|  |  |
| --- | --- |
|  |  |

**Техническое задание**

на инсталляцию и конфигурирование информационных систем

для нужд ПАО НПО «Наука»

г. Москва

2019

Содержание

[Аннотация 7](#_Toc525167859)

[1 Общие сведения](#_Toc525167864) 8

[1.1 Характеристика объекта автоматизации](#_Toc525167865) 8

[1.2 Перечень и наименование систем](#_Toc525167866) 8

[1.3 Сроки начала и окончания работ по внедрению](#_Toc525167867) 8

[1.4 Сведения о состоянии информационной инфраструктуры](#_Toc525167868) 9

[2 Внедрение базовых сервисов Microsoft](#_Toc525167869) 9

[2.1 Назначение базовых сервисов Microsoft](#_Toc525167870) 9

[2.2 Цели внедрения базовых сервисов Microsoft](#_Toc525167871) 9

[2.3 Объекты автоматизации базовых сервисов Microsoft 9](#_Toc525167872)

[2.3.1 Пользователи 10](#_Toc525167873)

[2.3.2 Группы 10](#_Toc525167874)

[2.3.3 Персональные данные и настройки пользователей 10](#_Toc525167875)

[2.3.4 Автоматизированные рабочие места 10](#_Toc525167876)

[2.3.5 Площадка 11](#_Toc525167877)

[2.3.6 Службы каталогов 11](#_Toc525167878)

[2.4 Требования к базовым инфраструктурным службам Microsoft 11](#_Toc525167879)

[2.4.1 Перечень подсистем Системы и их назначение 11](#_Toc525167880)

[2.4.2 Требования к способам и средствам связи для информационного обмена между компонентами Системы 11](#_Toc525167881)

[2.4.3 Требования к численности и квалификации персонала Системы 11](#_Toc525167882)

[2.4.4 Показатели назначения 12](#_Toc525167883)

[2.4.5 Требования к надежности 12](#_Toc525167884)

[2.4.6 Требования безопасности 12](#_Toc525167885)

[2.4.7 Требования к защите информации от несанкционированного доступа 12](#_Toc525167886)

[2.4.8 Требования к стандартизации и унификации 12](#_Toc525167887)

[2.4.9 Требования к масштабируемости 13](#_Toc525167888)

[2.4.10 Требования к функциям, выполняемым Системой 13](#_Toc525167889)

[2.5 Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу Системы в действие 15](#_Toc525167890)

[2.5.1 Готовность объекта автоматизации к этапу «Развертывание ядра Системы» 15](#_Toc525167891)

[3 Внедрение системы виртуализации Microsoft Hyper-V 16](#_Toc525167892)

[3.1 Цели и задачи внедрения Hyper-V 16](#_Toc525167893)

[3.2 Цели и задачи внедрения Hyper-V 16](#_Toc525167894)

[3.3 Ожидаемые результаты 16](#_Toc525167895)

[3.4 Общие требования 16](#_Toc525167896)

[3.4.1 Расположение 16](#_Toc525167897)

[3.4.2 Требования к документированию 17](#_Toc525167898)

[3.4.3 Общие требования к приемке работ 17](#_Toc525167899)

[3.4.4 Требования к сетевой инфраструктуре 17](#_Toc525167900)

[3.4.5 Требования к модели управления 17](#_Toc525167901)

[3.4.6 Требования к эргономике и технической эстетике 17](#_Toc525167902)

[3.4.7 Требования к защите от влияния внешних воздействий 17](#_Toc525167903)

[3.5 Требования к системе 18](#_Toc525167904)

[3.5.1 Требования к совместимости 18](#_Toc525167905)

[3.5.2 Требования к защите информации 18](#_Toc525167906)

[3.5.3 Требования к сохранности информации 18](#_Toc525167907)

[3.5.4 Требования к сетевой инфраструктуре 18](#_Toc525167908)

[3.5.5 Сети 18](#_Toc525167909)

[3.5.6 Сетевые настройки и IP-адреса 19](#_Toc525167910)

[3.5.7 DNS 19](#_Toc525167911)

[3.5.8 Роль домена 19](#_Toc525167912)

[3.5.9 Требования к сетевым коммуникациям 19](#_Toc525167913)

[3.5.10 Требования к ПО 19](#_Toc525167914)

[3.5.11 Разрядность 19](#_Toc525167915)

[3.5.12 Однородность 20](#_Toc525167916)

[3.5.13 Хранение 20](#_Toc525167917)

[3.5.14 Требования к именованию 20](#_Toc525167918)

[3.6 Требования к платформе 20](#_Toc525167919)

[3.6.1 Требования к операционным системам виртуальных машин 20](#_Toc525167920)

[3.6.2 Требования к виртуальной сети 21](#_Toc525167921)

[3.6.3 Ограничения, накладываемые на ВМ 21](#_Toc525167922)

[4 Внедрение системы объединенных коммуникаций на базе Microsoft Skype for Business 22](#_Toc525167923)

[4.1 Назначение и цели создания системы 22](#_Toc525167924)

[4.2 Назначение системы 22](#_Toc525167925)

[4.3 Цель внедрения системы 22](#_Toc525167926)

[4.4 Характеристика объекта автоматизации 22](#_Toc525167927)

[4.5 Общая организационная структура 22](#_Toc525167928)

[4.6 Центр обработки данных 23](#_Toc525167929)

[4.7 Требования к системе 23](#_Toc525167930)

[4.7.1 Требования к системе в целом 23](#_Toc525167931)

[4.7.2 Требования к структуре и функционированию системы 23](#_Toc525167937)

[4.1.1 Требования к надежности 24](#_Toc525167938)

[4.1.2 Требования к безопасности 24](#_Toc525167939)

[4.1.3 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы 25](#_Toc525167940)

[4.1.4 Требования по обеспечению пожарной безопасности и электробезопасности 25](#_Toc525167941)

[4.1.5 Требования к защите информации от несанкционированного доступа 25](#_Toc525167942)

[4.1.6 Требования по стандартизации и унификации 26](#_Toc525167943)

[4.8 Требования к функциям (задачам), выполняемым системой 26](#_Toc525167944)

[4.8.1 Общие требования к системе 26](#_Toc525167947)

[4.8.2 Общие требования к звонкам 26](#_Toc525167948)

[4.9 Состав и содержание работ по внедрению системы 26](#_Toc525167949)

[5 Внедрение системы почтовых сообщений на базе Microsoft Exchange 27](#_Toc525167950)

[5.1 Назначение и цели создания системы почтовых сообщений 27](#_Toc525167951)

[5.2 Назначение системы почтовых сообщений 27](#_Toc525167952)

[5.3 Цели создания СПС 27](#_Toc525167953)

[5.4 Характеристика объекта автоматизации 28](#_Toc525167954)

[5.5 Требования к СПС 28](#_Toc525167955)

[5.5.1 Требования к СПС в целом 28](#_Toc525167956)

[5.5.2 Требования к численности и квалификации персонала и режиму его работы 29](#_Toc525167957)

[5.5.3 Показатели назначения 29](#_Toc525167958)

[5.5.4 Требования к надежности 30](#_Toc525167959)

[5.5.5 Требования по безопасности 30](#_Toc525167960)

[5.5.6 Требования к защите информации от несанкционированного доступа 31](#_Toc525167961)

[5.5.7 Требования к защите и сохранности информации 31](#_Toc525167962)

[5.6 Требования к функциям (задачам) 32](#_Toc525167963)

[5.6.1 Требования к вычислительному оборудованию СПС 32](#_Toc525167964)

[5.6.2 Требования к СХД 32](#_Toc525167965)

[5.6.3 Требования к архитектуре службы почтовых сообщений 32](#_Toc525167966)

[5.6.4 Требования к подсистеме предварительной фильтрации 33](#_Toc525167967)

[5.6.5 Требования к подсистеме обеспечения внешнего доступа 34](#_Toc525167968)

[5.7 Требования к видам обеспечения 34](#_Toc525167969)

[5.7.1 Требования к лингвистическому обеспечению 34](#_Toc525167970)

[5.7.2 Требования к программному обеспечению 34](#_Toc525167971)

[5.7.3 Требования к техническому обеспечению 34](#_Toc525167972)

[5.7.4 Требования к организационному обеспечению 35](#_Toc525167973)

[6 Внедрение системы управления базами данных под управлением Microsoft SQL Server 35](#_Toc525167974)

[6.1 Назначение и цели внедрения системы 35](#_Toc525167975)

[6.2 Назначение системы 35](#_Toc525167976)

[6.3 Цели создания системы 36](#_Toc525167977)

[6.4 Характеристика ИТ-инфраструктуры заказчика 36](#_Toc525167978)

[6.5 Требования к системе 36](#_Toc525167979)

[6.6 Общие требования к системе 36](#_Toc525167980)

[6.6.1 Требования к структуре системы 36](#_Toc525167981)

[6.6.2 Требования к надежности 37](#_Toc525167988)

[6.6.3 Требования к защите информации от несанкционированного доступа 37](#_Toc525167989)

[6.7 Требования к видам обеспечения 38](#_Toc525167990)

[6.7.1 Требования к программному обеспечению 38](#_Toc525167991)

[6.7.2 Требования к аппаратному обеспечению 38](#_Toc525167992)

[6.7.3 Требования к сетевым протоколам 38](#_Toc525167993)

[6.7.4 Требования к учетным записям 38](#_Toc525167994)

[6.7.5 Требования к техническому обеспечению 38](#_Toc525167995)

[7 Система резервного копирования под управлением Microsoft System Center Data Protection Manager 39](#_Toc525167996)

[7.1 Структура и описание решения 39](#_Toc525167997)

[7.2 Назначение системы 39](#_Toc525167998)

[7.3 Описание объекта автоматизации 39](#_Toc525167999)

[7.4 Цели внедрения решения 39](#_Toc525168000)

[7.5 Ожидаемые результаты внедрения 39](#_Toc525168001)

[7.6 Задачи проекта 39](#_Toc525168002)

[7.7 Требования к проектируемой системе 40](#_Toc525168003)

[7.7.1 Состав системы 40](#_Toc525168004)

[7.7.2 Компоненты системы 40](#_Toc525168005)

[7.7.3 Безопасность 41](#_Toc525168006)

[7.7.4 Взаимодействие агентов с серверами управления 41](#_Toc525168007)

[7.8 Требования к функционированию системы 41](#_Toc525168008)

[7.8.1 Требования к функциональным возможностям системы 41](#_Toc525168009)

[7.8.2 Требования к системе резервного копирования 41](#_Toc525168010)

