

Государственное унитарное предприятие Республики Башкортостан
«Уфаводоканал»
(ГУП РБ Уфаводоканал)

УТВЕРЖДАЮ
Главный инженер

П.В. Серебряков
«__» _____ г.

**Построение локальной вычислительной сети объекта, подключение к
корпоративной сети ГУП РБ «Уфаводоканал»**

**Общие технические условия
на подраздел «Сети связи»**

2024г.

Содержание

1. Область применения	3
2. Используемые сокращения	3
3. Требования к составу работ	3
4. Требования к структуре и функционированию	4
5. Требования к оборудованию	5
6. Требования к сетевой безопасности	6
7. Требования к выполнению работ	7
8. Требования к безопасности	9
9. Правила приемки	9
10. Методы контроля	10
11. Транспортирование и хранение	10
12. Указания по эксплуатации	10
13. Гарантии изготовителя	10

1. Область применения.

1.1. Настоящий документ устанавливает требования к локальной вычислительной сети канализационной насосной станции и её подключению к корпоративной сети предприятия.

1.2. Настоящий документ распространяется на локальную вычислительную сеть канализационной насосной станции, на подключение локальной вычислительной сети канализационной насосной станции к корпоративной сети предприятия, на компоненты, используемые в составе локальной вычислительной сети и для подключения локальной вычислительной сети к корпоративной сети предприятия.

1.3. Настоящий документ предназначен для применения организациями и предприятиями, осуществляющими проектирование, разработку, изготовление, монтаж, наладку, эксплуатацию локальной вычислительной сети и подключения к корпоративной сети на канализационных насосных станциях ГУП РБ "Уфаводоканал".

2. Используемые сокращения

Объект - объект информатизации.

ЛВС - локальная вычислительная сеть.

Корпоративная сеть - единая компьютерная вычислительная сеть ГУП РБ "Уфаводоканал".

ПЛК - производственно-лабораторный комплекс ГУП РБ "Уфаводоканал".

АСУТП - автоматизированная система управления технологическими процессами.

ТЗ - техническое задание.

VPN (Virtual Private Network) - сетевая технология, обеспечивающая построение одной логической сети поверх другой.

3. Требования к составу работ

3.1. Для организации телекоммуникационной структуры на Объекте создается локальная вычислительная сеть. ЛВС обеспечивает возможность сетевого взаимодействия оборудования Объекта.

Для удаленной передачи телеметрической информации и сигналов управления технологическим процессом Объекта с/на диспетчерский пункт, Объект подключается к корпоративной сети предприятия. Подключение Объекта к корпоративной сети включает в себя организацию внешней линии связи и оборудование Объекта шлюзом доступа к корпоративной сети.

3.2. ЛВС Объекта и подключение Объекта к корпоративной сети должно соответствовать требованиям настоящих технических условий согласно техническому заданию на проектирование и разработку Объекта.

3.3. Состав работ.

- Подрядчик разрабатывает проектную документацию, содержащую разделы по построению ЛВС Объекта и подключению к корпоративной сети. В процессе проектирования Подрядчик согласовывает с ГУП РБ "Уфаводоканал" сетевую адресацию и требуемую пропускную способность внешнего канала связи.

- Проектная документация согласуется с ГУП РБ “Уфаводоканал”.
- Подрядчик выполняет поставку оборудования и монтажные работы.
- Подрядчик разрабатывает исполнительную документацию.

4. Требования к структуре и функционированию.

4.1. ЛВС Объекта должна обеспечивать возможность сетевого взаимодействия следующего оборудования:

- Логического контроллера (PLC);
- Расходомеров в составе с преобразователями интерфейсов (при наличии);
- IP-видеокамер (при наличии);
- Оборудования охранной сигнализации в составе с преобразователями интерфейсов (при наличии);
- Шлюза доступа в корпоративную сеть;
- Портативного персонального компьютера для отладки (временно);

ЛВС должна строиться по стандарту Fast Gigabit Ethernet

ЛВС должна иметь топологию “звезда” с единым центром коммутации.

