задание ЗАКАЗЧИКА

**«Система КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ»**

**Приложение №1 к Техническому заданию**

Объект: АО «Петербургская сбытовая компания»

Санкт-Петербург  
2023 г.

оглавление

1 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ 3

1.1 НАЗНАЧЕНИЕ СИСТЕМЫ 3

1.2 ЦЕЛЬ СОЗДАНИЯ СИСТЕМЫ 4

2 ХАРАКТЕРИСТИКИ ОБЪЕКТА 4

3 ТРЕБОВАНИЯ К СИСТЕМЕ 4

3.1 ТРЕБОВАНИЯ К СТРУКТУРЕ И ФУНКЦИОНИРОВАНИЮ СИСТЕМЫ 4

3.1.1 КОМПОНЕНТЫ СИСТЕМЫ 4

3.1.2 Требования к программному обеспечению. 7

3.1.3 Требования к базе данных программного обеспечения 8

3.1.4 Требования к интеграции программного обеспечения 9

3.1.5 Требования к интерактивной карте 9

3.1.6 Требования к протоколированию событий 11

3.1.7 Требования к удалённым рабочим местам 11

3.1.8 ТРЕБОВАНИЯ К СПОСОБАМ И СРЕДСТВАМ СВЯЗИ МЕЖДУ КОМПОНЕНТАМИ СИСТЕМЫ 12

3.1.9 ТРЕБОВАНИЯ К СОВМЕСТИМОСТИ С ДРУГИМИ СИСТЕМАМИ 13

3.2 ТРЕБОВАНИЯ К РЕЖИМАМ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ 13

3.2.1 ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ 13

3.3 ТРЕБОВАНИЯ К ЧИСЛЕННОСТИ ПЕРСОНАЛА 13

3.4 ПОКАЗАТЕЛИ НАЗНАЧЕНИЯ 14

3.5 ТРЕБОВАНИЯ К НАДЁЖНОСТИ 15

3.6 ТРЕБОВАНИЯ к БЕЗОПАСНОСТИ 15

3.7 ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ 16

4 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ 17

5 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ 18

6 ИСТОЧНИКИ РАЗРАБОТКИ 18

7 особые условия 19

# НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

## НАЗНАЧЕНИЕ СИСТЕМЫ

СКУД предназначена для обеспечения санкционированного доступа на территорию защищаемого объекта в соответствии с заданными алгоритмами и формирования сигналов тревоги при попытках несанкционированного доступа, а также предоставления информации о состоянии точек доступа и пользователях системы.

СКУД должна обеспечивать:

* защиту от несанкционированного доступа на охраняемый объект (помещение, зону);
* контроль и учет доступа персонала и посетителей на охраняемом объекте (помещение, зоне);
* исключение возможности двойного прохода в здание (использование одной карты дважды в одном направлении);
* возможность использования в качестве дополнительного условия доступа показателя температуры тела человека и показателя промилле от алкотестера;
* совместную работу с системой домофонной связи;
* возможность учета автотранспорта контроля его доступа на прилегающую территорию;
* защиту от несанкционированного проникновения в помещения с установленным оборудованием систем жизнеобеспечения здания;
* возможность учёта рабочего времени сотрудников и посетителей с возможностью формирования отчётов;
* возможность выдачи ключей от помещений в соответствие с предоставленными идентификационными признаками;
* работу в составе с любыми исполнительными устройствами (замки, защёлки и т. д.);
* работу в составе с любыми преграждающими и управляемыми устройствами (турникеты, шлагбаумы, ворота, шлюзовые кабины и т.д.);
* работу с картоприёмниками;
* наличие у считывающих устройств световой и звуковой индикации;
* возможность фото- и видеоверификации при разрешении/отклонении доступа на охраняемый объект (помещение, зону);
* возможность использования автомобильного номера в качестве дополнительного идентификатора при разрешении доступа автотранспорта на прилегающую территорию;
* отображение на интерактивных планах всех состояний системы;
* управление системой на рабочих местах с помощью интерактивной карты:
* гибкое взаимодействие с видеоподсистемой;
* разблокирование точек доступа, установленных на путях эвакуации, по сигналам АУПС;
* возможность блокирование точек доступа по сигналам СОТС;
* формирование и ведение протоколов событий на жестких дисках;
* распечатку протоколов из архива событий.

## ЦЕЛЬ СОЗДАНИЯ СИСТЕМЫ

Основной целью создания системы контроля и управления доступом является защита людей от возможных попыток террористических угроз, защита от возможных попыток хищения имущества, а также предотвращение несанкционированного доступа на территорию объекта.

# ХАРАКТЕРИСТИКИ ОБЪЕКТА

Объект представляет собой офисные здания капитальной постройки в соответствии с Приложением №1 к настоящему техническому заданию. Непосредственные характеристики зданий и помещений уточняются на этапе проектно-изыскательских работ.

