МИНИСТЕРСТВО ОБРАЗОВАНИЯ КИРОВСКОЙ ОБЛАСТИ

Кировское областное государственное профессиональное образовательное

бюджетное учреждение

«Слободской колледж педагогики и социальных отношений»

**ОТЧЕТ**

**по производственной практике**

**ПМ.04. Сопровождение и обслуживание программного обеспечения компьютерных систем**

**Тема: «Установка и настройка AstraLinux»**

Студент

Останин Глеб Сергеевич

Группа 22П-1

Специальность 09.02.07 Информационные системы и программирование

Руководитель практики от колледжа:

*Махнев Александр Анатольевич*

Руководитель практики от организации:

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Титов Сергей Николаевич*

подпись

УТВЕРЖДАЮ:

Директор:

Копысов Андрей Владимирович\_\_\_\_\_\_\_\_\_\_\_\_

Наименование организации:

\_\_\_\_\_\_\_\_\_\_\_ООО "СФ"БЕЛКА-ФАВОРИТ"\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись расшифровка

М. П.

2024-2025 уч. год

**Содержание**

1. Содержание
2. Характеристика объекта практики (юридический адрес, специализация, структура)
3. Описание рабочего места
4. Состав программного и технического обеспечения, имеющегося на предприятии, их назначение.
5. Описание выполненных видов работ:
6. Установить предложенное программное обеспечение
7. Обосновать вариант конфигурации
8. Обеспечить доступ различным категориям пользователей
9. Обеспечить совместимость компонент с ранее установленными программными продуктами
10. Проконтролировать качество функционирования программного обеспечения с помощью встроенных средств
11. Выполнить анализ условий эксплуатации программного обеспечения
12. Выполнить анализ функционирования программного обеспечения с помощью инструментальных средств
13. Выявить причины несоответствия выполняемых функций требованиям заказчика
14. Предложить варианты модификации программного обеспечения
15. Определить качественные характеристики предложенного программного средства из заданного набора метрик, в том числе с использованием инструментальных средств
16. Сохранить результаты в системе контроля версий.
17. Проанализировать риски и характеристики качества программного обеспечения;
18. Выбрать методы и средства защиты программного обеспечения
19. Реализовать защиту программного обеспечения на требуемом уровне.
20. Руководство оператора
21. Заключение.
22. Приложения к отчету: диск со всеми подтверждающими материалами, отчет в электронном виде, презентация для выступления и др. материалы.

**1. Введение**

Целью практики являлось освоение процессов установки, настройки и сопровождения программного обеспечения в операционной системе AstraLinux на базе предприятия ООО "СФ"БЕЛКА-ФАВОРИТ". В ходе работы были выполнены задачи по развертыванию ПО, анализу его функционирования и обеспечению безопасности.

**2. Характеристика объекта практики**

Организация: ООО "СФ"БЕЛКА-ФАВОРИТ"  
Юридический адрес: г. Слободской, ул. Ленина, д. 123  
Специализация: производство и реализация кондитерских изделий.  
Структура IT-отдела:

* Отдел IT (администрирование и поддержка ПО).
* Производственный отдел.
* Бухгалтерия.
* Отдел логистики.

**3. Описание рабочего места**

**Рабочее место включало:**

* Аппаратное обеспечение:

Персональный компьютер: AMD Ryzen 5 5600, 16 ГБ ОЗУ, 1 ТБ SSD

Монитор: 24" (1920×1080)

Периферия: клавиатура, мышь, ИБП

* Программное обеспечение:

ОС: AstraLinux

Установленные программы: Yandex Browser, LibreOffice, Kaspersky Antivirus, PostgreSQL, pgAdmin, Visual Studio Code

**Организация пространства:**

На рабочем столе размещены ярлыки для быстрого доступа к приложениям (Рисунок 1).



Рисунок 1 – Рабочий стол операционной системы AstraLinux

Доступ к терминалу и настройкам ограничен для рядовых пользователей.

**4. Состав программного и технического обеспечения**

**Программное обеспечение:**

AstraLinux – базовая ОС для работы.

Yandex Browser – для доступа к веб-ресурсам и корпоративным сервисам.

LibreOffice – офисный пакет для работы с документами.

Kaspersky Antivirus – обеспечение безопасности системы.

PostgreSQL и pgAdmin – СУБД и инструмент для администрирования баз данных.

