Об утверждении
организационно-технических
требований к системам обеспечения
безопасности на объектах г.Казани

В целях создания условий для повышения безопасности людей на территории г.Казани и унификации организационно-технических подходов к реализации систем обеспечения безопасности на объектах г.Казани **обязываю:**

1. Утвердить организационно-технические требования к системам обеспечения безопасности на объектах г.Казани (далее – требования) согласно приложению к настоящему распоряжению.

2. Ввести в действие с 01.12.2017;

3. Определить уполномоченным учреждением по реализации требований Муниципальное бюджетное учреждение «Департамент телекоммуникационных технологий»;

4. Муниципальные учреждения (муниципальные заказчики) строго соблюдать требования при строительстве объектов, при проведении текущего и капитального ремонтов, реконструкции объектов;

5. Антитеррористические комиссии при проведении обследования и категорировании объектов, в том числе мест массового пребывания людей, и при принятии решений о необходимости технического переоснащения этих объектов руководствоваться настоящими требованиями.

6. Контроль за выполнением настоящего распоряжения возложить на руководителя Аппарата Исполнительного комитета г.Казани Е.А.Варакина.

Руководитель **Д.Г.Калинкин**

Утверждены распоряжением
Исполнительного комитета
г.Казани
от _____ №_____

Организационно-технические требования к системам обеспечения безопасности на объектах г.Казани

г.Казань, 2017

Оглавление

I. Термины и определения

АКБ – аккумуляторная батарея;

АПС – автоматическая пожарная сигнализация;

БИБ – библиотека;

ГИС – геоинформационная система;

Документ, требования – организационно-технические требования к системам обеспечения безопасности на объектах г.Казани;

ДК – дом культуры;

ИОО – извещатель охранный объемный;

ДОУ – дошкольное образовательное учреждение;

ЕСОП – Единый стек открытых протоколов;

ИБП – источник бесперебойного питания;

ИО – извещатель охранный точечный электроконтактный ручной ТСО;

КВ – камера видеонаблюдения;

КООПИ – комплекс объектового оборудования передачи извещений на пульт централизованного наблюдения пожарной охраны;

КТС – кнопка тревожной сигнализации ТСО;

Объект – здание, сооружение, общественное пространство (парк, сквер, сад), находящееся в муниципальной собственности;

МВД по РТ – Министерство внутренних дел по Республике Татарстан;

МК – муниципальный контракт;

МЦ – молодежный центр;

ООШ – общеобразовательное учреждение;

ОС – охранная система;

ПоК – подростковый клуб;

ППК – прибор приемно-контрольный;

ПЦН ОО – пульт централизованного наблюдения охранной организации, с которой заключен МК на услуги по предупреждению и пресечению

правонарушений и преступлений с помощью тревожной сигнализации (МК на пультовую охрану Объекта);

ПЦН ПО – пульт централизованного наблюдения пожарной охраны Управления МЧС России по Республике Татарстан;

РПУ – радиоприемное устройство ТСО;

Схема СВН – схема организации системы видеонаблюдения, разрабатываемая уполномоченным учреждением и подлежащая согласованию в порядке, установленном настоящими требованиями;

СВН – система видеонаблюдения;

СКМ – система комплексного мониторинга систем безопасности;

СКУД – система контроля и управления доступом;

СОБ – система обеспечения безопасности;

СОО – спортивно-оздоровительное учреждение;

СОУЭ – система оповещения и управления эвакуацией людей при пожаре;

СРЦ – социально-реабилитационный центр;

ТКИ – телекоммуникационная инфраструктура;

ТРУ – товары, работы, услуги;

ТСО – технические средства охраны;

ТФОП – телефонные сети общего пользования;

УВО по городу Казани – филиал ФГКУ «УВО ВНГ России по Республике Татарстан» - Управление вневедомственной охраны по городу Казани – филиал Федерального государственного казенного учреждения «Управление вневедомственной охраны войск национальной гвардии Российской Федерации по Республике Татарстан»;

УДО – учреждение дополнительного образования;

УДПС – устройство дистанционной передачи сигнала ТСО;

УКЛСиП – линии устройства контроля линий связи и пуска;

УМВД РФ по г.Казани – Управление Министерства внутренних дел Российской Федерации по городу Казани;

УОБС – устройство охранной беспроводной сигнализации ТСО.

УФСБ по РТ – Управление Федеральной службы безопасности по Республике Татарстан

II. Введение

Город Казань занимает лидирующее положение в области информационных технологий, связи и телекоммуникаций. Активному развитию этой области город обязан курсу Правительства Республики Татарстан. Именно благодаря принятию грамотных решений в республике реализованы такие проекты, как единая межведомственная система электронного документооборота и государственная интегрированная система телекоммуникаций, инфраструктура для оказания услуг в электронном виде.

Сегодня связь и информационные технологии создают целое направление в обеспечении безопасности, антитеррористической защищенности, профилактике и пресечении правонарушений. Настоящий документ определяет организационные и технические требования к оснащению и обеспечению функционирования систем обеспечения безопасности на объектах г.Казани в рамках развития аппаратно-программного комплекса «Безопасный город».

III. Область применения

Целями настоящих требований являются повышение уровня общественной безопасности, повышение пожарной и антитеррористической безопасности Объектов на территории г.Казани.

Задачами требований являются:

- унификация технологических решений;

- единство организационных подходов к системам безопасности;

- обеспечение конкуренции технологий;

- применение открытых стандартов для целей использования информации ведомствами, чьи полномочия определены законодательством.

Положения настоящих требований обязательны для исполнения при осуществлении закупок муниципальными учреждениями товаров, работ и услуг, связанных с обеспечением безопасности Объектов, если иное не установлено организационно-распорядительным документом Исполнительного комитета г.Казани.

При оснащении СОБ Объектов допускается применение оборудования, материалов, программного обеспечения, обладающих повышенными характеристиками в сравнении с приведенными в настоящих требованиях, при условии, что применение такого оборудования, материалов, программного обеспечения не приводит к увеличению затрат более чем на 20% от стоимости оборудования, материалов, программного обеспечения, соответствующих настоящим требованиям.

Требования носят рекомендательный характер для физических лиц, организаций, органов государственной власти г.Казани при реализации организационных и технических мер, направленных на защиту Объектов вне зависимости от их типа и назначения, за исключением объектов жилищного строительства.

Перечень Объектов, на которых допускается полное либо частичное отклонение от положений настоящих требований, определяется

организационно-распорядительным документом Исполнительного комитета г.Казани.

Объекты, не указанные в настоящих требованиях, должны оснащаться СОБ в соответствии с требованиями, установленными законодательством Российской Федерации.

IV. Общие принципы построения систем безопасности

Построение систем безопасности осуществляется на базе оборудования и средств, использующих для обмена информацией (интеграции, сопряжения) ЕСОП, состоящий из протоколов, применяемых в отношении СОБ.

При интеграции существующих систем безопасности, организации сбора, агрегации и дистрибуции информации допускается использовать аппаратно-программные комплексы, преобразующие стандарты (протоколы) от одной СОБ в формат стека отрытых протоколов для последующего использования данной информации.

Не допускается реализация (внедрение) новых систем безопасности, не поддерживающих ЕСОП.

Построение систем безопасности должно соответствовать следующим принципам: современность, отказоустойчивость, надежность, интегрируемость, гибкость и масштабируемость, простота в обслуживании и ремонте, пониженная стоимость владения.

V. Состав систем безопасности

В состав СОБ входят:

1) СВН;
2) СКУД;
3) АПС и СОУЭ;
4) КООПИ;
5) ТСО;
6) СКМ.

Роль вспомогательной системы, но не являющейся СОБ, выполняет ТКИ.

VI. Требования к СВН

СВН представляет собой комплекс программно-аппаратных средств, ориентированных на предупреждение, выявление и идентификацию происходящих событий, восстановление динамики ранее случившихся событий.

Оснащению СВН подлежат следующие Объекты:

- места массового пребывания людей - в порядке, установленном постановлением Правительства Российской Федерации от 25.03.2015 №272 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)»;

- объекты образования – в порядке, установленном постановлением Правительства РФ от 7 октября 2017 года №1235 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства образования и науки Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»;

- объекты спорта - в порядке, установленном постановлением Правительства Российской Федерации от 06.03.2015 №202 «Об утверждении требований к безопасности объектов спорта»;

- объекты культуры - в порядке, установленном постановлением Правительства Российской Федерации от 11.02.2017 №176 «Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий)».

При наличии финансирования в бюджете г.Казани на текущий и плановый периоды организация видеонаблюдения осуществляется на объектах молодежной политики, в социально-реабилитационных учреждениях, детских

(молодежных) лагерях, на иных Объектах, определенных в настоящих требованиях.

6.1. Организационные требования к СВН

Построение СВН осуществляется на основании схемы организации видеонаблюдения на Объекте. Исходными данными для разработки Схемы СВН служат:

- планировка Объекта;

- технический паспорт Объекта;

- данные осмотра (обследования) Объекта;

- информация о количестве совершенных на территории Объекта правонарушений, оказывающих существенное влияние на состояние общественной безопасности на территории Объекта;

- информация ГИС о местоположении Объекта, социально-экономическом положении территории, на которой находится Объект;

- иные сведения, в том числе полученные из публичных источников, результаты опроса персонала Объекта, пожелания администрации Объекта.