# ТРЕБОВАНИЯ К СИСТЕМЕ

## ТРЕБОВАНИЯ К СТРУКТУРЕ И ФУНКЦИОНИРОВАНИЮ СИСТЕМЫ

### КОМПОНЕНТЫ СИСТЕМЫ

СКУД должна состоять из следующих компонентов:

* контроллеры доступа;
* считывающие устройства;
* исполнительные устройства;
* устройства, преграждающие управляемые;
* электронные устройства для хранения, выдачи и учёта ключей;
* идентификаторы;
* программное обеспечение для сбора, хранения и обработки информации, поступающей от аппаратной части.

Общие требования к контроллерам доступа:

* отечественная продукция;
* поддержка следующих интерфейсов связи со считывателя: Wiegand -26\37\44\52\58, R-bus, а также иметь возможность прямого подключения других устройств идентификации по интерфейсу PS/2 (KBW, “В разрыв клавиатуры”), RS-232 количество подключаемых считывателей: не менее 2 шт.;
* количество выход реле: не менее 8 шт.;
* количество входов охранной сигнализации: не менее 1 шт.;
* не менее 4х раздельных каналов питания нагрузок с индивидуальными электронными защитами от перегрузки.;
* энергонезависимая память контроллера с количеством ключей – до 1 000 000, с количеством событий – до 60 000;
* длина кода ключа, хранящаяся в контроллере, должна быть не менее 6 Байт;
* поддержка режимов различных идентификации: ключ, ключ +ПИН, ключ с подтверждением ключом, ключ с подтверждением внешним разрешением, лицо, ключ или лицо, ключ и лицо;
* возможность развития функционала прошивки контроллера под требования Заказчика;
* совместимость контроллеров с разными версиями прошивок;
* возможность удаленного обновления прошивок контроллеров;
* контроллеры доступа должны быть универсальными и поддерживать сразу несколько типов точек доступа (выбор типа точки доступа осуществляется настройкой контроллера): дверь, две двери, турникет с картоприемником, ворота/шлагбаум с картоприемником + управление светофорами;
* непрерывный мониторинг следующих параметров: отсутствие напряжения 220 В на блоке питания, низкий заряд батареи, вскрытие корпуса контроллера;
* система электропитания нагрузок, подключенных к контроллеру СКУД, должна обеспечивать защитное отключение подключенных нагрузок при перегрузках и коротких замыканиях в их цепях, а также аварийное ручное отключение и автоматическое восстановление электропитания после устранения причины неисправности. Сработка механизмов защитного отключения не должна приводить к отключению самого контроллера. Контроллер должен обеспечить передачу на сервер в режиме реального времени информации о неисправном канале питания, а также информации о восстановлении его работы в дежурный режим;
* Контроллеры должны обеспечивать возможность одновременного соединения их между собой по двухпроводному интерфейсу CAN-HS и прямого подключения к серверу по интерфейсу Ethernet;
* все входы и выходы контроллера должны быть свободно программируемыми и настраиваемыми посредством управляющего ПО;
* хранения всех ключей, режимов доступа, событий в энергонезависимой памяти контроллера. Независимо от наличия или отсутствия связи с сервером системы, контроллер должен принимать решение о разрешении/запрете доступа самостоятельно, на основании автономной базы ключей и режимов доступа. Произошедшее событие должны регистрироваться в энергонезависимой памяти контроллера, с указанием даты и времени встроенных часов реального времени. Автономный режим работы контроллеров должен обеспечивать возможность двухфакторной идентификации. При наличии связи с сервером события автоматически должны передаваться в базу данных СКУД на сервере;
* контроллеры должны аппаратно поддерживать режим Глобального (в сети из нескольких контроллеров) AntiPassBack без участия сервера;
* контроллеры должны иметь дополнительные входы для подключения охранных датчиков, а также дополнительные выходы для управления внешними цепями;
* интеграция с программным обеспечением для сбора и обработки информации по протоколам высокого и низкого уровней;
* гарантия производителя на контроллеры должна быть не менее 18 мес.;

Считывающие устройства должны поддерживать технологию бесконтактного считывания RFID. Допускается использовать устройства ближней идентификации, работающих на частотах 125 кГц или 13,56 МГц. Также считыватели должны отвечать следующим требованиям:

* отечественная продукция;
* одновременная поддержка следующих типов идентификаторов: NFC / BLE, EM-Marin, HID Prox II, Temic, Cotag, Indala, Mifare: ID / Ultralight / Classic / Plus / DesFire, банковских / транспортных карт;
* обеспечивать дополнительную защиту от копирования карт, неправильного включения;
* дополнительные сервисные возможности: Micro-USB для прошивки, конфигурирования, управления базой ключей, сервис заказных прошивок, возможность изменения логики работы в зависимости от задач Заказчика путем смены внутренней программы через Micro-USB;
* обеспечение зашиты от механических ударов по ГОСТ IEC 62262-2015 не хуже IK07;
* степень защиты корпуса по ГОСТ 14254-2015 (IEC 60529:2013) не ниже IP67;
* диапазон рабочих температур от -60°С до +60°С;

