**Федеральное государстве**

**Федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И   
ГОСУДАРСТВЕННОЙ СЛУЖБЫ   
при ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**НИЖЕГОРОДСКИЙ ИНСТИТУТ УПРАВЛЕНИЯ - ФИЛИАЛ РАНХиГС**

Cпециальность09.02.07 Информационные системы и программирование

**ОТЧЕТ**

**о прохождении практики**

УП.03.01. УЧЕБНОЙ ПРАКТИКИ

ПМ.03 РЕВЬЮИРОВАНИЕ ПРОГРАММНЫХ МОДУЛЕЙ

*Баринов Кирилл Ильич*

*(Ф.И.О. обучающегося)*

3 курс обучения учебная группа № Испб-033

Место прохождения практики Нижегородский институт управления - филиал ФГБОУ ВО РАНХиГС г. Нижний Новгород, ул. Пушкина, 10

Срок прохождения практики: с « 5 » декабря 2024 г. по « 11 » декабря 2024 г.

Руководители практики:

**Руководитель практики от института:**

Шиганова Марина Викторовна, преподаватель высшей категории

*(Ф.И.О., должность, подпись)*

**Руководитель практики от организации:**

Шиганова Марина Викторовна, преподаватель высшей категории

*(Ф.И.О., должность, подпись,* ***печать организации****)*

Отчет подготовлен \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(подпись обучающегося) (И.О. Фамилия*)

**Представитель отдела организации практики** **и трудоустройства** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(Ф.И.О., должность, подпись)*

г. Нижний Новгород , 2024 г.

**Содержание**

[Введение 3](#_Toc184693279)

[1 Определение характеристик персонального компьютера 5](#_Toc184693280)

[1.1 Определение технических характеристик ПК 5](#_Toc184693281)

[1.2 Определение характеристик ПО 10](#_Toc184693282)

[2 Рекомендации по использованию российских аналогов ПО 25](#_Toc184693283)

[2.1 Использование стационарных программ 25](#_Toc184693284)

[2.2 Разработать рекомендации по использованию онлайн версий - российских аналогов ПО. 26](#_Toc184693285)

[3 Установка и настройка систем контроля версий 28](#_Toc184693286)

[3.1 Установка системы контроля версий 28](#_Toc184693287)

[Заключение 32](#_Toc184693288)

[Список источников и литературы 33](#_Toc184693289)

### Введение

Учебная практика проходила в Колледже Нижегородского института управления – филиала РАНХиГС по адресу: г. Нижний Новгород, Советский район, ул. Пушкина, д.8 к. 214 с «05» декабря 2024г. по «11» декабря 2024г.

Учебная практика является неотъемлемой частью образовательного процесса, позволяя студентам не только закрепить теоретические знания, полученные в ходе обучения, но и приобрести практические навыки, которые необходимы для эффективной профессиональной деятельности. В рамках практики, проходившей в Колледже Нижегородского института управления - филиала РАНХиГС, была поставлена задача автоматизации и улучшения работы информационных систем. Одним из ключевых направлений этой работы стало внедрение системы удалённого администрирования, которая позволит эффективно управлять и контролировать работу компьютерных и сетевых систем предприятия.

Система удалённого администрирования представляет собой комплекс программных и аппаратных средств, которые позволяют администраторам ИТ-систем управлять компьютерами, серверами и другими устройствами без физического присутствия. Современные организации сталкиваются с проблемой управления большим количеством вычислительных ресурсов и с необходимостью обеспечения их стабильной работы, особенно если система распределена по нескольким офисам или производственным участкам. В таких случаях использование удалённого администрирования становится не только удобным, но и крайне необходимым.

Целью данного проекта является создание системы удалённого администрирования, которая обеспечит:

• Централизованное управление рабочими станциями и серверами;

• Удалённый доступ к устройствам для выполнения различных операций (установка обновлений, настройка программного обеспечения, мониторинг состояния);

• Эффективное решение проблем с минимальными временными затратами и без необходимости физического присутствия специалистов на месте.

Основные задачи, которые решались в ходе работы, включают:

1. Анализ существующих решений в области удалённого администрирования для определения наиболее подходящих инструментов и технологий.

2. Разработка и внедрение системы, которая будет отвечать требованиям безопасности, производительности и масштабируемости.

3. Тестирование системы для оценки её эффективности и стабильности в реальных условиях работы предприятия.

Удалённое администрирование позволило бы значительно повысить эффективность работы технической поддержки, ускорить решение проблем и снизить затраты на обслуживание информационной инфраструктуры. Внедрение такой системы помогает не только сэкономить время и ресурсы, но и улучшить безопасность, минимизируя риски, связанные с человеческим фактором, и улучшить контроль за состоянием всех аппаратных и программных компонентов.

Таким образом, данная учебная практика направлена на улучшение качества и надежности работы информационных систем предприятия, что, в свою очередь, поможет улучшить общую эффективность его функционирования и сократить затраты на техническое обслуживание.

### **1 Определение характеристик персонального компьютера**

### 1.1 **Определение технических характеристик ПК**

Определение технических характеристик ПК - это процесс сбора, анализа и описания параметров аппаратных компонентов компьютера, которые определяют его производительность, функциональность и возможности для выполнения различных задач.

Этот процесс помогает пользователю понять, какие компоненты установлены в компьютере, как они работают, насколько они совместимы между собой и способны ли обеспечить выполнение необходимых задач (например, офисной работы, игр, монтажа видео и т.д.).

**1. Процессор**

Модель: Intel® Core™ i5-10400 CPU @ 2.90GHz

Архитектура:

* + Процессор относится к линейке Comet Lake (10-е поколение Intel Core).
  + Построен на 14-нм техпроцессе, который обеспечивает баланс между производительностью и энергопотреблением.

Количество ядер и потоков:

* + 6 физических ядер и 12 потоков.
  + Поддержка технологии Hyper-Threading обеспечивает распределение задач между потоками для более эффективной многозадачности.

Тактовая частота:

* + Базовая частота - 2,90 ГГц.
  + В режиме Turbo Boost достигает до 4,30 ГГц, что полезно при выполнении ресурсоемких задач.

Кэш-память:

* + 12 МБ Intel Smart Cache, которая ускоряет доступ к часто используемым данным.

TDP (Thermal Design Power):

* + 65 Вт. Это низкое энергопотребление, что позволяет использовать процессор в системах с ограниченным охлаждением, таких как моноблоки.

**2. Материнская плата**

Материнская плата **ASRock B560M-HDV** - это современная модель форм-фактора Micro-ATX, которая предлагает базовый функционал для сборки производительных систем на платформе Intel 10-го и 11-го поколений. Она идеально подходит для офисных компьютеров, игровых систем начального уровня и универсальных домашних ПК.