При разработке схем организации видеонаблюдения следует руководствоваться следующими принципами:

1) сбалансированность числа КВ на Объекте. Число КВ должно обеспечивать максимальный охват периметра Объекта, отдельных помещений, входов в здание Объекта при минимально необходимом количестве КВ;

2) исключение возможного несанкционированного доступа к КВ и СВН в целом. При невозможности этого необходимо предусмотреть конструктивные элементы, затрудняющие доступ;

3) обеспечение максимальных углов обзора и отсутствие непрозрачных помех (препятствий);

4) соответствие мест установки КВ и кабельных линий от телекоммуникационного оборудования до КВ для внутренних КВ – СП 134.13330.2012, для наружных КВ - СП 134.13330.2012 и Правилам благоустройства г.Казани.

При разработке Схемы СВН и монтаже КВ следует учитывать высоту установки КВ (горизонтальные углы обзора) для возможно полной детализации внешнего вида объекта, попадающего в поле зрения КВ, и его последующей идентификации. При выборе места размещения КВ следует учитывать, что все объекты на входах и выходах из контролируемой зоны должны гарантированно попасть в поле зрения КВ, полностью перекрывающее контролируемую зону.

Схемы видеонаблюдения на Объектах подлежат обязательному согласованию с УМВД РФ по г.Казани и УВО по городу Казани – филиал ФГКУ «УВО ВНГ России по Республике Татарстан». Без согласования УМВД РФ по г.Казани и УВО по городу Казани – филиал ФГКУ «УВО ВНГ России по Республике Татарстан» Схема СВН признается недействительной и не может быть использована для организации видеонаблюдения на Объекте.

Схемы СВН должны содержать:

1) сведения о целях, задачах и основаниях разработки;

2) ситуационный план Объекта;

3) графическую интерпретацию расположения камер на Объекте с указанием потенциальных помех (например, деревьев), уникального номера КВ;

4) сведения о наружных КВ: уникальный порядковый номер КВ, тип объектива, местоположение, зона обзора, координаты камеры в формате WGS-84, разрешение камеры (Mpix);

5) сведения о типовых решениях по монтажу наружных КВ;

6) сведения о внутренних КВ: уникальный порядковый номер, тип монтажа, уровень/высота.

Допускается указание в схемах СВН фотографического материала – указаний для производства монтажных работ.

Сведения по пунктам 3-6 скрепляются подписью должностного лица и печатью уполномоченного учреждения и УМВД РФ по г.Казани.

Видеорегистратор (видеосервер) и телекоммуникационное оборудование в случае размещения в общедоступных местах Объектов размещаются в

металлическом шкафу, защищенном от несанкционированного доступа. В случае отсутствия металлического шкафа на Объекте требуется предусмотреть его установку. Местоположение металлического шкафа подлежит согласованию с Объектом.

Кабельные линии СВН внутри Объекта прокладываются в кабель-каналах, по наружным элементам Объекта - в металлическом защитном уголке, окрашенном в цвет элемента, по которому они проложены. Не допускаются провисы кабельных линий, отклонения кабельных линий относительно вертикальных и горизонтальных осей прокладки.

При устройстве ввода (вывода) кабелей в Объект (из Объекта) отверстия необходимо надежно герметизировать. Нарушенные (вскрытые) поверхности восстанавливаются до исходного состояния.

Для СВН в зависимости от типа Объекта устанавливается предельно допустимое число КВ в расчете на каждое здание, за исключением складов, теплиц, подсобных зданий, гаражей, ангаров и иных подобных зданий:

- для дошкольных образовательных учреждений – не более 6 КВ на Объект, в обоснованных случаях допускается увеличение числа КВ до 9 единиц;

- для общеобразовательных учреждений – не более 15 КВ, в обоснованных случаях допускается увеличение числа КВ до 19 единиц;

- для учреждений дополнительного образования – не более 10 КВ, в обоснованных случаях допускается увеличение числа КВ до 13 единиц;

- для учреждений-домов культуры – не более 15 КВ, в обоснованных случаях допускается увеличение числа КВ до 19 единиц;

- для учреждений образования, культуры, спорта, физической культуры, оздоровления и молодежной политики, помещения которых находятся в общественном здании либо в здании иного Объекта, в многоквартирном доме – не более 5 КВ с учетом (за вычетом) имеющихся КВ на таких зданиях, многоквартирных домах;

- для отдельно стоящих зданий библиотек – не более 6 КВ на Объект, в обоснованных случаях допускается увеличение числа КВ до 9 единиц.

Под отдельными помещениями на Объектах подразумеваются:

1) для общеобразовательных учреждений – спортивный зал, бассейн, точка раздачи питания, посадочный зал столовой, актовый зал. Для каждого из указанных помещений предусматривается не более 1 КВ;

2) для дошкольных образовательных учреждений – фойе либо музыкальный зал, либо спортивная комната. Для каждого из указанных помещений предусматривается не более 1 КВ;

3) для учреждений дополнительного образования – актовый зал либо фойе. Для каждого из указанных помещений предусматривается не более 1 КВ;

4) для учреждений-домов культуры – фойе, актовый зал. Для каждого из указанных помещений предусматривается не более 1 КВ;

5) для библиотек – читальный зал. Предусматривается не более 1 КВ на каждое помещение;

6) для учреждений молодежной политики – фойе либо место концентрации людей. Предусматривается не более 1 КВ.

Допускается оснащение складов, подсобных зданий, гаражей, ангаров и иных подобных зданий на территории Объекта в случаях:

- постоянного хранения товарно-материальных ценностей, утрата которых существенно превышает стоимость оснащения КВ таких зданий в расчете на один календарный год;

- если такие здания расположены вблизи въездов (входов) на территорию Объекта и отсутствует иная возможность для видеомониторинга контроля доступа на Объект;

- если такие здания граничат (находятся вблизи) с местами, на которых наблюдается скопление людей, ведущих себя агрессивно по отношению к окружающим.

При этом здания складов, подсобных зданий, гаражей, ангаров и иных подобных зданий на территории Объекта должны быть обеспечены постоянным и бесперебойным электроснабжением.

Не допускается установка КВ в туалетах, тамбурах туалетов, душевых, раздевалках, гардеробах.

Для объектов СОО предельное число КВ устанавливается схемой организации видеонаблюдения без установления предельного числа КВ при условии соблюдения следующих принципов:

- сбалансированность числа КВ;
- охват периметра Объекта;
- контроль въезда на Объект;
- контроль точек прохода на Объект;
- контроль чаши (спортивных залов) Объекта;
- контроль мест концентрации людей;
- контроль точек парковки автотранспорта;
- контроль досмотровых точек.

Допускается финансирование предельного числа КВ из внебюджетных источников Объектов. Финансирование числа КВ сверх числа, предусмотренного Схемой СВН, и вытекающих из их количества оборудования и работ по содержанию (техническому обслуживанию, услуг по организации видеонаблюдения) за счет бюджета г.Казани не допускается.

В случае установки на Объекте КВ сверх предельного числа, определенного Схемой СВН, такая установка осуществляется на основании технических условий, выдаваемых уполномоченным учреждением, с последующим изменением Схемы СВН.

Допускается установка КВ согласно Схеме СВН в местах, не указанных в настоящих требованиях, без превышения предельного числа КВ на Объекте. Установка КВ на Объектах без Схемы СВН либо в местах, не соответствующих Схеме СВН, не допускается.

При организации планирования закупок ТРУ в целях организации СВН на Объектах в МК (проектах) следует предусматривать достаточный срок для проведения монтажных и пуско-наладочных работ. Такой срок может быть определен на основании уже проведенных закупок ТРУ и на основании предложений потенциальных участников.

Организация видеонаблюдения на Объектах осуществляется преимущественно по сервисной модели – путем приобретения видеоизображений, формируемых в режиме реального времени, и видеоархива. В обоснованных случаях допускается организация видеонаблюдения на Объекте путем приобретения, монтажа и пуско-наладки оборудования с последующей организацией технического обслуживания и ремонта СВН. Заключение МК только на техническое обслуживание СВН не допускается.

Не допускается техническое обслуживание (ремонт) СВН, находящихся не в муниципальной собственности либо не на балансе (оперативном управлении) Объекта.

6.2. Технические требования к СВН

6.2.1. Организация видеонаблюдения на объектах видеонаблюдения с формированием видеоизображений в режиме реального времени

6.2.1.1. Функциональные требования

1) Съемка с использованием цифрового IP-оборудования, с поддержкой отраслевого стандарта ONVIF и протоколов RTSP и RTP;

2) Качество видеоизображения в режиме реального времени и видеозаписи – не ниже Full HD;

3) Разрешение изображения – не менее 2 мегапикселей;

4) Одновременная выдача видеоизображения – не менее двух видеопотоков с использованием двух кодеков сжатия видеоданных: JPEG и H.264, с частотой не менее 25 кадров в секунду по каждому потоку;

5) Поддержка передачи одного из потоков видеоизображения в формате H.264 по протоколу Multicast/PIM-SM;

6) Возможность использования в отношении видеоматериалов базовых аналитических функций: детектора движения, пересечения отмеченных зон, обнаружения лиц в кадре;

7) Поддержка электропитания по стандарту PoE либо HiPoE;

8) Интерфейс подключения – Ethernet, RJ-45;

9) Осуществление трансляции видеоизображений в режиме «день/ночь» с использованием механического или цифрового ИК-фильтра с автопереключением;

10) При съемке в условиях недостаточной освещенности используется ИК-подсветка с дальностью не менее 30 м; оборудование с высокой чувствительностью (не менее 0,5 люкса для хорошо освещенных участков местности или не более 0,05 люкса для плохо освещенных), для наблюдения слабо освещенных объектов, имеющих малую отражательную способность, используется оборудование с высокой чувствительностью не более 0,01 люкса;

11) Функции индивидуальной настройки параметров изображения для каждой камеры (яркость, цвет, контраст), настройка временного интервала записи, настройка записи по событиям (движениям в кадре).