Предусмотреть настольный считыватель для работы следующими типов идентификаторов: NFC / BLE, EM-Marin, HID Prox II, Temic, Cotag, Indala, Mifare: ID / Ultralight / Classic / Plus / DesFire, банковскими / транспортными картами;

* гарантия производителя на считыватели должна быть не менее 18 мес.;

В качестве средств сбора и обработки информации должны применяться модульная компьютерная клиент-серверная архитектура с необходимым программным обеспечением, установленным на рабочих местах. Общие требования к программной части:

* неограниченные возможности масштабирования, адаптации к специфике решаемых задач, перераспределения используемых ресурсов при изменении количества или качества задач по мониторингу состояния подконтрольных объектов и управления различного рода оборудованием, возможность маршрутизировать события внутри системы;
* отсутствие ограничений по количеству пользователей в системе, количества рабочих мест оператора, количества контроллеров, используемых в единой системе;
* использование многоуровневой интерактивной карты подконтрольного объекта, обеспечивающей реализацию следующих функций: автопереключение и рекурсивный поиск связей на карте; использование на карте активных символов устройств с возможностью управления устройствами из контекстного функционального меню;
* возможность самостоятельного создания любых сценариев работы системы с помощью макрокоманд, макрособытий и скриптов
* глубокая интеграция различных технических средств охраны: видео, ОПС, средства охраны периметра, и т. д.
* платформа должна быть открытой для внешней интеграции с использованием SDK позволяющим полностью управлять всеми элементами подсистемы, получать события и отсылать команды (реакции).
* должна быть предусмотрена возможность использования мобильного приложения.

Центральный сервер должен иметь единую базу данных аппаратных и программных компонентов, а также осуществлять взаимодействие всех рабочих мест системы. Программная часть должна включать следующие программные модули:

* бюро пропусков;
* учет рабочего времени;
* диспетчер событий «Фотоидентификация»;
* лицензия подключения контроллеров.

Система должна предусматривать возможность организации отдельных рабочих мест для администрирования системы, а также нескольких рабочих мест операторов системы (количество согласовывается с Заказчиком).

### Требования к программному обеспечению.

ПО СКУД должно иметь клиент-серверную архитектуру. Для организации УРММ система должна позволять:

* создавать любое количество одновременно работающих клиентских мест;
* удаленное управление контроллерами и точками доступа с клиентского места;
* разграничивать права пользователя по отделам и точкам доступа;
* для каждого из пользователей задавать определенный набор доступных для него операций, которые он может выполнять в рамках системы;
* для ограничения доступа в ПО СКУД должны использоваться гибкие режимы доступа, которые используются системой для принятия решения о возможности прохода объекта доступа относительно направления прохода и времени прохода;
* для учета рабочего времени ПО СКУД должно позволять организовать автоматический подсчет рабочего времени сотрудников, а также обеспечить:
* возможность просматривать кадровую структуру организации по отделам и получать информацию по каждому сотруднику;
* возможность формировать графики и схемы работы с различными периодами и назначать их индивидуально каждому сотруднику или отделу в целом;
* возможность вести учет оправдательных и сверхурочных документов;
* возможность производить расчет суммарного отработанного времени каждого сотрудника и представлять результаты в табличной форме;
* возможность составлять отчёт по суммарному отработанному времени сотрудников;
* следующий функционал: задание свойств сотрудников, создание периодов работы, создание схем работы, создание графиков работы, назначение праздничных дней, настройка начала и окончания ночи, назначение графиков работы отделам;

поддержку различных графиков: недельный (рабочую пятидневку); сменный (например, сутки через двое); месячный (например, когда рабочими являются четные дни месяца); скользящий: сотрудник должен отработать несколько часов в определенное время (например, 8 часов в интервале с 8:00 до 22:00).

* ПО СКУД должно иметь систему web-отчетов, позволяющую:
* формировать и экспортировать отчёты по протоколу событий, а также просматривать видеоархив со времени регистрации выбранного в отчёте события;
* формировать и экспортировать отчёты по протоколу изменений;
* формировать и экспортировать сводные и детальные отчёты по учету рабочего времени;
* формировать и экспортировать отчёты по количеству посетителей наблюдаемого объекта;
* настраивать дифференцированный доступ пользователей к отчётам;
* иметь возможность создавать файлы отчетов автоматически по расписанию с последующим сохранением на локальном компьютере и/или их отправкой по электронной почте;
* формировать отчет по суммарному отработанному времени сотрудников подразделений в Унифицированной форме №T-12/T-13, утвержденной постановлением Госкомстата России, с возможностью дальнейшей печати и редактирования;
* поддерживать следующие форматы сохранения отчетов: MS Word, MS Excel, PDF;
* ПО СКУД должно обеспечивать возможность подключения удалённых рабочих мест операторов через сеть Ethernet;
* ПО СКУД должно поддерживать работу с любыми видеокамерами для фотографирования сотрудников и посетителей;
* ПО СКУД должно поддерживать полную интеграцию с видеоподсистемой «Интеллект» для максимальной информативности работы в онлайн и офлайн режимах (аналитика и разбор инцидентов);
* ПО СКУД должно поддерживать функционал автоматического сканирования и распознавания документов (паспорт РФ, загран. паспорт, водительское удостоверение);
* механизм создания реакций с возможностью настройки действий: запуск внешнего приложения\скрипта, отправка SMS, отправка Email;

