УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 26 сентября 2016 г. № 969

ТРЕБОВАНИЯ
к функциональным свойствам технических средств обеспечения транспортной безопасности

I. Общие положения

1. Настоящие требования включают в себя требования к функциональным свойствам:

а) технических систем и средств сигнализации;

б) технических систем и средств контроля доступа;

в) технических систем и средств досмотра;

г) технических средств видеонаблюдения;

д) технических систем и средств интеллектуального видеонаблюдения;

е) технических систем и средств видеозаписи;

ж) технических систем и средств аудиозаписи;

з) технических средств связи, приема и передачи информации;

и) технических средств оповещения;

к) технических систем сбора и обработки информации.

2. Настоящие требования применяются с учетом основных функций технических средств обеспечения транспортной безопасности, для выполнения которых они предназначены в заданных условиях.

3. Используемые в настоящих требованиях понятия означают следующее:

"детекция" - обнаружение на произвольном изображении изображения лица человека;

"идентификация" (для систем видеонаблюдения) - процесс, при котором осуществляется поиск в регистрационной базе данных и предоставляется список кандидатов, содержащий от нуля до одного или более идентификаторов;

"система контроля доступа" - объединенные в комплексы электронные, механические, электротехнические, аппаратно-программные средства, обеспечивающие возможность доступа физических лиц в определенные зоны или к техническим средствам и ограничивающие доступ лиц, не имеющих права доступа;

"специфичность" - эксплуатационная характеристика алгоритма или аппаратно-программного средства, соответствующая доле истинно положительных срабатываний алгоритма или аппаратно-программного средства от общего числа срабатываний;

"сценарий "Движение в запрещенном направлении" - сценарий ситуации в регистрируемой сцене, по которому тревожным считается факт движения объекта (человека, транспортного средства, животного) в запрещенном направлении относительно условно заданных границ;

"сценарий "Нетипичные изменения в сцене" - сценарий ситуации в регистрируемой сцене, по которому тревожным считается снижение качества видеосигнала (затемнение, засветка, расфокусировка);

"сценарий "Оставленный (исчезнувший) предмет" - сценарий ситуации в регистрируемой сцене, по которому тревожным считается оставление предметов людьми в поле зрения камеры (либо ограниченной условными линиями зоне) либо исчезновение предмета, ранее находившегося в поле зрения камеры;

"сценарий "Стерильная зона" - сценарий ситуации в регистрируемой сцене, по которому тревожным считается факт появления объекта (человека, транспортного средства, животного) в поле зрения камеры, пересечения им условно заданной запрещенной линии либо нахождения в запрещенной зоне;

"чувствительность" - эксплуатационная характеристика алгоритма

или аппаратно-программного средства, соответствующая доле истинно положительных срабатываний алгоритма или аппаратно-программного средства от общего числа событий, которое требовалось обнаружить.

II. Требования к функциональным свойствам технических систем и средств сигнализации

4. Функциональные характеристики технических систем и средств сигнализации должны соответствовать требованиям ГОСТ Р 52435-2005 "Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний" и ГОСТ Р 54455-2011 (МЭК 62599-1:2010) "Системы охранной сигнализации. Методы испытаний на устойчивость к внешним воздействующим факторам".

5. Технические системы и средства сигнализации обеспечивают возможность создания необходимого количества рубежей охраны и сигнализации о попытках либо фактах незаконного проникновения на охраняемый объект (в зону ограниченного доступа) или совершения противоправных действий в отношении охраняемого имущества, а именно:

а) периметра территории охраняемого объекта;

б) территории (выделенной зоны) внутри периметра охраняемого объекта;

в) строительных конструкций зданий, строений и сооружений (стен, перекрытий);

г) оконных и дверных конструкций зданий, строений и сооружений;

д) внутреннего пространства зданий, строений и сооружений;

е) средств безопасности хранения имущества (сейфов, шкафов).

6. Технические системы и средства сигнализации должны обеспечивать возможность дистанционного контроля их работоспособности и выявления установки имитатора в линию связи.

7. Технические системы сбора, обработки, отображения, документирования и хранения информации, поступающей от технических систем и средств сигнализации, должны обеспечивать:

а) централизованную постановку и снятие с охраны канала сигнализации оператором по заявке уполномоченного пользователя;

б) для каждого канала сигнализации следующие режимы:

контроль состояния выходных цепей средств сигнализации, соединительной линии, датчиков вскрытия и дистанционного контроля работоспособности;

режим исключения канала сигнализации из конфигурации системы охранной сигнализации;

в) при информационной емкости более 16 источников (каналов сигнализации) - децентрализованную постановку и снятие с охраны канала сигнализации по командам уполномоченных пользователей с помощью удаленного пульта управления, оборудованного устройством ввода идентификационных признаков;

г) отображение на графических планах охраняемого объекта информации о состоянии технических средств, размещаемых на рубежах охраны, и возможность управления ими, а также оперативное отображение регистрируемых сообщений;

