УТВЕРЖДЕН
приказом директора

от "____"_____2012г. №____

Перспективный план развития информационно-телекоммуникационной инфраструктуры организации и подсистемы защиты информации

Содержание

1 Выделение зон безопасности

В процессе текущей эксплуатации и, при проектировании развития, выделены следующие виды сетей организации:

- Подключение к сети Интернет.
- Локальная вычислительная сеть.
- Сеть общесистемных и специализированных серверов.
- Сеть серверов для доступа к ресурсам удаленным пользователям из других учреждений здравоохранения.
- Сеть охранной и пожарной сигнализации.
- Сеть инженерного оборудования.
- Беспроводная сеть для пациентов перинатального центра, которая также используется для связи мобильного оборудования.
- Сеть для проведения видеоконференций и "телемедицины".
- Выделенная сеть для подключенных сторонних организаций.
- Выделенные сервера.
- Гараж.
- Мобильные пользователи.

2 Подключения к сети Интернет

Подключение к сети Интернет осуществляется провайдерами Томикой и Ростелекомом с использованием межсетевого экрана Cisco 3845. Подключение проводится по оптическим каналам связи с гарантированной шириной канала связи не менее 10Мбит/с.

Получены провайдер независимые адреса, распределение адресов следующее:

- Доступ в сеть Интернет пользователей ОГАУЗ "ОПЦ";
- Доступ в сеть Интернет пользователей сторонних организаций и из сети Wi-Fi;
- Подключение сервера видеоконференций;
- Размещение ресурсов, доступ к которым может быть получен из сети Интернет (web, ftp сервера, exchange);
- Подключение sip телефонии;
- Доступ удаленных и мобильных пользователей к серверам по защищенным каналам связи;

3 Локальная вычислительная сеть

Локальная вычислительная сеть представлена следующим оборудованием:

- Пользовательские персональные компьютеры и тонкие клиенты;
- Вспомогательные (служебные) персональные компьютеры;
- Сетевые принтеры, сканеры, многофункциональные устройства, факсы;
- Медицинское оборудование (анализаторы, УЗИ аппараты, мониторы состояния пациента).
- АТС и ip телефоны.
- Коммутаторы и ядро сети;

Данная сеть обрабатывает персональные данные первой категории. Персональные данные, относящиеся ко второй категории (бухгалтерия, кадры), в связи не значительным количеством пользователей/персональных компьютеров и тесной взаимосвязью с медицинской частью, будут защищаться согласно первой категории.

Перечень служебных компьютеров:

- Управление и конфигурирование ключей e-token, их учет и настройка;
- Генерация ЭЦП и управление сертификатами ЭЦП. Формирование сертификатов ЭЦП (Сайт госзаказа, СЭД, АКЦ и другие), использующие библиотеки КриптоПро. Централизованное управление сертификатами, находящимися в контейнерах пользователей КриптоПро;

3.1 Ядро сети

Ядро сети представляет собой коммутаторы Cisco Catalyst 3750X 48 Port Data IP Base, объединенные в стек для обеспечения отказоустойчивости.

Помимо стандартных параметров мониторинга, осуществляется мониторинг утилизации каналов связи (портов), аналогичный межсетевому экрану Cisco 3845.

К данным коммутаторам подключены все коммутаторы, задействованные для организации работы оборудования, относящегося к локальной вычислительной сети.

3.2 Система распределения адресов

Для систематизации адресного пространства локальной вычислительной сети принято следующее правило:

Назначение	Сеть/маска
Ядро сети и коммутаторы	192.168.0.0/24

Пользовательские рабочие станции и тонкие клиенты, АТС администрирование и ip телефоны, вспомогательные компьютеры	192.168.2.0/24 192.168.3.0/24 192.168.4.0/24 (резерв)
Сетевые принтеры, многофункциональные устройства, сетевые сканеры, сетевые факсы	192.168.5.0/24
Подключенное медицинское оборудование	192.168.6.0/24 192.168.7.0/24 (резерв)
Резерв	192.168.8.0/24 192.168.9.0/24 192.168.10.0/24

3.3 Категория обрабатываемой информации

Данная локальная вычислительная сеть обрабатывает информацию, относящуюся к персональным данным первой категории. Защита осуществляется согласно политики защиты информации.

4 Сеть общесистемных и специализированных серверов

Данная сеть содержит следующее оборудование:

- Сервера для обеспечения работы всех сервисов сети.
- Сервера для обеспечения отказоустойчивости ключевых сервисов сети.
- Сервер управления виртуальными машинами.
- Систему резервного копирования.

4.1 Описание основных функций серверов

Основными серверами являются:

4.1.1 Контроллер домена

Ведение каталога пользователей, централизованной аутентификации и авторизации. Для обеспечения отказоустойчивости на резервных серверах работает дополнительный контроллер домена.

4.1.2 Система мониторинга Zabbix

Система для организации мониторинга состояния серверов, каналов связи, инженерного и иного оборудования (если оборудование дает такую возможность). Функционирует под управлением операционной системы Linux CentOS. В качестве базы данных использует MySQL.

Обязательными параметрами для мониторинга являются (если применимо к оборудованию):

- Загрузка каналов связи (сетевых интерфейсов, портов) - общая и по протоколам, входящий и исходящий трафик;
- Загрузка процессоров;
- Объем и загрузка используемой оперативной памяти;
- Объем и загрузка разделов жесткого диска, процент их активности;
- Температура оборудования;

Срок хранения данных составляет 6 лет.

Система мониторинга позволяет отследить динамику изменения загрузки оборудования за любой период хранения информации. Также система мониторинга осуществляет информирование диспетчерской службы, инженерного персонала, руководства заинтересованных отделов и главного инженера в критичных ситуациях посредством отправки сообщения на электронную почту и sms сообщения на сотовый телефон.

В случаях, если настройка обязательных параметров мониторинга оборудования приводит к необоснованной загрузке оборудования, допускается их отключение.

Резервное копирование сервера осуществляется на систему резервного

копирования еженедельно.

