

ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ РАЗДЕЛОВ

Автоматизация, диспетчеризация и слаботочные системы

ТРЕБОВАНИЯ К РАЗДЕЛУ Автоматизированные системы управления технологическими процессами (АСУТП)

1. Общие положения

Основной целевой задачей АСУТП АО "Мосводоканал" является обеспечение автоматизированного режима управления технологическими процессами производственных подразделений. Также АСУТП решает задачи контроля, мониторинга, диспетчеризации управления технологическими процессами. АСУТП вместе с системой диспетчерского контроля и управления (SCADA) составляет единую Автоматизированную систему диспетчерского контроля и управления (АСДКУ) АО "Мосводоканал".

Автоматизированная система диспетчерского контроля и управления (АСДКУ) АО "Мосводоканал" охватывает все уровни управления производственным процессом. От пультов местного управления низший уровень- до дистанционного управление технологическими процессами из локальных диспетчерских пунктов средний уровень; и до централизованных диспетчерских систем управления отдельными производственными подразделениями, а также систем водоснабжения и канализации города в целом высший уровень. Все права на АСДКУ принадлежат АО "Мосводоканал" (свидетельство о государственной регистрации №2021618851). АСДКУ используется исключительно как внутренняя система для служебного использования сотрудниками Общества. Интеграция с внешними и сторонними системами производится в соответствии с действующими требованиями и регламентами АО "Мосводоканал".

Разработка, проектирование и внедрение системы автоматизированного управления технологическими процессами ОА «Мосводоканал» канализация и водопровода, выполняются в строгом соответствии ГОСТ, СНиП, РД и утвержденной нормативной документации ОА «Мосводоканал» ", размещенной на сайте Общества в разделе "Техническим специалистам» >> "Технические требования".

Перед началом работ проектная организация в обязательном порядке запрашивает, согласовывает техническое задание на проектирование. Только после утверждения ТЗ ответственными лицами ОА «Мосводоканал» проектная организация приступает к проектированию.

АО «Мосводоканал» оставляет за собой право проверять ход работ, дополнять (исключать) в процессе проектирования требования к составу и содержанию проекта.

Требования к составу и содержанию разделов проекта АСУТП определены

разделом №5. «Типовые требования к составу и содержанию проектной и рабочей документации АСУТП" стандарта АО "Мосводоканал"».

"Требования к оформлению технической документации автоматизированной системы управления технологическими процессами АО "Мосводоканал"

(<https://www.mosvodokanal.ru/forexperts/requirements/Требования%20к%20оформлению%20технической%20документации%20АСУТП%20МВК.doc>), которое уточняет и конкретизирует требования ГОСТ 34.601-90 "Автоматизированные системы. Стадии создания", ГОСТ 34.201-89 "Виды, комплектность и обозначение документов при создании автоматизированных систем", и РД 50-34.698-90 "Автоматизированные системы. Требования к содержанию документов" применительно к объектам водоснабжения и канализации.

Проектные организации в своей работе должны руководствоваться нормативными документами, ссылки на которые приведены в требованиях.

Так же к типовым требованиям проектов автоматизации АО «Мосводоканал» относятся требования по автоматизации режима управления технологическими процессами с последующей реализацией, если иное не оговорено в ТЗ.

АСУТП АО "Мосводоканал" реализует следующие режимы управления технологическими процессами:

- **местный** режим— управление с местного пульта или щита управления, используется в качестве резервного - при проведении ремонтных работ, либо отключении при аварии систем АСУТП;
- **автоматический** режим— основной режим работы, предусматривающий управление от контроллера с заданием режимов управления из диспетчерских пунктов с APM SCADA или посредством сенсорной панели местных органов управления шкафа контроллера;
- **дистанционный** режим — резервный режим работы, предусматривающий телеуправление и контроль работы оборудования для предотвращения аварийных ситуаций при частичном отказе систем АСУТП:

Режим реализуется в зависимости от требований в задании на разработку проекта из диспетчерских пунктов APM SCADA:

- диспетчерского пункта локального объекта/цеха (МДП);
- главного объектового диспетчерского пункта водопроводной станции либо канализационных сооружений (ГДП);
- центрального диспетчерского управления АО "Мосводоканал" (ЦДУ)

В составе работ проекта кроме строительно-монтажных и местных пуско-наладочных работ средств контроля и управления должно быть предусмотрено следующее:

- разработка алгоритмов программного обеспечения и согласование их с Заказчиком (Производственным подразделением и Управлением АСУТП и связи АО "Мосводоканал");
- программирование контроллеров на объектах и наладка всех режимов работы технологических сооружений (на действующих сооружениях по графику согласованному с Заказчиком);
- организация передачи данных на существующий либо проектируемый сервер систем диспетчерского контроля и управления (SCADA);
- организация сбора данных и параметров работы оборудования в базу данных истории технологических процессов, разработка мнемосхем, журналов действий оператора, аварий и работы оборудования, разработка исполнительной документации, разработка инструкций операторов и диспетчеров, а также регламентов эксплуатации систем и другие необходимые работы по обеспечению полной автоматизации управления объектом.

Электроснабжение и заземление систем автоматизации: программируемых контроллеров, шкафов телеуправления, приборов, средства контроля и управления, серверов и АРМ SCADA должно быть предусмотрено в соответствии с **"Требованиями по электроснабжению, электротехническим устройствам и заземлению АО "Мосводоканал"**

(https://www.mosvodokanal.ru/upload/picture_vs_files/tehnicheskim_spetsialistam/tehnic_heskie_trebovaniya_i_reglamentyi/Teh_treb_energосnab.doc).

Шкафы автоматики, контроллеры, приборы и средства контроля и управления должны быть выполнены в защищенном исполнении, степень защиты не ниже IP-55. В зонах возможного затопления – в герметичном исполнении с согласованием у Заказчика места их установки. В процессе проектирования при выборе оборудования, материалов должно учитываться климатическое исполнение, соблюдение температурных и влажностных режимов работы автоматики (кондиционирование/отопление и вентиляция).

Персональные требования к Контроллерам АСУТП описаны во внутреннем регламенте АО «Мосводоканал» **"Требованиям к контроллерам автоматизированной системы управления технологическими процессами АО "Мосводоканал"**

(https://www.mosvodokanal.ru/forexperts/requirements/тектребования_контроллеры.pdf)

Все приборы и средства измерений, применяемые в проектах автоматизации, должны быть оснащены аналоговым выходом 4-20 мА, а также цифровым выходом, определяемым по согласованию с Заказчиком. Управляемые интеллектуальные технические средства автоматизации также должны иметь цифровой интерфейс, определяемый по согласованию с Заказчиком. Все спецификации приборов и средств автоматизации предварительно согласовываются с АО "Мосводоканал", на этапе согласования основных технических решений проекта автоматизации.

В зависимости от условий и эксплуатационных требований объектов предусмотреть звуковую и световую сигнализацию срабатывания аварийных сигналов и средств контроля загазованности, затопления или иных средств промышленной безопасности. Вывод на программируемый контроллер и передачу информации в SCADA от вышеперечисленных систем аварийной сигнализации, а также средств контроля доступа в помещение и к оборудованию, систем бесперебойного энергоснабжения, систем охранной и пожарной сигнализации, устройств защиты и т.п. необходимо предусматривать проектом в обязательном порядке.

В обязательном порядке в проекте должна быть включена документация об используемых автоматизированных установках сторонних производителей: схема подключения, спецификация оборудования, протокол связи, таблица сигналов и команд управления, описание алгоритмов работы подключаемых систем и другая необходимая для реализации проекта документация.

2. Общие требования к АСУТП

Проектируемая АСУТП должна соответствовать следующим принципиальным требованиям:

- *Надежность* – свойство объекта сохранять работоспособное состояние в течении некоторого времени или некоторой наработки.

Реализуется путем внедрения технической политики, стандартов и требований к компонентам систем, внедрения в структурных подразделениях АО «Мосводоканал» системы ТОиР, создания базы неснижаемого (оперативного) запаса и унификации оборудования и запасных частей:

- *Ремонтопригодность* – возможность восстановления работоспособности систем за минимальное время при экономически оправданной стоимости ремонта;

Реализуется на уровне разработки как использование максимально простых, распространенных и универсальных компонент системы (реле, модулей ввода/вывода и т.п.) для обеспечения простой покомпонентной замены неисправных частей, а также для исключения взаимного влияния и предотвращения распространения последствий аварии.

- *Тестируемость* – возможность установления факта правильного функционирования системы и её составляющих частей;

Реализуется как система диагностики состояния основных подсистем АСУ ТП: энергоснабжения и линий связи и управления, так и состояния контроллеров, узлов SCADA, активного оборудования ЛВС. Минимальные требования – возможность

локальной проверки работы на месте, максимальные – создание централизованных систем мониторинга состояния систем и компонентов.

- *Диагностируемость* – возможность быстрого нахождения неисправной части/компонента-системы:

Реализуется в части системотехники как возможность визуального определения неисправных компонентов систем управления и оборудования связи (индикаторы и пр.), а также обеспечение поиска неисправности при помощи специализированного ПО либо штатными средствами контроллеров АСУ ТП.

- *Простота обслуживания и эксплуатации* – минимальные требования к квалификации и дополнительному обучению эксплуатирующего систему персонала;

Реализуется также как требования минимального количества максимально универсальных инструментальных и программных средств, необходимых для эксплуатации и выбора простых в освоении технических и программных средств.

- *Экономичность* – обеспечение минимальных расходов при внедрении и в процессе функционирования систем при условии выполнения основных производственных требований;

Реализуется как ограничение максимального уровня и объема автоматизации технологических процессов рамками экономической целесообразности с учетом требований надежности и безопасности работы. Учитывается оптимальная унификация программных и технических средств, обеспечивающая интеграцию уже имеющихся решений.

- *Внедряемость* – минимальное время на проектирование и развертывание (монтаж и пуско-наладку) системы.
- *Модифицируемость* – возможность модернизации систем без замены их ключевых компонентов для обеспечения работы с новым/дополнительным технологическим оборудованием и устройствами;
- *Расширяемость* – возможность ввода в систему дополнительных сигналов, устройств или функциональных возможностей контроля и управления, не предусмотренных в первоначальном техническом задании;
- *Наращиваемость* – возможность масштабирования, увеличения размера автоматизированной системы при увеличении размера или числа объектов автоматизации;
- *Открытость* – соответствие современным промышленным стандартам, которое обеспечивает возможность интеграции с другими открытыми

системами, возможность простой интеграции доступных модулей и частей системы достаточно широкого ряда производителей;

- *Взаимозаменяемость* – возможность замены любого компонента системы на аналогичный другого производителя, имеющийся в свободной продаже;
- *Модульность* – способность аппаратного или программного обеспечения к модификации путем добавления, удаления или замены отдельных модулей системы без влияния на оставшуюся ее часть;
- *Универсальность* – возможность перенастройки системы для работы с новыми технологическими процессами при модернизации технологического оборудования;
- *Стандартность пользовательского интерфейса* – стандартизация пользовательских интерфейсов с целью сокращения расходов на обучение и количества ошибок персонала в процессе эксплуатации систем;
- *Актуальность* – максимальная длительность жизненного цикла без существенного морального и физического старения системы, достигаемая путем постоянного обновления аппаратных и программных компонентов, на базе выбранных долгоживущих промышленных стандартов и оборудования;
- *Автономность* – слабая связанность элементов архитектуры между собой, т.е. деление системы на части следует производить так, чтобы поток информации через связи был минимален и через них не замыкались контуры автоматического регулирования; Реализуется как максимальная независимость на горизонтальном уровне систем управления отдельными технологическими процессами.
- *Безопасность* – соответствие требованиям промышленной безопасности в отношении управляемых и контролируемых объектов технологического процесса и технике безопасности обслуживающего и оперативного персонала; Реализуется разработка максимально надежных алгоритмов автоматической работы сооружений, не позволяющих ввод не корректных параметров и вмешательство в работу систем управления. Действия оператора и дистанционное управление максимально ограничиваются рамками технологического регламента работы сооружений.
- *Защищенность* – обеспечение современных требований по защите систем от действий злоумышленников и неквалифицированных пользователей; Реализуется путем максимальной изоляции и разделения АСУ ТП от корпоративных сетей, а также полной изоляции от общедоступных сетей. Разрабатывается также политика физического и программного ограничения

доступа к АСУ ТП, управления доступом, мониторинга действий персонала, разграничения и управления правами авторизованных пользователей АСУ ТП.

3. Типы объектов для АСУТП

С точки зрения проектирования внедрения или модернизации АСУТП в АО "Мосводоканал" существует три типа технологических (производственных) объектов.

Объекты первого типа

К объектам первого типа АО "Мосводоканал" относятся крупные производственные подразделения:

- ✓ водопроводные станции (РСВ, ЗСВ, ВСВ, ССВ);
- ✓ очистные сооружения (КОС, ЛОС);
- ✓ отдельные производственные управления (ЗВК, ТиНАО), с преобладающим автоматическим управлением.

