1. Постановка задачи

Общие сведения

Для повышения производительности труда и обеспечения возможности более эффективного управления деятельностью необходимо в здании построить структурированную кабельную сеть (далее – СКС) и создать системы информационно-коммуникационной инфраструктуры (далее – ИКИ) на 150 рабочих мест с возможностью будущего масштабирования до 200 рабочих мест. При проектировании использовать самые современные решения.

При проектировании исходить из необходимости создания типовой инфраструктуры для типовой организации. В составе ИКИ предусмотреть следующие подсистемы:

- локальная вычислительная сеть (ЛВС), включая беспроводную ЛВС;
- система унифицированных коммуникаций:
  1) подсистема телефонной связи;
  2) подсистема отображения состояния присутствия;
  3) подсистема беспроводной связи;
  4) факс-серврер.
- выделенная подсистема командно-диспетчерской связи и селекторных совещаний;
- система видео-конференц-связи (ВКС);
- оборудование конференцкомнат:
  1) подсистема отображения видеоинформации;
  2) подсистема звукоусиления и акустики;
  3) подсистема видеоконференции;
  4) подсистема аудио- и видео коммутации;
  5) подсистема управления элементами подсистем.
- оборудование конференцзала:
  1) подсистема видео-конференц-связи конференцзала;
  2) подсистема звукоусиления и акустики;
  3) подсистема аудиокоммутации;
  4) подсистема видеокоммутации;
  5) подсистема электронного голосования;
  6) подсистема синхронного перевода;
  7) подсистема управления;
- система обеспечения информационной безопасности:
  1) подсистема защиты взаимодействия с сетью Интернет;
  2) подсистема защиты ЛВС;
  3) подсистема управления и мониторинга.
- активное оборудование центров обработки данных:
  1) серверы и системы хранения, консоли управления,
  2) система/сеть хранения данных,
  3) система резервного копирования.
- программная инфраструктура информационной системы:
  1) подсистему виртуализации аппаратных ресурсов серверов;
  2) подсистему виртуализации аппаратных ресурсов рабочих станций;
  3) служба единого каталога;
  4) служба поддержки сетевых сервисов;
  5) служба обмена электронными почтовыми сообщениями;
  6) службы общих и персональных файловых ресурсов;
  7) система резервного копирования и восстановления данных;
- система документооборота.

1.1. ЛВС

Локальная Вычислительная Сеть (ЛВС) предназначена для обеспечения информационного взаимодействия пользователей и информационных систем. ЛВС аппарата должна обеспечивать передачу различных типов трафика, таких как данные, аудио и видео с надлежащим качеством обслуживания. Кроме того, ЛВС должна обладать высокой степенью надежности, производительностью и масштабируемостью. ЛВС должна сохранять свою полную работоспособность при единичных отказах, а время простоя при возникновении аварии должно быть минимальным.

ЛВС аппарата должна была построена по иерархическому принципу и должна включать явно выраженные уровни ядра и доступа. Уровень распределения может быть совмещен с уровнем ядра.

- Уровень ядра предназначен обеспечения неблокируемой коммутации IP пакетов на третьем уровне OSI между всеми устройствами в сети.
- Уровень доступа предназначен для подключения всех пользователей, IP-телефонов, точек беспроводного доступа БЛВС, сетевых принтеров и других сетевых периферийных устройств к ЛВС.

1.1.1. БЛВС

На начальном этапе Беспроводная локальная вычислительная сеть (далее БЛВС) должна быть развернута в публичных зонах и в переговорных комнатах для доступа к сети Интернет.

БЛВС должна поддерживать стандарты IEEE 802.11a/b/g/n и охватывать следующие помещения:

- Этаж 1:
  1) Атриум;
  2) Фойе гардероба;
  3) Зона ожидания;
- Этаж 2
  1) Буфет;
  2) Обеденный зал;
- Этаж 3
  1) Конференц-зал;
  2) Зал рабочих совещаний;
  3) Зона руководства;
- Этаж 4
  1) Зал совещаний управления;
- Этаж 5
  1) Зал совещаний управления;
- Этаж 6
  1) Начальник аналитического управления;
  2) Начальник управления – Главный бухгалтер;
- Этаж 7
  1) Зал совещаний и переговоров.

1.2. Система унифицированных коммуникаций

Для обеспечения телефонной связью и другими дополнительными видами обслуживания подразделений в многофункциональном здании и организации связи с городской телефонной сетью (ТфОП) предложить систему унифицированных коммуникаций на основе оборудования компании Avaya на 150 рабочих мест с возможностью будущего расширенияния до 200 рабочих мест.

Система унифицированных коммуникаций должна включать в себя следующие подсистемы:

– систему телефонной связи (СТС);
– подсистему отображения состояния присутствия и обмена мгновенными сообщениями;
– подсистему беспроводной связи;
– факс-сервер;
– подсистему селекторной связи.

СТС должна обеспечивать следующие виды обслуживания:
– установление телефонных соединений между сотрудниками;
– установление телефонных соединений по нажатию клавиши прямого набора между руководителем и его заместителями;
– установление телефонных соединений между сотрудниками и абонентами ТфОП;
– предоставлять другие дополнительные виды обслуживания, такие как перевод текущего вызова, музыка на удержании вызова, неуправляемая телефонная конференция и т.п.

Предусмотреть организацию взаимодействия системы телефонной связи с ТфОП. Требования к организации взаимодействия с ТфОП уточнить на этапе предпроектных изысканий. Способ организации взаимодействия с ТфОП необходимо определить на этапе проектирования с учётом с ТУ на подключение к ТфОП.

Система унифицированных коммуникаций должна содержать подсистему отображения состояния присутствия и обмена мгновенными сообщениями, предоставляющая возможность сотрудникам использовать перечисленные ниже сервисы:
– Presence (отображение присутствия пользователей в сети);
– IM (обмен короткими сообщениями);
– Click-to-Call (инициирование телефонного вызова нажатием на пиктограмму в приложениях Microsoft Office и других приложениях).

В системе унифицированных коммуникаций должна быть предусмотрена подсистема беспроводной связи стандарта DECT. Требования к зоне радио покрытия, к максимальному количеству одновременно поддерживаемых в различных точках здания телефонных соединений, а также к количеству терминалов подсистемы беспроводной связи необходимо определить на этапе пред проектных изысканий.

В систему унифицированных коммуникаций должна быть включена служба факс-сервер, обеспечивающая возможность получения факсимильных сообщений в электронном виде.

1.3. Выделенная подсистема командно-диспетчерской связи и селекторных совещаний

Необходимо предусмотреть организацию выделенной командно-диспетчерской связи и селекторных совещаний, которая будет обеспечивать:

– возможность установления видеотелефонных соединений Руководителя с руководителями подразделений;

– возможность организации аудио- и видео-конференций в режиме селекторных совещаний.

Подсистема должна обеспечивать возможность установления видеотелефонных соединений между следующими абонентами:

1. Руководитель
2. Управляющий делами
3. Руководитель секретариата
4. Заместитель Управляющего делами
5. Заместитель Управляющего делами
6. Заместитель руководителя секретариата
7. Начальник управления
8. Начальник управления
9. Начальник Аналитического управления
10. Начальник Организационного управления
11. Начальник Управления финансирования и обеспечения деятельности – Главный бухгалтер

Подсистема должна обеспечивать возможность проведения селекторных совещаний в режиме видеоконференций с участием перечисленных выше сотрудников, а также обеспечивать возможность подключения к селектору в телефонном режиме до 39 абонентов системы унифицированных коммуникаций организации и/или ТфОП.

Выделенная подсистема должна иметь точки сопряжения с системой унифицированных коммуникаций для организации аудио-вызовов сотрудникам организации и вызова абонентов ТфОП в ходе проведения селекторных совещания.

Для обеспечения возможности установления видеовызовов с абонентами, находящимися за периметром сети организации, или подключения этих абонентов в управляемый видео-селектор (видео-конференц-связь) необходимо предусмотреть соответствующий модуль сопряжения в составе подсистемы ВКС.

1.4. Система видео-конференц-связи

Система видеоконференцсвязи должна обеспечивать:

- поддержку аудио и видео вызовов «точка-точка»;
- организацию «многоточечных» аудио и видео конференций;
- протоколирование(запись) сеансов ВКС как в режиме «точка-точка» так и «многоточечном» режиме;
- трансляцию сеансов ВКС для коллег, не имеющих видео оборудования;
- возможность получения и восприятия дополнительной визуальной информации (документальная камера, презентация с PC);
- одновременную демонстрацию выступающего и его презентации;
- регистрацию и логическую адресацию терминального и серверного оборудования ВКС;
- централизованное управление видеосерверным оборудованием и всеми абонентскими комплектами ВКС из одной точки;

– обеспечение поддержки корпоративной адресной книги абонентов видеоконференцсвязи.

1.4.1. Оборудование рабочих кабинетов

Для участия в сеансах видеоконференцсвязи следующих рабочих кабинетов:
– Руководитель
– Управляющий
– Заместителя Управляющего делами

Необходимо установить персональные терминалы ВКС которые обеспечат следующие сервисы:
– создание видеоконференции типа «точка-точка»;
– участия в многоточечных сеансах видеоконференцсвязи;
– трансляцию в сеанс видеоконференцсвязи документов и презентации при помощи встроенной документ камеры или подключенного ПК;
– использование экрана персонального терминала ВКС в качестве HI-END монитор для своего ПК;

1.4.2. Оборудование кабинета VIP переговоров

Создаваемая Система должна обеспечивать следующие виды сервиса:
– видеоконференцсвязь;
– аудиоконференцсвязь;
– локальная демонстрация презентаций;
– дистанционная демонстрация презентаций
– дистанционная трансляция мультимедийного контента;
– локальное и фоновое озвучивание;
– управление оборудованием;

В переговорной необходимо установить систему отображения состоящую из широкоформатного экрана с проектором, а также дублирующих панелей.

Для всех участников переговорной установить микрофонную систему состоящую из 13 пультов делегатов и 1 пульта председателя.

Для охвата всех участников переговорной в сеанс ВКС предусмотреть установку нескольких камер.

Столы участников необходимо оборудовать необходимыми интерфейсами для возможности подключения ПК.

Системы отображения должны быть предназначены для отображения локальных презентаций, в режиме сеанса ВКС удаленных участников и удаленных презентаций.

Для звукового сопровождения видеоинформации, для озвучивания выступлений, ведения дискуссий и обсуждений в переговорной необходимо установить аудиооборудование.

Звук от микрофонных систем в режиме локальной презентации должен поступать в акустику переговорной, в режиме сеанса ВКС также в акустику переговорной и удаленным абонентам.

Для управления микрофонной системой, вызовов удаленных абонентов ВКС и тд, необходимо предусмотреть систему управления с сенсорным экраном, которая будет установлена на столе Руководителя.