Система мониторинга показывает комплексные экраны, размером по горизонтали 3 и по вертикали 2, отражающие для каждого сервера:

- CPU Loads;
- CPU Utilization;
- Network Utilization;
- Disk usage in %;
- Disk usage in Gb;
- Total login users;

4.1.3 Сервер электронной почты

Сервер обеспечивает работу почтовой службы, ведения календарей, заданий, адресной книги. Функционирует под управлением операционной системы Microsoft Windows 2008 R2 Standard. Почтовые функции обеспечиваются Microsoft Exchange Server 2010 Standard и соответствуют следующим требованиям:

- Вся входящая и исходящая почта, независимо с какого устройства (компьютер, планшетный компьютер, сотовый телефон и другие устройства) была отправлена, храниться на сервере. При подключении нового устройства происходит ее синхронизация (входящей и исходящей). Возможность назначения заместителя, которому (на время назначения) направляется входящая почта;
- Общие и личные контакты, списки контактов. Должны отражаться в списке ресурсов системы управления проектами. При подключении различных устройств происходит их синхронизация;
- Ведение календарей (личных и общих). При подключении различных устройств происходит их синхронизация;
- Ведение задач (заданий). Возможность назначения задания другому пользователю (из списка контактов или списку). Установка сроков исполнения. При подключении различных устройств происходит их синхронизация;
- Заметки. При подключении различных устройств происходит их синхронизация;
- Решение имеет web интерфейс, доступный из сети Wi-Fi и сети Интернет;
- Есть возможность работы с сервером как windows (Outlook, Outlook Express), так и linux (Evolution) почтовым клиентам;
- Доступ обеспечен из локальной сети (персональные компьютеры);
- Доступ обеспечен из сети Wi-Fi и сети Интернет (планшетники/ноутбуки мобильных пользователей) по защищенному каналу связи;
- Максимальная интеграция с системой совместной работы и системой управления проектами;

С целью реализации системы защиты информации устанавливается

дополнительный сервер в зоне выделенных серверов. Антивирусная и спам защита обеспечивается централизованно используемым антивирусом.

Настройка сервера и почтовых клиентов производится централизованно с использованием политик Active Directory (если применимо).

Резервное копирование сервера осуществляется еженедельно.

В случае если данный сервис будет предложен ЦОДом, будет осуществлен переход на использование данного сервиса.

4.1.4 Сервер совместной работы

Microsoft SharePoint Server

4.1.5 Сервер управления проектами

Microsoft Project Server

4.1.6 Сервер антивирусной защиты

Сервер обеспечивает антивирусную защиту серверов и рабочих станций. В качестве используемой версии выбран Антивирус Касперского, сертифицированный для защиты персональных данных первой категории.

Функционирование сервера антивируса производится под управлением операционной системы Windows Server 2008 R2 Standard. Используется база данных Microsoft SQL Server, располагаемая на централизованном SQL сервере.

Все настройки антивируса, установленного на рабочих станциях и серверах, осуществляются централизованно с сервера антивирусной защиты, в том числе настройки сетевого экрана.

Резервное копирование сервера осуществляется еженедельно.

4.1.7 Сервер баз данных Microsoft SQL Server.

Сервер баз данных SQL для используемого программного обеспечения. Функционирует под управлением следующего программного обеспечения:

- Операционная система Microsoft Windows 2008 R2 Enterprise;
- Система управления базами данных Microsoft SQL Server 2008 R2 Standard;
- Антивирус;

Обеспечивает работу следующих баз данных:

- МИС "Медиалог";
- Антивируса Касперского;
- СЭД Федерального Казначейства;
- Парус 10 Торнадо;
- Orion;

- Device Manager;
- WSUS;
- КодБезопасности: Инвентаризация;
- Анализаторы и медицинское оборудование (если применимо);

Отказоустойчивость обеспечивается созданием кластера серверов.

Резервное копирование баз данных осуществляется ежедневно. Резервное копирование серверов осуществляется еженедельно.

4.1.8 Сервер МИС "Медиалог"

Сервер для обеспечения работы пользователей с МИС "Медиалог" в терминальном режиме по протоколу RDP. Назначение – основная и единственная используемая МИС организации.

Сервер функционирует под управлением следующего программного обеспечения:

- Операционная система Microsoft Windows 2008 R2 Enterprise;
- Офисный пакет Microsoft Office 2010 Professional;
- МИС "Медиалог";
- Антивирус;

МИС "Медиалог" использует базу данных, расположенную на централизованном сервере баз данных SQL.

Настройка операционной системы, офисного пакета осуществляется с использованием политик Active Directory. Управление антивирусом осуществляется централизованно.

Система мониторинга осуществляет контроль, кроме стандартных параметров оборудования сервера, следующие:

- Количество работающих пользователей;

Обеспечение отказоустойчивости обеспечивается созданием терминального кластера.

Резервное копирование сервера осуществляется на систему резервного копирования с периодичностью 1 раз в неделю.

В перспективе переход на МИС, предложенную создаваемым ЦОДом.

4.1.9 Сервер "Парус"

Сервер для обеспечения работы программного продукта "Паруса 10 (Торнадо): Кадры для медицины" и "Парус 7". Работа пользователей проводится в терминальном режиме по протоколу RDP.

Сервер функционирует под управлением следующего программного обеспечения:

- Операционная система Microsoft Windows 2008 R2 Enterprise;
- Офисный пакет Microsoft Office 2010 Professional;
- Паруса 10 (Торнадо): Кадры для медицины;
- Парус 7;
- Антивирус;

Настройка операционной системы, офисного пакета осуществляется с использованием политик Active Directory. Управление антивирусом осуществляется централизованно.

Система мониторинга осуществляет контроль, кроме стандартных параметров оборудования сервера, следующие:

- Количество работающих пользователей;

Обеспечение отказоустойчивости обеспечивается созданием терминального кластера.

Резервное копирование сервера осуществляется на систему резервного копирования с периодичностью 1 раз в неделю.

В перспективе переход на экономический, бухгалтерский, кадровый учет на базе "1С:Предприятие Управление производственным предприятием" или переход на использование программного продукта, предложенного создаваемым ЦОДом.

4.1.10 Сервер баз данных Firebird

Сервер баз Firebird. Функционирует под управлением операционной системы Linux Centos и обеспечивает функционирование баз данных следующего программного обеспечения:

- МИС "Искус", предназначенный для обеспечения работы поликлиники и стационаров;
- МИС "Искус", предназначенный для мониторинга беременных женщин;
- МИС "Искус", предназначенный для проведения тренировок, изучения возможностей;
- ПО "Мистер", предназначенное для ведения отчетности;

Резервное копирование всех баз данных выполняется ежедневно, резервное копирование сервера осуществляется еженедельно.