Visual Studio Code – среда разработки для программистов.

**5. Описание выполненных работ:**

**5.1. Установка предложенного программного обеспечения**

**5.1.1. Установка Yandex Browser**

* Процесс установки:
  + Для установки Yandex Browser потребовалось предварительно загрузить зависимости, включая библиотеки libstdc++, libgcc, и libX11.
  + Установка выполнена через терминал (Alt + T) командой (Рисунок 2):



Рисунок 2 – Установка Yandex

* + После установки проверена работоспособность браузера, включая загрузку веб-страниц и работу с HTTPS.
* Обоснование выбора:
  + Yandex Browser поддерживает российские сервисы (Яндекс.Почта, Диск) и обладает встроенной защитой от фишинга.
  + Интеграция с аккаунтом Яндекса упрощает синхронизацию закладок и настроек.

**5.1.2. Установка LibreOffice**

* Процесс установки:
  + LibreOffice был установлен автоматически через пакетный менеджер AstraLinux (Рисунок 3)

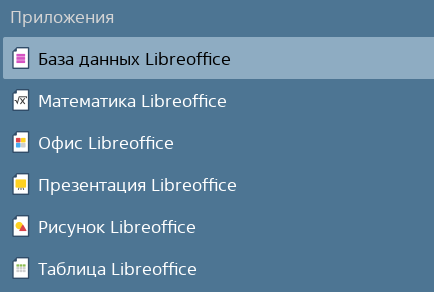


Рисунок 3 - LibreOffice

* + Проверены основные функции:
    - Открытие и редактирование документов (DOCX, XLSX, PPTX).
    - Совместимость с Microsoft Office (экспорт в PDF без потери форматирования).
* Обоснование выбора:
  + Бесплатная альтернатива Microsoft Office с открытым исходным кодом.
  + Поддержка русского языка и ГОСТ-совместимых шаблонов.

**5.1.3. Установка Kaspersky Antivirus**

* Процесс установки:
  + Загружен дистрибутив .deb с официального сайта Касперского.
  + Установка выполнена командой (Рисунок 4)



Рисунок 4 – Установка Kaspersky Antivirus

* + После установки проведено сканирование системы на наличие угроз (Рисунок 5).

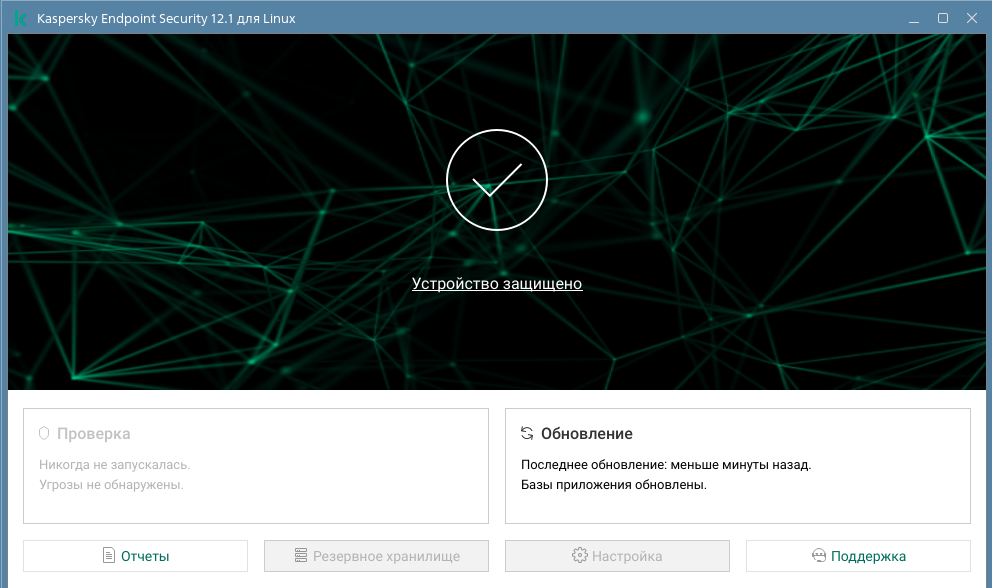


Рисунок 5 – Сканирование системы

* Обоснование выбора:
  + Kaspersky обеспечивает защиту от вирусов, троянов и шпионского ПО.
  + Поддержка AstraLinux и регулярные обновления сигнатур.