В этих подразделениях функционируют местные диспетчерские пункты управления отдельными технологическими процессами и главные диспетчерские пункты объектов, которые должны обеспечивать круглосуточный контроль и управление с высокой степенью надежности (время восстановления АСУТП после аварии не должно превышать 1-2 часа). На объектах данного типа обязательно предусматривается автономное ручное (местное) и автоматическое управление каждым отдельным технологическим процессом. Дистанционное управление предусматривается, как правило, для химически опасных объектов, объектов находящихся в зоне возможного затопления, а также на объектах без дежурного персонала в случаях необходимости реализации сценариев дистанционного управления при ликвидации аварийных ситуаций.

Для объектов первого типа является критически важным работоспособность систем автоматического управления, но не является критичным кратковременный выход из строя систем автоматического управления отдельными технологическими процессами. Полнофункциональное управление объектами подразделений первого типа без действующей АСУТП не возможно либо сильно затруднено.

В подразделениях первого типа контроллеры управления технологическими процессами, как правило, взаимодействуют по собственной отказоустойчивой внутренней сети передачи данных подразделения с резервированными объектовыми SCADA системами подразделения. Связи контроллеров непосредственного управления объектами для наиболее критичных объектов подразделений дублируются дополнительными каналами связи либо закольцовываются альтернативным кабелем связи. Данные передаются непосредственно между контроллерами и основными SCADA системами подразделений, а также

резервными SCADA системами подразделения. Данные также могут передаваться между контроллерами АСУТП в локальной промышленной сети подразделения с целью реализации надежных алгоритмов управления.

SCADA серверы подразделения и их клиенты объединены защищенной компьютерной сетью предприятия, гарантирующей необходимую производительность и исключающей не авторизованное подключение. Клиенты уровня производственного подразделения – МДП, ГДП взаимодействуют непосредственно с основными SCADA серверами подразделения, получая от них все необходимые данные для реализации автоматических режимов управления.

Сети, используемые АСУТП, как контроллерные объектовые сети, так и используемые для подключения SCADA отделены от административных и прочих сетей подразделений и являются составной частью единой сети АСУТП АО "Мосводоканал", к которой относятся также все прочие SCADA серверы и SCADA клиенты других подразделений и центрального офиса АО Мосводоканал.

Все Каналы передачи данных SCADA подразделений первого типа в МБК в обязательном порядке резервируются. Персонал ЦДУ использует данные объектовых SCADA, непосредственно влияющих и необходимых для управления городской системой водоснабжения и водоотведения в целом.

Мобильные пользователи могут быть подключены к SCADA серверам подразделений для просмотра оперативных данных на месте аварии либо в дороге через терминальный либо WEB сервисы SCADA, при этом используются только просмотрные, не управляющие клиенты SCADA.

Количество SCADA систем в подразделениях первого типа определяется в зависимости от общего количества сигналов контроля и Управления (из соображений производительности нагрузку на один двухпроцессорный сервер SCADA не желательно превышать 30 тысяч тэгов), а также от количества автономных производственно-технологических блоков и требований надежности и автономности при реализации управления технологическими процессами (на полностью автономных блоках технологических сооружений подразделений целесообразно иметь свои SCADA серверы).

SCADA системы подразделений первого типа должны быть расположены в оборудованных серверных помещениях, соответствующих требованиям к помещениям такого типа, установленным АО "Мосводоканал".

Для оперативного восстановления работоспособности объектовой SCADA системы в случае сбоя, обеспечивается реализация SCADA серверов "горячего" резерва в серверных комнатах подразделений. Помимо "горячего" резервирования основных SCADA серверов в подразделении первого типа, должно быть реализовано "холодное" резервирование (создание резервных копий серверов

SCADA) на случай серьезных аварий в серверной производственного подразделения.

Для контроля и управления отдельных объектов подразделений, оснащенных местными диспетчерскими пунктами контроля и управления, используются пульта и компьютерные сенсорные панели местного управления, реализующие функции SCADA, достаточные для управления данными объектами.

Прямого взаимодействия с целью обмена данными на уровне SCADA систем не осуществляется, т.е. данные не копируются с одного SCADA сервера на другой, а используются клиентами непосредственно с исходных SCADA серверов.

Объекты второго типа

- ✓ Регулирующие водопроводные узлы;
- ✓ Высоковольтные насосные станции;
- ✓ Объекты находящихся в режиме автоматического управления и контроля, оснащенных местными диспетчерскими пунктами управления.

Данные объекты не имеют столь жестких требований по объёмам и срокам восстановления автоматического управления, как объекты первого типа (время восстановления АСУТП после аварии не должно превышать 1-2 суток). Для объектов этого типа критичным является наличие контроля состояния объектов. Управление на некоторое время может быть переведено в режим ручного/местного автоматического. Реализуется управление технологическими системами с местного пульта управления контроллером объекта в автоматическом режиме, ручное управление объектом по месту либо использование SCADA клиента на объекте, соединенного с сервером SCADA в ЦОД АО "Мосводоканал", данные на который поступают от контроллера объекта.

Контроллеры управления технологическими системами взаимодействуют по резервированному каналу связи с центральной SCADA системой в ЦОД АО "Мосводоканал".

Клиенты SCADA как местные (на объектах второго типа), так и в ЦДУ либо других подразделениях взаимодействуют со SCADA системой в ЦОД.

Объекты третьего типа

К объектам третьего типа относятся все автономные небольшие производственные объекты и точки контроля без диспетчерского или дежурного персонала (канализационные станции, отдельные скважины, регулирующие камеры, точки контроля параметров городской водопроводной и канализационной сети и т.п.).

Контроллеры управления технологическими системами взаимодействуют с центральной SCADA системой в ЦОД. Передача данных в ЦОД осуществляется по дублированному (для критичных объектов) или обычному каналу передачи данных.

На данных объектах, как правило, нет управления либо реализовано управление технологическими системами в местном ручном режиме. АСУТП осуществляет только контроль параметров работы объекта. Отдельные объекты третьего типа, относящиеся к зоне ответственности ЦДУ, управляются в автоматическом и в дистанционном режиме.

Клиенты SCADA на объектах третьего типа отсутствуют. В ЦДУ либо других подразделениях клиенты взаимодействуют со SCADA системой в ЦОД.

4. Режимы управления

В АСУТП АО "Мосводоканал" предусматривается три основных режима управления: "Местное" и "Автоматическое", «Дистанционный»

Типичная схема автоматизации производственных процессов приведена на *рисунке 1*, ниже. Технологическое оборудование (насосы, поворотно-дисковые затворы и т.п.) расположено в цеху и снабжено местными электрифицированными пультами управления. Сигналы с пультов продублированы кнопками управления на шкафу автоматики, который, в свою очередь, передает данные и получает рецепты управления технологическим процессом через SCADA от диспетчера АСДКУ.

Шкафы управления АСУТП располагаются либо непосредственно в цеху, вблизи основного технологического оборудования (при необходимости визуального контроля объектов управления оператором) либо в местном диспетчерском пункте или помещениях РТЗО.

На шкафах АСУТП должен быть предусмотрен ключ переключения режимов управления: 1. Местное – с кнопок управления или графического терминала шкафа автоматики; 2. Автоматическое, а также дистанционное – посредством АСУТП с использованием контроллера; 3. Отключено – управление возможно только с кнопочных пультов непосредственно по месту установки оборудования.

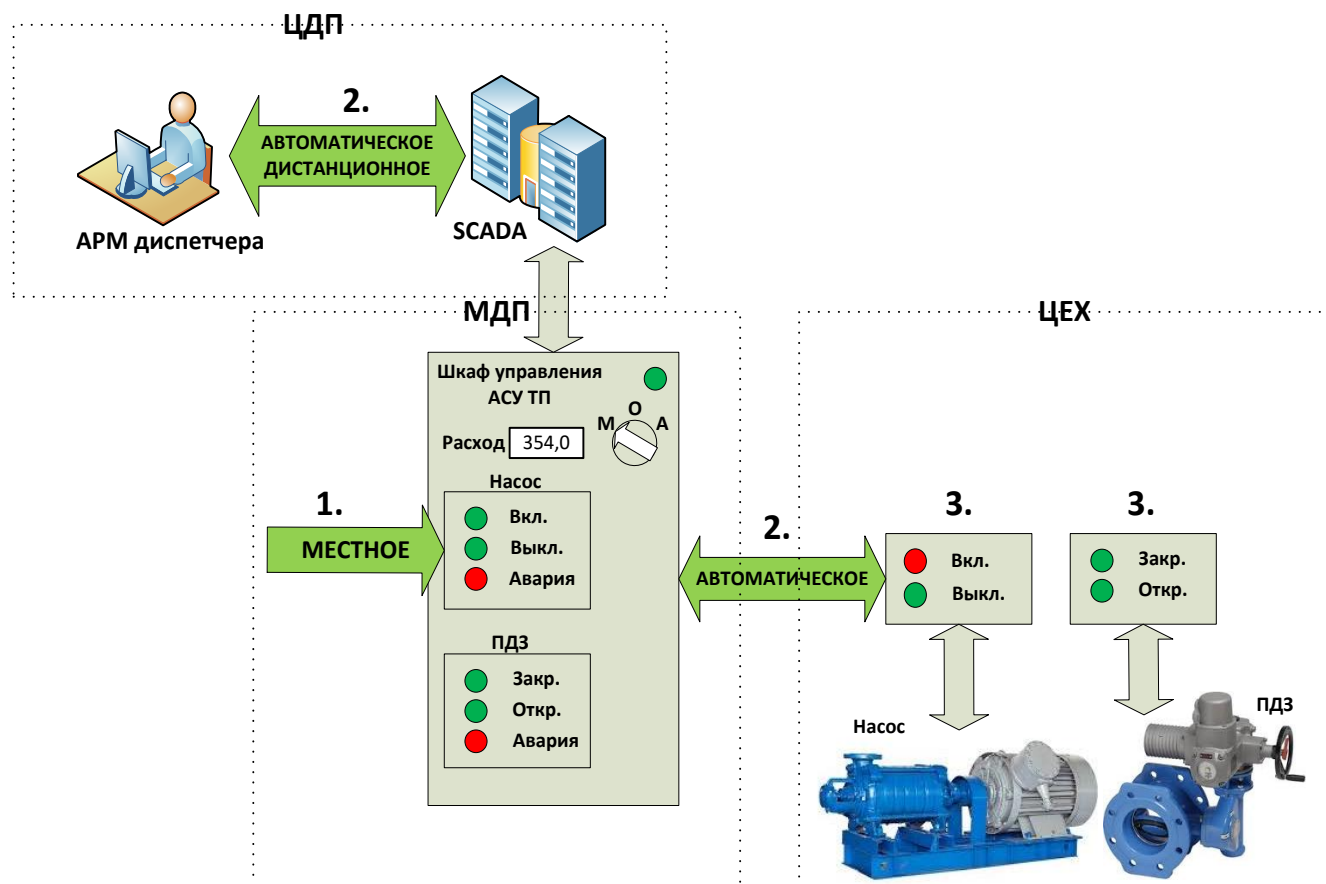


Рисунок 1

Традиционное "Местное" управление реализовано непосредственно с кнопочных пультов по месту установки оборудования (затворов, насосов и пр.). Местное управление оборудованием служит для гарантированного управления технологическим оборудованием в случае выполнения ремонтных, профилактических и или иных работ, выходящих за рамки алгоритмов систем автоматического управления, а также для обеспечения эксплуатации производственных объектов в случаях отказа систем автоматического управления. Также местное управление продублировано на шкафах управления для удобства оператора. Для достаточно сложных объектов управления, затрудняющих расположение значительного количества элементов управления на шкафу автоматики либо требующих вывода значительного количества информации оператору, местное управление от шкафа АСУТП может быть реализовано через графический терминал шкафа с использованием контроллера. В режиме "Местного" управление всегда осуществляет человек – оператор технологического процесса, принимающий и непосредственно выполняющий все решения по переключениям оборудования, в то время как контроллер либо не задействован в управлении либо используется для обеспечения функционирования графического терминала управления. В современной концепции управления технологическими процессами АО "Мосводоканал" местное управление не является основным режимом работы производственного оборудования и сохранено для обеспечения надежности в случае

отказа вычислительной техники и линий связи, а также для проведения работ не предусмотренных алгоритмами автоматического управления.

