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 сборка 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 операционной системе, формируется список предустановленных программ и настроек. 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 утилиты «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 5](#_Toc1)

[Перечень сокращений и обозначений 6](#_Toc2)

[ВВЕДЕНИЕ 7](#_Toc3)

[Основная часть 10](#_Toc4)

[1 Аналитическая часть 10](#_Toc5)

[1.1 Описание разрабатываемой системы 10](#_Toc6)

[1.2 Обзор аналогов 11](#_Toc7)

[1.2.1 ALT Linux 11](#_Toc8)

[1.2.2 Astra Linux 11](#_Toc9)

[1.2.3 РЕД ОС 12](#_Toc10)

[1.2.4 РОСА ОС 13](#_Toc11)

[1.2.5 Сравнительная таблица аналогов 13](#_Toc12)

[2 Проектная часть 15](#_Toc13)

[2.1 Функционал разрабатываемой системы 15](#_Toc14)

[2.2 Обзор важных компонентов системы 16](#_Toc15)

[2.2.1 Samba 16](#_Toc16)

[2.2.2 Kerberos 17](#_Toc17)

[2.2.3 PAM 19](#_Toc18)

[2.2.4 Winbind 20](#_Toc19)

[3 Практическая часть 21](#_Toc20)

[3.1 Структура конфигурации для live-build 21](#_Toc21)

[3.1.1 Директория package-lists 21](#_Toc22)

[3.1.2 Директория archives 22](#_Toc23)

[3.1.3 Директория includes.chroot 24](#_Toc24)

[3.1.4 Директория hooks 24](#_Toc25)

[3.1.5 Директория preseed 25](#_Toc26)

[3.2 Параметры сборки системы 25](#_Toc27)

[3.3 Настройка системы в процессе сборки 26](#_Toc28)

[3.4 Настройка подключения к домену и доменной авторизации 27](#_Toc29)

[3.4.1 Настройка DNS 28](#_Toc30)

[3.4.2 Настройка синхронизации времени 30](#_Toc31)

[3.4.3 Настройка авторизации через Kerberos 31](#_Toc32)

[3.4.4 Настройка Samba 33](#_Toc33)

[Заключение 36](#_Toc34)

[Список использованных источников 37](#_Toc35)

[Приложения 38](#_Toc36)

# Термины и определения

Active Direcory – службы каталогов корпорации Microsoft для операционных систем семейства Windows Server;

Доменная служба Active Directory – решение Microsoft для операционных систем Windows Server, позволяющая загружать, группировать и хранить информацию об объектах ИТ-инфраструктуры;

Дистрибутив GNU/Linux – общее определение и название операционных систем, использующих ядро Linux, готовых для конечной установки на пользовательское и серверное оборудование;

Debian – свободный дистрибутив GNU/Linux.

LiveCD (Live) – операционная система, которая загружается со сменного носителя (компакт-диска или USB-накопителя);

Критерии Debian по определению свободного ПО (англ. Debian Free Software Guidelines) – набор правил, по которым проект Debian определяет, какие лицензии являются свободными, и следовательно, приемлемыми для операционной системы Debian.

KDE

PAM

Flatpak

Flathub

Kerberos

Samba

DNS

NetworkManager

KDC

TGS

демон

# Перечень сокращений и обозначений

ЮГУ – Югорский государственный университет

AD – Active Directory

ОС – операционная система

Домен – Доменная служба Active Directory

ВКР – выпускная квалификационная работа

GPU – графический процессор

CPU – центральный процессор

PAM

DNS

NTP

UTC

ID

SID

RTC

CLI

SSH

# 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

### Описание 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 собираемой системы была выбрана стабильная версия дистрибутива Debian. Таким образом, конечная система 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;
* Возможность собрать систему, работающую в Live режиме.

### 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.

В «Astra Linux Common Edition» доступно три режима защищенности: «базовый» - «Орёл», «усиленный» - «Воронеж» и «максимальный» - «Смоленск». Начиная с режима «Усиленный», интерфейсы средств защиты информации «Astra Linux Special Edition» существенно сужают поверхность атаки, и формируют основной рубеж обороны от вредоносного внешнего воздействия.

«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 режима защищенности системы.