Модель: ASRock B560M-HDV

Чипсет Intel B560:

* + Среднеуровневый набор системной логики, который поддерживает процессоры Intel 10-го и 11-го поколения.
  + Поддержка разгона оперативной памяти (функция доступна на данной плате).

Слоты оперативной памяти:

* + 2 слота DDR4, максимальный объем - 64 ГБ.
  + Частота памяти до 5000 МГц (в режиме разгона).

Накопители:

* Поддержка M.2 SSD
  + Один слот Hyper M.2 для PCIe 4.0 x4.
  + Один слот Ultra M.2 для PCIe 3.0 x4 и SATA.
  + 4 порта SATA3 для подключения HDD и SSD.

Графические интерфейсы:

* + HDMI 2.0 с поддержкой 4K-разрешения при 60 Гц.
  + DVI-D и D-Sub для подключения мониторов.

Слоты расширения:

* + 1 слот PCIe 4.0 x16 для видеокарты.
  + 2 слота PCIe 3.0 x1 для дополнительных карт.

**3. Система охлаждения процессора**

Тип: Стандартный боксовый кулер Intel

Характеристики:

* Радиатор из алюминия.
* Встроенный вентилятор диаметром 92 мм.
* Скорость вращения вентилятора: до 2000 об/мин.
* Поддержка PWM (регулировка скорости вращения в зависимости от температуры).

Описание и применение:

Боксовый кулер обеспечивает базовое охлаждение процессора при стандартных нагрузках. Он эффективен в режиме простоя или при выполнении лёгких задач. Однако при высоких нагрузках температура процессора может достигать верхних пределов допустимого диапазона, что может повлиять на производительность.

**4. Видеокарта**

**Intel UHD Graphics 630**‑ интегрированная видеокарта, встроенная в процессоры Intel Core 8–10-го поколений. Предназначена для повседневных задач: офисная работа, мультимедиа, интернет-серфинг и запуск лёгких игр.

Модель: Intel® UHD Graphics 630

Характеристики:

* Тип: Встроенная графика
* Базовая частота графического ядра: 350 МГц
* Максимальная динамическая частота: 1,10 ГГц
* Поддержка DirectX: 12
* Поддержка OpenGL: 4.5
* Максимальное разрешение (HDMI 1.4): 4096x2304 @ 30Hz
* Максимальное разрешение (DP): 4096x2304 @ 60Hz
* Максимальное разрешение (eDP - встроенный дисплей): 4096

**Intel UHD Graphics 630 -**экономичное решение для базовых нужд без необходимости в дискретной видеокарте.

**5. Оперативная память**

Модель: Hynix/Hyundai DDR3 2x4 ГБ

Технические характеристики:

* Тип памяти: DDR3 SDRAM
* Частота: 1600 МГц.
* Пропускная способность: до 12,8 ГБ/с.
* Энергопотребление: 1,5 В.

Описание и недостатки:

Оперативная память DDR3 устарела и уступает DDR4 по скорости передачи данных и энергоэффективности. Объем в 8 ГБ достаточен для базовых задач, таких как работа в браузере, офисных приложениях и просмотр мультимедиа. Однако для современных игр, работы с большими массивами данных или виртуальных машин 8 ГБ может быть недостаточно.

Рекомендации:

* Увеличить объем до 16 ГБ (если материнская плата поддерживает).
* Перейти на модули DDR4 для повышения производительности.

**6. Устройство хранения данных**

Модель: Patriot Burst Elite 240GB

Преимущества:

* Высокая скорость работы, характерная для SSD: загрузка системы и приложений занимает считанные секунды.
* Низкое энергопотребление и отсутствие шума благодаря отсутствию механических частей.
* Компактность позволяет устанавливать его в любые системы, включая моноблоки.

Недостатки:

* Небольшой объем памяти (240 ГБ) может быстро закончиться при установке крупных приложений или игр.

**7. Корпус**  
Моноблок с компактным и минималистичным дизайном, включающий встроенный дисплей. Такой форм-фактор отлично подходит для экономии пространства, но ограничивает возможности апгрейда.

**8. Блок питания** **CHIEFTEC SFX-250VS**  
Мощность 250 Вт достаточна для работы текущей конфигурации. Однако при модернизации (например, добавлении видеокарты) потребуется блок питания большей мощности.

Основные характеристики:

Мощность:

* + Номинальная мощность: 250 Вт.
  + Максимальная мощность (кратковременно): 300 Вт.

Форм-фактор:

* + SFX - компактный размер, подходящий для небольших корпусов и моноблоков.

Эффективность:

* + Коэффициент полезного действия (КПД): до 85%.
  + Соответствует стандарту 80 PLUS Bronze, что обеспечивает высокую энергоэффективность.

Входное напряжение:

* + Диапазон: 230 В.

Линии питания:

* + +3.3 В: 13 А.
  + +5 В: 14 А.
  + +12 В1: 13 А.
  + +12 В2: 13 А.
  + -12 В: 0.3 А.

Система охлаждения:

* + Встроенный 80-мм вентилятор с термоконтролем, обеспечивающий эффективное охлаждение и низкий уровень шума.

Защита:

* + От перенапряжения (OVP).
  + От пониженного напряжения (UVP).
  + От перегрузки по мощности (OPP).
  + От короткого замыкания (SCP).

Сертификация и стандарты:

* + Соответствует стандартам CB, CE, TUV, FC.
  + Соответствие директиве RoHS (ограничение содержания вредных веществ).

Особенности:

* Компактный форм-фактор SFX позволяет использовать блок питания в небольших корпусах и моноблоках.
* Высокая энергоэффективность снижает энергопотребление и тепловыделение.
* Наличие нескольких линий +12 В обеспечивает стабильное питание для различных компонентов системы.
* Многоуровневая система защиты гарантирует безопасность работы устройства.

Совместимость со сборкой:

Блок питания CHIEFTEC SFX-250VS обеспечивает достаточную мощность и стабильное напряжение для следующих компонентов вашей системы:

* Процессор: Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz.
* Материнская плата: B560M-HDV.
* Оперативная память: DDR3 2x4GB Hynix/Hyundai.
* Видеокарта: Intel(R) UHD Graphics 630 (интегрированная).
* Устройство хранения данных: Patriot Burst Elite 240GB.

Учитывая энергопотребление указанных компонентов, блок питания CHIEFTEC SFX-250VS обеспечит надежную и эффективную работу вашей системы.

### **1.2 Определение характеристик ПО**

**1. Управление компьютерными ресурсами организации**

Управление компьютерными ресурсами с помощью систем удаленного администрирования (СУА) представляет собой комплекс мероприятий, направленных на обеспечение стабильной работы IT-инфраструктуры организации. Это включает в себя мониторинг состояния оборудования, настройку программного обеспечения, управление пользователями и автоматизацию задач.