Режим "Автоматического" управления является основным режимом функционирования технологических процессов, охваченных системами АСУТП. В этом режиме управление осуществляет контроллер по заранее заданному алгоритму проведения технологического процесса. Контроллер автоматически поддерживает работу оборудования без участия оператора. Оператор вмешивается в работу контроллера только эпизодически, меняя режимы работы системы посредством отправки "рецептов" управления с графического терминала шкафа управления либо через человеко-машинный интерфейс (ЧМИ) системы диспетчерского контроля и управления (SCADA). Для сложных объектов, не имеющих проработанных сценариев автоматического предотвращения последствий аварийных ситуаций либо не обладающих требуемой надежностью систем управления, может быть предусмотрен режим "Дистанционного" телеуправления оборудованием через интерфейс SCADA или графический терминал шкафа АСУТП.

Положение переключателя "Отключено" на шкафах управления используется для проведения ремонтных либо регламентных работ с оборудованием и обусловлено требованиями "Межотраслевых правила по охране труда (правила безопасности) при эксплуатации электроустановок" и "Правил технической эксплуатации электроустановок потребителей". Переключатель режимов местного и автоматического управления на шкафах автоматики обязательно выполняется механическим. Переключение автоматического режима в дистанционный, с АРМ оператора, напротив, реализуется программным способом.

При оснащении шкафов автоматического управления АСУТП сенсорным пультом оператора, должны предусматриваться следующие пользователи с соответствующими правами доступа и интерфейсами управления: 1. Просмотр данных (без пароля, без управления, только просмотр текущих режимов), 2. Оператор (с паролем и доступом к изменению технологических параметров управления объектом – уставок, режимов и пр.), 3. Инженер (с паролем и доступом к изменению параметров настроек и характеристик оборудования, диапазонов измерения приборов, параметров конкретных приводов и пр.). Для каждого из режимов должна разрабатываться инструкция пользователя.

5. Требования к серверному оборудованию и АРМ SCADA

Вё должно выбираться программное обеспечение SCADA в варианте поставки поддерживающем распределенное клиент-серверное сетевое взаимодействие с другими узлами SCADA.

При разработке проектов реконструкции/модернизации, проектная организация обязана учитывать возможность обновления существующих лицензий

SCADA, имеющихся в АО "Мосводоканал" с целью снижения закупочной стоимости программного обеспечения.

При разработке проектов автоматизации и определении лицензирования SCADA для технологических объектов должен быть обеспечен запас по точкам ввода/вывода не менее 20% относительно количества сигналов, входящих в проект.

Для обеспечения работы центральных SCADA-узлов крупных производственных объектов, объединяющих несколько технологических процессов или поддерживающих взаимодействие с другими серверами SCADA, должен выбираться вариант поставки со средствами разработки, допускающими on-line доработку SCADA без остановки функционирования АРМ диспетчеров и операторов.

Для автономных объектов и отдельных технологических процессов, на которых требуется полноценная SCADA оператора, но не планируется доработка интерфейсов SCADA систем без отключения функционирования АРМ диспетчерского пункта, допустимо использовать Runtime версию.

В качестве программного обеспечения SCADA в АО "Мосводоканал" в настоящее время используется программное обеспечение семейства GE iFIX, обеспечивающее разработку полную функциональность SCADA. Все вновь проектируемые SCADA-решения должны быть платформенно-независимыми и совместимыми с действующими системами на уровне интеграции данных и протоколов обмена информацией.

Для организации работы специалистов, не требующей доступа к управлению технологическим оборудованием, должна использоваться версия клиента Read-Only, предназначенная только для просмотра, где запись в базу данных и OPC-серверы отключена.

Для записи оперативных данных истории технологического процесса в АО "Мосводоканал" в настоящее время используется программное обеспечение семейства GE iHistorian – специализированная база данных для систем промышленной автоматизации, обработка данных в которой происходит по принципу реального времени в виде временных рядов. Независимо от использования GE iHistorian должна обеспечиваться запись данных в реляционную СУБД (например, MS SQL) – собственный сервер истории технологических процессов, в формате, выбранном АО "Мосводоканал".

Типовыми для АО "Мосводоканал" принимаются следующие возможные конфигурации АСУТП объектов применительно к использованию SCADA:

1. Объекты первого типа с несколькими SCADA-серверами и клиентскими АРМ SCADA.

2. Объекты второго типа с автономными серверами/APM SCADA либо без SCADA-серверов, но с клиентскими APM SCADA;
3. Объекты третьего типа без SCADA-серверов и без клиентов SCADA;

Объектом считается территория производственных подразделений, принадлежащая на тех или иных правах АО "Мосводоканал", на которой может быть реализована надежная проводная связь между компонентами АСУТП: управляемым и контролируемым оборудованием, контроллерными шкафами управления, SCADA-серверами и APM. В случаях, когда несколько территорий подразделений Общества не могут быть объединены собственной кабельной системой связи и управления, а используются каналы связи внешних провайдеров услуг связи, целесообразно различать, как несколько отдельных объектов управления, ввиду требований информационной и промышленной безопасности АСДКУ.

Критерии выбора типового решения по использованию SCADA следующие:

1. Объекты без SCADA-серверов и без клиентов SCADA:

- 1.1. Отсутствие постоянного диспетчерского персонала, для обеспечения работы которого непрерывно требуется SCADA;
- 1.2. Отсутствие необходимости осуществлять управление объектом автономно, в отрыве от АСДКУ АО "Мосводоканал", длительное время с полной функциональностью, которая может быть реализована только посредством интерфейсов SCADA (и не может быть реализована с локальных органов управления либо графических терминалов шкафов контроллеров);
- 1.3. Возможность реализации основных функций управления и контроля с кнопок управления локального щита управления либо графического терминала шкафа контроллера (то есть достаточная полнота систем автоматического контроля и управления, позволяющая реализовать все основные алгоритмы и режимы работы объекта без участия либо с минимальным участием оператора через продолжительные интервалы времени);
- 1.4. Наличие вышестоящего центра управления объектом, подразделения или всего АО "Мосводоканал" выполняющего данные функциональные задачи контроля и управления, к которому с достаточной надежностью могут быть подключены контроллеры АСУТП объекта, обеспечивающие централизованный контроль посредством вышестоящей SCADA.

Если критерии 1.1. – 1.4. выполнены, то SCADA на объекте не проектируется.

2. Объекты без SCADA-серверов, но с клиентскими APM SCADA

- 2.1. Наличие постоянного диспетчерского персонала, для обеспечения работы которого непрерывно требуется SCADA (например, в случае нескольких контроллеров на территориально распределенном объекте, управление которыми проще объединить через интерфейс SCADA, чем организовывать местный щит управления либо сводить вместе графические терминалы шкафов контроллеров);
- 2.2. Отсутствие необходимости осуществлять управление объектом автономно, в отрыве от АСДКУ АО "Мосводоканал", длительное время с полной функциональностью, которая может быть реализована только посредством интерфейсов SCADA либо при наличии резервного канала связи с объектом, обеспечивающего достаточную надежность (то есть функции SCADA не требуются в течении времени, за которое реально может быть восстановлена связь с объектом управления и в течении которого можно продолжать управлять объектом в местном режиме);
- 2.3. Наличие вышестоящего центра управления объекта, подразделения или всего АО "Мосводоканал" выполняющего данные функциональные задачи контроля и управления SCADA.

Если критерии 2.1. – 2.3. выполнены, то SCADA-сервер на объекте не проектируется, а устанавливается в центральном офисе (ЦОД или в серверной подразделения Общества), а на объекте планируется APM SCADA. Установка и расположение местных органов управления и частично дублирующих функции SCADA графических терминалов шкафов контроллеров определяется проектом.

3. Объекты с несколькими SCADA-серверами и клиентскими APM SCADA

- 3.1. Наличие постоянного диспетчерского персонала, для обеспечения работы которого непрерывно требуется SCADA (например, в случае нескольких контроллеров на территориально распределенном объекте, управление которыми проще объединить через интерфейс SCADA, чем организовывать местный щит управления либо сводить вместе графические терминалы шкафов контроллеров);
- 3.2. Наличие необходимости осуществлять управление объектом автономно, в отрыве от АСДКУ АО "Мосводоканал", длительное время с полной функциональностью, которая может быть реализована только посредством интерфейсов SCADA;
- 3.3. Наличие необходимости дублирования и резервирования функций контроля и управления между несколькими диспетчерскими пунктами объекта с целью обеспечения большей надежности контроля и управления;

- 3.4. Отсутствие возможности контроля и управления с локальных/местных органов управления либо графических терминалов шкафов контроллеров из-за отсутствия достаточного количества персонала либо недостаточной развитости локальных систем контроля и управления;
- 3.5. Отсутствие вышестоящего центра управления объекта, подразделения или всего АО "Мосводоканал" достаточной мощности, зарезервированного под выполнение данных функциональных задач контроля и управления.

Если критерии 3.1. – 3.5. выполнены, то на объекте проектируются и устанавливаются как SCADA-серверы, так и APM SCADA. Установка и расположение местных органов управления и частично дублирующих функции SCADA графических терминалов шкафов контроллеров определяется проектом.

Во всех случаях в данном разделе под надежностью понимается проектная оценка и расчет надежности по сформулированным заказчиком временным критериям доступности и работоспособности узлов управления.

Варианты с установкой сервера без клиентского ПО SCADA либо сервера SCADA с реализацией APM SCADA непосредственно на сервере не рассматривается ввиду нецелесообразности.

Детально принципы проектирования и создания SCADA, рассмотрены в документе СТП-42439-02-12-14 **"Стандарт разработки SCADA (iFix). Правила разработки систем диспетчерского контроля и управления (баз данных, мнемосхем, аварийной и предупредительной сигнализации, организации управления) SCADA (iFix) ОАО Мосводоканал"**

([https://www.mosvodokanal.ru/forexperts/requirements/Правила%20разработки%20СДКУ%20\(БД,%20мнемосхем,%20авар%20и%20предупр%20сигн,%20орг%20управл\)%20SCADA%20\(iFix\).pdf](https://www.mosvodokanal.ru/forexperts/requirements/Правила%20разработки%20СДКУ%20(БД,%20мнемосхем,%20авар%20и%20предупр%20сигн,%20орг%20управл)%20SCADA%20(iFix).pdf)).

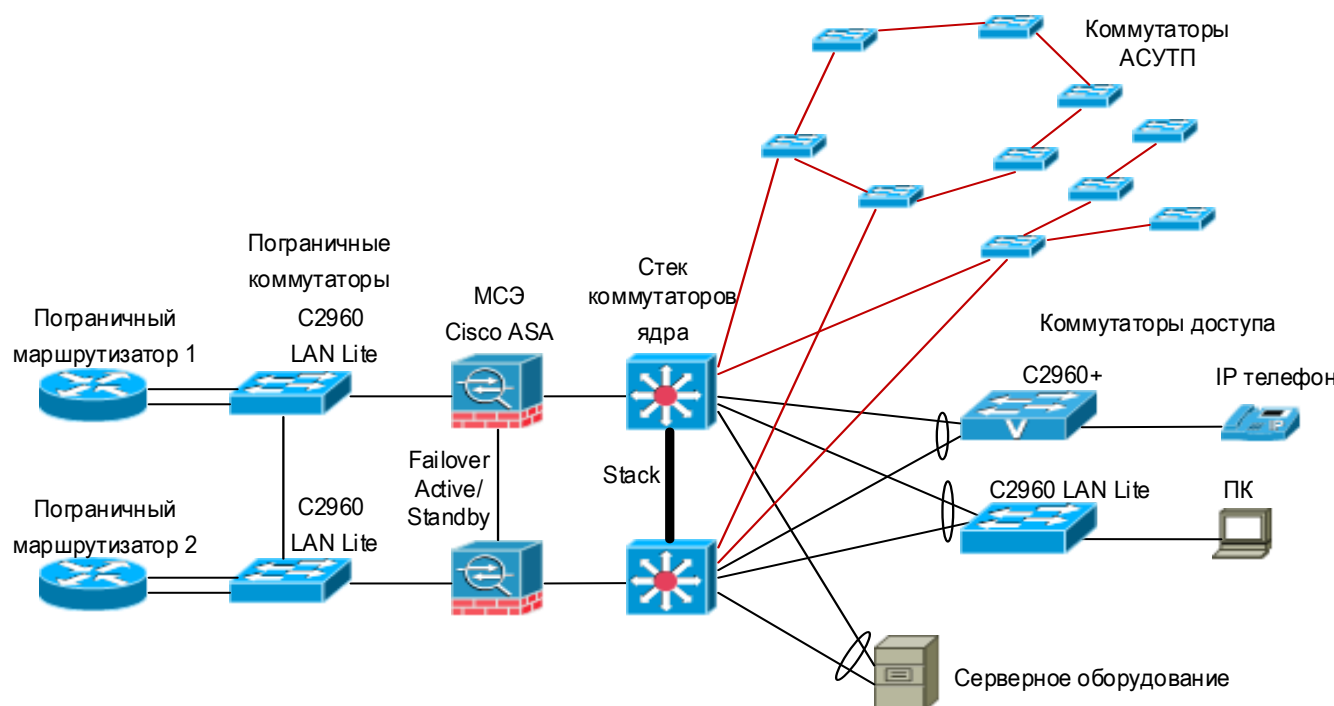
6. Промышленные сети и протоколы АСУТП

В данном разделе описываются общие требования и архитектурные решения построения промышленной сети производственных объектов АСУТП АО "Мосводоканал" и её стыковки с сетями предприятия верхнего уровня.