1.4.3. Оборудование зала рабочих совещаний на 100 мест

Создаваемая Система должна обеспечивать следующие виды сервиса:

– видеоконференцсвязь;
– аудиоконференцсвязь;
– локальная демонстрация презентаций;
– дистанционная демонстрация презентаций
– дистанционная трансляция мультимедийного контента;
– локальное и фоновое озвучивание;
– управление оборудованием;

В центре переговорной необходимо установить систему отображения, состоящую из 8 или более широкоформатных панелей. Панели необходимо и расположить так, чтобы отображаемую на них информацию могли видеть все участники совещания (предположительно правильным многоугольником под потолком).

Для всех участников переговорной установить микрофонную систему, состоящую из 102 пультов делегатов и 1 пульта председателя.

Для охвата всех участников переговорной в сеанс ВКС предусмотреть установку нескольких камер.

Столы участников необходимо оборудовать интерфейсами для возможности подключения ПК.

Система отображения должна быть предназначена для отображения локальных презентаций, в режиме сеанса ВКС удаленных участников и удаленных презентаций.

Для звукового сопровождения видеоинформации, для озвучивания выступлений, ведения дискуссий и обсуждений в переговорной необходимо установить аудиооборудование.

Звук от микрофонных систем в режиме локальной презентации должен поступать в акустику переговорной, в режиме сеанса ВКС также в акустику переговорной и удаленным абонентам.

Для управления микрофонной системой, вызовов удаленных абонентов ВКС и тд, необходимо предусмотреть систему управления с сенсорным экраном, которая будет установлена на столе председателя.

1.4.4. Оборудование конференц-зала на 100 мест

Создаваемая Система должна обеспечивать следующие виды сервиса:
– видеоконференцсвязь;
– аудиоконференцсвязь;
– локальная демонстрация презентаций;
– дистанционная демонстрация презентаций
– дистанционная трансляция мультимедийного контента;
– локальное и фоновое озвучивание;
– синхронный перевод на два языка;
– проведение электронных голосований и опросов;
– управление оборудованием;

На сцене конференц-зала устанавливается стол президиума на 10 человек и трибуна докладчика.

Места участников президиума необходимо оборудовать дискуссионными пультами с возможностью электронного голосования, а также необходимыми интерфейсами для возможности подключения ПК. Также для сидящих в президиуме необходимо предусмотреть системы отображения видеоинформации которые будут дублировать основную систему отображения. Предусмотреть камеры которые обеспечат захват в сеанс видеоконференцсвязи только участников президиума и докладчика.

Трибуна докладчика должна состоять из интерактивного планшета и дискуссионного пульта с возможностью электронного голосования.

Места слушателей в количестве 100 человек должны быть оборудованы системой электронного голосования. Основная система отображения для слушателей должна состоять из широкоформатного экрана и проектора с высоким световым потоком. Также для слушателей необходимо предусмотреть несколько радио микрофонов.

Системы отображения(основная и дублирующая) должны быть предназначены для отображения локальных презентаций, в режиме сеанса ВКС удаленных участников и удаленных презентаций.

Для звукового сопровождения видеоинформации, для озвучивания выступлений, ведения дискуссий и обсуждений в конференц-зале необходимо установить аудиооборудование.

Звук от микрофонных систем в режиме локальной презентации должен поступать в акустику зала, в режиме сеанса ВКС также в акустику зала и удаленным абонентам.

Необходимо предусмотреть систему синхронного перевода на два языка для всех участников конференц-зала.

Для управления всем оборудованием конференц-зала необходимо предусмотреть место оператора.

1.5. Система обеспечения информационной безопасности

Подсистема защиты подключения к сети Интернет должна обеспечивать

- фильтрацию пакетов на сетевом и транспортном уровнях стека протоколов TCP/IP с использованием списков доступа (ACL);
- статическую и динамическую трансляцию IP-адресов (NAT, Dynamic NAT, PAT);
- возможность организации ДМЗ для размещения информационных ресурсов, общедоступных из сети Интернет;
- работу в режиме кластера с балансировкой нагрузки (режим Active/Active);
- обнаружение и возможность предотвращения сетевых атак с использованием сигнатурного анализа (IPS);
- потоковую антивирусную защиту для протоколов HTTP, FTP, SMTP;
- защиту от нежелательной электронной почты («спам»);
- контентную web-фильтрацию доступа пользователей в сеть Интернет.

Подсистема антивирусной защиты должна обеспечивать:

- антивирусную защиту АРМ и файловых и почтовых серверов;
- централизованное управление настройками параметров антивирусных приложений, проведение автоматического обновления антивирусных баз на всех защищаемых АРМ и серверах;
- функции удаленной централизованной установки антивирусных приложений;
- централизованный сбор статистики о работе антивирусных приложений;
- возможность формирования отчетов.

Подсистема анализа защищенности должна обеспечивать:

- поиск уязвимостей в операционных системах, прикладных сервисах, межсетевых экранах, сетевом оборудовании путем сетевого сканирования;

- функции определения типов и имен сетевых сервисов (HTTP, FTP, SMTP, POP3, DNS и пр.);
- функции определения и поиска уязвимостей в RPC-сервисах;
- функции проверки парольной защиты на сетевых сервисах, требующих аутентификации;
- функции анализа структуры и содержимого веб-сервисов для поиска уязвимостей;
- функции идентификации сетевых сервисов на случайных портах;
- функции запуска сканирования по расписанию, заданному администратором;
- генерацию отчетов об обнаруженных уязвимостях с рекомендациями по их устранению;
- контроль защищенности не менее ста сетевых устройств, работающих по протоколу IP за один цикл проверки;
- анализ стойкости паролей в режиме Audit, включая сетевое оборудование, ОС, СУБД и прикладные системы;
- возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему в соответствии с требованиями «Положения о методах и способах защиты информации в информационных системах персональных данных» (Приказ ФСТЭК №58).

Подсистема межсетевого экранирования сегмента обработки ПДн должна обеспечивать:

- выделение средствами межсетевого экранирования в отдельный сетевой сегмент серверов и АРМ задействованных в обработке персональных данных;
- выделение средствами межсетевого экранирования в отдельный сетевой сегмент серверов и АРМ управления ИБ;
- разграничение доступа и защиту от несанкционированного доступа на сетевом и транспортном уровнях стека протоколов TCP/IP;
- функционирование в режиме кластера с балансировкой нагрузки.

Подсистема разграничения доступа должна обеспечивать:

- защиту серверов и АРМ в сегменте обработки ПД от НСД;
- контроль входа пользователей в систему на АРМ с использованием программно-аппаратных средств защиты;
- разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации;
- разграничение доступа пользователей к защищаемой информации;
- регистрацию событий безопасности и аудит;
- защиту АРМ от загрузки с внешних носителей вредоносного кода и компьютерных вирусов;
- поддержку персональных идентификаторов (eToken);
- контроль вывода защищаемой информации на отчуждаемые носители;
- контроль целостности файлов, каталогов, элементов системного реестра;
- возможность контроля целостности до загрузки операционной системы;
- автоматическое затирание данных на диске при удалении файлов пользователем;
- регистрация событий безопасности в журнале;
- возможность автоматического оповещения по электронной почте о событиях несанкционированного доступа.

Для защиты сегмента обработки ПДн должно применяться программное обеспечение средств защиты информации, соответствующее 4 уровню контроля отсутствия недекларированных возможностей.

1.6. Активное оборудование центров обработки данных

Активное оборудование ЦОД содержит следующие компоненты:

- вычислительная система (серверы);
- общая система хранения данных(СХД);
- общая сеть хранения данных (SAN);
- ленточная библиотека для системы резервного копирования;
- устройства доступа пользователей (рабочие места).

Требования к вычислительной системе

Вычислительная система должна включать в себя серверное оборудование для реализации подсистемы виртуализации серверов, виртуализации рабочих станций, службы единого каталога, службы поддержки сетевых сервисов, службы обмена электронными почтовыми сообщениями, службы общих и персональных файловых ресурсов, системы резервного копирования и восстановления данных, системы документооборота, а также серверное оборудование для вспомогательных систем и бизнес-приложений, приведенных в данном документе;

Локальные диски серверов должны быть объединены в RAID 1 с помощью средств встроенного RAID-контроллера и использоваться только для системной информации.

Для доступа к ЛВС должно использоваться не менее двух каналов встроенного адаптера Ethernet с пропускной способностью 1 Gigabit каждый для отдельностоящих серверов или использование транковых каналов для блейд-корзины.

Для доступа к общей системе хранения данных должно использоваться не менее двух каналов адаптера FC HBA с пропускной способностью не менее 8 Gbps.

Управление серверами и доступ к консоли серверов должны осуществляться через встроенный управляющий модуль по протоколу TCP/IP.

Допускается использование серверов повышенной плотности монтажа (блейд-серверов, blade).

Требования к общей сети и системе хранения данных (СХД)

Емкость дискового пространства общей системы хранения данных должна обеспечивать хранение всех данных всех описываемых систем.

СХД должна обеспечивать доступ к дисковым ресурсам системы хранения в случае отказа одного из контроллеров системы хранения.

Данные, хранящиеся на общей СХД, должны быть защищены в одной дисковой группе от выхода из строя не менее одного диска.

СХД должна обеспечивать подключение серверов двумя независимыми путями.

Подключение серверов вычислительной системы к общей СХД должно осуществляться через коммутаторы Fiber Channel

Коммутаторы FC должны обеспечивать резервирование доступа серверов к СХД в случае отказа одного из них.

Для обеспечения безопасности передачи данных между серверами и СХД должно быть предусмотрено зонирование портов и подключаемого оборудования к коммутаторам FC.

СХД должна обеспечивать доступ к данным и поддерживать кластера операционных систем семейства Windows Server и гипервизора VMware ESXi.

Программное обеспечение для управления СХД должно быть установлено на сервер резервного копирования.

Полезный объем данных СХД должен составлять не менее 10Тб.

Требования к ленточной библиотеке

Ленточная библиотека должна обеспечивать запись и считывание данных, манипуляции с носителями информации под управлением программного обеспечения системы резервного копирования.

Автоматизирование перемещения внутри библиотеки, загрузка и выгрузка носителей информации (картриджей) и чистящих лент должно осуществляться роботом.

Идентификация носителей информации (картриджей) библиотекой должна производиться с помощью штрих-кодовых наклеек

Управление ленточной библиотекой должно осуществляться через встроенный управляющий модуль по протоколам: HTTP, HTTPS.

Подключение серверов вычислительной системы к ленточной библиотеке осуществляется через коммутаторы Fiber Channel.

Коммутаторы FC должны обеспечивать резервирование доступа серверов к ленточной библиотеке в случае отказа одного из них

Требования к устройствам доступа пользователей

Устройства доступа пользователей в сеть должны быть унифицированы в рамках всей организации.

Устройства должны быть взаимозаменяемыми и требовать минимального уровня обслуживания, либо не требовать его вовсе («тонкие клиенты»).