[7.8.3 Требования к хранению данных 42](#_Toc525168011)

[7.8.4 Требования к клиентам системы 42](#_Toc525168012)

[7.8.5 Требования к взаимодействию с внешними системами 42](#_Toc525168013)

[7.8.6 Требования к надежности 43](#_Toc525168014)

[7.9 Требования к информационной безопасности 43](#_Toc525168015)

[7.9.1 Требования к взаимодействию между компонентами системы 43](#_Toc525168016)

[7.9.2 Требования к разделению доступа к системе 43](#_Toc525168017)

[7.9.3 Требования к использованию служебных учетных записей 44](#_Toc525168018)

[7.10 Требования к масштабированию 44](#_Toc525168019)

[7.11 Требования к программному обеспечению 44](#_Toc525168020)

[7.12 Требования к аппаратному обеспечению. 44](#_Toc525168021)

[7.13 Требования к сетевой инфраструктуре 45](#_Toc525168022)

[7.14 Состав и требования к проектной документации 45](#_Toc525168023)

[7.14.1 Требования к документу «Пояснительная записка» 46](#_Toc525168024)

[7.15 Требования к численности и квалификации персонала 46](#_Toc525168025)

[7.16 Условия и режим эксплуатации 46](#_Toc525168026)

# Аннотация

Данный документ содержит техническое задание на инсталляцию и последующую настройку различных информационных систем для ПАО НПО «НАУКА»

1. Общие сведения

Настоящее техническое задание (ТЗ) определяет назначение, общие и специальные требования к информационным системам и инфраструктурным сервисам, внедряемым в рамках проекта.

* 1. Характеристика объекта автоматизации

ПАО НПО «Наука» — российское промышленное предприятие, занимающееся разработкой и производством систем кондиционирования воздуха, систем автоматического регулирования давления летательных аппаратов, систем жизнеобеспечения космических аппаратов и входящих в них агрегатов

Полное наименование — Публичное акционерное общество Научно-производственное объединение «Наука».

* 1. Перечень и наименование систем

В документе изложены требования к следующим системам:

Базовые инфраструктурные сервисы Microsoft:

* + Служба каталогов Active Directory;
  + Система доменных имен DNS;
  + Служба DHCP;
  + Служба активации KMS;

Система виртуализации Microsoft Hyper-V;

Система объединенных коммуникаций Microsoft Skype for Business;

Система почтовых сообщений Microsoft Exchange;

Система управления базами данных Microsoft SQL Server;

Система резервного копирования Microsoft System Center Data Protection Manager;

Документ описывает требования к каждой системе индивидуально.

* 1. Сроки начала и окончания работ по внедрению

Контроль сроков ведется согласно план-графику ведения работ. Сроки могут быть скорректированы со стороны Исполнителя и Заказчика в рамках ведения работ по проекту. Для изменения сроков работ необходимо согласование обновленного план-графика работ со стороны Заказчика и Исполнителя.

* 1. Сведения о состоянии информационной инфраструктуры

НПО НАУКА на сегодняшний день не имеет полнофункциональных инфраструктурных сервисов Microsoft на развертываемой площадке во Владимирской обл, но имеет работающую инфраструктуру в г. Москве. По результатам проекта предполагается внедрение самостоятельных ИТ сервисов на площадке во Владимирской области и объединение их с московскими в единую сеть.

1. Внедрение базовых сервисов Microsoft
   1. Назначение базовых сервисов Microsoft

Внедрение базовых сервисов Microsoft в сети Заказчика предназначены для обеспечения следующих функций:

Аутентификация и идентификация пользователей и сетевых ресурсов.

Обеспечение IP адресации сети предприятия;

Единообразие настроек пользовательской рабочей среды;

Хранение данных и настроек информационной среды в централизованной базе данных;

Управление групповыми политиками;

Автоматизацию активации ПО и выдачи лицензий для программных продуктов Microsoft.

Объектом управления внедряемой системы является часть парка вычислительной техники Заказчика.

* 1. Цели внедрения базовых сервисов Microsoft

Целями создания инфраструктурных сервисов Microsoft в НПО НАУКА являются:

Снижение общих затрат на обслуживание инфраструктуры;

Повышение эффективности управления информационной инфраструктурой посредством создания единого каталога информационных ресурсов и, тем самым, обеспечение их быстрого поиска, унифицированного представления и удобства управления;

Повышение управляемости и безопасности информационной среды НПО НАУКА посредством назначения группам пользователей обязательных политик безопасности, а также использования встроенных в Windows XP/7/8/10 средств безопасности;

Обеспечение распределенного администрирования и централизованного контроля информационных систем НПО НАУКА;

Построение основы для внедрения современных систем коллективной работы и обмена информацией (информационные порталы, почтовые системы, средства документооборота и пр.);

Снижение затрат на обслуживание систем в филиалах НПО НАУКА;

Возможность использования функционала службы по активации лицензий.

* 1. Объекты автоматизации базовых сервисов Microsoft

Основными типами объектов автоматизации Заказчика в создаваемой Системе являются:

Пользователи.

Группы.

Персональные данные и настройки пользователей.

Автоматизированные рабочие места.

Сетевые устройства

Бизнес-приложения.

Службы каталогов.

* + 1. Пользователи

Под пользователем, в рамках проекта, понимается уникальная учетная запись пользователя, находящаяся в службе каталогов Microsoft Active Directory и активно использующаяся сотрудником Заказчика, за которым она закреплена, для доступа к ресурсам информационной среды.

В создаваемой Системе каждая учетная запись пользователя должна иметь уникальное значение атрибутов samAccountName и userPrincipalName.

* + 1. Группы

Под группой, в рамках проекта, понимается уникальная учетная запись группы, находящаяся в одной из унаследованных служб каталогов Microsoft Active Directory. Группы разделяются на следующие типы:

Группы (списки) рассылки.

Группы безопасности.

Группы также разделяются по области действия:

Локальные доменные группы.

Глобальные группы.

Универсальные группы.

В создаваемой Системе каждая учетная запись группы должна иметь уникальное значение атрибута samAccountName.

* + 1. Персональные данные и настройки пользователей

Под персональными данными и настройками пользователей, в рамках проекта, понимается содержимое локального профиля пользователя в системе Windows на его рабочей станции или перемещаемый профиль, расположенный на файловом сервере.

* + 1. Автоматизированные рабочие места

Под автоматизированным рабочим местом (АРМ), в рамках проекта, понимается совокупность компьютера, расположенного на площадке Заказчика, с установленной на нем клиентской ОС одной из следующих версий:

Microsoft Windows XP Professional Service Pack 3 или более поздняя версия;

Microsoft Windows Vista Business/Ultimate Service Pack 1 или более поздняя версия;

Microsoft Windows 7 Professional/Ultimate;

Microsoft Windows 8 Professional;

Microsoft Windows 10 Professional/Enterprise.

А также учетной записи компьютера, находящейся в службе каталогов Active Directory, удовлетворяющая следующим требованиям:

NetBIOS-имя АРМ уникально в пределах создаваемой Системы.

* + 1. Площадка

Под площадкой в рамках проекта понимается территориально обособленный объект, на котором размещены АРМ и/или серверное оборудование, входящие в состав создаваемой Системы.

* + 1. Службы каталогов

Под службами каталогов, в рамках проекта, понимаются развернутые леса и домены, входящие в состав служб каталогов производства компании Microsoft, на площадке Заказчика.

* 1. Требования к базовым инфраструктурным службам Microsoft
     1. Перечень подсистем Системы и их назначение

Система должна состоять из следующих основных подсистем:

Единая служба каталогов Microsoft Active Directory 2016 (ЕСК) – предназначена для обеспечения единой точки аутентификации пользователей Заказчика.

Подсистема групповых политик – предназначена для принудительного применения единых настроек безопасности операционных систем контроллеров домена, серверов и рабочих станций, настроек приложений и рабочего окружения пользователей.

Служба DNS на базе Microsoft Windows Server 2016 – предназначена для обеспечения разрешения доменных имен в IP-адреса и наоборот, наличие подсистемы является обязательным для функционирования ЕСК.

Служба DHCP на базе Microsoft Windows Server 2016 – предназначена для управления раздачей IP адресов устройствам во внутренней сети компании Заказчика.

Служба времени на базе Microsoft Windows Server 2016 – предназначена для синхронизации времени операционных систем на контроллерах домена, рядовых серверах и рабочих станциях в рамках единой службы каталогов.

Служба DFS на базе Microsoft Windows Server 2016 – предназначена для централизованного распространения и публикации корпоративных бизнес-приложений во внутренней сети компании Заказчика.

* + 1. Требования к способам и средствам связи для информационного обмена между компонентами Системы

Входящие в состав Системы подсистемы в процессе функционирования должны осуществлять автоматизированный информационный обмен данными на основе взаимодействия с сетевыми службами, реляционными базами данных или обмена файлами. Для обеспечения информационного обмена по сети должны использоваться прикладные протоколы на основе стека протоколов TCP/IP.

* + 1. Требования к численности и квалификации персонала Системы

Рекомендации по численности, квалификации, режиму работы и функциям эксплуатационного персонала Системы должны быть определены в проектной документации, разрабатываемой Исполнителем на этапе «Проектирование архитектуры».

* + 1. Показатели назначения

Система должна отвечать следующим показателям назначения:

Система должна быть рассчитана на обслуживание 200 пользователей и АРМ, должна иметь возможность увеличения количества пользователей и АРМ без изменения архитектуры Системы.

Система должна допускать горизонтальное масштабирование.

Система должна сохранять работоспособность при увеличении количества пользователей и рабочих станций в пределах поддерживаемых аппаратно-программной средой серверного ядра.

* + 1. Требования к надежности

Для обеспечения надежности Системы ее ключевые компоненты должны резервироваться. Резервирование должно предусматривать обеспечение функций аутентификации пользователей и авторизации их доступа к ресурсам при выходе из строя любого единичного сервера Системы.

Для выполнения требований надежности и доступности Системы должно быть предусмотрено резервное копирование серверов, обеспечивающих функционирование Системы. В рассматриваемом проекте Active Directory будет реализован на двух раздельных контроллерах домена. Тем самым будет обеспечиваться избыточность и доступность сервиса при отказе одного из контроллеров домена.

* + 1. Требования безопасности

Аппаратные помещения, предоставляемые Заказчиком для размещения серверного оборудования Системы, должны обеспечивать надежную физическую защиту оборудования Системы от доступа к ней посторонних. Круг лиц, имеющих допуск в эти помещения, должен быть ограничен и согласован со службой безопасности Заказчика.

