Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Высшая инженерная школа цифровых технологий

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(код и наименование направления подготовки, специальности)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-

(наименование профиля, специализации)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(БАКАЛАВРСКАЯ РОБОТА)

На тему «Разработка Linux дистрибутива на основе Debian для ЮГУ»

Студент (ка) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Фамилия имя отчество) (личная подпись)

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Фамилия имя отчество) (личная подпись)

Нормоконтролер \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Фамилия имя отчество) (личная подпись)

Допустить к защите

Руководитель образовательной программы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ученая степень, звание, фамилия имя отчество) (личная подпись)

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

г. Ханты-Мансийск

2024 год

Реферат

на выпускную квалификационную бакалаврскую работу

Щербакова Д.И.

Бакалаврская работа содержит (?) с., (?) рисунков, (?) таблиц, (?) приложений, (?) источников.

(?)(Перечень ключевых слов (с заглавной буквы))

Целью бакалаврской работы является разработка информационной системы «Ugrach».

Объектом исследования является (?). Предметом исследования является разработка операционной системы на базе ядра Linux, способной взаимодействовать с доменом Windows Active Directory.

Выполнение работы включает в себя несколько этапов.

На первом этапе составляются требования к конечной операционной системе. Пользователь должен иметь возможность с тем же успехом выполнять поставленные задачи, что и на операционной системе под управлением Windows (?).

На втором этапе формируется конфигурация для программы «live-build», которая будет использоваться для дальнейшей сборки.

На третьем этапе с помощью утилиты «lb build» реализуется сборка системы, по завершению которой формируется файл  с расширением «.iso», являющийся образом конечной системы.

На последнем этапе полученная система устанавливается на рабочую машину и тестируется (?).

Оглавление

[Термины и определения 4](#__RefHeading___Toc438_1193957621)

[ВВЕДЕНИЕ 5](#__RefHeading___Toc440_1193957621)

[Основная часть 9](#__RefHeading___Toc442_1193957621)

[Аналитическая часть 9](#__RefHeading___Toc13030_3987331531)

[Общее представление разрабатываемой системы(?) 9](#__RefHeading___Toc591_3987331531)

[Обзор аналогов 10](#__RefHeading___Toc593_3987331531)

[ALT Linux 10](#__RefHeading___Toc595_3987331531)

[Astra Linux 10](#__RefHeading___Toc597_3987331531)

[Проектная часть 12](#__RefHeading___Toc454_1193957621)

[Функционал конечной системы 12](#__RefHeading___Toc448_1193957621)

[Обзор важных компонентов системы 13](#__RefHeading___Toc450_1193957621)

[Samba 13](#__RefHeading___Toc599_3987331531)

[Kerberos 14](#__RefHeading___Toc601_3987331531)

[PAM 16](#__RefHeading___Toc452_1193957621)

[Winbind 17](#__RefHeading___Toc294_4285700929)

[Практическая часть 18](#__RefHeading___Toc456_1193957621)

# Термины и определения

Ывывыв

# ВВЕДЕНИЕ

После событий 24 февраля 2022 года на нашу страну многими зарубежными корпорациями были наложены санкции. Американская публичная транснациональная корпорация «Microsoft», наиболее известная производством семейства операционных систем «Windows» и офисных приложений «Microsoft Office», не стала исключением. В марте 2022 года было объявлено о приостановке продаж продуктов и услуг россиянам. Лицензии на офисные программы не продлевались даже частным пользователям. В сентябре того же года была заблокирована возможность обновления Windows 10 и 11. Сделать это можно было только с помощью обходных маневров — через VPN или приобретение ключей активации по параллельному импорту. В апреле 2023 года Microsoft объявила, что не будет предоставлять в России гарантийное обслуживание игровых консолей «Xbox». С 30 сентября 2023 года прекратит продлевать лицензии на программное обеспечение для корпоративных пользователей. Об этом сообщило агентство TelecomDaily со ссылкой на письмо, полученное от технической поддержки разработчика. Причиной является то, что американская компания больше не может принимать платежи за продление лицензий на российские счета.

Все эти ограничения создают серьёзные неудобства как для обычных пользователей, так и для организаций, поскольку и те и другие в основной совей массе используют операционные системы на базе «Windows» и офисный пакет «Microsoft Office». В текущих реалиях вполне вероятно, что «Microsoft» полностью уйдет с российского рынка, что сделает невозможным использования лицензионных продуктов компании.