д) формирование сигналов тревоги в виде цветовой и звуковой индикации, а также отображение на графическом плане охраняемого объекта места, времени и причины возникновения ситуации;

е) регистрацию и хранение всех событий, связанных с изменением состояния технических средств сигнализации, на срок не менее 6 месяцев;

ж) коммутацию цепи электропитания средств сигнализации;

з) управление параметрами средств сигнализации;

и) автоматический переход в автономный режим при пропадании связи с управляющим компьютером с регистрацией извещений о тревоге (или неисправности) и автоматическую передачу извещений на управляющий компьютер при восстановлении связи;

к) взаимодействие с системой сбора результатов технического

мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

л) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

III. Требования к функциональным свойствам технических систем и средств контроля доступа

8. Системы и средства контроля доступа должны соответствовать требованиям ГОСТ Р 51241-2008 "Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний".

9. Системы и средства контроля доступа должны обеспечивать:

а) санкционированный проход (проезд) людей (транспортных средств") на (из) охраняемый объект путем их идентификации по комбинации следующих признаков:

вещественный код (ключи, карты, брелоки);

запоминаемый код (клавиатуры, кодонаборные панели и другие аналогичные устройства);

биометрический код (отпечатки пальцев, сетчатка глаз и другие);

б) предотвращение несанкционированного прохода (проезда) людей (транспортных средств) на (из) охраняемый объект;

в) выдачу информации на пульт централизованного наблюдения о попытках несанкционированного прохода (проезда) людей (транспортных средств) на (из) охраняемый объект;

г) взаимодействие с другими подсистемами интегрированной системы безопасности обеспечения противокриминальной защиты с целью обеспечения противокриминальной защиты охраняемого объекта;

д) взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

е) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

10. В состав систем и средств контроля доступа должны входить:

а) считывающие устройства (считыватели и идентификаторы);

б) средства управления в составе аппаратных и программных средств;

в) управляемые преграждающие устройства в составе преграждающих конструкций и исполнительных устройств.

11. Системы и средства контроля доступа должны выполнять следующие основные функции:

а) открывание управляемых преграждающих устройств после считывания идентификационного признака, доступ по которому разрешен в данную зону доступа (помещение или территорию) в заданный временной интервал, или по команде оператора системы и средства контроля доступа;

б) запрет открывания управляемых преграждающих устройств после считывания идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение или территорию) в заданный временной интервал;

в) санкционированное изменение (добавление, удаление) идентификационных признаков в средства управления в составе аппаратных и программных средств и обеспечение их связи с зонами доступа (помещениями или территориями) и временными интервалами доступа;

г) защита от несанкционированного доступа к программным средствам средств управления для изменения (добавления, удаления) идентификационных признаков;

д) защита технических и программных средств от

несанкционированного доступа к элементам управления, к установке режимов и к информации в виде системы паролей и идентификации пользователей;

е) сохранение настроек и базы данных идентификационных признаков при отключении электропитания;

ж) ручное, полуавтоматическое или автоматическое открывание управляемых преграждающих устройств для прохода при чрезвычайных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;

з) открытие или блокировка любых дверей, оборудованных системой и средствами контроля доступа, с рабочего места оператора системы;

и) автоматическое открытие определенных дверей по пожарной тревоге;

к) автоматическое закрытие управляемых преграждающих устройств при отсутствии факта прохода через определенное время после считывания разрешенного идентификационного признака (кода);

л) закрытие управляемых преграждающих устройств на определенное время и выдача сигнала тревоги при попытках подбора идентификационных признаков (кода);

м) отображение на пульте оператора, регистрация и протоколирование текущих и тревожных событий;

н) возможность просмотра и печати протокола работы системы контроля доступа (действия оператора, системные события, проходы клиентов, тревоги и аварийные ситуации);

о) автономная работа считывателя с управляемых преграждающих устройств в каждой точке доступа при отказе связи со средствами управления в составе аппаратных и программных средств;

п) возможность архивирования базы данных и просмотра архива в автономном режиме;

р) возможность распределения работников охраняемого объекта по структуре предприятия для удобства работы с базой клиентов системы;

с) возможность идентификации работников и посетителей охраняемого объекта по фотографиям из базы данных системы при проходе (проезде) через управляемые преграждающие устройства;

т) учет клиентов системы по типу пропусков:

постоянные пропуска (действуют все время работы клиента системы);

временные пропуска (действуют определенный срок и удаляются из системы автоматически по окончании этого срока);

гостевые пропуска (действуют одно посещение).

12. Считывающие устройства должны обеспечивать:

а) считывание идентификационного признака с идентификаторов;

б) сравнение введенного идентификационного признака с хранящимся в памяти или базе данных средств управления в составе аппаратных и программных средств;

в) формирование сигнала на открывание управляемых преграждающих устройств при идентификации пользователя;

г) обмен информацией со средствами управления в составе аппаратных и программных средств.

13. Считывающие устройства защищаются от манипулирования путем перебора или подбора идентификационных признаков.