### Требования к базе данных программного обеспечения

База данных программного обеспечения должна выполнять следующие функции:

* сохранение данных о зарегистрированных системных объектах и параметрах их настройки;
* сохранение данных об учётных записях отделов, пользователей и прав пользователей;
* сохранение данных о зарегистрированных в системе событиях;
* сохранение данных об изменениях аппаратно-программной конфигурации;
* сохранение данных об изменениях перечня зарегистрированных системных объектов и параметров их настройки;
* сохранение данных о сетевых именах и IP-адресах компонентов и параметрах взаимодействия между ними;
* репликацию данных, хранящихся на различных компонентах системы;
* синхронизация базы данных серверных компонентов (синхронизация баз данных должна позволять хранить данные как централизованно (на одном серверном компоненте), так и распределено (репликация данных из баз различных серверных компонентов ИСБ).
* синхронизация баз данных должна обеспечивать параллельную работу с базами данных серверных компонентов и автоматическое обновление при их изменении.

### Требования к интеграции программного обеспечения

Интеграция ПО СКУД должна обеспечиваться посредством информационного обмена между программными ядрами. Центральным программным компонентом системы должно являться полнофункциональное программное ядро. С программным ядром системы должны взаимодействовать функциональные модули, являющиеся программной основой функциональных подсистем. Функциональные (программные) модули должны осуществлять непосредственное взаимодействие с аппаратными средствами, а также должны служить источником информации о состоянии подконтрольных объектов. Программное ядро подсистемы должно обрабатывать информацию, поступающую от различных функциональных модулей, и должны обеспечивать их интеграцию.

Исполнительные файлы, соответствующие функциональным подсистемам, должны запускаться ядром автоматически по мере конфигурирования СКУД.

Для упрощения процесса интеграции со смежными информационными системами, дополнительным программным обеспечением или функциональными модулями расширения в программном обеспечении должен быть разработан альтернативный интерфейс информационного обмена функциональных модулей с программным ядром – SDK. Должен быть доступен элемент управления ActiveX, являющийся полным аналогом интерфейсного объекта «монитор»и позволяющий управлять камерами, просматривать архив и использовать все функции монитора видеонаблюдения. Должен быть предоставлен программный интерфейс HTTP API, позволяющий отправлять команды и получать данные от СКУД при помощи HTTP-запросов.

### Требования к интерактивной карте

СКУД должна иметь возможность создания интерактивной карты защищаемого объекта. Интерактивная карта должна позволять использовать навигацию между компонентами подсистемы видеонаблюдения с использованием графических планов (схем) подконтрольных территорий. Интерактивная карта должна допускать управление объектами подсистемы из контекстных функциональных меню графических символов (значков) устройств, размещённых на карте, отображающих (индицирующих) состояние соответствующих системных объектов.

Интерактивная карта должна обладать следующими функциональными возможностями:

* представление объекта на карте в одном из следующих видов:
* изображение в формате .bmp, .jpg, .png;
* изображение в формате .bmp, .jpg, .png и индикатор;
* изображение в формате .svg (векторный формат);
* текст;
* линия;
* многоугольник с количеством вершин до 51;
* эллипс.
* добавление нескольких значков одного объекта разного вида на один или несколько слоёв интерактивной карты;
* использование набора планов (слоев), представляющих собой фотографии, карты, графические схемы, рисунки в формате bmp., при этом не должны накладываться ограничения на размер и разрешение используемых рисунков;
* задание цвета подложки, в том числе в случае, когда рисунок слоя не выбран;
* при использовании многослойных интерактивных карт – возможность установки правила перехода на слои, содержащие объекты, на которых был зарегистрирован сигнал «Тревога», а также на любые слои, в том числе предыдущий;
* наличие следующих механизмов поиска слоя, с объекта которого поступает тревожный сигнал:
* вывод окна интерактивной карты поверх всех активных интерфейсных окон при регистрации события «Тревога» на объектах, соответствующих символам, размещённым на слое, с отображением соответствующих слоя и символа;
* осуществление рекурсивного поиска слоя, с объектов которого поступает тревожный сигнал;
* подпись к объекту при размещении его на слое карты должна содержать идентификатор объекта после названия или перед ним;
* отключение отображения идентификатора объекта в подписи на карте;
* выбор местоположения подписи относительно значка объекта: сверху, снизу, слева, справа, отсутствует;
* при использовании многослойных интерактивных карт – возможность настраивать механизм перехода с текущего слоя на заданные слои как той же карты, так и других карт в системе (связи со слоем);
* если объект находится в нескольких состояниях, эти состояния должны отображаться на карте посредством последовательной смены изображения или цвета значка объекта;
* при выделении значка объекта справа от него должны отображаться уменьшенные значки всех его состояний;
* отключение отображения уменьшенных значков состояний объектов;
* задание порядка отображения объектов на карте при наложении их изображений друг на друга;
* отображение заданного количества последних событий выбранного объекта в окне Интерактивной карты;
* привязка координат карты к географическим координатам;
* отображение миникарты слоя для упрощения навигации по слою карты;
* возможность открыть/закрыть проход через точку доступа, удерживать дверь в разблокированном состоянии, разрешить доступ с подтверждением оператора; отображение изображения с камеры, наблюдающей за проходом, после нажатия на значок выбранной камеры на карте; автоматическое отображение камеры или нескольких камер, назначенных для выбранного прохода после нажатия значка двери на интерактивной карте;