4.1.11 Сервер МИС "ИСКУС"

Обеспечивает работу пользователей со следующим программным обеспечением:

- МИС "Искус", предназначенном для обеспечения работы поликлиники и стационаров;
- МИС "Искус", предназначенном для обеспечения работы мониторинга беременных женщин;
- МИС "Искус", предназначенном для проведения тренировок, изучения

возможностей системы;

- ПО "Мистер", предназначенное для ведения отчетности в ОГУЗ "Бюро медицинской статистики";

Функционирует под управлением следующего программного обеспечения:

- Операционная система Microsoft Windows 2008 R2 Standard;

Офисный пакет Microsoft Office 2010 Professional;

- Антивирус;

Работа с программным обеспечением осуществляется в терминальном режиме по протоколу RDP.

Настройка операционной системы, офисного пакета осуществляется с использованием политик Active Directory. Управление антивирусом осуществляется централизованно.

Система мониторинга осуществляет контроль, кроме стандартных параметров оборудования сервера, следующие:

- Количество работающих пользователей;

Резервное копирование сервера осуществляется на систему резервного копирования с периодичностью 1 раз в неделю.

В перспективе перенос выполняемых функций в МИС "Медиалог" или МИС, предложенную создаваемым ЦОДом.

4.1.12 Сервер приложений Windows

Данный сервер обеспечивает работу пользователей, подключающихся с тонких клиентов с офисным программным обеспечением. Доступ к серверам МИС, серверам Бухгалтерского программного обеспечения осуществляется с данного сервера в терминальном режиме. Также обеспечивает функционирование следующего программного обеспечения и раздачу приложений по сети для пользователей персональных компьютеров:

- Консультант;
- Comita;
- СЭД Федерального Казначейства;
- АЦК;

Функционирует под управлением следующего программного обеспечения:

- Операционная система Microsoft Windows 2008 R2 Enterprise;
- Microsoft Office 2010 Professional Plus;
- Антивирус;

Настройка операционной системы осуществляется с использованием политик Active Directory. Настройка антивируса осуществляется централизованно.

Ярлыки для запуска приложений на рабочих столах пользователей создаются с использованием политик Active Directory в соответствии с группами, в которые

включены пользователи.

Отказоустойчивость и балансировка нагрузки обеспечивается созданием кластера терминальных серверов.

Профили пользователей ограничены 128 Мб и хранятся на файловом сервере.

4.1.13 Сервер прокси

Прокси-сервер, обеспечивающий доступ пользователей в сеть Интернет. Обеспечивает следующие функции:

- Доступ в сеть Интернет пользователей, входящих в группу Internet;
- Ведение статистики использования сети интернет пользователями;
- Запрет доступа к сайтам, запрещенным политикой использования ресурсов сети Интернет;

Функционирует под управлением операционной системы Linux Centos. В качестве прокси используется squid.

4.1.14 Сервер печати

Сервер, обеспечивающий работу сетевых принтеров, сканеров, факсов. Обеспечивает следующие функции:

- Обеспечивает управление заданиями указанного оборудования;
- Ведет статистику по пользователям и историю заданий по каждому пользователю, количества напечатанных листов принтером, расходным материалам.
- Установку оборудования на персональный компьютер производиться с правами пользователя и недоступна неавторизированным пользователям;

Функционирует под управлением операционной системы Windows 2008R2 Standard.

Установка принтеров на терминальные сервера и рабочие станции пользователям осуществляется с использованием политик Active Directory.

4.1.15 Сервер DICOM

Обеспечивает хранение изображений с рентген аппаратов, аппаратов УЗИ, другого оборудования, поддерживающего протокол DICOM, PALC.

Функционирует под управлением операционной системы Linux Centos.

Интегрирован с используемой МИС.

В перспективе передача в создаваемый ЦОД.

4.1.16 Файловый сервер

Обеспечивает хранение пользовательских файлов, архивов, видеозаписей и т.д. Функционирует под управлением операционной системы Linux Centos.

4.1.17 Сервер Device Manager

Сервер Device Manager обеспечивает управление настройками тонких клиентов. Функционирует под управлением следующего программного обеспечения:

- Операционная система Microsoft Windows 2008 R2 Standard;

База данных SQL, расположенная на централизованном сервере SQL.

- Антивирус;

Настройка операционной системы осуществляется с использованием политик Active Directory. Управление антивирусом осуществляется централизованно.

Резервное копирование сервера осуществляется на систему резервного копирования с периодичностью 1 раз в неделю.

4.1.18 Сервер обновлений wsus

Назначение - обеспечение централизованного обновления Windows серверов и рабочих станций. Используя данный сервер, осуществляется обновление следующего программного обеспечения:

- Операционная система Windows;
- Офисный пакет Microsoft Office;

Функционирует под управлением следующего программного обеспечения:

- Операционная система Microsoft Windows 2008 R2 Standard;
- WSUS 3.0;
- База данных SQL располагается на централизованном сервере SQL;
- Антивирус;

Разрешенные обновления отмечаются вручную после проведения их тестирования на группе тестовых рабочих станций.

Резервное копирование сервера не производится.

4.1.19 Сервер 1С

Нужен, если учет работы кабинетов кризисной беременности будет построен на базе конфигурации 1С (в перспективе учет работы ЦКБ должен идти в используемой МИС) или Бухгалтерский учет будет переведен с Паруса на 1С. Работа будет осуществляться в терминальном режиме.

4.2 Система резервного копирования

Обеспечивает хранение резервных копий баз данных, виртуальных машин.

Резервное копирование виртуальных машин серверов осуществляется еженедельно, баз данных ежедневно в часы наименьшей загруженности (если не указано иное).

Сроки хранения резервных копий:

- Ежедневные копии баз данных – 3 месяца;
- Копии серверов (виртуальных машин) – 1 месяц;
- Резервные копии первого числа месяца баз данных – 5 лет;

4.3 Сервер vCenter

Сервер обеспечивает управление хостами виртуальных машин. Представляет собой выделенный физический сервер с установленной операционной системой Microsoft Windows 2008 R2 Standard, программным обеспечением VMware vCenter Server, антивирусом.