#### РЕД ОС

РЕД ОС — это российская операционная система на базе ядра Linux, которая разработана компанией «РЕД СОФТ» с использованием открытых исходных кодов и собственных решений. РЕД ОС имеет ряд преимуществ, которые делают её привлекательной для различных сфер применения, особенно для государственных и корпоративных заказчиков.

Операционная система поставляется в двух конфигурациях – РЕД ОС «Рабочая станция» и РЕД ОС «Сервер», и в двух редакциях – сертифицированная и стандартная. Сертифицированная прошла ряд испытаний в системе сертификации средств защиты информации. Стандартная система предназначена для серверов и рабочих станций и распространяется свободно, бесплатно для некоммерческого использования. Сертифицированная редакция является платной и требует приобретения лицензии.

РЕД ОС позволяет настраивать различные параметры системы, такие как интерфейс, сеть, безопасность, обновления и т.д. Система поддерживает различные графические оболочки, такие как «Mate» и «Cinnamon» и «Gnome».

#### РОСА ОС

Rosa Linux — линейка дистрибутивов Linux (изначально основанных на Mandriva), разработку которых ведёт российская компания «НТЦ ИТ РОСА». Так же как и РЕД ОС, представлена в двух версиях – для серверов и рабочих станций. Имеется несколько редакций: РОСА «Кобальт», РОСА «ХРОМ» и РОСА «КОБАЛЬТ». РОСА «ФРЕШ» – полностью бесплатная версия ОС для дома с обширным набором предустановленного ПО. РОСА «КОБАЛЬТ» и «ХРОМ» – универсальные операционные системы, предназначенные для оснащения рабочих мест пользователей в корпоративной среде. Редакция «КОБАЛЬТ» оснащена дополнительными средствами для защиты от внешних и внутренних угроз. В качестве основной графической среды рабочего стола используется KDE.

Все редакции системы, кроме «ФРЕШ», являются платными.

#### Сравнительная таблица аналогов

Для того, чтобы подытожить всю информацию об аналогах, составим таблицу, в которой наглядно будут видны преимущества и недостатки каждого варианта:

Таблица 1: Сравнение аналогов

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | Astra Linux | ALT Linux | РЕД ОС | РОСА ОС | Ugrach |
| Стоимость лицензии, руб./год | Для физических лиц | - | Бесплатно | Бесплатно | Бесплатно | Бесплатно для ЮГУ |
| Для юридических лиц | 8950 | 5280 | 4600 | 4400 | Бесплатно для ЮГУ |
| Стоимость поддержки | | 4200 | 2160 | 2500 | 3300 | Бесплатно для ЮГУ |
| Возможность доменной авторизации «из коробки» | | Нет | Да | Да | Да | Да |
| Программное обеспечение | | Офис, почта, веб-сервер, средства работы с изображениями | Офис, почта, веб-сервер, средства работы с изображениями | Офис, почта, веб-сервер, средства работы с изображениями | Офис, почта, веб-сервер, средства работы с изображениями | Заточено строго под потребности университета |
| Семейство ОС | | Debian/Linux | Mandrake/Linux | Red Hat | Mandriva/Linux | Debian/Linux |

Как видим, все аналоги, кроме Astra Linux, предоставляют доменную авторизацию «из коробки», обладают набором жизненно необходимых приложений, и имеют сравнительно невысокую стоимость поддержки. Однако возможность включить в Ugrach набор приложения и настроек, специфичных только для ЮГУ, и отсутствие необходимости приобретать лицензию являются сильными аргументами в пользу выбора разрабатываемой системы.

## Проектная часть

### Функционал разрабатываемой системы

Для того, чтобы сотрудники и студенты могли успешно пользоваться системой, она должна удовлетворять ряду требований. Требования были получены от научного руководителя данной работы. Приведем их ниже:

* Возможность ввода машины в домен с помощью специальной консольной утилиты;
* Авторизация пользователей по домену;
* Возможность монтирования сетевых директорий доменных пользователей;
* Работа с принтерами и сканерами;
* Возможность запуска приложений, написанных под Windows;
* Невозможность авторизации локальными пользователями (за исключением Администратора);
* Наличие программ для виртуализации;
* Тема оформления схожая с Windows 10;
* Наличие программ для работы с документами, таблицами, графикой, мультимедиа, базами данных, носителями данных.

### 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

### Структура конфигурации для live-build

Для сборки системы сначала необходимо составить конфигурацию, из которой утилита lb build уже будет собирать систему. Она представляет из себя набор вложенный директорий, содержащих файлы, из которых читается конфигурация, а также файлы, которые будут включены в конечную файловую систему.