14. Конструкция, внешний вид идентификатора и считывателя, надписи на них не должны приводить к раскрытию применяемых кодов.

15. Средства управления в составе аппаратных и программных средств должны обеспечивать:

а) прием информации от считывающих устройств, ее обработку, отображение в заданном виде и выработку сигналов управления управляемым преграждающим устройствам;

б) ведение баз данных работников охраняемого объекта с возможностью задания характеристик их доступа (кода, временного интервала доступа, уровня доступа и других);

в) ведение электронного журнала регистрации прохода работников

охраняемого объекта через точки доступа;

г) приоритетный вывод информации о тревожных ситуациях в точках доступа;

д) контроль исправности состояния управляемых преграждающих устройств, считывающих устройств и линий связи.

16. Конструктивно системы и средства контроля доступа строятся по модульному принципу и обеспечивают:

а) взаимозаменяемость сменных однотипных технических средств;

б) удобство технического обслуживания и эксплуатации, а также ремонтопригодность;

в) исключение возможности несанкционированного доступа к элементам управления систем и средств контроля доступа;

г) санкционированный доступ ко всем элементам, узлам и блокам, требующим регулирования, обслуживания или замены в процессе эксплуатации.

17. Устойчивость электромеханического запирающего устройства к криминальному открыванию и взлому должна соответствовать классу U1 по ГОСТ Р 52582-2006 "Замки для защитных конструкций. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому".

18. Запирающие устройства, используемые на объектах транспортной инфраструктуры 1 и 2 категорий, должны соответствовать:

а) 4 классу по ГОСТ 5089-2011 "Замки, защелки, механизмы цилиндровые. Технические условия" - для входов в критические зоны;

б) 2 классу по ГОСТ 5089-2011 "Замки, защелки, механизмы цилиндровые. Технические условия" - для входов в остальные зоны.

19. Запирающие устройства для объектов, используемые на объектах транспортной инфраструктуры 3 и 4 категорий, должны соответствовать:

а) 3 классу по ГОСТ 5089-2011 "Замки, защелки, механизмы цилиндровые. Технические условия" - для входов в критические зоны;

б) 2 классу по ГОСТ 5089-2011 "Замки, защелки, механизмы цилиндровые. Технические условия" - для входов в остальные зоны.

IV. Требования к функциональным свойствам технических систем и средств досмотра

20. Технические системы и средства досмотра должны обеспечивать:

а) не менее 49 случаев правильного обнаружения радиоактивных веществ, взрывчатых веществ, оружия, боеприпасов, патронов к оружию, взрывных устройств, элементов взрывных устройств из 50 испытаний;

б) не менее 49 случаев правильного идентифицирования радиоактивных веществ, взрывчатых веществ, оружия, боеприпасов, патронов к оружию, взрывных устройств, элементов взрывных устройств из 50 испытаний;

в) не более 3 случаев ложного обнаружения радиоактивных веществ, взрывчатых веществ, оружия, боеприпасов, патронов к оружию, взрывных устройств, элементов взрывных устройств из 50 испытаний;

г) не более 3 случаев ложной идентификации радиоактивных веществ, взрывчатых веществ, оружия, боеприпасов, патронов к оружию, взрывных устройств, элементов взрывных устройств из 50 испытаний;

д) взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

е) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

V. Требования к функциональным свойствам технических средств видеонаблюдения

21. Системы охранные телевизионные должны соответствовать требованиям ГОСТ Р 51558-2014 "Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний" и Рекомендациям "Р 78.36.008-99. Проектирование и монтаж систем охранного телевидения и домофонов", утвержденным Главным управлением вневедомственной охраны Министерства внутренних дел Российской Федерации 27 июня 1998 г.

22. Системы охранные телевизионные должны обеспечивать:

а) видеоверификацию тревог (подтверждение с помощью видеонаблюдения факта несанкционированного проникновения в зону охраны и выявление ложных срабатываний);

б) визуальный контроль объектов охраны и прилегающих к ним территорий (прямое видеонаблюдение);

в) оперативный контроль действий сотрудников службы безопасности (подразделения охраны) и предоставление необходимой информации для координации этих действий;

г) запись видеоинформации в архив для последующего анализа состояния охраняемого объекта, тревожных ситуаций, идентификации нарушителей;

д) программирование режимов работы;

е) взаимодействие с другими подсистемами интегрированной системы безопасности обеспечения противокриминальной защиты с целью обеспечения противокриминальной защиты охраняемого объекта;

ж) взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

з) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

23. Системы охранные телевизионные должны позволять проводить наблюдение за охраняемыми зонами объекта и в случае получения извещения о тревоге определить характер нарушения, место нарушения, количество нарушителей, направление движения нарушителя (нарушителей) и оптимальные меры противодействия.

