Правительство Санкт-Петербурга

Комитет по науке и высшей школе

Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение

«Политехнический колледж городского хозяйства»

**КУРСОВОЙ ПРОЕКТ**

**Администрирование КС областной больницы**

**ЛИСТ УТВЕРЖДЕНИЯ**

ПКГХ 09.02.06 СА-22-2. 062-22-ЛУ

|  |  |
| --- | --- |
|  | **Студент**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Краснов С.Е.)  **Руководитель**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Травкина Ю.И) |
|  |  |

Санкт-Петербург

2025

Содержание

[Введение 3](#_Toc198155375)

[1.Теоритическая часть 5](#_Toc198155376)

[Виртуализация и серверная инфраструктура 5](#_Toc198155377)

[Системное ПО и технологии 5](#_Toc198155378)

[Администрирование пользователей и данных 6](#_Toc198155379)

[Мониторинг и обслуживание 7](#_Toc198155380)

[2.Аналитическая часть 8](#_Toc198155381)

[Заключение 9](#_Toc198155382)

[Список использованных источников 10](#_Toc198155383)

[Приложения 11](#_Toc198155384)

# Введение

Эффективное функционирование компьютерных сетей в медицинских учреждениях является важнейшим условием обеспечения качества медицинских услуг, оперативности обработки информации и безопасности персональных данных пациентов. Однако, несмотря на наличие разработанных стандартов построения сетей, на практике в больницах России часто наблюдаются проблемы, связанные с недостаточной масштабируемостью, устаревшими техническими решениями, низкой отказоустойчивостью и недостаточной защитой информации. Это свидетельствует о противоречии между потребностью в современных высоконадёжных сетевых решениях и фактическим состоянием сетевой инфраструктуры медицинских организаций. Данная проблема требует глубокого изучения и поиска эффективных путей её решения, что обуславливает актуальность выбранной темы.

Целью данной курсовой проекта является эффективное администрирование компьютерной сети больницы с учетом особенностей её функционирования и современных требований к безопасности и надежности.

Для достижения поставленной цели были сформулированы следующие задачи:

* Проанализировать теоретические основы администрирования компьютерных сетей медицинских учреждений;
* Провести анализ состояния существующих компьютерных сетей в больницах;
* Развернуть и настроить виртуальные и физические сервера
* Обеспечить отказоустойчивость и резервное копирование.
* Управление пользователями и правами доступа.
* Обеспечить защиту данных.
* Настроить мониторинг сети и серверов
* Организовать удаленный доступ

Объектом исследования является процесс построения и администрирования компьютерной сети в медицинском учреждении.

Предметом исследования являются методы, средства и организационные подходы к обеспечению надёжной и безопасной работы компьютерной сети больницы.

Структура курсового проекта обусловлена необходимостью перехода от теоретического анализа к практическому проектированию: в первой части представлены теоретические основы построения сетей; во второй — проведен аналитический обзор состояния сети в медицинском учреждении и предложены практические решения на примере существующего корпуса больницы. Работа опирается как на общедоступные источники и стандарты, так и на личный практический опыт автора в процессе работы системным администратором в медицинском учреждении.

Практическая значимость исследования заключается в возможности использования предложенного проекта при построении или модернизации компьютерных сетей в медицинских учреждениях, что позволит повысить их надёжность, безопасность и эффективность функционирования.

# 1.Теоритическая часть

## Серверная инфраструктура и системное ПО

Серверы и их роли:

|  |  |  |
| --- | --- | --- |
| Имя | ОС | Роль |
| DC | WServer 2022 | Active Directory, DNS, DHCP |
| FILE | WServer 2022 | samba, медкарты, архивы, базы данных |
| WEB | Ubuntu Server | внутренний портал больницы, база знаний. |
| BACKUP | Ubuntu Server | Резервное копирование |
| MONITORING | Ubuntu Server | Мониторинг |
| VPN | pfSense/WServer 2022 | OpenVPN/WireGuard/DirectAccess/SSTP для удаленного доступа сотрудников |
|  |  |  |

Платформы виртуализации:

Hyper-V— для серверов на базе Windows.

KVM/QEMU— для Linux-серверов.

VMware ESXi/ProxMox— Хосты виртуализации.

Основное ПО для серверов:

Windows-серверы:

Active Directory - централизованная аутентификация.

Microsoft SQL Server- базы данных медсистем.

PowerShell - автоматизация задач.

FSRM - общего доступа

Linux-серверы:

Docker - развертывание приложений.

NGINX или Apache - веб сервера

PostgreSQL или MySQL – базы данных для веб-сервера

Ansible - управление конфигурациями и развертывание.

Zabbix - мониторинг

## Отказоустойчивость и резервное копирование

RAID 10 на файловых серверах.

Репликация баз данных MASTER-MASTER

Резервное копирование (Bacula, Veeam, RSync,crontab).

KeepAliveD для перенаправления трафика

## Администрирование пользователей и данных

Управление доступом:

Доменная структура Active Directory: Централизованное управление пользователями. Пример структуры

med.local:

OU=IT

OU=Врачи

Группа "Кардиология"

Группа "Хирургия"

Группа ""

Группа ""

Группа ""

OU=Серверы

OU=Гости

Групповые политики:

* Ограничение доступа к МИС (Медицинская Информационная Система).
* Запрет USB-накопителей для групп "Врачи".
* Обязательная смена пароля каждые 90 дней.

#TBD

DNS/DHCP

DNS: Интеграция с AD для именования узлов.

DHCP: Авто назначение IP с резервированием для критичных устройств.

## Хранение данных и безопасность

Безопасность:

* Group Policy для ограничения прав пользователей.
* Fail2Ban - защита SSH от брутфорса.
* LetsEncrypt - SSL-сертификаты для веб-сервисов.

Хранение данных:

* Медицинские данные хранить в зашифрованных контейнерах (Veracrypt).
* Резервные копии на сервере BACKUP

## Мониторинг и обслуживание

Zabbix — мониторинг загрузки CPU, RAM, дисков.

UptimeRobot — оповещения о простое сервисов.

Логирование через ELK-стек (Elasticsearch + Logstash + Kibana) для анализа логов.

Тестирование отказоустойчивости (отключение сервера DC-01, проверка переключения на DC-02).

Четкое разделение ролей серверов (Windows/Linux).

Автоматизация (PowerShell/Ansible).

Безопасность (GPO, шифрование, мониторинг).

Отказоустойчивость (виртуализация, RAID, репликация).

## Удаленный доступ

SHH для доступа к серверам

RDP для удаленной работы сотрудников

Удаленный доступ через зашифрованный канал связи

# 2.Аналитическая часть

#TBD

Разобрать настройку серверов

Сравнить Hyper-V и KVM.

Проанализировать риски

# Заключение

# Список использованных источников

# Приложения