* + 1. Требования к защите информации от несанкционированного доступа

Должна быть обеспечена программная и аппаратная защита от неквалифицированных действий пользователя и от попыток несанкционированного доступа пользователей к внутрисистемной информации.

В зависимости от статуса пользователя, должны быть предусмотрены различные уровни доступа к внутрисистемной информации.

Должна быть обеспечена физическая защита компонентов Системы от попыток несанкционированного доступа посторонних лиц.

* + 1. Требования к стандартизации и унификации

При создании Системы необходимо руководствоваться принципом унификации с точки зрения использования типовых проектных и конструктивных решений, а также принципом стандартизации с точки зрения соответствия стандарту именования, принятому в рамках проекта. Следование указанным принципам обеспечивает возможность многократного использования проектных решений, простоту наращивания и взаимодействия, а также взаимозаменяемость на уровнях блоков, устройств, модулей и программно-алгоритмического обеспечения.

* + 1. Требования к масштабируемости

Система должна обеспечивать возможность отражения изменений организационной структуры предприятия, увеличения численности персонала и территориального расположения объектов без переработки основных проектных решений.

* + 1. Требования к функциям, выполняемым Системой

Требования к подсистеме ЕСК

Создаваемая ЕСК должна удовлетворять следующим функциональным требованиям:

Обеспечить единую точку аутентификации пользователей Заказчика на основе протоколов NTLM и Kerberos при подключении из любой точки внутри корпоративной сети.

Обеспечить непосредственную защиту от несанкционированного доступа к информационным ресурсам Заказчика.

Обеспечить поиск информационных ресурсов внутри каталога, унифицированное представление данных и средств управления.

Реализовать централизованную модель управления серверами и сервисами с автоматизированным делегированием утвержденных полномочий специалистам Заказчика.

Поддерживать авторизацию доступа пользователей к объектам ЕСК и подключенных к ЕСК систем на базе ОС семейства Microsoft Windows.

Обеспечить возможность использования набора групповых политик для управления конфигурацией рабочих мест.

Обеспечить возможность управления трафиком репликации собственных данных, в том числе, возможность минимизации объема этого трафика за счет оптимального проектирования логической и физической структуры ЕСК, а также применения механизма репликации данных Active Directory по расписанию.

Позволять осуществлять автоматизированную миграцию пользователей и ресурсов из унаследованных служб каталогов семейства Microsoft Active Directory.

Позволять осуществлять автоматизированное развертывание новых контроллеров доменов.

Позволять осуществлять автоматизированное управление сайтами и подсетями Active Directory.

Поддерживать версии Lightweight Directory Access Protocol (LDAP), соответствующие LDAPv2 и LDAPv3.

Административная модель ЕСК должна обеспечить:

Централизованное управление структурой доменов Microsoft Active Directory.

Делегирование отдельных административных задач в подразделения для создания распределенной модели управления ресурсами и учетными записями.

Требования к службе DNS

Служба DNS должна удовлетворять следующим функциональным требованиям:

Обеспечить предоставление IP адреса сетевого объекта по запросу с указанием в качестве параметра такого запроса доменного имени данного сетевого объекта.

Обеспечить предоставление IP адреса сервера, реализующего запросы службы, по запросу с указанием в качестве параметра имени службы.

Обеспечить предоставление доменного имени сетевого объекта по запросу с указанием в качестве параметра такого запроса IP адреса данного сетевого объекта.

Обеспечить динамическое поддержание соответствия IP адресов сетевых объектов их доменным именам.

Иерархия имен DNS должна отражать иерархию имен ЕСК.

В создаваемой Системе основной службой разрешения имён должна выступать служба DNS.

Обеспечить внесение защищенных динамических обновлений в зоны DNS на любом из серверов DNS.

Обеспечить корректное взаимное разрешение доменных имен между создаваемой Системой и унаследованной инфраструктурой.

DNS Сервер должен поддерживать создание прямых и обратных зон.

Поддерживать записи типа SRV, MX, CNAME, A.

Должна быть интегрирована с подсистемой ЕСК.

Должна быть реализована в отказоустойчивой конфигурации: отказ отдельного сервера DNS не должен приводить к невозможности разрешения имен в рамках всей организации Заказчика.

Требования к службе времени

Создаваемая служба времени должна удовлетворять следующим функциональным требованиям:

Синхронизация времени должна выполняться на всех рабочих станциях и серверах, включенных в состав Системы.

Различие в системном времени между АРМ при нормальной работе Системы не должно превышать 5 минут.

Сервера службы времени должны быть реализованы на базе контроллеров доменов ЕСК.

Служба времени должна обеспечивать синхронизацию с внешними источниками точного времени не ниже второго уровня по протоколу NTP.

Требования к подсистеме Групповых политик

Групповые политики новой ЕСК должны отвечать требованиям безопасности Заказчика.

Требования к службе DHCP

Динамическое предоставление IP адресов для сетевых устройств заказчика, в том числе АРМ, серверов, принтеров, мобильных персональных устройств и др.

Система службы DHCP должна иметь высокую производительность для обеспечения функциональных требований инфраструктуры заказчика.

Служба DHCP должна отвечать требованиям отказоустойчивости, даже в случае выхода из строя одного из серверов системы.

Требования к использованию службы KMS

Для возможности использования службы KMS, должны быть выполнены следующие условия:

Сервер службы KMS должен быть установлен на Windows Server 2016, настроен и включен.

Клиенты KMS должны иметь доступ к серверам DNS организации и к серверу службы KMS.

Средство управления активацией корпоративных лицензий должно быть установлено на центральном компьютере, имеющем сетевой доступ ко всем клиентским компьютерам.

Активируемые продукты должны быть добавлены в Средство управления активацией корпоративных лицензий. Должны быть установлены ключи на все активируемые продукты.

Средство Средство управления активацией корпоративных лицензий должно иметь административные разрешения на всех активируемых компьютерах, а инструментарий управления Windows должен быть доступен через брандмауэр Windows.

* 1. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу Системы в действие
     1. Готовность объекта автоматизации к этапу «Развертывание ядра Системы»

Заказчиком должно быть предоставлено оборудование и программное обеспечение, необходимое для создания.

Заказчиком должна быть утверждена готовность объекта автоматизации к развертыванию ядра по всем перечисленным критериям. Перед подписанием данного документа Заказчиком должны быть выполнены следующие подготовительные работы:

Обеспечено наличие помещений для размещения оборудования Системы, непосредственная установка оборудования в коммутационные шкафы, а также подключение этого оборудования к сети электропитания и к корпоративной вычислительной сети на всех площадках, где предполагается его установка.

Обеспечены условия для отсутствия несанкционированного физического доступа к серверам Системы.

Обеспечено использование стека протокола TCP/IP всеми серверами, входящими в состав создаваемой Системы.

Выделены необходимые IP-адреса для оборудования, входящего в состав создаваемой Системы.

Обеспечено использование единого пространства IP-адресов для создаваемой Системы без использования механизма преобразования адресов NAT.

Обеспечено наличие возможности установления соединения между серверами, составляющими Систему (между собой).

1. Внедрение системы виртуализации Microsoft Hyper-V
   1. Цели и задачи внедрения Hyper-V

Microsoft Hyper-V — система виртуализации для x64-систем на основе гипервизора. Гипервизор обеспечивает параллельное выполнение нескольких ОС на одном и том же хосте, изоляцию операционных систем друг от друга, защиту и безопасность, разделение ресурсов между различными запущенными ОС и управление ресурсами.

Система в среде Заказчика служит нескольким задачам:

Уменьшает потребность в физических серверах путем разделения ресурсов между разными ОС;

Изолирует операционные системы друг от друга;

Обеспечивает защиту и безопасность;

Сокращает расходы на электропитание и охлаждение серверов;

Упрощает управление ресурсами.

* 1. Цели и задачи внедрения Hyper-V

Задачами внедрения системы являются:

Установка и настройка средств Hyper-V;

Сокращение количества и времени простоя информационных систем для повышения непрерывности бизнеса за счет преимуществ виртуализации;

Обеспечение максимальной работоспособности и производительности используемых в компании приложений, сервисов и операционных систем;

Повышение управляемости и безопасности IT-инфраструктуры;

Стандартизация конфигураций и соответствие требованиям;

Обеспечение единым решением по управлению виртуальной средой всей компании, в том числе в удаленных офисах.

* 1. Ожидаемые результаты

Ожидаемым результатом внедрения Hyper-V Windows Server 2016 является работоспособная система без необходимости дополнительной настройки.

* 1. Общие требования
     1. Расположение

Реализуемое внедрение выполняется на существующей инфраструктуре Заказчика. При необходимости в текущую инфраструктуру должны быть внесены соответствующие изменения, добавлены новые компоненты или изменены настройки и состав уже существующих компонентов.

* + 1. Требования к документированию

Комплект проектных материалов должен быть предоставлен в следующем объеме:

Техническое задание.

Пояснительная записка.

Вся разрабатываемая проектная документация должна быть выполнена на русском языке в формате Word 2007 и выше.

* + 1. Общие требования к приемке работ

Порядок контроля и приёмки работы: на время проведения работ Заказчик предоставляет рабочее место для сотрудников Исполнителя, а также согласовывает с Исполнителем выделение последнему административных полномочий в ИТ-инфраструктуре, необходимых для реализации работ. Работы по проекту проводятся в офисе Заказчика в г. Москве. По согласованию с Исполнителем Заказчик предоставляет рабочее время своих специалистов для консультаций по внутренним бизнес-процессам, служебным обязанностям и влиянию системы на них.

* + 1. Требования к сетевой инфраструктуре

Все части системы связаны между собой информационными сетями, с использованием имеющихся локальных и глобальных вычислительных сетей Заказчика.

Внутри объектов автоматизации в рамках разрабатываемой системы компоненты системы связаны между собой высокоскоростной локальной сетью на базе технологий Ethernet с пропускной способностью не менее 1000 Мбит/с.

В качестве основного транспортного протокола данных информационных сетей используется протокол TCP/IP.

* + 1. Требования к модели управления

В рамках проекта для разграничения прав доступа должны быть использованы ролевые группы. Ролевые группы размещаются в специальном контейнере, доступ к которому имеет только администратор домена. Первичное делегирование прав выполняет администратор домена.

* + 1. Требования к эргономике и технической эстетике

Предлагаемое решение должно строиться на базе последних версий ПО компании Microsoft.