24. Системы охранные телевизионные, предназначенные для работы в автоматизированном режиме (видеоверификация тревог), используются в дополнение к системе охранной сигнализации. Видеоизображение выводится на видеомонитор оператора видеонаблюдения в случае возникновения тревоги (по сигналу тревоги, получаемому от системы охранной сигнализации) с целью предоставления оператору видеонаблюдения дополнительной информации о состоянии охраняемой зоны, исключения ложных тревог и включения видеозаписи для последующего анализа ситуации или контроля действий сотрудников службы безопасности (подразделения охраны).

25. Системы охранные телевизионные, предназначенные для работы в неавтоматизированном режиме (прямое видеонаблюдение), применяются для реального видеонаблюдения за обстановкой на охраняемом объекте. В этих целях:

а) организуется отдельный пост видеонаблюдения с дежурным оператором видеонаблюдения;

б) видеокамеры работают в непрерывном режиме;

в) изображение от каждой видеокамеры выводится на отдельный видеомонитор оператора (допускается вывод на один видеомонитор не более 4 видеокамер для непрерывного наблюдения одним оператором).

26. Для целей настройки и контроля работоспособности системы охранной телевизионной допускается вывод видеоинформации на дополнительный видеомонитор (видеомонитор администратора системы охранной телевизионной) от большего количества видеокамер (более 8).

27. Системы охранные телевизионные должны обеспечивать

автоматическую запись видеоинформации в архив для последующего просмотра и анализа.

28. Видеозапись в зависимости от требований безопасности охраняемого объекта может производиться следующим образом:

а) непрерывно;

б) периодически по заданному расписанию;

в) по срабатыванию средств обнаружения проникновения;

г) по срабатыванию видеодетектора системы охранной телевизионной.

29. Технические средства архивации должны обеспечивать хранение необходимых объемов видеоинформации в течение времени, которое задается условиями и режимом охраны объекта.

30. В состав системы охранной телевизионной должны входить:

а) источники видеосигнала (видеокамеры с объективами, цифровые видеорегистраторы);

б) аппаратура передачи и коммутации видеосигнала;

в) устройства приема и обработки видеоданных для цифровых систем охранных телевизионных (платы видеоввода, видеосерверы, программное обеспечение автоматизированного рабочего места системы охранной телевизионной);

г) устройства вывода видеоизображения (видеомониторы);

д) устройства видеозаписи;

е) источники электропитания;

ж) коммутационное оборудование;

з) соединительные кабели;

и) кожуха для видеокамер;

к) средства инфракрасной подсветки;

л) другое оборудование, необходимое для обеспечения работоспособности системы охранной телевизионной.

31. К функциональным свойствам источников видеосигнала предъявляются следующие требования:

а) разрешение (число пикселей в каждом кадре) - не менее 1,2 мегапикселя;

б) горизонтальное разрешение кадра - не менее 1200 пикселей;

в) вертикальное разрешение кадра - не менее 1000 пикселей;

г) геометрические параметры пикселя должны соответствовать требованиям ГОСТ Р ИСО/МЭК 19794-5-2013 "Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица";

д) использование чересстрочной развертки не допускается;

е) оптическая разрешающая способность по горизонтали должна составлять не менее 800 линий на горизонтальный размер кадра;

ж) оптическая разрешающая способность по вертикали должна составлять не менее 650 линий на вертикальный размер кадра;

з) частота кадров - не менее 25 кадров в секунду;

и) цветность видеоизображения - цветное;

к) максимальное отношение "сигнал - шум" (с выключенной функцией автоматического усиления сигнала) - не менее 42 дБ;

л) относительная дисторсия согласно ГОСТ 20825-75 "Объективы съемочные. Методы измерения аберраций" - не более 1 процента;

м) коэффициент виньетирования согласно ГОСТ 24775-81 "Объективы. Методы измерения виньетирования" - не менее 0,9.

VI. Требования к функциональным свойствам технических систем и средств интеллектуального видеонаблюдения

32. К техническим системам и средствам интеллектуального видеонаблюдения относятся:

а) технические системы и средства идентификации физических лиц;

б) технические системы и средства обнаружения тревожных ситуаций.

33. К техническим системам и средствам идентификации физических лиц предъявляются следующие требования:

а) вероятность ложного пропуска для алгоритмов и аппаратно-программных средств детекции - не более 5 процентов;

б) вероятность ложноотрицательной идентификации для алгоритмов и аппаратно-программных средств - не более 15 процентов;

в) вероятность ложноположительной идентификации для алгоритмов и аппаратно-программных средств - не более 1 процента;

г) пропускная способность аппаратно-программных средств идентификации - не более 3 секунд.