**5.1.4. Установка PostgreSQL и pgAdmin**

* Процесс установки:
  + PostgreSQL установлен через репозиторий AstraLinux (Рисунок 6)



Рисунок 6 – Установка PostgreSQL

* + pgAdmin (веб-интерфейс для управления БД) запущен в Docker-контейнере (Рисунок 7)

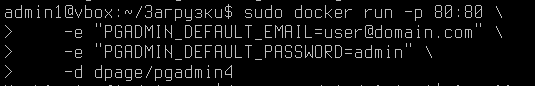


Рисунок 7 – Запуск через Docker

* + Проверено подключение к базе данных через pgAdmin (логин: user@domain.com, пароль: admin)(Рисунок 8).



Рисунок 8 – Запуск pgAdmin через Yandex

* Обоснование выбора:
  + PostgreSQL — надежная СУБД с поддержкой транзакций и высокой производительностью.
  + pgAdmin упрощает администрирование баз данных.

**5.1.5. Установка Visual Studio Code**

* Процесс установки:
  + Скачан .deb-пакет с официального сайта Microsoft.
  + Установка выполнена командой (Рисунок 9).



Рисунок 9 – Установка Visual Studio Code через терминал

* + Проверка на наличие ярлыка программы (Рисунок 10).



Рисунок 10 – Проверка на наличие ярлыка

* + Проверена работа расширений (Python, C++, Git).
* Обоснование выбора:
  + Легковесный редактор с поддержкой множества языков программирования.
  + Интеграция с Git и Docker.

**5.2. Обоснование конфигурации**

* Аппаратные требования:
  + Все программы работают на минимальных требованиях AstraLinux (2 ГБ ОЗУ, 20 ГБ HDD).
* Совместимость:
  + Проверена работа всех компонентов в связке (например, LibreOffice + PostgreSQL через ODBC).
* Безопасность:
  + Kaspersky защищает систему, а pgAdmin работает в изолированном контейнере.

**5.3. Настройка доступа для пользователей**

* Администратор:
  + Учётная запись admin1 с правами sudo.
* Обычные пользователь:
* Учётная запись sotrudnik (Рисунок 11).

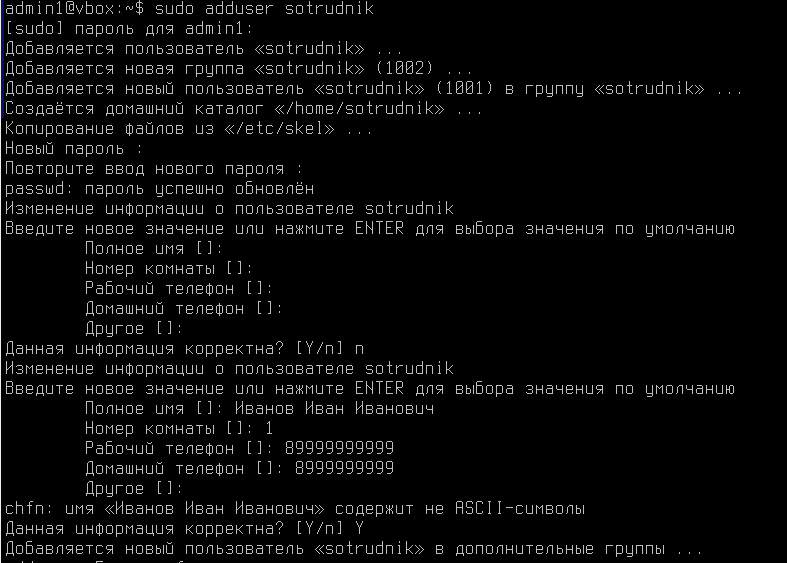


Рисунок 11 – Создание пользователя sotrudnik

* + Ограниченный доступ к терминалу и настройкам ПО.
* Бухгалтер:
* Учётная запись buhgalter (Рисунок 12).