Для ряда пользователей допускается использование другого типа оборудования для обеспечения повышенных требований к защите информации.

1.7. Программная инфраструктура информационной системы

Общие требования

Создаваемая ИИС должна представлять собой программно-аппаратный комплекс, основанный на оборудовании и программном обеспечении.

Под программным комплексом подразумевается набор следующих подсистем:

- служба единого каталога;
- подсистема сетевых служб;
- служба обмена электронными почтовыми сообщениями;
- служба общих файловых ресурсов;
- служба сетевой печати;
- подсистема виртуальных серверов;
- подсистема виртуальных персональных компьютеров;
- подсистема резервного копирования и восстановления.

Вычислительные ресурсы необходимые для функционирования подсистем должны быть организованы в виде виртуальных машин.

ИИС должна быть рассчитана на непрерывную круглосуточную работу, допускающую запланированные перерывы на обслуживание.

Проект должен предусматривать применение современных технических решений, обеспечивающих наращивание мощности и увеличение функциональности ИИ без ее существенной перестройки.

Требования к подсистеме службы каталога

Подсистема службы каталога (ПСК) должна быть построена на базе технологии Active Directory, входящей в состав Microsoft Windows Server 2008 R2.

ПСК должна обеспечивать аутентификацию и авторизацию пользователей.

ПСК должна обеспечивать возможность логической организации ресурсов подсистемы.

ПСК должна предоставлять возможность делегирования административных полномочий на управление объектами подсистемы.

ПСК должна предоставлять механизм перемещаемых профилей и перенаправления папок пользователей.

ПСК должна обеспечивать возможность управления и настройки объектов подсистемы на основе централизованных механизмов и шаблонов.

ПСК должна непрерывно функционировать при выходе из строя одного из серверов подсистемы.

Требования к подсистеме сетевых служб

Подсистема сетевых служб (ПСС) должна включать в себя сервисы Domain Naming System (DNS) и Dynamic Host Configuration Protocol (DHCP).

ПСС должна быть построена на базе технологий, входящих в состав Microsoft Windows Server 2008 R2.

ПСС должна обеспечивать автоматическую настройку сетевых клиентских устройств подключенных по локальной сети.

ПСС должна обеспечивать прямое и обратное разрешение DNS-имен серверов, сетевых устройств и рабочих станций компании в ip-адреса.

ПСС должна обеспечивать прямое и, по возможности, обратное разрешение DNS-имен серверов в сети Интернет.

ПСС должна обеспечивать интеграцию с подсистемой виртуальных ПК.

ПСС должна непрерывно функционировать при выходе из строя одного из серверов подсистемы.

Требования к подсистеме почтовой службы

Подсистема почтовой службы (ППС) должна быть построена на базе служб, входящих в состав Microsoft Windows Server 2008 R2 и ПО Microsoft Exchange Server 2010.

ППС должна обеспечивать обмен электронными сообщениями пользователей как с внутренними получателями, так и с внешними.

ППС должна быть тесно интегрирована с ПСК для механизмов поиска адресатов и доступа к почтовым ящикам.

ППС должна обеспечивать возможность создания единой адресной книги для всех пользователей корпоративной почтовой системы.

ППС должна обеспечивать работу 200 пользователей.

ППС должна обеспечивать хранение не менее 1 ГБ почтовых сообщений в расчете на одного пользователя системы, и не менее 5 ГБ – для привилегированного. Число привилегированных пользователей составляет 10% от общего числа пользователей.

ППС должна обеспечивать контроль и ограничение используемого объема почтовых ящиков, а также уведомление пользователей и администраторов о достижении ограничений.

В качестве почтового клиента для ППС должен использоваться Microsoft Outlook 2007 и более новый.

ППС должна обеспечивать возможность доступа к почтовым сервисам по протоколам HTTPS через web-броузер.

Требования к подсистеме файловой службы

Подсистема файловой службы (ПФС) должна быть построена на базе технологий, входящих в состав Microsoft Windows Server 2008 R2.

ПФС должна обеспечивать интеграцию с ПСК для механизма разграничения доступа к ресурсам подсистемы.

ПФС должна обеспечивать возможность хранения перемещаемых профилей пользователей. Максимальный объем профиля – 300МБ, количество пользователей - 200.

ПФС должна обеспечивать возможность хранения перенаправляемых личных папок пользователей. Максимальный объем личных папок – 2 ГБ, количество пользователей – 200.

ПФС должна обеспечивать возможность хранения общих файловых ресурсов. Максимальный объем – 100 ГБ.

ПФС должна обеспечивать контроль объема используемых ресурсов с возможностью блокирования работы пользователей при превышении выделенного объема.

ПФС должна обеспечивать возможность уведомления об объеме используемых ресурсов и блокировании пользователей.

Требования к подсистеме сетевой печати

Подсистема сетевой печати (ПСП) должна быть построена на базе технологий, входящих в состав Microsoft Windows Server 2008 R2.

ПСП должна обеспечивать создание очередей печати для сетевых принтеров.

ПСП должна обеспечивать интеграцию с ПСК и предоставлять механизма разграничения полномочий по управлению очередями печати и доступа на основе групп безопасности.

Требования к подсистеме виртуальных серверов

Подсистема виртуальных серверов (ПВС) должна быть построена на базе ПО VMware vSphere.

ПВС должна обеспечивать возможность хранения виртуальных машин (ВМ) на внешней системе хранения данных.

ПВС должна обеспечивать работоспособность ВМ в случае выхода из строя одного из физических серверов.

ПВС должна обеспечивать возможность автоматического перезапуска ВМ в случае выхода из строя физического сервера.

ПВС должна обеспечивать возможность ограничения и резервации вычислительных ресурсов для группы ВМ.

ПВС должна обеспечивать автоматическую балансировку нагрузки на физические серверы в процессе запуска и работы ВМ.

ПВС должна обеспечивать возможность переноса ВМ без остановки ее работы с одного физического сервера на другой.

ПВС должна обеспечивать уведомления о критических событиях по электронной почте.

ПВС должна обеспечивать возможность управления подсистемой, как с помощью специализированного ПО, так и через web-браузер Internet Explorer.

ПВС должна предоставлять возможность делегирования административных полномочий на управление объектами подсистемы.

Требования к подсистеме виртуальных ПК

Подсистема виртуальных ПК (ПВПК) должна быть построена на базе ПВС и ПО Citrix XenDesktop.

ПВПК должна обеспечивать возможность одновременного подключения до 200 пользователей.

ПВПК должна предоставлять пользователю стандартный русскоязычный интерфейс ОС Windows.

Требования к подсистеме резервного копирования и восстановления

Подсистема резервного копирования и восстановления (ПРКВ) должна быть построена на базе ПО Symantec Backup Exec версии 2010;

ПРКВ должна обеспечивать резервное копирование и восстановление данных следующих подсистем: ПСК, ППС, ПФС, ПРКВ;

ПРКВ должна обеспечивать резервное копирование данных без прерывания функционирования служб, предоставляющих данные;

ПРКВ должна обеспечивать резервное копирование и восстановление виртуальных машин на уровне файловой системы средства виртуализации;

ПРКВ должна обеспечивать восстановление отдельных элементов файловой системы и данных подсистем из резервной копии виртуальной машины;

ПРКВ должна обеспечивать механизм создания повторяющихся задач для реализации периодического запуска заданий на резервное копирование;

ПРКВ должна использовать в качестве хранилища резервных копий ленточную библиотеку, подключаемую по интерфейсу Fiber Channel (FC);

ПРКВ может располагаться в виртуальной машине в составе ПВС;

ПРКВ должна функционировать на основе заданной политики резервного копирования, подразумевающей создание ежемесячных, еженедельных и ежедневных копий данных;

Гарантированному хранению подлежат копии полного резервного копирования всех ресурсов виртуальных машин за последний месяц, полных копий данных подсистем за 4 последних недели и результаты дифференциального копирования данных подсистем за последнюю неделю по рабочим дням за исключением пятницы;

ПРКВ должна обеспечивать функционирование заданий по созданию резервных копий без вмешательства человека, при необходимости перезаписывая старые носители новыми данными по мере потери их актуальности;

Все копируемые данные должны проходить процедуру проверки целостности;

Уведомления о всех событиях в ПРКВ должны отсылаться на заданный адрес электронной почты;

В случае аварии, включая выход из строя ПВС, ПРКВ должна обеспечивать возможность восстановления данных всех подсистем на предыдущий день согласно процедурам, описанным в регламенте восстановления.

ПРКВ должна поддерживать возможность одновременное функционирование двух приводов ленточной библиотеки для ускорения и распараллеливания выполнения заданий;

В рамках настоящей работы должны решаться следующие задачи:

настройка аппаратной платформы для обеспечения работоспособности серверного системного и прикладного программного обеспечения;

создание и настройка программной платформы для обеспечения механизмов аутентификации, обмена почтовыми сообщениями, хранения и обмена файловыми ресурсами, обеспечения сетевой печати, выполнения резервного копирования информации;

реализация программной платформы на базе средств серверной виртуализации;

организация работы пользователей на базе средств виртуализации рабочих станций.

2. Описание предлагаемых решений

2.1. ЛВС

Структурная схема ЛВС приведена на рисунке 1.