### Требования к протоколированию событий

В подсистеме СКУД должно вестись протоколирование зарегистрированных событий. Протоколирование должна обладать следующими функциональными возможностями:

* вывод протокола событий на экран в интерфейсном окне;
* выбор в протоколе событий типа объекта, для которого может быть зарегистрировано требуемое событие;
* по умолчанию если ни один тип объекта администратором не задан, то в протокол событий должны записываться все события по всем объектам подсистемы;
* интерфейсное окно протокола событий должно предоставлять возможность просмотра архивных видеозаписей из списка сообщений;
* при выборе объекта в проколе событий – просмотр данного объекта подсистемы в интерактивной карте защищаемого объекта;
* создание печатной формы отчёта о событиях;
* задание срока хранения архива событий в базе данных протокола событий;
* фильтрация списка событий с использованием заранее настроенных фильтров;
* наличие специализированного протокола событий, предназначенного для оператора, с реализацией следующих функций:
* отображение в интерфейсном окне событий, зарегистрированных объектами подсистемы;
* присваивание статуса (типа) зарегистрированному событию (не менее трёх типов);
* добавление комментария к событию;
* запись событий в архив;
* поиск событий в архиве;
* просмотр видеозаписи события;
* возможность однократно отложить обработку события на заданный период;
* эскалация событий в интерфейс вышестоящего лица;
* генерация событий указанного типа;
* построение отчётов по фактам обработки событий операторами;
* построение отчётов по зарегистрированным событиям;
* определение положения объекта-источника события на карте;
* подтверждение присвоения типа событию паролём;
* сортировка событий по приоритету или времени поступления.

### Требования к удалённым рабочим местам

Клиентское рабочее место должно быть предназначено для использования в качестве рабочих мест операторов и должно реализовывать функции удалённого наблюдения за событиями в системе, контроля состояния тревожных входов, управления исполнительными устройствами и др.

В СКУД должна производиться регистрация следующих категорий пользователей:

* администратор;
* оператор, опционально наделённый правами на администрирование, управление и мониторинг.

Требования к основным интерфейсам рабочих мест (оператора, администрирования):

* древовидная структура расположения объектов (дерево объектов) – многоуровневый вложенный список объектов;
* иерархия объектов – младший в иерархии (дочерний) объект должен быть создан только на базе старшего (родительского объекта);
* возможность отображать дерево объектов в развёрнутом виде, раскрывая и просматривая содержимое всех его групп (ветвей), свёртывать снова, скрывая ненужные для наблюдения в данный момент объекты;
* наличие функции, позволяющей передать ключ активации, регламентирующий конфигурацию системы, на все компьютеры, входящие в систему СКУД;
* поддержка функции создания резервной копии баз данных;
* наличие утилиты, предназначенной для редактирования шаблонов баз данных и файлов внешних настроек;
* наличие утилиты, предназначенной для создания диалоговых окон пользователя;
* наличие утилиты, предназначенной для конвертирования, выбора шаблона и создания резервных копий баз данных;
* наличие утилиты, предназначенной для назначения экранов компьютерам в распределённой системе.

### ТРЕБОВАНИЯ К СПОСОБАМ И СРЕДСТВАМ СВЯЗИ МЕЖДУ КОМПОНЕНТАМИ СИСТЕМЫ

Связь между контроллерами и считывателями должна осуществляться по интерфейсу Wiegand -26\37\44\52\58, R-bus, а также иметь возможность прямого подключения других устройств идентификации по интерфейсу PS/2 (KBW, “В разрыв клавиатуры”), RS-232. Тип интерфейса и способы подключения согласовываются с Заказчиком.

Связь между контроллерами и программным обеспечением для сбора и обработки информации должна осуществляться с использованием изолированного участка Ethernet-сети, развёрнутой на объекте, по протоколу TCP/IP.

Связь между рабочими местами и центральным сервером должна осуществляться по протоколу TCP/IP с использованием изолированного участка Ethernet-сети, развёрнутой на объекте.

В качестве среды передачи данных должны использоваться провода с медными жилами, оптоволоконные кабели.

Взаимодействие между серверами, УРМА (удалённое рабочее место администрирования), УРММ (удалённое рабочее место мониторинга) должно включать в себя репликацию баз данных (только для серверов и УРМА) и обмен событиями. Настройка взаимодействия компонентов системы должна выполняться с сервера администрирования или, при наличии выделенных подсетей, с узлового сервера или УРМА.