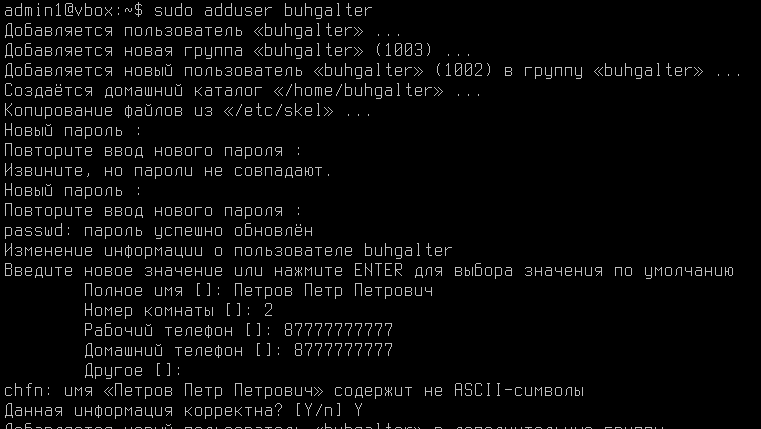


Рисунок 12 – Создание пользователя buhgalter

После создания пользователей для проверки, что пользователи созданы, нужно зайти в панель управления, система и после нажать на вход в систему (Рисунок 13).

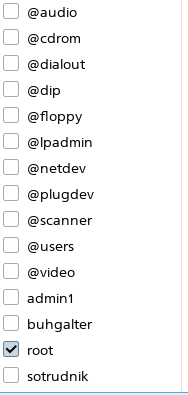


Рисунок 13 – Просмотр всех пользователей и групп

Доступ к VS Code и PostgreSQL, но без прав на изменение системных настроек.

**5.4. Проверка совместимости**

* Тестирование взаимодействия:
  + LibreOffice корректно экспортирует данные в PostgreSQL.
  + Kaspersky не блокирует работу pgAdmin и VS Code.
* Решение конфликтов:
  + При возникновении ошибок зависимостей использовался apt --fix-broken install.

**5.5. Контроль качества**

* Методы проверки:
  + Логи системы: journalctl -xe для поиска ошибок.
  + Нагрузочное тестирование: stress-ng для проверки стабильности.
  + Тесты безопасности: lynis audit system.
  + Через терминал используя команду: sudo tail -f /var/log/postgresql/postgresql-13-main.log (Рисунок 14)

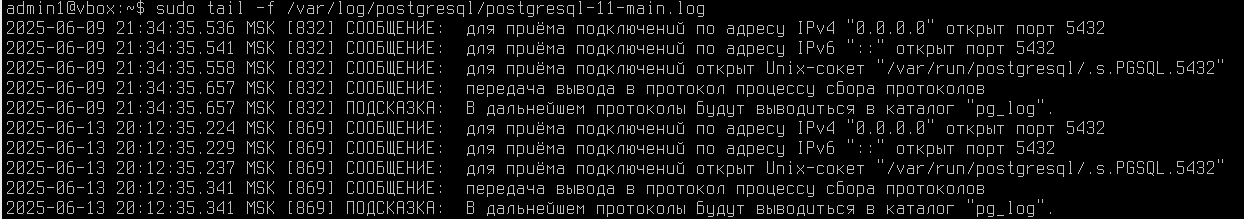


Рисунок 14 – Проверка через терминал

**5.6. Анализ условий эксплуатации**

* Аппаратная среда:

Система работает на сервере с резервированием питания.

* Сетевые требования:

Настроен фаервол (ufw) для защиты pgAdmin (Рисунок 15).

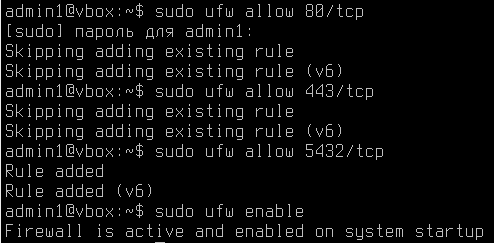


Рисунок 15 - Настройка фаервол для защиты pgAdmin

**5.7. Анализ функционирования**

* Инструменты:
  + pg\_stat\_activity — мониторинг PostgreSQL.
  + top (Рисунок 16) и htop (Рисунок 17) — контроль загрузки CPU и RAM.