В корне конфигурации находятся директории auto и config. Директория auto содержит sh-скрипты, включающие в себя параметры, которые применяются при вызове утилит пакета live-build. Директория config содержит основную конфигурацию и состоит из нескольких поддиректорий, каждая из которых отвечает за определенные компоненты собираемой системы. Рассмотрим её структуру подробно.

#### Директория package-lists

Директория package-lists содержит списки пакетов, которые будут включены в конечную систему. Может состоять из одного или нескольких файлов, имеющих расширение .list.chroot и .list.binary. Пакеты из файлов с расширением .list.chroot попадают как в устанавливаемую, так и в live систему. Пакеты из файлов с расширением .list.binary включаются только на binary стадии и, как следствие, попадают только в live систему.

Название каждого пакета в файле должно быть с новой строки, а также не должно содержать синтаксических ошибок. В противном случае он не будет найдет и, либо не будет включен в систему, либо прервет сборку с ошибкой.

В файлах допускается использование комментариев и условных конструкций. Например можно включить те или иные пакеты в сборку в зависимости от указанной в конфигурации архитектуры:

#if ARCHITECTURES i386 amd64

memtest86+

#endif

В данном пример в систему будет включена программа для проверки целостности оперативной памяти memtest86+, если в параметрах сборки указаны архитектуры i386 либо amd64.

В текущей конфигурации используется следующий набор файлов со списками пакетов:

* development.list.chroot – программы для разработки ПО и моделирования;
* graphics.list.chroot – программы для работы с графикой;
* media.list.chroot – программы для работы с мультимедиа;
* office.list.chroot – офисный пакет и прочие программы для работы с документами разных форматов;
* virtualization.list.chroot – программы для виртуализации;
* system.list.chroot – системные программы и утилиты;
* games.list.chroot – драйвера для GPU и игровые лаунчеры (также могут использоваться для запуска Windows приложений).

#### Директория archives

Директория archives содержит список дополнительных репозиториев, с которых live-build может скачивать пакеты. При добавлении соответствующего репозитория нужный пакет можно прописать в package-lists также, как и все остальные пакеты. После сборки прописанные репозитории попадают в директорию /etc/apt/sources.list.d/, где хранятся все дополнительные репозитории в Debian системе.

Названия файлов с репозиториями имеют следующий шаблон:

(название\_репозитория).list.(стадия\_сборки)

Название может быть любым, но лучше, чтобы оно отражало содержимое репозитория во избежании путаницы. В качестве стадии сборки могут быть указаны либо chroot, либо binary. От неё зависит, на каком этапе сборки пакеты будут установлены в систему, и, как следствие, наличие или отсутствие соответствующих программ в live системе.

Само содержимое файлов должно иметь следующую структуру:

(тип\_архива) (url репозитория) (псевдоним\_релиза) [ветка...]

Тип архива может быть либо deb, либо deb-src. deb указывает на бинарные пакеты, а deb-src – на пакеты с исходным кодом. В качестве псевдонима релиза указывается одно из названий стабильных релизов Debian. Ветки репозиториев могут быть следующими:

* main – пакеты, считающиеся частью дистрибутива Debian. Являются полностью свободными для любого использования;
* contrib – свободные пакеты, имеющие зависимости, которые могут быть не свободными;
* non-free – не свободные пакеты;
* nom-free-firmware – не свободные пакеты драйверов устройств.

Пример файлы репозитория Visual Studio Code:

deb https://packages.microsoft.com/repos/vscode stable main

Помимо самих списков репозиториев необходимо также добавить соответствующие ключи. Это текстовые файлы, содержащие ключи в формате PGP. Шаблон их именования имеет почти такую же структуру:

(название\_репозитория).key.(стадия\_сборки)

Ключи, также как и списки репозиториев, попадают в конечную систему. За счёт этого пакеты, скачанные в процессе сборки от туда, будут обновляться вместе со всеми остальными после установки системы.

#### Директория includes.chroot

Эта директория содержит файлы, которые буду включены в корневую директорию конечной системы на этапе chroot. Здесь в основном содержатся конфигурации для работы некоторых программ системы, в том числе всех программ, отвечающих за взаимодействие с доменом. Её содержимое будет подробнее рассмотрено далее.