34. Функциональные свойства технических систем и средств идентификации физических лиц, указанные в пункте 33 настоящих требований, должны обеспечиваться при следующих условиях:

а) освещенность в плоскости лица - от (100 ± 10) до (1000 ± 50) люкс;

б) неравномерность освещенности лица - не более (50 ± 5) процентов;

в) характеристики видеоизображения:

разрешение видеоизображения, обеспечивающее регистрацию изображений лиц на рабочей дистанции съемки видеокамеры не менее 1,5 метра с расстоянием между центрами глаз (40 ± 2) пикселей (для алгоритмов и аппаратно-программных средств детекции) и (60 ± 2) пикселей (для алгоритмов и аппаратно-программных средств идентификации);

динамический диапазон интенсивности изображения в области лица - не менее 8 бит;

цветность видеоизображения - черно-белое;

частота - не менее 16 кадров в секунду;

г) плотность потока людей - 1 чел/м ;

д) скорость движения - не более 5 км/ч;

е) ракурс лица относительно фронтального ракурса, определяемый в соответствии с ГОСТ Р ИСО/МЭК 19794-5-2013 "Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица" угловыми координатами поворота, наклона и отклонения лица:

для алгоритмов и аппаратно-программных средств детекции - в диапазоне от 0 до (30 ± 2) градусов;

для алгоритмов и аппаратно-программных средств идентификации - в диапазоне от 0 до (15 ± 2) градусов;

ж) структура фона (подвижный случайно неоднородный фон съемки с перепадами контраста) - от (0,2 ± 0,05) до (0,8 ± 0,05);

з) объем базы данных эталонных изображений лиц - не менее 1000 лиц условно-фронтального типа (в соответствии с ГОСТ Р ИСО/МЭК 19794-5-2013 "Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица").

35. В состав технических систем и средств идентификации физических лиц включаются средства регистрации видеоизображений, к которым предъявляются следующие требования:

а) разрешение регистрируемого видеоизображения - не менее 1,2 мегапикселя;

б) частота кадров - не менее 16 кадров в секунду;

в) разрешающая способность - разрешение на рабочей дистанции съемки объектов размером 2 миллиметра и более (значения для области в центре кадра и на расстоянии до одной третьей ширины, высоты и диагоналей кадра от центра включительно);

г) глубина резко отображаемого пространства - не менее 1 метра (для области в центре кадра и на расстоянии до одной третьей ширины, высоты и диагоналей кадра от центра включительно);

д) расстояние между центрами глаз на изображении лица, зарегистрированном на рабочей дистанции съемки, - не менее (60 ± 2) пикселей (для области в центре кадра и на расстоянии до одной третьей ширины, высоты и диагоналей кадра от центра включительно);

е) максимальное отношение "сигнал - шум" (с выключенной функцией автоматического усиления сигнала) - не менее 45 дБ;

ж) дисторсия - не более 5 процентов (по краям кадра - на

расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).

36. Технические системы и средства идентификации физических лиц должны обеспечить:

а) взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

б) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

37. К техническим системам и средствам обнаружения тревожных ситуаций предъявляются следующие требования:

а) для алгоритмов и аппаратно-программных средств, работающих по сценарию "Стерильная зона":

чувствительность - не менее 99 процентов;

специфичность - не менее 99 процентов;

время реакции на появление объекта (человека, транспортного средства, животного) в запрещенной зоне настраивается в диапазоне от 1 до 300 секунд с шагом 1 секунда;

б) для алгоритмов и аппаратно-программных средств, работающих по сценарию "Оставленный (исчезнувший) предмет":

чувствительность - не менее 95 процентов;

специфичность - не менее 95 процентов;

время реакции на оставление (исчезновение) предмета настраивается в диапазоне от 1 до 300 секунд с шагом 1 секунда;

в) для алгоритмов и аппаратно-программных средств, работающих по сценарию "Движение в запрещенном направлении" (характеристики должны обеспечиваться при потолочном способе размещения видеокамеры):

чувствительность - не менее 95 процентов;

специфичность - не менее 99 процентов;

время реакции на факт движения объекта (человека, транспортного средства, животного) в запрещенном направлении настраивается в диапазоне от 1 до 300 секунд с шагом 1 секунда;

г) для алгоритмов и аппаратно-программных средств, работающих по сценарию "Нетипичные изменения в сцене":

чувствительность - не менее 90 процентов;

специфичность - не менее 95 процентов;

время реакции на нетипичные изменения в сцене (затемнение изображения, расфокусировка, засветка) настраивается в диапазоне от 1 до 300 секунд с шагом 1 секунда.

38. Функциональные свойства технических систем и средств обнаружения тревожных ситуаций, указанные в пункте 37 настоящих требований, должны обеспечиваться при следующих условиях:

а) освещенность в зоне регистрации - от (100 ± 10) до (1000 ± 50) люкс;

б) дистанция съемки - от 5 до 30 метров;

в) угол наклона оптической оси видеокамеры относительно горизонтальной плоскости:

не менее 15 градусов (для наклонного способа размещения);

(90 ± 10) градусов (для потолочного способа размещения);

г) разрешение видеокамеры - от 1,3 до 2 мегапикселей;

д) плотность потока людей - не более 1 чел/м ;

е) объем оставленного предмета - от 3 куб. дециметров;

ж) структура фона - подвижный случайно неоднородный фон съемки с перепадами контраста от (0,2 ± 0,05) до (0,8 ± 0,05).