Промышленные сети АО "Мосводоканал" должны поддерживать физические интерфейсы связи Ethernet: "10BASE-T"/"100BASE-TX"/"100BASE-FX"/"100BASE-FX WDM" и RS485 с промышленными протоколами обмена данными с устройствами и средствами автоматизации: Modbus RTU, Modbus TCP, CANOpen, Profibus DP, Ethernet/IP, DNP3, МЭК 60870-101/104, AS-Interface, HART.

На Рисунке *"Структурная схема подключения технологического сегмента в корпоративную вычислительную сеть объекта"* ниже показан пример схемы

подключения коммутаторов технологической сети к оборудованию КВС объекта. Показанные подключения предоставляют максимальную гибкость в применяемых топологиях для коммутаторов АСУТП (кольцо, звезда, расширенная звезда и др.).



Структурная схема подключения технологического сегмента в корпоративную вычислительную сеть объекта

Группа коммутаторов технологической сети, представляющая из себя неделимый массив в виде звезды, кольца или иной топологии, подключается к стеку коммутаторов ядра КВС. Для нужд подключения оборудования технологической сети резервируется не менее двух SFP-портов на каждом коммутаторе ядра. Это – предпоследние по нумерации оптические порты на коммутаторе уровня ядра КВС или коммутаторе распределения КВС, в зависимости от физического размещения кабелей от оборудования АСУТП. В зависимости от модели коммутатора КВС это будут порты G0/3, G0/27 или G0/51 на обоих коммутаторах в стеке (коммутаторы доступа), либо G1/0/27 и G2/0/27 (G1/0/51 и G2/0/51) для стекируемых 24-портовых (48-портовых) коммутаторов (коммутаторы ядра, распределения).

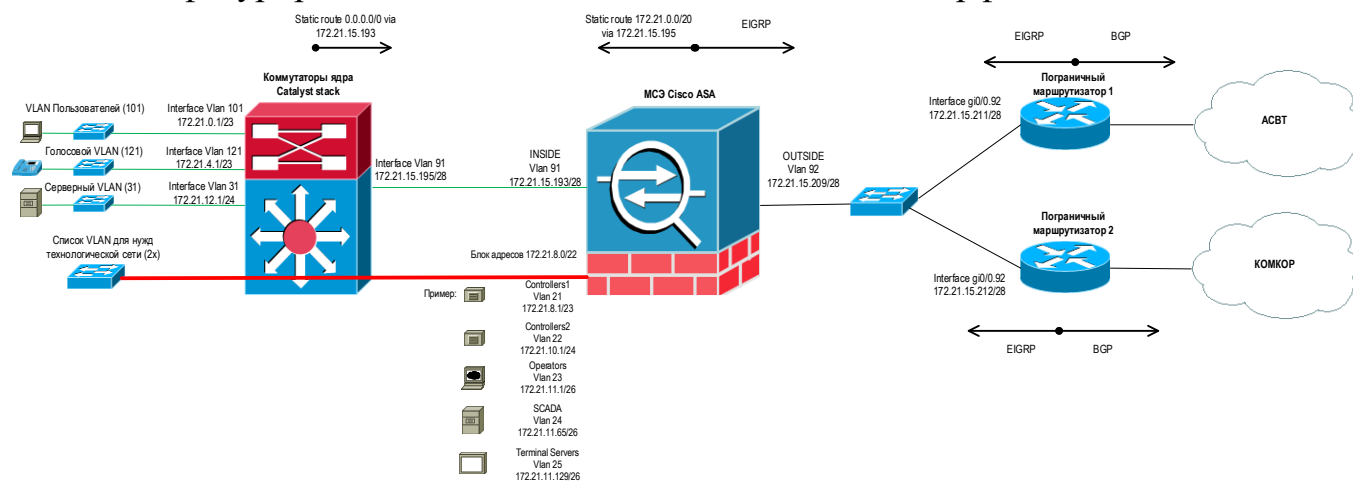
Для обеспечения отказоустойчивости необходимо использовать резервные физические линии. Также при осуществлении взаимодействия между коммутаторами ядра КВС и сетью АСУТП допустимо использовать технологию агрегирования каналов (Etherchannel).

Выделение IP-подсетей для АСУТП осуществляется в соответствии с общим планом адресации Общества. Для различных нужд АСУТП выделяется диапазон номеров VLAN (с 21 по 29). Если на технологических коммутаторах филиала не применяются VLAN, то порты коммутаторов ядра КВС, предназначенные для подключения коммутаторов АСУТП конфигурируются как порты доступа в VLAN

21. В случае применения VLAN на технологических коммутаторах стык между КВС и сетями АСУТП осуществляется с помощью транковых соединений.

Для защиты от петель коммутации применяется протокол STP (рекомендуется использование Rapid-STP).

Для задач АСУТП с целью обеспечения безопасности на межсетевых экранах создаются соответствующие логические интерфейсы. Шлюзом по умолчанию для оборудования АСУТП указываются IP-адреса этих интерфейсов. На Рисунке *"Маршрутизация трафика и обеспечение безопасности подсетей АСУТП"* ниже показан пример подобного разделения, а также логика маршрутизации трафика между оборудованием КВС. Минимально для задач АСУТП создается один логический интерфейс на межсетевых экранах для VLAN 21. При необходимости могут быть сконфигурированы дополнительные логические интерфейсы.



Маршрутизация трафика и обеспечение безопасности подсетей АСУТП

Политики безопасности и гибкой фильтрации трафика для доступа к оборудованию АСУТП на технологических объектах Общества осуществляются на межсетевых экранах.

На них применяются следующие методы обеспечения безопасности:

- ✓ Списки управления доступом и инспектирование сетевого трафика;
- ✓ Политики инспектирования трафика по различным протоколам;
- ✓ Подробное логирование;
- ✓ Детектирование аномалий сетевого трафика (сканирование сети, атаки фрагментами и т.п.).

Также может быть осуществлена дополнительная аутентификация пользователей, обращающихся к оборудованию АСУТП из подсетей общего назначения.

Подробнее реализация политик защиты АСУТП в соответствии требованиям к обеспечению защиты информации в автоматизированных системах управления

производственными и технологическими процессами на критически важных объектах (Приказ ФСТЭК России № 31 от 14 марта 2014 г.) и другими нормативными документами описывается в соответствующих стандартах предприятия (см. нормативные ссылки).

ТРЕБОВАНИЯ К РАЗДЕЛУ технические системы безопасности и телефонная связь

Основополагающие нормативные документы для проектирования технических систем безопасности и телефонной связи:

- ГОСТ Р 21.1101.2013.
- Постановление Правительства Российской Федерации №87 от 16.02.2008г. (ред. от 12.11.2016 с изм. от. 28.01.2017).
- ГОСТ Р МЭК 60065-2002.
- ГОСТ Р 50009-2000.
- ГОСТ Р 50776-95.
- ГОСТ 12.1.046-2014.
- Пособие к РД 78.145-93.
- РД 25.952-90.
- Р 78.36.002-2010.
- Р 78.36.005-2011.
- Р 78.36.032-2013.
- Р 78.36.032-2014.
- Р 78.36.039-2014.
- Приказ №937 МВД РФ от 16.11.2006г. (в ред. от 05.06.2007).
- Постановление Правительства Российской Федерации №272 от 25.03.2015г.
- ГОСТ Р 51558-2000.

Проектируемое оборудование должно быть согласовано с Управлением режима и отделом слаботочных систем и телефонной связи управления АСУТПиС.

Общие технические требования для проектирования систем охранной и периметральной охранной сигнализации:

1. Проектные работы выполняются в соответствии с требованиями ГОСТ 21.1101.2013, ГОСТ Р 50776-95, СНиП 11-01-95.
2. Проектно-сметная документация должна содержать следующий комплект документации:
 - техническое задание на разработку проекта, выполненное в соответствии с требованиями
 - пояснительную записку;
 - общие данные;
 - планы разводов (схемы закладных) трубопроводов, кабелей, проводов и мест установки технических средств охраны на объекте (по требованию заказчика или монтажной организации);
 - планы разводов шлейфов сигнализации и линий связи технических средств охраны (совмещенный или отдельный по каждому виду сигнализации);

- схему соединений структурную общую (совмещенная или раздельная по каждому виду сигнализации);
 - схемы электрические подключения технических средств охраны;
 - схемы установки технических средств охраны в охраняемых помещениях;
 - схемы блокировки отдельных конструкций (окон, дверей, воздуховодов, стен и других конструкций);
 - 5
 - схему установки оборудования в помещении охраны,
 - схему (таблицу) разводки электропитания;
 - расчет постоянного тока потребления технических средств охраны в режиме тревоги (выбор резервного источника питания);
 - кабельный журнал (по требованию заказчика или монтажной организации);
 - спецификацию оборудования;
 - таблицу исходных данных для программирования технических средств охраны;
 - чертежи общих видов нетиповых решений, конструкций и оборудования.
3. Технические средства охранной сигнализации периметра должны выбираться в зависимости от вида предполагаемой угрозы объекту, помеховой обстановки, рельефа местности, протяженности и технической укреплённости периметра, типа ограждения, наличия дорог вдоль периметра, зоны отторжения, ее ширины.
 4. Охранная сигнализация периметра объекта проектируется, как правило, двух , либо, однорубежной. Для усиления охраны, определения направления движения нарушителя, блокировки уязвимых мест следует применять многорубежную охрану. При проектировании двух и более рубежной охраны необходимо обеспечить наличие в системах охранной сигнализации средств защиты, основанных на различных физических принципах действия.
 5. Технические средства охранной сигнализации периметра могут размещаться на ограждении, зданиях, строениях, сооружениях или в зоне отторжения. Охранные извещатели должны устанавливаться на стенах, специальных столбах или стойках, обеспечивающих отсутствие колебаний, вибраций.
 6. Периметр, с входящими в него воротами и калитками, следует разделять на отдельные охраняемые участки (зоны) с подключением их отдельными шлейфами сигнализации к ППК малой емкости или к пульту внутренней охраны, установленных на КПП или в специально выделенном помещении охраны объекта. Длина участка определяется исходя из тактики охраны, технических характеристик аппаратуры, конфигурации внешнего ограждения, условий прямой видимости и рельефа местности, но не более 200 м для удобства технической эксплуатации и оперативности реагирования. Следует выделять следующие основные зоны охраны: Фронт, Тыл, Правый фланг, Левый фланг. Основные ворота должны выделяться в самостоятельный участок периметра. Запасные ворота, калитки должны входить в тот участок периметра, на котором они находятся.

7. В качестве пультов внутренней охраны могут использоваться ППК средней и большой емкости (концентраторы), СПИ, автоматизированные системы передачи извещений (АСПИ) и радиосистемы передачи извещений (РСПИ). Пульты внутренней охраны могут работать как при непосредственном круглосуточном дежурстве персонала на них, так и автономно в режиме "Самоохраны".
8. При использовании для блокировки периметра извещателей, требующих зону отторжения, необходимо организовать ее следующим образом: Зона отторжения должна быть тщательно спланирована и расчищена. В ней не должно быть никаких строений и предметов, затрудняющих применение технических средств охраны и действия службы безопасности. Зона отторжения может быть использована для организации охраны объекта с помощью служебных собак. В этом случае зона отторжения должна иметь предупредительное сетчатое или штакетное ограждение высотой не менее 2,5 м. Ширина зоны отторжения, в которой размещаются технические средства охраны периметра, должна превышать ширину их зоны обнаружения.
9. Установка охранных извещателей по верху ограждения должна производиться только в случае, если ограждение имеет высоту не менее 2 м.
10. На КПП, в помещении охраны следует устанавливать технические устройства графического отображения охраняемого периметра (компьютер, световое табло с мнемосхемой охраняемого периметра и другие устройства.
11. Все оборудование, входящее в систему охранной сигнализации периметра должно иметь защиту от вскрытия.
12. Открытые площадки с материальными ценностями на территории объекта должны иметь предупредительное ограждение и оборудоваться объемными, поверхностными или линейными извещателями различного принципа действия.
13. Техническими средствами охранной сигнализации должны оборудоваться все помещения с постоянным или временным хранением материальных ценностей, а также все уязвимые места здания (окна, двери, люки, вентиляционные шахты, короба и т. п.), через которые возможно несанкционированное проникновение в помещения объекта.
14. Объекты подгрупп АІ, АІІ и БІІ оборудуются многорубежной системой охранной сигнализации, объекты подгруппы БІ – однорубежной (в соответствии с Р 78.36.032-2013).
15. Первым рубежом охранной сигнализации, в зависимости от вида предполагаемых угроз объекту, блокируют:
 - деревянные входные двери, погрузочно-разгрузочные люки, ворота - на "открывание" и "разрушение" ("пролом");
 - остекленные конструкции - на "открывание" и "разрушение" ("разбитие") стекла;
 - металлические двери, ворота - на "открывание" и "разрушение",

- стены, перекрытия и перегородки, не удовлетворяющие требованиям настоящего Руководящего документа или за которыми размещаются помещения других собственников, позволяющие проводить скрытые работы по разрушению стены - на "разрушение" ("пролом"),
- оболочки хранилищ ценностей - на "разрушение" ("пролом") и "ударное воздействие";

- решетки, жалюзи и другие защитные конструкции, установленные с наружной стороны оконного проема - на "открывание" и "разрушение";
- вентиляционные короба, дымоходы, места ввода/вывода коммуникаций сечением более 200х200 мм - на "разрушение" ("пролом");
Вместо блокировки остекленных конструкций на "разрушение", стен, дверей и ворот на "пролом" и "ударное воздействие", допускается, в обоснованных случаях, производить блокировку указанных конструкций только на "проникновение" с помощью объемных, поверхностных или линейных извещателей различного принципа действия. При этом следует иметь в виду, что использование в данных целях пассивных оптико-электронных извещателей обеспечивает защиту помещений только от непосредственного проникновения нарушителя.