Реализация управления ресурсами:

1. **Удаленный доступ к устройствам:**  
   СУА обеспечивает администратору возможность подключаться к любому устройству организации. Это включает:
   * Рабочие станции сотрудников: Управление настройками, диагностика и обновления.
   * Серверы и сетевое оборудование: Доступ к настройкам серверов, маршрутизаторов и коммутаторов.
   * Протоколы и технологии: Использование RDP, SSH, или веб-интерфейсов для взаимодействия с устройствами.
2. Мониторинг оборудования в реальном времени:
   * Отслеживание загрузки процессора, оперативной памяти, температуры компонентов.
   * Уведомления о сбоях или критических состояниях оборудования через электронную почту, SMS или push-уведомления.
   * Визуализация данных на панели управления (графики, диаграммы).
3. Централизованное управление программным обеспечением:
   * Удаленная установка, обновление и удаление программ.
   * Проверка соответствия установленного ПО требованиям безопасности.
   * Управление лицензиями и отслеживание их срока действия.

**Особенности и преимущества управления ресурсами через СУА:**

1. Масштабируемость:
   * Подходит для компаний с 10, 100 или 1000+ устройств.
   * Простая интеграция новых устройств в существующую инфраструктуру.
2. Экономия времени:
   * Администратор может выполнять задачи одновременно на нескольких устройствах.
   * Удаленная диагностика и ремонт сокращают время простоя.
3. Повышение безопасности:
   * Контроль всех подключений и действий через зашифрованные каналы (SSL/TLS).
   * Ограничение доступа по IP-адресам или географическим зонам.

Примеры применения:

1. В крупных корпорациях:  
   Управление тысячами рабочих станций, серверов и сетевых устройств из единого центра.
2. В образовательных учреждениях:  
   Контроль компьютерных классов, серверов и онлайн-сервисов (например, Moodle).
3. В медицинских учреждениях:  
   Мониторинг и управление IT-ресурсами, используемыми для обработки данных пациентов и управления медицинским оборудованием.
4. В производственных предприятиях:  
   Удаленное управление серверами, автоматизированными станками, сетями IT.

Системы удаленного администрирования предоставляют организациям гибкие, масштабируемые и безопасные инструменты для управления ресурсами, значительно упрощая работу IT-отделов.

**2. Обеспечение пользователя инструментами для извлечения пользы из ресурсов.**

Системы удаленного администрирования (СУА) обеспечивают пользователей разнообразным набором инструментов для оптимального взаимодействия с компьютерными ресурсами организации. Эти инструменты охватывают управление, мониторинг, автоматизацию и интеграцию, помогая пользователям эффективно выполнять свои обязанности. Ниже рассмотрены ключевые аспекты более подробно.

1. Доступность и упрощение работы с ресурсами

* Централизованный доступ:  
  Пользователь получает доступ ко всем необходимым приложениям и данным через единую панель управления. Это упрощает поиск информации и ускоряет выполнение задач.
* Универсальность доступа:  
  Возможность работы с ресурса через ПК, ноутбук, планшет или смартфон с сохранением полного набора функций.
* Кроссплатформенность:  
  Поддержка различных операционных систем (Windows, macOS, Linux) и мобильных платформ (iOS, Android) позволяет работать на любых устройствах.

2. Расширенные инструменты для работы

* Инструменты диагностики и мониторинга:
  + Отслеживание загрузки системы, сетевой активности и использования памяти в реальном времени.
  + Диагностика состояния оборудования и программного обеспечения с автоматическими уведомлениями о возможных сбоях.
  + Мониторинг производительности приложений и сети.
* Системы контроля доступа:
  + Ограничение доступа к данным и ресурсам в зависимости от роли пользователя в организации.
  + Настройка различных уровней доступа, включая гостевой доступ и административный режим.
* Интеграция со сторонними инструментами:
  + Возможность подключения к облачным сервисам (например, Google Drive, Dropbox) и корпоративным приложениям (например, SAP, Jira).
  + Поддержка интеграции с базами данных, системами управления проектами и аналитическими платформами.

3. Обеспечение безопасности данных

* Защищенные каналы связи:  
  Передача данных через зашифрованные протоколы (VPN, SSH, SSL/TLS) для предотвращения перехвата информации.
* Управление учетными записями:
  + Принудительная смена паролей, настройка политики сложности паролей.
  + Использование многофакторной аутентификации (MFA).
* Антивирусная защита и контроль угроз:
  + Интеграция с решениями для обнаружения вредоносного ПО и защиты от фишинга.
  + Мониторинг подозрительных действий пользователей и автоматическая блокировка угроз.

**Выполнение роли посредника между организациями и хранимой информацией.**

Система удаленного администрирования (СУА) выступает связующим звеном между пользователями, организациями и хранимыми данными, обеспечивая эффективное управление информацией, доступность данных и их защиту.

1. Централизация данных и их управление

Единая база данных:  
СУА позволяет хранить всю информацию в едином месте (на локальном сервере или в облаке), что обеспечивает согласованность данных и уменьшает вероятность их дублирования. Все пользователи получают доступ к актуальной версии информации.

Мониторинг и учет операций:  
СУА отслеживает все действия, связанные с доступом и изменением информации. Это помогает поддерживать прозрачность процессов и проводить аудит данных.

2. Обеспечение безопасного взаимодействия

Управление доступом:

* Пользователи получают доступ к данным в зависимости от их ролей и полномочий. Например, сотрудники бухгалтерии видят только финансовые документы, а ИТ-специалисты управляют только технической частью.

Многофакторная аутентификация (MFA):  
СУА использует современные методы аутентификации, включая одноразовые пароли (OTP), биометрическую идентификацию и токены безопасности. Это предотвращает несанкционированный доступ к данным.

Шифрование данных:

* Все данные, хранимые на серверах или передаваемые между устройствами, шифруются с использованием протоколов SSL/TLS. Это защищает информацию даже в случае ее перехвата.

**Упрощение взаимодействия между подразделениями и внешними партнерами**

Обмен данными в реальном времени:  
СУА позволяет организациям обмениваться данными с филиалами, клиентами и партнерами без задержек. Например, складские данные обновляются сразу после изменения количества товаров.

Создание ограниченного доступа для партнеров:

* Партнерские организации могут получать ограниченный доступ к определенным данным (например, статусу заказов или поставок) через защищенные интерфейсы.

Интеграция через API:  
СУА часто поддерживает программные интерфейсы (API), позволяющие подключать сторонние приложения, такие как системы аналитики или платформы электронной торговли.