ЛВС должна поддерживать круглогодичный и круглосуточный режим работы.

4.2. Кабельная система ЛВС должна поддерживать скорость передачи данных 1 Гбит/с. Для построения кабельной системы должен применяться медный кабель типа “витая пара”, категории 5е и выше.

Разводка кабельной системы ЛВС должна быть преимущественно сконцентрирована в шкафу (стойке) оборудования АСУТП Объекта и выполнена с использованием возможностей шкафа по организации кабельной структуры. При прокладке кабелей вне шкафа АСУТП должны быть приняты меры по защите кабелей (кабель каналы, трубы и т.п.). Для прокладки кабелей на открытом воздухе должна применяться специально предназначенная для этого марка кабеля.

Все концы кабелей должны быть промаркированы в соответствии с документацией.

4.3. Подрядчик оборудует Объект внешним каналом связи компании провайдера, имеющего подключение к ПЛК предприятия и обеспечивающего необходимую пропускную способность. В настоящее время подключение к ПЛК предприятия имеют АО “Уфанет” (Ethernet). Необходимая пропускная способность внешнего канала связи определяется процедурой согласования пропускной способности внешнего канала связи на этапе проектирования Объекта Подрядчиком совместно со специалистами группы сетевого администрирования ГУП РБ “Уфаводоканал”. Внешний канал связи должен иметь круглогодичный и круглосуточный режим работы, предусмотренный договором с фирмой-провайдером.

4.4. Для осуществления прозрачной маршрутизации и защиты сетевого оборудования Объекта от несанкционированного доступа, Объект оборудуется шлюзом корпоративной сети, включаемым между ЛВС Объекта и сетью провайдера.

4.5. В настоящее время для подключения Объекта к корпоративной сети используется следующая схема: шлюз корпоративной сети Объекта по необходимости устанавливает

защищенные соединения через внешний канал связи с другими шлюзами корпоративной сети предприятия. Все пакеты (за исключением заблокированных сетевым экраном) ЛВС Объекта маршрутизируются в установленный VPN канал. . Таким образом достигается единое прозрачное сетевое взаимодействие для всех Объектов.

4.6. Взаимодействие всех Объектов накладывает ограничения на пропускную способность канала связи Объекта - сумма пропускных способностей каналов связи всех Объектов не может быть больше пропускной способности канала связи шлюза, принимающего запросы с учетом загрузки канала связи другими потребителями корпоративной сети.

4.7. Специалисты группы сетевого администрирования предприятия оставляют за собой право изменять топологию корпоративной сети, а также использовать автоматические способы маршрутизации в зависимости от загрузки каналов связи или требований к отказоустойчивости.

4.8. "Прозрачная" организация корпоративной сети накладывает дополнительные требования на организацию защиты ЛВС Объекта от внутренних нарушителей. Организация защиты требует установки и настройки межсетевого экрана на шлюзе корпоративной сети .

5. Требования к оборудованию.

5.1. В качестве коммутатора ЛВС должен быть применён управляемый коммутатор 2 уровня стандарта 1000BASE-T с возможностью установки в стандартную 19" телекоммуникационную стойку. Коммутатор должен обеспечивать подключение всего сетевого оборудования Объекта с резервом в 3 свободных порта. Коммутатор должен поддерживать следующие технологии:

- поддержка протокола восстановления сетевой топологии Spanning tree protocol STP/RSTP для обнаружения и предотвращения колец в логической топологии сети,
- поддержка стандарта IEEE802.1Q VLAN-виртуальная локальная сеть,
- поддержку возможности обновления встроенного программного обеспечения,
- поддержка возможности загрузки и сохранения конфигурации,
- поддержка протокола управления и мониторинга SNMP v1,v2,v3,
- регистрацию событий на внешний сервер по протоколу syslog,
- поддержка удаленного управления через telnet, ssh, web-console

Предпочтение должно быть отдано выбору устройства с пассивной вентиляцией.