16. При невозможности блокировки входных дверей проемов (тамбуров) техническими средствами раннего обнаружения, необходимо в дверном проеме между основной и дополнительной дверью устанавливать охранные извещатели, обнаруживающие проникновение нарушителя. Данные извещатели следует включать в один шлейф охранной сигнализации блокировки дверей.

Для исключения возможных ложных срабатываний при взятии объекта под охрану указанный шлейф сигнализации необходимо выводить на ППК, имеющий задержку на взятие объекта под охрану.

17. Извещатели, блокирующие входные двери и не открываемые окна помещений, следует включать в разные шлейфы сигнализации, для возможности блокировки окон в дневное время при отключении охранной сигнализации дверей. Извещатели, блокирующие входные двери и открываемые окна допускается включать в один шлейф сигнализации.

18. Вторым рубежом охранной сигнализации защищаются объемы помещений на "проникновение" с помощью объемных извещателей различного принципа действия.

19. В помещениях больших размеров со сложной конфигурацией, требующих применение большого количества извещателей для защиты всего объема, допускается блокировать только локальные зоны (тамбуры между дверьми, коридоры, подходы к ценностям и другие уязвимые места).

20. Третьим рубежом охранной сигнализации в помещениях блокируются отдельные предметы, сейфы, металлические шкафы, в которых сосредоточены ценности.

21. Устанавливаемые в зданиях технические средства охраны должны вписываться в интерьер помещения и по возможности устанавливаться скрыто или маскироваться.
22. В разных рубежах необходимо применять охранные извещатели, работающие на различных физических принципах действия.
23. Количество шлейфов охранной сигнализации должно определяться тактикой охраны, размерами зданий, строений, сооружений, этажностью, количеством уязвимых мест, а также точностью локализации места проникновения для оперативного реагирования на сигналы тревоги.
24. Периметр охраняемого здания, как правило, следует разделять на охраняемые зоны (фасад, тыл, боковые стороны здания, центральный вход и другие участки) с выделением их в самостоятельные шлейфы сигнализации и выдачей отдельных сигналов на ППК или внутренний пульт охраны объекта.
25. Для усиления охраны и повышения ее надежности на объектах следует устанавливать дополнительные извещатели - ловушки. Сигналы ловушек выводятся по самостоятельным или, при отсутствии технической возможности, по имеющимся шлейфам охранной сигнализации.
26. Каждое помещение подгрупп АІ и АІІ (в соответствии с Р 78.36.032-2013) должно оборудоваться самостоятельными шлейфами охранной сигнализации. Помещения подгрупп БІ и БІІ (в соответствии с Р 78.36.032-2013), закрепленные за одним материально ответственным лицом, собственником или объединяемые по каким-либо другим признакам также должны оборудоваться самостоятельными шлейфами охранной сигнализации, причем, для удобства эксплуатации, одним шлейфом следует блокировать не более пяти соседних помещений, расположенных на одном этаже.
27. В помещениях, где круглосуточно должен находиться персонал, охранной сигнализацией должны оборудоваться отдельные участки периметра помещения, а также сейфы и металлические шкафы для хранения ценностей и документов.
28. Пропуск сотрудников и посетителей на объект через пункты контроля доступа следует осуществлять:
 - в здание и в служебные помещения - по одному признаку;
 - входы в зоны ограниченного доступа (хранилища ценностей, сейфовые комнаты, комнаты хранения оружия) - не менее чем по двум признакам идентификации.

Общие технические требования для проектирования автоматизированной системы контроля доступа:

1. АСКД должна обеспечивать выполнение следующих основных функций:
 - открывание УПУ (устройств преграждающих управляемых) при считывании идентификационного признака, доступ по которому разрешен в данную зону

доступа (помещение) в заданный временной интервал или по команде оператора АСКД;

- запрет открывания УПУ (устройств преграждающих управляемых) при считывании идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение) в заданный временной интервал;
 - санкционированное изменение (добавление, удаление) идентификационных признаков в УУ (устройств управления) и связь их с зонами доступа (помещениями) и временными интервалами доступа;
 - защиту от несанкционированного доступа к программным средствам УУ (устройств управления) для изменения (добавления, удаления) идентификационных признаков;
 - защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации;
 - сохранение настроек и базы данных идентификационных признаков при отключении электропитания;
 - ручное, полуавтоматическое или автоматическое открывание УПУ (устройств преграждающих управляемых) для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;
 - автоматическое закрытие УПУ (устройств преграждающих управляемых) при отсутствии факта прохода через определенное время после считывания разрешенного идентификационного признака;
 - выдачу сигнала тревоги (или блокировку УПУ (устройств преграждающих управляемых) на определенное время) при попытках подбора идентификационных признаков (кода);
 - регистрацию и протоколирование текущих и тревожных событий;
 - автономную работу считывателя с УПУ (устройств преграждающих управляемых) в каждой точке доступа при отказе связи с УУ (устройств управления).
2. На объектах, где необходим контроль сохранности предметов, следует устанавливать АСКД, контролирующую несанкционированный вынос данных предметов из охраняемых помещений или зданий по специальным идентификационным меткам.
3. УПУ (устройств преграждающих управляемых) с устройствами исполнительными должно обеспечивать:
- частичное или полное перекрытие проема прохода;
 - автоматическое и ручное (в аварийных ситуациях) открывание;
 - блокирование человека внутри УПУ (для шлюзов, проходных кабин);
 - требуемую пропускную способность.
4. Считыватели УВИП (устройств ввода идентификационных признаков) должно обеспечивать:
- считывание идентификационного признака с идентификаторов;

- сравнение введенного идентификационного признака с хранящимся в памяти или базе данных УУ;
- формирование сигнала на открывание УПУ при идентификации пользователя;
- обмен информацией с УУ.

УВИП должны быть защищены от манипулирования путем перебора или подбора идентификационных признаков.

Идентификаторы УВИП должны обеспечить хранение идентификационного признака в течении:

- всего срока эксплуатации - для идентификаторов без встроенных элементов электропитания;
- не менее 3 лет - для идентификаторов со встроенными элементами электропитания.

Конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию применяемых кодов.

5. УУ (устройств управления) должно обеспечивать:
 - прием информации от УВИП, ее обработку, отображение в заданном виде и выработку сигналов управления УПУ;
 - ведение баз данных сотрудников и посетителей объекта с возможностью задания характеристик их доступа (кода, временного интервала доступа, уровня доступа и другие);
 - ведение электронного журнала регистрации проходов сотрудников и посетителей через точки доступа;
 - приоритетный вывод информации о тревожных ситуациях в точках доступа;
 - контроль исправности и состояния УПУ, УВИП и линий связи с ними.
6. Конструктивно АСКД должны строиться по модульному принципу и обеспечивать:
 - взаимозаменяемость сменных однотипных технических средств;
 - удобство технического обслуживания и эксплуатации, а также ремонтпригодность;
 - исключение возможности несанкционированного доступа к элементам управления;
 - санкционированный доступ ко всем элементам, узлам и блокам, требующим регулирования, обслуживания или замены в процессе эксплуатации.

Общие технические требования для проектирования систем охранной телевидения и видеонаблюдения.

1. Системы охранного телевидения и видеонаблюдения (далее системы видеонаблюдения) должны обеспечивать передачу визуальной информации о состоянии охраняемых зон, помещений, периметра и территории объекта в помещение охраны. Применение охранного телевидения позволяет в случае получения извещения о тревоге определить характер нарушения, место

нарушения, направление движения нарушителя и определить оптимальные меры противодействия. Кроме того, система охранного телевидения позволяет проводить наблюдение охраняемых зон объекта.

2. В охране объектов должны использоваться системы цветного изображения.
3. В системах видеонаблюдения должно использоваться оборудование, приоритетно, российского производства.
4. Работа аппаратных средств систем видеонаблюдения должна быть синхронизирована.
5. Видеокамеры (в дальнейшем ВК), предназначенные для контроля территории объекта или ее периметра, должны иметь класс защиты не менее IP-65 и должны быть ориентированы на местности под углом к линии горизонта (лучи восходящего и заходящего солнца не должны попадать в объектив ВК). Размещение ВК должно препятствовать их умышленному повреждению.
6. В темное время суток, если освещенность охраняемой зоны ниже чувствительности ВК, объект (зона объекта) должен иметь встроенные источники или оборудоваться дополнительными источниками охранного освещения видимого или инфракрасного диапазона. Зоны охранного освещения должны совпадать с зоной обзора ТК.
7. Для наблюдения с помощью одной ВК больших территорий объекта рекомендуется применять объективы с переменным фокусным расстоянием либо ВК с поворотными устройствами с дистанционным управлением.
8. В помещениях объекта следует использовать ВК с электронным затвором, укомплектованные объективом с ручной регулировкой диафрагмы. Вне помещений объекта (на улице) следует применять ТК с автоматической регулировкой диафрагмы объектива.
9. В системах видеонаблюдения следует использовать обнаружители движения, либо интегрировать данные системы с системами охранной сигнализации таким образом, чтобы выдаваемый сигнал системой видеонаблюдения дублировался в систему охранной сигнализации и наоборот.
10. При необходимости записи телевизионных изображений должны применяться специализированные цифровые видеонакопители с объемом памяти, позволяющем вести круглосуточную запись видеoinформации как по детектору движения, так и в режиме реального времени, не менее 30 суток, с последующей перезаписью.
11. Время реагирования систем видеонаблюдения на сигнал извещения о тревоге должно быть не более времени, достаточного на преодоление нарушителем,двигающимся со скоростью 3 м/с, половины зоны наблюдения ВК по ширине, в любом месте зоны.
12. Устройства управления и коммутации должны обеспечивать приоритетное автоматическое отображение на экране мониторов зон, откуда поступило извещение о тревоге.

13. Конструктивно системы видеонаблюдения должны строиться по модульному принципу и обеспечивать:
- взаимозаменяемость сменных однотипных технических средств;
 - удобство технического обслуживания и эксплуатации, а также ремонтпригодность;
 - исключение несанкционированного доступа к элементам управления;
 - санкционированный доступ ко всем элементам, узлам и блокам, требующим регулирования, обслуживания или замены в процессе эксплуатации.

Общие технические требования для проектирования систем тревожного оповещения.

1. Оповещение людей, находящихся на объекте, должно осуществляться с помощью технических средств, которые должны обеспечивать:
 - подачу звуковых и/или световых сигналов в здания и помещения, на участки территории объекта с постоянным или временным пребыванием людей;
 - трансляцию речевой информации о характере опасности, необходимости и путях эвакуации, других действиях, направленных на обеспечение безопасности
2. Эвакуация людей по сигналам оповещения должна сопровождаться:
 - включением аварийного освещения;
 - передачей специально разработанных текстов, направленных на предотвращение паники и других явлений, усложняющих процесс эвакуации (скопление людей в проходах, тамбурах, на лестничных клетках и другие местах);
 - включением световых указателей направления и путей эвакуации;
 - дистанционным открыванием дверей дополнительных эвакуационных выходов (например, оборудованных электромагнитными замками).
3. Сигналы оповещения должны отличаться от сигналов другого назначения. Количество оповещаете, их мощность должны обеспечивать необходимую слышимость во всех местах постоянного или временного пребывания людей.
4. На охраняемой территории следует применять рупорные громкоговорители. Они могут устанавливаться на опорах освещения, стенах зданий и других конструкциях.

