Приложение №1/2 к Извещению

**СКОЛКОВО**

**КОРПУС 4 НА ТЕРРИТОРИИ ШТАБА СТРОИТЕЛЬСТВА**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА СПД**

**МОСКВА**

**2013 г.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| А | ДД.ММ.ГГГГ | Внутреннее рассмотрение | ФИО | ФИО | ФИО |
| Редакция | Дата выпуска | Задачи | Разработал | Проверил | Утвердил |

ЛИСТ СОГЛАСОВАНИЯ

**ОПИСАНИЕ РЕДАКЦИЙ**

|  |  |  |
| --- | --- | --- |
| **Редакция** | **Дата** | **Описание** |
| A | ДД.ММ.ГГГГ | Выпуск для внутреннего рассмотрения и замечаний |
| B | ДД.ММ.ГГГГ | Для рассмотрения и замечаний Заказчика |
| C | ДД.ММ.ГГГГ | Утверждено для проектирования |

# Содержание

[Содержание 5](#_Toc367190635)

[1 Общие сведения 6](#_Toc367190636)

[1.1 Полное наименование системы и ее условное обозначение 6](#_Toc367190637)

[1.2 Наименование предприятий разработчика и Заказчика системы и их реквизиты 6](#_Toc367190638)

[2 Назначение и цели создания (развития) системы 7](#_Toc367190639)

[2.1 Назначение системы 7](#_Toc367190640)

[2.2 Цели создания системы 7](#_Toc367190641)

[3 Требования к системе 8](#_Toc367190642)

[3.1 Требования к системе в целом 8](#_Toc367190643)

[3.1.1 Требования к структуре и функционированию системы 8](#_Toc367190644)

[3.1.2 Показатели назначения 9](#_Toc367190645)

[3.1.3 Требования к надежности 10](#_Toc367190646)

[3.1.4 Требования безопасности 10](#_Toc367190647)

[3.1.5 Требования к эргономике и технической эстетике 10](#_Toc367190648)

[3.1.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы 11](#_Toc367190649)

[3.1.7 Требования к защите информации от несанкционированного доступа 12](#_Toc367190650)

[3.1.8 Требования по сохранности информации при авариях 12](#_Toc367190651)

[3.1.9 Требования к защите от влияния внешних воздействий 13](#_Toc367190652)

[3.1.10 Требования к патентной чистоте 13](#_Toc367190653)

[3.1.11 Требования по стандартизации и унификации 13](#_Toc367190654)

[3.1.12 Дополнительные требования 13](#_Toc367190655)

[3.2 Требования к функциям (задачам), выполняемым системой 14](#_Toc367190656)

[3.2.1 Требования к подсистеме ЛВС 14](#_Toc367190657)

[3.2.2 Требования к подсистеме беспроводной сети передачи данных 18](#_Toc367190658)

[3.2.3 Требования к подсистеме доступа к внешним сетям 19](#_Toc367190659)

[3.2.4 Требования к информационной безопасности 21](#_Toc367190660)

[4 Состав и содержание работ по созданию системы 22](#_Toc367190661)

[4.1 Подсистема ЛВС 22](#_Toc367190662)

[4.2 Подсистема беспроводной сетевой инфраструктуры 22](#_Toc367190663)

[4.3 Подсистема доступа к внешним сетям 23](#_Toc367190664)

[4.4 Подсистема коммутации оптических волокон 23](#_Toc367190665)

[5 Спецификация оборудования 24](#_Toc367190666)

[6 Источники разработки 25](#_Toc367190667)

[6.1 Источники разработки 25](#_Toc367190668)

[7 Приложения 27](#_Toc367190669)

[7.1 Приложение № 1 27](#_Toc367190670)

[**Глоссарий** 27](#_Toc367190671)

# Общие сведения

## Полное наименование системы и ее условное обозначение

Настоящий документ является техническим заданием на создание объектов информационной технологии (ИТ), представляющих собой системное программное обеспечения серверов, персональных компьютеров и периферийной офисной техники, аппаратное обеспечение серверов, персональных компьютеров и периферийной офисной техники, офисные локальные вычислительные сети, распределенные сети передачи данных, системы резервного копирования, хранения и аварийного восстановления данных, инженерные системы специализированных технических помещений для размещения компьютерного оборудования, системы управления технической и системной инфраструктурой, системы обеспечения, контроля и управления доступом к данным и носителям информации.

Полное наименование системы – сеть передачи данных корпуса 4 на территории Штаба строительства (бывшего д/о "Полет") инновационного центра "Сколково". Условное обозначение системы: СПД.

## Наименование предприятий разработчика и Заказчика системы и их реквизиты

**Наименование Организатора процедуры закупки:** Некоммерческая организация Фонд развития Центра разработки и коммерциализации новых технологий

**Наименование Заказчика процедуры закупки:**

Общество с ограниченной ответственностью «Объединенная дирекция по управлению активами и сервисами Центра разработки и коммерциализации новых технологий (инновационного центра «Сколково»)».

**Адрес местонахождения Заказчика Процедуры закупки:** 143005, Московская область, Одинцовский район, г. Одинцово, ул. Луговая, д. 4.

**Адрес местонахождения, почтовый адрес Организатора Процедуры закупки:** 123610, Москва, Краснопресненская набережная, д.12, подъезд 9, этаж 24, офис № 2410.

**Почтовый адрес Заказчика Процедуры закупки:**

143005, Московская область, Одинцовский район, г. Одинцово, ул. Луговая, д. 4, а/я 25.