5.2. Для шлюза корпоративной сети должно выбираться оборудование обеспечивающее маршрутизацию сетевых пакетов протокола IP, имеющее 2 или более сетевых интерфейса с разным назначением, один для внешней сети провайдера, тип зависит от физической среды передачи внешней сети, и второй порт (или несколько коммутируемых портов) для внутренней ЛВС.

В качестве шлюза корпоративной сети на может быть применено следующее оборудование:

Производитель	Наименование	Аппаратная ревизия*
Маршрутизационное оборудование бренда Mikrotik с пропускной способностью портов 1000 Мбит/с с количеством портов не менее 4-х		

* способы определения аппаратной ревизии оборудования приводятся на web-сайте производителя в разделе “Поддержка”.

За поддержкой в выборе оборудования сетевого шлюза Объекта, Вы можете обратиться к специалистам группы сетевого администрирования предприятия.

5.3. Оборудование шлюза, коммутатор должны монтироваться в единый шкаф АСУТП Объект.

5.4. Электроснабжение сетевого оборудования (шлюза, коммутатора ЛВС) должно производиться от резервированного источника питания имеющего возможность удаленного мониторинга состояния (работа от сети/батарей). Удаленный мониторинг состояния источника бесперебойного электропитания интегрируется в систему АСУТП Объекта.

6. Требования к сетевой безопасности.

6.1. Требования к сетевой безопасности обусловлены наличием угроз несанкционированного доступа к оборудованию Объекта со стороны нарушителя и возможными рисками предприятия в результате реализации данных угроз.

6.2. При разработке модели безопасности объекта следует принимать во внимание наличие 2х категорий нарушителей: внешних и внутренних. В качестве внешнего нарушителя принимается нарушитель, находящийся в сетях провайдера или Интернет, в качестве внутреннего нарушителя принимается нарушитель, находящийся в корпоративной сети ГУП РБ “Уфаводоканал”.

6.3. Защита оборудования Объекта от несанкционированного воздействия производится на 2х уровнях: аутентификация и авторизация на уровне оборудования Объекта и использование VPN и фильтрации сетевых пакетов на уровне шлюза корпоративной сети.

6.4. Внутренняя и внешняя сетевая адресация должна согласовываться со специалистами группы сетевого администрирования и назначаться в соответствии с таблицей сетевой адресации, включаемой в состав документации.

6.5. Для реализации аутентификации и авторизации на уровне оборудования Объекта применяемое оборудование должно обеспечивать парольную защиту доступа.

6.6. В процессе настройки оборудования Подрядчик использует временные пароли доступа, которые по завершению приемо-сдаточных работ сообщаются специалистам отдела АСУТП. Специалисты отдела АСУТП при принятии объекта в обслуживание должны выполнить смену паролей доступа на сетевое оборудование за исключением шлюза и коммутатора. Пароли на шлюз корпоративной сети и коммутатор устанавливаются специалистами группы сетевого администрирования предприятия и не подлежат разглашению.

6.7. Защита от внешних нарушителей осуществляется использованием технологии VPN между шлюзами корпоративной сети.

6.8. Защита от внутренних нарушителей осуществляется фильтрацией сетевых пакетов на шлюзе корпоративной сети в соответствии с таблицей фильтрации сетевых адресов, включаемой в состав документации. Настройка сетевого фильтра выполняется специалистами группы сетевого администрирования.

7. Требования к выполнению работ.

7.1. Подрядчик должен разработать и предоставить в составе рабочего проекта Объекта следующую документацию:

- Пояснительную записку. Пояснительная записка должна содержать краткое описание характеристик применяемого оборудования и раздел “Сетевая безопасность”, включающий в себя описание подсистем сетевой безопасности на каждом активном сетевом устройстве и таблицу фильтрации сетевых адресов для шлюза корпоративной сети.
- Структурную схему ЛВС.
- Монтажный план, где указываются размещение сетевого оборудования, прокладка кабельных трасс, электропитание сетевого оборудования.
- Спецификацию материалов ЛВС и активного сетевого оборудования.
- Маркировку элементов ЛВС.
- Таблицу адресации сетевого оборудования.
- Таблицу фильтрации сетевых адресов (в составе раздела “Сетевая безопасность” пояснительной записки).
- Регламент и инструкции по периодическому обслуживанию оборудования ЛВС и шлюза доступа к корпоративной сети (при необходимости периодического обслуживания).