* + 1. Требования к защите от влияния внешних воздействий

В предоставленных Заказчиком помещениях для размещения серверов, где будут располагаться сервера Hyper-V, должны обеспечиваться условия эксплуатации, определяемые требованиями со стороны производителей этого оборудования.

Оборудование должно размещаться в помещениях, имеющих выделенную розеточную электросеть 220В 10%, 50 Гц с защитным заземлением. Должно обеспечиваться бесперебойное электропитание такого оборудования при пропадании внешнего электропитания, достаточного для штатного выключения.

* 1. Требования к системе
     1. Требования к совместимости

Проектные решения должны учитывать необходимость интеграции разворачиваемого программного обеспечения с существующей службой каталога Active Directory Заказчика.

* + 1. Требования к защите информации

Разграничение и администрирование доступа к компонентам Hyper-V должно осуществляться системными администраторами в соответствии с компетенцией должностных лиц. Уровень компетенции определяется в соответствии с организационными распорядительными документами Заказчика.

Разрабатываемая система должна обеспечивать логическое разграничение прав доступа на чтение и изменение хранящейся информации на уровне объектов подсистемы службы единого каталога.

* + 1. Требования к сохранности информации

Сохранность информации должна быть обеспечена в случае наступления следующих событий:

Отключение электропитания технических средств;

Отказ линий связи;

Отказ аппаратуры сервера (процессор, накопители на жестких дисках) - отказ технических средств;

Отказ программного обеспечения.

Для повышения отказоустойчивости системы должны быть разработаны специальные процедуры защиты важнейших информационных ресурсов при отказах и сбоях.

Защите подлежат следующие информационные ресурсы:

* Роли
* Приложения
* Виртуальные машины
* Конфигурационные файлы
* Информация о текущем состоянии ОС на конечном сервере (System State).
  + 1. Требования к сетевой инфраструктуре
    2. Сети

Рекомендуется использовать как минимум две сети: общедоступную сеть, которая позволяет клиентам подключаться к системе и отдельной сети, которая используется только для связи между серверами. При необходимости вы можете настроить дополнительные сети для определенных параметров хранения или для резервирования.

* + 1. Сетевые настройки и IP-адреса

При использовании идентичных сетевых адаптеров для сети также используйте одинаковые настройки связи для этих адаптеров (например, скорость, дуплексный режим, управление потоком и тип носителя). Кроме того, необходимо, чтобы настройки между сетевым адаптером и коммутатором, к которому он подключается, не содержали конфликтующей конфигурации.

* + 1. DNS

Серверы должны использовать систему доменных имен (DNS) для разрешения имен. Можно использовать протокол динамического обновления DNS.

* + 1. Роль домена

Все серверы должны находиться в домене Active Directory.

* + 1. Требования к сетевым коммуникациям

Компоненты системы взаимодействуют между собой по портам и протоколам, представленным в следующей таблице:

| Номера порта,  Протокол | Описание |
| --- | --- |
| 443, TCP | HTTPS (HTTP over TLS/SSL) |
| 1433, TCP | Microsoft SQL Server |
| 5986, TCP | Используется для подключения к хостам Hyper-V |
| 8100, TCP | Используется для подключения консоли к серверу |

* + 1. Требования к ПО

Ниже приведены требования к программному обеспечению для использования функций Hyper-V:

* Windows Server 2016 Datacenter
* Все серверы должны иметь одинаковые обновления программного обеспечения (патчи) и пакеты обновления.
* Hyper-V-специфичные командлеты для Windows PowerShell.

Требования к серверному оборудованию

* + 1. Разрядность

Для Hyper-V требуется 64-разрядный процессор, который включает в себя следующее:

* Аппаратная виртуализация. Это доступно в процессорах, которые включают в себя вариант виртуализации - в частности, процессоры с технологией Intel Virtualization Technology (Intel VT) или AMD Virtualization (AMD-V).
* Предотвращение выполнения данных (DEP) должно быть доступно и включено. В частности, вы должны включить бит Intel XD (выполнить бит блокировки) или бит AMD NX (без бит выполнения).
  + 1. Однородность

Microsoft рекомендует использовать набор подходящих компьютеров, которые содержат либо те же, либо аналогичные функции.

* + 1. Хранение

Для нужд Hyper-V предполагается использовать локальные системы хранения на каждом из четырех серверов.

* + 1. Требования к именованию

Именование Hyper-V серверов должно соответствовать текущему соглашению об именовании и иметь следующие имена компонентов:

|  |  |  |
| --- | --- | --- |
| # | Имя компонента | Сущность |
| 1. |  | Имена Hyper-V серверов |

* 1. Требования к платформе
     1. Требования к операционным системам виртуальных машин

Hyper-V Windows Server 2016 поддерживает следующие операционные системы:

1. Семейство Windows Server:

Windows Server 2016

Windows Server 2012R2

Windows Server 2012

Windows Server 2008R2 SP1

Windows Server 2012R2 SP2

1. Семейство Windows Client:

* Windows 10
* Windows 8.1
* Windows 7 SP1

1. Семейство RHEL/CentOS x64:

* RHEL/CentOS 7.x
* RHEL/CentOS 6.x за исключением 6.0-6.3
* RHEL/CentOS 5.x за исключением версий раньше 5.9

1. Семейство Debian:

* Debian 9.0-9.5 (stretch)
* Debian 8.0-8.11 (jessie)
* Debian 7.0-7.11 (wheezy)

1. Семейство Oracle Linux x64:

* RHCK 6.4-6.8 и 7.0-7.3
* UEK R4
* UEK R3 QU3
* UEK R3 QU2
* UEK R3 QU1

1. Семейство SUSE x64:

* SLES 12 SP2
* SLES 12 SP1
* SLES 12
* SLES 11 SP4
* SLES 11 SP3
* SLES 11 SP2
* Open SUSE 12.3

1. Семейство Ubuntu:

* 17.04
* 16.10
* 16.04 LTS
* 14.04 LTS
* 12.04 LTS

1. Семейство FreeBSD:

* 11.1
* 11.0
* 10.3
* 10.2
* 10.0-10.1
* 9.1-9.3, 8.4
  + 1. Требования к виртуальной сети

Гипервизор должен обеспечивать подключение виртуальных машин к ЛВС через настроенные виртуальные коммутаторы

* + 1. Ограничения, накладываемые на ВМ

На виртуальные машины в Hyper-V Windows Server 2016 накладываются следующие ограничения:

* Не более 50 чекпоинтов;
* Максимальный объем оперативной памяти для виртуальных машин второго поколения -12 ТБ, для первого – 1 ТБ;
* Не более двух COM-портов;
* Не более четырех виртуальных Fiber Channel адаптеров;
* Максимальный объем жесткого диска не превышает 64 ТБ для VHDX формата, 2040 ГБ для VHD формата;
* Не более четырех IDE дисков;
* Максимальное количество виртуальных процессоров не превышает 240 для виртуальных машин второго поколения, 64 – для первого, 320 доступных для операционной системы хоста;
* Не более четырех виртуальных SCSI контроллеров;
* Не более 256 виртуальных SCSI дисков;
* Не более 12 виртуальных сетевых адаптеров: 8 специальных сетевых адаптеров Hyper-V и 4 legacy сетевых адаптеров;

1. Внедрение системы объединенных коммуникаций на базе Microsoft Skype for Business
   1. Назначение и цели создания системы

В данном разделе приведено описание целей внедрения системы объединённых коммуникаций.

* 1. Назначение системы

Система предназначена для обеспечения пользователей возможностями современных технологий и инструментов системы объединённых коммуникаций.

* 1. Цель внедрения системы

Целью внедрения системы является повышение эффективности деятельности сотрудников НПО "НАУКА" за счет подключения пользователей к унифицированной системе объединённых коммуникаций, а также оптимизация затрат на каналы связи, аренду прямых городских номеров и командировочные расходы.

* 1. Характеристика объекта автоматизации

В данном разделе приведено краткое описание объекта автоматизации.

* 1. Общая организационная структура

Организационная структура Заказчика предоставляет из себя 2 локации с общей численностью рабочих станций в 700 штук. Все площадки входят в единый автономный доменный лес.

* 1. Центр обработки данных

Центр обработки данных для размещения сервиса расположен на площадке в городе Владимир. По адресу: 601023, Владимирская область, Киржачский район, пос.Першино, ул.Школьная, д.7а

* 1. Требования к системе
     1. Требования к системе в целом

Внедряемые решения должны соответствовать разработанным решениям, описанным в проектной документации.

Серверы и объекты должны входить в состав Единого леса Службы каталога Заказчика.

4. 1. 1. Требования к структуре и функционированию системы

Требования к способам и средствам связи для информационного обмена между компонентами системы

Информационный обмен между компонентами системы объединённых коммуникаций должен осуществляться через единое информационное пространство и посредством использования стандартизированных протоколов и форматов обмена данными поверх TCP/IP-соединения.

Требования к характеристикам взаимосвязей создаваемой системы со смежными системами

Перечень смежных систем, взаимодействующих с системой объединённых коммуникаций и алгоритмы взаимодействия уточняются на этапе рабочего проектирования.

Система объединённых коммуникаций не должна нарушить работоспособность существующих приложений на момент модернизации.

Требования к режимам функционирования системы

Система объединённых коммуникаций должна функционировать в следующих режимах:

* штатный режим производственной эксплуатации - период времени в течении, которого в системе объединённых коммуникаций не зафиксировано сбоев в работе служб и сервисов;
* нештатный режим производственной эксплуатации - любой период времени, в течение которого один или несколько компонентов системы объединённых коммуникаций полностью или частично недоступны;
* режим технического обслуживания и модернизации (время, не занятое штатным режимом производственной эксплуатации). В этом режиме допускаются перерывы в работе отдельных служб и сервисов системы объединённых коммуникаций.

Перспективы развития, модернизации системы

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

Система объединённых коммуникаций должна предусматривать возможность тиражирования проектного решения в будущем на филиалы НПО «НАУКА». Данная возможность должна быть отражена в проектной документации к системе объединённых коммуникаций.

Система объединенных коммуникаций должна предусматривать типовые решения для предприятий системы «НПО «НАУКА»»

* + 1. Требования к надежности

Система объединенных коммуникаций должна выполнять возложенные на нее функции в круглосуточном режиме. Вариант с возможностью системы противостоять различным авариям и сбоям в заданных условиях и отвечать предъявляемым требованиям к доступности и отказоустойчивости в рамках данного проекта не внедряется, однако, система может быть масштабирована до данного уровня в будущем. Штатный режим работы системы объединенных коммуникаций 24 часа в сутки и 7 дней в неделю.