Все эти факторы побуждают искать аналоги вышеупомянутых цифровых продуктов. В первую очередь, в этом заинтересованы организации, поскольку использование ими нелицензионных продуктов недопустимо(?).

Среди офисных решений можно найти немало продуктов с открытым исходным кодом, которые могут стать достойной заменой «Microsoft Office». (Среди них: «LibreOffice», «OnlyOffice», «OpenOffice», «МойОфис» и другие.) Выбрать подходящий аналог не является сложной задачей.

С операционными системами же ситуация обстоит иначе. Существует немало российских систем на базе ядра «Linux», которые могут стать достойной альтернативой Microsoft Windows. (Самые известные из них: «ALT Linux», «РЕД ОС», «Astra Linux», «ЛотОС», «ROSA Linux».) Хотя некоторые из них являются бесплатными для физических лиц, для юридических лиц все из них, также как и «Microsoft Windows», являются платными. Более того, любая из вышеперечисленных систем требует детальной настройки для того, что удовлетворять всем требованиям конкретной организации. Это могут требования к безопасности, производительности, наличию тех или иных программных пакетов и так далее.

Решением может стать сборка своей собственной операционной системы, удовлетворяющей всем необходимым критериям, чему и посвящена данная исследовательская работа. Поскольку ядро «Linux» имеет открытый исходный код и распространяется по лицензии «GNU General Public License», сборка на его основе является наиболее удобной. Создание своей операционной системы «с нуля» является весьма нетривиальной задачей, требующей немало временных и трудовых ресурсов, а также квалифицированных специалистов, что может сделать разработку очень недешёвой. Альтернативой может быть сборка «Linux» системы на основе уже существующих дистрибутивов с помощью предназначенных для этого утилит. Наиболее известными среди них являются «live-build» и «Archiso», позволяющие создать свою кастомизированную(?) операционную систему на базе дистрибутивов «Debian» и «Arch Linux» соответственно.

Организацией, для которой будет собираться конечная операционная система, является Югорский государственный университет. Утилитой для сборки была выбрана «live-build». Причиной данного выбора является то, что «Arch Linux» - «роллинг-релиз» дистрибутив (?)и, как следствие, требует регулярных обновлений, которые могут негативно сказаться на стабильности работы системы. «Debian» же, напротив, получает глобальные обновления раз в два года. При этом, каждый релиз предварительно тщательно тестируется, что повышает отказоустойчивость системы.

Создание своего собственного дистрибутива «Linux» позволит Югорскому государственному университету использовать на своих компьютерах операционные системы из двух разных семейств, если на то будет необходимость, и, случае полного ухода компании «Microsoft» с российского рынка, совершить плавный переход с операционной системы «Windows».

# Основная часть

## Аналитическая часть

### Общее представление разрабатываемой системы(?)

Дистрибутив Linux – общее определение и название операционных систем, использующих ядро Linux, готовых для конечной установки на пользовательское и серверное оборудование. Такая операционная система состоит из ядра Linux, набора библиотек и утилит, а также, как правило, графической подсистемы и набора приложений, требуемых для работы с документами, таблицами, мультимедиа, графикой, базами данных и т. д.

Дериватив – дистрибутив, построенный и выпускающий релизы на основе другого дистрибутива. Это в первую очередь означает, что пакетная база дериватива полностью наследуется из оригинального дистрибутива, и, при необходимости, расширяется дополнительными пакетами.

Разработка дериватива удобна тем, что изначальный дистрибутив уже готов к установке, способен выполнять базовые задачи и, как правило, тщательно протестирован. С другой стороны, имеется зависимость от решений, принимаемых разработчиками базовой системы. Любые изменения, сделанные в базовой системе, даже если они являются нежелательными, в любом случае попадут в дериватив со следующим релизом.

За основу сборки нашей системы был выбрала выбрана стабильная версия дистрибутива «Debian», то есть результат будет являться деривативом. Этот подход к разработке был выбран по следующим причинам:

* Проверенная надежность дистрибутива «Debian»;
* Скорость разработки;
* Значительно меньшая сложность разработки по сравнению со сборкой системы «с нуля»;
* Не требует вложения денежных средств.