4.4 Обеспечение отказоустойчивости ключевых сервисов

Перечень ключевых сервисов:

- Служба каталогов ActiveDirectory;
- Сервер баз данных Microsoft SQL Server R2 Standard;
- Терминальный сервер МИС "Медиалог";
- Терминальный сервер "Паруса";
- Терминальный сервер приложений Windows;
- Сервер DICOM;

Отказоустойчивость ключевых сервисов достигается следующим образом:

- Разнесение контроллеров домена на физически разные серверы.
- Сервера баз данных SQL, Терминальные сервера МИС "Медиалог", Паруса, приложений Windows работают в режиме отказоустойчивого кластера, узлы которого располагаются на физически разных серверах.
- DICOM сервер путем копирования на систему резервного копирования еженедельно;

4.5 Обеспечение восстановления в случае сбоев

Обеспечение резервного копирования баз данных (при необходимости виртуальных машин) на систему резервного копирования.

Проведение тренировок по восстановлению информации.

4.6 Развертывание серверов

Развертывание серверов производится в виртуальной среде VMware. Управление виртуальными машинами осуществляется с использованием сервера vCenter.

4.7 Система адресации

Адреса оборудования находятся в сети 192.168.1.0/24

5 Сервера для удаленных пользователей

Зона серверов, на которых будут размещаться ресурсы, доступ к которым может быть получен из сети интернет по защищенному каналу связи.

Сервера представлены виртуальными машинами, находящимися на выделенном физическом сервере. Управление виртуальными машинами производится сервером vCenter.

5.1 Сервер МИС "Медиалог"

Сервер МИС "Медиалог" для удаленных клиентов. Доступ с разрешенных ip адресов учреждений здравоохранения по протоколу RDP по защищенному каналу связи.

Назначение – ввод данных, касающихся мониторинга беременных, перевод учреждений для работы с одной МИС в рамках работы с единой базой данных, организация работы Центров Кризисной Беременности.

Сервер функционирует под управлением следующего программного обеспечения:

- Операционная система Microsoft Windows 2008 R2 Standard;
- Офисный пакет Microsoft Office 2010 Professional;
- Антивирус;
- МИС "Медиалог";

МИС "Медиалог" использует базу данных, расположенную на централизованном сервере баз данных.

Настройка операционной системы, офисного пакета осуществляется с использованием политик Active Directory. Управление антивирусом осуществляется централизованно.

Система мониторинга осуществляет контроль, кроме стандартных, следующие параметры сервера:

- Количества работающих пользователей;

Резервное копирование сервера осуществляется на систему резервного копирования с периодичностью 1 раз в неделю.

В случае перехода на МИС, предложенную ЦОДом, осуществляется переход на использование данной МИС.

5.2 Сервер МИС "ИСКУС"

Назначение, требования к серверу по настройке и резервному копированию аналогичны серверу Медиалога. В качестве МИС будет использоваться ИСКУС. Для организации работы центров кризисной беременности будет использоваться сервер 1С:ЦКБ.

Данный сервер не нужен, если все работы будут проводиться в МИС "Медиалог".

5.3 Сервер 1С:ЦКБ

Назначение сервера 1С:ЦКБ - организация работы центров (кабинетов) кризисной беременности. Доступен с ip адресов учреждений здравоохранения, открывших кабинеты кризисной беременности по протоколу RDP. Работа на сервере осуществляется с конфигурацией 1С, расположенной на сервере 1С, посредством web интерфейса.

Не нужен, если назначение сервера будет реализовано в МИС "Медиалог".

Требования к серверу по настройке и резервному копированию аналогичны серверу МИС "Медиалог".

6 Сеть охранной и пожарной сигнализации

Сеть охранной и пожарной сигнализации содержит:

- Сервер охранной и пожарной сигнализации Orion;
- Видеорегистраторы;
- Компьютеры охраны;
- Систему оповещения МЧС.

Сервер охранной и пожарной сигнализации представляет собой выделенный сервер с операционной системой Windows 2008 R2 Standard, установленной системой управления базами данных Microsoft SQL Server 2008 R2, установленным программным обеспечение Orion, антивирусом, агентом ПО "КодБезопасности: Инвентаризация".

Компьютеры охраны представляют собой персональные компьютеры с установленной операционной системой Microsoft Windows 7, программным обеспечением для просмотра видеокамер с видеорегистраторов, антивирусом, агентом ПО "КодБезопасности: Инвентаризация".

Оборудование, подключенное в сеть охранной и пожарной сигнализации, осуществляет синхронизацию времени с сервером точного времени.

Система мониторинга осуществляет контроль следующих параметров оборудования сети, кроме стандартных:

- Работоспособность СУБД SQL Server;
- Использование места на видеорегистраторах;
- Загрузку процессора, объема используемой памяти и жесткого диска компьютеров охраны;
- Работоспособность системы оповещения МЧС.

Управление антивирусом осуществляется централизованно.

7 Сеть инженерного оборудования

Перечень оборудования:

- Лифты
- Сервер диспетчеризации и обслуживаемое им оборудование.
- Другое оборудование.

8 Беспроводная сеть Wi-Fi

Содержит точки доступа, коммутатор для подключения и управления точками доступа. С использованием открытой сети подключаются компьютеры пациентов для выхода в сеть интернет. Доступ в сеть Интернет ограничен протоколами http, https.

Также с использованием сети подключаются мобильные рентген аппараты. Для защиты рентген аппаратов от воздействия из внешних сетей устанавливается сертифицированный межсетевой экран. В качестве сертифицированного межсетевого экрана выбран "Континент АП", совместимый и управляемый сертифицированным межсетевым экраном "Континент-К" IPC-100.

Система мониторинга отслеживает следующие параметры:

- Доступность точек доступа;
- Количество подключенных пользователей к каждой точке доступа;
- Объем входящего и исходящего трафика каждой точки доступа;
- Общее и используемое количество ip адресов dhcp сервера сети Wi-Fi.

9 Видеоконференции и телемедицина

Сеть включает в себя видеокамеры, проектор, компьютеры для управления видеокамерами (сервер), компьютер для организации видеоконференций, сервер видеоконференций (TandbergC60 (?)).

Возможность доступа из локальной вычислительной сети выделенным пользователям к камерам только на просмотр.