**Логика работы программного обеспечения (на примере системы удаленного администрирования)**

Система удаленного администрирования (СУА) функционирует, используя последовательные процессы для выполнения своих задач. Основная цель программного обеспечения — обеспечить управление ресурсами, доступ к данным и контроль за действиями пользователей в режиме реального времени. Логика работы СУА делится на несколько ключевых этапов:

1. Авторизация и аутентификация

Перед использованием системы пользователь проходит процесс проверки личности:

1. Вход в систему:
   * Пользователь вводит учетные данные (логин и пароль).
   * Система сравнивает введенные данные с базой, чтобы подтвердить их корректность.
2. Дополнительные уровни защиты:
   * Использование многофакторной аутентификации (например, одноразового пароля или подтверждения через мобильное приложение).
3. Назначение ролей:
   * После успешной аутентификации пользователю назначаются права доступа на основе его роли в системе (администратор, пользователь, наблюдатель).

2. Доступ к ресурсам

СУА предоставляет доступ только к тем ресурсам, которые определены политиками безопасности:

* Идентификация узлов: Система сканирует сеть и определяет подключенные устройства (серверы, рабочие станции, принтеры и т. д.).

3. Мониторинг и контроль

Программное обеспечение обеспечивает постоянное наблюдение за состоянием системы:

1. Сбор данных:
   * Система получает данные о загрузке процессора, памяти, сети и других ресурсов.
   * Устройства отправляют логи событий (например, попытки доступа, ошибки системы, обновления).
2. Анализ информации:
   * Система анализирует полученные данные и выявляет потенциальные проблемы (перегрузка сети, сбои оборудования).
3. Уведомления и отчеты:
   * В случае аномалий система отправляет уведомления администраторам через интерфейс, email или SMS.

4. Выполнение команд и управление

СУА позволяет администраторам удаленно управлять устройствами:

1. Передача команд:
   * Команды передаются через защищенные каналы связи (например, через протоколы RDP, SSH или VPN).
   * Администратор может перезапустить устройство, обновить ПО или изменить конфигурацию системы.
2. Реализация задач:
   * Задачи выполняются устройством, а результат отправляется обратно в систему администрирования.

3. Хранение и защита данных

Программное обеспечение организует работу с данными следующим образом:

1. Централизация данных:
   * Все конфигурации, журналы и отчеты хранятся в центральной базе данных.
2. Резервное копирование:
   * Система автоматически создает резервные копии для защиты от потерь.
3. Шифрование:
   * Данные, хранящиеся в системе или передаваемые по сети, защищены шифрованием (например, AES-256).

**Функциональная пригодность**

Это характеристика качества, которая определяет способность программного обеспечения выполнять все функции, заявленные в требованиях, и обеспечивать удовлетворение потребностей пользователей.

Для системы удаленного администрирования функциональная пригодность может быть оценена по следующим критериям:

1. Соответствие функциональным требованиям

Каждая система удаленного администрирования имеет перечень функций, которые должны быть реализованы. Эти функции могут включать:

* Удаленное управление: возможность управлять сервером или рабочей станцией через сеть, запускать и останавливать приложения, изменять настройки.
* Мониторинг состояния: возможность отслеживать состояние устройств, серверов, служб, ресурсов системы (например, процессора, памяти, сети).
* Конфигурация и настройка системы: возможность настроить параметры системы, обновления и модификации программного обеспечения.
* Управление пользователями и правами доступа: возможность добавлять, удалять пользователей, настраивать их права доступа, разграничивать уровни доступа.

2. Покрытие требований

Процесс тестирования функциональной пригодности включает в себя проверку, насколько точно система выполняет все заявленные функции. Это может включать:

* Проверку каждого элемента функциональных требований.
* Проверку правильности обработки исключений, ошибок и непредвиденных ситуаций.
* Тестирование в реальных условиях эксплуатации (например, с реальными пользователями и реальными нагрузками).

3. Производительность функций

Важной частью функциональной пригодности является не только наличие нужных функций, но и их производительность. Например:

* Как эффективно выполняются операции управления в условиях высокой нагрузки (многозадачность, параллельная работа с несколькими устройствами).
* Насколько система справляется с большим объемом данных и интенсивными операциями (например, при удаленном доступе к большому количеству серверов или виртуальных машин).

**Уровень производительности системы удаленного администрирования**

Это характеристика качества, которая определяет, насколько эффективно и быстро система выполняет свои функции при различных условиях эксплуатации.

Оценка производительности системы удаленного администрирования включает следующие ключевые аспекты:

1. Время отклика

Одним из главных показателей производительности является время отклика системы на действия пользователя. Для системы удаленного администрирования это включает:

* Время отклика на запросы мониторинга: сколько времени потребуется для получения информации о состоянии системы (например, процессора, памяти, диска, сети).
* Отображение интерфейса: время, которое требуется для обновления данных в графическом интерфейсе, отображения статистики и текущего состояния системы.

Для оценки этого показателя важно проводить тесты с различными сценариями работы, например:

* Подключение и выполнение команды на сервере с высокой загрузкой.

2. Пропускная способность

Пропускная способность системы удаленного администрирования оценивается по количеству данных, которые система может обработать за определенное время. Важно оценить:

* Пропускная способность канала связи: например, сколько данных передается между клиентом и сервером за единицу времени.
* Скорость передачи команд и данных: как быстро система может передать информацию о состоянии сервера, конфигурации или любых других данных.

Для тестирования пропускной способности необходимо оценить систему при разных типах соединений (локальная сеть, VPN, интернет), а также при разных объемах передаваемой информации.

**Совместимость системы удаленного администрирования**

Совместимость с аппаратным обеспечением

Оценка совместимости с аппаратным обеспечением включает в себя:

* Поддержка различных архитектур: система должна быть совместима с различными типами аппаратных архитектур, такими как x86, ARM и другие.
* Поддержка различных типов устройств: например, серверов, рабочих станций, маршрутизаторов, коммутаторов и других устройств, с которыми будет взаимодействовать система.
* Поддержка периферийных устройств: возможность работы с различными периферийными устройствами (например, принтерами, сканерами, USB-устройствами), если это необходимо для удаленного администрирования.

Тестирование аппаратной совместимости включает в себя проверку всех типов устройств, с которыми система должна работать, и оценку того, как она взаимодействует с ними.

Проверка совместимости с другими системами включает тестирование взаимодействия с внешними сервисами и приложениями, чтобы убедиться, что они могут корректно интегрироваться.

**Удобство использования (юзабилити) системы удаленного администрирования**

Это характеристика, которая определяет, насколько легко и удобно пользователям взаимодействовать с системой для выполнения своих задач. Оценка юзабилити включает в себя изучение того, насколько интерфейс системы интуитивно понятен, как быстро можно освоить систему и насколько эффективно она решает поставленные задачи.