**Адрес электронной почты Организатора Процедуры закупки:** SkZakupki@sk.ru

# Назначение и цели создания (развития) системы

## Назначение системы

Назначение системы – предоставление сервиса передачи данных для подключаемого вычислительного и терминального оборудования (рабочих станций, серверов, иных программно-аппаратных комплексов, имеющих соответствующие интерфейсы для подключения  к системе), а так же каналообразующего оборудования организующего каналы связи с внешними системами.

Сервис передачи данных обеспечивается для корпоративных информационных систем и пользователей этих систем с использованием стандартизованных протоколов сетевого взаимодействия.

Система не предназначена для предоставления сервиса передачи данных для каких-либо систем управления и мониторинга технологических или производственных процессов.

Система обеспечивает сервис передачи данных для всех необходимых объектов административного и общехозяйственного назначения находящихся в рамках производственной площадки Заказчика, а так же обеспечивает возможность обмена данными с внешними системами.

## Цели создания системы

Целями создания системы являются:

* обеспечение информационного обмена и организация совместной работы с корпоративными информационными системами;
* создание современной и надежной платформы для функционирования сервисов, предоставляемых корпоративными информационными системами;
* обеспечение отказоустойчивости сетевых сервисов обеспечивающих доступ к корпоративными информационными системами;
* обеспечение гибкости и масштабируемости информационной инфраструктуры Заказчика в целом в рамках функциональных возможностей системы;
* построение наблюдаемой и управляемой сети передачи данных Заказчика.

В результате создания системы должны быть обеспечен сервис передачи данных для корпоративных информационных систем и пользователей этих систем, находящихся в рамках производственной площадки Заказчика.

Критерием достижения целей создания системы является возможность сетевого взаимодействия подключаемого вычислительного и терминального оборудования с использованием стандартного протокола сетевого взаимодействия IP (Internet Protocol) версии 4 (RFC 791 Internet Protocol) на 3-ем уровне базовой эталонной модели взаимодействия открытых систем.

# Требования к системе

## Требования к системе в целом

### Требования к структуре и функционированию системы

Система должна удовлетворять следующим общим требованиям:

* масштабируемость – способность к увеличению функциональных возможностей системы путем наращивания числа функциональных блоков, выполняющих одни и те же задачи;
* конвергентность – способность к одновременной передачи различных видов данных (голос, видео, данные);
* открытость – использование унифицированных решений, обеспечивающих простоту наращивания и взаимодействия;
* самодостаточность – реализация функциональной завершенности и независимости развития компонентов СМ ИТР;
* надежность – способность выполнять свои функции в заданных условиях эксплуатации;
* адаптивность – способность выполнять свои функции при меняющихся условиях эксплуатации.

Система должна содержать следующие функциональные подсистемы:

* подсистема локальной вычислительной сети (ЛВС) на объектах производственной площадки;
* подсистема беспроводной сетевой инфраструктуры;
* подсистема доступа к внешним сетям;
* подсистема СКС.

Оборудование, аппаратные средства и материалы СПД должны соответствовать стандартам РФ, техническим требованиям и прочим нормативным актам, согласованным в установленном порядке.

#### Подсистема ЛВС

Для поддержки функционирования подсистемы, эксплуатирующий персонал должен обладать знаниями в области информационных и сетевых платформ, на базе которых будет реализована подсистема, а так же в области технологий построения современных сетей передачи.

Подготовка персонала должна осуществляться на стадии ввода в действие по учебным программам, подготовленным Исполнителем.

#### Подсистема беспроводной сетевой инфраструктуры

Для поддержки функционирования подсистемы, эксплуатирующий персонал должен обладать знаниями в области информационных и сетевых платформ, на базе которых будет реализована подсистема, а так же в области технологий современных сетей передачи, включая технологии беспроводных сетей передачи данных и безопасности беспроводных сетей.

#### Подсистема доступа к внешним сетям

Для поддержки функционирования подсистемы эксплуатирующий персонал должен обладать знаниями в области информационных и сетевых платформ, на базе которых будет реализована подсистема, а так же в области технологий построения современных сетей передачи, включая технологии глобальных сетей передачи данных, технологии виртуальных частных сетей, систем сетевой безопасности и защиты периметра.

### Показатели назначения

#### Требования к адаптивности системы

Система должна сохранять работоспособность при увеличении количества пользователей в рамках характеристик аппаратно-программной среды.

#### Требования к модернизации и развитию системы

Проект разрабатываемой СПД должен содержать рекомендации к развитию.

Разрабатываемая СПД должна предусматривать возможность корректной работы в рамках ограничений аппаратного обеспечения и используемых каналов связи. Количество одновременно работающих пользователей определяется ограничениями аппаратного обеспечения и требованиями приложений в процессе эксплуатации.

СПД должна предусматривать возможность развития и модернизации, как путем добавления модулей/устройств, так и за счет модернизации программного обеспечения.

### Требования к надежности

Система должна поддерживать круглосуточный режим функционирования. Допускается временная недоступность сервисов, предоставляемых системой, при проведении регламентных работ.

Надежность системы должна обеспечиваться избыточностью (резервированием основных компонент).

Избыточность может быть реализована путем горячего резервирования для наиболее критичных элементов подсистем или соответствующим набором запасных частей и принадлежностей (ЗИП) для менее критичных элементов подсистем или элементов, для которых не применимо горячее резервирование вследствие их функциональных особенностей.

В случае горячего резервирования, применяемые архитектурные решения должны обеспечивать автоматическую перенастройку системы в случае выхода из строя компонента (надежность которого обеспечена избыточностью) на использование избыточного компонента.