* + 1. Требования к безопасности

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

Должно быть обеспечено соблюдение общих требований безопасности в соответствии с ГОСТ 12.2.003-91 «ССБТ. Оборудование производственное. Общие требования безопасности» при обслуживании системы объединенных коммуникаций в процессе эксплуатации.

Аппаратная часть системы объединенных коммуникаций должна быть заземлена в соответствии с требованиями ГОСТ Р 50571.22-2000 «Электроустановки зданий. Часть 7. Требования к специальным электроустановкам. Раздел 707. Заземление оборудования обработки информации».

Значения эквивалентного уровня акустического шума, создаваемого аппаратурой системы объединенных коммуникаций, должно соответствовать ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение», но не превышать следующих величин:

* 50 дБ – при работе технологического оборудования и средств вычислительной техники без печатающего устройства;
* 60 дБ – при их же работе с печатающим устройством.
  + 1. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Система объединенных коммуникаций должна обеспечивать непрерывный круглосуточный режим эксплуатации с учетом времени на техническое обслуживание.

В помещениях, предназначенных для эксплуатации системы объединенных коммуникаций, должны отсутствовать агрессивные среды, массовая концентрация пыли в воздухе должна быть не более 0,75 мг/м3, электрическая составляющая электромагнитного поля помех не должна превышать 0,3 В/м в диапазоне частот от 0,15 до 300,00 МГц. Напряжение питания сети должно быть (220 ± 5) В при частоте 50 Гц.

* + 1. Требования по обеспечению пожарной безопасности и электробезопасности

Заземления в помещениях должны быть выполнены в соответствии с ГОСТ 12.1.004-91 «ССБТ. Пожарная безопасность. Общие требования», ГОСТ Р 50571.22-2000 «Электроустановки зданий». Часть 7. «Требования к специальным электроустановкам». Раздел 707. «Заземление оборудования обработки информации», «Правилами устройства электроустановок», «Правилами техники безопасности при эксплуатации электроустановок потребителей».

Климатические факторы помещения для эксплуатации изделий должны соответствовать ГОСТ 15150-69 (с изм. 2004 г.) «Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды» для вида климатического исполнения УХЛ категории 4.2.

Нормальными климатическими условиями эксплуатации системы являются:

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

Система объединенных коммуникаций должна сохранять работоспособность при воздействии следующих климатических факторов:

* температура окружающего воздуха от 10 до 35 °С;
* относительная влажность воздуха от 40 до 80 % при температуре 25 °С.
  + 1. Требования к защите информации от несанкционированного доступа

Система объединенных коммуникаций должна предоставлять гибкие возможности по разграничению прав доступа к системе, обеспечивать защиту информации от несанкционированного доступа и средства контроля безопасности для администраторов системы объединенных коммуникаций.

Должно быть обеспечено разграничение полномочий между всеми техническими сотрудниками, занятыми обслуживанием системы.

* + 1. Требования по стандартизации и унификации

Должен быть обеспечен единый вход и прозрачный доступ к информационным ресурсам системы объединенных коммуникаций в соответствии с делегированными правами.

Должно быть обеспечено средство централизованного управления ролями пользователей и ролями администраторов системы объединенных коммуникаций.

* 1. Требования к функциям (задачам), выполняемым системой

Система объединенных коммуникаций, кроме стандартных функций и возможностей, существующих в Microsoft Skype for Business 2015 (либо с заменых этих функций более современными решениями), должна соответствовать требованиям, описание которых приведено в данном разделе.

* 2. 1. Общие требования к системе

Система должна обеспечивать весь доступный стандартный функционал, описанный в документации производителя и не требующий внедрения дополнительных служб и оборудования

В рамках проекта производится интеграция системы с шлюзами AUDIOCODES

* + 1. Общие требования к звонкам

В части звонков на SfB совместимые телефонные аппараты к системе предъявляются следующие требования:

Должна быть обеспечена возможность выполнения звонков с телефонных аппаратов, зарегистрированных в СОК, на программные клиенты SfB;

Должна быть обеспечена возможность выполнения звонков на телефонные аппараты, зарегистрированные в СОК, с программных клиентов SfB;

Должна быть обеспечена возможность выполнения звонков на городские телефонные номера, с программных клиентов SfB;

Должна быть обеспечена возможность выполнения звонков на сотовые телефонные номера, с программных клиентов SfB;

Должна быть обеспечена возможность настройки, на программных клиентах SfB, переадресации входящих звонков на сотовые телефонные номера.

* 1. Состав и содержание работ по внедрению системы

К стадиям и этапам разработки предъявляются следующие требования:

Работы по модернизации СОК должны быть выполнена в пять этапов:

* На первом этапе выполняются следующие работы:
  + Проводится обследование текущей инфраструктуры;
  + Разрабатывается Техническое задание на систему;
  + Разрабатывается План-график работ.
* На втором этапе выполняются следующие работы:
  + Разрабатывается документ Пояснительная записка;
  + Разрабатывается документ Программа и методика испытаний;
* На третьем этапе выполняются следующие работы:
  + Выполняется пилотное развертывание системы в Московском филиале Компании;
  + Проводится тестирование функционала на тестовой группе пользователей;
  + Выполняется перевод пилотного развертывания в промышленную эксплуатацию.

1. Внедрение системы почтовых сообщений на базе Microsoft Exchange
   1. Назначение и цели создания системы почтовых сообщений
   2. Назначение системы почтовых сообщений

Система почтовых сообщений (далее СПС) предназначена для решения следующих задач:

обеспечение обмена почтовыми сообщениями между сотрудниками НПО «НАУКА» и внешними получателями;

организация совместной работы сотрудников НПО «НАУКА» по управлению задачами и планированию рабочего времени.

* 1. Цели создания СПС

Основными целями создания СПС являются:

* повышение эффективности работы сотрудников Заказчика за счет предоставления новых возможностей работы с почтовой перепиской, планирования задач и рабочего времени сотрудников;
* организация доступа к почтовой службе с различных рабочих мест, в том числе извне офисов Заказчика, используя различные устройства доступа;
* повышение отказоустойчивости системы хранения почтовых сообщений;
* увеличение степени защищенности системы хранения почтовой информации;
* уменьшение рисков потери почтовых сообщений за счет обеспечения резервного копирования;
* повышение информационной безопасности за счет интеграции со службами единого каталога, новых политик фильтрации сообщений, использования ЭП и шифрования сообщений;
* уменьшение расходов на приобретение нового серверного оборудования за счет увеличения плотности вычислений;
* уменьшение общих временных затрат на выполнение типовых операций по обслуживанию системы;
* централизация управления;
* обеспечение повышенной доступности работы системы в случае выхода из строя одного из серверов;

Критериями оценки достижения целей создания СПС являются:

* перевод почты всех пользователей Заказчика на новую почтовую систему;
* использование существующей сетевой учетной записи пользователя для работы с почтой;
* использование единой адресной книги;
* использование общих календарей;
* предоставление пользователям мобильного доступа к почтовой системе;
* настройка архивных политик хранения почтовых сообщений;
* предоставление мобильного доступа из сети интернет к рабочей почте, календарям и задачам.
  1. Характеристика объекта автоматизации

Объектами автоматизации системы почтовых сообщений являются:

* Адрес площадки Заказчика;
* Существующая почтовая система Заказчика;
* Существующая служба каталогов Заказчика.
  1. Требования к СПС
     1. Требования к СПС в целом

Требования к структуре СПС

СПС должна включать в себя следующие подсистемы:

* вычислительные средства в составе:
  + серверное оборудование;
  + системы хранения данных (СХД);
* программно-техническая инфраструктура в составе:
  + служба почтовых сообщений (СПС).

Требования к совместимости со смежными системами

В СПС должна быть обеспечена интеграция и совместимость со смежными системами:

* Служба каталога Active Directory

Требования к режимам функционирования СПС

СПС должна предусматривать следующие режимы эксплуатации:

* штатный режим производственной эксплуатации;
* режим технического обслуживания;
* аварийный режим эксплуатации.

СПС в штатном режиме производственной эксплуатации должна эксплуатироваться 24 часа в сутки, 7 дней в неделю, 365 дней в году, за исключением плановых отключений компонентов СПС для регулярного обслуживания.

Режим, в котором производятся работы по модернизации, техническому обслуживанию и резервному копированию данных, считается режимом технического обслуживания. При работе в данном режиме допускается кратковременное нарушение работоспособности служб СПС.

Режим, при котором происходит отказ всей СПС или одного из ее компонентов, считается аварийным режимом эксплуатации.

Требования по диагностированию системы

Информация об отказах в работе служб, входящих в состав, и их компонентов должна заноситься в журналы событий на серверах почтовой системы.

Перспективы развития СПС

СПС должна иметь длительный жизненный цикл (не менее 5 лет). Для поддержания соответствия характеристик СПС актуальным требованиям на протяжении всего периода эксплуатации, при разработке СПС необходимо обеспечить возможность ее модернизации в процессе эксплуатации за счет выбора соответствующей архитектуры программного обеспечения и технических средств, а также за счет использования стандартизованных решений.

* + 1. Требования к численности и квалификации персонала и режиму его работы

Весь персонал, участвующий в эксплуатации, должен быть разделен на следующие функциональные группы:

пользователи, использующие в своей деятельности средства автоматизации, реализуемые СПС;

администраторы - выделенный персонал, в обязанности которого входит выполнение технологических функций по обслуживанию программных и аппаратных компонентов СПС, таких как управление настройками параметров функционирования компонентов СПС, наблюдение за работой СПС, выполнение штатного обслуживания СПС, в случае возникновения внештатных ситуаций или неисправностей - выполнение необходимых действий по устранению неисправностей.

На этапе проектирования к персоналу СПС должны быть сформулированы квалификационные требования (с учетом принадлежности к группам персонала), без выполнения которых невозможно обеспечить надлежащее функционирование СПС.

СПС не должна предусматривать принципиальных ограничений на число одновременно работающих пользователей. Это число должно зависеть только от технических характеристик используемых аппаратных средств и сетевого оборудования.

* + 1. Показатели назначения

СПС должна быть реализована как открытая и допускать наращивание функциональных возможностей.

Целевое назначение СПС должно сохраняться на протяжении всего срока эксплуатации СПС. Срок эксплуатации СПС определяется сроком устойчивой работы технических средств, своевременным проведением работ по замене (обновлению) технических средств, по сопровождению программного обеспечения СПС и его модернизации, а также при выполнении регламентных работ, которые должны быть указаны в соответствующей разрабатываемой документации. При условии постоянного выполнения этих работ целевое назначение СПС сохраняется неограниченно долго.