Основные аспекты оценки удобства использования (юзабилити) системы удаленного администрирования:

1. Интуитивность интерфейса

Интерфейс системы должен быть понятным и легким для восприятия, чтобы пользователи могли быстро освоить основные функции. Это включает:

* Простота навигации: ясная структура меню и панелей инструментов, логичное распределение функций по разделам.
* Минимизация количества шагов для выполнения основных операций, таких как подключение к удаленному серверу, выполнение команд или мониторинг состояния системы.
* Единообразие интерфейса: одинаковый стиль элементов управления, таких как кнопки, формы, меню и т.д., на всех экранах системы.

Для оценки этого аспекта можно провести тестирование с реальными пользователями, не знакомыми с системой, и измерить, сколько времени им нужно, чтобы выполнить простую задачу (например, подключиться к серверу и выполнить базовую команду).

2. Обучаемость

Система должна быть достаточно простой для освоения, даже если пользователи не имеют глубоких технических знаний. Оценка обучаемости включает:

* Документация и обучающие материалы: наличие подробных инструкций, руководств пользователя, видеоуроков и FAQ.
* Встроенная помощь: контекстные подсказки, подсказки на экране или помощники, которые объясняют, как использовать различные функции.
* Поддержка новичков и опытных пользователей: система должна быть доступна как для начинающих администраторов, так и для более опытных пользователей, предлагая простые и расширенные функции в зависимости от уровня знаний.

Оценка обучаемости может включать анализ доступных обучающих материалов и тестирование времени, необходимого для освоения системы новичками.

**Оценка удобства использования системы удаленного администрирования**

Включает в себя тестирование интуитивности интерфейса, обучаемости, эффективности работы, качества обратной связи и удобства взаимодействия с пользователем. Важным аспектом является доступность обучающих материалов и возможность адаптации системы под потребности разных пользователей.

Защищённость системы удаленного администрирования - это способность системы обеспечивать защиту данных и ресурсов от несанкционированного доступа, утечек, повреждений, потерь и других угроз безопасности.

1. Контроль доступа

Контроль доступа - это основа безопасности системы. Он включает в себя механизмы, которые ограничивают доступ к системе только авторизованным пользователям и защищают систему от несанкционированного входа.

* Аутентификация: система должна поддерживать надёжные методы аутентификации пользователей. Это может быть:
* Пароли: с требованиями к сложности паролей (например, длина, использование спецсимволов и т.д.).
* Многофакторная аутентификация (MFA): использование нескольких факторов для подтверждения личности пользователя, таких как SMS-коды, биометрия (например, отпечатки пальцев, распознавание лиц), аппаратные токены.
* Авторизация: после успешной аутентификации система должна предоставлять доступ только к тем данным и функциям, которые соответствуют роли пользователя. Это может включать:

Оценка контроля доступа включает в себя анализ используемых методов аутентификации и авторизации, проверку настроек доступа и тестирование на уязвимости (например, попытки брутфорс-атак).

2. Шифрование данных

Шифрование является важной мерой для защиты данных от перехвата или несанкционированного доступа. Все передаваемые данные, а также данные, хранящиеся в системе, должны быть защищены.

* Шифрование данных в транзите: это защита данных, которые передаются через сеть (например, при удалённом подключении). Используемые протоколы должны обеспечивать надёжную защиту, такие как:
* Шифрование паролей: пароли и другие чувствительные данные должны храниться в зашифрованном виде, а не в открытом виде в базе данных.

Для проверки шифрования можно провести анализ протоколов передачи данных, тестирование на наличие уязвимостей в методах шифрования и оценку конфигурации системы на соответствие стандартам безопасности.

**Сопровождаемость системы удаленного администрирования**

Это способность системы поддерживать её работоспособность и актуальность в процессе эксплуатации с минимальными затратами времени и ресурсов. Этот аспект качества касается того, как легко система может быть обновлена, исправлена, поддержана в рабочем состоянии, а также как быстро можно устранять возникающие проблемы.

1. Документация

Качественная документация является основой сопровождения системы, так как она позволяет специалистам легко понять и поддерживать систему, устранять ошибки и реализовывать новые функции.

* Техническая документация: должна содержать подробные описания всех компонентов системы, их взаимодействий, конфигурации, архитектуры и возможностей для диагностики проблем.
* Пользовательская документация: должна быть доступной для администраторов, помогая им эффективно управлять системой, выполнять настройки и устранять возникающие проблемы.

2. Поддержка и обслуживание

Для обеспечения долгосрочной работы системы необходимо организовать эффективное обслуживание и поддержку.

* Обновления и патчи: система должна обеспечивать регулярные обновления для устранения уязвимостей, исправления ошибок и добавления новых функций.
* Обратная совместимость: при добавлении новых функций или обновлений система должна сохранять совместимость с предыдущими версиями, чтобы не возникало проблем при миграции или обновлении.
* Гибкость в исправлении ошибок: система должна позволять администратору быстро выявлять и исправлять ошибки в настройках, программных компонентах или конфигурации.

**Переносимость (мобильность) системы удалённого администрирования**

Это способность системы эффективно работать на различных аппаратных и программных платформах, а также её способность легко перемещаться или переноситься с одной среды в другую.

1. Совместимость с различными операционными системами

Система удалённого администрирования должна поддерживать работу на различных операционных системах, таких как:

* Windows: наличие клиента или сервера для удалённого администрирования, совместимого с версиями Windows.
* Linux/Unix: поддержка командных интерфейсов, удалённых соединений через SSH, возможности настройки и управления через терминал.
* macOS: поддержка взаимодействия с macOS, включая управление и мониторинг через клиентские приложения или консольные утилиты.

### **2 Рекомендации по использованию российских аналогов ПО**

### 2.1 **Использование стационарных программ**

Внедрение российских программных продуктов для систем удаленного администрирования важно в контексте повышения уровня информационной безопасности и соблюдения требований импортозамещения. Ниже представлены рекомендации по использованию отечественных стационарных программ для удаленного администрирования.

**1. Российские аналоги зарубежного ПО для удаленного администрирования**

Российский рынок предлагает множество решений, которые могут заменить зарубежные продукты (например, TeamViewer, AnyDesk или LogMeIn) для удаленного управления системами и сетями.

**2. Решения для удаленного доступа и управления:**

* **Рутокен СЦ**
  + Программное обеспечение для безопасного удаленного доступа, использующее российские криптографические алгоритмы.
  + Подходит для администрирования рабочих станций, серверов и других устройств.
  + Рекомендации: Использовать в организациях с высокими требованиями к безопасности данных.
* **Стахановец Администратор**
  + Инструмент для удаленного мониторинга и управления IT-инфраструктурой.
  + Включает функции удаленного доступа, мониторинга работы сотрудников, защиты данных.
  + Рекомендации: Подходит для предприятий с большим количеством рабочих мест.
* **MyOffice Access**
  + Система для безопасного доступа к рабочему столу и файлам через защищённое соединение.
  + Рекомендации: Использовать в средах, где требуется защищённый доступ к корпоративным данным.