6.2.1.2. Требования к надежности

Надежность обеспечивается антивандальной устойчивостью используемого оборудования, соответствием применяемого оборудования климатическим условиям (от - 40º до + 40ºС) и защите от влаги и загрязнений классом не ниже IP66.

6.2.2. Организация хранения фото-, видеоданных

6.2.2.1. Функциональные требования

1) Возможность выгрузки видеозаписей в отдельное хранилище;

2) Сохранение видеосигнала, поступающего от КВ при скорости не менее 12 кадров в секунду и разрешении не ниже FullHD;

3) Аутентификация при доступе к настройкам средств обработки и просмотра видеоданных (защищенность паролем, разграничение прав доступа);

4) Запись видеосигналов от всех установленных на контролируемом объекте КВ в непрерывном режиме с фиксацией времени и даты записи, а также хранение данных по каждой КВ за последние 30 (тридцать) суток с циклической перезаписью;

5) Обеспечение записи видеоданных на встроенный массив жестких дисков и осуществление видеоархивации при максимальном качестве и разрешении, в формате сжатия H.264 или MJPEG;

6) Возможность использования записи по детектору движения;

7) Обеспечение:

7.1) возможности поиска событий по времени и дате просмотра и копирования видеоинформации для ее воспроизведения иными техническими средствами;

7.2) экспорта фрагментов архива в общедоступных форматах;

7.3) возможности удаленного использования видеоархива УФСБ по РТ, МВД по РТ, УВО по городу Казани – филиал ФГКУ «УВО ВНГ России по Республике Татарстан»;

8) Структура организации видеоархива:

8.1) локальная - на Объекте, с сегментацией по принципу: сегмент наружного видеонаблюдения/сегмент внутреннего видеонаблюдения. Необходимо предусмотреть возможность поиска видеоинформации на всю глубину видеоархива;

8.2) удаленная - на оборудовании, размещенном в помещении, защищенном от несанкционированного доступа, с гарантированным электропитанием и резервированием электропитания от не менее двух независимых источников, с системой автоматической пожарной сигнализации и пожаротушения. Сегментация: сегмент наружного видеонаблюдения/сегмент внутреннего видеонаблюдения. Необходимо предусмотреть возможность поиска видеоинформации на всю глубину видеоархива.

9) Исключение возможности удаления/модификации данных из хранилища до истечения срока хранения;

10) Все действия пользователей журналируются и хранятся не менее одного года. Журнал действий пользователей защищен от модификации/удаления/искажения/редактирования;

11) Регистрация, удаление, редактирование и учет пользователей.

6.2.2.2. Требования к надежности

1) Наличие внутренней энергонезависимой памяти для хранения установленных параметров при пропадании напряжения питания;

2) Запись видеоданных на встроенный массив жестких дисков, построенный по технологии виртуализации данных, объединяющей несколько дисков в логический элемент для избыточности и повышения производительности;

3) Защита оборудования СВН и КВ от скачка напряжения;

4) Ограничение физического доступа к оборудованию, защита от несанкционированного использования.

6.3. Требования к интеграции

6.3.1. Функциональные требования

Подключение и обеспечение взаимодействия оборудования обработки, записи, архивации и хранения видео- и фотоматериалов по каналам передачи данных, организуемых (предоставляемых) уполномоченным учреждением (Объектом, иным лицом), с использованием стандарта ONVIF и протоколов RTSP и RTP, с информационной системой уполномоченного учреждения с обеспечением реализации следующих функций:

- доступность отдельно взятой/группы КВ на отдельно взятом/группе объекте(-ов);
- удаленное управление настройками камер с использованием инструментария стандарта ONVIF;
- удаленное отключение оборудования обработки, записи, архивации и хранения видео- и фотоматериалов;
- мониторинг записи по каждой камере, мониторинг качества записи;
- мониторинг архивации видеоизображений;

– управление учетными записями на КВ и оборудовании обработки, записи, архивации и хранения видео- и фотоматериалов;

– удаленное отключение/включение функционала просмотра, выгрузки и сохранения видеоизображений;

– удаленный просмотр журнала событий, действий пользователей.

Интеграция видеопотоков (онлайн и архив) в действующее программное обеспечение видеомониторинга МВД по РТ, УФСБ по РТ, УВО по городу Казани – филиал ФГКУ «УВО ВНГ России по Республике Татарстан» по стандарту ONVIF и протоколов RTSP/RTP при предоставлении заказчиком каналов передачи данных.

6.3.2. Требования к надежности

Обеспечение защиты единого сетевого маршрутизируемого поля с использованием отдельной сети VPN от сетевых атак (лавина, шторм, отказ в обслуживании), перехвата данных, фальсификации ответов, несанкционированного доступа и иных несанкционированных (противоправных) действий.

6.4. Требования к ограничению доступа к СВН

Организациями, оказывающими услуги видеонаблюдения на Объектах, администрациями Объектов, на которых организовано видеонаблюдение, принимаются все необходимые меры по ограничению несанкционированного физического доступа к СВН.

Не допускается предоставление доступа в режиме реального времени физическим и юридическим лицам к фото- и видеоизображениям, если иное не установлено договором и (или) организационно-распорядительным документом Исполнительного комитета г.Казани.

VII. Требования к ТСО

ТСО представляют собой конструктивно законченные, выполняющие самостоятельные функции устройства, предназначенные для подачи сигнала «Тревога» с Объекта на ПЦН ОО.

Сигнал «Тревога» с Объекта в зависимости от состава и назначения ТСО может быть подан:

- путем ручного приведения в действие ТСО, выполняющих функцию КТС;

- путем автоматического срабатывания ТСО при проникновении на Объект, выполняющих функцию ОС.

В состав ТСО в объеме комплекта КТС включаются:

- ППК, 1 единица;

- ИО, 1 единица;

- АКБ, 1 единица;

- ИБП, 1 единица;

- УОБС (1 РПУ, 2 УДПС, 1 комплект);

- необходимая кабельно-проводниковая продукция.

В состав ТСО в объеме комплекта ОС включаются:

- ППК, 1 единица;

- ИОО не более 1 единицы на каждую точку прохода;

- АКБ, 1 единица;

- ИБП, 1 единица;

- необходимая кабельно-проводниковая продукция.

Допускается совмещение на программном (аппаратном, программно-аппаратном уровнях) ОС и КТС.

7.1. Организационные требования к ТСО

ТСО на Объекте размещаются в помещении охраны либо ином помещении по согласованию с Объектом. Места размещения элементов ТСО необходимо выбрать исходя из наивысшей доступности ИО для персонала

Объекта. При выборе размещения ТСО также следует учитывать ограничение возможности несанкционированного использования ИО третьими лицами.

При выборе места монтажа ИБП с АКБ, ППК и РПУ требуется учитывать ограничение возможности несанкционированного доступа к ним третьих лиц. РПУ размещается исходя из цели наивысшего охвата территории Объекта.

Оснащению ТСО в объеме КТС с последующим содержанием в обязательном порядке подлежат следующие Объекты:

- места массового пребывания людей - в порядке, установленном постановлением Правительства Российской Федерации от 25.03.2015 №272 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)»;

- объекты спорта - в порядке, установленном постановлением Правительства Российской Федерации от 06.03.2015 №202 «Об утверждении требований к безопасности объектов спорта»;

- объекты культуры - в порядке, установленном постановлением Правительства Российской Федерации от 11.02.2017 №176 «Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий)».

При наличии финансирования в бюджете г.Казани на текущий и плановый периоды оснащение ТСО и содержание в объеме КТС осуществляется на объектах молодежной политики, в социально-реабилитационных учреждениях, детских (молодежных) лагерях, на иных Объектах, определенных в настоящих требованиях.

Оснащению ТСО в объеме ОС с последующим содержанием при наличии финансирования в бюджете г.Казани на текущий и плановый периоды подлежат объекты образования, культуры, спорта и физической культуры, молодежной политики по предложению главных распорядителей бюджетных средств соответствующей сферы.

В зависимости от типа Объекта устанавливается предельно допустимое число ТСО в расчете на каждое здание Объекта, за исключением складов, теплиц, подсобных зданий, гаражей, ангаров и иных подобных зданий:

- не более одного комплекта КТС для учреждений образования, культуры, спорта и физической культуры, молодежной политики. В случае если на Объекте повседневно используется несколько входов на Объект (на территорию Объекта), каждый такой вход оборудуется не более чем одним комплектом КТС;

- не более одного комплекта ОС для учреждений образования, культуры, спорта и физической культуры, молодежной политики. ДОД должны обеспечить контроль проникновения на Объект через входы.

Склады, теплицы, подсобные здания, гаражи, ангары и иные подобные здания оснащению ТСО за счет средств бюджета г.Казани не подлежат. Объект вправе осуществить оснащение таких зданий за счет средств внебюджетных источников на основании технических условий уполномоченного учреждения.