Управление видеокамерами осуществляется с использованием физических серверов, выделенных для этих целей.

Сервисы телемедицины должны обеспечивать как "удаленные" консультации пациентов, так и возможность проведения видеоконференций, селекторных совещаний с другими ЛПУ.

В перспективе передача данных функций в ЦОД (МИАЦ).

10 Сеть сторонних организаций

Подключение сторонних организаций (кафедры СибГМУ). Разные сторонние организации подключены в разные виртуальные сети.

11 Выделенные сервера

Данные сервера представлены следующим списком:

- Web сервер;
- Exchange;

Данные сервера располагаются на выделенном физическом сервере, функционируют в виртуальной среде VMware и являются виртуальными машинами.

11.1 Web сервер

Web сервер для размещения сайта. Доступ из сети интернет с любого адреса по протоколам http, https. Также с использованием сайта осуществляется запись на прием пациентов.

Функционирует под управлением операционной системы Linux Centos. В качестве web сервера используется apache и 1С:Битрикс.

В перспективе запись на прием осуществляется через централизованный web сайт.

11.2 Exchange сервер

Exchange сервер обеспечивает web интерфейс для доступа удаленных пользователей к ресурсам электронной почты.

В случае передачи данных сервисов в создаваемый ЦОД, данные функции также передадутся в ЦОД.

12 Гараж

Сеть, включающая:

- Компьютер механика;
- Видеорегистратор;

Настройки и защита компьютера механика идентичная входящим в домен и соответствует политики защиты персональных данных первой категории.

Видеорегистратор установлен в сейфе, находящийся в гараже. Видеосигнал с камер, подключенных к видеорегистратору, передается с видеорегистраторов на посты охраны.

Для осуществления контроля по ГЛОНАСС за местонахождением автомобилей установлено соответствующее программное обеспечение.

Связь между гаражом и серверным помещением осуществляется по оптическому кабелю. Для обеспечения телефонной связи и связи датчиков охранной и пожарной сигнализации с сервером Orion проложен кабель емкостью 10 пар.

13 Мобильные пользователи

Организация доступа мобильных пользователей к ресурсам сети осуществляется по защищенным каналам связи с использованием Континент АП. Двухфакторная авторизация пользователей происходит под доменным именем.

Типовая настройка рабочих мест мобильных пользователей:

- Ноутбук;
- Операционная система Microsoft Windows 7;
- Офисный пакет Microsoft Office 2010 Professional;
- Система управления проектами Microsoft Project 2010 Professional;
- Антивирус Касперского;
- Континент АП;

Настройка и управление программным обеспечением осуществляется централизованно с серверов организации, согласно политики настройки типовых рабочих станций.

14 Тонкие клиенты

В соответствии с рекомендациями Минздравсоцразвития, основное обеспечение рабочих мест пользователям будет производиться на базе тонких клиентов. Персональные компьютеры будут приобретаться только в случае обоснованной необходимости.

Требования к программному обеспечению тонких клиентов. ОС linux, возможность централизованного управления, поддержка протоколов RDP, Citrix.

При включении тонких клиентов будет предложено одно подключение к серверу приложений Windows, с которого уже можно подключиться к серверам МИС, Бухгалтерским.

Управление тонкими клиентами производится централизованно с сервера. К тонким клиентам могут подключаться локальные принтеры по usb порту.

15 Программное обеспечение

Поскольку в основу построения сети положен домен windows 2008, на рабочих станциях будет использоваться ОС windows 7. В качестве почтового клиента должен использоваться, умеющий работать с сервером Exchange и обеспечивающий возможность переписка, ведения календаря, назначения заданий.

В качестве основного офисного пакета должен использоваться MSOffice, LibreOffice, OpenOffice.

Для обеспечения совместимости файлов между офисными пакетами текстовые файлы должны сохраняться в формате rtf.

В случае принятия решения организацией, управляющей ЦОДом, или, в связи с реализацией распоряжения правительства от 17 декабря 2010 г. №2299-pi, будет осуществлен переход на использование СПО.

16 Защита информации

Обеспечение защиты информации разделено на следующие этапы:

- Организационные мероприятия, приводящие к систематизации информационных систем, обрабатывающих персональные данные. Разработка необходимых документов;
- Технические средства для реализации положений, приказов, регламентов, согласно проведенных организационных мероприятий;

16.1 Организационные меры

Организационные меры.

16.2 Средство защиты информации от несанкционированного доступа SecretNet.

16.2.1 Разграничение доступа

Усиленная идентификация и аутентификация пользователей Система Secret Net 6 совместно с ОС Windows обеспечивает идентификацию и аутентификацию пользователя с помощью программно-аппаратных средств при его входе в систему. В качестве устройств для ввода в нее идентификационных признаков могут быть использованы:

- iButton;
- eToken Pro,
- eToken PRO Java (USB, смарт-карты);
- Rutoken;

Управление доступом пользователей к конфиденциальным данным. Функция управления доступом пользователей к конфиденциальной информации. Каждому информационному ресурсу назначается один их трёх уровней конфиденциальности: «Не конфиденциально", "Конфиденциально", "Строго конфиденциально", а каждому пользователю – уровень допуска. Доступ осуществляется по результатам сравнения уровня допуска с категорией конфиденциальности информации.

Разграничение доступа к устройствам Функция обеспечивает разграничение доступа к устройствам с целью предотвращения несанкционированного копирования информации с защищаемого компьютера. Существует возможность запретить, либо разрешить пользователям работу с любыми портами/ устройствами.

Разграничивается доступ к следующим портам/устройствам:

- Последовательные и параллельные порты;

- Сменные, логические и оптические диски;
- USB-порты.
- Контроль подключения устройств на шинах USB, PCMCIA, IEEE1394 по типу и серийному номеру, права доступа на эти устройства задаются не только для отдельных пользователей, но и для групп пользователей.
- Возможность запретить использование сетевых интерфейсов — Ethernet, 1394 FireWire, Bluetooth, IrDA, WiFi.

16.2.2 Доверенная информационная среда

Защита от загрузки с внешних носителей. С помощью средств аппаратной поддержки можно запретить пользователю загрузку ОС с внешних съёмных носителей. В качестве аппаратной поддержки система Secret Net 6 использует программно-аппаратный комплекс "Соболь" и Secret Net Card. Плату аппаратной поддержки невозможно обойти средствами BIOS: если в течение определённого времени после включения питания на плату не было передано управление, она блокирует работу всей системы.