### Обзор аналогов

#### ALT Linux

ALT Linux – отечественное семейство дистрибутивов, являющееся отдельной ветвью дистрибутивов Linux. Основан на дистрибутиву Mandrake. Разработкой занимается компания «Базальт СПО». Является одним из самых старых отечественных дистрибутивов – его разработка началась в 1999 году.

Дистрибутив доступен в нескольких редакциях: «Альт Рабочая станция», «Альт Рабочая станция K», «Альт Сервер», «Альт Сервер Виртаулизации», «Альт Образование» и «Симпли Линукс». Все редакции являются бесплатными для скачивания и использования физическим лицам, но платными для юридических.

Интересной для рассмотрения является редакция «ALT Рабочая Станция». Это операционная система широкого назначения, имеющая широкий набор программ и драйверов для современных устройств. Поставляется с графической оболочкой «MATE». «ALT Рабочая Станция K», в свою очередь, поставляется с графической оболочкой «KDE Plasma». Дистрибутив настроен для работы в корпоративной сети, в том числе с доменной структурой. В качестве контроллера домена может выступать как Microsoft AD, так и «Альт Сервер».

#### Astra Linux

Astra Linux – операционная система на базе ядра Linux, внедряемая в России в качестве альтернативы Microsoft Windows в государственных организациях. Основывается на Debian. Разработкой системы занимается группа компания «Астра» – один из лидеров российского рынка информационных технологий в области разработки ПО и средств защиты информации.

Доступно два варианта операционной системы – «Astra Linux Common Edition», «Astra Linux Special Edition». «Astra Linux Common Edition» является системой общего назначения, предназначения для решения повседневных задач. «Astra Linux Special Edition» в свою очередь подразделяется на четыре редакции: «Astra Linux Server», «Astra Linux Desktop», «Astra Linux Mobile» и «Astra Linux Embedded». Ключевой особенностью данной редакции является её высокая защищенность. Система может без труда противостоять как различным киберугрозам, так и вредоносной активности, вызванной пользователями или системным администратором. Является единственной системой в России, которая полностью соответствует требованиям безопасности информации всех основных регуляторов страны.

«Astra Linux Common Edition» хоть и является бесплатной для физических лиц, но на данный момент неактуальна, и не лицензируется для использования юридическими лицами. «Astra Linux Special Edition» является полностью платной и её стоимость варьируется от уровня защищенности системы.

## Проектная часть

### Функционал конечной системы

Получившаяся в результате сборки система должна обладать следующим характеристиками:

* Авторизация пользователей по домену «Windows Active Direcorty»;
* Возможность монтирования сетевых директорий доменных пользователей;
* Работа с принтерами и сканерами;
* Возможность запуска приложений, написанных для «Windows»;
* Невозможность авторизации локальными пользователями (за исключением Администратора);
* Наличие программ для виртуализации;
* Тема оформления схожая с «Windows 11»;
* Наличие программ для работы с документами, таблицами, графикой, мультимедиа, базами данных, носителями данных;
* Присоединение к домену «Windows Active Directory» сразу после установки системы;
* .....

### Обзор важных компонентов системы

#### Samba

Ключевым компонентом системы, обеспечивающим подключение к домену «Windows Active Directory», возможность монтирования сетевых папок и взаимодействие с принтерами и сканерами, является Samba. Samba – пакет программ, являющийся свободной реализацией сетевого протокола SMB, изначально разработанный Триджеллом Эндрю. Samba предоставляет файловые сервисы и сервисы печати, а также может интегрироваться с доменом «Microsoft Windows Server», и как контроллер, и как член домена.

Samba работает на большинстве Unix-like подобных системах, таких как Linux, BSD, Solaris, macOS и др. Является стандартом практически для всех Linux дистрибутивов, в которых обычно включается как базовый компонент.

Название Samba происходит от SMB (Server Message Block), названия проприетарного протокола, использующегося в сетевой файловой системе Microsoft Windows.

Для аутентификации пользователей Samba может использовать либо Kerberos, либо NTLM протоколы. Поскольку начиная с версии Windows 2000 Kerberos используется как стандартный протокол аутентификации, рассмотрим его подробнее.

#### Kerberos

Kerberos – сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними. Kerberos выполняет аутентификацию в качестве службы аутентификации доверенной третьей стороны, используя криптографический ключ. Построен на криптографии симметричных ключей и требует наличия центра распределения ключей. Расширения Kerberos могут обеспечить использование криптографии с открытым ключом на определённых этапах аутентификации.