Выбор путей обеспечения надежности (горячее резервирование, ЗИП) должны быть уточнены на стадии рабочего проектирования.

### Требования безопасности

Все технические решения (монтаж, наладка, эксплуатация, обслуживание и ремонт технических средств) должны соответствовать действующим нормам и правилам техники безопасности, защиты от воздействий электрических полей и электромагнитного излучения, пожарной безопасности, а также охраны окружающей среды.

Используемые технические средства не должны допускать возможности нанесения вреда здоровью или поражения пользователей системы электрическим током и электромагнитными излучениями при условии соблюдения правил ее эксплуатации.

Используемые технические средства не должны допускать возможности нанесения ущерба окружающей среде.

### Требования к эргономике и технической эстетике

Автоматизированные рабочие места персонала, обслуживающего КСПД, должны оборудоваться в соответствии с Санитарными Правилами и Нормами 2.2.2. 542-96 – "Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работ".

### Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Условия эксплуатации, а также виды и периодичность обслуживания комплекса технических средств СПД должны соответствовать требованиям по эксплуатации, техническому обслуживанию, ремонту и хранению, изложенным в документации завода-изготовителя на них.

Для электропитания комплекса технических средств СПД должна быть предусмотрена трехфазная четырехпроводная сеть с глухо заземленной нейтралью 380/220 В (+10-15)% частотой 50 Гц (+1-1) Гц.

Каждое техническое средство запитывается однофазным напряжением 220 В частотой 50 Гц через сетевые розетки с заземляющим контактом. Оборудование должно быть полностью работоспособным при изменении напряжения источника питания в диапазоне +/- 5% и при изменении частоты питающего напряжения +/- 5%.

Во всех местах размещения оборудования должно быть обеспечено стандартное питание переменного тока, отвечающее требованиям ТУ на 220-230 В переменного тока с частотой 50 Гц; от всех устройств, подсоединяемых к источникам питания, должны быть проведены соответствующие кабели со стандартными разъемами.

Не допускается использование переносных розеток; все стандартные соединения и проводка должны проходить в кабельных каналах или в лотках.

В случае использования электропитания постоянного тока источники питания постоянного тока должны быть электрически изолированы от источника напряжения переменного тока.

Оборудование СПД должно снабжаться электроэнергией от постоянно включенного источника бесперебойного питания (ИБП):

1. для помещений телекоммуникационного оборудования ИБП должен обеспечить питание в течение 3 часов при температуре окружающей среды 25 °С в случае отказа основного источника электроэнергии, при условии наличия необходимых площадей для размещения ИБП, и выполнения условий нагрузки по весу на полы и перекрытия.
2. аккумуляторная батарея ИБП должна автоматически полностью зарядиться в пределах 12 часов с момента восстановления основного источника электроэнергии;
3. аккумуляторные батареи должны быть герметичными и не выделять газов;

Стойки для размещения оборудования СПД должны подключаться к шине защитного заземления, соединённой с главной шиной защитного заземления либо шиной уравнивания потенциалов, желто-зелёным ПВХ (PVC) защищенным кабелем с 6мм2 жилами.

Заземляющие шины должны быть промаркированы на русском и английском языках.

Оборудование СПД должно соответствовать требованиям стандарта безопасности IEC 60950.

Техническое обслуживание комплекса технических средств СПД должно осуществляться эксплуатационным персоналом. Численность, квалификация, режим работы и функции эксплуатационного персонала, а также регламент технического обслуживания определяются на стадии технического проекта.

Техническое обслуживание и эксплуатация технических средств должны осуществляться в соответствии с документацией производителя технических средств и определяться в эксплуатационной документации на СПД.

### Требования к защите информации от несанкционированного доступа

Средства защиты информации от несанкционированного доступа должны представлять собой комплексную систему защиты от несанкционированного доступа, в составе которой необходимо обеспечить:

* размещение технических средств СПД в помещениях, оборудованных системой контроля доступа;
* ограничение доступа к управлению техническими средствами СПД (п. 4.2.6.2.2).

### Требования по сохранности информации при авариях

Система должна восстанавливать свое функционирование при корректном перезапуске аппаратных средств. Элементы системы должны сохранять конфигурационные настройки и программное обеспечение в энергонезависимой памяти.

Должна быть предусмотрена возможность организации автоматического и (или) ручного резервного копирования конфигурационных данных системы средствами подсистемы управления СПД.

Приведенные выше требования не распространяются на компоненты системы, разработанные третьими сторонами и действительны только при соблюдении правил эксплуатации этих компонентов, включая своевременную установку обновлений, рекомендованных производителями покупного программного обеспечения.

Сохранность конфигурационных настроек должна быть обеспечена в случае следующих событий (аварий, отказов и т.п.):

* потеря электропитания;
* аппаратно-программные сбои.

### Требования к защите от влияния внешних воздействий

По возможности, транзитные коммуникации и кабельные системы должны быть вынесены за пределы помещения, где будут располагаться компоненты СПД.

В серверном помещении, где будут располагаться компоненты СПД, должны быть проведены работы по гидроизоляции, необходимость полной или частичной гидроизоляции определяется на этапе технического проектирования.

Используемые в строительстве серверного помещения, где будут располагаться компоненты СПД, материалы и конструкции должны иметь минимальную остаточную кристаллическую влажность. Обязательным является наличие сертификата на партии материалов и конструкций с результатами испытаний, если это предусмотрено действующими строительными нормами.

Наличие окон в серверном помещении, где будут располагаться компоненты СПД, не допускается.

### Требования к патентной чистоте

Применяемые в СПД программные средства должны быть лицензионными или подпадать под действие GNU GPL.