Для каждого компонента СКУД необходимо обеспечить возможность задания списка компонентов, с которыми он осуществляет обмен данными о параметрах конфигурации системы. Для каждого компонента СКУД необходимо обеспечить возможность задания IP-адресов других компонентов СКУД, с которыми требуется осуществлять обмен параметрами конфигурации и событиями.

Для каждого компонента СКУД необходимо обеспечить возможность задания списка компонентов, с которыми он осуществляет обмен событиями.

### ТРЕБОВАНИЯ К СОВМЕСТИМОСТИ С ДРУГИМИ СИСТЕМАМИ

В СКУД должна быть предусмотрена интеграция со следующими смежными системами:

* системой видеонаблюдения «Интеллект» по высокоуровневому протоколу (софт-софт): должно обеспечиваться:
* настройка записи видеокамер на заданное событие в системе, настройка работы поворотной камеры по предварительным настройкам (перевод камер в preset), возможность быстрого перехода по событию к связанной с ним записи видеоархива;
* системой домофонной связи с помощью дискретных выходов;
* системой пожарной сигнализации с помощью дискретных выходов;
* системой охранной сигнализации с помощью дискретных выходов;

Тип дискретных выходов (NC или NO) выбирается на основании технических условий предоставленных разработчиками смежных систем.

### ТРЕБОВАНИЯ К РЕЖИМАМ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ

СКУД должна функционировать в непрерывном круглосуточном режиме (с учетом проведения регламентного технического обслуживания).

### ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ

СКУД должна иметь длительный жизненный цикл. Для поддержания соответствия характеристик актуальным требованиям на протяжении всего периода эксплуатации, при разработке СКУД необходимо обеспечить возможность её модернизации в процессе эксплуатации за счёт выбора соответствующей архитектуры программного обеспечения и технических средств, а также за счёт использования стандартизованных и эффективно сопровождаемых решений.

## ТРЕБОВАНИЯ К ЧИСЛЕННОСТИ ПЕРСОНАЛА

Персонал СКУД должен включать следующие категории специалистов:

* пользователи, выполняющие функции администрирования системы;
* операторы системы, выполняющие функции наблюдения и управления системой;
* обслуживающий персонал, обеспечивающий сервисную поддержку работы СКУД.

Администратор должен обладать правами администрирования всех компонентов ИСБ в полном объёме. Оператором должен считаться зарегистрированный в системе пользователь, которому могут быть предоставлены права на администрирование, управление и/или мониторинг отдельных компонентов подсистем.

Регистрация Оператора должна выполняться путём создания учётной записи пользователя и предоставления данному пользователю прав и полномочий на администрирование, управление и/или мониторинг. При регистрации Оператору должен назначаться пароль, используемый для авторизации при запуске и завершении работы программного обеспечения. Дополнительно должна иметься возможность запрета на завершение работы Оператора с программным обеспечением.

Для Администратора не должна создаваться учётная запись, по паролю администратора системы не должна быть выполнена авторизация при запуске программного обеспечения. Пароль Администратора должен использоваться только для получения доступа к диалоговому окну настройки системы, панелям настройки системных объектов, функциям изменения авторизированного пользователя и завершения работы с программным обеспечением.

Учётные записи пользователей должны регистрироваться в программном обеспечении путём создания системных объектов «Пользователь». Для каждого Оператора должна создаваться индивидуальная учётная запись, в которую в дальнейшем должны добавляться сведения о назначенных правах и заданном для авторизации в программном обеспечении пароле. Должна иметься возможность задавать фамилию, имя и отчество Оператора в различных полях. Полные Ф.И.О. Оператора должны отображаться в дереве системных объектов «Пользователь».

Учётная запись Оператора помимо прав и пароля должна содержать информацию о подразделении предприятия, сотрудником которого является Оператор. Учётные записи подразделений должны регистрироваться в программном обеспечении путём создания системных объектов «Отдел». Объекты «Отдел» и «Пользователь» должны обеспечивать двухуровневую иерархическую структуру учётных записей.

Группа функций администрирования должна включать в себя следующие функции:

* создание и удаление системных объектов;
* редактирование параметров настройки системных объектов;
* перемещения системных объектов по дереву объектов.

По умолчанию Оператору должно быть полностью запрещено использование функций администрирования, но должно быть полностью разрешено использование функций управления и мониторинга на всех объектах, для которых предусмотрены данные функции. Должна иметься возможность запретить Оператору администрирование одного или нескольких объектов, ограничить перечень доступных функций управления объектами, а также ограничить возможности по мониторингу. При предоставлении Оператору прав на администрирование отдельного системного объекта должно выполняться условие — одновременно Оператору предоставляются права на управление и мониторинг по данному объекту.

Право на использование функций управления должно давать возможность использования функциональных интерфейсных кнопок, команд из функциональных меню и прочих средств управления объектами, для которых предусмотрено использование данных функций (дверьми, турникетами, видеокамерами, протоколом событий и т.д.).