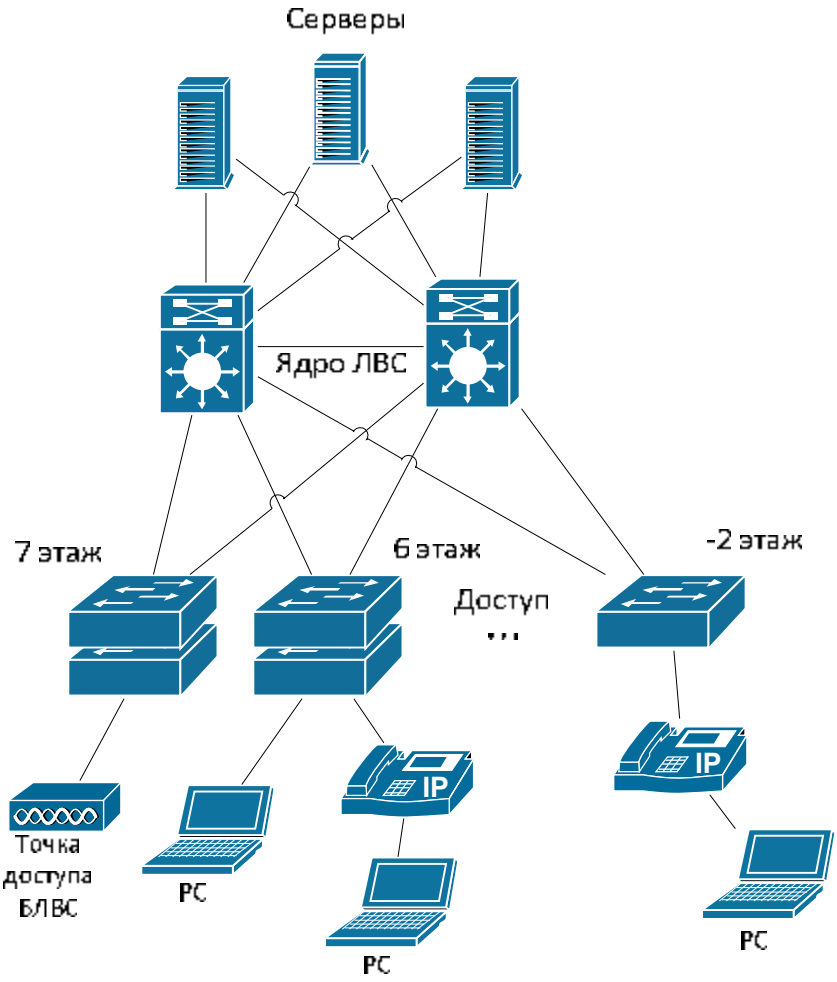

Рисунок 1 — Структурная схема ЛВС

Уровень ядра ЛВС должен состоять из двух высокопроизводительных модульных коммутаторов Extreme Networks Black Diamond 8800. Коммутаторы ядра должны размещаться в центральном телекоммуникационном центре (ТС), расположенном на втором этаже здания. Каждый коммутатор ядра должен быть оснащен двумя управляющими модулями, работающими в отказоустойчивом режиме «Active-Passive». Наличие двух модулей управления и коммутации необходимо для поддержания производительности фабрики коммутации 48 Гбит/с на слот. Коммутация трафика в коммутаторах ядра должна быть распределённой. Каждый коммутатор ядра должен иметь не менее 4 слотов для установки интерфейсных модулей.

В каждый коммутатор ядра должны быть установлены по два 8-портовых интерфейсных модуля 10 Gigabit Ethernet с форм-факторами интерфейсов для трансиверов XFP. Кроме того, в каждый коммутатор ядра должно быть установлено по одному 48 портовому интерфейсному модулю Gigabit Ethernet с портами Ethernet 10/100/1000BASE-T. Коммутаторы ядра должны быть соединены между собой двумя каналами 10 Gigabit

Ethernet, объединенными в единое логическое агрегированное соединение (LAG), и обеспечивающими межъядерное взаимодействие.

В базовой конфигурации каждый коммутатор ядра должен иметь один свободный слот под интерфейсные модули для будущих потребностей. Блоки питания коммутатор ядра должны быть дублироваться, причем выход из строя одного блока питания не должен нарушать работы коммутатора ядра.

Коммутаторы ядра также совмещают в себе функции коммутаторов серверной фермы, т.е. все серверные ресурсы подключаются к коммутаторам ядра. Blade-шасси подключаются к коммутаторам ядра каналами 10 Gigabit Ethernet (10GE) по отказоустойчивой схеме, причем эти каналы объединяются в единое логическое агрегированное соединение (LAG). Коэффициент переподписки (oversubscription) для Blade-серверов, расположенных в Blade-шасси не превышает 1:4. Прочие серверы подключаются к ядру каналами Gigabit Ethernet (GE) по отказоустойчивой схеме, эти каналы также объединяются в единое логическое соединение (LAG). Коэффициент переподписки (oversubscription) для этих серверов - 1:1.

Уровень доступа должен быть построен коммутаторах Extreme Networks Summit 460X. Коммутаторы обладают неблокируемой коммутацией и возможностью стекирования. Необходимо стремиться к унификации коммутаторов доступ и использовать коммутаторы с одинаковой плотностью портов. Коммутаторы должны размещаться в этажных телекоммуникационных центрах (ТС). В телекоммуникационных центрах 7,6,5,4,2 и 1 этажей должно быть установлено по два коммутатора доступа, в ТС 3,-1 и -2 этажей должно быть установлено по одному коммутатору. Если в этажном ТС устанавливается два и более коммутаторов доступа, эти коммутаторы должны объединяться в единое логическое устройство - стек при помощи технологии Extreme UniStack.

Коммутаторы или стеки коммутаторов доступа должны подключаться к коммутаторам ядра по отказоустойчивой схеме каналами 10 Gigabit Ethernet (10GE). Персональные компьютеры (ПК), IP-телефоны, беспроводные точки доступ, сетевые принтеры и другое периферийное сетевое оборудование должны подключаться к портам коммутаторов доступа через Ethernet 100/1000BASE-T. Коммутаторы доступа должны обеспечивать функцию передачи электропитания через Ethernet (Power over Ethernet, 802.3af) и обеспечивать до 15 ватт мощности не менее чем на 24 порта в одном коммутаторе доступа. Блоки питания коммутаторов доступа должны дублироваться, и при выходе из строя одного из блоков питания коммутатора, работа коммутатора не должна быть нарушена.

2.1.1. БЛВС

Архитектура решения подразумевает централизацию функций управления и конфигурирования беспроводной ЛВС (БЛВС) на специализированном устройстве – выделенном контроллере. Таким образом, беспроводная сеть представляет собой интеллектуальную среду, поддерживающую развитый набор дополнительных сервисов в отличие от традиционной модели БЛВС 802.11, которая состоит из отдельных и независимых компонентов. Данная модель упрощает процессы управления и развития сети, консолидируя задачи управления индивидуальными независимыми устройствами в единой управляемой системе контроллеров БЛВС.

В данной архитектуре точка беспроводного доступа является «облегченной» точкой доступа, это означает, что она не может работать независимо от контроллера. С помощью контроллера происходит конфигурирование точки доступа и обновление ее программного кода. Точки доступа, сами по себе, не требуют каких либо действий для их индивидуальной настройки.

Данные клиентов беспроводной сети между точкой доступа и контроллером передаются инкапсулированными в CAPWAP туннеле. Контроллер осуществляет передачу данных пользователей через себя, подвергая инкапсуляции трафик до них и декапсуляцию, соответственно, на обратном пути. Пакет, переданный беспроводным клиентом, получившая его точка доступа расшифровывает (если применяются механизмы шифрования), инкапсулирует в заголовок CAPWAP и передает дальше контроллеру. Контроллер разбирает (декапсулирует) заголовок CAPWAP и передает (коммутирует) его в ЛВС. Если клиент в проводной части ЛВС посылает пакет беспроводному клиенту, пакет, прежде всего, попадает на контроллер, где инкапсулируется в заголовок CAPWAP и передается соответствующей точке доступа. Точка доступа декапсулирует заголовок CAPWAP, осуществляет шифрование пакета и затем, передает его по радио искомому клиенту.

Управляющие сообщения CAPWAP передаются в зашифрованном виде с помощью протокола AES-CCM. Общий сессионный ключ шифрования вычисляется каждый раз, когда точка доступа подключается к контроллеру. Шифрования данных клиентов беспроводной сети в CAPWAP не осуществляется. Предполагается, что точки доступа взаимодействуют с контроллерами по ЛВС, которая в свою очередь является «доверительной» средой передачи данных.

Точки доступа получают электропитание из сети от коммутатора ЛВС по стандарту IEEE 802.3af (PoE).

2.2. Система унифицированных коммуникаций

Обобщённая схема организации связи приведена на рисунке 3.

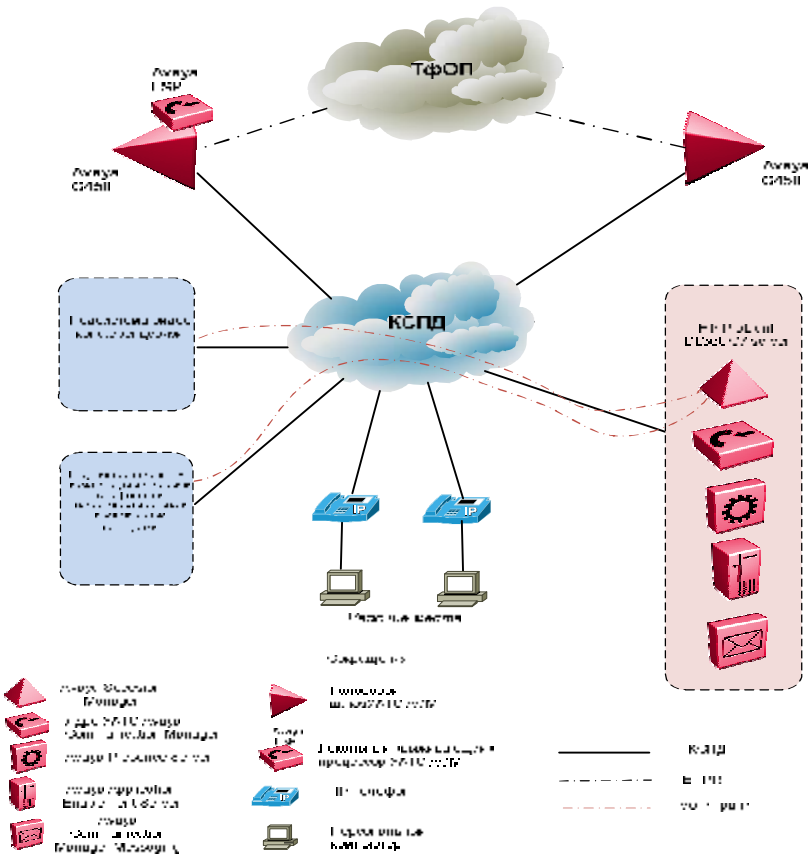

Рисунок 2 — Обобщённая схема организации связи

Для организации системы унифицированных коммуникаций предлагается решение компании Avaya Inc - Avaya Aura® for Midsize Enterprise. Это решение унифицированных коммуникаций на базе консолидированного сервера HP DL360G7, поддерживающее голосовую телефонию, обмен сообщениями, конференц-связь, а также обеспечивающее доступ к инструментам взаимодействия в рабочих группах, видеокоммуникациям и многим другим функциями – с учетом специфических потребностей обеспечения коммуникациями современного офиса.

Полная базовая система реализована на одном сервере и включает в себя компоненты : Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® Presence Server, Avaya Aura® Communication Manager Messaging, Avaya Aura® Application Enablement Services, Avaya Aura® System Platform.

За счет того, что все приложения Avaya Aura – голосовая связь, обмен сообщениями, видео, интеграция приложений, программные медиасервисы и полные возможности SIP – размещены на одном сервере, упрощается установка, администрирование и текущее обслуживание.

В качестве шлюзов для организации стыка с ТфОП и подключения аналоговых абонентских устройств (аналоговых телефонов факсов, модемов) предлагается использовать шлюзы Avaya G450. Для обеспечения отказоустойчивого подключения к ТфОП предлагается платы интерфейсов E1 установить в два различные шлюза G450, в разных серверных помещениях.