7.2. Технические требования к ТСО

Комплект ТСО (КТС, ОС) выбирается исходя из принципов совместимости как элементов ТСО между собой, так и с ПЦН ОО с соблюдением следующих требований:

- не менее четырех шлейфов сигнализации на ППК;

- работа радиомодуля ППК в диапазонах частот GSM 1900/1800/900 МГц для связи с ПЦН ОО на скорости не менее 9600 бит/сек по GPRS-каналу связи;

- наличие в ППК интерфейса Ethernet стандарта 10BASE-T/100BASE-TX;

- срок службы ППК - не менее 10 лет;

- поддержка радиомодулем ППК отправки SMS на заданный номер: взятие, снятие, тревога, неисправность, пожар, питание от сети, питание от АКБ;

- перечень сообщений, передаваемых на ПНЦ ОО, не ограничиваясь: тревога, взят, снят, неисправность, норма, отключение, сброс по питанию, нет сети, команда выполнена (не выполнена);

- наличие индикации на ИБП, не ограничиваясь: «Наличие сети»; «Состояние АКБ. ЗАРЯД»; «Нагрузка»; Диагностические выходы тип «ОК»: «Авария»;

- емкость АКБ должна обеспечивать работоспособность ТСО в течение 40 минут при пропадании постоянного источника электропитания, но не менее 7 Ач;

- возврат в исходное состояние кнопки ИО должен осуществляться с помощью магнитного ключа;

- предельная дальность гарантированной передачи сигнала от УДПС до РПУ – не менее 150 метров в условиях прямой видимости.

7.3. Требования к ограничению доступа к ТСО

Администрациями Объектов, оснащенных ТСО, принимаются все необходимые меры по ограничению несанкционированного физического доступа к ТСО.

Не допускается выдача (предоставление) УДПС лицам, не являющимся персоналом Объекта либо сотрудниками организации, осуществляющей физическую охрану Объекта.

VIII. Требования к АПС и СОУЭ

АПС предназначена для обнаружения пожара на ранней стадии развития, подачи тревожных сигналов на пульт охраны, а также для включения системы оповещения людей о пожаре.

СОУЭ предназначена для оповещения персонала и посетителей о возгорании и определения путей эвакуации для вывода людей в безопасную зону.

8.1. Организационные и технические требования к АПС и СОУЭ

АПС и СОУЭ на Объектах устанавливаются в соответствии с проектным решением.

При проектировании и устройстве АПС следует учитывать следующие требования:

1) Установка ППК АПС и СОУЭ предусматривается в помещении охраны первого этажа либо в помещении, защищенном от несанкционированного доступа, по согласованию с Объектом. Местоположение ППК определяется исходя из доступности источников электроснабжения, возможности размещения (установки) вблизи КООПИ. Необходимо предусмотреть установку источника постоянного тока с требуемой емкостью аккумуляторных батарей.

2) При проектировании и устройстве АПС следует учитывать систему адресного типа. Допускается устройство адресно-аналоговой АПС. Устройство аналоговой АПС не допускается.

3) При техническом дооснащении уже имеющихся АПС аналогового типа на Объекте, не выработавших нормативный срок эксплуатации и соответствующих национальным стандартам, допускается установка элементов АПС аналогового типа.

4) При проектировании и устройстве СОУЭ следует учитывать проектные показатели Объекта и число пребывающих в нем лиц. СОУЭ предусматривается проектом (МК), но не ниже третьего класса.

5) Оснащение пожарными дымовыми оптико-электронными извещателями в требуемом количестве всех помещений Объекта, в том числе чердачных помещений, подвалов, кладовых, складов (в том числе отдельно стоящих), подсобных помещений. В отдельных случаях (спортивные залы, актовые залы) предусматривается установка двухпозиционных линейных пожарных дымовых извещателей.

6) Для двухпозиционных линейных пожарных дымовых извещателей и подходящих к ним кабельных линий необходимо предусмотреть защитные устройства.

7) Оснащение пожарными ручными извещателями помещений Объекта в требуемом объеме.

8) Наличие табло «Выход» 12В громкоговорителей СОУЭ в требуемом объеме в соответствии с планировкой Объекта.

9) Кабельная проводка выполнена в кабель-каналах, лотках. Проводка открытым способом по поверхностям не допускается.

10) Оборудование АПС должно быть оснащено интерфейсами интеграции (сопряжения) для целей удаленного мониторинга как состояния оборудования в целом, так и отдельных извещателей.

11) Шлейфы пожарной сигнализации и линии оповещения в защищаемых помещениях прокладываются отдельно от всех силовых, осветительных кабелей и проводов. При параллельной прокладке расстояние между проводами пожарной сигнализации с силовыми и осветительными проводами должно быть не менее 0,5 м. При необходимости прокладки этих проводов на расстоянии менее 0,5 м от силовых и осветительных проводов они должны иметь защиту от наводок. Допускается уменьшить расстояние до 0,25 м от проводов АПС без защиты от наводок до одиночных осветительных кабелей и проводов. При прокладке проводов системы пожарной сигнализации, охранной сигнализации и системы оповещения по одной трассе разрешается располагать их вплотную друг к другу.

12) Трассы электропроводок следует выбирать наикратчайшими, с учетом расположения силовых, осветительных, радиотрансляционных сетей, водопроводных и газовых магистралей, а также других коммутаций.

13) В местах прохода проводов и кабелей через стены, перекрытия или их выхода наружу следует заделывать зазоры между проводами, кабелями и трубой (коробом, проемом) легко удаляемой массой из несгораемого материала.

14) Элементы электропроводок закрепляются клипсами или скобами у вводов в приборы и коробки на расстоянии 50-100 мм от них. При прокладке кабелей в местах поворота под углом поворота, близким к 90 градусам, радиус изгиба должен быть не менее десяти диаметров кабеля. Допускается только однократный поворот с радиусом изгиба в семь диаметров кабеля. При прокладке нескольких проводов в одной трассе следует располагать их в одной трубе или одном кабель-канале. Соединения и ответвления элементов электропроводок должны производиться в коробках или внутри корпусов электроустановок изделий способом пайки или с помощью винтов (не допускается применение винтовых соединений в местах с повышенной влажностью). Соединения кабелей пожарной сигнализации требуется производить в огнестойких монтажных коробках. В местах присоединения жил следует предусмотреть запас проводника, обеспечивающий возможность повторного присоединения. В местах соединений и ответвлений проводки не должны испытывать механических усилий. Места соединений и ответвлений должны быть доступны для осмотра и ремонта.

15) Размещение оборудования должно исключать его случайное падение или перемещение по установочной поверхности, при котором возможно повреждение подключаемых проводов. При размещении приборов необходимо обеспечить нормальную освещенность приборных панелей. Дымовые пожарные извещатели необходимо установить на потолке на расстоянии не менее 0,1 м от стен. В местах, где имеется опасность механического

повреждения извещателя, следует предусмотреть защитную конструкцию, не нарушающую работоспособность извещателя.

16) Извещатели следует устанавливать не ближе чем на расстоянии 1 м от приточно-вытяжной вентиляции и не ближе чем на расстоянии 0,5 м от осветительных приборов. Дымовые пожарные извещатели в помещениях с высотой потолков до 3,5-6,0 м следует устанавливать на расстоянии не более чем 4,0 м от стены и не более чем 8,5 м между ними. В помещениях и коридорах, ширина которых не превышает 3 м, разрешается увеличивать расстояние между извещателями в 1,5 раза. Ручные пожарные извещатели должны устанавливаться на стене, на высоте 1,5 м от уровня пола, на удалении от источников сильных электромагнитных излучений, на расстоянии не менее 0,75 м от других органов управления.

СОУЭ должна соответствовать следующим требованиям:

1) Речевые оповещатели установлены на стене, на высоте не менее 2,3 м от уровня пола и не менее 150 мм от потолка до верхней части. Световые оповещатели «Выход» и указатели направления движения устанавливаются в местах, определенных проектом, над эвакуационными выходами (или сбоку, в непосредственной близости от эвакуационных выходов) на высоте не менее 2 м от уровня пола и не ближе 0,1 м от потолка.

2) Для предотвращения несанкционированного нажатия и ложной сработки систем пожарной сигнализации и оповещения все ручные пожарные извещатели подлежат опломбировке.

3) Звуковые сигналы СОУЭ должны обеспечивать уровень звука не менее чем на 15 дБА выше допустимого уровня звука постоянного шума в защищаемом помещении. Измерение уровня звука должно проводиться на расстоянии 1,5 м от уровня пола. В спальных помещениях звуковые сигналы СОУЭ должны иметь уровень звука не менее чем на 15 дБА выше уровня звука постоянного шума в защищаемом помещении, но не менее 70 дБА. Измерения должны проводиться на уровне головы спящего человека. Выбор количества и мест установки оповещателей производится с учетом:

3.1) размеров защищаемого помещения и уровня шума в нем, определяемого по перечню [Источник шума - Уровень шума, дБ(А)]: спокойное дыхание - 10, шелест страниц - 20, шепот - 30, холодильник - 40-43, компьютер - 37-45, кондиционер - 40-45, вытяжной вентилятор - 50-55, телевизор, электробритва - 60, спокойный разговор - 66, речь по радио, громкий разговор - 70, пылесос - 75, детский плач - 78, игра на пианино - 80, музыка по радио, электрополотер - 83, перфоратор, громкий крик - 90-95, домашний кинотеатр на полную мощность - 110;

3.2) вида установки оповещателей – настенная;

3.3) звукового давления устанавливаемых оповещателей;

3.4) рекомендаций проектных организаций, специализирующихся на проектировании систем оповещения о пожаре и управления эвакуацией людей.

Расстановка оповещателей определяется путем расчета уровня звукового давления, который должен развить оповещатель в точке измерения: РΣ = Р + 15дБ, где:

РΣ определяется суммой уровня постоянного шума в помещении (Р) и необходимого превышения над ним, которое составляет 15 дБ.

Уровень шума при расчетах определяется на основании исходных данных, в зависимости от назначения защищаемого помещения.

В качестве технических средств светового оповещения людей о пожаре применяются:

- оповещатель пожарный световой «Выход»;

- оповещатель пожарный световой - указатель направления движения.