* + 1. Требования к надежности

В технических средствах СПС должно быть предусмотрено резервирование основных компонентов, определяющих надежность технических средств.

Должна быть предусмотрена возможность увеличения показателей надежности СПС за счет избыточности программно-аппаратного обеспечения СПС.

При выходе из строя одного сервера либо площадки целиком должна обеспечиваться возможность функционирования системы.

* + 1. Требования по безопасности

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

Аппаратное обеспечение СПС должно соответствовать требованиям пожарной безопасности в производственных помещениях по   
ГОСТ 12.1.004-91 «ССБТ. Пожарная безопасность. Общие требования».

Должно быть обеспечено соблюдение общих требований безопасности в соответствии с ГОСТ 12.2.003-91 «ССБТ. Оборудование производственное. Общие требования безопасности» при обслуживании СПС в процессе эксплуатации.

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

Значения эквивалентного уровня акустического шума, создаваемого аппаратурой СПС, должно соответствовать ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение», но не превышать следующих величин:

50 дБ - при работе технологического оборудования и средств вычислительной техники без печатающего устройства;

60 дБ - при их же работе с печатающим устройством.

* + 1. Требования к защите информации от несанкционированного доступа

Схема определения доступа должна предусматривать возможность группового или ролевого доступа, то есть создание абстрактного профиля прав пользователя. При включении нового пользователя в конкретную группу он автоматически должен наследовать все права, присущие пользователям данной группы. При этом суммарные права пользователя должны проверяться на непротиворечивость, должен применяться принцип поглощения более широкими разрешительными правами более узких (суммирование прав) и принцип преимущества запретительных прав над разрешительными. Также должна присутствовать возможность копирования (наследования) прав пользователя с возможностью последующей корректировки.

Для каждого информационного объекта должен существовать владелец объекта (с возможностью в дальнейшем заменить одного владельца на другого) с полными правами доступа. Система должна контролировать обязательное наличие хотя бы одного пользователя (владельца или администратора) для каждого информационного объекта.

Разграничение и администрирование доступа к компонентам СПС должно осуществляться администраторами СПС в соответствии с компетенцией должностных лиц. Уровень компетенции определяется в соответствии с организационными распорядительными документами Заказчика.

Разрабатываемая СПС должна обеспечивать максимально возможный уровень безопасности в соответствии с внутренними организационно-распорядительными документами Заказчика по обеспечению защиты от несанкционированного доступа.

Защита аппаратного обеспечения и системного ПО, включая антивирусную защиту, защиту каналов связи, использующихся и необходимых для функционирования СПС, осуществляется силами Заказчика.

* + 1. Требования к защите и сохранности информации

Должна быть обеспечена защита на уровне ПО от неквалифицированных действий пользователя и от попыток несанкционированного доступа пользователей к внутрисистемной информации. В зависимости от статуса пользователя, должны быть предусмотрены различные уровни доступа к внутрисистемной информации.

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

* выход из строя оборудования из состава ПС;
* выход из строя систем или каналов передачи данных;
* ошибки в программных средствах;

Требования по сохранности информации в системе должны обеспечиваться выбором технических средств, содержащих аппаратные и программные средства защиты информации, а также соответствующими организационными решениями.

Сохранность информации, размещенная в СПС, должна обеспечиваться средствами резервного копирования Заказчика.

Для восстановления данных СПС из резервной копии должны быть разработаны методики и процедуры резервного копирования.

* 1. Требования к функциям (задачам)
     1. Требования к вычислительному оборудованию СПС

Серверы виртуализации должны удовлетворять следующим требованиям:

обладать достаточными аппаратными ресурсами для размещения компонент системы;

иметь возможность подключения к сети передачи данных по протоколу TCP/IP;

иметь возможность подключения к системе хранения данных.

* + 1. Требования к СХД

Подсистема хранения данных должна удовлетворять следующим требованиям:

обеспечивать необходимое дисковое пространство, требуемое для размещения файлов СПС;

* + 1. Требования к архитектуре службы почтовых сообщений

Служба почтовых сообщений (далее - СПС) должна быть реализована на базе ПО Microsoft Exchange Server 2016.

СПС должна обеспечить выполнение следующих функций:

* предоставить пользователям компании сервис электронной почты со своих АРМ доступ должен предоставляться через установленный локально клиент Microsoft Outlook (версии не ниже 2010) и через Outlook Web App (OWA);
* обеспечить доступ к электронной почте и к сетевым ресурсам с помощью единой учетной записи;
* обеспечить изменение пароля для доступа к сетевым ресурсам и электронной почте раз в три месяца;
* обеспечить единую адресную книгу адресов электронной почты (корпоративный справочник контактов) сотрудников Заказчика на всех объектах автоматизации, единая адресная книга должна содержать атрибуты:
  + ФИО;
  + E-mail;
  + Внутренний телефон;
  + Номер комнаты;
  + Возможность расширения списка атрибутов.
* обеспечить возможность использования электронной цифровой подписи для подписи и шифрования отправляемых сообщений;
* предоставить пользователям СПС возможность доступа к собственному электронному почтовому ящику из любой точки мира с компьютера, мобильного телефона или планшета;
* обеспечить отдельным пользователям СПС возможность работы с собственным электронным почтовым ящиком с помощью web-интерфейса;
* обеспечить доступ к СПС из сети Интернет только для отдельных учетных записей;
* поддерживать возможность взаимодействия с внешними системами по протоколу SMTP;
* обеспечить хранение всех почтовых ящиков пользователей на сервере;
* предоставлять возможность квотирования размера почтовых ящиков;
* предоставлять возможность квотирования размера входящих и исходящих электронных писем;
* реализовать несколько серверных политик для архивации сообщений на сервере;
* реализовать политики отправки сообщений с вложенными файлами между почтовыми ящиками из разных подсетей Заказчика;
* реализовать политики запрета отправки и получения внешних сообщений с вложениями для отдельных почтовых ящиков.
  + 1. Требования к подсистеме предварительной фильтрации

Подсистема предварительной фильтрации должна обеспечивать:

* использование инструментов для анализа и ограничения доставки почты на основе фильтрации подключений к почтовой системе и фильтрации почтовых сообщений по признакам:
* «запрещенные» и «разрешенные» списки отправителей (RBL), включая «запрещенные» и «разрешенные» имена почтовых доменов. ПС должна обеспечивать работу со списками, сформированными администраторами ПС, пользователями ПС, независимыми поставщиками RBL списков;
* наличие получателя в почтовой системе;
* фильтрация по SURBL;
* анализ формальных признаков письма;
* объема пересылаемых сообщений с учетом вложений;
* типа вложений (формат).
* возможность создания новых правил фильтрации;
* расширенную языковую поддержку, включая русский язык и языки азиатской группы;
* удаление (помещение в карантин) отфильтрованных сообщений.

Требования к функциональному комплексу защиты от вредоносного программного обеспечения

Функциональный комплекс защиты от вредоносного программного обеспечения (ФКЗВПО) должен обеспечивать:

* обнаружение компонентов вредоносного программного обеспечения (ВПО)
* регулярное обновление своей базы данных информацией для поиска любых (включая наиболее свежих) образцов ВПО;
  + 1. Требования к подсистеме обеспечения внешнего доступа

Подсистема обеспечения внешнего доступа (ПОВнеД) должна обеспечивать пользователям доступ к ПС через Интернет.

Должен поддерживаться доступ к ПС с совместимых мобильных устройств при помощи технологии Exchange ActiveSync.

Технические средства ПОВнеД должны состоять из серверов, работающих под управлением Операционной системы Windows Server 2012 R2/2016.

* 1. Требования к видам обеспечения
     1. Требования к лингвистическому обеспечению

Взаимодействие конечных пользователей с системой должно осуществляться на русском языке. Исключение могут составлять только системные сообщения, интерфейсы и команды администрирования СПС.

* + 1. Требования к программному обеспечению

Необходимое для создания СПС программное обеспечение должно быть приобретено и оформлено Заказчиком в соответствии с лицензионными соглашениями, предлагаемыми производителями ПО.

Программное обеспечение СПС должно быть достаточным для выполнения всех функций СПС, реализуемых с применением средств вычислительной техники, а также иметь средства организации всех требуемых процессов обработки данных, позволяющие своевременно выполнять все автоматизированные функции во всех регламентированных режимах функционирования СПС.

СПС должна включать следующие покупные программные средства:

* Microsoft Exchange Server 2016;
* Microsoft Windows Server 2012 R2/2016.
  + 1. Требования к техническому обеспечению

Технические средства, используемые в рамках СПС, должны соответствовать рекомендуемым требованиям производителя используемых программных и аппаратных средств.

Технические средства должны размещаться в выделенных серверных комнатах, обеспечивающих постоянное функционирование основных сервисов, оборудованных системой кондиционирования, пожаротушения и системой бесперебойного питания, и должны быть защищены от несанкционированного доступа.

В технических средствах серверов должны быть установлены резервные блоки питания для снижения вероятности отказа функционирования СПС при отказе основного блока питания.

В технических средствах серверов должны быть предусмотрены резервные сетевые порты для снижения вероятности отказа работы СПС при отказе одного сетевого порта. Требования к подключению сетевых портов серверов к различным отказоустойчивым элементам активного сетевого оборудования должны быть сформулированы на этапе проектирования.

Технические средства должны иметь возможность установки в стандартные стойки шириной 19 дюймов.

* + 1. Требования к организационному обеспечению

Для функционирования СПС должна быть создана организационная структура по обслуживанию СПС. Требования к численности, квалификации, функциональным обязанностям и режиму работы персонала должны быть разработаны на этапе проектирования.

Защита от ошибочных действий персонала СПС должна быть обеспечена за счет следующих мероприятий:

* четкое определение функциональных обязанностей и разграничение полномочий;
* подтверждение и документирование действий, выполнение которых может привести к трудно обратимым или необратимым изменениям в ресурсах самой СПС;
* восстановление информации в базах данных и программного обеспечения СПС в случае их разрушений;
* диагностирование ресурсов СПС;
* аттестация администраторов СПС на соответствие требуемому уровню квалификации;
* аттестация пользователей СПС на соответствие требуемому уровню квалификации.

1. Внедрение системы управления базами данных под управлением Microsoft SQL Server
   1. Назначение и цели внедрения системы
   2. Назначение системы

Проект по внедрению системы управления базами данных Microsoft SQL Server 2017 предназначен для автоматизации ряда задач по обработке и хранению информации в формате, совместимом с СУБД.