Также допустимо наличие директории includes.binary, файлы из которой попадают в образ live системы, но поскольку для нашей системы в ней нет особой необходимости, в конфигурацию она включена не была.

#### Директория hooks

Данная директория может состоять из поддиректорий hooks/normal и hooks/live, содержащих скрипты, исполняемые на этапе сборки системы. Они позволяют произвести более точную настройку. Директория hooks/normal содержит скрипты, исполняемые при сборки регулярной системы, а hooks/live – при сборке live системы.

Шаблон именования файлов имеет следующий вид:

(номер)(название\_скрипта).(этап сборки)

Номер – это четырёх-значное число, указывающие на очередность исполнения скрипта. Чем оно больше, тем позднее скрипт будет выполнен. Этапами сборки могут быть либо chroot, либо binary, указывающие на соответствующие этапы сборки системы.

Содержание данных скриптов будет подробнее рассмотрено далее.

#### Директория preseed

Директория preseed содержит файл preseed.cfg, которые позволяет предопределить параметры установщика системы. Это позволяет практически полностью автоматизировать процесс установки.

### Параметры сборки системы

Параметры для сборки системы хранятся в файле auto/config. Содержимое файла config представлено ниже:

#!/bin/sh

set -e

lb config noauto \

—apt-recommends true \

—apt-indices true \

—architectures amd64 \

—archive-areas "main contrib non-free non-free-firmware" \

—binary-images iso-hybrid \

—binary-filesystem fat32 \

—bootappend-live "boot=live components locales=ru\_RU.UTF-8 keyboard-layouts=ru,us keyboard-options=grp:alt\_shift\_toggle timezone=Asia/Yekaterinburg" \

—clean \

—color \

—debian-installer live \

—debian-installer-distribution bookworm \

—debian-installer-gui true \

—debootstrap-options "--include=apt-transport-https,ca-certificates,openssl" \

—distribution bookworm \

—firmware-binary true \

—firmware-chroot true \

—security true \

—iso-volume ugrach \

—image-name ugrach.beta \

—linux-packages "linux-image linux-headers" \

—mirror-bootstrap "http://mirror.yandex.ru/debian/" \

—mirror-chroot "http://mirror.yandex.ru/debian/" \

"${@}"

Рассмотрим основные параметры:

* architectures amd64 – архитектура системы
* archive-areas "main contrib non-free non-free-firmware" – ветки репозитория, откуда будут скачиваться пакеты. Установлены все ветки, чтобы в процессе сборки были установленны проприетарные программы и драйвера.
* bootappend-live "boot=live components locales=ru\_RU.UTF-8 keyboard-layouts=ru,us keyboard-options=grp:alt\_shift\_toggle timezone=Asia/Yekaterinburg" – установка дополнительных параметров для live системы: русская локализация, раскладки клавиатуры, комбинация для переключения раскладок и регион.
* debian-installer live – тип установщика. Данная опция добавляет установщик в меню live системы.
* debian-installer-gui true – версия установщика. Добавляется графический вариант. Текстовая версия установщика при этом также присутствует.
* distribution bookworm – релиз Debian. Используется последний – Debian 12 «Bookworm»
* mirror-bootstrap "http://mirror.yandex.ru/debian/" – репозиторий, используемый на bootstrap стадии сборки. В данном случае используется репозиторий Яндекса.
* mirror-chroot "http://mirror.yandex.ru/debian/" – репозиторий, используемый на chroot стадии сборки. Также используются репозитории Яндекса.
* binary-images iso-hybrid – тип собираемого образа. Используется iso-hybrid для возможности записи на USB носитель в будущем.

### Настройка системы в процессе сборки

Для настройки системы в процессе сборки используются скрипты из директории config/hooks/normal. Рассмотрим, что делает каждый из них:

* install-we10xos-theme – скрипт для установки темы оформления KDE.

#!/bin/sh

set -e

git clone https://github.com/yeyushengfan258/We10XOS-kde.git

cd We10XOS-kde

./install.sh

cd ../

rm -rf We10XOS-kde

Сначала клонируем файлы темы из репозитория. Затем переходим в директорию с файлами и запускаем скрипт установки. После успешной установки можем удалить клонированный репозиторий.

* pam-auth-update – скрипт для настройки модулей PAM. Необходим для корректной работы авторизации с систему как доменных пользователей, так и локальных (Администратора).