Центр распределения ключей (KDС) — это служба, работающая на физически защищённом сервере. Центр хранит базу данных с информацией об учётных записях всех клиентов сети. Вместе с информацией о каждом абоненте в базе центра распределения ключей хранится криптографический ключ, известный только этому абоненту и службе центра. Этот ключ служит для связи клиента с центром.

Процесс аутентификации пользователя по протоколу Kerberos можно описать следующим образом:

1. Запрос к серверу аутентификации. Клиент отправляет незашифрованный запрос  аутентификации KDC серверу;
2. Ответ сервера аутентификации. Если пользователь, отправивший запрос не найден в базе данных, то он не может быть авторизован, и процесс аутентификации прекращается. Если же он был найден, то сервер аутентификации выдает клиенту TGT (Ticket Grant Ticket) – билет на получение билетов и ключ сессии;
3. Как только клиент прошел процедуру аутентификации сервером KDS, он обращается к TGS (Ticket Granting Server) – серверу выдачи мандатов и разрешений. Запрос должен сопровождаться TGT, полученном на предыдущем этапе;
4. Если TGS может осуществить аутентификацию клиента, он отправляет реквизиты для входа и билет обратно клиенту. Эта операция шифруется ключом сессии;
5. Теперь клиент авторизован и может совершать запросы к сервисам.

#### PAM

Linux Pluggable Authentication Modules (PAM, подключаемые модули аутентификации) — набор библиотек, позволяющих настроить методы аутентификации пользователей в UNIX-системах. Он предоставляет возможность гибко и централизованно переключать методы аутентификации для защищенных приложений, используя конфигурационные файлы вместо изменения кода самих приложений. Является одной из частей стандартного механизма обеспечения безопасности UNIX-систем.

Linux-PAM разделяет задачи аутентификации на четыре независимые группы:

* модуль «account» проверят, что указанная учетная запись является допустимой целью аутентификации;
* модуль «authentication» проверят личность пользователя путем запроса пароля или другого секрета;
* модуль «password» отвечает за обновление паролей и, как правило, связаны с модулями, используемыми на этапе аутентификации. Также используются для проверки надежности паролей;
* модуль «session» определяет действия, которые исполняются в начале и конце каждой сессии пользователя. Сессия начинается, когда пользователь успешно прошел аутентификацию.

Поскольку в разрабатываемой системе требуется аутентификация как локальных пользователей, так и пользователей домена Windows Active Directory, необходимо так настроить каждый PAM модуль, чтобы аутентификация одних не мешала аутентификации других.

#### Winbind

Winbind — Name Service Switch «демон» для распознания имен Micfrosoft Windows, являющийся частью пакета Samba. Предоставляет набор сервисов для Name Service Switch, присутствующей в большинстве современных библиотек C, произвольных приложений PAM, а также для самой Samba.

The Name Service Switch позволяет позволяет получать информацию о пользователях и системную информацию из различных баз данных, таких как NIS и DNS. Точное поведение может быть настроено в файле /etc/nsswitch.conf. Пользователи и группы выделяются по мере их разрешения в диапазоне идентификаторов, указанных администратором системы Samba.

Сервис, предоставляемый winbindd называется «winbind» и может быть использован для разрешения информации о группах и пользователях Windows Server. Сервис также предоставляет механизм аутентификации через соответствующий PAM модуль.

Существует множество способов собрать свою собственную операционную систему на базе ядра «Linux». Среди них можно выделить следующие: «Linux From Scratch (LFS)», «Buildroot», «SUSE Studio Express», «Cubic» и т. д. Разберем возможности каждой из них.

.....

## Практическая часть

Для реализации поставленной задачи в первую очередь понадобится утилита «live-build». Скачать её можно из официальных репозиториев дистрибутива «Debian» с помощью команды «sudo apt install live-build» на компьютере с уже установленной системой «Debian» или его производными, однако для корректной работы лучше использовать ту же систему, на основе которой будет осуществляться сборка. Для локального (?) тестирования потребуется программа для виртуализации, с помощью которой можно будет запустить виртуальную машину с собранной системой.

«live-build» позволяет собрать систему, которую можно запустить в «live» режиме (не устанавливая на диск) и далее установить её с того же носителя.