Объектами хранения будут выступать таблицы, файлы и прочая информация поддерживаемая СУБД.

* 1. Цели создания системы

Целями внедрения решения являются:

* надежное хранение информации в отказоустойчивой конфигурации СУБД;
* сокращение количества и времени простоя информационных систем для повышения непрерывности бизнеса;
* обеспечение максимальной работоспособности и производительности используемых в компании приложений, сервисов и операционных систем.
  1. Характеристика ИТ-инфраструктуры заказчика

Описание инфраструктуры осуществляется исполнителем на этапе предварительного обследования объекта автоматизации.

На текущий момент ИТ-инфраструктура, рассматриваемая в проекте, представлена рядом серверов, ПК и различных сервисов.

* 1. Требования к системе
  2. Общие требования к системе
     1. Требования к структуре системы

Структура системы должна разрабатываться исходя из следующих положений:

* Внедряемая система должна быть настроена согласно базовой конфигурации продукта MSSQL;
* система должна быть масштабируемой;

Система управления базами данных должна:

* иметь интерфейс создания новых и управления имеющимися базами данных;
* поддерживать размещение баз данных для различных ИТ-систем;
* иметь интерфейс для исполнения TSQL запросов;
* поддерживать размещения в кластерной конфигурации Windows Server Failover Cluster;
* поддерживать размещение групп доступности AlwaysOn;



Интерфейс создания и управления БД

В СУБД должен быть предусмотрен механизм создания баз данных. Интерфейс должен быть как графическим, так и управляемым через командную строку или PowerShell.

Интерфейс должен разграничивать права доступа к СУБД.

Интерфейс должен по требованию предоставлять пользователю, прошедшему аутентификацию информацию о базах данных.

Интерфейс должен по требованию предоставлять пользователю, прошедшему аутентификацию информацию о конфигурации сервера баз данных.

Поддержка размещения баз данных для различных ИТ систем

Microsoft SQL Server 2017 должен поддерживать создание и размещение на нем баз данных для различных ИТ систем в инфраструктуре Заказчика.

Интерфейс исполнения TSQL запросов

В системе должен быть предусмотрены различные интерфейсы для выполнения запросов на языке TSQL. Необходимо, чтобы была возможность взаимодействовать с запросами, как из графического интерфейса, так и из программируемого или интерфейса командной строки.

Поддержка размещения в кластерной конфигурации Microsoft Windows Server 2016

СУБД должна иметь механизмы по установке и интеграции с кластерной конфигурацией ОС Windows Server 2016.

Поддержка групп доступности AlwaysOn

СУБД должна иметь функцию размещения новых или имеющихся баз данных в группы доступности AlwaysOn. Группы доступности должны сдержать минимум 1 первичную реплику базы данных и до 4х вторичных реплик. Реплики должны иметь механизмы ограничения доступа как в режиме «Только чтение» так и в режиме записи.

* + 1. Требования к надежности

Сохранность информации при аварийных ситуациях должна обеспечиваться сторонней системой резервного копирования. Встроенные механизмы кластеризации WSFC и группы доступности должны повышать надежность хранения информации и исключать возможность единственной точки отказа.

* + 1. Требования к защите информации от несанкционированного доступа

Система должна поддерживать разграничение прав доступа к компонентам системы на основе ролей. Доступ к системе разграничивается по принципу предоставления минимальных полномочий для выполнения должностных обязанностей персонала. Сеансы подключения к консоли должны отражаться в журналах работы клиента. Правила создания ролей и порядок предоставления полномочий доступа к системе определяет заказчик созданием соответствующего регламента на этапе опытной эксплуатации.

* 1. Требования к видам обеспечения
     1. Требования к программному обеспечению

Требования к СУБД Microsoft SQL Server 2017:

* ОС Microsoft Windows Server 2012 R2 или 2016 в конфигурации WSFC;
* Microsoft SQL Server 2017 Standard/Datacenter;

В рамках проекта предполагается установка и базовая настройка 3х кластеров WSFC, каждый из 2 серверов. Каждый их кластеров, должен, в свою очередь, размещать необходимое количество групп доступности AlwaysOn

* + 1. Требования к аппаратному обеспечению

В проекте будет задействовано 6 физических серверов. Они объединены в 3 независимых кластера WSFC по 2 узла в каждом.

Физические серверы должны удовлетворять следующим требованиям:

* 64-битный процессор с тактовой частотой не менее 1,4 ГГц;
* ОЗУ: не менее 512 Мб;
* не менее 6Гб свободного места;
  + 1. Требования к сетевым протоколам

Подробные требования к сетевым протоколам содержаться в онлайн документации Microsoft по ссылкам:

* [Windows Server Failover Cluster](https://docs.microsoft.com/en-us/windows-server/failover-clustering/clustering-requirements);
* [Microsoft SQL Server](https://docs.microsoft.com/ru-ru/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-2017)
  + 1. Требования к учетным записям

Для установки и конфигурация кластеров WSFC и серверов MSSQL понадобятся следующие учетные записи:

* локальный администратор Windows Server;
* учетная запись с правами sa для конфигурации СУБД.
  + 1. Требования к техническому обеспечению

Серверное ПО установить на существующей физической платформе.

Конкретная конфигурация технических средств должна быть определена на этапе реализации проекта.

Технические средства, применяемые для организации системы, должны иметь соответствующие сертификаты и лицензии.

1. Система резервного копирования под управлением Microsoft System Center Data Protection Manager
   1. Структура и описание решения
   2. Назначение системы

Проектируемая система предназначена для автоматизации резервного копирования и восстановления серверной инфраструктуры Заказчика.

* 1. Описание объекта автоматизации

Объектом автоматизации является инфраструктура Заказчика в части следующих информационных систем:

* Контроллеры доменов, расположенные в Центральном офисе и филиалах;
* Сетевые хранилища и локальные диски серверов по управлением семейства ОС Windows Server;
* Кластеры служб Hyper-V, расположенные в Центральном офисе Заказчика;
* Кластеризованные и изолированные СУБД MS SQL, расположенные в Центральном офисе Заказчика;
* Сервера и кластера серверов под управлением ОС Windows Server.
  1. Цели внедрения решения

Внедрение продукта DPM позволит реализовать следующее:

* Возможность резервного копирования в облачные хранилища Azure;
* Поддержку резервного копирования кластеризованых СУБД MS SQL;
* Возможность использования виртуальных томов .vhd как хранилищ резервных копий;
* Возможность установки компонентов DPM в виртуальную среду;
* Уменьшение объема дискового пространства, за счет улучшенных механизмов дедупликации.
  1. Ожидаемые результаты внедрения

В ходе проекта должны быть достигнуты следующие результаты:

* Собраны и проанализированы требования заказчика к системе резервного копирования серверной инфраструктуры;
* Установлено серверное ядро системы;
* Произведена установка агентов резервного копирования до актуальной версии;
* Произведена настройка заданий резервного копирования;
* Установлена и настроена подсистема генерации отчетов;
* Проектные решения и настройки задокументированы в Пояснительной записке.
  1. Задачи проекта

Проектируемая система разворачивается в инфраструктуре корпоративной сети Заказчика и предназначена для решения следующих задач:

* Резервное копирование компонентов служб каталога Active Directory;
* Резервное копирование компонентов почтовой системы на базе Microsoft Exchange;
* Резервное копирование компонентов систем управления базами данных MS SQL;
* Резервное копирование компонентов систем виртуализации на базе продукта Microsoft Hyper-V;
* Резервное копирование компонентов и состояния ОС Windows Server и отдельных файлов;
* Резервное копирование компонентов файловых хранилищ Windows Server DFS;
* Сбор статистики по ключевым параметрам для указанных выше систем.
  1. Требования к проектируемой системе
     1. Состав системы
     2. Компоненты системы

Система резервного копирования на базе продукта System Center Data Protection Manager состоит из следующих компонентов:

* Операционной базы данных;
* Сервер управления;
* Хранилище резервных копий;
* Агентов, устанавливаемых на серверах и рабочих станциях.

Операционная база данных

Операционная база данных представляет собой БД под управлением СУБД Microsoft SQL Server и предназначена для хранения всей конфигурационной информации (настройки агентов, правила и расписания задач копирования, настройки безопасности и т.д.). Операционная БД не требует установки на сервер СУБД дополнительных компонентов.

Сервер управления

Сервер управления является точкой взаимодействия агентов с группой управления. Сервера управления осуществляют централизованное управления задачами восстановления и резервного копирования. Вся информация о настройках системы и задачи резервного копирования хранятся в операционной БД.

Хранилище резервных копий

В качестве хранилища резервных копий DPM может использовать следующие типы носителей:

* Диск VHD;
* Транзитный диск с непосредственно подключенным к узлу хранилищем (DAS);
* Транзитный iSCSI LUN, подключенный к узлу;
* Транзитный Fibre Channel LUN, подключенный к узлу;
* Целевой LUN, подключенный непосредственно к виртуальной машине DPM по интерфейсу iSCSI;
* Fibre Channel LUN, подключенный к виртуальной машине DPM с помощью виртуального контроллера Fibre Channel (VFC) Windows Server.
* Максимально поддерживаемый размер хранилища составляет 17 Тб при использований GPT дисков.

Агент DPM

Агент защиты DPM (DPM protection agent) — приложение, устанавливаемое на каждый компьютер, защищаемый с помощьюDPM*.* Выполняет следующие функции:

* При защите файловых ресурсов: Записывает изменения защищенных данных в журнал изменений. Создает отдельный журнал для каждого защищенного тома. Журналы хранит в скрытых разреженных файлах на тех же защищенных томах. Передает журнал изменений с защищенного компьютера на сервер DPM, что позволяет DPM синхронизировать реплику (принимает журнал и синхронизирует данные другой агент на стороне сервера DPM).
* При защите различных приложений и баз данных: Передает журналы транзакций соответствующих приложений с защищенного компьютера на сервер DPM. При выполнении быстрой полной архивации действует аналогично защите файловых ресурсов через журнал изменений.
* Позволяет серверу DPM просматривать общие папки, тома и папки на защищенном компьютере.
* Формирует список ресурсов, которые возможно включить в группу защиты, на защищаемом компьютере.
* Участвует в процессе восстановления данных.

Агент защиты контролируется сервером DPM, с которого был установлен, либо на который был настроен выполнением команды SetDpmServer. Приложение Агент защиты состоит из самого агента и Координатора агента. Координатор агента — программа, временно устанавливаемая на защищаемый компьютер в процессе установки, обновления или удаления Агента защиты. Как явно следует из определения, Координатор агента выполняет функции управления процессом установки, обновления и удаления агента.