**3** **Системы для управления IT-инфраструктурой:**

* **АдминTool**
  + Отечественный инструмент для управления IT-инфраструктурой, предоставляющий возможность удалённого администрирования серверов и рабочих станций.
  + Особенности: Централизованное управление, журналирование всех действий администратора.
  + Рекомендации: Подходит для малых и средних организаций.
* **Системный монитор СМ-3000**
  + Стационарное программное решение для удаленного управления и мониторинга сети.
  + Особенности: Анализ нагрузки на сеть, управление конфигурациями и диагностика оборудования.
  + Рекомендации: Рекомендуется для крупных организаций с распределенной IT-инфраструктурой.

### **2.2 Разработать рекомендации по использованию онлайн версий - российских аналогов ПО**.

Онлайн-версии программ для удаленного администрирования становятся все более популярными благодаря их доступности, минимальным требованиям к локальному оборудованию и возможности работы из любой точки с доступом к интернету. Российские аналоги таких систем способны обеспечить безопасность данных и соответствие требованиям локальных нормативов.

**1. Российские онлайн-сервисы для удаленного администрирования**

**1.1** **Облачные системы удаленного доступа**

* **RuDesktop Online**
  + Облачное решение для удаленного управления устройствами.
  + Особенности: Безопасное соединение через защищенные протоколы, поддержка многоплатформенности (доступ через веб-браузер).
  + Рекомендации: Использовать в организациях, где требуется оперативное подключение к нескольким устройствам.
* **Рутокен VPN Web**
  + Сервис для удаленной работы с использованием российских криптографических алгоритмов.
  + Особенности: Удобный интерфейс для настройки доступа, поддержка работы через интернет-браузеры.
  + Рекомендации: Подходит для работы с конфиденциальными данными.

**1.2** **Инструменты для совместной работы и администрирования**

* **MyOffice Professional Online**
  + Онлайн-платформа для организации удаленного доступа, совместной работы с документами и управления IT-инфраструктурой.
  + Особенности: Поддержка удаленного администрирования серверов и рабочих станций, интеграция с другими продуктами MyOffice.
  + Рекомендации: Использовать в корпоративной среде для объединения функций удаленного доступа и управления документами.
* **Ростелеком Контур**
  + Платформа для удаленной работы и администрирования с возможностью подключения к корпоративным сетям через облачный сервис.
  + Особенности: Централизованное управление устройствами, контроль сетевой активности.
  + Рекомендации: Подходит для крупных организаций с распределенными филиалами.

### **3 Установка и настройка систем контроля версий**

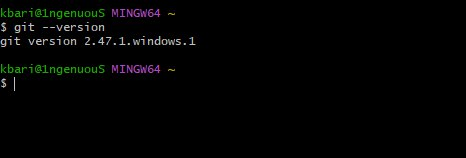
### **3.1 Установка системы контроля версий**

Git - это распределённая система контроля версий, которая используется для отслеживания изменений в коде и совместной работы над проектами. Git позволяет программистам сохранять историю изменений, легко откатываться к предыдущим версиям, объединять изменения, созданные разными разработчиками, и многое другое.

Нужно установить Git. Я перехожу на официальный сайт Git, где предлагаются версии для разных операционных систем (Windows, macOS, Linux).  
В зависимости от вашей ОС:

* Windows: загружаю .exe файл и запускаю установщик.
* macOS: использую Homebrew команду brew install git.

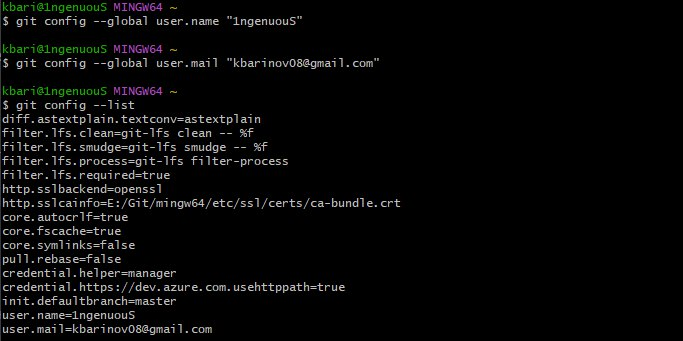
Для проверки установки Git, был открыт терминал(cmd) и использую команду git --version на рисунке 1.