7.2. Адресация сетевого оборудования выполняется согласно таблицы адресации, полученной в результате согласования Подрядчика со специалистами отдела телекоммуникаций предприятия. Представитель Подрядчика в процессе разработки проекта Объекта обращается с заявкой в группу сетевого администрирования отдела телекоммуникаций предприятия для выделения группы сетевых адресов. К заявке представитель подрядчика

прилагает перечень активного сетевого оборудования Объекта, а также сетевой адрес, маску и адрес шлюза внешнего канала связи, полученные от компании провайдера. На основании перечня активного сетевого оборудования, специалист группы сетевого администрирования выделяет сетевые адреса для шлюза корпоративной сети, коммутатора, остального сетевого оборудования и формирует таблицу адресации включающую в себя перечень сетевого оборудования, адрес, маску, шлюз по-умолчанию. Таблица адресации передаётся Подрядчику для включения в состав проектной документации.

7.3. Защита оборудования Объекта от несанкционированного доступа со стороны внутренних нарушителей выполняется согласно таблицы фильтрации сетевых адресов, разрабатываемой Подрядчиком. Таблица фильтрации сетевых адресов должна иметь вид (пример - указаны вымышленные адреса):

Наименование оборудования Объекта (сетевой адрес оборудования, протокол, порт)	Удаленные адреса, протоколы, порты, [направление], комментарии
1. Контроллер PLC (192.168.33.4) TCP порт 1234	Опрос Объекта: Сервер (192.168.26.11) Сервер ПЛК (10.10.10.10)
2. Преобразователь расходомера (192.168.33.5) TCP порт 3333	Снятие показаний: Сеть (192.168.26.0/25)
...	...

Для определения протоколов, номеров портов и т.п. используемого оборудования Подрядчик обращается к документации по оборудованию или к производителю.

Специалисты группы сетевого администрирования оставляют за собой право вносить в настройки шлюза дополнительные правила не перечисленные в таблице фильтрации, не ухудшающие сетевой безопасности объекта.

7.4. Для определения необходимой пропускной способности внешнего канала связи Подрядчик проводит процедуру согласования пропускной способности со специалистами группы сетевого администрирования предприятия. Согласование выполняется по заявке представителя Подрядчика в группу сетевого администрирования. К заявке представитель подрядчика прилагает перечень активного сетевого оборудования Объекта и техническое задание на Объект. На основании технического задания и перечня активного сетевого оборудования, специалист группы сетевого администрирования совместно с представителем Подрядчика определяют необходимую и реально достижимую пропускную способность внешнего канала связи. Специалисты группы сетевого администрирования оставляют за собой право требовать от Подрядчика документацию на применяемое сетевое оборудование (в т.ч. на сетевые IP-камеры, системы телефонии и др.) и сценарий предполагаемого использования оборудования, если он не содержится в ТЗ для определения необходимой пропускной способности канала. Если документация не содержит необходимой информации, специалисты оставляют за собой право запросить у Подрядчика сетевое оборудование на тестирование.

Результат согласования пропускной способности канала связи оформляется актом, где указываются необходимые и реально достижимые значения пропускной способности канала связи Объекта.

В случае если необходимая пропускная способность канала связи не достижима, Исполнитель и руководство Заказчика извещаются служебной запиской с приложением копии акта согласования.

7.5. После согласования проектной документации подрядчик выполняет монтажные работы, включающие в себя:

- Монтаж ЛВС, внешнего канала связи.
- Доставка, установка и подключение сетевого оборудования.
- Тестирование ЛВС, внешнего канала связи и внешнего сетевого доступа к оборудованию.