Для обеспечения локальной «выживаемости» системы телефонной связи предлагается использовать аппаратно-программное решение Local Survivable Processor (LSP). Local Survivable Processor (LSP) – это решение, позволяющее автоматически определять сбой сети (например, потеря связи с центральным кластером) и использовать шлюз для обработки вызовов телефонов на этом объекте. Шлюз выполняет обработку телефонных соединений в течение периода сбоя, тем самым обеспечивая функционирование телефонов. После восстановления LAN-канала и соединения с сетью система автоматически переводит обработку вызовов на основной сервер обработки вызовов.

Для организации беспроводной офисной связи в здании предлагается решение Avaya IP DECT, которое сочетает в себе гибкость IP сетей распределенного типа, высокое качество голосового соединения DECT, внушительный радиус покрытия, обладает минимальной чувствительностью к помехам и способно выдержать большие нагрузки.

2.3. Выделенная подсистема командно-диспетчерской связи и селекторных совещаний

Для построения выделенной подсистемы командно-диспетчерской связи и селекторных совещаний предлагается использовать предназначенный для организации управляемых аудио- и видео-конференций продукт AMT IP FORUM. В качестве системы коммутации предполагается задействовать используемое в составе системы видео-конференц-связи решение Cisco TelePresence VCS. Обобщённая схема организации ВКС и командно-диспетчерской связи и селекторных совещаний представлена на рисунке 4.

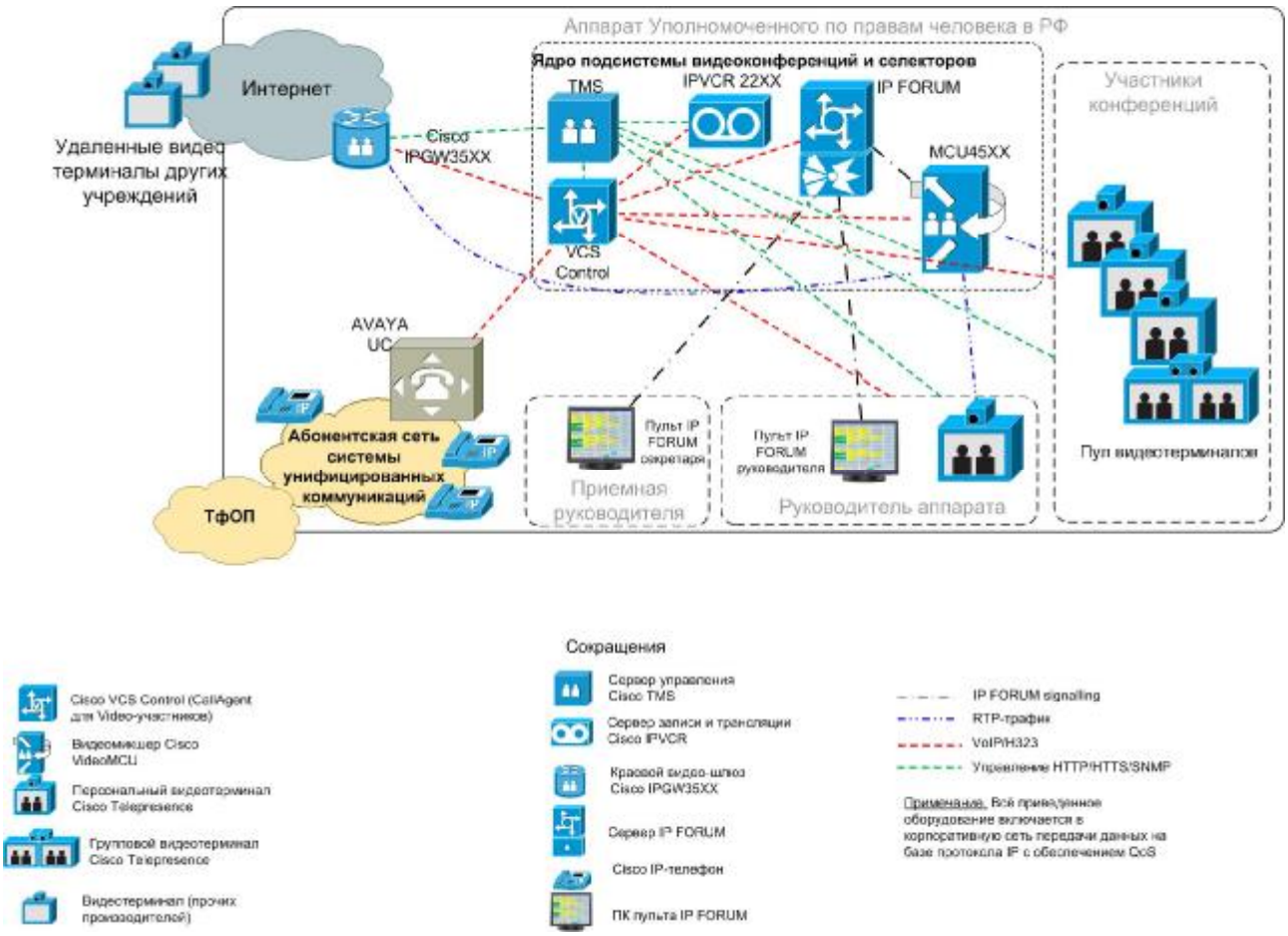

Рисунок 3 — Обобщённая схема организации видеоконференцсвязи, командно-диспетчерской связи и селекторных совещаний

Сотрудники, использующие на своих рабочих местах терминалы системы ВКС, будут использовать их также в качестве терминалов подсистемы командно-диспетчерской связи и селекторных совещаний. На рабочих местах остальных абонентов системы командно-диспетчерской связи и селекторных совещаний предполагается установить аналогичные видеотерминалы Cisco TelePresence EX60/EX90, что позволит проводить селекторные совещания с качеством видеосигнала 720p. Использование терминалов, которые поддерживают одинаковое качество приема/передачи видеоизображения, позволит обеспечить высокое качество микшированного видео для всех участников.

Кроме того, на рабочих местах руководителя организации и его помощника предполагается установить два пульта IP FORUM. Это позволит руководителю нажатием кнопок на пульте устанавливать видеотелефонные соединения с руководителями подразделений, а также самостоятельно организовывать локальный видеоселектор с участием этих сотрудников. Конференции в режиме селекторной связи с большим количеством участников сможет организовывать как сам руководитель, так и его помощник.

Использование решения IP FORUM позволит использовать следующие функции:

а) подключение в аудио-конференцию абонентов с любыми типами телефонов (в т.ч. домашние, мобильные) путем исходящего дозвона до абонентов через ядро системы видео-конференц-связи Cisco TelePresence VCS:

- индивидуальный или групповой обзвон абонентов с пульта; подключение заранее сформированной группы абонентов одним нажатием;
- вызов абонента с пульта оператора путем перебора альтернативных номеров абонента;
- автоматический сбор совещаний по расписанию путем исходящего обзвона абонентов по заранее сформированному списку;

б) включение и отключение микрофонов участников с пульта оператора или IP-телефона председателя;

в) возможность назначить председателя (председателей) с неотключаемым микрофоном;

г) автоматическое переподключение участников, отсоединившихся до завершения совещания

При проведении конференций/селекторов только в аудио-режиме[1] дополнительно IP FORUM обеспечивает следующие функции:

- аудиозапись и ведение журнала совещаний при проведении;
- возможность веб-публикации журналов и аудиозаписей совещаний для дальнейшего прослушивания участниками совещания или любыми зарегистрированными в базе данных IP FORUM абонентов;

Управление конференцией выполняется с пульта оператора, который представляет собой виртуальное кнопочное поле, реализуемое клиентским приложением IP FORUM, которое устанавливается на ПЭВМ.

Пульт (кнопочное поле) имеет следующие функциональные свойств:

- аутентификация оператора при начале работы;
- наличие индивидуальных кнопок для участников конференции; цвет подсветки кнопки индицирует статус участника (не подключен, подключается, подключен, микрофон включен, председатель, не удалось подключить);
- наличие групповых кнопок для выбора заранее сконфигурированных групп абонентов;
- наличие кнопок для выполнения операций подключения, отключения участников, подключения и отключения их микрофонов, назначения председателей.

При организации управляемых конференций в режиме видео-селектора будет использоваться видео-микшер Cisco MCU подсистемы видео-конференц-связи, что позволит проводить конференции в режиме постоянного присутствия (Continues Presence). Для обеспечения возможности подключения к селекторным совещаниям большого количество абонентов телефонных сетей будет использоваться встроенный аудио-микшер IP FORUM, что позволит использовать ресурсы оптимальным образом.

2.4. Система видео-конференц-связи

Система видеоконференцсвязи (далее – система ВКС) создается как новый сервис сети связи. Система ВКС – комплекс программно-технических средств и организационных мероприятий, обеспечивающий возможность оперативного обмена между удаленными абонентами всеми типами медиа-информации (визуальной и звуковой) в режиме реального времени. Процедура обмена информацией в системе ВКС в дальнейшем называется видеоконференцией. Обобщённая схема организации ВКС представлена на рисунке 4 (на схеме также отображены компоненты подсистемы командно-диспетчерской связи и селекторных совещаний) .

Технические средства узлов, составляющих систему ВКС, разделяют на следующие подсистемы:

— терминальное оборудование;

— серверное оборудование.

[1] Для режима ВИДЕО конференции/селектора планируется записывать с использованием дополнительных модулей, описанных в разделе по системе видео-конференц-связи

Терминальное оборудование представлено персональными и групповыми абонентскими терминалами видеоконференцсвязи. Персональные терминалы устанавливаются на столах руководителей, групповые в конференцкомнатах и конференц-зале.

Серверное оборудование входит в состав центрального узла системы ВКС и представлено следующими устройствами:

- сервер многоточечной видеоконференцсвязи;
- сервер записи и передачи потокового видео;
- сервер регистрации и логической адресации;
- сервер управления;

Данное техническое решение основывается на использовании оборудования компаний CISCO SYSTEMS.

Система ВКС имеет топологию логическая звезда, центром является серверный узел, к которому подключаются оконечные узлы ВКС (абонентские точки доступа к сервису ВКС). Узлы системы ВКС связываются между собой телекоммуникационными каналами (собственными или арендуемыми).

Сервер многоточечной видеоконференцсвязи предназначен для организации сеансов многоточечной видеоконференцсвязи между абонентами системы ВКС. Видеосервер выполняет микширование видео и аудиопотоков и формирует «раскладку» из участников для каждого абонента.

Сервер записи и передачи потокового видео обеспечивает запись проводимых сеансов видеоконференцсвязи, как в режиме «точка-точка», так и в «многоточечном» режиме, а также последующую трансляцию и архивацию записанного материала.

Сервер регистрации и логической адресации обеспечивает контроль соединения, регистрацию и логическую адресацию всего оборудования ВКС, управление пропускной способностью, маршрутизацию вызовов. А также обеспечивает возможность интеграции с IP телефонией, унифицированными коммуникациями и тд.

