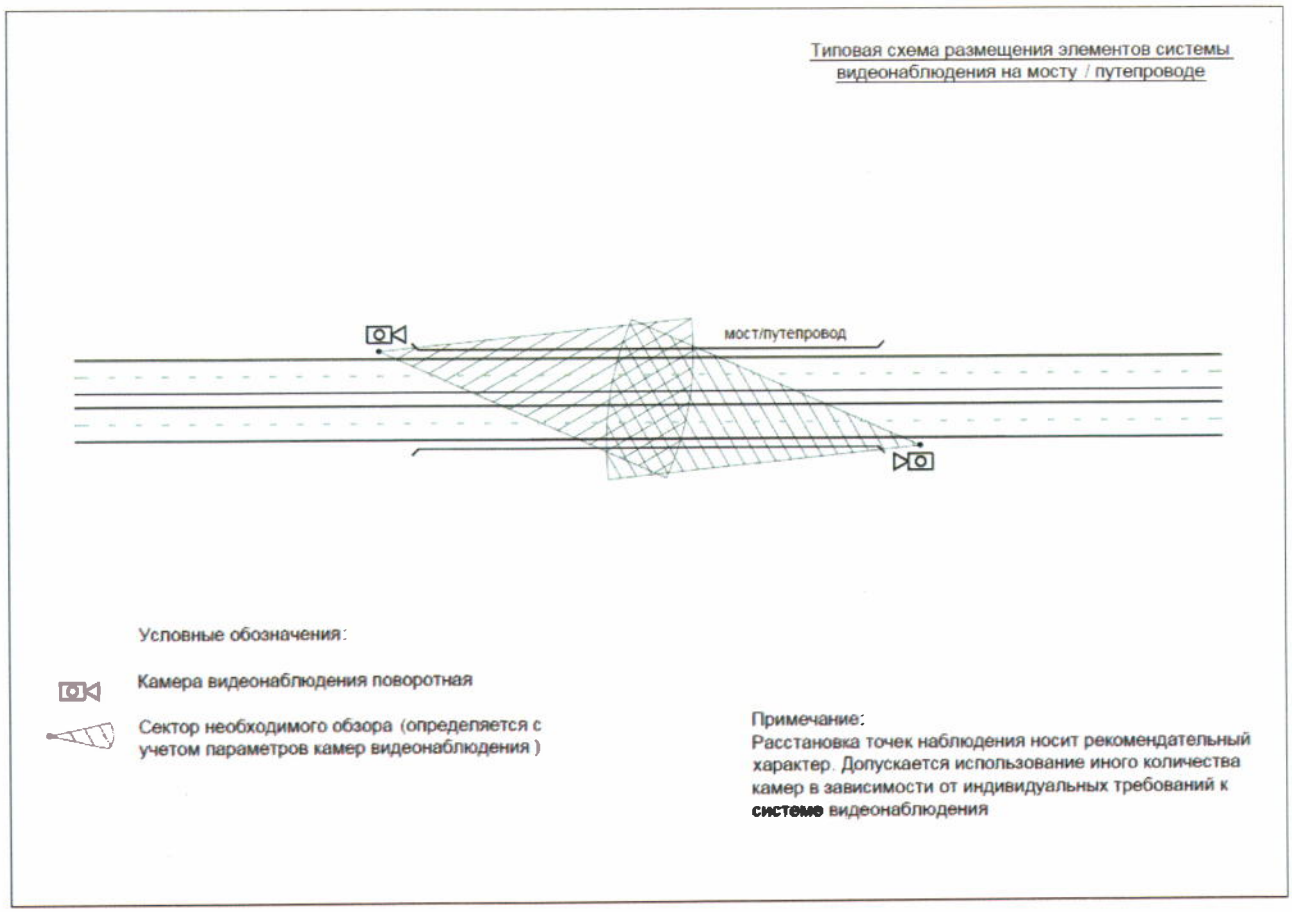
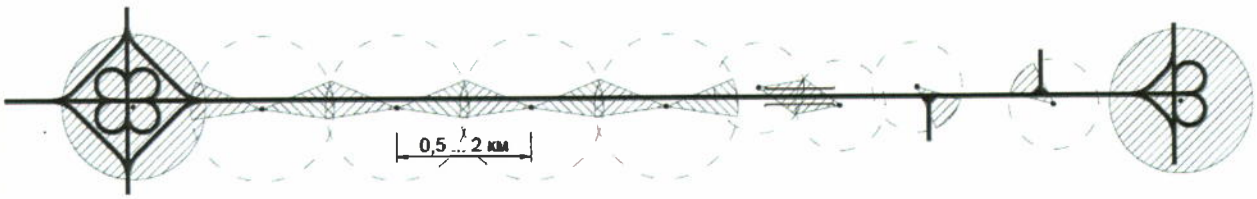