### Требования по стандартизации и унификации

Решения по построению СПД должны быть унифицированы и соответствовать стандартам, принятым в Фонде.

СПД должна быть разработана в соответствии с требованиями государственных стандартов (ГОСТ 34.201-89, 34.603-92, 34.602-89, РД 50-34.698-90.

### Дополнительные требования

Требования не предъявляются.

## Требования к функциям (задачам), выполняемым системой

### Требования к подсистеме ЛВС

#### Общие требования

Подсистема ЛВС предназначена для предоставления сервиса передачи данных для подключаемого терминального оборудования и организации информационного обмена с подсистемами, подключаемыми к подсистеме ЛВС. Подсистема ЛВС обеспечивает следующие типы подключений:

* подключение терминального оборудования (рабочих станций, периферийных устройств, ip телефонов, ip видеотерминалов);
* подключение подсистемы доступа к внешним сетям;
* подключение подсистемы беспроводной сетевой инфраструктуры;
* подключение к шлюзам других систем (без обеспечения транизитной передачи данных для этих систем) комплекса автоматизации Заказчика.

#### Основные технические требования.

* подсистема ЛВС должна представлять собой иерархическую многоуровневую систему передачи данных, состоящую из:
* уровня ядра;
* уровня доступа;
* требования к уровню ядра:
* основой подсистемы ЛВС должен быть уровень ядра (высокоскоростная корпоративная магистраль), производительность которого должна удовлетворять потребностям информационного обмена и может быть наращиваема в дальнейшем;
* уровень ядра должен обеспечивать подключение следующих уровней и подсистем со скоростью передачи данных не ниже приведенной:
* подсистема доступа к внешним сетям: скорость – 100Мбит/c, тип интерфейса – 100/1000Base-T или 1000Base-LX;
* подсистема беспроводной сетевой инфраструктуры: скорость – 1Гбит/c, тип интерфейса – 1000Base-T или 1000Base-LX;
* другие системы комплекса автоматизации Заказчика (через соответствующие шлюзы): скорость – 100/1000Мбит/c, тип интерфейса – 100/1000Base-T или 1000Base-LX;
* Обмен информацией о маршрутах должен осуществляться средствами протоколов динамической маршрутизации. В качестве протоколов динамической маршрутизации могут использоваться протоколы EIGRP, OSPF, IS-IS;
* надежность уровня ядра должна обеспечиваться путем горячего резервирования его компонентов:
* уровень ядра должен состоять из не менее 2-х коммутаторов идентичной аппаратной конфигурации обеспечивающих горячее резервирование уровня ядра;
* коммутаторы ядра должны иметь внутреннее горячее блоков питания;
* каждый уровень (подсистема) должны подключаться к уровню ядра не менее чем двумя каналами к различным коммутаторам уровня ядра;
* единичный отказ любого элемента магистрали не должен приводить к прекращению предоставления сервиса передачи данных;
* уровень ядра выполняет агрегирование подключений уровня доступа;
* подключение уровня доступа к уровню ядра должно быть выполнено на скорости 1Гбит/c, тип интерфейса 1000Base-T;
* уровень ядра должен выполнять маршрутизацию трафика для протокола IP версии 4 между виртуальными ЛВС;
* уровень ядра должен поддерживать ретрансляцию широковещательных запросов на получение ip адресов;
* уровень ядра должен поддерживать фильтрацию пакетов на основе заголовков второго-четвертого уровня модели OSI;
* подключение каждого элемента уровня доступа должно производиться двумя канала к различным коммутаторам уровня ядра;
* требования к уровню доступа:
* уровень доступа должен обеспечивать подключение конечных устройств. Подключение должно поддерживать скорости 10,100 Мбит/c, тип интерфейса 10/100Base-T;
* уровень доступа должен поддерживать технологию виртуальных локальных сетей (802.1q) и транковые соединения;
* уровень доступа должен поддерживать функциональность предотвращения широковещательных штормов в широковещательном домене;
* уровень доступа должен обеспечивать на каждом пользовательском порту функциональность подачи питания через кабель категории не ниже 5e (PoE);
* надежность уровня доступа должна обеспечиваться подключением розеток с каждого рабочего места на различные коммутаторы уровня доступа;
* подсистема ЛВС должна обеспечивать подключение 100% рабочих мест с возможностью расширения на 50%;
* подсистема ЛВС должна допускать поэтапную модернизацию отдельных узлов;
* для обеспечения высокого быстродействия структура сети должна быть сегментирована на втором или третьем уровне модели OSI, что позволяет уменьшить количество широковещательных сообщений в ЛВС и, тем самым, увеличить ее производительность;
* подсистема ЛВС должна использовать адресацию на третьем уровне модели OSI, использующую диапазоны адресов, определенные в RFC-1918 для приватного использования; структура адресного плана должна быть иерархической и обеспечивать возможность суммаризации информации о маршрутах;
* подсистема ЛВС должна обеспечивать возможность работы с протоколом IP версии 4;
* при необходимости подсистема ЛВС должна обеспечивать возможность модернизации для поддержки протокола IP версии 6 путем обновления ПО и лицензионного соглашения с производителем оборудования;
* подсистема ЛВС должна обеспечивать сервисы качества обслуживания (QoS) для трафика наиболее важных приложений и голосового/видео трафика;
* подсистема ЛВС должна обеспечивать работу служб DNS и DHCP на серверном оборудовании с горячим резервированием;
* подсистема ЛВС должна быть отказоустойчивой, как с точки зрения структуры сети и дублирования каналов связи подсистемы магистральных кабельных соединений, так и благодаря использованию сетевых устройств, поддерживающих горячее резервирование; отказоустойчивая структура сети должна подкрепляться соответствующими протоколами для минимизации времени восстановления работоспособности сети после сбоя;
* общие требования к аппаратному составу подсистемы ЛВС:
* аппаратный состав ЛВС должен быть представлен коммутаторами Ethernet с различным функциональными характеристиками;
* все коммутаторы ЛВС должны обладать следующими общими характеристиками:
* ассиметричная коммутация между портами различных режимов работы (10/100/1000Base-T);
* автоматическое согласование режима работы порта;
* поддержка подачи питания по стандарту 803.2ad на все порты коммутатора;
* поддержка виртуальных локальных сетей (802.1q);
* поддержка агрегирования портов (802.3ad);
* коммутация на втором и третьем уровне модели OSI;
* поддержка протокола прокрывающего дерева (802.1d, 802.1s);
* управление по сети при помощи протоколов TELNET, SSH, SNMP и RMON;
* управление с помощью консольного порта;
* ограничение доступа к устройствy для управления (многоуровневая система пользователей/паролей, ограничения по исходным IP адресам);
* поддержка протоколов авторизации RADIUS, TACACS+;
* программное обеспечение операционной системы и информация о конфигурации должны храниться в энергонезависимой флэш-памяти;
* установка в стандартных 19-дюймовых (482,6 мм) стойках;
* светодиодная индикация состояния портов и устройства;
* индикационная панель должна быть на фронтальной стороне устройства, обеспечивая непосредственный обзор состояния устройства с помощью светодиодной индикации;
* коммутаторы уровня ядра должны обладать следующими характеристиками в дополнение к общим:
* поддержка подачи питания по стандарту 803.2at на все порты коммутатора;
* производительность центральной шины или коммутирующей матрицы не менее 40 Гб/с, скорость обработки пакетов размером 64 байт не ниже 40 млн. пак./с;
* достаточное количество интерфейсов со скоростью до 10Гбит/c для подключения подсистем СПД;
* возможность агрегирования портов (802.3ad), расположенных на разных модулях в рамках шасси одного коммутатора/стека коммутаторов;
* фильтрация трафика по информации второго - четвертого уровней модели OSI;
* классификация (маркировка) трафика по различным критериям первого - четвертого уровней модели OSI, приоритезация трафика в соответствии с классификацией;
* горячее резервирование блоков питания;
* коммутаторы уровня доступа должны обладать следующими характеристиками в дополнение к общим:
* скорость обработки пакетов не ниже 10 млн. пак./с;
* интерфейсы пользовательских портов 10/100Base-T, интерфейсы портов подключения к уровню распределения 1000Base-T/1000Base-LX;
* функциональность PoE 802.3af;
* возможность обеспечения горячего резервирования вышедшего из строя блока питания для группы коммутаторов доступа с помощью специализированного устройства (Cisco RPS или аналог).