Замкнутая программная среда. Для каждого пользователя компьютера формируется определённый перечень программ, разрешенных для запуска. Он может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей. Применение этого режима позволяет исключить распространение вирусов, "червей" и шпионского ПО, а также использования ПК в качестве игровой приставки.

Контроль целостности. Используется для слежения за неизменностью контролируемых объектов с целью защиты их от модификации. Контроль проводится в автоматическом режиме в соответствии с некоторым заданным расписанием.

Объектами контроля могут быть файлы, каталоги, элементы системного реестра и секторы дисков. Каждый тип объектов имеет свой набор контролируемых параметров. Так, файлы могут контролироваться на целостность содержимого, прав доступа, атрибутов, а также на их существование, т.е. на наличие файлов по заданному пути. При обнаружении несоответствия предусмотрены следующие варианты реакции на возникающие ситуации нарушения целостности:

Регистрация события в журнале Secret Net; блокировка компьютера; восстановление повреждённой/модифицированной информации; отклонение или принятие изменений.

Контроль аппаратной конфигурации компьютера осуществляет своевременное обнаружение изменений в аппаратной конфигурации компьютера и реагирования на эти изменения. Предусмотрено два вида реакций:

- Регистрация события в журнале Secret Net;
- Блокировка компьютера;

Функциональный самоконтроль подсистем Самоконтроль производится перед входом пользователя в систему и предназначен для обеспечения гарантии того,

что к моменту завершения загрузки ОС все ключевые компоненты Secret Net 6 загружены и функционируют.

16.2.3 Защита информации в процессе хранения

Контроль печати конфиденциальной информации. Печать осуществляется под контролем системы защиты. При разрешённом выводе конфиденциальной информации на печать документы автоматически маркируются в соответствии с принятыми в организации стандартами. Факт печати отображается в журнале защиты Secret Net 6.

Гарантированное уничтожение данных Уничтожение достигается путем записи случайной последовательности на место удаленной информации в освобождаемую область диска. Для большей надежности может быть выполнено до 10 циклов (проходов) затирания.

Регистрация событий Система Secret Net 6 регистрирует все события, происходящие на компьютере: включение / выключение компьютера, вход / выход пользователей, события НСД, запуск приложений, обращения к конфиденциальной информации, контроль вывода конфиденциальной информации на печать и отчуждаемые носители и т.п.

16.2.4 Удобство управления и настроек

Сетевая версия системы Secret Net 6 обладает всеми возможностями автономной версии, кроме того в нее включены средства централизованного управления, что существенно облегчает работу администратора безопасности.

Сетевой вариант Secret Net может быть успешно развернут в сложной доменной сети с большим количеством филиалов и удаленных офисов. При этом можно выстроить сервера безопасности с иерархией подчиненности.

16.2.5 Система централизованного управления

В качестве хранилища информации в системе централизованного управления используется Active Directory (AD). Для нужд централизованного управления Secret Net 6 схема Active Directory расширяется — создаются новые объекты и изменяются параметры существующих.

Для выполнения этих действий используется специальный модуль изменения схемы AD, который устанавливается и запускается на контроллере домена при установке системы централизованного управления. Для приведения параметров работы защитных средств компьютера в соответствие настройкам безопасности Secret Net 6, задаваемым с помощью групповых политик, используется агент Secret Net 6, установленный на каждом сервере или рабочей станции защищаемой сети.

Столь тесная интеграция Системы Управления с Active Directory позволяет легко использовать Secret Net 6 для организации защиты сети, использующей многодоменную структуру. Построение защитной системы сети, использующей многодоменную структуру, на основе выделенного сервера безопасности, как это

было в системах защиты предыдущего поколения, имело ряд существенных недостатков. Постоянно возникающие проблемы синхронизации данных между контроллером домена и сервером безопасности, завышенные требования к аппаратной части сервера безопасности – всё это значительно затрудняло централизованное управление безопасностью информационной системы. В Secret Net 6 эти проблемы принципиально отсутствуют.

16.2.6 Оперативный мониторинг и аудит

В Secret Net 6 предусмотрена функция оперативного мониторинга и аудита безопасности информационной системы предприятия, которая позволяет решать такие задачи, как:

- Оперативный контроль состояния автоматизированной системы предприятия (получение информация о состоянии рабочих станций и о работающих на них пользователях).
- Централизованный сбор журналов с возможностью оперативного просмотра в любой момент времени, а также хранение и архивирование журналов.
- Оповещение администратора о событиях НСД в режиме реального времени.
- Оперативное реагирование на события НСД — выключение, перезагрузка или блокировка контролируемых компьютеров.
- Ведение журнала НСД.
- Система Оперативного управления имеет свою базу данных, в которой хранится вся информация, связанная с работой сервера по обеспечению взаимодействия компонентов, а также журналы, поступающие от агентов. В качестве базы данных используется СУБД Oracle 9i, 10g Express, 11g.

16.2.7 Мониторинг

Программа мониторинга устанавливается на рабочем месте администратора оперативного управления — сотрудника, уполномоченного контролировать и оперативно корректировать состояние защищаемых компьютеров в режиме реального времени.

С помощью программы мониторинга администратор может управлять сбором журналов с рабочих станций. Предусмотрено два варианта. Первый - сервер оперативного управления собирает журналы по команде администратора. Второй - администратор составляет расписание и передает его серверу, далее сервер собирает журналы в соответствии с этим расписанием.

Также предусмотрена возможность создать удобный для администратора вид представления сети – т.н. "срез" (например, по отделам, по территориальному размещению и т.п.), в случае крупной распределённой сети, делегировать другим администраторам выделенные им для управления сегменты сети.

16.2.8 Аудит

В системе Secret Net 6 для проведения аудита используются 4 журнала, три из которых – штатные журналы ОС и один хранит сведения событий, происходящих в Secret Net 6. Журналы ведутся на каждом защищаемом компьютере сети и хранятся в его локальной базе данных. Сбор журналов осуществляется по команде аудитора или по расписанию.

Программа работы с журналами позволяет аудитору просматривать записи журналов и тем самым отслеживать действия пользователей, связанные с безопасностью автоматизированной информационной системы предприятия.