Типовая схема размещения элементов системы видеонаблюдения на мосту / путепроводе
мост/путепровод
Условные обозначения:
Камера видеонаблюдения поворотная
Сектор необходимого обзора (определяется с учетом параметров камер видеонаблюдения)
Примечание:
Расстановка точек наблюдения носит рекомендательный характер. Допускается использование иного количества камер в зависимости от индивидуальных требований к системе видеонаблюдения

Схема 4

Типовая схема размещения элементов системы видеонаблюдения на автомобильной дороге



Условные обозначения:

сектор необходимого обзора (определяется с учетом параметров камер видеонаблюдения)

Примечание:
Расстановка точек наблюдения носит рекомендательный характер. Допускается использование иных вариантов расстановки камер в зависимости от параметров автомобильной дороги, особенностей объекта, индивидуальных требований к системе видеонаблюдения

Библиография

[1] Федеральный закон от 10.12.1995 N 196-ФЗ	О безопасности дорожного движения
[2] Федеральный закон от 27.04.1993 N 4871-1	Об обеспечении единства измерений
[3] Федеральный закон от 27.12.2002 N 184-ФЗ	О техническом регулировании
[4] Гражданский кодекс РФ	Ст. 152.2. Определяет аспекты в неприкосновенности и охране частной жизни
[5] ГОСТ Р 51558-2014	Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний
[6] ГОСТ Р 56294-2014	Интеллектуальные транспортные системы. Требования к функциональной и физической архитектурам интеллектуальных транспортных систем
[7] СН 512-78	Инструкция по проектированию зданий и помещений для электронно-вычислительных машин
[8] ПУЭ	Правила устройства электроустановок. Издание 7
[9] СП 42.13330.2016	Градостроительство. Планировка и застройка городских и сельских поселений
[10] СП 28.13330.2017	Защита строительных конструкций от коррозии. Актуализированная редакция СНиП 2.03.11-85
[11] Руководящий документ ФСТЭК	Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» по классу защищенности не менее «1Г»

ПРИЛОЖЕНИЕ № 2
к приказу Государственной компании
«Российские автомобильные дороги»
от «28» декабря г. № 382

ПЛАН МЕРОПРИЯТИЙ
по внедрению стандарта организации СТО АВТОДОР 8.8-2017 «Требования к подсистеме ИТС «Видеонаблюдение» на автомобильных дорогах Государственной компании «Российский автомобильные дороги»

Подразделение-заказчик разработки Стандарта: Департамент информационных технологий и интеллектуальных транспортных систем (ДИТ)

Разработчик Стандарта: Общество с ограниченной ответственностью «АРМО-Системы» (ООО «АРМО-Системы»)

№ п/п	Наименование мероприятия	Ответственное подразделение	Участники работ	Сроки проведения
1	2	3	4	5
1	Информирование структурных подразделений об утверждении СТО АВТОДОР 8.8-2017 «Требования к подсистеме ИТС «Видеонаблюдение» на автомобильных дорогах Государственной компании «Российский автомобильные дороги» (далее – Стандарт)	ДИТ	Структурные подразделения	3 дня с даты утверждения
2	Публикация на сайте Государственной компании: - информации об утверждении Стандарта - текста утвержденного Стандарта	ДИТ	Пресс-служба	5 дней с даты утверждения
3	Включение Стандарта в Перечень нормативных документов, включаемых в проекты долгосрочных инвестиционных соглашений, концессионных соглашений, в договоры на выполнение работ по подготовке технико-экономического обоснования, проектированию, строительству, реконструкции, капитальному ремонту, ремонту автомобильных дорог и комплексному обустройству, по подготовке территорий строительства и на оказание услуг по строительному контролю на объектах Государственной компании «Российские автомобильные дорог» (далее – Перечень)	ДП	Структурные подразделения	При плановой актуализации Перечня

1	2	3	4	5
4	Включение Стандарта в состав конкурсной документации (документации об аукционе) на выполнение работ по договорам и соглашениям в отношении интеллектуальных транспортных систем.	Структурное подразделение, осуществляющее функции по формированию конкурсной документации; Структурное подразделение, осуществляющее функции ЦФО	Структурные подразделения, осуществляющие функции подразделений-соисполнителей по договорам (соглашениям)	С даты утверждения в сроки, установленные конкурсными процедурами
5	Сбор информации и мониторинг применения Стандарта контрагентами Государственной компании «Автодор»	Структурное подразделение, осуществляющее функции ЦФО	Структурные подразделения, осуществляющие функции подразделений-соисполнителей по договорам (соглашениям) ДИТ	С даты утверждения