#### Требования к информационной безопасности.

* подсистема ЛВС должна обеспечивать возможности реализации аутентификации доступа к среде передачи данных на уровне доступа с помощью:
* аутентификации по протоколу 802.1x;
* аутентификации по MAC адресу;
* подсистема ЛВС должна обеспечивать возможности реализации ограничения по количеству MAC адресов на порту уровня доступа;
* подсистема ЛВС должна обеспечивать возможности реализации политики управления оборудованием с помощью:
* аутентификации подключений администраторов;
* ролевой системы администраторов;
* ограничения сессий управления по исходным ip адресам.

### Требования к подсистеме беспроводной сети передачи данных

#### Общие требования

Подсистема беспроводной сети передачи данных должна предоставлять сервис передачи данных для подключаемого вычислительного и терминального оборудования с беспроводными сетевыми интерфейсами. К такому оборудованию могут относиться: персональные компьютеры, портативные компьютеры, планшетных ПК, персональные цифровые секретари и сотовые телефоны.

Границы зоны покрытия беспроводной сети передачи данных в рамках производственной площадки Заказчика, а так же необходимая емкость беспроводной сети и необходимые параметры пропускной способности должны быть определены на этапе проектирования подсистемы.

Подсистема беспроводной сети передачи данных должна быть реализована в соответствии с централизованной архитектурой, включающей:

* Точки беспроводного доступа
* Контроллеры беспроводной сети в резервируемой конфигурации

#### Основные технические требования

Подсистема беспроводной сети передачи данных должна обеспечивать выполнение следующих требований:

* точки беспроводного доступа должны работать в частотном диапазоне 2,4 ГГц по стандарту IEEE802.11b/g/n;
* точки беспроводного доступа должны поддерживать централизованное управление и мониторинг;
* точки беспроводного доступа должны поддерживать виртуальные сети VLAN с разделением по сетевому идентификатору SSID;
* точки беспроводного доступа должны обеспечивать защиту информации, передаваемой в беспроводной сети с использованием протокола WPA и WPA2 (IEEE802.11i); аутентификацию пользователей по протоколу LEAP, 802.1x (EAP); аутентификацию пользователей на внешнем сервере RADIUS;
* подсистема беспроводной сети передачи данных должна обеспечивать роуминг мобильных пользователей при перемещении из зоны действия одной точки доступа к другой;
* подсистема беспроводной сети передачи данных должна обеспечивать поддержку сервисов качества обслуживания (QoS), для реализации возможности передачи трафика критичного к качеству обслуживания;
* контроллеры беспроводной сети должны обеспечивать применение политик безопасности, предотвращение атак, осуществлять мониторинг радио-ресурсов, динамическое управления мощностью передатчиков, сервисы обеспечения качества обслуживания и мобильность пользователей;
* подсистема беспроводной сети передачи данных должна обеспечивать способность изменять и прекращать трансляцию идентификатора беспроводной сети (SSID);
* подсистема беспроводной сети передачи данных должна иметь возможность обеспечивать контроль доступа по адресу управления доступом к среде передачи (MAC);
* подсистема беспроводной сети передачи данных должна обеспечивать соответствие протоколу для виртуальной локальной сети (VLAN) IEEE 802.1Q;
* точки беспроводного доступа должны обеспечивать возможность подключения внешних антенн, если в процессе проектирования выяснится их необходимость.