В журналах предусмотрена удобная система фильтрации по различным критериям, которая значительно упрощает работу, связанную с поиском и анализом событий.

С помощью программы работы с журналами аудитор может выдавать команды серверу на архивацию журналов, а также на восстановление журналов из архива.

Предусмотрена возможность просмотра архивов, а также сохранения журнала в файл для последующей передачи и анализа записей вне системы Secret Net 6.

16.3 Средство доверенной загрузки электронный замок "Соболь"

В качестве средства доверенной загрузки выбран электронный замок "Соболь", обладающий следующими возможностями:

- Аутентификация пользователей;
- Блокировка загрузки ОС со съемных носителей;
- Контроль целостности программной среды;
- Контроль целостности системного реестра Windows;
- Контроль конфигурации компьютера (PCI-устройств, ACPI, SMBIOS);
- Сторожевой таймер;
- Регистрация попыток доступа к ПЭВМ;

16.4 Межсетевой экран

Межсетевая защита информации, разделение сетей по категориям обрабатываемой информации и функциональному назначению осуществляется с использованием следующего оборудования:

- Межсетевой экран Cisco 3845;
- Сертифицированный межсетевой экран АПКШ "Континент" IPC-100;

16.4.1 Межсетевой экран Cisco 3845

Назначение: Подключение к сети Интернет, разбиение сетей по функциональному назначени.

Для межсетевого экрана, помимо стандартных параметров мониторинга оборудования, осуществляется мониторинг утилизации каналов связи по протоколамii согласно нижеследующей таблицы:

Приложения	Протоколы	% канала
Удаленные МИС и учетные системы: терминальный доступ	RDP	10%
Удаленные МИС и учетные системы: web-клиент	HTTP	15%
АРМ удаленных систем(GUI-клиенты)	протоколы используемые Oracle, MS-SQL, Cache и др.	10%
Почта, офисные приложения	протоколы используемые в Exchange, а также SMTP,IMAP,HTTP и т.п.	10%
Обмен данными PACS	DICOM, XML	5%
Обмен данными через файлы,СУБД, web-сервисы	CIFS,HTTP протоколы используемые Oracle, MS-SQL, Cache и т.п.	15%
IP-фония, ВКС, телемедицина	SIP,RTP,H.323 и др.	10%
Служебный и управляюший трафик	Netbios,DNS,SNMP,ICMP,LDAP и др.	2%
Резерв		23%

При превышении допустимого процента утилизации канала производится дополнительный анализ трафика

16.4.2 Сертифицированный межсетевой экран АПКШ "Континент"

Назначение: разбиение имеющихся сетей по функциональному назначению сертифицированным межсетевым экраном, позволяющим защищать персональные данных первой категории.

Рассматривались следующие "железные" межсетевые экраны, сертифицированные для защиты информационных систем персональных данных до К1 включительно.

- АПКШ "Континент-IPC100"
- АПКШ "Континент-IPC400"
- АПКШ "Континент-IPC1000"

Сравнительная таблица возможностей рассматриваемых МСЭ

Характеристика	Континент IPC-100	Континент IPC-400	Континент IPC-1000
Форм-фактор	1U	1U rack	1U rack
Пропускная способность VPN	250 Мбит/с	450 Мбит/с	800 Мбит/с
Пропускная способность МЭ	400 Мбит/с	600 Мбит/с	1 Гбит/с
Количество, тип сетевых интерфейсов	6x Ethernet 10/100/1000	4x Ethernet 10/100/1000	6x Ethernet 10/100/1000
Наличие оптических интерфейсов	2x SFP оптический	нет	нет
Поддержка протоколов динамической маршрутизации	OSPF	OSPF	OSPF
Кластер высокой доступности (горячее резервирование)	Да (активно-пассивный кластер)	Да (активно-пассивный кластер)	Да (активно-пассивный кластер)
Количество абонентов Континент АП в сети с одним СД	250	500	1000

Поддержка технологии Statefulinspection	да	да	да
Количество КШ в сети с одним ЦУС	До 500	До 1000	До 1000
Количество одновременных открытых сессий (TCP)	Неограниченно	Неограниченно	Неограниченно
Рекомендуемое количество хостов защищаемой сети	20-250	250-400	более 400
Приоритезация трафика	да	да	да
Резервирование гарантированной полосы пропускания за определенными сервисами	да	да	да
Поддержка VLAN (IEEE802.1Q)	да (254)	да (65000)	да (65000)
Порт RS232 для подключения Dial-UP модема	да	нет	нет
Интеллектуальное управление ИБП (UPS)	да	да	да
Поддержка SNMP	да	да	да
Поддержка VoIP	да	да	да
Интеграция с системами IPS/ IDS	да	да	да

Поддержка технологии NAT/ PAT	да	да	да
Удаленное обновление ПО криптошлюзов	да	да	да
Блок питания	1x 270W	1x 650W	2x 650W с "горячей" заменой
Работа в необслуживаемом режиме 24x7	да	да	да
Среднее время наработки на отказ (MTBF)	40 000 часов	10 000 часов	10 000 часов
Стоимость	135 000 рублей	465 000 рублей	660 000 рублей

Исходя из сравнительной таблицы характеристик и стоимости оборудования выбран IPC-100.

Для подключения рентген аппаратов из зоны Wi-Fi будет использоваться Континент АП.

Для обеспечения резерва на случай выхода из строя приобретено 2 шт и настроен отказоустойчивый кластер.

В перспективе построения защищенной телекоммуникационной сети между учреждениями здравоохранения может использоваться данный МСЭ.

Для выделения ДМЗ выбран Cisco 3845.

Для организации защищенного канала связи между сервисами организации и рентген аппаратами, мобильными пользователями, компьютером механика приобретен ЦУКС.

Для межсетевого экрана, помимо стандартных параметров мониторинга оборудования, осуществляется мониторинг утилизации каналов связи по протоколам, аналогично маршрутизатору Cisco 3845.

16.4.3 Антивирусная защита

Антивирусная защита обеспечивается антивирусом Касперского, функционирует и управляется с соответствующего сервера.