Помимо этих понятий, при работе с DPM, отдельно необходимо выделить службу Агент защиты (он же DPM Replication agent, DPMRA, DPM Protection agent service) и службу Координатор агента.

* + 1. Безопасность
    2. Взаимодействие агентов с серверами управления

Как описывалось выше, при подключении к серверу управления агент должен пройти аутентификацию с использованием либо протокола Kerberos. Передаваемые между агентом и сервером управления данные шифруются, при этом используется тот же механизм, что и при аутентификации.

* 1. Требования к функционированию системы
     1. Требования к функциональным возможностям системы
     2. Требования к системе резервного копирования

Система должна обеспечивать:

Возможность создания полных, инкрементальных и дифференциальных резервных копий следующих сервисов:

* + Компонентов служб каталога Active Directory;
  + Компонентов почтовой системы на базе Microsoft Exchange;
  + Компонентов систем управления базами данных MS SQL (в том числе кластеризованых);
  + Компонентов систем виртуализации на базе продукта Microsoft Hyper-V и виртуальных машин;
  + Компонентов и снимков состояния ОС Windows Server и отдельных файлов;
  + Компонентов файловых хранилищ Windows Server DFS;

Автоматическое и автоматизированное выполнение задач резервного копирования согласно настроенным задачам;

Сбор и отображение консолидированных отчетов по выполняемым процессам резервного копирования;

Возможность выполнения оператором управляющих воздействий на объекты управления.

* + 1. Требования к хранению данных

Вся собираемая системой информация должна храниться в базах данных под управлением СУБД Microsoft SQL Server.

Система резервного копирования должна обеспечивать возможность переноса используемых баз данных с одного сервера СУБД на другой без потери собранной информации (допускается остановка системы на время переноса БД).

* + 1. Требования к клиентам системы

Система должна обеспечивать функционирование клиентских компонентов (агентов системы) на серверах под управлением следующих операционных систем:

* Windows Server 2016
* Windows Server 2012 Service Pack 1 и выше;
* Windows Server 2012 R2;
* Windows Server 2008 и выше;
* Windows Server 2008 R2.

Заказчик обеспечивает настройку установленного на серверах системного программного обеспечения (антивирус, сетевые экраны и т.п.) таким образом, чтобы оно не препятствовало распространению и функционированию агентов системы.

* + 1. Требования к взаимодействию с внешними системами

Система должна использовать единую службу каталога на базе Microsoft Active Directory Заказчика для следующих целей:

* Аутентификация при взаимодействии между компонентами системы, входящими в доменный лес;
* Разделение доступа к функциям и объектам системы.
  + 1. Требования к надежности

Отказоустойчивость системы должна обеспечиваться регулярным резервным копированием, выполняемым в нерабочее время. Процедура резервного копирования не должна влечь за собой остановку системы.

Восстановление из резервных копий должно выполняться на остановленной системе. Процедура восстановления не должна занимать более 4 часов.

Система должна обеспечивать возможность безостановочной работы. Кратковременные остановки работы системы допускаются только для проведения регламентных работ, таких как обновление ПО, обслуживание аппаратной части системы и т.п. Такие перерывы не должны превышать 8 часов и по возможности должны проводиться в ночные смены или выходные дни.

* 1. Требования к информационной безопасности
     1. Требования к взаимодействию между компонентами системы

Взаимодействие между компонентами системы должно удовлетворять следующим условиям:

* Любое взаимодействие между серверами управления и агентами системы должно происходить только после взаимной аутентификации;
* Вся передаваемая между серверами и агентами информация должна шифроваться;
* Передача любой учетной информации (имена пользователей и пароли) должна осуществляться только с использование защищенных (использующих шифрование) протоколов;
* Взаимодействие между компонентами системы должно происходить по фиксированным (не динамическим) портам протокола TCP/IP.
  + 1. Требования к разделению доступа к системе

Система резервного копирования должна обеспечивать:

* Разграничение доступа на основе ролевой модели;
* Ограничение области видимости данных резервного копирования на основе ролевой модели;
* Ограничение доступа к выполнению заданий (runtime tasks) на основе ролевой модели;
* Назначение сотрудниками ролей на основе их учетных записей и членства в группах в Active Directory.

Для разграничения доступа к системе резервного копирования должны быть созданы следующие роли:

|  |  |
| --- | --- |
| Роль | Назначение |
| Администраторы | Полные права на просмотр и изменение конфигурации системы. |
| Оператор смены | Включает набор полномочий, необходимых для операторов системы, работающих со всей информацией, но без возможности изменения конфигурации. |

* + 1. Требования к использованию служебных учетных записей

В качестве служебных учетных записей система должна использовать либо локальные системные учетные записи (Local System, Local Service, Network Service), либо непривилегированные доменные учетные записи (не обладающие административными полномочиями в доменах Active Directory или организации Microsoft Exchange).

Допускается использование привилегированных учетных записей (при необходимости с привлечением специалистов Заказчика) в ходе установки компонентов системы и настройки расписания резервного копирования.

* 1. Требования к масштабированию

Внедряемая система должна удовлетворять следующим требованиям к масштабированию:

* Производительность системы не должна ухудшаться при известном на этапе проектирования росте количества подключаемых приложений и сервисов, входящих в рамки проекта;
* При необходимости увеличения количества подключаемых приложений и сервисов система должна позволять наращивание мощности силами Заказчика.
  1. Требования к программному обеспечению

Серверная часть системы резервного копирования должна строиться на основе следующих программных продуктов компании Microsoft:

* Microsoft Windows Server;
* Microsoft SQL Server;
* Microsoft System Center Data Protection Manager.

На все программные продукты должны быть установлены текущие версии пакетов обновления ПО (Service Packs) и все необходимые обновления безопасности, в соответствии с рекомендациями компании-производителя ПО и политиками безопасности Заказчика.

Все программные средства, необходимые для создания системы, а также лицензии на их использование должны быть приобретены и оформлены в соответствии с лицензионными соглашениями, предлагаемыми производителями соответствующего ПО.

* 1. Требования к аппаратному обеспечению.

Для серверных компонентов системы резервного копирования должно быть выделено оборудование в составе двух серверов, соответствующих следующим минимальным требованиям:

* 2 CPU (по 4 ядра или более);
* 8G RAM;
* Дисковая подсистема:
  + Системный раздел: 80Gb;

Оборудование должно быть смонтировано в стойках в серверных помещениях, подключено к электрической и информационной сети.

* 1. Требования к сетевой инфраструктуре

Для обеспечения взаимодействия между компонентами системы должны быть открыты следующие порты:

|  |  |  |
| --- | --- | --- |
| **Протокол** | **Порт** | **Описание взаимодействия** |
| DCOM | 135/Динамические порты RPC | Протокол управления DPM использует DCOM.  DPM выдает команды агенту защиты путем создания вызовов DCOM.  Агент защиты отвечает создавая вызовы на стороне DPM сервера. TCP порт 135 используется для конечных точек распределенной вычислительной среды DCOM. По умолчанию, DCOM динамически назначает порты из диапазона TCP 1024-65535. |
| TCP | 5718/TCP 5719/TCP | Канал передачи данных DPM. Сервер и агент DPM инициируют соединения для выполнения операций DPM, таких как синхронизация и восстановление. DPM связывается с координатором агента используя порт 5718 и с агентом защиты — порт 5719. |
| DNS | 53/UDP | Используется между DPM и контроллером домена, между защищенным компьютером и контроллером домена для разрешения имен хостов. |
| Kerberos | 88/UDP 88/TCP | Используется между DPM и контроллером домена, между защищенным компьютером и контроллером домена для аутентификации конечной точки. |
| LDAP | 389/TCP 389/UDP | Используется для запросов между DPM и контроллером домена. |
| NetBIOS | 137/UDP 138/UDP 139/TCP 445/TCP | Используется между DPM и защищенным компьютером, между DPM и контроллером домена, между защищенным компьютером и контроллером домена для различных операций. Используется для SMB непосредственно размещенного на TCP/IP для функций DPM. |

* 1. Состав и требования к проектной документации

Все документы передаются Заказчику на согласование и утверждение в электронном виде, в формате Microsoft Word.

Планируемый срок согласования документов – одна неделя, увеличение длительности согласования не входит в общие сроки проекта.

В рамках построения системы должен быть разработан следующий набор документов:

* «Техническое задание» (данный документ);
* «Пояснительная записка»;
* «Инструкция администратора».
  + 1. Требования к документу «Пояснительная записка»

Документ должен содержать подробное описание проектных решений и состоять из следующих разделов:

* Общие положения;
* Основные технические решения:
  + Архитектура системы;
  + Настройки системы;
  + Безопасность системы;
  + Установка агентов системы;
  + Совместимость со смежными системами;
  + Пользователи системы;
  + Техническое обеспечение;
  + Программное обеспечение.
  1. Требования к численности и квалификации персонала

Для эксплуатации системы требуется 1 человек на роль администратора системы, требуемая загрузка – в среднем 25%.

Рекомендуемый уровень квалификации:

Сертификация MCSA или MSITP либо соответствующий уровень квалификации;

* 1. Условия и режим эксплуатации

Проектируемая система должна обеспечивать выполнение возлагаемых на нее задач в режиме круглосуточного функционирования.

Система должна обеспечивать функционирование в следующих режимах:

Штатный режим. Режим функционирования системы, при котором обеспечивается выполнение функциональных возможностей системы в объеме функций, соответствующем текущему этапу реализации;

Автономный режим. Характеризуется ограничением возможностей системы, связанного с нарушением информационного взаимодействия между компонентами системы, которые могут быть обусловлены как отсутствием сетевого соединения между компонентами системы, так и сбоями в функционировании службы каталога Active Directory. В этом режиме информация от агентов системы сохраняется в локальном кэше агента и передается на сервер управления при восстановлении режима функционирования. При длительном отсутствии связи часть данных может быть потеряна.

В качестве аппаратной платформы системы должны использоваться средства с повышенной надежностью.

Оборудование системы должно размещаться в серверных помещениях, имеющих выделенную розеточную электросеть 220В ±10%, 50 Гц с защитным заземлением и обеспечивающих следующие климатические условия:

Температура окружающей среды – от 15 до 30 градусов С;

Относительная влажность воздуха - от 30% до 80% (без конденсата);

Атмосферное давление - от 630 мм. р.с. до 800 мм. р.с;

Отсутствие пыли и агрессивных по отношению к оборудованию веществ.