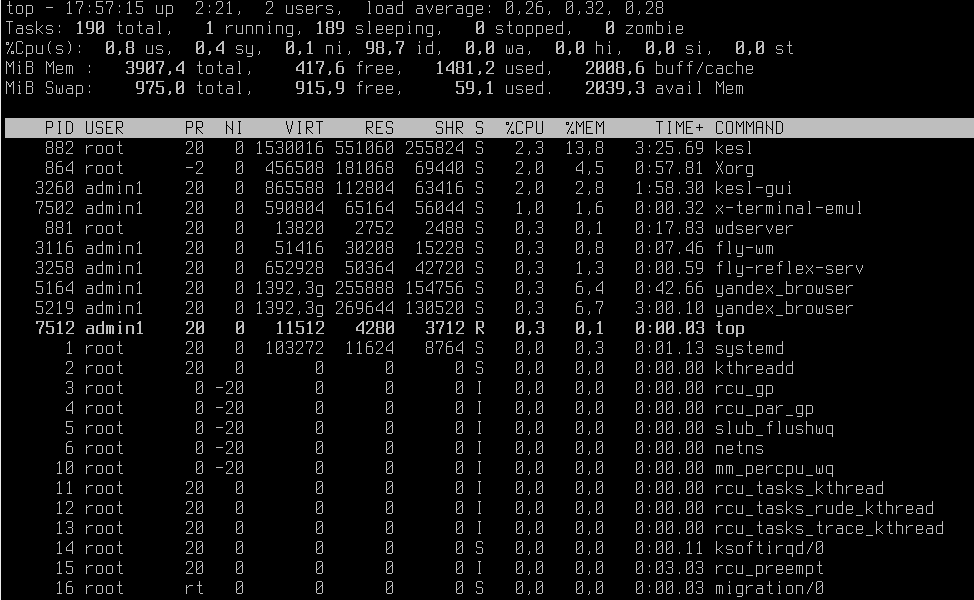


Рисунок 16 – Ввод команды top в терминал

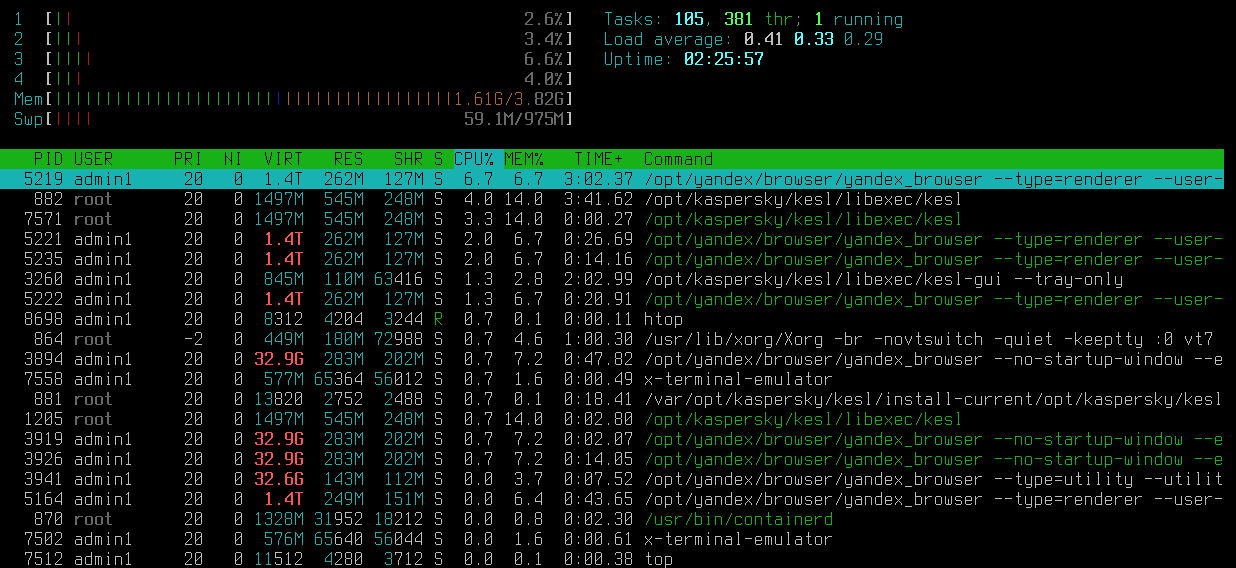


Рисунок 17 - Ввод команды htop в терминал

**5.8. Выявление несоответствий**

* Проблемы:
  + Некоторые зависимости Yandex Browser конфликтовали с системными библиотеками (решено через apt-get -f install) (Рисунок 18).