#!/bin/bash

set -e

sudo pam-auth-update --disable krb5 --enable unix winbind systemd mkhomedir --force

С помощью специальной утилиты для настройки PAM включаемый все нужные нам модули: unix – для авторизации локальных пользователей, winbind – для авторизации доменных пользователей, systemd – для регистрации сессий пользователя в менеджер входа в систему systemd и mkhomedir – для создания домашнего каталога пользователя при входе в систему, если таковой отсутствует.

* add-flathub-repo – скрипт для добавления flathub репозитория в систему для установки flatpak приложений.

#!/bin/sh

set -e

flatpak remote-add --if-not-exists flathub https://dl.flathub.org/repo/flathub.flatpakrepo

### Настройка подключения к домену и доменной авторизации

Для реализации доменной авторизации в систему и взаимодействия с сетевыми папками используется пакет программ Samba, система сетевой аутентификации Kerberos и служба Winbind пакета Samba.

В ЮГУ имеется два домена: edu.ugrasu – студенческий домен, и ugrasu.ru – домен для преподавателей. Необходимо настроить систему так, чтобы она могла взаимодействовать с каждым из них. Машина не может одновременно находится в двух доменах, поэтому необходимо реализовать простой способ выхода из одного домена и присоединения к другому. Настройку по умолчанию произведем для преподавательского домена.

Для упрощения этой задачи был написан скрипт «joindomain», отдельные части которого будут рассмотрены в главах далее.

#### Настройка DNS

Для того, чтобы система смогла найти контроллеры домена, необходимо произвести настройку DNS. На установленной системе это можно сделать в файле /etc/resolf.conf. Записи DNS серверов в нём имеют следующий вид:

nameserver (адрес\_сервера)

Директива nameserver указывает на адрес DNS сервера, используемого при разрешении доменных имен. Если от указанного DNS сервера не был получен IP адрес доменного имени, проверяется следующий по списку.

В ЮГУ имеется два контроллера домена: dc.edu.ugrasu – с адресом 192.168.0.200, и pdc.ugrasu.ru – с адресом 192.168.0.128. Так как настройку по умолчанию мы делаем для ugrasu.ru, адрес его контроллера домена должен находится в списке выше.

Однако нельзя просто добавить файл с необходимым содержимым в config/includes/chroot/etc/resolf.conf, поскольку NetworkManager будет перезаписывать его при каждом запуске системы. В этом случае необходимо произвести настройку самого NetworkManager’a, чтобы при каждом запуске он записывал в /etc/resolf.conf DNS адреса контроллеров домена. Сделать это можно в файле /etc/NetworkManager/conf.d/dns-servers.conf. Добавим файл config/includes.chroot/etc/NetworkManager/conf.d/dns-servers.conf со следующим содержимым:

[global-dns-domain-\*]

servers=192.168.0.200,192.168.6.128

Секция global-dns-domain позволяет определить глобальную конфигурацию DNS для конкретного домена. \* в конце указывает на то, что применить это нужно ко всем доменам. Таким образом, после установки сисетмы получим следующий файл /etc/resolf.conf:

# Generated by NetworkManager

nameserver 192.168.0.200

nameserver 192.168.6.128

После чего доменные имена ugrasu.ru и edu.ugrasu будут успешно разрешаться. За разрешения всех остальных доменных имен отвечают DNS службы контроллеров домена.

Помимо файла /etc/resolf.conf необходимо также настроить файл /etc/hosts так, чтобы в нём была запись с полным доменным именем компьютера и коротким именем хоста. Здесь имеются определенные подводные камни. Дело в том, что lb build в процессе сборки переопределяет содержимое этого файла, поэтому мы не сможем просто добавить файл с нужным содержимым в конфигурацию. В отличие от /etc/resolf.conf, /etc/hosts не генерируется NetworkManagerom’ом, так что можно внести необходимые изменения прямо перед подключением к домену. Сделаем это в joindomain:

function configure\_hosts(){

sudo sed -i "s/.\*127.0.0.1.\*/127.0.0.1 $(hostname).$1 localhost/" /etc/hosts

sudo sed -i "s/.\*127.0.1.1.\*/127.0.1.1 $(hostname).$1 $(hostname)/" /etc/hosts

sudo sed -i "0,/::1/ s/.\*::1.\*/::1 $(hostname).$1 localhost ip6-localhost ip6-loopback/" /etc/hosts