Правильность расстановки и количество громкоговорителей на территории определяется расчетом и уточняется на месте экспериментальным путем на разборчивость передаваемых речевых сообщений, но не менее одного 10-ваттного громкоговорителя на каждый участок территории.
5. Коммуникации систем оповещения в отдельных случаях допускается проектировать совмещенными с радиотрансляционной сетью объекта.
6. Управление системой оповещения должно осуществляться из помещения охраны, диспетчерской или другого специального помещения.

Общие технические требования для проектирования систем охранного освещения.

1. Периметр территории, здания охраняемого объекта должен быть оборудован системой охранного освещения согласно ГОСТ 12.1.046-2014.
2. Охранное освещение должно обеспечивать необходимые условия видимости ограждения территории, периметра здания, зоны отторжения, тропы наряда (путей обхода).
3. Система охранного освещения должна обеспечивать:
 - освещенность горизонтальную на уровне земли или вертикальную на плоскости ограждения, стены не менее 0,5 лк в темное время суток;
 - равномерно освещенную сплошную полосу шириной 3-4 м;
 - возможность автоматического включения дополнительных источников света на отдельном участке (зоне) охраняемой территории (периметра) при срабатывании охранной сигнализации;
 - ручное управление работой освещения из помещения КПП, помещения охраны,
 - совместимость с техническими средствами охранной сигнализации и охранного телевидения;
 - непрерывность работы на КПП, в помещении и на постах охраны.
4. Сеть охранного освещения по периметру объекта и на территории должна выполняться отдельно от сети наружного освещения и разделяться на самостоятельные участки в соответствии с участками охранной сигнализации периметра и/или охранного телевидения. Сеть охранного освещения должна подключаться к отдельной группе щита освещения, расположенного в помещении охраны или на КПП. Допускается установка щита освещения на внешней стене КПП со стороны охраняемой территории. Щит освещения должен быть закрыт на висячий (навесной) замок и заблокирован охранной сигнализацией.
5. Осветительные приборы охранного освещения могут быть любого типа: подвесные, консольные, прожектора и другие типы. В качестве источника света рекомендуется использовать лампы накаливания, либо энергосберегающие светодиодные прожекторы, напряжением 220 В.
6. Светильники охранного освещения по периметру территории должны устанавливаться не выше ограждения. Магистральные и распределительные сети охранного освещения территории объекта должны прокладываться, как правило, под землей или по ограждению в трубах. При невозможности выполнить данные требования воздушные сети охранного освещения должны располагаться достаточно глубоко на территории объекта, чтобы исключить возможность повреждения их из-за ограждения.
7. В ночное время охранное освещение должно постоянно работать. Дополнительное охранное освещение должно включаться только при

нарушении охраняемых участков в ночное время, а при плохой видимости и в дневное.

8. Лампы охранного освещения должны быть защищены от механических повреждений.

Общие технические требования для проектирования систем электропитания технических средств безопасности.

1. Установленные на объекте технические средства охраны следует относить к I категории электроприемников по надежности электроснабжения согласно ПУЭ, в силу чего их электропитание должно быть бесперебойным (либо от двух независимых источников переменного тока, либо от одного источника переменного тока с автоматическим переключением в аварийном режиме на резервное питание от аккумуляторных батарей).
2. Рабочий ввод электропитания, как правило, должен выполняться от электрической сети переменного тока напряжением 220 В.
3. Резервный ввод электропитания должен выполняться от одного из следующих источников питания или их любых сочетаний:
 - электрической сети переменного тока напряжением 220 В;
 - аккумуляторных батарей бесперебойных источников электропитания.
4. Электроснабжение технических средств охраны от электрической сети переменного тока осуществляется от отдельной группы электроцита дежурного освещения.
При отсутствии на объекте электроцита дежурного освещения или отдельной группы на нем, необходимо запроектировать самостоятельный электроцит на соответствующее количество групп. Помещение, в котором размещены электроциты, необходимо оборудовать охранной сигнализацией. Вне охраняемого помещения электроциты следует размещать в запираемых металлических шкафах, заблокированных охранной сигнализацией.
5. При использовании в качестве резервного источника питания аккумуляторных батарей источников бесперебойного электропитания, должна обеспечиваться работа систем охранной сигнализации, систем тревожного оповещения и автоматизированных систем контроля доступа в течение не менее 24 часов в дежурном режиме и в течение не менее 3 часов в режиме тревоги. Для систем охранного телевидения и видеонаблюдения - в течение не менее 4 часов в дежурном режиме и в течение не менее 1 часа в режиме тревоги, учитывая тот факт, что в режиме тревоги электропитание систем охранного телевидения и видеонаблюдения должно обеспечивать запись изображения от всех технических средств на цифровые носители в режиме реального времени.
6. Переход технических средств охраны на работу от резервного источника электропитания и обратно должен осуществляться автоматически без выдачи сигналов тревоги.

7. Линии электропитания, проходящие через незащищаемые охранной сигнализацией помещения, должны быть выполнены скрытым способом или открытым способом в трубах, коробах или металлорукавах.
8. Линии электропитания технических средств охраны периметра следует выполнять:
 - кабелями в траншее, в подземном коллекторе или открыто по внутренней стороне бетонного ограждения (стене здания) бронированными кабелями. В обоснованных случаях допускается прокладка небронированных кабелей (проводов) по внутренней стороне бетонного ограждения (стене здания) в стальных трубах и ПНД трубах с толщиной стенки не менее 2мм;
 - подвеской кабелей на тросе на высоте не менее 3 м или на отдельных участках в охраняемой зоне, при условии защиты кабеля от механических повреждений до высоты 2,5 м.
9. Соединительные или ответвительные коробки должны устанавливаться в охраняемых помещениях (зонах), и иметь класс защищенности не менее IP-54.
10. Защитное заземление или зануление технических средств охраны, соединительных и ответвительных коробок и других элементов должно соответствовать требованиям ПУЭ, СНиП 3.05.06-85, РД 78.145-93 (пособия к нему) и технической документации на изделия.

Общие технические требования для проектирования ip телефонии.

1. При проектировании ip телефонии согласовать применяемое оборудование с отделом слаботочных систем и телефонной связи Управления АСУТПиС.
2. IP-АТС должна отвечать следующим требованиям:
 - Поддерживать не менее 25 одновременных вызовов;
 - Иметь аналоговые порты FXO;
 - Поддерживать порты FXO/FXS при установке дополнительных модулей;
 - Поддерживать до GSM-порты (Quad-Band GSM/GPRS850/900/1800/1900 MHz) при установке дополнительных модулей;
 - Поддерживать UMTS-порты (UMTS 900/2100МГц или 850/2100МГц или 850/1900МГц) при установке дополнительных модулей;
 - Поддерживать BRI-порты при установке дополнительных модулей;
3. Иметь следующие функции:
 - Запись всех телефонных разговоров с возможностью хранения записей на внешнем жестком диске с последующим их копированием в сетевую папку файлового сервера;
 - Оповещение абонента о записи телефонного разговора;
 - Запись голосовой почты с возможностью хранения до 3000 минут голосовых сообщений на встроенной флеш-памяти;
 - Трансфер вызова;
 - Переадресация вызова;

- Парковка вызова;
- Захват вызова;
- Групповой вызов;
- Маршрутизация вызова;
- Режим ожидания;
- Оповещение (Paging Call);
- Интерком;
- Конференц-комнаты;
- Режим не беспокоить (DND);
- Очередь;
- Интерактивный голосовой автоответчик (IVR) с гибкой конфигурацией;
- Музыка в режиме ожидания (Music On Hold);
- Быстрый набор;
- Система внешнего доступа к линиям АТС (DISA - Direct Inward System Access);
- Личный кабинет пользователя;
- Отображение статуса абонента (BLF);
- Autoprovision;
- Доступ к линиям по PIN-коду;
- Привязка мобильного номера к внутреннему номеру абонента;
- Записная книга;
- Черный список;
- Детализация звонков (CDR);
- SIP SMS;
- Функция вмешательства (прослушивание, подсказка, вмешательство);
- Поддержка видео.
- Поддерживать не менее 64 внешних SIP-регистраций;
- Поддерживать не менее 64 транков;
- Поддерживать не менее 32 меню IVR;
- Поддерживать не менее 128 входящих/исходящих маршрутов;
- Поддерживать не менее 16 групп обзвона;
- Поддерживать не менее 16 очередей;
- Поддерживать VoIP-протоколы SIP 2.0 (RFC3261) и IAX2;
- Поддерживать транспортные протоколы UDP, TCP, TLS;
- Поддерживать аудиокодеки G.711, GSM, SPEEX, G.722, G.726, ADPCM, G.729A;
- Поддерживать видеокодеки H261, H263, H263p, H264, MPEG4;
- Поддерживать стандарты факсимильной связи T.30, T.37, T.38, G.711 Passthrough;
- Поддерживать режимы DTMF Inband, RFC2833, SIP INFO;
- Поддерживать следующие режимы работы с вычислительной сетью:
- Статический IP;

- Динамический IP;
- PPPoE.
- Иметь встроенный межсетевой экран;
- Иметь встроенный DHCP-сервер;
- Поддерживать функционал VLAN, DDNS, QoS;
- Иметь полностью русифицированный web-интерфейс управления;
- Иметь не менее 1 порта LAN 10/100/1000 Мб/с;
- Иметь не менее 1 порта WAN 10/100/1000 Мб/с;
- Иметь не менее 1 порта USB 2.0;
- Иметь не менее 1 порта audio in;
- Иметь не менее 1 порта audio out;
- Иметь форм-фактор для монтажа в серверную стойку шириной 19 дюймов;
- Иметь высоту не более 1U;
- Иметь энергопотребление не более 60 Вт;
- Иметь сертификат соответствия требованиям нормативных документов ГОСТ Р МЭК 60950-1-2009, ГОСТ Р 51318.22-99, ГОСТ Р 51318.24-99, ГОСТ Р 51317.3.2-2006 Разд. 6 и 7, ГОСТ Р 51317.3.3-2008;
- Иметь декларацию о соответствии требованиям ТР ТС 004/2011 и ТР ТС 020/2011;

ТРЕБОВАНИЯ К РАЗДЕЛУ СЕТИ СВЯЗИ

1. Общие положения

Для связи внутри объектов или между объектами, расположенными на территории подразделений АО "Мосводоканал" применяются локальные вычислительные сети (ЛВС). Для связи между территориально распределенными подразделениями и технологическими объектами АО "Мосводоканал" используется услуга организации защищенной сети предприятия и передачи данных по каналам L2/L3 VPN, предоставляемая провайдерами (операторами связи).

Провайдер, предоставляющий услуги передачи данных обеспечивает:

- гарантированную полосу пропускания;
- гарантированное качество обслуживания отдельных категорий сетевого трафика (QoS);
- уровень обслуживания согласно заявленным требованиям;
- дублирование и автоматизированное резервирование каналов связи, исключающее совпадение трасс каналов вплоть до входа в здание;
- поддержку MPLS L3 VPN.

Предоставляемые операторами каналы связи должны иметь Аттестат соответствия требованиям по безопасности информации по классу защищенности 1«Г» в части защиты от НСД к информации.

Операторы обязаны иметь точки присутствия на площадках РЦОД Общества и обеспечивать связь данных объектов с точкой обмена интернет-трафиком MSK-IX.

ЛВС территориально распределенных подразделений и технологических объектов реализуется на собственном оборудовании АО "Мосводоканал".

Все проектируемые локальные вычислительные сети объектов Общества должны иметь резерв по количеству возможных подключений к ним и по пропускной способности не менее 20%.

Все технические решения по архитектуре, применяемому оборудованию и материалам должны быть согласованы с УАСУТПиС АО "Мосводоканал".

2. Внутренние сети объектов

При проектировании создания или модернизации локальных вычислительных сетей объектов Общества (производственных и структурных подразделений) необходимо решать вопросы создания структурированной кабельной сети и обеспечения необходимым активным сетевым (телекоммуникационным) оборудованием (АСО).

Архитектура сети должна представлять собой иерархическую звезду, состоящую из набора медных кабелей неэкранированная витая пара UTP, коммутационных патч-панелей, патч-кордов, телекоммуникационных розеток и вспомогательного оборудования.

Пропускная способность сети должна позволять использовать ее для поддержки работы всех основных приложений, а также предоставлять возможность гибкого изменения конфигурации кабельной сети. Все компоненты компьютерной сети должны иметь характеристики передачи, соответствующие требованиям категории 5е.

Узлами архитектуры должны являться 19-дюймовый шкафы, функциональными элементами которых является активное коммутационное оборудование. Расположение узлов архитектуры обеспечивает физическую длину канала горизонтальной подсистемы, не превышающей 100 м.

В соответствии со стандартом ISO/IRC 11801 на каждом рабочем месте должно быть предусмотрено не менее двух телекоммуникационных розеток RJ-45. Телекоммуникационные информационные розетки должны соответствовать стандарту разъема RJ-45.

2.1. Структурированная кабельная система (СКС).