****

**Рисунок 1 – Установка Git**

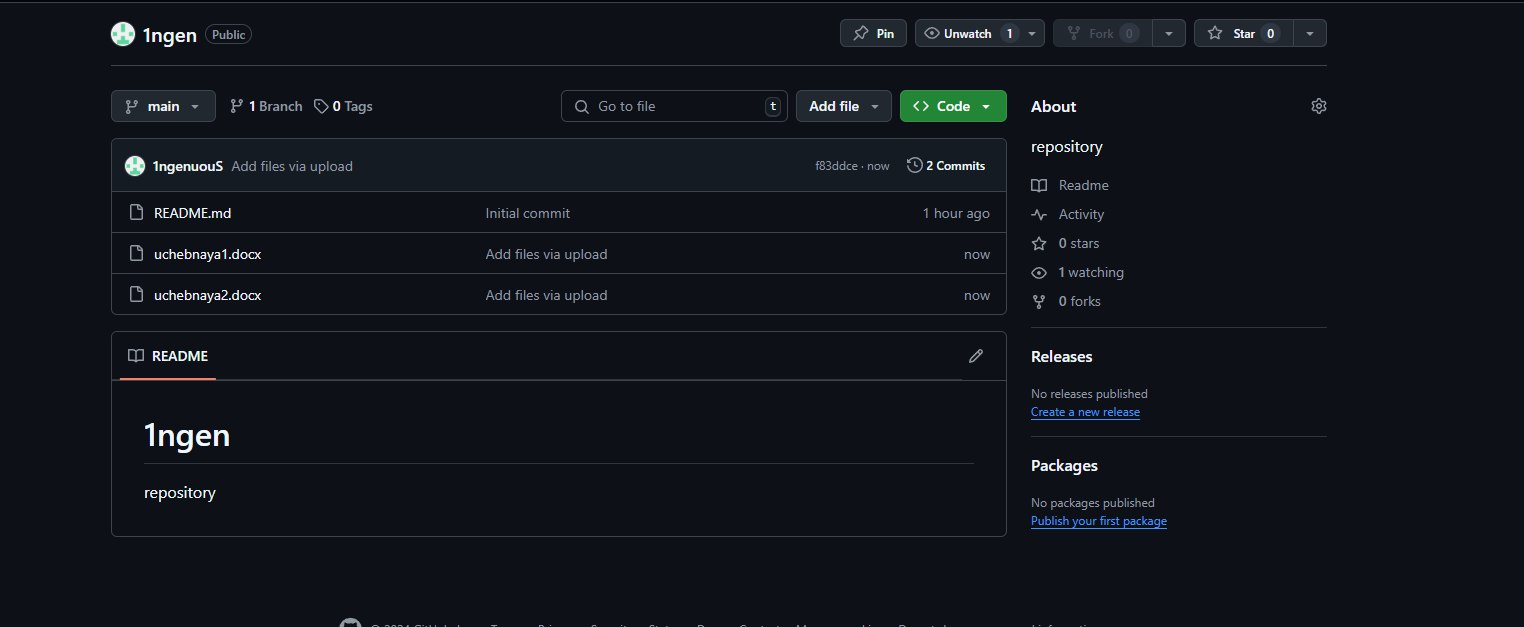
**3.2 Настройка Git**

Настройка имени пользователя и электронной почты в Git необходима для идентификации автора коммитов в истории изменений. Каждый раз, когда вы сохраняете изменения в репозитории, Git добавляет к коммиту подпись, содержащую ваше имя и email. Это важно для совместной работы, чтобы участники команды могли видеть, кто внёс изменения, а также для прозрачности истории проекта.

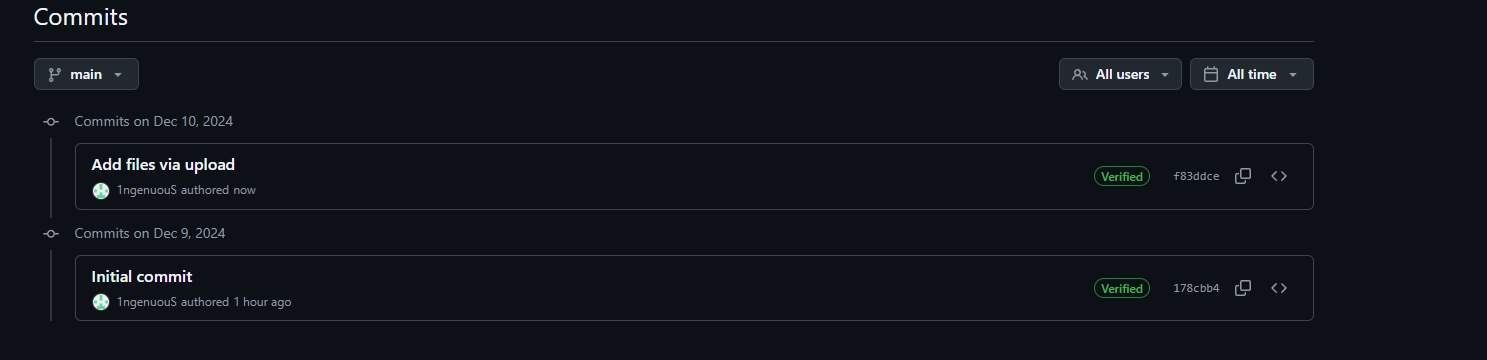
Настройка производиться с помощью команд git config --global user.name "Ваше Имя" git config --global user.email "ваша\_почта@домен.ру", введя эти команды, нужно проверить настройки командой git config --list как на 2 рисунке.

**Рисунок 2 – Настройка Git**

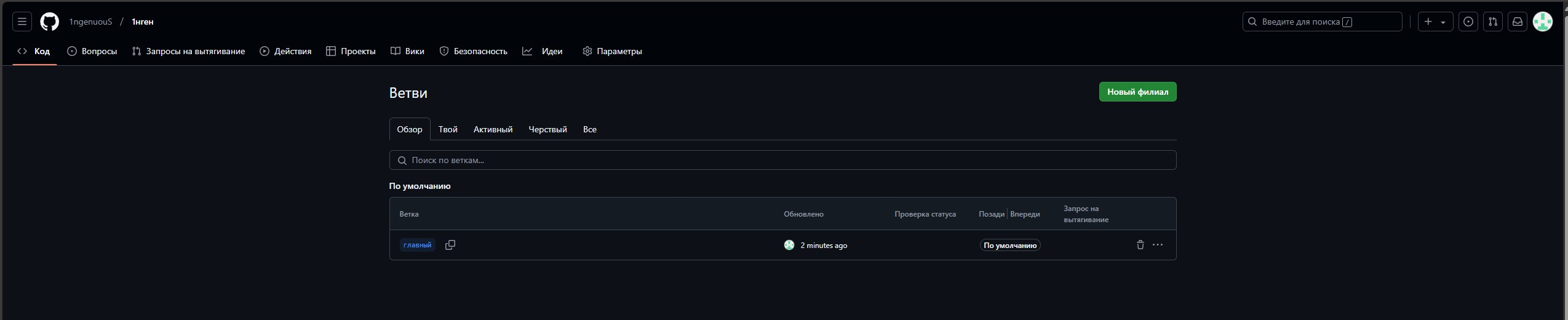
**3.3 Загрузки в проекта в GitHub**

Для загрузки отчета была выбрана система GitHub. На рисунке 3 был создан проект, куда был загружена версия данного отчета