Звуковые и световые оповещатели включаются в УКЛСиП. УКЛСиП обеспечивают контроль линии подключенных исполнительных устройств. Световые табло горят постоянно. Линии речевого оповещения требуется выполнить кабелем для охранно-пожарной сигнализации (соответствует требованиям, установленным в ГОСТ Р МЭК 60332-3-22-2005 по нераспространению горения при пучковой прокладке, а также требованиям ГОСТ Р МЭК 60331-23-2003, НПБ 248-97 по сохранению работоспособности

при воздействии открытого пламени в течение 180 минут) по потолку и стенам в гофротрубе ПВХ за подвесным потолком или в кабель-канале в помещениях без подвесного потолка. Линии светового оповещения (табло) должны быть выполнены кабелем для охранно-пожарной сигнализации (соответствует требованиям, установленным в ГОСТ Р МЭК 60332-3-22-2005 по нераспространению горения при пучковой прокладке, а также требованиям ГОСТ Р МЭК 60331-23-2003, НПБ 248-97 по сохранению работоспособности при воздействии открытого пламени в течение 180 минут) по потолку и стенам в гофротрубе ПВХ за подвесным потолком или в кабель-канале в помещениях без подвесного потолка.

В отношении АПС и СОУЭ предусматривается проведение работ по техническому обслуживанию и ремонту. Заключение МК только на техническое обслуживание АПС и СОУЭ не допускается, если иное не установлено организационно-распорядительным документом Исполнительного комитета г.Казани.

В отношении АПС и СОУЭ, по которым сроки эксплуатации, указанные в паспорте изделия, уже истекли или истекут в ближайший календарный год, следует предусматривать дополнительные организационно-технические меры, направленные на обеспечение их работоспособности.

8.2. Требования к ограничению доступа к АПС и СОУЭ

Администрациями Объектов, оснащенных АПС и СОУЭ, принимаются все необходимые меры по ограничению несанкционированного физического доступа к АПС и СОУЭ.

Не допускается выдача (предоставление) кодов (паролей, ключей) к ППК АПС лицам, не являющимся персоналом Объекта, за исключением сотрудников уполномоченного учреждения и сотрудников организации, осуществляющей техническое обслуживание и ремонт АПС и СОУЭ.

IX. Требования к СКУД

СКУД представляет собой совокупность программно-аппаратных технических средств, имеющих целью ограничение и регистрацию входа-выхода объектов (людей) на заданной территории через точки доступа. В отдельных случаях СКУД используется для целей регулирования доступа внутри Объектов.

9.1. Организационные требования

Для СКУД в зависимости от типа Объекта устанавливается предельно допустимое число точек прохода в расчете на каждое здание (таблица 1), за исключением складов, теплиц, подсобных зданий, гаражей, ангаров и иных подобных зданий.

Таблица 1

Тип точки доступа	ООШ	ДОУ	СОО	УДО	ДК, КМЦ	БИБ	ПоК	СРЦ
Наружная дверь на Объект	Допускается, не более 2	Допускается, не более 3	Допускается, не более 2					
Калитка в составе ограждения Объекта по периметру	Допускается, не более 1	Допускается, не более 2	Не допускается					
Двери внутри Объекта	Не допускается	Не допускается	Допускается для отдельных помещений	Не допускается				

Действие требований, указанных в таблице 1, не распространяется на точки прохода, оснащенные СКУД до утверждения настоящих требований.

СКУД оснащаются исключительно подготовленные (приспособленные) для этих целей точки прохода:

- двери: из вандалоустойчивого материала (либо вандалоустойчивой конструкции) толщиной, достаточной для установки исполнительных устройств (доводчик, электромагнитный замок) СКУД; не должны иметь

отклонений относительно вертикальной оси, должны плотно прилегать к притворной рамке;

- калитки: выполнены из цельнометаллического листа либо сварены из металлических прутов (труб, уголков) с обрамлением рамкой; расстояние от вертикальной торцевой части полотна до рамки - не более 2 см, с наличием необходимых площадок для установки исполнительных устройств.

Не допускается оснащение СКУД:

1) калиток в составе ограждений, высота которых составляет менее двух метров от уровня земли, либо ограждений, выполненных не из металлоконструкций. Действие настоящего пункта не распространяется на точки прохода – калитки, оснащенные СКУД до утверждения настоящих требований;

2) калиток в составе ограждений, имеющих лазы, дыры в ограждениях.

Организация ограждений, приведение в соответствие ограждений, дверей, калиток для целей оснащения СКУД осуществляется Объектами в пределах средств, предусмотренных бюджетом г.Казани и (или) внебюджетными источниками Объектов.

Допускается финансирование предельного числа точек прохода в том числе из внебюджетных источников Объектов. Финансирование точек прохода сверх числа, предусмотренного таблицей 1, и вытекающих из их количества оборудования и работ по содержанию (техническому обслуживанию, услуг по организации контроля доступа) за счет бюджета г.Казани не допускается.

В случае установки на Объекте точек доступа сверх предельного числа, определенного таблицей 1, такая установка осуществляется на основании технических условий, выдаваемых уполномоченным учреждением.

В отношении точек доступа, не оснащенных СКУД, Объектом принимаются все необходимые меры по ограничению доступа, в том числе путем установки механических запорных механизмов и замков.

Установка точек доступа на Объектах в местах, не соответствующих таблице 1, не допускается.

При организации планирования закупок ТРУ в целях организации СКУД на Объектах в МК (проектах) следует предусматривать достаточный срок для проведения монтажных и пуско-наладочных работ. Такой срок может быть определен на основании уже проведенных закупок ТРУ и на основании предложений потенциальных участников.

Организация СКУД на Объектах осуществляется преимущественно по сервисной модели. В обоснованных случаях допускается организация СКУД на Объекте путем приобретения, монтажа и пуско-наладки оборудования с последующей организацией технического обслуживания и ремонта СКУД. Заключение МК только на техническое обслуживание СКУД не допускается, если иное не установлено организационно-распорядительным документом Исполнительного комитета г.Казани.

Не допускается техническое обслуживание (ремонт) СКУД, находящейся не в муниципальной собственности либо не на балансе (оперативном управлении) Объекта.

В объектах типа СОО в качестве отдельных выделяются следующие помещения:

- серверные, радиоузлы;

- помещения, в которых размещены органы управления (диспетчеризации) инженерных систем, несанкционированное вмешательство в работу которых может оказать существенное влияние на нормальное функционирование Объекта;

- помещения, занимаемые правоохранительными органами в период подготовки и проведения спортивных, культурно-массовых мероприятий для целей оперативного контроля за ситуацией на Объекте.

Оснащение СКУД складов, подсобных зданий, гаражей, ангаров и иных подобных зданий на территориях Объектов допускается только за счет

внебюджетных средств Объектов на основании технических условий, выдаваемых уполномоченным учреждением.

При установке элементов СКУД следует руководствоваться следующими принципами:

1) исключение возможного несанкционированного доступа на Объект через точки доступа;

2) соответствие мест установки СКУД и кабельных линий Правилам благоустройства г.Казани;

3) электрическая безопасность всех элементов СКУД;

4) антивандальная устойчивость и всепогодное исполнение наружных элементов СКУД.

Управляющее оборудование СКУД в случае установки в общедоступном месте Объекта размещается в металлическом шкафу, защищенном от несанкционированного доступа.

Кабельные линии внутри Объекта прокладываются в кабель-каналах, по наружным элементам Объекта - в металлическом защитном уголке, окрашенном в цвет элемента, по которому они проложены, либо в металлорукаве. Не допускаются провисы кабельных линий, отклонения кабельных линий относительно вертикальных и горизонтальных осей прокладки.

Кабельные линии в грунте обустраиваются в соответствии со строительными нормами и правилами, ведомственными строительными нормами в зависимости от типа кабельных линий. Проведение земляных работ должно соответствовать Правилам благоустройства г.Казани, утвержденным решением Казанской городской Думы от 18.10.2006 №4-12 (с изменениями и дополнениями), и Положению об организации и проведении земляных, строительных и ремонтных работ, связанных с благоустройством территории г.Казани.

9.2. Технические требования

9.2.1. Функциональные требования

1) Реализация базы данных пропусков на не менее 1300 учетных записей на каждом Объекте;

2) Ведение журнала событий периодом не менее чем 30 дней;

3) Удаленное управление учетными записями;

4) Интеграция (сопряжение) с автоматической пожарной сигнализацией Объекта по реле (сухому контакту) для реализации режима экстренной эвакуации;

5) Режимы работы управляющего оборудования СКУД отражаются с использованием световой и звуковой индикации;

6) Допускается доступ к интерфейсу управляющего оборудования СКУД в том числе обеспечивается посредством Ethernet либо Wi-Fi, либо GSM, либо RS-485;

7) Допускается возможность в том числе удаленного создания/ведения/редактирования групп доступа;

8) Типы записываемых ключей: простой, мастер;

9) Поддержка исполнительных устройств (запорных механизмов) на Объекте в зависимости от точки доступа: электромеханический/электромагнитный замок, турникет;

10) Поддержка установки длительности открывания запорного механизма;

11) Поддержка режимов:

11.1) обычный режим – проход простым ключам согласно базе данных пропусков;

11.2) экстренной эвакуации – автоматическая разблокировка исполнительных устройств (запорных механизмов) на весь период действия режима, в том числе по сигналу автоматической пожарной сигнализации;

11.3) режим восстановления базы данных ключей – разрешение доступа всем подносимым ключам с занесением ключей в базу данных.