39. В состав технических систем и средств обнаружения тревожных ситуаций включаются средства регистрации видеоизображений, к которым предъявляются следующие требования:

а) разрешение регистрируемого видеоизображения - не менее 1,2 мегапикселя;

б) частота кадров - не менее 25 кадров в секунду;

в) цветность регистрируемого видеоизображения - цветное;

г) максимальное отношение "сигнал - шум" (с выключенной функцией автоматического усиления сигнала) - не менее 42 дБ;

д) дисторсия - не более 10 процентов (по краям кадра - на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).

40. Технические системы и средства обнаружения тревожных ситуаций должны обеспечить:

а) взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

б) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

VII. Требования к функциональным свойствам технических систем и средств видеозаписи

41. К техническим системам и средствам видеозаписи предъявляются следующие требования:

а) цикличность видеозаписи - не менее 24 часов при использовании максимального для изделия количества видеокамер и следующих характеристик видеопотока:

разрешение (число пикселей в каждом кадре) - не менее 1,2 мегапикселя;

горизонтальное разрешение кадра - не менее 1200 пикселей;

вертикальное разрешение кадра - не менее 1000 пикселей;

геометрические параметры пикселя должны соответствовать ГОСТ Р ИСО/МЭК 19794-5-2013 "Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица";

б) использование чересстрочной развертки не допускается;

в) степень сжатия - не более 30 процентов по стандарту H 264 или MJPEG. Степень сжатия определяется по ГОСТ Р 54830-2011 "Системы охранные телевизионные. Компрессия оцифрованных видеоданных. Общие технические требования и методы оценки алгоритмов";

г) оптическая разрешающая способность по горизонтали - не менее 800 линий на горизонтальный размер кадра;

д) оптическая разрешающая способность по вертикали - не менее 650 линий на вертикальный размер кадра;

е) частота кадров - не менее 12 кадров в секунду.

42. Технические системы и средства видеозаписи должны обеспечить:

а) автоматическое обнаружение движения (сценарий "Детектор движения"):

с вероятностью не менее 99 процентов истинно положительной идентификации (по ГОСТ Р ИСО/МЭК 19795-1-2007 "Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура");

с вероятностью не более 0,1 процента ложноположительной идентификации (по ГОСТ Р ИСО/МЭК 19795-1-2007 "Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура");

б) взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

в) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

43. Настройка скорости видеозаписи при отсутствии движения в кадре в диапазоне от 3 до 30 кадров в секунду с шагом 1 секунда и при автоматическом обнаружении движения должна составлять не менее 12 кадров в секунду.

VIII. Требования к функциональным свойствам технических систем и средств аудиозаписи

44. К техническим системам и средствам аудиозаписи предъявляются следующие требования:

а) стандарт цифровой записи - PCM (импульсно-кодовая модуляция), 16 бит, моно/стерео;

б) сжатие данных - без сжатия;

в) частота дискретизации - 11025/16000 Гц;

г) неравномерность амплитудно-частотной характеристики - не более 2 дБ;

д) соотношение "сигнал - шум" на микрофонном входе - не менее 75 дБ;

е) коэффициент нелинейных искажений - не более 1 процента.

45. Технические системы и средства аудиозаписи должны обеспечить:

а) выполнение требований Научно-производственного объединения "Специальная техника и связь" Министерства внутренних дел Российской Федерации к качеству аудиоинформации и ее пригодности для проведения идентификационных исследований по голосу и речи;

б) взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

в) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

IX. Требования к функциональным свойствам технических средств связи, приема и передачи информации

46. Технические средства связи, приема и передачи информации должны обеспечить:

а) связь, прием и передачу информации в дуплексном режиме. Допускается использование полудуплексного режима для передачи документальной информации;

б) связь, прием и передачу информации в цифровом (дискретном) канале связи;

в) возможность работы от автономного или резервного (аварийного) источника электропитания;

г) возможность непрерывной круглосуточной работы;

д) возможность использования протоколов гарантированной доставки информации для передачи документальной информации.

47. К абонентским средствам радиосвязи, приема и передачи информации предъявляются следующие требования:

а) осуществление абонентскими радиостанциями соединения с базовыми и абонентскими станциями в дуплексном режиме по цифровым каналам связи в частотных диапазонах, установленных решением Государственной комиссии по радиочастотам;

б) передача информации в сети связи должна осуществляться в канальном или пакетном режимах;

в) наличие международного идентификационного номера для каждой абонентской радиостанции сети подвижной радиотелефонной связи;

г) наличие функции контроля (самоконтроля), позволяющей осуществлять проверку функционирования канала связи и работоспособности средства связи, приема и передачи информации.

48. Требования к параметрам радиоинтерфейса устанавливаются для каждого вида сети связи конкретного стандарта.