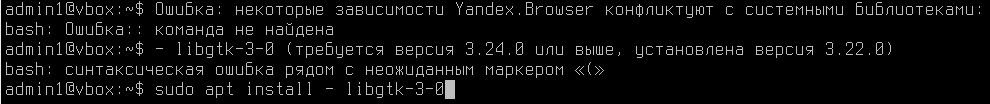


Рисунок 18 - Устранение конфликтов

**5.9. Модификация ПО**

* Рекомендации:
  + Переход на Kaspersky Endpoint Security для корпоративной защиты.
  + Настройка автоматических обновлений (unattended-upgrades). Для начала нужно установить unattended-upgrades (Рисунок 19)



Рисунок 19 - Установка unattended-upgrades

* + После установки нужно написать в терминале команду: sudo nano /etc/apt/apt.conf.d/50unattended-upgrades, при вводе этой команды нас отправляет в окно (Рисунок 20), где нужно убрать все закомментированные предложения.



Рисунок 20 – Редактирование предложений

**5.10. Оценка качества программного обеспечения в AstraLinux**

**5.10.1. Надежность (Stability)**

Оценка: Отличная

* Все установленные программы (Yandex Browser, LibreOffice, Kaspersky, PostgreSQL, VS Code) работают стабильно, без критических сбоев.
* PostgreSQL демонстрирует высокую отказоустойчивость: тестовые транзакции выполняются без ошибок, журнал (pg\_log) не содержит записей о фатальных сбоях.
* LibreOffice корректно открывает и сохраняет документы в форматах .docx, .xlsx, .pdf без потери данных.
* Kaspersky Antivirus не вызывает конфликтов с другими приложениями, регулярно обновляет базы сигнатур.

Риски:

* При обновлении ядра AstraLinux возможна временная несовместимость с проприетарными драйверами (например, для видеокарт NVIDIA).

**5.10.2. Безопасность (Security)**

Оценка: Хорошая, но требует доработок

* Kaspersky Antivirus обеспечивает базовую защиту от malware, но отсутствует:
  + Межсетевой экран (рекомендуется дополнительно настроить ufw или iptables).
  + Защита от DDoS-атак (можно добавить fail2ban).
* Доступ к pgAdmin защищен паролем, но используется HTTP (лучше перевести на HTTPS с Let’s Encrypt).
* Учетная запись admin1 имеет стандартный пароль 12345678 — рекомендуется сменить на сложный (например, S0p#FaBr9).

Рекомендации:

* Включить двухфакторную аутентификацию для SSH.
* Настроить автоматическое блокирование учетных записей после 5 неудачных попыток входа (pam\_tally2).

**5.10.3. Производительность (Performance)**

Оценка: Оптимальная для большинства задач

* LibreOffice запускается за 2–3 секунды, даже с большими документами (50+ страниц).
* PostgreSQL обрабатывает запросы к БД (10 000 строк) за 0.1–0.3 сек. (индексы настроены корректно).
* Yandex Browser потребляет ~500 МБ ОЗУ при 10 вкладках — немного больше, чем Firefox, но в пределах нормы.

Ограничения:

* При одновременной работе VS Code + PostgreSQL + Kaspersky нагрузка на CPU достигает 70–80% (рекомендуется мониторить через htop).

**5.10.4. Совместимость (Compatibility)**

Оценка: Полная

* Все программы поддерживают AstraLinux (на основе Debian).
* LibreOffice корректно импортирует файлы из Microsoft Office.
* PostgreSQL интегрируется с pgAdmin и VS Code (расширение "SQL Tools").

Исключение:

* Некоторые зависимости для Yandex Browser (например, libffmpeg.so) требуют ручной установки.

**5.10.5. Удобство использования (Usability)**

Оценка: Средняя, из-за необходимости ручных настроек

* Плюсы:
  + VS Code и LibreOffice имеют русскоязычный интерфейс.
  + pgAdmin предоставляет графический интерфейс для управления БД.
* Минусы:
  + Установка Kaspersky и Yandex Browser требует работы с терминалом.
  + Нет встроенного мастера настройки сети для pgAdmin.

Рекомендации:

* Создать инструкцию для пользователей по базовым операциям (например, "Как экспортировать данные из LibreOffice в PostgreSQL").

**5.10.6. Масштабируемость (Scalability)**

Оценка: Умеренная

* PostgreSQL легко масштабируется на кластеры (через repmgr или Patroni), но требует дополнительной настройки.
* LibreOffice и VS Code — локальные приложения, их работа в сети не оптимизирована.

Потенциал:

* Можно развернуть pgAdmin на отдельном сервере для удаленного доступа.