СКС должна состоять из:

- ✓ Горизонтальной подсистемы;
- ✓ Подсистемы коммутации;
- ✓ Подсистемы рабочих мест (конечных подключений).

Горизонтальная подсистема предназначена для связи Подсистемы коммутации с Подсистемой рабочих мест. При этом в качестве физической среды передачи данных используется:

- ✓ между зданиями, находящимися на территории АО "Мосводоканал" – одномодовые оптические каналы связи не менее, чем с восьмью волокнами;
- ✓ между зданиями в сложных условиях рельефа, при расстоянии более 8 км или при необходимости прокладывания каналов связи по территории, не принадлежащей АО "Мосводоканал" – радиорелейная связь;
- ✓ внутри зданий – витая пара категории не ниже 5е для подключения пользователей и серверов; оптические каналы могут применяться для межкоммутаторных соединений в зависимости от расстояния и условий эксплуатации.

Максимальная длина кабельных трасс горизонтальной подсистемы не должна превышать требований стандартов. Полоса пропускания должна обеспечить передачу данных со скоростью 1000 Мбит/с.

Подсистема коммутации обеспечивает: соединение кабельной системы с коммутационными панелями, а также коммутацию кроссового поля кабельной системы. Подсистема коммутации состоит из телекоммуникационного оборудования, 19- дюймовых патч-панелей, патч-кордов.

Подсистема рабочих мест (конечных подключений) служит для подключения оконечных устройств (компьютеров и другого сетевого оборудования). Подсистема рабочих мест должна состоять из комплектов монтажа розеток RJ-45 cat.5e.

2.2. Телекоммуникационное оборудование

Согласно принципам построения отказоустойчивых систем внутриобъектовой коммутации, требуется блок устройств и соединений, обеспечивающий сбалансированное и отказоустойчивое прохождение трафика между всеми пользователями вычислительных сетей, серверами, вспомогательными системами (такими как IP-телефоны, IP-камеры видеонаблюдения, терминалы ВКС и т.д.).

Активное сетевое (телекоммуникационное) оборудование должно обеспечить реализацию и взаимодействие со следующими существующими логическими подсетями:

- ✓ пользовательская;
- ✓ серверная;
- ✓ АСУТП;
- ✓ IP-телефония;
- ✓ СКУД и СВН;
- ✓ ВКС.

В качестве типового оборудования для построения подсистемы коммутации и маршрутизации используется следующее оборудование:

- ✓ Коммутаторы ядра – два коммутатора, объединяемых в стек для обеспечения отказоустойчивого подключения коммутаторов доступа и серверного оборудования;
- ✓ Коммутаторы доступа – с 24 или 48 портами 10/100/1000 Мбит/с. Для подключения IP телефонов и другого оборудования, работающего по стандарту 802.3af, используются модели с поддержкой PoE и функционалом LAN Base. Для подключения рабочих мест пользователей используются модели с функционалом LAN Lite.
- ✓ Пограничные коммутаторы обеспечивают отказоустойчивое взаимодействие между пограничными маршрутизаторами и межсетевыми экранами. Оборудование операторов связи также подключается к данным коммутаторам.
- ✓ Межсетевые экраны объединяются в отказоустойчивый кластер (failover) по принципам Active/Standby.

Оборудование СКС и телекоммутационное оборудование должно размещаться в напольном 19-дюймовом шкафу, размещаемом в специализированном серверном помещении.

Защитное заземление (зануление) кабельных каналов и оборудования должно быть выполнено в соответствии с требованиями ПУЭ, СНиП 3.05.06-85, ГОСТ 12.1.030-81, технической документацией предприятий-изготовителей на данное оборудование.

3.Подключение объектов к корпоративной вычислительной сети (КВС)

Корпоративная вычислительная сеть обеспечивает информационный обмен между компонентами ИТ-инфраструктуры, автоматизированными информационными системами и пользователями Общества. КВС предназначена для организации единого информационного пространства для обеспечения бизнес- и технологических процессов компании. КВС обеспечивает: гибкость, мультисервисность, отказоустойчивость и расширяемость для сервисов, работающих по протоколу IPv4 (в перспективе и IPv6)

В зависимости от типа и роли объекта выбирается способ подключения его к КВС.

К объектам первого типа АО "Мосводоканал" относятся крупные производственные подразделения: водопроводные станции (РСВ, ЗСВ, ВСВ, ССВ), очистные сооружения (КОС, ЛОС), отдельные производственные управления (ЗВК, ТиНАО), районы водопроводной (РЭВС) и канализационной (РКС) сети. Такие объекты должны быть подключены к КВС по волоконно-оптическим линиям связи (ВОЛС) на скорости не менее 100 Мбит/с со 100% "горячим" резервированием.

К объектам первого типа АО "Мосводоканал" относятся регулирующие водопроводные узлы, высоковольтные насосные станции и ряд других объектов находящихся в режиме автоматического управления и контроля, оснащенных местными диспетчерскими пунктами управления. Такие объекты должны быть подключены к КВС по волоконно-оптическим линиям связи (ВОЛС) на скорости не менее 30 Мбит/с (определяется фактической информационной мощностью объекта и оснащенностью различными автоматизированными системами) со 100% "горячим" резервированием, допускающим резервирование по беспроводным (сотовым) каналам связи.

К объектам третьего типа относятся все автономные небольшие производственные объекты и точки контроля без диспетчерского или дежурного персонала (канализационные станции, водозаборные узлы, отдельные скважины, регулирующие камеры, точки контроля параметров городской водопроводной и канализационной сети и т.п.). Для таких объектов приоритетным является подключение к КВС по волоконно-оптическим линиям связи (ВОЛС) на скорости не менее 2 Мбит/с (определяется фактической информационной мощностью объекта и

оснащенностью различными автоматизированными системами) со 100% "горячим" резервированием по беспроводным (сотовым) каналам связи. Допускается применение также основного беспроводного (сотового) канала связи.

4.Создание серверных помещений

Требования составлены на основании следующих документов:

3.1. ГОСТ 2.051-2013 "Единая система конструкторской документации. Электронные документы. Общие положения" (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. N 1628-ст).

3.2. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

3.3. ГОСТ 34.201-89 Комплекс стандартов на автоматизированные системы. Виды комплексность и обозначение документов при создании автоматизированных систем.

3.4. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

3.5. ГОСТ 34.602-89 Информационная технология Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

3.6. ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем.

3.7. Национальный стандарт РФ ГОСТ Р 50839-2000 "Совместимость технических средств электромагнитная. Устойчивость средств вычислительной техники и информатики к электромагнитным помехам. Требования и методы испытаний" (введен в действие постановлением Государственного комитета РФ по стандартизации и метрологии от 26 декабря 2000 г. N 416-ст).

3.8. СНиП 21-01-97 "Пожарная безопасность зданий и сооружений" Госстроя России.

3.9. Изменение N 2 СН 512-78 "Инструкция по проектированию зданий и помещений для электронно-вычислительных машин" (принято постановлением Госстроя РФ от 24 февраля 2000 г. N 17).

3.10. Инструкция по устройству молниезащиты зданий и сооружений РД 34.21.122-87 (утв. Главтехуправлением Минэнерго СССР 12 октября 1987 г.).

3.11. EIA/ TIA-568B - стандарт по проводке в коммерческих зданиях, определяет кабельную систему, которая поддерживает активное оборудование от различных производителей.

3.12. EIA/TIA-569 – Требования к серверному помещению.

3.13. Требования по электроснабжению, электротехническим устройствам и заземлению средств автоматизации технологических процессов и слаботочных систем.

3.14. СН 512-78 "Инструкция по проектированию зданий и помещений для электронно-вычислительных машин"

3.15. СП 4.13130.2013 "Свод правил. Системы противопожарной защиты. Ограничение распространения пожара на объектах защиты"

3.16. СП 5.13130.2009 "Свод правил. Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические нормы и правила проектирования"

3.17. Правила противопожарного режима в Российской Федерации.

3.18. СП 3.13130.2009 "Свод правил. Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности"

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К СЕРВЕРНОМУ ПОМЕЩЕНИЮ

4.1. Выбор серверного помещения

4.1.1. Серверное помещение рекомендуется размещать как можно ближе к магистральным кабельным каналам. Желательно расположить серверное помещение рядом с главным распределительным пунктом (Main Cross, MC), а если есть возможность, то установить главный распределительный пункт в серверном помещении. Не допускается размещение серверного помещения рядом с лифтовыми шахтами, лестничными пролетами, вентиляционными камерами и другими элементами здания, которые могут ограничить расширение аппаратного помещения в будущем.

4.1.2. Серверное помещение рекомендуется размещать так, чтобы была возможность расширения серверного помещения за счет площади смежного помещения.

4.1.3. Размер серверного помещения выбирается исходя из размера обслуживаемой рабочей области и количества устанавливаемого оборудования. Важно учесть не только размеры самого оборудования, но и способы монтажа, обеспечения доступа и обслуживания оборудования, возможность установки дополнительных устройств. Высота серверного помещения должна быть не менее 2,5 метра. Минимально рекомендуемый размер серверной должен быть не менее

14 м².

4.1.4. Несущие конструкции здания в помещении серверной, где планируется размещение оборудования, должны выдерживать расчетную нагрузку, включающую вес компьютерного и телекоммуникационного оборудования, обслуживающего персонала, оборудования систем инфраструктуры.

4.2. Требования к отделке серверного помещения

Стены, потолок, и пол должны иметь покрытие, которое затрудняет выделение, оседание и накапливание пыли на поверхности. Потолок должен иметь гидроизоляцию, чтобы исключить протечку воды. Стены должны быть окрашены светлой краской.

Допускается использование подвесных потолков для возможности размещения над подвесным потолком воздуховодов и воздухораспределителей, аппаратуры потолочных люминесцентных светильников, установок газового пожаротушения.

В серверном помещении запрещается использование ковровых покрытий.

4.3. Требования к фальшполу

4.3.1. Наличие фальшпола и использования прецизионных кондиционеров в серверной обоснованно при суммарной тепловой нагрузке от технологического оборудования не менее 10 кВт (4 стойки).

4.3.2. Просвет между фальшполом и потолком должен быть не менее 2,5 м.

4.3.3. Расстояние между строительным полом и фальшполом должно быть не менее 200 мм (рекомендуемое 400 мм).

4.3.4. Крутизна устанавливаемого на входе в серверную пандуса не должна превышать значение 1:10.

4.3.5. Конструкция фальшпола должна выдерживать расчетные нагрузки и состоять из легко съемных модулей (плиток). При этом необходимо учитывать то, что отдельные устройства вычислительной системы могут создавать точечную нагрузку на пол до 455 кг.

6.3.6. Материал покрытия фальшпола должен иметь электрическое сопротивление относительно земли от 1,0 МОм (минимум) до 20 МОм (максимум) при изменениях относительной влажности от 20 до 60% и температуры от +18 до +24°C, а также обладать повышенной износостойкостью, плохой возгораемостью, повышенной стойкостью к царапанью и выкрашиванию.

4.3.7. Поверхности под фальшполом должна окрашиваться или герметизироваться для предотвращения отслаивания и пыления штукатурки или бетона перекрытия.

4.3.8. В строительном перекрытии под фальшполом обязательно необходимо сделать дренаж для оттока воды в случае аварийного протекания.

4.3.9. Конструкция съемного пола должна обеспечивать:

- свободный доступ к коммуникациям при обслуживании;
- устойчивость к горизонтальным усилиям при частично снятых плитах;
- возможность выравнивания поверхностей пола с помощью регулируемых опорных элементов;
- взаимозаменяемость плит съемного пола.

4.3.10. Конструкция съемного пола должна быть рассчитана на равномерно распределенную нормативную нагрузку 1000 кг/м^2 и сосредоточенную нормативную нагрузку 250 кг, приложенную в любом месте плиты на площади 25 см^2 . Прогиб плиты не должен превышать 1 мм.

4.3.11. Плиты съемного пола в собранном состоянии должны плотно прилегать друг к другу, обеспечивая герметичность в стыках.

4.3.12. Плиты съемного пола должны быть трудносгораемыми, с пределом огнестойкости не менее 0,5 ч, или несгораемыми. Опоры и стойки съемных полов должны быть несгораемыми. Покрытие плит пола допускается предусматривать из сгораемых материалов.

Покрытие плит пола должно быть гладким, прочным, антистатическим, позволяющим выполнять уборку пола пылесосом или влажную уборку. Конструкция плит должна обеспечивать стекание и отвод электростатического электричества.

Расположение отверстий в плитах для прокладки соединительных кабелей, заземления, воздухопроводов централизованного охлаждения устройств следует определять по месту установки устройств в соответствии с технологическими планами размещения ЭВМ и техническими характеристиками устройств.