49. К проводным и оптическим системам передачи абонентского

доступа предъявляются следующие требования:

а) использование в оборудовании одного из следующих интерфейсов или их комбинации (двух и более):

двухпроводный аналоговый интерфейс к телефонной сети связи общего пользования (FXO);

двухпроводный аналоговый интерфейс к оконечному оборудованию телефонной сети связи общего пользования (FXS);

четырехпроводный интерфейс к каналам тональной частоты;

четырехпроводный цифровой интерфейс к телефонной сети связи общего пользования (S/T-интерфейс);

двухпроводный цифровой интерфейс к телефонной сети связи общего пользования (U-интерфейс);

интерфейсы для организации передачи сигналов по физическим линиям в тональном и надтональном диапазонах частот;

интерфейсы передачи данных (интерфейсы группы V);

интерфейсы цифровых абонентских линий (xDSL);

интерфейсы к сети передачи данных с использованием контроля несущей и обнаружением коллизий (Ethernet);

интерфейсы к оборудованию плезиохронной цифровой иерархии (PDH), включая оптические интерфейсы PDH;

интерфейсы к оборудованию синхронной цифровой иерархии (SDH);

интерфейсы к оборудованию оптических систем со спектральным разделением (WDM);

интерфейсы к оборудованию, использующему режим асинхронного переноса (ATM);

интерфейсы к оборудованию, использующему режим ретрансляции кадров (FR);

интерфейсы к сетям передачи данных, поддерживающим работу по протоколу IP;

интерфейсы к сетям передачи данных, поддерживающим мультипротокольное коммутирование по меткам (MPLS);

интерфейсы к оборудованию передачи сигналов видеосервиса;

интерфейсы внешней синхронизации;

интерфейс к пассивным волоконно-оптическим сетям G-PON;

б) обеспечение между оконечным оборудованием и транспортными системами организации каналов и (или) трактов (одного типа или нескольких):

двухпроводный телефонный канал тональной частоты;

четырехпроводный канал тональной частоты;

четырехпроводный канал ISDN 192 кбит/с;

канал базового доступа ISDN 160 кбит/с (BRI);

канал первичного доступа ISDN 2048 кбит/с (PRI);

цифровой тракт вычислительной сети с использованием контроля несущей и обнаружением коллизий;

комбинированный канал (тракт), оканчивающийся интерфейсами разных типов.

X. Требования к функциональным свойствам технических средств оповещения

50. Технические средства оповещения должны соответствовать требованиям ГОСТ Р 42.3.01-2014 "Гражданская оборона. Технические средства оповещения населения. Классификация. Общие технические требования".

51. Технические средства оповещения должны обеспечить:

а) доведение сигналов оповещения и экстренной информации до органов управления, должностных лиц, сил ликвидации чрезвычайных ситуаций и населения;

б) передачу сигналов оповещения и экстренной информации по стационарным и подвижным сетям связи общего пользования, а также технологическим сетям связи.

52. К техническим средствам оповещения предъявляются следующие требования:

а) средняя наработка на отказ - не менее 30000 часов;

б) среднее время восстановления состояния - не более 30 минут при наличии запасного имущества и принадлежностей;

в) средний срок сохраняемости - не менее 12 лет при хранении в условиях отапливаемых и неотапливаемых хранилищ с температурой от минус 40 градусов Цельсия до плюс 40 градусов Цельсия и относительной влажностью воздуха 80 процентов;

г) средний срок службы до списания - не менее 12 лет;

д) средний ресурс до первого капитального ремонта - не менее 10000 часов;

е) достоверность воспроизводимой речевой информации:

для слоговой разборчивости - не менее 90 процентов;

для словесной разборчивости - не менее 97 процентов;

ж) наличие функции контроля (самоконтроля), позволяющей осуществлять проверку функционирования работоспособности средства оповещения;

з) возможность круглосуточной работы.

53. Электропитание технических средств оповещения должно осуществляться от источников переменного тока напряжением 230/380 В (при допустимых отклонениях напряжения сети от минус 15 процентов до плюс 10 процентов) частотой 50 Гц ± 2 процента (если не указано иное требование).

54. К светодиодным экранам предъявляются следующие требования:

а) размер экрана - не менее 30 кв. метров;

б) ресурс жизни светодиодов - не менее 100000 часов;

в) яркость должна составлять:

при шаге между пикселями от 14 до 17 миллиметров - от 8000 до 10000 кд/м^2;

при шаге между пикселями от 18 до 20 миллиметров - от 7500 до 8500 кд/м^2;

при шаге между пикселями от 21 до 28 миллиметров - от 6500 до 7500 кд/м^2;

при шаге между пикселями от 29 до 34 миллиметров - от 6000 до 7500 кд/м^2;

г) частота обновления информации в модулях - от 250 до 10000 Гц;

д) удельный вес с системой электропитания - не более 45 кг/м^2;

е) полезный угол обзора (когда информацию еще можно разобрать) должен составлять:

по горизонтали - от 140 до 160 градусов;

по вертикали - от 60 до 80 градусов;

ж) коэффициент мощности - не менее 0,98;

з) диапазон переменного питающего фазного напряжения - от 90 до 265 В;

и) температура холодного пуска - не ниже минус 40 градусов Цельсия;

к) толщина видеоэкрана со встроенной системой питания - от 90 до 150 миллиметров;

л) степень защиты кластеров и блоков питания должна соответствовать IP 65;

м) необходимый уровень устойчивости функционирования к внешним воздействующим факторам при размещении на открытом пространстве должен обеспечиваться при:

температуре окружающей среды от минус 60 градусов Цельсия до плюс 70 градусов Цельсия;

относительной влажности воздуха от 30 до 95 процентов;

атмосферном давлении от 74,8 до 106,7 кПа.