Подключение контроллеров беспроводной сети должно быть обеспечено в отказоустойчивом режиме дублированными сетевыми интерфейсами, к различным коммутаторам серверных ферм.

Точки беспроводного доступа должны поддерживать получение питания по медному кабелю интерфейса Ethernet по стандарту IEEE 802.3at. Точки беспроводного доступа подключаются к коммутаторам уровня доступа, поддерживающим данный стандарт.

#### Требования к информационной безопасности

В подсистеме беспроводной сети передачи данных должны быть обеспечены возможности разграничения доступа беспроводных абонентов, аутентификации и авторизации, посредством:

* создания изолированных виртуальных беспроводных сетей, с соответствующими правилами доступа;
* разграничения доступа и контролирования трафика всех виртуальных беспроводных сетей выделенным межсетевым экраном, либо отдельным контекстом (виртуальный межсетевой экран) и системой обнаружения и предотвращения вторжений;
* использованием аутентификации 802.1x для виртуальных беспроводных сетей, обеспечивающих доступ к конфиденциальным ресурсам;
* обеспечением дополнительной аутентификации на уровне доступа к среде передачи по MAC адресам для виртуальных беспроводных сетей, обеспечивающих доступ к конфиденциальным ресурсам.

### Требования к подсистеме доступа к внешним сетям

#### Общие требования

Подсистема доступа к внешним сетям предназначена для обеспечения доступа к ресурсам публичной сети Интернет, а так же обеспечения демилитаризованной зоны для размещения публичных информационных ресурсов Заказчика.

#### Основные технические требования

* подсистема доступа к внешним сетям должна поддерживать возможность подключения к двум и более операторам Интернет;
* подсистема должна поддерживать классификацию и маркировку трафика по различным критериям третьего - четвертого уровней модели OSI и приоритезацию пакетов в соответствии с классификацией;
* подключение серверов демилитаризованной зоны должна выполняться на отдельных коммутаторах, не входящих в состав других подсистем;
* надежность подсистемы должна обеспечиваться горячим резервированием всех элементов подсистемы доступа к внешним сетям;
* единичный отказ любого элемента подсистемы не должен приводить к прекращению предоставления сервиса;
* требования к аппаратному составу подсистемы доступа к внешним сетям:
* подключение подсистемы к сети оператора Интернет производится с помощью межсетевого экрана (МСЭ). МСЭ должен обладать следующими характеристиками:
* не менее 4 интерфейсов 1000BASE-T;
* поддержка протоколов IPv4, IPv6;
* динамическая маршрутизация с использованием стандартных протоколов маршрутизации OSPF, EIGRP;
* фильтрация трафика по информации второго - четвертого уровней модели OSI;
* управление по сети при помощи протоколов TELNET, SSH, SNMP и RMON;
* управление с помощью консольного порта;
* ограничение доступа к устройствy для управления (многоуровневая система пользователей/паролей, ограничения по исходным IP адресам);
* поддержка протоколов авторизации RADIUS, TACACS+;
* программное обеспечение операционной системы и информация о конфигурации должны храниться в энергонезависимой флэш-памяти;
* установка в стандартных 19-дюймовых (482,6 мм) стойках;
* расширенные функции безопасности, в том числе функционал предотвращения вторжения и контекстной фильтрации;

#### Требования к информационной безопасности.

* подсистема доступа к внешним сетям должна обеспечивать контроль состояний сессий при доступе пользователей к внешним сетям и при доступе из внешних сетей к публичным ресурсам; функциональность контроля состояния сессий должна обеспечиваться межсетевыми экранами;
* подсистема должна обеспечивать инспектирование доступа пользователей к внешним сетям и доступа из внешних сетей к публичным ресурсам средствами обнаружения/предотвращения вторжения и другой вредоносной активности;

### Общие требования к информационной безопасности

Все активное сетевое оборудование должно иметь выделенный логический или физический интерфейс управления, доступ к которому ограничивается IP адресами виртуальных сетей управления и виртуальных сетей администрирования.

Адресация IP интерфейсов управления активного сетевого оборудования должна иметь унифицированную структуру, позволяющую определить идентификатор площадки размещения объекта управления.

Подсистема управления СПД взаимодействует с оборудованием СПД через интерфейсы управления активного сетевого оборудования посредством протоколов управления. Необходимо использовать только защищенные протоколы управления, обеспечивающие криптографическую защиту данных учетных записей, используемых для управления оборудованием.

Должна обеспечиваться аутентификация и авторизация администраторов и операторов при доступе к интерфейсам управления подсистемы управления СПД.

Для взаимодействия с интерфейсами управления подсистема управления СПД должны использоваться только защищенные протоколы, обеспечивающие криптографическую защиту учетных записей, используемых для доступа к подсистеме;

Доступ к интерфейсам управления подсистемы управления СПД должен ограничиваться IP адресами виртуальных сетей администрирования.