9.2.2. Требования к надежности

Надежность СКУД обеспечивается соответствием применяемого оборудования климатическим условиям (от + 5ºС до + 40ºС), защите от неправильного включения, наличию внутренней энергонезависимой памяти и функции автоматического восстановления настроек и базы данных.

9.3. Организация работы точек доступа

9.3.1. Функциональные требования

1) Фиксация исполнительных устройств (запорных механизмов) в соответствии с режимом, установленным управляющим оборудованием СКУД;

2) Обеспечение принудительного закрывания двери (калитки) при входе/выходе на Объект;

3) Разблокировка исполнительных устройств (запорных механизмов) при срабатывании считывателя при успешной идентификации карты доступа, по режиму управляющего оборудования СКУД, по нажатию кнопки выхода;

4) Поддержка голосовой связи на одной из точек доступа с дежурным (ответственным) сотрудником Объекта с возможностью дистанционной разблокировки ответственным сотрудником исполнительного устройства (запорного механизма). Точка доступа, на которой поддерживается голосовая связь с ответственным сотрудником Объекта определяется Объектом.

9.3.2. Требования к надежности

Надежность точек доступа обеспечивается антивандальным исполнением оборудования, соответствием применяемого оборудования климатическим условиям (от - 40ºС до + 40ºС).

9.4. Требования к организации доступа на Объект с использованием СКУД.

Функциональные требования

1) Организация доступа на Объект через точки доступа осуществляется с использованием:

– голосовой связи в соответствии с 9.3.1 настоящих требований и в соответствии с правилами внутреннего распорядка Объекта;

– карт доступа – при организации персонифицированного учета таких карт (идентификаторов). Тип считывателя - RFID для работы с не менее чем двумя типами идентификаторов, стандартов EM-Marine и Temic (T5557), с защитой от использования дубликатов (клонов) идентификаторов доступа, имеющий температурный режим работы от -30ºС до +40ºС;

– программно-аппаратных, программных средств – при организации персонифицированного учета дистрибуции таких средств.

2) Организация персонифицированного доступа на Объект реализуется по технической готовности заказчика в течение 30 календарных дней после получения исполнителем соответствующего уведомления от заказчика.

Допускается интеграция со СКУД на Объекте внешних аппаратно-программных (программных/аппаратных) средств (оборудования), в том числе реализующих функции внешнего управления СКУД (разблокировка (блокировка) запорного механизма, статус СКУД, положение запорных механизмов).

9.5. Требования к ограничению доступа к управляющему оборудованию СКУД

Администрациями Объектов, оснащенных СКУД, принимаются все необходимые меры по ограничению несанкционированного физического доступа к управляющему оборудованию СКУД.

Не допускается выдача (предоставление) мастер-ключей (блокирующих ключей) лицам, не являющимся персоналом Объекта, за исключением сотрудников уполномоченного учреждения и сотрудников организации, осуществляющей техническое обслуживание и ремонт СКУД (оказывающей услуги по организации СКУД на Объекте).

9.6. Порядок учета карт (ключей) доступа к СКУД на Объектах

При организации СКУД необходимо предусмотреть выдачу ключей персоналу Объекта в количестве, указанном в таблице 2.

Таблица 2

Число карт (ключей) доступа на Объект, не менее/не более	**Тип Объекта**							
	ООШ	**ДОУ**	**СОО**	**УДО**	**ДК, КМЦ**	**БИБ**	**ПоК**	**СРЦ**
	4/6	2/4	8/12	4/6	4/6	1/3	1/3	1/3

Выдача карт (ключей) доступа лицам, не указанным в Таблице 2, за счет бюджета г.Казани не допускается, если иное не установлено организационно-распорядительным документом Исполнительного комитета г.Казани.

В зависимости от заключенного договора (МК) на организацию СКУД (техническое облуживание и ремонт СКУД) Объектом или уполномоченным учреждением допускается организация выдача карт (ключей) доступа СКУД посетителям Объекта. При этом Объект, принявший такое решение, определяет источник финансирования выдачи карт (ключей) доступа с учетом настоящих требований и обеспечивает учет выданных карт (ключей) с предоставлением такой информации в адрес уполномоченного учреждения в течение 7 рабочих дней с даты выдачи карт (ключей) доступа с последующей ежеквартальной актуализацией. Информация о выданных картах (ключах) доступа не должна содержать персональных данных лиц, получивших данные карты, но должна содержать уникальные номера выданных карт (ключей) доступа с привязкой к Объекту.

X. Требования к КООПИ

КООПИ представляет собой совокупность программно-аппаратных средств, включающую в себя объектовую станцию и устройство оконечное объектовое автоматического вызова и предназначенную для автоматической передачи извещений (без участия персонала Объекта) от объектовой АПС на ПЦН ПО.

10.1. Организационные требования

КООПИ на Объекте размещается в помещении охраны первого этажа либо в помещении, защищенном от несанкционированного доступа, по согласованию с Объектом. Местоположение КООПИ определяется исходя из доступности источников электроснабжения, возможности размещения (установки) вблизи ППК АПС, точки подключения к ТФОП, наименьшего уровня электромагнитных помех в целях устойчивой передачи сигнала посредством радиоканальной системы и (или) сетей сотовой связи.

КООПИ должен быть интегрирован (сопряжен) с ППК АПС в порядке, установленном паспортом изделия КООПИ. Работа КООПИ без интеграции (сопряжения) с АПС не допускается.

КООПИ в обязательном порядке оснащаются здания образовательных учреждений, в том числе ООШ, ДОУ, УДО, СОО. Допускается оснащение КООПИ ДК, КМЦ, ПоК, СРЦ.

Оснащение КООПИ складов, подсобных зданий, гаражей, ангаров и иных подобных зданий на территориях Объектов допускается только за счет внебюджетных средств Объектов на основании технических условий, выдаваемых уполномоченным учреждением.

При закупках ТРУ в МК следует предусматривать условия:

1) по организации исполнителем передачи извещений от КООПИ на Объекте на ПЦН ПО;

2) технического обслуживания и ремонта КООПИ силами и за счет исполнителя.

Заключение МК только на техническое обслуживание КООПИ не допускается, если иное не установлено организационно-распорядительным документом Исполнительного комитета г.Казани.

10.2. Технические требования к КООПИ

Передача извещений от КООПИ на ПЦН ПО осуществляется с использованием ТФОП/GSM/радиоканальной системы в зависимости от типа устройства оконечного объектового автоматического вызова. При проведении капитального ремонта (плановой замены) устройства оконечного объектового автоматического вызова следует выбирать такие устройства с поддержкой интерфейса Ethernet и/или стандарта GSM.

Передача извещений посредством радиоканальной системы осуществляется согласно письму Приволжского регионального центра МЧС России от 01.04.2014 №4633-17-2 «О назначении радиочастот», по решению Министерства обороны Российской Федерации от 29.11.2010 №205/307/1979 и в соответствии с выделенными для этих целей частот.

В случае если для передачи извещений от КООПИ на ПЦН ПО используется ТФОП, то для нормального функционирования КООПИ следует предусматривать отдельную линию ТФОП либо осуществить выбор наименее загруженной линии ТФОП на Объекте. Обязанность по организации и обеспечению работоспособности линий ТФОП, используемых для целей передачи извещений от КООПИ на ПЦН ПО, возлагается на Объект.

КООПИ должен поддерживать следующий функционал:

1) контроль состояния АПС с настраиваемой частотой передачи статуса АПС на ПЦН ПО;

2) контроль вскрытия объектовой станции;

3) интерфейс RS-232;

4) интерфейс USB;

5) интерфейс модуля входов контроля (МВК-RS);

6) интерфейс модуля сопряжения (МС-RS);

7) емкость АКБ должна обеспечивать работоспособность КООПИ в течение 40 минут при пропадании постоянного источника электропитания, но не менее 7 Ач.

10.3. Требования к ограничению доступа к КООПИ

Администрациями Объектов, оснащенных КООПИ, принимаются все необходимые меры по ограничению несанкционированного физического доступа к КООПИ.

Не допускается выдача (предоставление) ключей к КООПИ лицам, не являющимся персоналом Объекта, за исключением сотрудников уполномоченного учреждения и сотрудников организации, осуществляющей техническое обслуживание и ремонт КООПИ.

XI. Требования к СКМ

СКМ представляет собой программно-аппаратное решение для целей мониторинга работоспособности (состояния) АПС, СОУЭ, КТС, КООПИ, СКУД на Объекте и передачи информации в информационные системы мониторинга.

11.1. Организационные требования

Установка оборудования СКМ осуществляется в помещении охраны или ином помещении, защищенном от несанкционированного доступа, по согласованию с Объектом.

СКМ оснащаются здания Объектов ООШ, ДОУ, УДО, СОО, ДК, КМЦ, ПоК, СРЦ, на которых функционируют любые из следующих СОБ: АПС и СОУЭ, КООПИ, КТС, СКУД.

Оснащение СКМ складов, подсобных зданий, гаражей, ангаров и иных подобных зданий на территориях Объектов не допускается.

При организации планирования закупок ТРУ в целях организации СКМ на Объектах в МК (проектах) следует предусматривать достаточный срок для проведения монтажных и пуско-наладочных работ. Такой срок может быть определен на основании уже проведенных закупок ТРУ и на основании предложений потенциальных участников.

Организация СКМ на Объектах осуществляется как по сервисной модели, так и путем приобретения, монтажа и пуско-наладки оборудования с последующей организацией технического обслуживания и ремонта СКМ. Заключение МК только на техническое обслуживание СКМ не допускается, если иное не установлено организационно-распорядительным документом Исполнительного комитета г.Казани.