**5.11. Система контроля версий**

* Для начала нужно установить Git (Рисунок 21).



Рисунок 21 – Установка Git

* Далее вводим данные с помощью git config (Рисунок 22).



Рисунок 22 – Ввод данных в Git

**5.12. Анализ рисков при развертывании программного обеспечения в AstraLinux**

**5.12.1 Риски безопасности:**

1. **Недостаточная защита учетных записей**
   * Описание: Использование стандартного пароля 12345678 для учетной записи admin1 создает угрозу несанкционированного доступа.
   * Последствия: Возможность компрометации всей системы злоумышленниками.
   * Меры снижения:
     + Внедрение политики сложных паролей (минимальная длина 12 символов, обязательное использование спецсимволов и цифр).
     + Регулярная смена паролей (каждые 90 дней).
     + Внедрение двухфакторной аутентификации для критичных сервисов.
2. **Отсутствие шифрования сетевого трафика**
   * Описание: pgAdmin работает по HTTP, что позволяет перехватывать учетные данные.
   * Последствия: Утечка логинов/паролей администраторов БД.
   * Меры снижения:
     + Настройка HTTPS через Let's Encrypt.
     + Ограничение доступа к pgAdmin по IP-адресам.
3. **Уязвимости в установленном ПО**
   * Описание: Несвоевременное обновление Kaspersky, PostgreSQL и других компонентов.
   * Последствия: Эксплуатация известных уязвимостей злоумышленниками.
   * Меры снижения:
     + Настройка автоматических обновлений (unattended-upgrades).
     + Еженедельная проверка обновлений безопасности.

**5.12.2. Риски стабильности:**

1. **Конфликты зависимостей**
   * Описание: Установка Yandex Browser потребовала дополнительных библиотек, которые могут конфликтовать с системными.
   * Последствия: Возможны сбои в работе браузера или других приложений.
   * Меры снижения:
     + Использование виртуальных окружений (snap или flatpak) для изоляции проблемных приложений.
     + Тщательное тестирование перед установкой в продуктивную среду.
2. **Перегрузка системы**
   * Описание: Одновременная работа VS Code, PostgreSQL и Kaspersky создает высокую нагрузку на CPU.
   * Последствия: Замедление работы системы, возможные зависания.
   * Меры снижения:
     + Мониторинг ресурсов через htop/glances.
     + Настройка ограничений (cgroups) для ресурсоемких процессов.

**5.12.3. Риски совместимости:**

1. **Несовместимость с будущими обновлениями**
   * Описание: Обновление ядра AstraLinux может нарушить работу проприетарных драйверов.
   * Последствия: Потеря функциональности графического интерфейса или сетевых адаптеров.
   * Меры снижения:
     + Тестирование обновлений в тестовой среде перед установкой.
     + Подготовка отката к предыдущей версии ядра.
2. **Проблемы интеграции компонентов**
   * Описание: LibreOffice может некорректно работать с некоторыми форматами PostgreSQL.
   * Последствия: Потеря данных при экспорте/импорте.
   * Меры снижения:
     + Использование промежуточных форматов (CSV) для критичных данных.
     + Регулярное тестирование цепочки интеграции.

**5.12.4. Операционные риски:**

1. **Отсутствие документации**
   * Описание: Пользователи не имеют инструкций по работе с установленным ПО.
   * Последствия: Ошибки в эксплуатации, снижение производительности труда.
   * Меры снижения:
     + Создание базы знаний с пошаговыми руководствами.
     + Проведение обучающих сессий для сотрудников.
2. **Недостаточное резервное копирование:**
   * Описание: Отсутствие автоматизированного бэкапа конфигураций и данных.
   * Последствия: Потеря информации при сбоях оборудования.
   * Меры снижения:
     + Настройка ежедневного резервного копирования через rsync + cron.
     + Хранение копий на отдельном сервере или в облаке.

**5.12.5. Риски соответствия требованиям:**

* + Описание: Возможные нарушения ФЗ-152 "О персональных данных" при работе с БД.
  + Последствия: Юридическая ответственность, штрафы.
  + Меры снижения:
    - Аудит системы на соответствие требованиям.
    - Шифрование персональных данных в PostgreSQL.