# Состав и содержание работ по созданию системы

Работы по созданию СПД состоят из работ по проектированию, установке и монтажу оборудования, установке и монтажу оптических патч-панелей, настройке и сдаче в эксплуатацию подсистем. При работах необходимо учитывать как требования к подсистемам из раздела 4, так и требования к системе передачи данных в целом. Работы проводятся согласно проектной документации.

## Подсистема ЛВС

Работы по подсистеме ЛВС должны включать в себя:

* написание проектной документации;
* монтаж оборудования согласно спецификации;
* коммутацию питания и портов СКС;
* коммутацию серверного оборудования;
* стекирование коммутаторов ядра;
* настройку базовой конфигурации;
* настройку VTP, STP;
* настройку VLAN;
* установку серверного оборудования;
* настройку служб DHCP, DNS с возможностью работы в режиме горячего резервирования;
* настройку интерфейсов управления;
* настройку удалённого управления по протоколу SSH;
* настройку портов доступа согласно требованиям к системе;
* настройку политик безопасности согласно требованиям к системе;
* настройку маршрутизации между пользовательскими, серверными и телефонными виртуальными сетями;
* настройку политик приоритезации трафика виртуальных сетей;

## Подсистема беспроводной сетевой инфраструктуры

Работы по подсистеме беспроводной сетевой инфраструктуры должны включать в себя:

* написание проектной документации;
* радиообследование;
* монтаж оборудования согласно спецификации;
* коммутацию питания и портов СКС;
* настройку базовой конфигурации;
* настройку VLAN;
* настройку интерфейсов управления;
* настройку удалённого управления по протоколу SSH;
* настройку политик безопасности согласно требованиям к системе;
* настройку беспроводных идентификаторов SSID согласно требований заказчика;
* настройку возможности гостевого доступа к беспроводной сети;

## Подсистема доступа к внешним сетям

Работы по подсистеме ЛВС должны включать в себя:

* написание проектной документации;
* монтаж оборудования согласно спецификации;
* коммутацию питания и портов;
* настройку базовой конфигурации;
* настройку интерфейсов управления;
* настройку интерфейсов маршрутизации;
* настройку удалённого управления по протоколу SSH;
* настройку политик безопасности согласно требованиям к системе;
* настройку маршрутизации между пользовательскими, серверными и телефонными виртуальными сетями;
* настройку политик приоритезации трафика виртуальных сетей;
* настройку маршрутизации сетей провайдера;
* настройку трансляции сетевых адресов;
* настройку политик приоритезации трафика виртуальных сетей;

## Подсистема коммутации оптических волокон

Работы по подсистеме коммутации оптических волокон включают в себя:

* монтаж оборудование согласно спецификации;
* разварку оптических волокон на оптической панели согласно проектной документации;
* тестирование портов оптической панели;
* нанесение маркировки портов оптических панелей;

# Спецификация оборудования

Спецификация оборудования и материалов доступна в Приложении №1 к Извещению о проведении Открытого Запроса в цен целях отбора поставщика на право заключения договора на поставку и монтаж активного оборудования серверной корпуса 4 на территории Штаба строительства (бывшего д/о "Полет") инновационного центра "Сколково", расположенного по адресу: МО, Одинцовский р-н, г.Одинцово, ул.Луговая д.4 для нужд Общества с ограниченной ответственностью «Объединенная дирекция по управлению активами и сервисами Центра разработки и коммерциализации новых технологий (инновационного Центра «Сколково»)»

# Источники разработки

## Источники разработки

Разработка технических решений должна проводиться на основании требований следующих документов:

Указы Президента РФ:

* Указ Президента РФ «Об основах государственной политики в сфере информатизации», № 170, 1994 г.
* Указ Президента РФ «Вопросы Федеральной службы по техническому и экспортному контролю», № 1085, 2004 г.,

Российские государственные и международные стандарты:

* ГОСТ Р 1.4-93 “Государственная система стандартизации Российской Федерации. Стандарты отраслей, стандарты предприятий, стандарты научно-технических, инженерных обществ и других общественных организаций. Общие положения”;
* ГОСТ 1.5-2001 “Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Общие требования к построению, изложению, оформлению, содержанию и обозначению”;
* ГОСТ Р 1.5-2002 “Государственная система стандартизации Российской Федерации. Стандарты. Общие требования к построению, изложению, оформлению, содержанию и обозначению“;
* ГОСТ 34.201-89. “Виды, комплектность и обозначение документов при создании автоматизированных систем”;
* ГОСТ 34.601-90 “Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания”;
* ГОСТ 34.602-89 “Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы”;
* РД 50–34.698–90 “Автоматизированные системы. Требования к содержанию документов”;
* ГОСТ 34.003-90. ИТ. Комплекс стандартов на АС. Термины и определения.
* ГОСТ Р ИСО 7498-1-99. ИТ. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.
* ГОСТ 34;601:1990; информационная технология; автоматизированные системы; стадии создания;
* ГОСТ 34;602:1989; информационная технология; техническое задание на создание автоматизированных систем;
* ГОСТ 34;603:1992; информационная технология; виды испытаний автоматизированных систем;
* ГОСТ 34;201:1989; информационная технология; виды, комплектность и обозначение документов при создании автоматизированных систем;
* РД 50-34;698:1990; методические указания; информационная технология; автоматизированные системы; требования к содержанию документов.
* ISO 8402:1994; управление качеством и обеспечение качества – словарь;
* ISO 9000-3:1997; стандарты в области административного управления качеством и обеспечения качества; часть 3; руководящие указания по применению ISO 9001 при разработке, поставке, монтаже и обслуживании программного обеспечения;
* ISO/IEC 12207:1995; информационная технология; процессы жизненного цикла программного обеспечения;
* ISO/IEC 9126-1:1998; информационная технология; характеристики и метрики качества программного обеспечения; часть 1: характеристики и подхарактеристики качества;
* ISO/IEC 12119:1994; информационная технология; пакеты программ; требования к качеству и оценка качества;
* ISO/IEC 14598-1:1997; информационная технология; оценивание программного продукта; часть 1: общее руководство;
* ISO/IEC 14598-4:1999; информационная технология; разработка программных средств; процессы для заказчика;
* ISO/IEC 15288: 2000; управление жизненным циклом; процессы жизненного цикла системы;
* MIL-STD-498:1994; разработка и документирование программного обеспечения;
* ISO TR 9127:1988; системы обработки информации – документация пользователя и сопроводительная информация для пакетов программ потребителя;
* ISO 14102:1995; информационная технология – Оценивание и выбор инструментальных средств CASE.
* ГОСТ Р ИСО/МЭК 12207:2000; информационная технология; процессы жизненного цикла программного обеспечения;
* ГОСТ Р ИСО/МЭК 9126:1993; информационная технология; оценка программной продукции; характеристики качества и руководство по их применению;
* ГОСТ Р ИСО/МЭК ТО 9294:1993; информационная технология; руководство по управлению документированием программного обеспечения;
* ГОСТ Р ИСО 9127:1994; системы обработки информации; документация пользователя и информация на упаковке для потребительских программных пакетов;
* ГОСТ 28195:1989; оценка качества программных средств; общие положения