Сервер управления обеспечивает централизованное управление всей видеосетью: как местными, так и удаленными видеосистемами. А также поддержку, настройку, планирование видеоконференций и составление отчетов. Сервера управления могут интегрироваться с почтовыми серверами для планирования конференций при помощи почтовых клиентов.

В качестве транспортной среды используется сетевая инфраструктура объекта. Подключение оборудования ВКС осуществляется по интерфейсу Ethernet (10/100Base-T, RJ-45)..

В системе ВКС предлагается использовать только стандартные протоколы передачи, сигнализации и физические интерфейсы в соответствии с H.323 и SIP стандартами.

Требования к сети передачи данных

Для обеспечения необходимого качества обмена видео- и аудио информацией между удаленными абонентами системы ВКС в течение сеанса видеоконференцсвязи требуется наличие телекоммуникационных каналов связи, удовлетворяющих следующим характеристикам:

- минимальная пропускная способность каналов связи, выраженная в Мбит/с, между видеосервером и абонентом Системы должна составлять: скорость информационного соединения + 22% для учета трафика заголовков IP-пакетов (overhead). Для HD(720p) качества скорость информационного соединения составляет 2 Мбит/с;

- должно обеспечиваться свободное прохождение трафика в соответствии с H.323 между узлами связи абонентов подистемы ВКС при применении Proxy-server, NAT, Firewall и других средств;
- задержка прохождения пакетов: не более 150 мс в каждом направлении;
- джиттер пакетов (колебания сетевой задержки): не более 30мс;
- гарантированное качество обслуживания для нескольких типов трафика.

Требования к освещению

Система освещения должна обеспечивать:

- блокировку поступающего солнечного цвета;
- цветовую температуру (зависит от цвета стен и типа используемой видеокамеры) в пределах 3200-3600 К;
- интенсивность света для стола в пределах 800-1400 л;
- интенсивность света для стен: минимум ½ значения интенсивности света для стола и максимум ¾ этого значения;
- низкую контрастность интенсивности света.

В остальном система освещения помещений предназначенных для проведения видеоконференций должна отвечать требованиям СНиП 32-05-95.

Масштабируемость системы ВКС

Предлагаемая система ВКС является гибкой и масштабируемой. Благодаря тому, что при построении системы используются только открытые стандарты, система может со временем дополняться и модернизироваться, используя продукты разных производителей, которые поддерживают стандарты H.323 и SIP.

2.4.1. Оборудование рабочих кабинетов

Предлагается несколько вариантов персональных терминалов:

Вариант 1:

Персональный терминал ВКС CISCO EX90

- 24-дюймовый экран Full HD 1080p который можно использовать как монитор для ПК или ноутбука;
- Full HD видеокамера с автоматической фокусировкой и возможностью использования как ДОКУМЕНТ КАМЕРУ;
- 8–дюймовый сенсорный экран для управления терминалом ВКС;
- 2 громкоговорителя + сабвуфер;
- встроенный микрофон;
- разъемы для подключения ПК и дополнительного средства отображения.

– соединение в режиме «точка-точка» с разрешением до 720p(опционально до 1080p)

Вариант 2:
Персональный терминал ВКС CISCO EX60

– 21.5-дюймовый экран Full HD 1080p, который можно использовать как монитор для ПК или ноутбука;
– Full HD видеокамера с автоматической фокусировкой и возможностью использования как ДОКУМЕНТ КАМЕРУ;
– 8–дюймовый сенсорный экран для управления терминалом ВКС;
– 2 громкоговорителя;
– встроенный микрофон;
– разъем для подключения ПК.
– соединение в режиме «точка-точка» с разрешением до 720p(опционально до 1080p)

2.4.2. Оборудование кабинета VIP переговоров

В состав кабинета VIP переговоров, входят следующие подсистемы:
– подсистема видеоконференцсвязи (ВКС);
– подсистема аудиоконференцсвязи;
– подсистема отображения информации;
– аудио подсистема;
– подсистема видеокоммутации;
– подсистема управления;

Оборудование **подсистемы видеоконференцсвязи** (ВКС) выполняет функции по организации связи с удалёнными и локальными пользователями ВКС, декодированию и передачи аудио и видеосигналов на локальные подсистемы отображения и озвучивания. Система ВКС предоставляет пользователям услуги видеосвязи в режиме «точка-точка», «многоточка», а также возможность дистанционной демонстрации презентаций.

В качестве оборудования подсистемы видеоконференцсвязи предлагается использовать кодек группового абонентского терминала CISCO TELEPRESENCE C60 и 3 Full HD видеокамеры. Оборудование подсистемы поддерживает работу с видеосигналом высокого разрешения HD 720p.

Система освещения в зонах работ камер ВКС должна соответствовать требованиям, указанным выше.

В состав оборудования **подсистемы аудио-конференцсвязи** входит следующее оборудование:

- конгресс система BOSCH в состав которой входит:
    - центральный процессор;
    - дискуссионные пульты в количестве 14шт;

Дискуссионные пульты конгресс системы устанавливается каждому участнику, дискуссионные пульты оборудованы микрофоном на гибкой шее и клавишами управления. Пульт Руководителя дополнительно оборудован клавишей приоритета, при нажатии на которую микрофоны всех абонентов отключатся и раздастся сигнал привлечения внимания.

В состав оборудования **подсистемы отображения** входит:
- HD мультимедийный проектор Panasonic с экраном формата 16:9;
- две дублирующие ЖК панели отображения Samsung диагональю 46” и разрешением FullHD;

В состав оборудования **аудио подсистемы** входит следующее оборудование производителей Polycom, Kramer и RCF:
- автоматический микшер;
- подавитель обратной акустической связи;
- аудиоусилитель;
- потолочная акустика;

Подсистема видеокоммутации представлена следующими производителями KRAMER, OPTICIS, QTEX и предназначена для обеспечения функционирования подсистемы отображения информации, подсистемы управления и тд. В состав коммутационной подсистемы входят следующие устройства:
- усилители;
- распределители;
- матричные коммутаторы;
- преобразователи интерфейсов;
- удлинители интерфейсов: электрические, оптические;
- лючки со следующим набором интерфейсов:
    - силовая розетка;
    - розетка ЛВС;
    - розетка AUDIO;
    - розетка VGA.

Лючки устанавливаются на столе участников и столе Руководителя.

Подсистема управления представлена производителем CRESTRON и предназначена для управления всем оборудованием подсистем кабинета VIP переговоров. В состав подсистемы управления входят следующие устройства:
- контроллер;
- сенсорная панель управления;
- датчики сухих контактов и реле;
- порты управления по RS232, LAN

Сенсорная панель управления устанавливаются на рабочем столе Руководителя, что позволит ему запускать презентации, вызывать удаленных абонентов ВКС, и тд.

2.4.3. Оборудование зала рабочих совещаний на 100 мест

В состав зала рабочих совещаний, входят следующие подсистемы:
- подсистема видеоконференцсвязи (ВКС);
- подсистема аудиоконференцсвязи;

- подсистема отображения информации;
- аудио подсистема;
- подсистема видеокоммутации;
- подсистема управления;

Оборудование **подсистемы видеоконференцсвязи** (ВКС) выполняет функции по организации связи с удалёнными и локальными пользователями ВКС, декодированию и передачи аудио и видеосигналов на локальные подсистемы отображения и озвучивания. Система ВКС предоставляет пользователям услуги видеосвязи в режиме «точка-точка», «многоточка», а также возможность дистанционной демонстрации презентаций.

В качестве оборудования подсистемы видеоконференцсвязи предлагается использовать кодек группового абонентского терминала CISCO TELEPRESENCE C60 и 4 Full HD видеокамеры для охвата всех участников зала совещаний. Оборудование подсистемы поддерживает работу с видеосигналом высокого разрешения HD 720p.

Система освещения в зонах работ камер ВКС должна соответствовать требованиям, указанным выше.

В состав оборудования **подсистемы аудиоконференцсвязи** входит следующее оборудование:

- конгресс система BOSCH в состав которой входит:
    - центральный процессор;
    - дискуссионные пульты в количестве 103шт;

Дискуссионные пульты конгресс системы устанавливается каждому участнику, дискуссионные пульты оборудованы микрофоном на гибкой шее и клавишами управления. Пульт председателя дополнительно оборудован клавишей приоритета, при нажатии на которую микрофоны всех абонентов отключатся и раздастся сигнал привлечения внимания.

Подсистема отображения состоит из 32 ЖК панелей Samsung диагональю 46”с ультратонкой рамкой. ЖК панели располагаются в центре переговорной в виде правильного 8-ми угольника, каждая грань которого состоит из 4 ЖК панелей. Подсистема отображения закрепляется на потолке и охватывает всех участников совещания.

В состав оборудования **аудио подсистемы** входит следующее оборудование производителей Polycom и d&b audiotechnik:

- автоматический микшер;
- подавитель обратной акустической связи;
- аудиоусилитель;
- профессиональная акустическая система;

Подсистема видеокоммутации представлена следующими производителями KRAMER, OPTICIS, QTEX и предназначена для обеспечения функционирования подсистемы отображения информации, подсистемы управления и тд. В состав коммутационной подсистемы входят следующие устройства:

- усилители;
- распределители;
- матричные коммутаторы;
- преобразователи интерфейсов;
- удлинители интерфейсов: электрические, оптические;
- лючки со следующим набором интерфейсов:
    - силовая розетка;
    - розетка ЛВС;
    - розетка AUDIO;

- розетка VGA.

Лючки устанавливаются по периметру стола совещания.

Подсистема управления представлена производителем CRESTRON и предназначена для управления всем оборудованием подсистем конференц-зала. В состав подсистемы управления входят следующие устройства:

- контроллер;
- сенсорная панель управления;
- датчики сухих контактов и реле;
- порты управления по RS232, LAN

Сенсорная панель и ПК с монитором устанавливаются на рабочем месте оператора, что позволит ему управлять всем оборудование зала рабочих совещаний, запускать презентации, подключать зал к видеоконференциям, управлять микрофонами, камерами, и тд.

2.4.4. Оборудование конференцзала на 100 мест

В состав конференц-зала, входят следующие подсистемы:

- подсистема видеоконференцсвязи (ВКС) конференц-зала;
- подсистема аудиоконференцсвязи;
- подсистема отображения информации;
- подсистема ввода и коррекции информации;
- аудио подсистема;
- подсистема видеокоммутации;
- подсистема электронного голосования;
- подсистема синхронного перевода;
- подсистема управления;

Оборудование **подсистемы видеоконференцсвязи** (ВКС) выполняет функции по организации связи с удалёнными и локальными пользователями ВКС, декодированию и передачи аудио и видеосигналов на локальные подсистемы отображения и озвучивания. Система ВКС предоставляет пользователям услуги видеосвязи в режиме «точка-точка», «многоточка», а также возможность дистанционной демонстрации презентаций.

В качестве оборудования подсистемы видеоконференцсвязи предлагается использовать кодек группового абонентского терминала CISCO TELEPRESENCE C60 и 2 Full HD видеокамеры. Оборудование подсистемы поддерживает работу с видеосигналом высокого разрешения HD 720p.