}

С помощью утилиты редактирования текста sed подменяем в файле все исходные записи на нужные. Команда «$(hostname)» вернет нам имя хоста, указанное пользователем во время установки. Параметр «$1» передаётся в функцию и содержит название домена. После подключения компьютера с именем хоста «ugrach» к домену «ugrasu.ru» файл /etc/hosts будет иметь следующий вид:

127.0.0.1 debian.ugrasu.ru localhost

127.0.1.1 debian.ugrasu.ru debian

# The following lines are desirable for IPv6 capable hosts

::1 debian.ugrasu.ru localhost ip6-localhost ip6-loopback

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

#### Настройка синхронизации времени

Далее необходимо произвести настройку синхронизации времени между компьютером с контроллером домена. В случае, если разница во времени между ними будет более пяти минут, Kerberos не сможет установить подключение.

Для этой задачи будем использовать программу Chrony, которая является одной из реализация протокола NTP и может подключиться к NTP службе контроллера домена. Состоит из демона chronyd, CLI chronyc и конфигурационного файла chrony.conf. Демон автоматически включается после установки пакеты, поэтому это не нужно делать вручную. Файл хранится в /etc/chrony/chrony.conf, поэтому добавим соответствующий файл в config/includes.chroot/. Он содержит следующие настройки:

keyfile /etc/chrony/chrony.keys

driftfile /var/lib/chrony/chrony.drift

log tracking measurements statistics

logdir /var/log/chrony

maxupdateskew 100.0

hwclockfile /etc/adjtime

rtcsync

makestep 1 3

bindcmdaddress 0.0.0.0

bindcmdaddress ::

server dc.ugrasu.ru iburst

server pdc.edu.udgrasu iburst

* keyfile – расположение файла, содержащего пары ID/ключ для NTP аутентификации;
* driftfile – расположение файла, в котором хранится информация о скорости, с которой системные часы опережают реальное время или же отстают от него;
* log tracking measurements statistics – данная настройка указывает, какую именно информацию нужно логировать;
* logdir – директория, в которой сохраняются логи;
* maxupdateskew – устанавливает порог, при котором отставание или опережение реального времени системным считается недостаточно надёжным для использования;
* hwclockfile – расположение файла adjtime, который используется программой hwclock в Linux, позволяющей определить, использует ли компьютер местное время или UTC;
* rtcsync – включает синхронизацию времени между ядром и RTC;
* makestep – позволяет установить системные часы на необходимое значение вместо постепенной настройки сразу после старта системы, когда разница во времени с контроллером домена может быть ощутимой;
* bindcmdaddress – указывает, на каких интерфейса принимать пакеты. В нашем случае на всех;
* server – доменное имя источника, с которым нужно синхронизировать время. В нашем случае адреса контроллеров домена.

При правильной настройке синхронизации времени присоединение к домену и вход доменных пользователей в систему должен происходить успешно и без задержек.

#### Настройка авторизации через Kerberos

Поскольку для авторизации пользователей домена используется протокол Kerberos, необходимо осуществить его настройку. Файл конфигурации находится в /etc/krb5.conf. Также включим его в конфигурацию для lb build, добавив в config/includes.chroot/etc/krb5.conf. Файл имеет следующее содержание:

[libdefaults]

default\_realm = UGRASU.RU

dns\_lookup\_realm = false

dns\_lookup\_kdc = true

default\_tgs\_enctypes = rc4-hmac des-cbc-crc des-cbc-md5

defaukt\_tkt\_enctypes = rc4-hmac des-cbc-crc des-cbc-md5

permitted\_enctypes = rc4-hmac des-cbc-crc des-cbc-md5

allow\_weak\_crypto = true

Секция [libdefaults] содержит основные настройки для Kerberos. Рассмотрим значение параметров этой секции:

* default\_realm – адрес KDC. Контроллера домена;
* dns\_lookup\_realm – данный параметр позволяет включить или отключить поиск kerberos-имени домена через DNS;
* dns\_lookup\_realm – поиск kerberos-настроек домена через DNS;
* default\_tgs\_enctypes – поддерживаемые алгоритмы шифрования для TGS;
* defaukt\_tkt\_enctypes – поддерживаемые алгоритмы шифрования для TGT;
* permitted\_enctypes – определяет все поддерживаемые алгоритмы шифрования для ключей сессий;
* allow\_weak\_crypto – определяет, можно ли использовать слабые алгоритмы шифрования.