55. К полноцветным панелям предъявляются следующие требования:

а) размер диагонали экрана - 42 дюйма (106,6 сантиметра);

б) видимая диагональ экрана - 106,6 сантиметра;

в) формат экрана - 16:9;

г) разрешение - не менее 852 x 480 пикселей;

д) максимальное разрешение входного сигнала - не менее 1024 x 768 пикселей;

е) яркость - не менее 1500 кд/м ;

ж) контрастность - 10000:1;

з) максимальный угол обзора по горизонтали - 170 градусов;

и) максимальный угол обзора по вертикали - 170 градусов;

к) поддержка систем цветности - PAL, SECAM, NTSC;

л) поддержка стандартов - VGA, SVGA, SXGA, XGA, HDMI;

м) необходимый уровень устойчивости функционирования к внешним воздействующим факторам при размещении на открытом пространстве должен обеспечиваться при:

температуре окружающей среды от минус 60 градусов Цельсия до плюс 70 градусов Цельсия;

относительной влажности воздуха от 30 до 95 процентов;

атмосферном давлении от 74,8 до 106,7 кПа.

56. К электронным табло типа "бегущая строка" предъявляются следующие требования:

а) максимальный размер отображаемого символа - 16 x 16 точек (6 x 8, 8 x 8, 4 шрифта для вертикальной установки табло плюс 2 шрифта, загружаемые пользователем);

б) максимальное количество отображаемых символов - 36;

в) цвет отображения - красный;

г) средняя яркость минимального элемента отображения - от 30 до 80 мкд;

д) угол обзора - 160 градусов;

е) максимальное расстояние обзора - 25 метров;

ж) необходимый уровень устойчивости функционирования к внешним воздействующим факторам при размещении на открытом пространстве должен обеспечиваться при:

температуре окружающей среды от минус 60 градусов Цельсия до плюс 70 градусов Цельсия;

относительной влажности воздуха от 30 до 95 процентов;

атмосферном давлении от 74,8 до 106,7 кПа.

57. К техническим средствам звукового оповещения предъявляются следующие требования:

а) разборчивость слов при передаче речевых сообщений - не менее 93 процентов;

б) диапазон воспроизводимых частот речевого тракта - от 0,3 до 3,4 кГц;

в) коэффициент нелинейных искажений на частоте 1000 Гц - не более 5 процентов;

г) уровень звука речевых сообщений - не менее 75 дБ на расстоянии 3 метров от специального оконечного устройства оповещения населения, но не более 120 дБ в любой точке озвучивания пространства;

д) уровень звука речевых сообщений - не менее чем на 15 дБ выше допустимого уровня звука постоянного шума;

е) сохранение работоспособности при отключении централизованного энергоснабжения - не менее 6 часов в дежурном режиме ожидания и не менее 1 часа в режиме передачи сигналов и информации оповещения;

ж) степень защиты оболочки - не ниже IP 54;

з) возможность объединения в единый аппаратно-программный комплекс технических средств по локальной сети Ethernet;

и) обеспечение звукового сопровождения трансляции видеоконтента на терминальных комплексах;

к) возможность различных настроек уровня громкости сигнала для повседневного режима работы и для режима возникновения угрозы;

л) необходимый уровень устойчивости функционирования к внешним воздействующим факторам при размещении на открытом пространстве

должен обеспечиваться при:

температуре окружающей среды от минус 50 градусов Цельсия до плюс 50 градусов Цельсия;

относительной влажности воздуха от 30 до 95 процентов;

атмосферном давлении от 74,8 до 106,7 кПа.

XI. Требования к функциональным свойствам технических систем сбора и обработки информации

58. К техническим системам сбора и обработки информации предъявляются следующие требования:

а) выполнение запросов на сбор, обработку и получение информации в соответствии с полномочиями, задаваемыми в процессе администрирования прав пользователей, инициировавших запросы;

б) срок хранения собранной информации - не менее 30 суток;

в) скорость получения информации - не более 15 секунд в расчете на 1 сутки запрашиваемого диапазона времени;

г) скорость получения информации - не более 60 секунд в расчете на 30 суток запрашиваемого диапазона времени;

д) количество одновременно обрабатываемых запросов на получение информации - не менее 30.

59. Технические системы сбора и обработки информации должны обеспечить:

а) взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

б) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.