Не допускается техническое обслуживание (ремонт) СКМ, находящихся не в муниципальной собственности либо не на балансе (оперативном управлении) Объекта.

11.2. Требования к ограничению доступа к СКМ

Администрациями Объектов, оснащенных СКМ, принимаются все необходимые меры по ограничению несанкционированного физического доступа к СКМ.

Не допускается выдача (предоставление) кодов (паролей) к СКМ лицам, не являющимся персоналом Объекта, за исключением сотрудников уполномоченного учреждения и сотрудников организации, осуществляющей техническое обслуживание и ремонт СКМ.

11.3. Технические требования

СКМ должна обеспечивать:

- интеграцию с АПС, в том числе осуществлять мониторинг работоспособности АПС в целом, а в случае если АПС адресного (адресно-аналогового) типа, то отдельно взятого датчика (зоны);

- интеграцию с КТС, в том числе принимать/обрабатывать и передавать дублирующий сигнал тревоги;

- интеграцию с КООПИ, обеспечивающую контроль рабочего состояния;

- интеграцию со СКУД, обеспечивающую мониторинг состояния СКУД, в том числе положение исполнительных устройств.

Срок службы оборудования СКМ должен составлять не менее 10 лет непрерывной эксплуатации.

СКМ должен быть оснащен модулями интерфейсов сопряжения, перечисленными в настоящих требованиях по отношению к СОБ на Объектах.

СКМ должен быть оснащен интерфейсом Ethernet/802.11(a/b/g/n) либо GSM, при этом скорость передачи данных по сетям GSM должна обеспечивать гарантированную передачу данных при величине потери пакетов не более 99,9%.

Емкость АКБ должна обеспечивать работоспособность СКМ в течение 40 минут при пропадании постоянного источника электропитания, но не менее 7 Ач.

XII. Требования к ТКИ

ТКИ не относится к СОБ на Объектах и выполняет функцию по передаче данных с Объекта и на Объект, в том числе межмашинного взаимодействия (M2M) для целей:

- мониторинга СОБ;

- мониторинга СВН;

- получения статистической и динамической информации с Объектов;

- удаленного подключения как к КВ, так и к видеорегистраторам (видеосерверам), в том числе путем M2M;

- мониторинга информационной безопасности Объекта;

- решения иных задач в области обеспечения безопасности на Объектах и достижения целей Объектами, ради которых они созданы.

12.1. Организационные и технические требования к ТКИ

ТКИ организуется на базе:

- сетей фиксированной связи, в том числе беспроводной передачи данных;

- сетей сотовой связи;

- виртуальных (ведомственных сетей);

- сетей передачи данных на Объекте.

Подключение Объекта к ТКИ осуществляется приоритетно по волоконно-оптическим линиям связи, затем по беспроводным сетям передачи данных и только потом – по сетям сотовой связи. Выбор способа подключения Объекта к ТКИ определяется уполномоченным учреждением с учетом технической возможности, экономической целесообразности и результатов изысканий (исследований).

При Подключении Объектов к сетям фиксированной связи при размещении оборудования беспроводной передачи данных, оборудования сотовой связи следует руководствоваться Правилами благоустройства г.Казани.

Размещаемое оборудование ТКИ на Объекте должно обладать необходимыми сертификатами в области санитарно-гигиенической, пожарной, электрической и электромагнитной безопасности.

Передача данных ТКИ осуществляется в рамках единого сетевого маршрутизируемого поля с использованием отдельной сети VPN (Virtual Private Network). Использование локальной вычислительной сети Объекта, используемой в хозяйственной (образовательной) деятельности Объекта, для целей построения ТКИ допускается только при условии разделения сетей на уровне коммутаторов и реализации соответствующих политик безопасности, исключающих несанкционированный доступ к СОБ и/или получение (перехват) данных.

При организации ТКИ следует предусматривать защиту единого сетевого маршрутизируемого поля с использованием отдельной сети VPN (Virtual Private Network) от сетевых атак (лавина, шторм, отказ в обслуживании), перехвата данных, фальсификации ответов, несанкционированного доступа и иных несанкционированных (противоправных) действий.

Организационные и технические меры должны позволять выявлять и предотвращать атаки по содержанию и контексту сетевых пакетов с использованием списка шаблонов атак, эвристического анализа и обнаружения аномалий:

1) предотвращение атак типа «лавина» или «шторм»;

2) предотвращение атак «Отказ в обслуживании» (DoS);

3) проверка атак на нестандартных портах;

4) реализация защиты от сетевых червей, «троянских коней» и вирусов путем анализа сетевой активности;

5) применение защиты от атак против CGI-скриптов или веб-атаки;

6) организация защиты от атак типа «переполнение буфера»;

7) организация защиты от атак на протокол RPC;

8) организация защиты от Unicode-атак;

9) организация защиты от фрагментированных атак;

10) организация защиты от атак на протоколы IP-телефонии H.323 и H.235;

11) организация защиты от атак с использованием протокола ICMP;

12) организация защиты от атак на приложения (SMTP, Sendmail, IMAP или POP, FTP, SSH, Telnet и rlogin, DNS);

13) организация защиты от перехвата соединений протокола TCP (TCP hijack) и защита приложений, использующих TCP;

14) организация защиты от атак с использованием уязвимостей ОС Microsoft Windows и атак против протокола NetBios.

Программно-аппаратные средства ТКИ должны обладать следующим функционалом:

1) анализ содержания IP-пакетов на всех уровнях сетевой модели OSI, начиная с третьего;

2) обнаружение попыток несанкционированного доступа (НСД) в режиме реального времени;

3) предупреждение попыток НСД в режиме реального времени путем блокирования или завершения нежелательных сетевых сессий;

4) реализация динамического изменения списков доступа на маршрутизаторах, изменения правил на межсетевом экране, изменения списков контроля доступа на коммутаторе, разрыв соединения или регистрация IP-соединений;

5) создание нескольких политик безопасности (виртуальные контексты).

В целях идентификации на уровне доступа и при доступе к консоли управления всеми устройствами сеть должна работать с использованием следующих возможностей:

1) безопасность портов (Port Security) – возможность использования порта коммутатора заранее заданными физическими адресами пользовательских ПК. При попытке подключения неавторизованного устройства – отключение этого порта и уведомление системы управления сети;

2) автоматическое конфигурирование портов коммутаторов – автоматизация изменения конфигурации порта на основе логического подключения пользователя к сети (login);

3) аутентификация административного доступа на серверах TACACS+ и/или RADIUS – идентификация, авторизация и учет при доступе к командной строке устройства;

4) IP permit lists – ограничение на доступ к командной строке устройства, системной консоли, SNMP;

5) Port Protocol Filtering – автоматическая фильтрация трафика неиспользуемых протоколов на портах коммутаторов;

Следующие системные средства мониторинга политики качества обслуживания и безопасности, планирования сети и сервисов должны работать на всех телекоммуникационных устройствах сети:

- Embedded RMON (Events, Alarms, History, Etherstat) – возможность сбора статистики RMON с точностью до порта сети для анализа производительности сети;

- Switch Port Analyzer (SPAN) – возможность перенаправлять трафик отдельных портов, групп портов и виртуальных портов на анализатор протоколов для детального анализа;

- статистика NetFlow – углубленный анализ потоков сетевого и транспортного уровней;

- отладка/диагностика (Debug/Diagnostics) – расширенные встроенные возможности мониторинга событий в реальном времени для расширения возможностей диагностики помимо внешних анализаторов;

- Syslog – сбор и сохранение информации о существенных сетевых событиях, включая изменения конфигураций устройств, изменения топологии, программные и аппаратные ошибки;

- HTTP/Web-Based Management – доступ к интерфейсу управления устройством и отчетам через стандартный web-браузер;

- Plug-and-Play Protocols – автоматическая конфигурация Fast/Gigabit EtherChannel, виртуальных сетей, транков VLAN;

- агенты распознавания топологии (Topology Discovery Agents) – автоматическое распознавание топологии сети.

12.2. Требования к уровням сервиса и отказоустойчивости ТКИ

1) Универсальный характер обслуживания разных приложений;

2) Независимость от технологий связи и гибкость получения набора, объема и качества сервисов;

3) Интеграция трафика разнородных данных; выделенные цифровые каналы с постоянной скоростью передачи; пакетная передача данных (FR) с требуемым качеством сервиса; передача изображений, видеоконференцсвязь; телевидение; сервис по требованию (On-Demand); IP-телефония;

4) Широкополосный доступ в Интернет; сопряжение удаленных ЛВС, в том числе работающих в различных стандартах; создание виртуальных корпоративных сетей, коммутируемых и управляемых уполномоченным учреждением;

5) Возможность передачи большому количеству пользователей в реальном времени больших объемов информации с необходимой синхронизацией и использованием сложных конфигураций соединений;

6) Интеллектуальность (управление сервисом, вызовом и соединением со стороны пользователя или поставщика сервиса);

7) Инвариантность доступа (организация доступа к сервисам независимо от используемой технологии);

8) Комплексность сервисов (возможность участия нескольких операторов связи в предоставлении сервисов и разделение их ответственности сообразно с видом деятельности каждого);

9) Масштабируемость – подразумевает возможность наращивания пропускной способности сети и количества подключений конечных абонентов

сети без внесения существенных изменений в логическую структуру сетевой системы и с наименьшими затратами на дополнительное сетевое оборудование;

10) Мультисервисность – создаваемая сеть имеет полный набор сервисов доступа к информационным ресурсам, включая передачу цифрового и голосового трафика, данных мультимедиа (видеотрансляции и видеоконференции), а также поддержку всех применяемых сетевых протоколов передачи данных;

11) Отказоустойчивость – обеспечивается за счет резервирования основных узлов и блоков активного сетевого оборудования, создания резервных линий связи и применения современных протоколов управления потоками данных. Доступность каналов передачи данных ТКИ должна составлять не менее 99,9% времени. Совокупная доля потерянных пакетов не должна превышать 99,999%.