При правильной настройке Kerberos, пользователь должен иметь возможность получить TGT, выполнив команду «kinit [(имя\_пользователя)@(имя\_домена](http://username@DOMAIN.COM))». Выполнив команду klist можно вывести список всех TGT, и убедиться в том, что билет был действительно получен

???

#### Настройка Samba и Winbind

Самым важным этапом в настройке подключения к домену является конфигурация Samba, так именно она отвечает за присоединение к домену и взаимодействие с ним. Также необходимо настроить проецирование групп и пользователей домена в систему, чтобы можно было совершать операции, завязанные на них. Например, назначения пользователей домена владельцами директорий и файлов. За это отвечает Winbind. Оба этих компонента настраиваются в одном файле – /etc/samba/smb.conf. Добавим его в конфигурацию lb build в config/includes.chroot/etc/samba/smb.conf. Рассмотрим его настройки:

[global]

workgroup = UGRASU

security = ADS

realm = UGRASU.RU

kerberos method = system keytab

winbind use default domain = Yes

winbind expand groups = 1

winbind enum users = yes

winbind enum groups = yes

winbind cache time = 36

idmap config \* : range = 20000-40000

template homedir = /home/%D/%U

template shell = /usr/bin/false

obey pam restrictions = yes

В секции [global] указываются параметры, применяемые к клиенту в целом и являющиеся значениями по умолчанию для всех остальных разделов, где явно не определенны соответствующие элементы.

Значения параметров:

* workgroup – указывает, в какой группе будут находится пользователи домена, авторизовавшиеся в системе. Этот параметр долежн совпадать с рабочей группой контроллера домена;
* security – указывает на то, как клиенты взаимодействуют с Samba. Если указано значение ADS, то Samba будет взаимодействовать как член домена. Для работы в этом режиме на клиенте должен быть установлен и настроен Kerberos;
* realm – указывает на KDC сервер, который нужно использовать при аутентификации пользователей;
* kerberos method – указывает на то, как проверяются TGT. При значении параметра «system keytab» используется локальная таблица ключей;
* winbind use default domain – указывает, нужно ли winbindd обрабатывать пользователей, не имеющих названия домена в их имени;
* winbind expand groups – управляет максимальной глубиной, которую будет проходить winbindd при выравнивании членства во вложенных группах пользователей домена, так как Linux не имеет вложенных групп. При значении параметра «0» группы пользователей ну будут запрашиваться вовсе;
* winbind enum users - определяет, будет ли winbind перечислять пользователей домена;
* winbind enum groups - определяет, будет ли winbind перечислять группы домена;
* winbind cache time – определяет время кеширования информации о пользователях и группах перед повторным запросом;
* idmap config \* – отвечает за сопоставление между SID’ами пользователей домена и ID’ами Linux системы. При текущем значении параметра пользователям системы будут присваиваться ID из диапазона 20000-40000;
* template homedir – расположения и шаблон создания домашних директория доменных пользователей. Параметр «%D» подставляет имя домена и используется по причине того, что системе предстоит взаимодействовать с двумя доменами. Параметр «%U» подставляет имя пользователя домена;
* template shell – оболочка входа в систему, которая будет присваиваться пользователям домена. Поскольку им нет необходимости входить в систему через терминал или подключаться по SSH, оболочка для них отключена;
* obey pam restrictions – указывает, нужно ли подчиняться настройкам PAM по управлению сессиями и учётными записями.

# Заключение

# Список использованных источников

# Приложения

sh-скрипты build, clean и config, вызывающиеся при запуске утилит lb build, lb clean и lb config соответственно. Они содержат список параметров, которые будут применены при вызове каждой конкретной утилиты, что позволяет нам не прописывать их при всяком вызове.

В файле build мы перенаправляем вывод lb build в файл build.log для дальнейшего изучения логов сборки и отслеживания возможных ошибок.

lb build noauto "${@}" 2>&1 | tee build.log

В файле clean помимо параметров для утилиты lb clean содержатся команды для удаления оставшихся продуктов сборки. Это позволяет запускать последующие сборки «с нуля».

Наибольший интерес представляет файл config. В нём прописаны все параметры, применяемые во время сборки системы.

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.