16.4.4 Система контроля доступа

Система контроля доступа в помещения организации

16.4.5 Соответствие стандартам

В качестве программного обеспечения, которое позволит провести внутреннюю экспертизу создаваемой инфраструктуры, контролировать ее этапы исполнения выбран программный продукт "Код Безопасности: Инвентаризация", который позволяет:

- Провести автоматизированную инвентаризацию установленного программного и аппаратного обеспечения;
- Отслеживать изменения в установленном/используемом программном и аппаратном обеспечении;
- Обнаружить ПО запрещенное регламентом (например – игры, средства общения, всевозможные музыкальные и видео проигрыватели) или постороннее ПО, которое не относится к выполнению служебных обязанностей;
- Построить реестр программного обеспечения, которое используется в организации;
- Вести учёт закупленных лицензий;
- Формировать отчёты о проделанной работе;

В результате использование ПО"Код Безопасности: Инвентаризация" поможет:

- Оптимизировать инвестиции в IT-инфраструктуру;
- Соответствовать законодательным, отраслевым и корпоративным требованиям к программному обеспечению (Стандарт Банка России, Стандарт ISO 27001,

Стандарт PCI DSS в области мониторинга, установки и обновления специальных программ и сервисов);

- Осуществить контроль за наличием трансляторов и отладчиков в корпоративной сети (требование ФСТЭК при построении ИСПДн);
- Снизить бизнес риски, за счет получения достоверной информации о программном обеспечении в сети компании;
- Проводить регулярный аудит программного и аппаратного обеспечения;

ПО представлено следующими компонентами:

- Серверная часть;
- База данных;
- Программа управления;
- Сервер отчетов;
- Агент;

Серверная часть и программа управления установлены на виртуальную машину с

операционной системой Microsoft Windows 2008 R2 Standard. База данных располагается централизованном сервере баз данных SQL. В качестве сервера отчетов используется Microsoft SQL Reporting Services.

Агент устанавливается на все персональные компьютеры в организации, при наличии возможности, с использованием политик Active Directory.

17 АТС

Для организации внутренней телефонной связи используется АТС.

Городские линии подводятся по 50-ти парному кабелю и посредством sip телефонии. Подключение sip телефонии производится с использованием межсетевого экрана Cisco 3845.

С целью сокращения расходов на междугороднюю связь осуществляется связь между АТС организации и АТС других ЛПУ по sip протоколу.

18 Обмен данными со сторонними организациями

Обмен производить в pdf формате, rtf. Данные регламенты должны быть предложены создаваемым центром обработки данных.

19 Центр обработки данных

Подавляющее большинство сервисов, описанных в настоящем документе, следует реализовывать в рамках создаваемого центра обработки данных (МИАЦ). Положительные стороны такого решения:

- Более оптимальное вложение инвестиций, экономия финансовых и трудовых ресурсов. Для реализации данных сервисов нет необходимости в приобретении серверного оборудования (или значительно уменьшается в нем потребность), программного обеспечения и устанавливать в каждом ЛПУ. Установка, настройка и дальнейшее сопровождение программного обеспечения будет осуществляться централизованно, более качественно и работать сразу на всю область. Обязательное условие: привлечение специалистов высокой квалификации или передача на аутсорсинг подрядной организации, имеющей таких специалистов. Не все ЛПУ области силами собственных специалистов смогут реализовать данные сервисы на должном уровне. Причем в список централизованных сервисов должны попасть не только медицинские и "экономические, кадровые, бухгалтерские" информационные системы, а также и структура каталогов пользователей по всем ЛПУ, и электронная почта, системы совместной работы и управления проектами, и другие сервисы, описанные в настоящем документе.
- Использование свободного программного обеспечения (СПО). Распоряжение правительства от 17 декабря 2010 г. №2299-р "О плане перехода на использование СПО", хотя и не затрагивает Департамент здравоохранения и подчиненные структуры, но в перспективе лучше строить собственную IT инфраструктуру с использованием СПО. Также нельзя исключать, что в 2015 году (плюс – минус несколько лет) выйдет распоряжение администрации области о переводе областных учреждений на использование СПО. Здесь и экономия финансовых средств на приобретении СПО и лицензий к нему (не всё СПО бесплатное), и более высокая лицензионная чистота использования программного обеспечения, и более высокая надежность решений. Реализовать собственными силами ЛПУ промышленные решения вряд ли получится, поскольку трудозатраты при настройке linux решений гораздо выше, чем windows решений (также имеют значение привычки человека, как пользователя, так и IT специалиста).
- Сохранность информации. Обеспечить резервное копирование информации на местах (особенно в районах области), гораздо сложнее: нет необходимого оборудования и персонала. В рамках центра обработки данных (если он "строится" в соответствии с международными нормами, ГОСТ`ами, СанПиН`ами) это предусматривается "по умолчанию". Это и резервное энергоснабжение, и возможность использования высокотехнологичного оборудования и программного обеспечения. На местах на должном уровне не хватит средств реализовать это на должном уровне.
- Защита информации. Разработанные организационными мерами приказы, регламенты по системе защиты информации, будут гораздо более тщательно проработаны с привлечением экспертов в этой области, контролирующих структур (ФСБ, ФАПСИ, РосКомНадзор, Россвязь) и исполняться(!).

У любого решения есть отрицательные стороны:

- Централизация работ по информатизации здравоохранения приведет к сокращению рабочих мест обслуживающего персонала ЛПУ, и как следствие (если объемы обслуживаемого населения не изменились) увеличению оплаты труда медицинских работников.
- Необходимо создавать высококвалифицированную службу поддержки пользователей по электронной почте и телефону (если не реализовать ip телефонию между ЛПУ, возрастут расходы на междугороднюю связь).
- Организации, которые не согласятся на использование ресурсов, предложенных центром обработки данных. Необходимо налаживать связи между их и нашим программным обеспечением, прорабатывать регламенты и форматы обмена информацией. По состоянию на сегодня, данные регламенты, форматы разрабатываются на уровне либо области, либо Москвы, в зависимости от структуры подчиненности организаций.
- Внесение любых изменений, доработок в сервисы будет осуществляться медленнее, поскольку эти изменения будут затрагивать всю область. Некорректные изменения также могут затронуть всех пользователей сервисов, поэтому необходимо выделить несколько учреждений в качестве пилотных проектов и проводить на них "испытания" доработок.

В зависимости от того, какие сервисы, как и когда будут реализовываться, данный документ может претерпеть значительные изменения.