7.6. В процессе монтажных работ, Подрядчик выполняет программирование сетевых адресов активного сетевого оборудования, за исключением шлюза корпоративной сети согласно таблицы адресации. Настройка шлюза корпоративной сети выполняется специалистами группы сетевого администрирования предприятия по заявке представителя Подрядчика, для чего требуется предоставление в отдел телекоммуникаций предприятия подготовленных и согласованных таблицы адресации и таблицы фильтрации сетевых адресов и шлюза корпоративной сети.

7.7. По завершению монтажных и наладочных работ Подрядчик разрабатывает и предоставляет Заказчику исполнительную документацию, содержащую те же разделы, что и рабочий проект, но учитывающие доработки выполненные в процессе монтажных и пуско-наладочных работ.

8. Требования к безопасности

8.1. ЛВС и оборудование подключения к корпоративной сети должно соответствовать действующим требованиям по электро- и пожаро-безопасности.

8.2. В оборудовании должна быть реализована автоматическая электрическая защита оборудования при отклонениях параметров электропитания от номинальных значений.

8.3. Все составные части оборудования и их компоненты должны быть заземлены.

9. Правила приемки

9.1. К приёмке допускаются только полностью укомплектованная и смонтированная ЛВС, настроенное сетевое оборудование, исправный внешний канал связи.

9.2. Исполнитель должен уведомить заказчика о начале испытаний не менее чем за 15 дней до начала испытаний.

9.3. Представитель заказчика участвует в испытаниях, если это предусмотрено требованиями нормативной и технической документации или договором.

9.4. Результаты испытаний считают положительными, а ЛВС и подключение к корпоративной сети выдержавшими испытания, если они испытаны в полном объеме и

соответствуют всем показателям, установленным в ТУ, конструкторской и эксплуатационной документации, а также требованиям настоящего документа.

10. Методы контроля

10.1. Для ЛВС и подключения к корпоративной сети должны быть выполнены следующие проверки:

- проверка комплектности документации;
- проверка комплектности оборудования;
- проверка маркировки;
- проверка габаритных размеров;
- проверка обеспечения бесперебойного электропитания;
- проверка работоспособности внешнего канала связи;
- проверка работоспособности подключения к корпоративной сети;
- проверка наличия и работоспособности паролей и доступа к коммутатору и маршрутизатору ЛВС.

11. Транспортирование и хранение

11.1. Оборудование в транспортной таре должно сохранять свои характеристики после воздействия на него следующих климатических факторов:

- температура окружающего воздуха – от минус 30°C до 50°C;
- относительная влажность воздуха при 35°C без конденсации от 10% до 95%.

11.2. Оборудование должно храниться в упаковке предприятия-производителя.

11.3. Оборудование в упаковке предприятия-производителя должно обеспечивать возможность транспортирования автомобильным, железнодорожным, водным и воздушным транспортом.

12. Указания по эксплуатации

12.1. Периодичность и объем обслуживания оборудования и составных частей должны быть однозначно определены регламентом и/или инструкциями по периодическому обслуживанию.

13. Гарантии изготовителя

13.1. Гарантийный срок эксплуатации оборудования, указанный в паспорте на оборудование, должен быть не менее 12 месяцев со дня ввода в эксплуатацию.

13.2. В течение гарантийного срока предприятие-производитель обязан проводить безвозмездно замену вышедших из строя комплектующих или изделия в целом, если потребитель не нарушал правил монтажа и условий эксплуатации, указанных в эксплуатационной документации.

Периодичность и объем обслуживания оборудования и составных частей должны быть однозначно определены регламентом и/или инструкциями по периодическому обслуживанию.

13. Гарантии изготовителя

Гарантийный срок эксплуатации оборудования, указанный в паспорте на оборудование, должен быть не менее 12 месяцев со дня ввода в эксплуатацию.

В течение гарантийного срока предприятие-производитель обязан проводить безвозмездно замену вышедших из строя комплектующих или изделия в целом, если потребитель не нарушал правил монтажа и условий эксплуатации, указанных в эксплуатационной документации.

Зам. главного специалиста
службы АСУ



А.И. Дивеев