4.4. Требования к прокладке коммуникаций

4.4.1. В помещении серверной не должно проходить никаких магистралей и ответвлений инженерных систем, включая общую хозяйственную канализацию, холодное и горячее водоснабжение, общую вентиляцию и кондиционирование, распределительная сеть электропитания и освещение, и другие слаботочные системы, за исключением систем, располагаемых в самой серверной.

4.4.2. В зданиях и помещениях ЭВМ с односменным и двухсменным режимом работы следует предусматривать центральное водяное отопление в сочетании с приточной вентиляцией или кондиционированием воздуха.

4.4.3. Отопление помещений с трехсменным режимом работы, как правило, проектируется воздушным.

4.4.4. Расчет водяных систем отопления помещений, в которых предусматривается кондиционирование воздуха, следует производить на поддержание внутренней температуры воздуха 17°C.

4.4.5. В помещениях, внешних запоминающих устройств, графопостроителей и графоповторителей, сервисной аппаратуры, подготовки данных, архивов машинных носителей, вскрытия и обработки дисков, барабанов и лент должна предусматриваться возможность отключения системы отопления.

4.4.6. Температура на поверхности нагревательных приборов в зданиях и помещениях для ЭВМ не должна превышать 95°C.

4.4.7. Нагревательные приборы, устанавливаемые в зданиях и помещениях для ЭВМ, должны иметь гладкую, легко очищаемую поверхность.

4.4.8. В помещениях, которые должны иметь гидроизоляцию, не допускается наличие разъемных соединений и размещение запорной и регулирующей арматуры на трубопроводах систем отопления.

4.5. Химическое воздействие

Содержание в воздухе серверного помещения загрязняющих веществ не должно превышать следующих предельных значений:

- Хлор – 0,01%;
- Сероводород – 0,05%;
- Окислы азота – 0,1%;
- Двуокись серы – 0,3%;
- Углеводороды – 4×10^{-6} (г/м³) в сутки.

ТРЕБОВАНИЯ К ИНФРАСТРУКТУРЕ СЕРВЕРНОГО ПОМЕЩЕНИЯ

В помещении серверной должны быть установлены следующие системы:

4.6. Система электропитания, освещения и заземления (СЭ), включающая в себя:

4.6.1. Подсистема гарантированного электропитания (ПГЭ):

ПГЭ предусматривает наличие двух вводов электропитания от разных электроподстанций. Оба источника электроэнергии подаются на автомат ввода резерва (АВР), осуществляющий автоматическое переключение фидеров при пропадании электропитания на основном (резервном) фидере. Параметры линий электропитания АВР определяются исходя из суммарной потребляемой мощности оборудования и подсистем серверной. Линии внешнего электропитания должны быть выполнены по пятипроводной схеме с жилами неравного сечения. Вывод информации состояния и срабатывания АВР со звуковой и световой индикацией о пропадании электроэнергии.

4.6.2. Подсистема бесперебойного электропитания (ПБЭ):

ПБЭ предусматривает электроснабжение оборудования и систем серверной через источники бесперебойного питания (ИБП). Мощность и конфигурация ИБП рассчитывается с учетом всего запитываемого оборудования и запаса для будущего развития. Время автономной работы от ИБП рассчитывается с учетом потребностей, а так же с учетом необходимого времени для перехода на резервные линии (не менее 20 минут) и обратно. ИБП должен обеспечивать не менее 30% запаса по мощности для развития оборудования серверной.

4.6.3. Подсистема технологического заземления (ПТЗ):

В помещении серверной должно быть обеспечено наличие контура заземления. Сопротивление технологического заземления должно быть менее 1 Ом. Присоединение технологического заземления к защитному заземлению здания производится непосредственно у защитных электродов, расположенных в грунте. Все металлические части и конструкции серверной должны быть заземлены. Каждый шкаф (стойка) с оборудованием заземляется отдельным проводником. Не сварные металлические конструкции серверной должны иметь заземляющие шайбы в болтовых соединениях, улучшающие электрический контакт между частями конструкции.

4.6.4. Подсистема электрического освещения (ПЭО)

Освещенность помещения серверной определяется в соответствии с *Таблицей 4* СН 512-78 "Инструкция по проектированию зданий и помещений для электронно-вычислительных машин". Для освещения серверной допустимо применять светильники с люминесцентными или светодиодными лампами. Применение газоразрядных ламп не рекомендовано из-за наличия электромагнитных помех при их работе. Питание ПЭО осуществляется от системы гарантированного электропитания серверной.

4.7. Система кондиционирования (СК)

В помещении серверной должны соблюдаться следующие климатические условия:

- Температура воздуха в помещении: 18-24°C;
- Допустимые отклонения температуры: +/-2°C;
- Относительная влажность воздуха: 40-50%;
- Точность поддержания влажности: +/-1%.

Фактическая холодильная мощность системы кондиционирования воздуха должна превышать суммарное тепловыделение всего оборудования и систем, размещенного в помещении серверной. Система кондиционирования должна обеспечивать возможность удаленного мониторинга (с использованием протоколов

HTTP, SNMP). Электропитание кондиционеров серверной должно осуществляться от ПГЭ или ПБЭ.

Кондиционирование серверных помещений рационально иметь с показателем 50 - 100% резервирования.

Для небольшой серверной, где теплопритоки составляют от 3 до 10 кВт необходимо использовать промышленную высоконадежную сплит-систему, оснащённую низкотемпературным комплектом, позволяющим использовать кондиционер в режиме "охлаждения" при температурах наружного воздуха ниже нулевой отметки.

При работе системы кондиционирования при температурах наружного воздуха до -30°C в ней должно быть предусмотрено:

- обогрев картера компрессора для улучшения вязкости масла и устранения эффекта "вскипания" хладагента при пуске;
- уменьшение потока воздуха через теплообменник наружного блока чиллера для стабилизации давления конденсации.

Наиболее эффективным решением для кондиционирования серверных помещений, где теплоприток более 10 кВт являются прецизионные системы кондиционирования со свободным охлаждением. В соответствующих случаях с дублирующей системой кондиционирования и вентиляции.

Прецизионные кондиционеры представляют собой специализированные системы кондиционирования серверных помещений, способные с большой точностью поддерживать требуемую температуру и влажность круглый год. Также осуществляется очистка воздуха. Таким образом, в помещении образовывается идеальная атмосфера для функционирования стоек с дорогостоящим оборудованием.

4.8. Система организации оборудования и кабельного хозяйства (СО), включающая в себя:

4.8.1. Средства распределения кабелей и организации кабельных потоков

Для распределения кабелей и организации кабельных потоков в телекоммуникационном помещении необходимо использовать кабелепроводы и организаторы.

Средства распределения и организации кабельных потоков должны быть надёжно закреплены, выдерживать вес кабеля, должны обеспечить защиту и распределение кабелей с минимально допустимым радиусом изгиба кабеля.

Кабелепроводы должны быть установлены от кабельного ввода в телекоммуникационное помещение до телекоммуникационных шкафов. Кабелепроводы расположенные под потолком, должны быть открыты и доступны

для проведения дальнейших работ по прокладке кабелей, шнуров или перемычек.

Для упрощения коммуникаций и исключения поломки разъемов оборудования, необходимо применять патч-панели. Все кабели, кроссовые коммуникации и патч-панели должны иметь маркировку, позволяющую однозначно идентифицировать каждый кабель (разъем, порт).

4.8.2. Подсистема телекоммуникационных шкафов и стоек (ПШС)

Все оборудование серверной размещается в закрытых шкафах или открытых стойках. Количество стоек (шкафов) определяется исходя из имеющегося оборудования и его типоразмеров, способов монтажа. Промежутки между шкафами не допускаются. Распределение оборудования по шкафам (стойкам) осуществляется с учетом совместимости (возможного взаимного влияния), оптимального распределения потребляемой мощности (а значит и тепловыделения), оптимальности коммуникаций, габаритам и массе оборудования. Вводные каналы в телекоммуникационные шкафы и стойки должны обеспечивать свободную протяжку требуемого количества кабелей вместе с оконечными разъемами.

4.9. Система безопасности (СБ), включающая в себя:

4.9.1. Подсистема контроля доступа (ПКД)

Подсистема контроля и управления доступом должна исключить попадание в серверную лиц, в чьи обязанности не входит монтаж, эксплуатация и техническое обслуживание размещённого в серверной оборудования. Для идентификации допущенных лиц применяются следующие средства:

- Ключи от механических замков;
- Кодонаборные панели;
- Карты и метки электронной идентификации;
- Комбинация вышеперечисленных методов.

Для блокирования доступа в помещение могут применяться:

- Механические замки;
- Электромеханические замки;
- Электромагнитные замки;
- Комбинация вышеперечисленных средств.

4.9.2. Подсистема охранной сигнализации (ПОС)

Охранная сигнализация серверной должна быть выполнена отдельно от систем безопасности здания. Сигналы оповещения выводятся в помещение круглосуточной охраны в виде отдельного пульта. Дополнительно сигналы оповещения могут доставляться средствами связи: телефон, СМС, пейджер. Контролю и охране подлежат все входы и выходы серверной, объем помещения,

оконные проемы (если есть). ПОС должна иметь собственный источник резервированного питания.

4.9.3. Подсистема видеонаблюдения (ПВН)

Система охранного видеонаблюдения предназначена для визуального наблюдения и фиксации текущей обстановки в помещениях серверной. Камеры необходимо разместить таким образом, чтобы контролировать входы и выходы в помещение, пространство возле технологического оборудования (ИБП, кондиционеры, серверные шкафы и телекоммуникационные стойки). Разрешения видеокамер должно быть достаточным, чтобы уверенно различать лица сотрудников, обслуживающих технологическое оборудование. Видеокамеры должны быть снабжены светодиодной подсветкой для наблюдения в темноте.

При построении системы охранного видеонаблюдения серверной глубина хранения видеоархива должна быть не менее 14 дней. В случае если ёмкости видеосервера не достаточно для реализации такой глубины сохранения архива, то необходимо предусмотреть увеличение дискового массива основного сервера при помощи добавления к нему дополнительных полок с дисками.

4.9.4. Подсистема пожарной сигнализации (ППС)

Помещение серверной, не зависимо от площади, необходимо оборудовать пожарной сигнализацией. В случае наличия пожарной сигнализации в остальном здании необходимо предусмотреть интеграцию пожарной сигнализации помещения серверной с пожарной сигнализацией и системой оповещения и управления эвакуацией людей (СОУЭ) здания. При не возможности интеграции пожарной сигнализации помещения серверной допускается вывести сигнал на отдельный пульт управления в помещения с круглосуточным пребыванием персонала, но так же необходимо произвести коммутацию системы пожарной сигнализации помещения серверной и СОУЭ здания.

В помещение серверной, как правило, применяют дымовые пожарные извещатели. Извещатели должны контролировать как общее пространство помещений, так и полости, образованные фальшполом и фальшпотолком. Сигналы оповещения ППС дополнительно выводятся в SCADA- систему и на входную дверь. ППС может быть объединена с ПОС серверной.

С целью предотвращения распространения очага пожара помещение серверной необходимо отделять от остальных помещений противопожарной перегородкой 1-го типа (противопожарная дверь с пределом огнестойкости не менее 60 минут).

4.9.5. Подсистема газового пожаротушения (ПГП)

Помещения серверных площадью более 24 м² должны оборудоваться автоматической системой газового пожаротушения (АУГП). ПГП размещается

непосредственно в помещении серверной (или вблизи ее) в специально оборудованном для этого шкафу. Запуск ППП производится от датчиков раннего обнаружения пожара, реагирующих на появление дыма, а также от ручных пожарных извещателей, расположенных у входа в помещение или с пульта управления в ручном режиме. ППП должна иметь световые табло оповещения о срабатывании тушения, размещаемые внутри и снаружи помещения. Звуковой оповещатель располагается снаружи у входа в серверное помещение. Кабели и способы их прокладки должны соответствовать требованиям СП 5.13130.2009 п. 13.15.3 и ГОСТ Р 53315 и ГОСТ Р 53325. Необходимо использовать огнестойкие кабели и провода типа НГ-FRLS или НГ-FRHF.

4.9.6. Подсистема газо и дымоудаления (ПГУ)

Подсистема должна обеспечивать отвод газовоздушной смеси от автоматической системы газового пожаротушения в объеме, втрое превышающем объем серверной. Допускается использование переносных дымососов.

4.10. Требования пожарной безопасности к серверным помещениям

4.10.1. Помещения серверных должны выделяться противопожарными перегородками не ниже 1-го типа и перекрытиями не ниже 3-го типа.

4.10.2. Помещения серверной площадью 24 м² и более должны быть защищены установкой автоматического пожаротушения, а площадью менее 24 м² системой автоматической пожарной сигнализации.

4.10.3. Помещения серверной должны оснащаться системой оповещения и управления эвакуацией при пожаре.

4.10.4. Помещения должны оснащаться огнетушителями.

4.10.5. Двери помещений серверной должны быть противопожарными.