XIII. Порядок доступа к информации о состоянии СОБ и информации, формируемой СОБ

13.1. Требования к организации доступа к фото- и видеоизображениям

13.1.1. Требования к организации доступа к фото- и видеоизображениям в режиме реального времени

Доступ к фото-, видеоизображениям в режиме реального времени реализуется:

1) непосредственно на Объекте, путем установки оборудования отображения информации (АРМ, монитор), позволяющего получать регламентированный доступ к видеоизображениям в режиме реального времени;

2) удаленно, к КВ на объекте по потоковому протоколу реального времени RTP/RTSP по стандарту ONVIF profile S. В случае если задержка видеоизображения при удаленном доступе к фото- и видеоизображениям с видеорегистратора (сервера видеонаблюдения) не превышает более 1 секунды от реального времени, то доступ может быть организован путем подключения к такому видеорегистратору (серверу видеонаблюдения), поддерживающему стандарт ONVIF profile S и/или необходимый программный интерфейс (API).

Удаленный доступ к фото- и видеоизображениям организуется только для целей:

1) передачи видеопотоков от наружных КВ [сегмента наружного видеонаблюдения на видеорегистраторе (сервере видеонаблюдения)] в интересах правоохранительных органов;

2) мониторинга работоспособности КВ и СВН на Объектах в целом;

3) передачи видеопотоков в информационные системы (программное обеспечение), используемые уполномоченным учреждением.

Приоритетный доступ к фото- и видеоизображениям по потоковому протоколу реального времени RTP/RTSP по стандарту ONVIF profile S при организации удаленного доступа предоставляется правоохранительным органам на условиях равноправного (согласованного) использования или в

ином порядке, определяемом принципами межведомственного взаимодействия правоохранительных органов.

Предоставление удаленного доступа к фото- и видеоизображениям в режиме реального времени осуществляется при наличии на Объектах каналов передачи данных необходимой пропускной способности.

13.1.2. Требования к организации доступа к архивным фото- и видеоматериалам

Доступ к архивным фото-, видеоизображениям реализуется:

1) непосредственно на Объекте, путем установки оборудования отображения информации (АРМ, монитор), позволяющего получать регламентированный доступ к архивным фото- и видеоизображениям;

2) удаленно, путем подключения к видеорегистратору (серверу видеонаблюдения), поддерживающему стандарт ONVIF profile G и/или необходимый программный интерфейс (API).

Удаленный доступ к архивным фото- и видеоизображениям организуется только для целей:

1) передачи видеопотоков от видеорегистратора (сервера видеонаблюдения) в интересах правоохранительных органов;

2) мониторинга работоспособности КВ и СВН на Объектах в целом;

3) передачи видеопотоков в информационные системы (программное обеспечение), используемые уполномоченным учреждением.

Приоритетный доступ к архивным фото- и видеоизображениям при организации удаленного доступа предоставляется правоохранительным органам на условиях равноправного (согласованного) использования или в ином порядке, определяемом принципами межведомственного взаимодействия правоохранительных органов.

Выгрузка (копирование) архивных фото- и видеоматериалов непосредственно с Объекта (при отсутствии каналов передачи данных либо при неработоспособности каналов передачи данных) осуществляется

уполномоченным учреждением в течение 72 часов с даты регистрации соответствующего обращения правоохранительных органов.

Предоставление удаленного доступа к архивным фото- и видеоматериалам осуществляется при наличии на Объектах каналов передачи данных необходимой пропускной способности.

13.2. Требования к доступу к информации о состоянии АПС и СОУЭ

Информация о состоянии АПС и СОУЭ представляет собой актуальные на дату представления акт работоспособности АПС и СОУЭ, записи в журналах технического обслуживания и ремонта АПС и СОУЭ. Акт работоспособности АПС и СОУЭ представляется по первому требованию контрольных (надзорных) органов и иным органам в соответствии с их полномочиями в течение 7 суток с даты поступления соответствующего письменного запроса.

Объекты, если иное не установлено МК или организационно-распорядительным документом Исполнительного комитета г.Казани, обеспечивают наличие на Объекте актуального акта работоспособности АПС и СОУЭ, надлежащее заполнение журналов технического обслуживания и ремонта АПС и СОУЭ.

Администрациями Объектов принимаются все необходимые меры по ограничению несанкционированного доступа к документам, касающимся состояния АПС и СОУЭ.

13.3. Требования к доступу к информации о состоянии СКУД

Информация о состоянии СКУД представляет собой актуальные на дату представления акт работоспособности СКУД, записи в журналах технического обслуживания и ремонта СКУД. Акт работоспособности СКУД представляется по первому требованию контрольных (надзорных) органов и иным органам в соответствии с их полномочиями.

Объекты, если иное не установлено МК или организационно-распорядительным документом Исполнительного комитета г.Казани, обеспечивают наличие на Объекте актуального акта работоспособности СКУД, надлежащее заполнение журналов.

Администрациями Объектов принимаются все необходимые меры по ограничению несанкционированного доступа к документам, касающимся состояния СКУД.

Информация о времени, дате и идентификаторах карт (ключей) доступа, журнал доступа на Объект представляется по первому требованию контрольных (надзорных) органов и иным органам в соответствии с их полномочиями в течение 7 суток с даты поступления соответствующего письменного запроса при наличии соответствующей технической возможности.

Представление информации о времени, дате и идентификаторах карт (ключей) доступа, журнал доступа на Объект физическим и юридическим лицам, в том числе являющимся посетителями Объекта, не допускается, если иное не установлено организационно-распорядительным документом Исполнительного комитета г.Казани.

13.4. Требования к доступу к информации о состоянии КООПИ

Информация о состоянии КООПИ представляет собой актуальные на дату представления акт работоспособности КООПИ, записи в журналах технического обслуживания и ремонта КООПИ. Акт работоспособности КООПИ представляется по первому требованию контрольных (надзорных) органов и иным органам в соответствии с их полномочиями в течение 7 суток с даты поступления соответствующего письменного запроса.

Объекты, если иное не установлено МК или организационно-распорядительным документом Исполнительного комитета г.Казани, обеспечивают наличие на Объекте актуального акта работоспособности КООПИ, надлежащее заполнение журналов технического обслуживания и ремонта КООПИ.

Администрациями объектов принимаются все необходимые меры по ограничению несанкционированного доступа к документам, касающимся состояния КООПИ.

13.5. Требования к доступу к информации о состоянии ТСО

Информация о состоянии ТСО представляет собой актуальные на дату представления акт работоспособности ТСО, записи в журналах технического обслуживания и ремонта ТСО. Акт работоспособности ТСО представляется по первому требованию контрольных (надзорных) органов и иным органам в соответствии с их полномочиями в течение 7 суток с даты поступления соответствующего письменного запроса.

Объекты, если иное не установлено МК или организационно-распорядительным документом Исполнительного комитета г.Казани, обеспечивают наличие на Объекте актуального акта работоспособности ТСО, надлежащее заполнение журналов технического обслуживания и ремонта ТСО.

Администрациями Объектов принимаются все необходимые меры по ограничению несанкционированного доступа к документам, касающимся состояния ТСО.

13.6. Требования к доступу к информации о состоянии СКМ

Информация о состоянии СКМ представляет собой актуальные на дату представления акт работоспособности СКМ, записи в журналах технического обслуживания и ремонта СКМ. Акт работоспособности СКМ представляется по первому требованию контрольных (надзорных) органов и иным органам в соответствии с их полномочиями в течение 7 суток с даты поступления соответствующего письменного запроса.

Объекты, если иное не установлено МК или организационно-распорядительным документом Исполнительного комитета г.Казани, обеспечивают наличие на Объекте актуального акта работоспособности СКМ, надлежащее заполнение журналов технического обслуживания и ремонта СКМ.

Администрациями Объектов принимаются все необходимые меры по ограничению несанкционированного доступа к документам, касающимся состояния СКМ.

13.7. Требования к доступу к информации о ТКИ

Информация об аппаратно-программной реализации ТКИ, практической реализации построения ТКИ является строго конфиденциальной. Информация о ТКИ представляется по первому требованию контрольных (надзорных) органов и иным органам в соответствии с их полномочиями в течение 7 суток с даты поступления соответствующего письменного запроса.

XIV. Требования к защите, восстановлению СОБ при проведении текущего и капитального ремонта объектов

При планировании текущего (капитального) ремонта Объект за 30 календарных дней до плановой даты начала работ надлежащим образом информирует уполномоченное учреждение о необходимости проведения мероприятий по защите (укрытию, демонтажу, консервации) СОБ. Уполномоченное учреждение на основании информации Объекта принимает все необходимые меры по защите (укрытию, демонтажу, консервации) СОБ с передачей под акт организации, производящей работы на Объекте.

Восстановление работоспособности СОБ до исходного состояния осуществляется организацией, производящей работы на Объекте, с последующей сдачей под акт уполномоченному учреждению.

В случае если Объект не уведомил уполномоченное учреждение или уведомил с нарушением срока, установленного настоящим разделом, то такой Объект несет полную ответственность за состояние СОБ, самостоятельно обеспечивает защиту (укрытие, демонтаж, консервацию) СОБ и последующее восстановление работоспособности СОБ.

_____