Система освещения в зонах работ камер ВКС должна соответствовать требованиям, указанным выше.

В состав оборудования **подсистемы аудиоконференцсвязи** входит следующее оборудование:

- конгресс система BOSCH в состав которой входит:
  - центральный процессор;
  - дискуссионные пульты в количестве 11шт устанавливаются только на столе президиума и трибуне докладчика;
- радио-микрофонная система SHURE;

Конгресс система устанавливается на столе президиума, дискуссионные пульты оборудованы микрофоном на гибкой шее и клавишами управления. Пульт председателя дополнительно оборудован клавишей приоритета, при нажатии на которую микрофоны всех

абонентов отключатся и раздастся сигнал привлечения внимания. Таким образом, председатель может без труда управлять совещанием и контролировать его.

В состав оборудования **подсистемы отображения** входит:
- FullHD мультимедийный проектор Christie с экраном формата 16:9;
- дублирующие ЖК панели отображения Christie диагональю 55” с разрешением FullHD для президиума;

В состав оборудования **подсистемы ввода и коррекции информации** входит следующее оборудование:
- документальная камера WolfVision потолочного типа устанавливаемая над столом президиума;
- интерактивный планшет докладчика Smart Podium устанавливаемый на трибуне;
- ПК

В состав оборудования **аудио подсистемы** входит следующее оборудование производителей Polycom и d&b audiotechnik:
- автоматический микшер;
- подавитель обратной акустической связи;
- аудиоусилитель;
- профессиональная акустическая система;

Подсистема видеокоммутации представлена следующими производителями KRAMER, GEFEN, OPTICIS, QTEX и предназначена для обеспечения функционирования подсистемы отображения информации, подсистемы управления и тд. В состав коммутационной подсистемы входят следующие устройства:
- усилители;
- распределители;
- матричные коммутаторы;
- преобразователи интерфейсов;
- удлинители интерфейсов: электрические, оптические;
- лючки со следующим набором интерфейсов:
    - силовая розетка;
    - розетка ЛВС;
    - розетка AUDIO;
    - розетка VGA.

  Лючки устанавливаются только на столе президиума.

Подсистема электронного голосования состоит из программно-аппаратного комплекса и будет использоваться для проведения голосований, опросов, их обработки и представления в наглядном графическом виде, а также долговременного хранения данных. В состав комплекса входят следующие элементы:
- центральный процессор;
- встраиваемые в кресло каждому участнику пульты голосования со считывателем чип-карт;
- ПК;
- программатор чип-карт;
- программное обеспечение интерактивной системы голосования;
- программное обеспечение для проведения опросов и голосований с идентификацией участников;
- программное обеспечение для обработки результатов и вывода их в наглядном графическом виде;

Подсистема синхронного перевода BOSCH, представляющая собой систему беспроводного распределения аудио сигналов при помощи инфракрасного излучения. В состав подсистемы входят следующие элементы:

- центральный процессор;
- цифровой передатчик;
- пульты переводчиков;
- наушники;
- модуль каналов;
- инфракрасные излучатели;
- инфракрасные приемники;
- чемодан для подзарядки приемников;

Подсистема управления представлена производителем CRESTRON и предназначена для управления всем оборудованием подсистем конференц-зала. В состав подсистемы управления входят следующие устройства:

- контроллер;
- сенсорная панель управления;
- датчики сухих контактов и реле;
- порты управления по RS232, LAN

Сенсорная панель и ПК с мониторами устанавливаются на рабочем месте оператора, что позволит ему управлять всем оборудование конференц-зала, запускать презентации, подключать конференц-зал к видеоконференциям, управлять микрофонами, камерами, выводить результаты голосования и тд.

2.5. Система обеспечения информационной безопасности

Подсистема защиты подключения к сети Интернет

В состав подсистемы входят:

- кластер из универсальных шлюзов безопасности FortiGate;
- кластер из сенсоров предотвращения сетевых вторжений StoneGate IPS.

Устройства FortiGate объединены в кластер с балансировкой нагрузки. Кластер FortiGate обеспечивает проверку трафика и контроль доступа при взаимодействии устройств из разных сетей (зон). Контроль доступа обеспечивается с помощью списка правил взаимодействия между зонами. Проверка трафика осуществляется с помощью совокупности сервисов:

- антивирус,
- защиту от нежелательной электронной почты («антиспам»);
- фильтрации web-контента.

В состав функций FortiGate входит МСЭ с возможностью контроля состояния сессий (stateful firewall). Фильтрация на сетевом и транспортном уровне происходит на основе правил фильтрации трафика между зонами, в которые заносятся интерфейсы устройства, либо между интерфейсами.

По умолчанию любое взаимодействие между зонами или интерфейсами запрещено.

Для любого правила фильтрации трафика можно включить опцию трансляции адресов и портов.

Для любого правила фильтрации можно включить проверку трафика на наличие вирусов, червей, шпионского и вредоносного ПО или активности.

StoneGate IPS имеет сертификат соответствия требованиям руководящих документов по четвертому уровню контроля на отсутствие НДВ и может использоваться в ИСПДн до класса К1 включительно.

Подсистема антивирусной защиты

Для антивирусной защиты серверов и рабочих станций ЛВС используется программное обеспечение Trend Micro OfficeScan.

Trend Micro OfficeScan сертифицирован на соответствие требованиям руководящих документов по 4-му уровню контроля на отсутствие НДВ и сможет использоваться в ИСПДн до класса К1 включительно.

Программное обеспечение Trend Mirco OfficeScan обеспечивает защиту рабочих станций и серверов ЛВС от компьютерных вирусов. ПО включается в режиме постоянного мониторинга для выполнения следующих действий:

- анализ файлов, открываемых на чтение, запись и исполнение;
- при обнаружении зараженного объекта: попытка «лечения», если «лечение» невозможно – удаление объекта, с сохранением копии объекта в резервном хранилище;
- при обнаружении подозрительного объекта – помещение на «карантин»;
- при обнаружении потенциально опасной программы - блокирование ее выполнения и фиксация информации в отчете;
- проверка макрокоманд VBA, использующихся приложениями, при обнаружении подозрительной макрокоманды - блокирование ее выполнения;
- проверка скриптов VBScript и JavaScript, при обнаружении подозрительного скрипта - блокирование его выполнения.

Управление и мониторинг ПО Trend Micro на серверах и рабочих станциях ЛВС осуществляется администраторами ИБ с помощью специализированного ПО, которое устанавливается на выделенном сервере под управлением ОС Microsoft Windows Server.

Подсистема анализа защищенности

Подсистема анализа защищенности используется для проведения периодического анализа защищенности серверов, рабочих станций, активного сетевого оборудования ЛВС, средств ИБ путем сетевого сканирования. В подсистеме применяется ПО MaxPatrol производства компании Positive Technologies.

MaxPatrol Server – это серверный компонент, выполняющий все основные функции распределенного сканера безопасности: сканирование, сбор данных, их обработку, сохранение в БД и выпуск отчетов. В состав каждого MaxPatrol Server входит модуль MaxPatrol Scanner, который занимается собственно сканированием. Такой состав функционального модуля позволяет решать следующий спектр задач:

- инвентаризация ресурсов;
- контроль технических уязвимостей;
- обнаружение ошибок в конфигурации узлов и систем;
- отслеживание изменений в информационных системах;
- контроль соблюдения требований технических стандартов по безопасности;
- оценка эффективности процессов мониторинга и эффективности на основе метрик безопасности и ключевых показателей эффективности.

Сервер MaxPatrol Server устанавливается в сегмент управления ИБ и производит мониторинг всех рабочих станций ЛВС, серверного и сетевого оборудования.

Отчеты о проведенных сканированиях используются администраторами ИБ для контроля настроек оборудования и ПО, оценки защищенности и выработки необходимых мер по защите информации, а также для оценки соответствия системы защиты ПДн требованиям нормативных документов.

ПО MaxPatrol имеет сертификат соответствия требованиям руководящих документов по четвертому уровню контроля на отсутствие НДВ и может использоваться в ИСПДн до класса К1 включительно.

Управление осуществляется при помощи консоли управления (MaxPatrol Console), которая представляет собой графический интерфейс для администраторов, операторов и пользователей системы. В качестве СУБД применяется ПО MS SQL Server.

Подсистема межсетевого экранирования сегмента обработки ПДн

Средства межсетевого экранирования данной подсистемы обеспечивают выделение серверов и рабочих станций, задействованных в обработке информации, содержащей персональные данные, в логический сегмент – защищенная ЛВС, а также разграничение доступа и защиту от несанкционированного доступа на сетевом и транспортном уровнях стека протоколов TCP/IP в точке подключения ЗЛВС к общей ЛВС Организации и в точках сопряжения ИСПДн разного класса.

На межсетевых экранах также организуется сегмент, в котором размещаются сервера управления ИБ.

Технические средства ИСПДн одного класса размещаются в выделенной подсети, информационное взаимодействие между двумя или более ИСПДн различного класса происходит через межсетевые экраны описываемого функционального модуля.

На межсетевых экранах ЗЛВС задействуются интерфейсы для подключения различных сегментов сети и интерфейс для обеспечения горячего резервирования.

Межсетевые экраны StoneGate имеют сертификат соответствия требованиям руководящих документов по четвертому уровню контроля на отсутствие НДВ и 2-му классу для межсетевых экранов и может использоваться в ИСПДн до класса К1 включительно.

Подсистема разграничения доступа

В состав подсистемы входит следующее оборудование и ПО:

- ПО «SecretNet 6.5 Клиент (сетевой вариант)», устанавливаемое на рабочие станции и сервера сегмента обработки ПДн;
- электронные замки «Соболь», устанавливаемые в рабочие станции сегмента обработки ПДн;
- сервер с ПО «SecretNet – Сервер безопасности» для мониторинга/управления ПО «SecretNet 6.5 Клиент (сетевой вариант)» на серверах и рабочих станциях сегмента обработки ПДн.

ПО SecretNet обеспечивает выполнение следующих функций:

- реализует разграничение доступа к конфиденциальной информации;
- контролирует каналы распространения конфиденциальной информации;
- контролирует действия привилегированных пользователей;
- поддерживает терминальный режим работы пользователей с рабочей станцией;
- работает совместно с ОС Windows, расширяя, дополняя и усиливая стандартные механизмы защиты.

ПО SecretNet 6.5 имеет сертификат ФСТЭК на соответствие руководящим документам по 4-му уровню контроля на отсутствие НДВ и 5-му классу защищенности по СВТ и может использоваться в ИСПДн до класса К1 включительно.

Электронные замки «Соболь» используются в качестве средства защиты от НСД к рабочим станциям сегмента обработки ПДн.

Электронные замки «Соболь» 3.0 имеют сертификат ФСТЭК на соответствие руководящим документам по 2-му уровню контроля на отсутствие НДВ и могут использоваться в ИСПДн до класса К1 включительно.