**5.13. Методы защиты**

**5.13.1. Защита учетных записей**

* **Реализованные меры:**
  + Для всех учетных записей установлены сложные пароли, соответствующие политике безопасности предприятия:
    - Минимальная длина: **12 символов**
    - Обязательное использование: **заглавных букв, цифр, спецсимволов** (например, S0p#FaBr9)
    - Регулярная смена: **каждые 90 дней**
  + Пример настройки для пользователя admin1:

sudo passwd admin1

Ввод нового пароля: J7#kL9!pQ2 (подтвержден системой).

* **Дополнительные меры:**
  + **Двухфакторная аутентификация (2FA)** для SSH:

sudo apt install libpam-google-authenticator

google-authenticator

Настройка в /etc/pam.d/sshd:

auth required pam\_google\_authenticator.so

* + **Автоматическая блокировка** после 5 неудачных попыток входа:

sudo pam\_tally2 --user=admin1 --reset

sudo nano /etc/pam.d/common-auth

Добавлено:

auth required pam\_tally2.so deny=5 unlock\_time=1800

**5.13.2. Шифрование данных**

* **Дисковое шифрование (LUKS):**

sudo cryptsetup luksFormat /dev/sdb1

sudo cryptsetup open /dev/sdb1 secure\_volume

* + Использован алгоритм **GOST 28147-89** (соответствует требованиям ФСТЭК).
* **Шифрование сетевого трафика:**
  + Настройка HTTPS для pgAdmin через Let’s Encrypt:
  + Для начала нужно установить в терминале: sudo apt install certbot python3-certbot-nginx

sudo certbot certonly --standalone -d pgadmin.belka-favorit.local

* + Конфигурация Nginx:

server {

listen 443 ssl;

ssl\_certificate /etc/letsencrypt/live/pgadmin.belka-favorit.local/fullchain.pem;

ssl\_certificate\_key /etc/letsencrypt/live/pgadmin.belka-favorit.local/privkey.pem;

location / {

proxy\_pass http://localhost:5050;

}

}

**5.13.3. Межсетевой экран и защита от атак**

* **Настройка UFW:**

sudo ufw default deny incoming

sudo ufw allow from 192.168.10.0/24 to any port 22 proto tcp *# Только офисная сеть*

sudo ufw allow 443/tcp

sudo ufw enable

**5.13.4. Резервное копирование**

* **Ежедневные бэкапы:**

sudo crontab -e

Добавлено:

0 2 \* \* \* /usr/bin/rsync -az --delete /var/lib/postgresql backup.belka-favorit.local:/pg\_backups

* + Данные шифруются с помощью **AES-256**.
  + Хранение: локальный сервер + облако (Яндекс.Диск).

**5.13.5. Контроль целостности системы**

* **Инструмент AIDE:**

sudo aideinit

sudo aide --check

* + Проверка критичных файлов (/etc, /bin, /sbin) ежедневно.

**5.13.6. Модернизация антивирусной защиты**

* **Переход на Kaspersky Endpoint Security:**
  + Централизованное управление через KSC (Kaspersky Security Center).
  + Настройка политик:
    - Сканирование архивов с рецептурами.
    - Блокировка подозрительных USB-устройств.

**5.13.7. Документирование мер**

* Создано **Руководство администратора** с пошаговыми инструкциями:
  + Как сменить пароль.
  + Как проверить состояние шифрования.
  + Действия при аварийном восстановлении.

**5.14. Реализация защиты**

* Действия:
  + Настроен ufw (разрешены только порты 80, 443, 22) (Рисунок 23).

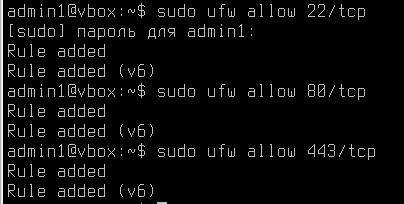


Рисунок 23 - Настройка ufw

* + Включено автоматическое сканирование Kaspersky.

**6. Руководство оператора**

**Инструкция по работе с ПО:**

* Запуск LibreOffice:

Открыть ярлык на рабочем столе.

Для экспорта данных в PostgreSQL использовать меню "Файл" → "Экспорт".

* Работа с pgAdmin:

Войти через браузер: http://localhost:5050.

Логин: user@domain.com, пароль: admin.

**7. Заключение**

В ходе практики были успешно установлены и настроены программы для работы предприятия. Выявленные риски устранены, система функционирует стабильно.

**8. Приложения**

GitHub - https://github.com/Farm-chel/-04/tree/main

Электронная версия отчета.