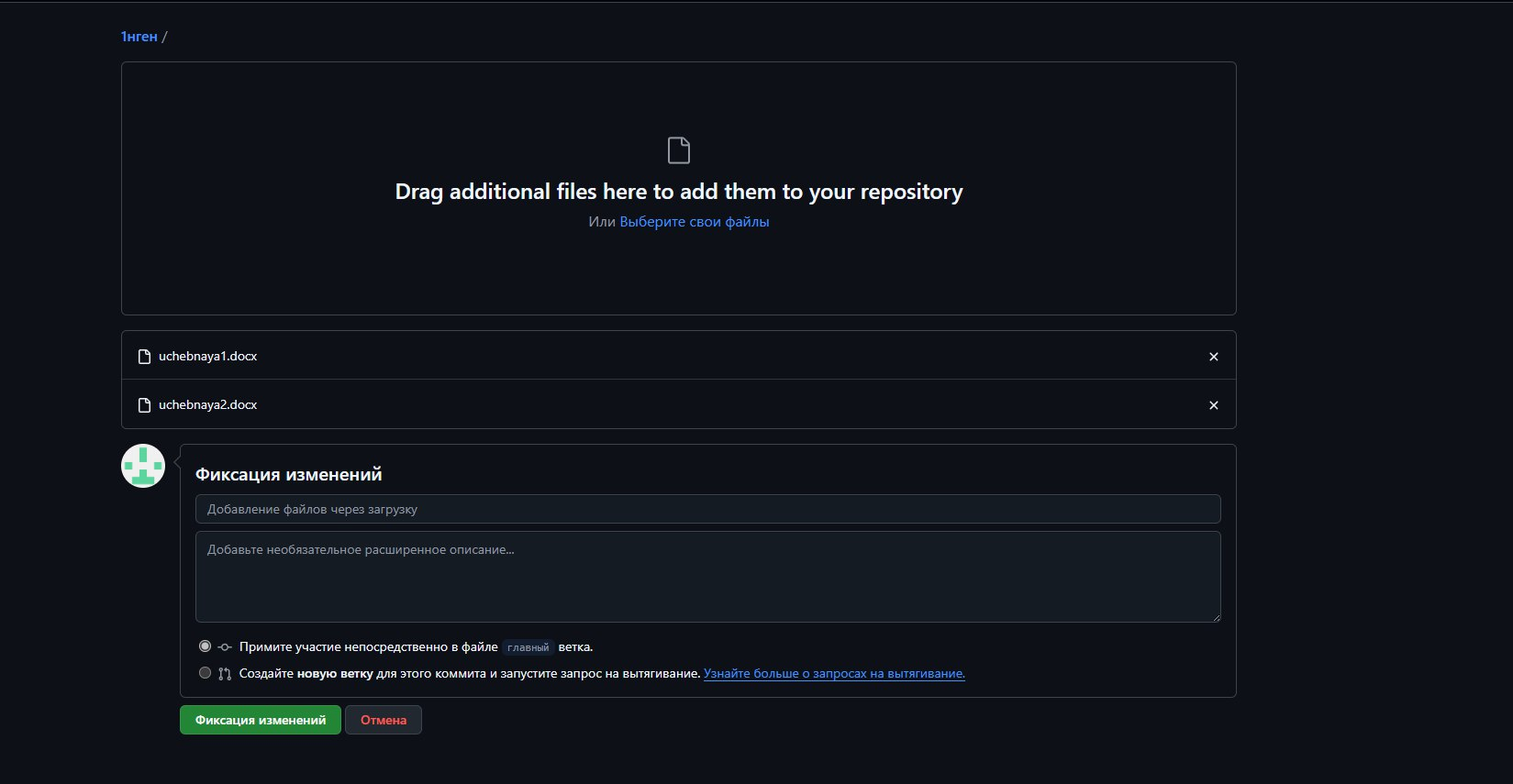
**Рисунок 3 – Создание проекта**

На 4 рисунке проиллюстрированы коммиты, где показаны все изменения в проекте с измененными файлами.

**Рисунок 4 – Коммиты**

На 5 рисунке показаны активные ветви На изображении показана вкладка "Ветви" в репозитории GitHub.

**Рисунок 5 – Ветви**

На изображении 6 показан интерфейс загрузки файлов в репозиторий на GitHub. Было добавлено два документа: uchebnaya1.docx и uchebnaya2.docx. В поле "Фиксация изменений" указано описание коммита: "Добавление файлов через загрузку". Ниже предлагаются два варианта действий: зафиксировать изменения непосредственно в текущей ветви (главный) или создать новую ветвь для фиксации и открыть запрос на слияние. Внизу расположены кнопки "Фиксация изменений" для подтверждения и "Отмена" для отмены действий.

**Рисунок 6 - Загрузка новых файлов**

В этом репозитории собраны разные версии отчёта, каждая из которых отражает изменения в оформлении и содержании. Эти версии позволяют проследить эволюцию документа, оценить внесённые улучшения и выбрать наиболее подходящий вариант. Репозиторий можно использовать как пример управления версиями или для анализа подходов к оформлению.   
Ссылка на репозиторий - <https://github.com/1ngenuouS>

### Заключение

Учебная практика, проведенная в Колледже Нижегородского института управления – филиала РАНХиГС, позволила мне закрепить теоретические знания, полученные в процессе обучения, и приобрести важные практические навыки, необходимые для дальнейшей профессиональной деятельности. В течение практики были выполнены задачи, поставленные руководителем, что способствовало достижению поставленных целей и углублению знаний в области информационных технологий.

Одним из ключевых результатов стало формирование навыков самостоятельной работы в рамках поставленных задач, что включало анализ характеристик персонального компьютера и программного обеспечения. В процессе выполнения задания были изучены основные компоненты аппаратного обеспечения, их параметры и взаимосвязь, а также проведен детальный анализ система удаленного администрирования как важного программного обеспечения. Это позволило понять, как аппаратная часть ПК влияет на эффективность работы с ПО, а также какие характеристики программного обеспечения определяют его функциональность, надежность и совместимость.

Важным этапом практики стало изучение и оценка российских аналогов программного обеспечения. Были разработаны рекомендации по их использованию, как для стационарных программ, так и для онлайн-сервисов. Это дало возможность не только изучить современные отечественные решения в области ИТ, но и оценить их соответствие требованиям безопасности, производительности и удобства использования, что особенно актуально в условиях перехода на импортозамещающее программное обеспечение.

В ходе практики освоена работа с Git и GitHub, что важно для командной разработки: отслеживание изменений, история версий и совместное редактирование. Практическое применение инструментов дало опыт в современных технологиях разработки ПО.

### Список источников и литературы

**1. ГОСТ 34.602-2020. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.** URL: <https://allgosts.ru/01/040/gost_34.602-2020>  
(дата обращения: 05.12.2024).

**2. ГОСТ 34.603-92. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем.** URL: <https://docs.cntd.ru/document/1200008642>  
(дата обращения: 05.12.2024).

3. **ГОСТ Р ИСО/МЭК 25010-2015. Информационная технология. Методы и средства обеспечения качества. Модели качества систем и программного обеспечения.** URL: https://docs.cntd.ru/document/1200125297  
(дата обращения: 06.12.2024).

          4. **ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности.**URL: <https://docs.cntd.ru/document/1200181890>  
(дата обращения: 07.12.2024).

5. **ГОСТ Р 58833-2020. Национальный стандарт Российской Федерации. Защита информации. Идентификация и аутентификация. Общие положения.**  
URL: <https://docs.cntd.ru/document/1200172576>  
(дата обращения: 07.12.2024).

6. **ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Стадии создания.**URL:<https://docs.cntd.ru/document/1200006921>  
(дата обращения: 08.12.2024).

7. **ГОСТ Р ИСО 9241-110-2009. Национальный стандарт Российской Федерации. Эргономика взаимодействия человек-система. Принципы организации диалога.**URL: <https://docs.cntd.ru/document/1200076559>  
(дата обращения: 08.12.2024).

8. **ГОСТ 24.701-86. Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления.**  
URL: <https://meganorm.ru/Index2/1/4294830/4294830195.htm>  
(дата обращения: 08.12.2024).

9.**ГОСТ 24.104-2023. Межгосударственный стандарт. Единая система стандартов автоматизированных систем управления. Общие требования.**  
URL: [https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=STR&n=3318](https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=STR&n=33187)  
(дата обращения: 09.12.2024).

**10. ГОСТ Р ИСО/МЭК 29119-2019. Информационные технологии. Процессы тестирования программного обеспечения. Общие положения.**URL: https://docs.cntd.ru/document/1200178857  
(дата обращения: 09.12.2024).