# Приложения

## Приложение № 1

**Глоссарий**

| **Название термина** | **Толкование термина** |
| --- | --- |
| **BGP** | Border Gateway Protocol основной [протокол](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8) динамической [маршрутизации](http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) в сети Интернет |
| **EIGRP** | [Протокол](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) [маршрутизации](http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F), разработанный фирмой [Cisco](http://ru.wikipedia.org/wiki/Cisco) Systems на основе протокола [IGRP](http://ru.wikipedia.org/wiki/IGRP) той же фирмы. EIGRP использует механизм DUAL для выбора наиболее короткого [маршрута](http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82). |
| **GRE** | Generic Routing Encapsulation протокол туннелирования, инкапсулирующий пакеты сетевого уровня [модели OSI](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI) в [IP](http://ru.wikipedia.org/wiki/IP) пакеты. |
| **HTTP** | протокол прикладного уровня передачи данных в первую очередь в виде текстовых сообщений. Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом. |
| **HTTPS** | расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTP, «упаковываются» в криптографический протокол SSL или TLS, тем самым обеспечивается защита этих данных |
| **IPsec** | Механизмы защиты передаваемых данных по протоколу Internet IP путем шифрования и проверки целостностности данных при их передаче по сетям IP |
| **IP** | Internet Protocol [маршрутизируемый](http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) [протокол](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) третьего уровня модели OSI |
| **IS-IS** | Intermediate system to intermediate system протокол внутридоменной динамической маршрутизации |

|  |  |
| --- | --- |
| **MAC-адрес** | уникальный идентификатор, сопоставляемый с различными типами оборудования для компьютерных сетей. Большинство сетевых протоколов канального уровня используют одно из трёх пространств MAC-адресов, управляемых IEEE: MAC-48, EUI-48 и EUI-64. Адреса в каждом из пространств теоретически должны быть глобально уникальными. Не все протоколы используют MAC-адреса, и не все протоколы, использующие MAC-адреса, нуждаются в подобной уникальности этих адресов |
| **OSI** | Open Systems Interconnection Basic Reference Model абстрактная [сетевая модель](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C) для коммуникаций и разработки [сетевых протоколов](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) |
| **OSPF** | Open Shortest Path First) — протокол динамической [маршрутизации](http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F), основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути [Алгоритм Дейкстры](http://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%94%D0%B5%D0%B9%D0%BA%D1%81%D1%82%D1%80%D1%8B) |
| **RADIUS** | Remote Authentication in Dial-In User Service протокол передачи аутенфикационной/авторизационной информации |
| **SSH** | Secure Shell [сетевой протокол](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) прикладного уровня, позволяющий производить [удалённое управление](http://ru.wikipedia.org/wiki/%D0%A3%D0%B4%D0%B0%D0%BB%D1%91%D0%BD%D0%BD%D0%BE%D0%B5_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5) устройствами с использованием шифрования |
| **VLAN** | Virtual Local Area Network виртуальная локальная вычислительная сеть |
| **КСПД** | Совокупность географически распределенных ЛВС и каналов связи, объединенных единое информационное пространство |
| **ЛВС** | [Компьютерная Сеть](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), покрывающая обычно относительно небольшую территорию или небольшую группу зданий |
| **НСД** | Несанкционированный доступ |
| **ОС** | базовый комплекс компьютерных программ, обеспечивающий управление аппаратными средствами компьютера, работу с файлами, ввод и вывод данных, а также выполнение прикладных программ и утилит |
| **СКС** | Структурированная кабельная система представляет собой иерархическую [кабельную](http://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C) среду передачи [электрических](http://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE) или [оптических](http://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D1%82%D0%B8%D0%BA%D0%B0) [сигналов](http://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%B3%D0%BD%D0%B0%D0%BB_%28%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D0%BA%D0%B0%29) в здании, разделённую на структурные подсистемы и состоящую из элементов — кабелей и [разъёмов](http://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B7%D1%8A%D1%91%D0%BC) |