В СКУД должна быть предусмотрена возможность смены пароля Оператора в следующих случаях:

* по требованию Оператора;
* по истечении срока действия пароля Оператора;
* при первом входе Оператора в систему.

## ПОКАЗАТЕЛИ НАЗНАЧЕНИЯ

СКУД должна отвечать следующим показателям назначения:

* количество и тип точек доступа определяется в соответствие с приложением 1 к данному техническому заданию;
* места, через которые возможен доступ на территорию объекта со стороны внешнего мира, должны быть оснащены двусторонним (считыватель на вход и выход) контролем доступа;
* количество электронных ключей, хранящихся в памяти контроллера: не менее 1 000 000;
* глубина отчетов о событиях в базе данных системы: не менее 6 месяцев;
* количество записей в энергонезависимый буфер событий контроллера (при обрыве связи с центральным сервером): не менее 60 000;
* количество мест оператора системы: не менее 1;
* количество мест администратора системы: не менее 1.

Окончательные значения показателей уточняются в процессе разработки проектной документации и согласовываются протоколом с Заказчиком на стадии разработки рабочей документации.

## ТРЕБОВАНИЯ К НАДЁЖНОСТИ

СКУД должна обеспечивать защиту электрических соединительных цепей от несанкционированных воздействий, приводящих к разблокировке исполнительных устройств.

При размещении оборудования на местах, удовлетворяющих требованиям эксплуатационной документации, СКУД должна обеспечивать необслуживаемое функционирование в круглосуточном режиме с допустимыми перерывами на профилактику и перенастройку, а также простоями в связи с неисправностью не более 48 часов в год, при среднем времени устранения неисправности, вызвавшей простой, не более 4 часов.

При возникновении сбоев между аппаратной частью и программным обеспечением для сбора и обработки информации система должна продолжать локальное функционирование. В данном случае контроллеры доступа должны продолжить выполнять свои функции в соответствии с алгоритмами, заложенными в их локальной базе данных, а после устранения неисправности контроллер должен передать центральному серверу информацию, накопленную в журнале событий, за время отсутствия связи.

При аварийном отключении электропитания СКУД должна переходить на резервный источник электропитания без нарушения функционирования основных компонентов. Расчётное время работы от резервного источника питания должно быть не менее 2 часов.

СКУД должна иметь возможность получать информацию о состояниях основного и резервного источниках питания и отображать её на рабочих местах операторов.

СКУД должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях СКУД должна выдавать пользователю соответствующие аварийные уведомления, после чего возвращаться в рабочее состояние, предшествовавшее неверной команде или некорректному вводу данных.

СКУД должна иметь возможность исключения вмешательства в логику работы системы со стороны операторов путём разграничения прав доступа к функционалу системы.

Гарантийный срок контроллеров должен составлять не менее 7 лет, на считыватели – не менее 5 лет. Гарантийный срок на поставляемые комплектно товары устанавливается в соответствии с предоставленными паспортами производителей на данные товары и гарантиями производителей, но не менее 12 месяцев.

В соответствие с требованиями Федерального закона Российской Федерации от 27 июля 2007 г. №152-ФЗ «О персональных данных» помещение, в котором будет установлен центральный сервер с базой данных, должно быть оборудовано системами охранной сигнализации и контроля доступа.

## ТРЕБОВАНИЯ к БЕЗОПАСНОСТИ

При монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств СКУД должны выполняться меры электробезопасности в соответствии с ПУЭ и «Правилами техники безопасности при эксплуатации электроустановок потребителей».

Устанавливаемое оборудование СКУД должна отвечать требованиям пожарной безопасности по ГОСТ 12.2.007.0-75 «Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности».

Устанавливаемое оборудование СКУД должна быть заземлена в соответствии с требованиями ГОСТ Р 50571.22-2000 «Электроустановки зданий. Часть 7. Требования к специальным электроустановкам. Раздел 707. Заземление оборудования обработки информации».

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

## ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ

Силовое питание всей аппаратуры должно осуществляться централизованно, от сети электроснабжения объекта при отсутствии источников импульсных помех от других потребителей.

Средства СКУД должны работать от однофазной промышленной сети переменного тока напряжением 220В, 50Гц по I категории надёжности электроснабжения. Допускается осуществлять электропитания средств СКУД по III категории надежности электроснабжения. В данном случае резервное питание средств СКУД должно осуществляться от независимого автономного источника питания с резервированием от аккумуляторных батарей.

Электропитание 220В, 50Гц СКУД осуществить от отдельной группы электрощита дежурного освещения, расположенного на объекте.

Контроллер СКУД должен представлять собой законченное устройство в виде печатной платы, помещённой в металлический бокс, который оснащён следующими компонентами:

* сетевой преобразователь на 12В с функцией ИБП;
* датчик открытия дверцы шкафа;
* автоматический выключатель электропитания;
* комплект промаркированных кабелей;
* крепление аккумулятора 7-15А/ч, габариты до 215x280x91,5 мм;

В помещениях, предназначенных для эксплуатации СКУД, должны отсутствовать агрессивные среды.