В качестве персонального идентификатора используются электронные ключи Aladdin eToken. Электронные ключи eToken имеют сертификат ФСТЭК и могут использоваться в ИСПДн до класса К1 включительно.

2.6. Активное оборудование центров обработки данных

Вычислительная система

Платформа виртуализации рабочих станций развертывается с использование единого блейд-шасси и четырех блейд-серверов HP ProLiant BL460. Каждый сервер оснащен двумя шестиядерными процессорами Intel Xeon 5650, оперативной памятью объемом 144 ГБ, двумя SFF дисками 146GB 6G SAS 15K с возможностью горячей замены.

Платформа виртуализации серверов развертывается с использование единого блейд-шасси и трех блейд-серверов HP ProLiant BL460. Каждый сервер оснащен двумя шестиядерными процессорами Intel Xeon 5650, оперативной памятью объемом 96 ГБ, двумя SFF дисками 146GB 6G SAS 15K с возможностью горячей замены.

Для подсистем резервного копирования и IP FORUM выделены физические блейд-серверы HP ProLiant BL460. Каждый сервер оснащен одним шестиядерными процессором Intel Xeon 5650, оперативной памятью объемом 12 ГБ, двумя SFF дисками 300GB 6G SAS 10K с возможностью горячей замены.

Все блейд-серверы, за исключением сервера для подсистемы IP FORUM имеет возможность подключения к сети SAN по протоколу FC 8Гбит/сек

Для управления и мониторинга серверов используется встроенный управляющий модуль обеспечивающий внеполосное удаленное управление через выделенный сетевой порт по протоколу TCP/IP.

Для серверов подсистемы информационной безопасности предусмотрены три отдельно-стоящих сервера HP Proliant DL360 G7, предназначенных для монтажа в стандартные серверные 19-ти дюймовые стойки. Высота корпуса – 1 U. . Каждый сервер оснащен одним шестиядерными процессором Intel Xeon 5645, оперативной памятью объемом 12 ГБ, двумя SFF дисками 300GB 6G SAS 10K с возможностью горячей замены.

Система и сеть хранения данных

Для размещения файловых ресурсов и виртуальных машин будет использована дисковая система хранения данных HP 3PAR F-Class Storage System, оснащенная 4 полками по 12 LFF дисков 600GB 6G SAS 15K и обеспечивает хранение до 11ТБ данных в массиве RAID10. Полка подключаются двумя независимыми путями к двум контроллерам массива, что обеспечивает отсутствие единой точки отказа. Дисковый массив поддерживает различные уровни RAID, что позволяет максимальной эффективно использовать дисковое пространство с заданной производительность и доступностью.

СХД подключается через FC интерфейс к двум FC-коммутаторам, что обеспечивает отсутствие единой точки отказа.

СХД предназначена для монтажа в стандартные серверные 19-ти дюймовые стойки. Высота всех компонентов СХД, включая контроллеры, дисковые полки и PDU – 21 U.

Для организации сети передачи данных SAN используются два Fiber Channel коммутатора HP StorageWorks 8/24 SAN Switch, что обеспечивает отсутствие единой точки отказа.

Ленточная библиотека

В качестве ленточной библиотеки для подсистемы резервного копирования используется HP StorageWorks MSL2024. Данная библиотека оснащена двумя ленточным приводом Ultrium 3000 (LTO-5), 24 слотами для кассет HP LTO-5 Ultrium 3,0TB RW Data

Cartridge и роботом со сканером штрих-кодовых меток кассет, обеспечивающим автоматизированное управление и перемещение носителей внутри библиотеки. Библиотека подключатся через интерфейс FC к двум FC-коммутаторам.

Ленточная библиотека HP StorageWorks MSL2024 предназначена для монтажа в стандартные серверные 19-ти дюймовые стойки. Высота корпуса – 2 U.

2.7. Программная инфраструктура информационной системы

Платформа виртуализации

Все серверы, требуемые для организации подсистем, описанных в данном предложении, будут реализованы в виде виртуальных машин.

В качестве платформы для реализации информационной системы предлагается использовать платформу виртуализации VMware vSphere Enterprise. Основной компонент vSphere – ESXi обеспечивает одновременную работу нескольких изолированных виртуальных машин (ВМ), позволяя динамически разделять между ними физические ресурсы сервера, такие как процессоры, оперативная память, сетевая и дисковая подсистемы. Компоненты VMware vSphere – vCenter, Distributed Resource Scheduler (DRS), High Availability (HA), VMotion обеспечат высокую доступность виртуальных машин и эффективное использование вычислительных ресурсов, а также предоставят инструмент централизованного управления всей инфраструктурой.

Данные подсистемы и диски виртуальных машин будут размещены на внешней системе хранения данных (СХД).

Служба (DRS) позволяет объединить ресурсы нескольких серверов в единый пул и динамически распределять его между виртуальными машинами на основании существующих правил. Виртуальные машины, обеспечивающие работу общесистемных и прикладных приложений, будут разделены между разными пулами ресурсом. Для ВМ с приложениями с высокими требованиями вычислительные ресурсы будут зарезервированы для эксклюзивного использования.

В состав VMware vCenter включено средство мониторинга производительности, включая диаграммы использования процессоров, памяти, дисковой и сетевой подсистемы, а также механизмы уведомления о событиях. vCenter предоставляет подробные сведения, необходимые для анализа производительности физических серверов и работающих на них виртуальных машин.

Каждому физическому серверу платформы виртуализации будет назначены лицензии Windows Server 2008 Datacenter Edition, позволяющие запускать неограниченное количество экземпляров виртуальных машин с операционной системой Windows Server на одном физическом сервере.

Инфраструктура виртуальных рабочих мест

Рабочие места пользователей предлагается организовать в соответствии с концепцией Virtual Desktop Infrastructure(VDI). Концепция VDI предусматривает размещение персональных компьютеров пользователей в виде виртуальных машин на высокопроизводительных серверах под управлением платформы виртуализации. Доступ к виртуальным ПК осуществляется посредством терминального протокола с различных конечных устройств, таких как тонкие клиенты или рабочие станции под управлением ОС Windows или Linux. Управление данными пользователей обеспечивают технологии перенаправления папок пользователей и перемещаемых профилей, которые применяют персональные настройки пользователя к виртуальному ПК независимо от устройства доступа и размещения пользователя.

Подсистема виртуальных рабочих мест будет организована на базе ПО Citrix XenDesktop, обеспечивающей подключение пользователей и управлением виртуальными машинами размещенных на платформе виртуализации под управлением VMware vSphere.

Для размещения виртуальных серверов и ПК используется единая платформа виртуализации. Подобный подход позволит организовать централизованное управление и динамическое распределение вычислительных ресурсов между подсистемами.

Виртуальные ПК будут динамически собираться из эталонного образа с предустановленной ОС и набором приложений. В качестве источника эталонного образа предлагается использовать виртуальную машину под управлением Microsoft Windows 7 с объемом оперативной памяти – 2048 МБ. Для управления персональными настройками и данными пользователей будет использовано ПО Citrix Profile Manager.

Для лицензирования виртуальных ПК будет использована лицензия Windows Virtual Desktop Access (Windows VDA). Лицензия Windows VDA поставляется в рамках соглашения Microsoft Open Value в виде подписки на каждое устройство доступа. Лицензия Windows VDA предусматривает право downgrade, позволяющее использовать Windows 7 Professional или предыдущие версии данной ОС, в том числе и Windows XP.

Предлагаемая инфраструктура обеспечит работу 200 пользователей с виртуальными ПК с возможностью масштабирования без изменения архитектуры.

В качестве основного устройства доступа предлагается использовать тонкие клиенты HP t5470, подключающиеся по протоколу ICA к виртуальным ПК через корпоративную СПД.

В сравнении с традиционными настольными компьютерами виртуальные рабочие станции обладают рядом преимуществ:

Централизованное размещение виртуальных машин позволяет упростить их обслуживание и обновление. Вместо того чтобы обслуживать несколько десятков компьютеров по отдельности, необходимо следить за несколькими серверами, расположенными в ЦОД. Обслуживание виртуальных ПК или изменение их параметров выполняется удаленно.

Для доступа к виртуальным ПК могут быть использованы как тонкие клиенты, так и маломощные или устаревшие рабочие станции. Таким образом, существенно увеличивается жизненный цикл аппаратного обеспечения.

Устройство доступа не привязано к конкретному пользователю и не требует специальной настройки. Срок ввода в эксплуатацию нового рабочего места сводится к минимуму и не требует специальных навыков.

Все данные пользователей хранятся централизованно, что снижает вероятность их потери и облегчает возможность резервного копирования.

Тонкие клиенты, использующиеся для доступа к виртуальным ПК, занимают меньше места, тратят меньше электроэнергии и в большинстве случаев стоят дешевле, чем традиционные рабочие станции.

Служба каталога

В качестве подсистемы службы каталога предлагается служба Active Directory, построенная в виде единого леса с единственным доменом на базе Windows Server 2008 R2. Разворачивается корневой домен леса и устанавливается два доменных контроллера для обеспечения необходимого уровня отказоустойчивости. На всех контроллерах домена будут также размещены базовые сетевые службы, такие как DHCP и DNS.

Подсистема общих файловых ресурсов и сетевой печати

Файловый сервис и служба печати реализуются посредством стандартных сервисов и приложений, входящих в состав Windows Server 2008 R2. Подсистема обеспечит пользователям возможность печати на офисных принтерах и хранения до 100 Гб общих файловых данных на сервере. Также в рамках этой системы будут размещены профили пользователей и их личные каталоги. Файловые ресурсы и данные службы печати будут размещены на внешней системе хранения данных.

Почтовая система

В качестве службы обмена почтовыми сообщениями используется служба Microsoft Exchange 2010 Server, работающая на платформе Windows Server 2008 R2. Для обеспечения высокой доступности почтового сервиса будет использована технология непрерывной репликации между двумя серверами и балансировка сетевой нагрузки.

Каждому пользователю в компании предоставляется почтовый ящик объемом не более 1000 Мб или 5000 Мб в зависимости от категории. Доступ к ящику может осуществляться посредством почтовых клиентов Outlook, Outlook Express или через web-интерфейс браузера Internet Explorer.

Кроме обмена почтовыми сообщениями предусматривается возможность коллективной работы с общими папками и службой календарного планирования, а также использования общей адресной книги.

Подсистема резервного копирования

Для резервного копирования и восстановления данных в случае их утери планируется использовать ПО Symantec BackupExec 2010. Данный продукт обеспечивает интеграции. с платформой виртуализации VMware vSphere за счет использования технологии vStorage API и позволяет выполнять резервное копирование виртуальных машин как файлов, инкрементальное копирование.

Для копирования и восстановления данных службы каталога и почтового сервера используются специализированные агенты

В качестве хранилища долговременных резервных копий выступает ленточная библиотека.