Оборудование и аппаратура, устанавливаемые в помещениях объекта, должны быть устойчивы к внешним воздействиям по ГОСТ 15150-69 (с изм. 2004 г.) «Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды» для вида климатического исполнения УХЛ категории 4.2.

Нормальными климатическими условиями эксплуатации системы являются:

* температура окружающей среды (20±5)°С;
* относительная влажность окружающего воздуха (60±15)% при атмосфере воздуха (20±5)°С;
* атмосферное давление (101,3±4) кПа (760±30) мм.рт.ст.

СКУД должна сохранять работоспособность при воздействии следующих климатических факторов:

* температура окружающего воздуха от - 40°С до 50°С;
* относительная влажность воздуха от 40% до 80% при температуре 25°С.

Должны обеспечиваться следующие требования к обслуживанию и ремонту СКУД:

* блоки, модули устанавливаемого оборудования должны быть взаимозаменяемыми с аналогичными блоками из ЗИП (холодного резерва) с минимальной настройкой;
* должна быть предусмотрена возможность оперативного ремонта путем замены отказавших узлов и устройств на аналогичные из ЗИП;
* оборудование должно быть размещено таким образом, чтобы обеспечить легкую доступность для проведения оперативного ремонта и замены.

# СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

Стадии разработки и этапы работ, соответствующие ГОСТ 34.601-90, сроки их выполнения, перечень организаций-производителей работ, ответственных за проведение работ по этапам и перечень документов по ГОСТ 34.201-89, предъявляемых после окончания соответствующих стадий и этапов работ, приведены в таблице 1.

Таблица 1

| **Этап работ** | **Продолжит. этапа,**  **р.д.** | **Организации- производители работ** | **Ответственный за проведение работ** | **Документы, предъявляемые по окончанию этапа** |
| --- | --- | --- | --- | --- |
| Разработка и утверждение технического задания. | 2 | АО «ПСК»  <подрядчик> |  | Техническое задание |
| Разработка рабочей документации | 14 | <подрядчик> |  | Комплект рабочей документации |
| Строительно-монтажные работы | 20 | <подрядчик> |  | Акт завершения работ |
| Пусконаладочные работы | 10 | <подрядчик> |  | Акт завершения работ |
| Проведение предварительных испытаний | 3 | <подрядчик> |  | Акт приёмки в опытную эксплуатацию |
| Проведение опытной эксплуатации | 10 | АО «ПСК»  <подрядчик> |  | Акт о завершении опытной эксплуатации и допуске к приёмочным испытаниям |
| Проведение приёмочных испытаний | 2 | АО «ПСК»  <подрядчик> |  | Акт о завершении приёмочных испытаний и допуске в промышленную эксплуатацию. Акт приёма-сдачи работ. |

При проведении экспертизы или согласовании технической документации, разрабатываемой Подрядчиком, на последнего возлагается осуществление технического сопровождения, а также внесение изменений в документацию по обоснованным замечаниям.

# ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Вся документация должна быть передана как в напечатанном виде, так и на электронном носителе (текстовая часть в формате DOC или PDF, графическая часть в формате PDF).

Перечень разрабатываемых Подрядчиком комплектов и видов документов на СКУД в целом приведён в таблице 2.

Таблица 2

| **Стадия (этап) создания СКУД** | **Предъявляемые документы** | **Кол-во экземпляров** |
| --- | --- | --- |
| Техническое задание | Техническое задание |  |
| Рабочая документация | Комплект рабочей документации в составе:   * Пояснительная записка; * Основной комплект рабочих чертежей (общие данные, структурная схема, планы с прокладкой кабельных трасс, принципиальная схема, кабельный журнал); * Прилагаемая документация (спецификация оборудования и материалов, задания на подключение электропитания 220 В, таблицы для начального конфигурирования приборов и устройств СКУД). | 2+1 |

# ИСТОЧНИКИ РАЗРАБОТКИ

Разработка СКУД должна выполняться с учётом следующих документов:

* [Р 064-2017](https://www.normacs.ru/Doclist/doc/12BT5.html) «Методические рекомендации. Выбор и применение технических средств и систем контроля, и управления доступом»;
* СП 132.13330.2011 «Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования»;
* ГОСТ Р 21.101-2020 «Система проектной документации для строительства. Основные требования к проектной и рабочей документации»;
* Федеральный закон от 22 июля 2008 г. №123-ФЗ "Технический регламент о требованиях пожарной безопасности".
* [Постановление Правительства РФ от 16.09.2020 N 1479 "Об утверждении Правил противопожарного режима в Российской Федерации"](http://www.consultant.ru/document/cons_doc_LAW_363263/).

# особые условия

Техническое задание может изменяться и дополняться по согласованию сторон.

|  |  |  |
| --- | --- | --- |
| От Заказчика Руководитель направления по ИТСО | | |
|  |  | Д.В. Артемьев |